

网络安全专用产品指南

第二版（下册）



中国网络安全产业联盟
2025年1月

序

2017年6月1日,《中华人民共和国网络安全法》正式实施,明确规定“网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求,由具备资格的机构安全认证合格或者安全检测符合要求后,方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录,并推动安全认证和安全检测结果互认,避免重复认证、检测”。为落实《中华人民共和国网络安全法》有关规定,国家互联网信息办公室会同工业和信息化部、公安部、国家认监委等相关部门相继发布网络关键设备和网络安全专用产品目录,确定承担安全认证和安全检测任务的机构,明确认证检测结果统一发布流程,制定《信息安全技术网络安全专用产品安全技术要求》强制性国家标准。

为进一步加强网络安全专用产品安全管理,推动安全认证和安全检测结果互认,避免重复认证、检测,2023年4月和7月,国家互联网信息办公室会同相关部门联合发布《关于调整网络安全专用产品安全管理有关事项的公告》(以下简称《公告》),并更新《网络关键设备和网络安全专用产品目录》(以下简称《目录》)。《公告》明确要求,统一网络安全专用产品认证检测制度,自2023年7月1日起,停止颁发《计算机信息系统安全专用产品销售许可证》,停止执行政府采购领域信息安全产品强制认证要求。列入《目录》的数据备份与恢复产品、防火墙、入侵检测系统(IDS)等34类网络安全专用产品,需要按照《公告》要求进行安全认证或安全检测后,方可销售或者提供。

2024年,中国网络安全产业联盟(CCIA)启动《网络安全专用产品指南》(以下简称《指南》)编制工作,4月发布第一版,本书为第二版。《指南》第二版共收录了84家企业的391款产品,覆盖了《目录》所列的31类网络安全专用产品(除安全网络存储、信息过滤产品、数据销毁软件产品外),所收录的产品信息均更新至2024年12月底。

相较于第一版,《指南》第二版主要变化包括:新增了102款产品,涵盖27类网络安全专用产品;对74款变更了安全认证或安全检测结果证明的产品信息进行了更新;删除了95款计算机信息系统安全专用产品销售许可证超过有效期的产品。未来,CCIA将定期对《指南》进行更新和完善,以便用户单位能够及时获取最新的网络安全专用产品信息。

本册为《指南》下册,共收录了56家企业提供的191款产品,涉及统一威胁管理产品(UTM)、病毒防治产品、安全操作系统、公钥基础设施、网络安全态势感知产品、信息系统安全管理平台、网络型流量控制产品、负载均衡产品、抗拒绝服务攻击产品、终端接入控制产品、USB移动存储介质管理系统、文件加密产品、数据泄露防护产品、安全配置检查产品、运维安全管理产品、日志分析产品、身份鉴别产品、终端安全监测产品、电子文档安全管理产品等19类网络安全专用产品,其中每类产品均按企业名称首字母进行排序。

中国网络安全产业联盟

2025年1月

目 录

关于调整网络安全专用产品安全管理有关事项的公告.....	1
关于调整《网络关键设备和网络安全专用产品目录》的公告.....	3
网络关键设备和网络安全专用产品目录.....	5

统一威胁管理产品（UTM）

奇安信科技集团股份有限公司.....	9
启明星辰信息技术集团股份有限公司.....	12
天融信科技集团.....	17

病毒防治产品

安天科技集团股份有限公司.....	23
北京安信天行科技有限公司.....	26
北京猎鹰安全科技有限公司.....	32
北京威努特技术有限公司.....	37
奇安信科技集团股份有限公司.....	39
三六零数字安全科技集团有限公司.....	41
深信服科技股份有限公司.....	45
深圳市联软科技股份有限公司.....	48
沈阳东软系统集成工程有限公司.....	50
腾讯云计算（北京）有限责任公司.....	52
天融信科技集团.....	54
长扬科技（北京）股份有限公司.....	58
浙江远望信息股份有限公司.....	61

安全操作系统

北京威努特技术有限公司.....	65
绿盟科技集团股份有限公司.....	68

公钥基础设施

北京数字认证股份有限公司.....	73
北京天威诚信电子商务服务有限公司.....	75
北京信安世纪科技股份有限公司.....	77
奇安信科技集团股份有限公司.....	79
腾讯云计算（北京）有限责任公司.....	82
长春吉大正元信息技术股份有限公司.....	84
中移互联网有限公司.....	86

网络安全态势感知产品

安天科技集团股份有限公司.....	91
北京百度网讯科技有限公司.....	94
北京观成科技有限公司.....	96
北京国舜科技股份有限公司.....	100
北京珞安科技有限责任公司.....	102
北京威努特技术有限公司.....	104
北京长亭科技有限公司.....	107
福建省海峡信息技术有限公司.....	111
杭州迪普科技股份有限公司.....	113
杭州美创科技股份有限公司.....	116
绿盟科技集团股份有限公司.....	119
南京聚铭网络科技有限公司.....	122
奇安信科技集团股份有限公司.....	125
启明星辰信息技术集团股份有限公司.....	129
三六零数字安全科技集团有限公司.....	137
山东云天安全技术有限公司.....	139
深信服科技股份有限公司.....	141
神州灵云（北京）科技有限公司.....	146
沈阳东软系统集成工程有限公司.....	150
腾讯云计算（北京）有限责任公司.....	153
亚信安全科技有限公司.....	156

远江盛邦（北京）网络安全科技股份有限公司.....	159
长扬科技（北京）股份有限公司.....	161
浙江木链物联网科技有限公司.....	164

信息系统安全管理平台

北京安博通科技股份有限公司.....	169
北京珞安科技有限责任公司.....	175
北京天地和兴科技有限公司.....	177
北京威努特技术有限公司.....	179
福建中信网安信息科技有限公司.....	181
杭州安恒信息技术股份有限公司.....	184
杭州迪普科技股份有限公司.....	188
杭州美创科技股份有限公司.....	191
绿盟科技集团股份有限公司.....	193
南京众智维信息科技有限公司.....	195
奇安信科技集团股份有限公司.....	198
启明星辰信息技术集团股份有限公司.....	201
天融信科技集团.....	209

网络型流量控制产品

深信服科技股份有限公司.....	221

负载均衡产品

北京信安世纪科技股份有限公司.....	225
杭州迪普科技股份有限公司.....	228
绿盟科技集团股份有限公司.....	231
启明星辰信息技术集团股份有限公司.....	233
深信服科技股份有限公司.....	235
天融信科技集团.....	238

抗拒绝服务攻击产品

北京百度网讯科技有限公司.....	243

杭州迪普科技股份有限公司.....	246
绿盟科技集团股份有限公司.....	248
奇安信科技集团股份有限公司.....	251
启明星辰信息技术集团股份有限公司.....	254
天融信科技集团.....	256
网宿科技股份有限公司.....	259
亚信安全科技股份有限公司.....	264
远江盛邦（北京）网络安全科技股份有限公司.....	268
中新网络信息安全股份有限公司公司.....	270

终端接入控制产品

北京猎鹰安全科技有限公司.....	275
北京珞安科技有限责任公司.....	278
北京威努特技术有限公司.....	280
福建省海峡信息技术有限公司.....	283
奇安信科技集团股份有限公司.....	286
深信服科技股份有限公司.....	289
深圳市联软科技股份有限公司.....	291
深圳万物安全科技有限公司.....	294
腾讯云计算（北京）有限责任公司.....	297
长扬科技（北京）股份有限公司.....	299
浙江远望信息股份有限公司.....	302

USB 移动存储介质管理系统

北京珞安科技有限责任公司.....	307
北京威努特技术有限公司.....	309
长扬科技（北京）股份有限公司.....	311
浙江远望信息股份有限公司.....	314

文件加密产品

北京信安世纪科技股份有限公司.....	319
江苏敏捷科技股份有限公司.....	322

数据泄露防护产品

北京梆梆安全科技有限公司.....	327
北京明朝万达科技股份有限公司.....	330
北京数安行科技有限公司.....	332
北京天空卫士网络安全技术有限公司.....	335
北京亿赛通科技发展有限责任公司.....	338
杭州安恒信息技术股份有限公司.....	342
杭州亿格云科技有限公司.....	345
江苏敏捷科技股份有限公司.....	349
绿盟科技集团股份有限公司.....	351
奇安信科技集团股份有限公司.....	354
启明星辰信息技术集团股份有限公司.....	356
深圳市联软科技股份有限公司.....	359
天融信科技集团.....	362
远江盛邦（北京）网络安全科技股份有限公司.....	365

安全配置检查产品

北京威努特技术有限公司.....	369
启明星辰信息技术集团股份有限公司.....	371
深圳万物安全科技有限公司.....	375
远江盛邦（北京）网络安全科技股份有限公司.....	378

运维安全管理产品

北京珞安科技有限责任公司.....	385
北京威努特技术有限公司.....	387
北京亿赛通科技发展有限责任公司.....	389
北京云弈科技有限公司.....	392
北京长亭科技有限公司.....	395
福建省海峡信息技术有限公司.....	399
福建中信网安信息科技有限公司.....	402
杭州安恒信息技术股份有限公司.....	405
江苏保旺达软件技术有限公司.....	408

南京聚铭网络科技有限公司.....	410
奇安信科技集团股份有限公司.....	412
启明星辰信息技术集团股份有限公司.....	415
山东中网云安智能科技有限公司.....	418
上海派拉软件股份有限公司.....	420
深信服科技股份有限公司.....	423
深圳万物安全科技有限公司.....	426
沈阳东软系统集成工程有限公司.....	429
腾讯云计算（北京）有限责任公司.....	432
天融信科技集团.....	434
长扬科技（北京）股份有限公司.....	441
浙江远望信息股份有限公司.....	444

日志分析产品

北京安信天行科技有限公司.....	449
北京珞安科技有限责任公司.....	453
北京威努特技术有限公司.....	455
北京长亭科技有限公司.....	457
福建省海峡信息技术有限公司.....	461
福建中信网安信息科技有限公司.....	463
杭州安恒信息技术股份有限公司.....	466
南京聚铭网络科技有限公司.....	469
奇安信科技集团股份有限公司.....	472
启明星辰信息技术集团股份有限公司.....	475
深信服科技股份有限公司.....	478
天融信科技集团.....	482
亚信安全科技股份有限公司.....	489
浙江木链物联网科技有限公司.....	492
浙江远望信息股份有限公司.....	494

身份鉴别产品

北京数字认证股份有限公司.....	499

北京芯盾时代科技有限公司.....	501
杭州迪普科技股份有限公司.....	504
奇安信科技集团股份有限公司.....	506
启明星辰信息技术集团股份有限公司.....	508
上海派拉软件股份有限公司.....	511
天融信科技集团.....	515
长春吉大正元信息技术股份有限公司.....	517
长扬科技（北京）股份有限公司.....	520
浙江远望信息股份有限公司.....	523

终端安全监测产品

北京杰思安全科技有限公司.....	527
北京珞安科技有限责任公司.....	530
北京信安世纪科技股份有限公司.....	532
杭州安恒信息技术股份有限公司.....	536
杭州迪普科技股份有限公司.....	538
奇安信科技集团股份有限公司.....	541
厦门嘉佑安科信息技术有限公司.....	543
深圳市联软科技股份有限公司.....	546
神州灵云（北京）科技有限公司.....	548
腾讯云计算（北京）有限责任公司.....	551
天融信科技集团.....	553
亚信安全科技股份有限公司.....	556
浙江远望信息股份有限公司.....	558

电子文档安全管理产品

北京亿赛通科技发展有限公司.....	563
深圳市联软科技股份有限公司.....	566

关于调整网络安全专用产品安全管理有关事项的公告

2023 年第 1 号

为加强网络安全专用产品安全管理，推动安全认证和安全检测结果互认，避免重复认证、检测，依据《中华人民共和国网络安全法》、《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017 年第 1 号）、《国家认监委 工业和信息化部 公安部 国家互联网信息办公室关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告》（2018 年第 12 号）、《关于统一发布网络关键设备和网络安全专用产品安全认证和安全检测结果的公告》（2022 年第 1 号），现将调整网络安全专用产品安全管理有关事项公告如下：

一、自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构是指列入《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》的机构。

国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会发布更新《网络关键设备和网络安全专用产品目录》、《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》。

二、自 2023 年 7 月 1 日起，停止颁发《计算机信息系统安全专用产品销售许可证》（简称销售许可证），产品生产者无需申领。此前已经获得销售许可证的产品在有效期内可继续销售或者提供。

三、自 2023 年 7 月 1 日起，停止执行《关于调整信息安全产品强制性认证实施要求的公告》（原国家质检总局、财政部、国家认证认可监督管理委员会 2009 年第 33 号）和《财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知》（财库〔2010〕48 号）。

四、国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。

特此公告。

国家互联网信息办公室

工业和信息化部

公安部

财政部

国家认证认可监督管理委员会

2023 年 4 月 12 日

关于调整《网络关键设备和网络安全专用产品目录》的公告

2023 年第 2 号

依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门更新了《网络关键设备和网络安全专用产品目录》，现予以公布，自印发之日起施行。

2017 年国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会联合发布的《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017 年第 1 号）中的网络关键设备和网络安全专用产品目录同步废止。

特此公告。

国家互联网信息办公室
工业和信息化部
公安部
国家认证认可监督管理委员会
2023 年 7 月 3 日

网络关键设备和网络安全专用产品目录

一、网络关键设备

序号	设备类别	范围
1	路由器	整系统吞吐量 (双向) $\geq 12\text{Tbps}$ 整系统路由表容量 ≥ 55 万条
2	交换机	整系统吞吐量 (双向) $\geq 30\text{Tbps}$ 整系统包转发率 $\geq 10\text{Gpps}$
3	服务器 (机架式)	CPU 数量 ≥ 8 个 单 CPU 内核数 ≥ 14 个 内存容量 $\geq 256\text{GB}$
4	可编程逻辑控制器 (PLC 设备)	控制器指令执行时间 ≤ 0.08 微秒

二、网络安全专用产品

序号	产品类别	产品描述
1	数据备份与恢复产品	能够对信息系统数据进行备份和恢复,且对备份与恢复过程进行管理的产品。
2	防火墙	对经过的数据流进行解析,并实现访问控制及安全防护功能的产品。
3	入侵检测系统 (IDS)	以网络上的数据包作为数据源,监听所保护网络节点的所有数据包并进行分析,从而发现异常行为的产品。
4	入侵防御系统 (IPS)	以网桥或网关形式部署在网络通路上,通过分析网络流量发现具有入侵特征的网络行为,在其传入被保护网络前进行拦截的产品。
5	网络和终端隔离产品	在不同的网络终端和网络安全域之间建立安全控制点,实现在不同的网络终端和网络安全域之间提供访问可控服务的产品。
6	反垃圾邮件产品	能够对垃圾邮件进行识别和处理的软件或软硬件组合,包括但不限于反垃圾邮件网关、反垃圾邮件系统、安装于邮件服务器的反垃圾邮件软件,以及与邮件服务器集成的反垃圾邮件产品等。
7	网络安全审计产品	采集网络、信息系统及其组件的记录与活动数据,并对这些数据进行存储和分析,以实现事件追溯、发现安全违规或异常的产品。
8	网络脆弱性扫描产品	利用扫描手段检测目标网络系统中可能存在的安全弱点的软件或软硬件组合的产品。
9	安全数据库系统	从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的数据库系统,目的是在数据库层面保障数据安全。
10	网站数据恢复产品	提供对网站数据的监测、防篡改,并实现数据备份和恢复等安全功能的产品。
11	虚拟专用网产品	在互联网链路等公共通信基础网络上建立专用安全传输通道的产品。
12	防病毒网关	部署于网络和网络之间,通过分析网络层和应用层的通信,根据预先定义的过滤规则和防护策略实现对网络内病毒防护的产品。

序号	产品类别	产品描述
13	统一威胁管理产品 (UTM)	通过统一部署的安全策略,融合多种安全功能,针对面向网络及应用系统的安全威胁进行综合防御的网关型设备或系统。
14	病毒防治产品	用于检测发现或阻止恶意代码的传播以及对主机操作系统应用软件和用户文件的篡改、窃取和破坏等的产品。
15	安全操作系统	从系统设计、实现到使用等各个阶段都遵循了一套完整的安全策略的操作系统,目的是在操作系统层面保障系统安全。
16	安全网络存储	通过网络基于不同协议连接到服务器的专用存储设备。
17	公钥基础设施	支持公钥管理体制,提供鉴别、加密、完整性和不可否认服务的基础设施。
18	网络安全态势感知产品	通过采集网络流量、资产信息、日志、漏洞信息、告警信息、威胁信息等数据,分析和处理网络行为及用户行为等因素,掌握网络安全状态,预测网络安全趋势,并进行展示和监测预警的产品。
19	信息系统安全管理平台	对信息系统的安全策略以及执行该策略的安全计算环境、安全区域边界和安全通信网络等方面的安全机制实施统一管理的平台。
20	网络型流量控制产品	对安全域的网络进行流量监测和带宽控制的流量管理系统。
21	负载均衡产品	提供链路负载均衡、服务器负载均衡、网络流量优化和智能处理等功能的产品。
22	信息过滤产品	对文字、图片等网络信息进行筛选控制的产品。
23	抗拒绝服务攻击产品	用于识别和拦截拒绝服务攻击、保障系统可用性的产品。
24	终端接入控制产品	提供对接入网络的终端进行访问控制功能的产品。
25	USB 移动存储介质管理系统	对移动存储设备采取身份认证、访问控制、审计机制等管理手段,实现移动存储设备与主机设备之间可信访问的产品。
26	文件加密产品	用于防御攻击者窃取以文件等形式存储的数据、保障存储数据安全的产品。
27	数据泄露防护产品	通过对安全域内部敏感信息输出的主要途径进行控制和审计,防止安全域内部敏感信息被非授权泄露的产品。
28	数据销毁软件产品	采用信息技术进行逻辑级底层数据清除,彻底销毁存储介质所承载数据的产品。
29	安全配置检查产品	基于安全配置要求实现对资产的安全配置检测和合规性分析,生成安全配置建议和合规性报告的产品。
30	运维安全管理产品	对信息系统重要资产维护过程实现单点登录、集中授权、集中管理和审计的产品。
31	日志分析产品	采集信息系统中的日志数据,并进行集中存储和分析的安全产品。
32	身份鉴别产品	要求用户提供以电子信息或生物信息为载体的身份鉴别信息,确认应用系统使用者身份的产品。
33	终端安全监测产品	对终端进行安全性监测和控制,发现和阻止系统和网络资源非授权使用的产品。
34	电子文档安全管理产品	通过制作安全电子文档或将电子文档转换为安全电子文档,对安全电子文档进行统一管理、监控和审计的产品。



统一威胁管理产品 (UTM)

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：网神 SecGate 3600 防火墙

产品概述

网神 SecGate3600 防火墙是一款能够全面应对传统网络攻击和高级威胁的创新型防火墙产品，可广泛运用于政府机构、各类企业和组织的业务网络边界，实现网络安全域隔离、精细化访问控制、高效的威胁防护和高级威胁检测等功能。该产品在下一代防火墙基础上超越性的集成了威胁情报、大数据分析和安全可视化等创新安全技术，并通过与网络威胁感知中心、安全管理分析中心、终端安全管理系统等的智能协同，为用户在网络边界构建数据驱动的新一代威胁防御平台。

功能特点

◎智慧防御——全面防护网络攻击

通过威胁情报、安全大数据和协同联动等新技术的运用，极大消除传统防御盲区，高效防御并预防病毒、漏洞利用、恶意软件、僵尸网络等主流威胁由网络边界侵入，进而实现全面、

高效的业务网络防护。

◎智慧感知——及时洞察潜在威胁

基于精准的高级威胁发现能力和配套的可视化工具、平台运用，显著增强网络的全局可见性和网络威胁的感知能力，通过实时洞察威胁态势、防御漏洞和失陷资产，及时发现网内潜伏的异常风险及高级威胁。

◎智慧管理——提升响应处置效率

基于智能化的人机协同设计及配套的管理分析平台，持续助推用户的安全运营落地，大幅降低规模化部署用户的运维管理成本，避免误配置风险，并显著提升快速响应和处置的能力。

技术指标

◎基础组网功能

- ★部署模式：支持路由模式、透明模式、交换模式、混合模式以及旁路模式接入。
- ★路由特性：默认路由、静态路由、策略路由、支持 RIP、RIPng、OSPF、BGP 等动态路由。
- ★IP 协议：支持支持 IPV4、IPV6 双栈。
- ★NAT：支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式。
- ★负载均衡：支持基于 IP、ISP、应用、用户、服务等多的链路负载均衡，支持 DNS 流量的负载均衡，支持基于服务器地址的负载均衡；支持 IPSec VPN 的多链路备份和负载。
- ★网络服务：支持 DHCP 服务器、DNS 透明代理、ARP 代理等网络服务。
- ★VPN：支持 IPSec VPN、SSL VPN、L2TP、PPTP、GRE，IPSecVPN 支持国密算法，SSL VPN 支持 Windows 客户端、安卓客户端和 IOS 客户端；DS-Lite 支持作为 B4 和 AFTR。
- ★虚拟系统：支持虚拟系统路由、交换、监控、审计、安全、防护等全隔离。
- ★高可靠性：支持双机热备功能，支持路由和透明模式下的“主-备”、“主-主”模式，支持接口联动，链路探测。
- ★LLDP 功能：可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。

◎精细化访问控制功能

- ★访问控制：支持基于 IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，支持一条安全策略配置应用控制、入侵防护、URL 过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，并支持安全策略的快速检索，冗余策略分析，命中时间分析和安全策略推荐。
- ★应用识别：可精确识别 5000 余种互联网应用，700 余种移动应用，支持应用云识别。
- ★行为管控：支持对 HTTP、SMTP、POP3、IMAP、FTP、TELNET 协议进行细粒度的控制，过滤不受信任的网络行为。

★用户认证：支持基于 web 的无客户端方式的用户认证，具备集成 AD 活动目录、LDAP、RADIUS 的第三方认证。

★文件过滤：不基于后缀名方式实现对文档、压缩、归档三大类共 30 多种常用文档类型过滤。

★邮件过滤：支持对邮件收发件人进行过滤，基于 RBL 黑名单及自定义 IP 地址黑名单两种方式的反垃圾邮件支持。

★URL 过滤：预置 133 类 URL 资源库，可手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。

★内容过滤：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。

★带宽管理：支持根据 IP 地址、用户、服务、应用、时间等信息划分虚拟 QoS 通道进行带宽管理，支持多层次调度类嵌套的最大带宽限制和最小带宽保证。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00055-A

★有效期：2023 年 09 月 01 日至 2025 年 09 月 01 日

所属品牌：奇安信网神

发布时间：2014 年

产品适用领域：全行业

产品照片：



产品咨询二维码

产品咨询邮箱：kefu@qianxin.com

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I³”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高速增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

集团总部位于北京市中关村软件园启明星辰大厦，DT（数据时代）总部位于杭州高新区（滨江），全国云安全总部位于苏州高新区，在全国各省、市、自治区设立了分支机构，拥有覆盖全国的渠道和服务体系，为用户提供网络安全产品、服务和解决方案。

网址：<http://www.venustech.com.cn>

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：天清汉马 USG 一体化安全网关系统

产品概述

天清汉马 USG 一体化安全网关（UTM 统一威胁管理）采用了业界先进的基于多核硬件架构和一体化的软件设计，集防火墙、VPN、入侵防御（IPS）、防病毒、上网行为管理、内网安全、反垃圾邮件、抗拒绝服务攻击（Anti-DoS）、内容过滤等多种安全技术于一身，高性能、绿色低碳，同时全面支持各种路由协议、QoS、高可用性（HA）、日志审计等功能，为网络边界提供了全面实时的安全防护，帮助用户抵御日益复杂的安全威胁。

启明星辰天清汉马 USG 一体化安全网关（UTM 统一威胁管理）经过 10 多年的持续发展，拥有目前国内众多的客户群体。根据赛迪顾问报告，从 2007 年至今连续多年位居中国统一威胁管理硬件市场占有率第一。

功能特点

◎智能化的异常流量管理

内建了 50 多组异常检测模块，可以检测各项偏离预期的网络行为。

◎业务处理引擎

通过合适的数学模型计算出复杂、多变流量数据共有的属性，把混合在其中的大多数简单、重复流量数据预先检出并进行快速转发，能极大提升系统处理性能。

◎高效线速转发

通过把占网络流量大多数的、经常发生的简单、重复流量，从主数据处理任务队列剥离出来，交予协议加速引擎处理，可以释放大量系统计算资源处理更加复杂的运算。

◎应用识别

基于应用行为和数据特征的应用识别，有效地提升了应用的识别率，避免了误判。

网络安全专用产品安全认证或安全检测结果证明

（1）网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2018-CS006-029

★有效期：2023 年 07 月 01 日至 2028 年 06 月 30 日

（2）网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS006-298

★有效期：2023 年 07 月 25 日至 2028 年 07 月 24 日

所属品牌：启明星辰

发布时间：2023 年 07 月 01 日

产品适用领域：政府、公安、企业、军队、媒体、能源、医疗，教育、金融等

产品照片：



产品咨询二维码

产品咨询邮箱：li_zhiqiang3@venusgroup.com.cn

产品名称：网御安全网关系统

产品概述

UTM 是统一威胁管理（Unified Threat Management）的缩写。UTM 安全网关是指由硬件、软件和网络技术组成的具有专门用途的设备，它主要提供一项或多项安全功能，将多种安全特性集成于一个专用设备中，通过统一部署的安全策略，融合多种安全功能，针对面向网络及应用系统的安全威胁进行综合防御的网关型设备或系统。

UTM 安全网关应该具备的基本功能包括网络防火墙、网络入侵检测 / 防御、VPN 和网关防病毒等功能，这几项功能并不一定要同时都得到使用，不过它们应该是 UTM 设备自身固有的功能。UTM 安全网关也可能包括其它特性，例如内容过滤、安全审计、安全管理、日志、服务质量（QoS）、高可用性（HA）和带宽管理等。

功能特点

◎高性能网络访问控制

在网御安全网关系统产品，通过深度防护规则实现网络访问控制，深度防护规则包含源地址、目的地址、源端口、源 MAC、流入网口、流出网口、访问控制、时间调度、服务、是否为长连接、深度防护策略等多个控制子选项，对于不符合规则的访问，系统可以拦截并发出日志告警。

◎性能和功能完美匹配的病毒防御

网御安全网关系统产品的病毒检测引擎针对非缓存流检测模式进行了全面结构调整和优化，使安全网关的病毒检测率和处理性能获得质的突破：在保持高病毒检测率的同时，系统性能下降不超过 20%，是业界第一个建议用户把网络访问控制、病毒防御、入侵防御等全部功能同时开启使用的安全网关产品。

◎精准高效的入侵防御

网御安全网关系统产品系列产品经过多年的研发和持续的改进，在蠕虫、后门、木马、间谍软件、Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，完全满足用户的各种应用需要。

◎完善的应用监控

网御安全网关系统产品不仅具有网络入侵防御和网络病毒防御功能，同时还具有丰富的应用监控功能。可以根据不同的时间、群组，来对即时聊天软件、网游、P2P 软件等下达严格的管理策略。网御安全网关系统对应用的识别基于应用行为和数据特征，而不是基于端口号，有效地提升了应用的识别率，避免了误判。尤其对 P2P 应用中的加密传输，网御安全网关系统产品基于应用行为识别与主动探测相结合的方式，有效地克服了加密后无法识别的业内难题。通过精确的识别，网御安全网关系统对 IM 软件实现了细粒度的控制，不但可以控制登陆，而且对文字聊天，文件传输，音频、视频都可以实现分类控制。

◎多层次的高可用性设计

网御安全网关系统产品通过在物理层、链路层、网络层、实体层等多个层面实现多元化冗余设计，可有效地保障产品在用户网络应用中的高可用性。

◎统一的集中管控

通过部署网御安全管理系统软件，可实现对网御安全网关系统产品的集中管理，有利于快速完成多台安全网关设备的部署实施工作，并方便管理员对多台安全网关进行管理维护。

技术指标

功能类别	功能描述
操作系统	支持多系统引导，并可配置启动顺序
	支持系统分区备份，支持将系统 A 克隆至系统 B
	支持多个系统配置文件，可导入导出恢复配置
工作模式	透明模式，路由模式，混合模式，支持多透明桥、端口聚合
IPv6	支持 IPv6 地址、地址组配置
	支持 IPv6 安全控制策略设置，能针对 IPV6 的目的 / 源地址、目的 / 源服务端口、服务、扩展头属性等条件进行安全访问规则的设置
	支持 IPv6 静态路由、动态路由
	支持 IPv6/IPv4 翻译策略技术，包括支持静态 NAT-PT、动态 NAT-PT 技术，
	支持双栈、6to4 隧道实现 IPv6 网络之间穿越 IPV4 网络的访问
安全选项	支持近百种标准服务（如 SIP、GRE、H323、OSPF），支持用户定义服务和组
	ALG 应用代理（SIP、H.323、TNS、RSTP、RAS 等 NAT 穿越）
	支持 IP/MAC 地址绑定
网络访问控制	支持单条包过滤规则源目的地址引用 1000 个以上的地址对象（同时包含地址列表、地址组），实现包过滤规则条目数的优化。
入侵防护	具备 3000 种以上攻击特征库规则列表，并可自定义特征库。
	支持入侵场景保留，可记录入侵行为相关的网络数据报文，报文可保存至 U 盘或某台内网服务器。
	支持实时的入侵防护事件分级报警列表，可按事件的源 IP、目的 IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源 IP，阻断时间可控。
	支持抗 DDOS/DOS 攻击，可积极防御 syn flood、Ping flood、up flood、teardrop、sweep、land-base、ping of death、smurf、winnuke、圣诞树、碎片等 DDOS 攻击
防病毒	支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境
	支持病毒感染主机分析与隔离，防止病毒进一步扩散，提高网络整体安全性
	病毒库不少于 600 万种病毒特征，支持根据用户需求自定义病毒特征
带宽管理	基于主机的带宽管理，支持仅通过一条策略即可实现对指定的 IP 地址组里每 IP 用户进行上下行限速，也可以只对单个 IP 进行上下行限速，截图证明
上网行为管理	支持常见的应用识别。
	支持依据协议、源目的端口、特征码等条件自定义应用
	识别和控制 20 种以上炒股软件，包括大智慧、同花顺、等。
	识别和控制常见文档类型的传输，包括但不限于电影类 rmvb、flv、swf 等文件，音乐类 mp3、wma、wav、ogg 等文件，且文档类型和分类库可自定义。

功能类别	功能描述
Web 安全	具备对 Web 恶意扫描行为的防护能力，至少包含对弱口令、版本探测、漏洞扫描三种行为的防护能
	可发现 Webshell 恶意上传行为并进行拦截，具备 50 种以上的行为特征库
	可对 SQL 注入攻击行为 /XSS 跨站脚本攻击行为进行防护

网络安全专用产品安全认证或安全检测结果证明

（1）网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS006-362

★有效期：2023 年 8 月 23 日至 2028 年 8 月 22 日

（2）计算机信息系统安全专用产品销售许可证

★证书编号：0402231541

★有效期：2023 年 6 月 9 日至 2025 年 6 月 9 日

所属品牌：网御星云

发布时间：2007 年 4 月 18 日

产品适用领域：政府、公安、企业、军队、媒体、能源、医疗，教育、金融等

产品照片：



产品咨询二维码

产品咨询邮箱：cui_xueguang@venusgroup.com.cn

天融信科技集团

天融信科技集团（证券代码：002212）创始于 1995 年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获 2 次国家级科技进步奖和 7 次省部级科技进步奖。同时，天融信防火墙已连续 23 年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP 等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路 10 号院西区 11 号楼东侧天融信科技集团

产品名称：天融信应用安全网关系统

产品概述

天融信应用安全网关系统，具备完整的 IPv4/IPv6 网络接入能力，融入了 AI 驱动的一体化智能检测引擎，并集入侵防御、WAF、僵尸蠕、URL 过滤、DDoS 防护、HTTPS 流量检测、高级威胁防护、异常行为分析、DLP、威胁情报等多个安全模块于一身，既能处理传统安全业务，又能检测未知威胁，还能够联动云管端多个网元，最终为用户提供融入 AI 单点防御、多元智慧协同、云检测赋能的智能、主动、安全“零”死角的综合防护方案。

天融信应用安全网关系统采用自主研发的 64 位高性能多核并行安全操作系统 NGTOS。NGTOS 操作系统能为每个 CPU 核分配一套独立的 TCP/IP 协议栈，通过多 CPU 核多协议栈架构设计，避免共享协议栈拥塞问题。同时，系统采用了先进的用户态协议栈，该协议栈不但避免了传统内核态协议栈带来的中断调度和数据复制问题，同时兼容最新的 IPv4/IPv6 协议，为各种 IPv4/IPv6 应用提供支撑。天融信高性能多核并行安全操作系统解决了通用操作系统多核性能瓶颈问题，为软件系统层面高性能处理机制提供操作系统层面的资源支撑和保障。

在高性能架构的基础上，天融信应用安全网关系统还引入了一体化流检测机制，采用多模

式匹配算法，一次检查，可以同时覆盖多个安全引擎的检查需要，无需多个引擎多次检查，能够大大提高检测效率。

功能特点

天融信应用安全网关系统，具备完整的 IPv4/IPv6 网络接入能力。除具备常规应用安全网关功能外，还增加了针对 Web 应用、僵尸蠕、DDOS、DLP、数据库、HTTPS 加密流量等安全威胁的防护能力，并通过融入 AI 智能检测引擎、异常行为分析机制实现本地高级威胁检测防御。同时，通过联动机制获取 APT、IDS、DLP、WAF、EDR、态势感知、云端检测等安全组件的检测结果，感知整网安全风险点，实现动态安全监控和处置，为客户提供覆盖端点、网络和服务的全域协同防护安全解决方案。

天融信应用安全网关提供全面的资产管理功能。一键资产扫描发现、资产导入导出、资产手工录入、资产联动上报，资产分组。可根据指定的网络范围，通过被动资产发现和主动资产发现等多种方式，识别出资产及其不同类型。

天融信应用安全网关内置多种高级威胁攻击防御解决手段，包括基于 AI 的高级威胁检测、基于行为分析的异常威胁检测和基于联动的未知威胁检测，多方位对高级威胁进行深度检测防御。

天融信以应用安全网关为核心，通过调动网内其他安全组件（如 IDS、APT、EDR、DLP、态势感知平台等）的检测能力，实时联动，协同共享，构成全域协同的自动化处置系统。实现从单点防御向全域覆盖、智能协同的主动化纵深防御体系，联动终端和网端，实现全局预警、协同防护、风险可视，帮助客户实现安全威胁事前防御、事中控制、事后分析。

天融信应用安全网关能根据 IP 地址数据库，展示各个地理位置威胁地图，也可以根据地理位置设置不同的访问控制策略。天融信应用安全网关提供对威胁的全方位可视化，其中包括攻击者维度，受害者维度，事件维度的等多维度多视角的展示：通过对攻击者从地理信息，ip 地址，攻击统计信息对攻击者进行肖像刻画；通过对受害者资产属性分析对受害者进行画像；通过对攻击类型及过程和时间等元素分析，对攻击过程进行全视角的分析和刻画，让攻击威胁无处遁形，全方位可视。天融信应用安全网关支持攻击溯源，持续性威胁感知，并可针对攻击源头进行有效阻断，能大幅降低安全事件对用户资产的影响。快速推送告警事件，协助用户第一时间响应处置，助安全一臂之力。

为了便于用户掌握网络中安全情况以及降低运维管理工作量，天融信应用安全网关提供了智能运维管理的一系列工具，包括安全监控、数据中心、安全中心、安全策略管理、安全中心、集中管理、第三方管理接口等。

技术指标

TopGate(万兆)V3: 吞吐 20G-100G

TopGate(千兆)V3: 吞吐 2G-20G

网络安全专用产品安全认证或安全检测结果证明

(1) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2018-CS006-014

★有效期：2023 年 7 月 1 日至 2028 年 6 月 30 日

(2) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS006-402

★有效期：2023 年 8 月 28 日至 2028 年 8 月 27 日

所属品牌：天融信

发布时间：2000 年

产品适用领域：所有领域。如交通、教育、金融、能源、政法、
运营商、卫生、公安、医疗、电力、水利等。

产品照片：



产品咨询二维码



TopGate(万兆)V3



TopGate(千兆)V3

产品咨询邮箱：feng_chong@topsec.com.cn



病毒防治产品

安天科技集团股份有限公司

安天是引领威胁检测与防御能力发展的网络安全国家队，依托自主先进核心技术与安全理念，致力于为网信主管部门、军队、部委、保密和关键信息基础设施等高安全需求客户提供整体安全解决方案。安天产品和服务为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等基础能力，建设实战化的态势感知体系，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，赋能客户筑起可对抗高级威胁的网络安全防线。

安天为全球超过一百三十万台网络设备和网络安全设备、超过三十亿部智能终端设备提供安全检测能力；安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑，多次收到相关部门的感谢信。

安天已发展成为以哈尔滨为总部基地，建有七地研发中心、九家控股子公司，拥有一个国家企业技术中心和三个省级重点实验室、工程技术研究中心和新型研发机构，参与一个国家工程实验室建设，建立一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

网址：<https://www.antiy.cn>

电话：010-82893723

地址：北京市海淀区闵庄路 3 号清华科技园玉泉慧谷一期 1 号楼

产品名称：安天移动终端威胁检测系统 V1.0

产品概述

安天移动终端威胁检测系统是一款专业性强的多形态移动终端检测和数据采集的智能化工具，支持对安卓系统手机进行检测，可快速圈定手机中的病毒并及时警报。集成安天自主研发的 AVL 反病毒引擎，基于庞大的底层数据做支撑，结合科学合理的筛查规则，提供专业准确的检测结果。

功能特点

安天移动终端威胁检测系统有两部分组成，分别为检查终端管理器、采集终端，检查终端通过 WIFI 网络或扫描二维码方式与采集终端连接，检测完成后，数据回传至检查终端管理器，对数据留存记录，并输出相应的检测内容和数据的统计分析与每个采集终端的详情报告，用户可根据需要导出相应的数据报告。

可检测来自存储介质和网络媒介传输到手机设备中的文件，精确识别和判定传输的文件是否是病毒，一经发现及时报警。检测到设备中的病毒启动，会实时阻止病毒的生效和对设备的破坏，同时还可以卸载病毒或删除文件。

对安卓手机系统、装机应用进行全面扫描，可检测出安卓手机中的恶意应用、可疑应用，输出恶意应用的应用图标、应用名称、病毒类型、病毒描述、文件大小、应用 MD5、包名、版本信息、文件路径、应用来源等。

检测完毕后，会发送卸载病毒应用的指令，弹框提示卸载恶意应用，同时会自动删除检出的病毒文件。

技术指标

◎病毒样本入侵报警：若有来自存储介质、数据连接线、WIFI、蓝牙、WAP/WWW、电子邮件、移动聊天等渠道的病毒样本入侵移动终端，系统会自动进行报警提示；

◎自启动远程实时扫描：在移动终端启动恶意应用时，系统会自动扫描到恶意应用并进行报警提示；

◎阻止病毒的传播：在移动终端下载恶意样本时，系统会自动报警提示并清理掉下载的病毒样本；

◎即时清除病毒样本：当有病毒样本入侵移动终端时，系统会自动清除病毒样本，无需手动操作，清除率大于 90%；

◎检测病毒：对移动终端的病毒样本进行扫描检测，支持检出样本格式为 .apk、.dex、.zip，检出率超过 98%，检测结束后展示检出的恶意应用和恶意安装包数量；

◎备份病毒样本：当有病毒样本入侵移动终端时，系统会自动清理并备份病毒样本，备份的样本可导出至 U 盘进行进一步分析；

◎按计划扫描：支持设置扫描路径、扫描时间、扫描文件类型，设置成功后，系统会自动按时按路径扫描病毒样本；

◎生成活动日志：检测完毕后会自动生成活动日志，支持查看并导出检测日志。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全认证机构名称：国家计算机病毒应急处理中心

★证书编号：24BD00361-A

★有效期：2024 年 3 月 29 日至 2026 年 3 月 29 日

所属品牌：安天

发布时间：2023 年 5 月 18 日

产品适用领域：军工、政府、事业单位、能源电力、金融

产品照片：



产品咨询二维码

产品咨询邮箱：support@antiy.cn

北京安信天行科技有限公司

北京安信天行科技有限公司是国有控股企业，立足于自主知识产权网络安全产品、提供可管理信息安全服务的综合解决方案提供商。

以提供专业的网络安全服务为核心，安信天行建立了完备的安全运营服务体系、权威的安全服务资质体系 and 专业化安全服务团队，为政务、卫生、纪检、教育、广电、企业等各领域千余家单位信息化建设保驾护航。作为国家重大活动网络安全保卫技术支持单位，安信天行持续为 2008 年北京奥运会、国庆 70 周年、中国共产党成立 100 周年庆祝大会、2022 年冬奥会冬残奥会等重大活动提供网络安全保障工作，为活动的顺利举办做出重要贡献。

以人为本，开拓创新，安信天行先后承担工信部、国家保密局等国家科技攻关和课题研究项目，荣获“科技进步奖”、“高新技术企业”、“国家信息安全漏洞库技术支撑单位”、“国家信息安全漏洞平台成员单位”等荣誉。目前，安信天行已取得国家专利技术及自主知识产权近百项，打造了安全态势感知、安全防御、数据安全、保密安全等四条产品线，帮助用户构建全方位的网络安全保障体系，并已在各个行业取得了广泛应用。

安信天行将坚持“以服务求生存、用创新谋发展”理念，保障用户网络空间安全，致力于成为用户最信赖的网络安全企业。

网址：www.axtx.com.cn

电话：010-58045858

地址：北京市海淀区北四环西路 68 号左岸工社 10 层 1001

产品名称：安信天行主机病毒检测与防护系统

产品概述

安信天行主机病毒检测与防护系统是基于威胁情报和大数据安全分析方面的优势，为了满足政府、军队、能源、教育、金融等行业对终端未知威胁检测和 APT 防御方面需求开发的下一代终端安全防护系统，利用丰富的威胁情报信息，智能机器学习、漏洞利用检测、高级行为分析等技术帮助用户有效防范未知威胁带来的风险，对安全事件实现快速响应和处置。

功能特点

◎轻量级探针

通过不断的调优，部署在终端的探针对于终端资源占用达到最低，运行状态中 CPU 占用不超过 1%，内存占用小于 20M，可以更好的兼容性能较低的终端部署，为用户提供了一键安装和升级，部署维护更方便。

◎漏洞利用检测

系统不再关注终端是否存在漏洞，而是通过检测终端运行中是否存在漏洞利用的行为来抵御漏洞利用攻击，有效防止 0day 漏洞带来的安全威胁，同时也可以避免用户补丁更新不及时造成的防御真空。

◎防勒索软件

通过主动防御以及行为分析技术使用，系统可以有效识别已知以及未知勒索软件和勒索软件变种，实时阻断勒索软件运行，避免用户文件资料被加密带来的损失。

◎高级行为分析

从关注单一行为请求转变为对终端行为的关联分析，通过检测攻击者的攻击路径和手法发现被隐藏的攻击痕迹，行为动作以提升威胁发现能力，避免过去单一行为检测造成的漏报和误报，同时也可以有效检测病毒以及恶意软件变种，弥补静态样本比对方式的不足。

◎威胁情报

威胁情报的引入极大地提升了系统在高级威胁发现和安全事件响应方面的能力，通过威胁情报与终端行为数据的碰撞，帮助用户发现当前终端存在的异常行为，并实现对安全事件的多维度关联分析，做出快速响应和处置。

◎威胁脑图

威胁脑图以直观的形式将安全事件整个过程为用户展示，帮助用户快速建立起整个安全事件全貌，同时将不同维度的告警信息进行关联呈现，方便用户的安全溯源和响应处置。

◎安全调查

系统为用户提供了基于计算机名、文件、文件传输、签名、域名 IP、用户、IOC 扫描 7 大类安全调查方式，帮助用户从不同角度快速查看网络内威胁情况，了解当前网络中存在的安全威胁，以实现网络安全的实时监测以及为快速响应和处置提供数据支撑。

技术指标

◎威胁检测与展示

支持恶意文件的检测以及自动隔离，管理平台提供恶意文件的下载，同时通过脑图展示恶意文件的来源以及文件执行情况；支持通过 weblogic 等 web 服务器的漏洞上传的 webshell 的检测以及自动隔离，从而阻止利用 webshell 进行命令执行、反弹 shell、提权等操作；对威胁来源能够自动追溯到是通过网页（下载）、邮件（附件）或者 USB（拷贝）等；针对可疑 IP 告警，提供该 IP 地址所在国家以及访问这个可疑 IP 的用户来自哪些国家以判断是否是针对性攻击；支持 IIS、Apache、Weblogic 等 web 服务器通过 https 发起的 SQL 注入攻击的检测并记录攻击 URL。

◎安全追查和溯源

支持记录和追查文件全生命周期事件，包括文件的创建、重命名 / 移动、删除以及执行或

者打开等事件；支持计算机历史 IP 追查，显示一台计算机在指定时间范围内被分配 IP 的情况或者是一个 IP 在指定时间范围内分配给哪些计算机的信息；支持 IOC 批量追查，自动提取业内通用威胁情报文件里面的 IP、URL、域名等，进行批量回溯。

◎联动功能

支持第三方平台通过 api 查询计算机相关信息，包括 IP、历史 IP、MAC 地址、操作系统等信息。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106232065

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：北京安信天行科技有限公司

发布时间：2020 年 7 月 30 日

产品适用领域：政府、金融、电信、医疗、教育以及互联网等对网络安全要求高的企业或组织

产品照片：



产品咨询二维码

产品咨询邮箱：axtxmarketing@bjca.org.cn

产品名称：安信天行主机免疫系统

产品概述

安信天行主机免疫系统是一款为提升主机计算环境安全而设计的产品，是整个网络安全体系和威胁情报体系中不可或缺的一部分。在可持续、自适应网络安全框架下，利用可信计算、机器学习、行为分析等技术，实现系统层全面安全监控、内核级细粒度安全管控等能力。可对系统运行环境的整体安全状态进行全面监控，洞察影响主机安全的多方面因素，及时发现安全隐患并予以处置；能够在内核层对可执行程序以及用户的行为进行精准的控制，确保合法的用户、合法的进程、合法地访问文件，防止恶意代码、非法入侵等网络安全问题的发生；提供资源完整性保护、进程保护、主机网络防护、双因素身份鉴别等主机安全功能，并支持安全事件还原与分析。在满足网络安全相关政策标准的同时，全面提升主机安全主动防御能力，实现全面洞察、精准管控和敏锐反馈。

功能特点

◎内核级安全管控

主机免疫系统在 Ring0 级实现安全管控，拥有根权限，可以有效地控制使用 rootkit 技术开发的木马、病毒以及其他非法程序。

- ★应用程序运行控制
- ★安全访问控制
- ★资源完整性保护
- ★业务进程保护
- ★文件属性保护
- ★端口扫描防护
- ★ U-Key 身份鉴别

◎系统级安全监控

通过对业务计算环境安全的全面监控，可以洞察系统存在的安全隐患，及时发现安全威胁，并采取相应的应对措施。

- ★硬件资产监控
- ★软件资产监控
- ★系统运行状态监控
- ★系统安全监控

◎安全管理

管理中心可对所有管辖的主机进行远程统一安全管理，进行安全策略配置，并汇聚所有安全审计或告警数据。

- ★安全态势展示

- ★安全数据分析
- ★应用程序安全分析
- ★系统管理

技术指标

◎安全监控

★支持以下监控：

- (1) 主机硬件信息（CPU、硬盘、内存、网卡、外设）；
- (2) 软件信息（PE/ELF、安装软件）；
- (3) 系统信息（OS、账户、进程、服务、共享文件夹、开机启动程序、端口、驱动等）；
- (4) 安全信息（补丁漏洞、安全配置检查项）；
- (5) 进程网络行为信息。

★监控数据采集频率可自定义。

★监控的操作系统安全配置项，其中 Windows 系统提供的配置项 ≥ 170 项，Linux 系统提供的配置项 ≥ 100 项。

★支持硬件、账户、开机启动程序、共享文件夹、系统服务、进程、驱动、端口等信息的基线设定与比对功能，提供差异值实时告警、展示，精确定位告警信息。

◎安全管控

★提供基于黑、白、灰名单机制的主机可执行程序（包括驱动、动态库等）安全验证，执行程序启动进行实时的可信校验，校验不通过应拒绝其启动、运行；支持用户、进程等主体对指定客体（如文件/夹、注册表等）的访问控制策略，权限包括读、写、所有权限、禁止所有操作；支持文件、文件夹、注册表项等敏感资源的访问控制，能够阻止添加、删除、修改对应信息；支持对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问；能够对主机中的重要资源（如配置文件、数据文件、口令文件等）的完整性进行保护，出现被篡改时，及时告警并能一键恢复；能够对文件的属主、执行权限、修改时间等属性进行保护，防止恶意修改；可保护重要进程被恶意停止或删除；能够防止主机端口被恶意扫描，可以根据配置策略阻断相应的访问；支持基于 U-Key 的双因素身份鉴别；

★支持依据业务安全需求等级不同设置防护等级：

- (1) 依据业务安全需求等级不同可设置不同的管控模式；
- (2) 对 dll、sys 等系统进程主体和注册表等客体的管控可配置。

★能够针对已发生的安全事件（如敏感资源的非法访问），进行事件还原与溯源，提供进程、源 IP、访问时间、操作行为等信息；提供应用程序静态分析功能。可剖析 PE、ELF 等二进制可执行程序，利用特征规则，发掘威胁特征行为，识别灰色应用威胁度。

◎安全审计

支持对用户、文件、进程、服务、注册表等对象的操作行为进行审计；应能记录各管理员

角色在安全管理中心上的操作行为并进行审计；支持审计信息自动备份、导入导出。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106232065

★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：北京安信天行科技有限公司

发布时间：2019 年 1 月 10 日

产品适用领域：政府、金融、电信、医疗、教育以及互联网等对网络安全要求高的企业或组织

产品照片：



产品咨询二维码

产品咨询邮箱：axtxmarketing@bjca.org.cn

北京猎鹰安全科技有限公司

北京猎鹰安全科技有限公司（原金山安全）是猎豹移动、绿盟科技、安天科技等国内知名安全企业共同投资成立的国内领先的互联网安全技术及云安全平台解决方案提供商，是拥有完全自主知识产权的中国信息安全企业。北京猎鹰安全科技有限公司以“全面保障数字化环境安全”为企业使命，协助政府、军队、大型集团化企业和专用网络等企事业单位，构建专属的终端信息安全保障体系。

网址：www.ejinshan.net

电话：010-82663885

地址：北京市海淀区中关村大街 27 号中关村大厦 1112 室

产品名称：毒霸防病毒系统网络版 V9.0

产品概述

毒霸防病毒系统网络版 V9.0 能够为政府、企事业单位网络范围内的工作站和服务器提供可伸缩的跨平台病毒防护。毒霸防病毒系统网络版 V9.0 实现了集中式配置、部署、策略管理和报告，并支持管理员对网络安全进行实时审核，以确定哪些节点易于受到病毒的攻击，以及在出现紧急病毒情况时采取何种应急处理措施。网络管理员可以通过逻辑分组的方式管理终端和服务器的反病毒相关工作，并可以创建、部署和锁定安全策略和设置，从而使得网络系统保持最新状态和良好的配置。

功能特点

◎控制台功能

★可移动的 Web 管理控制台

控制台基于 WEB 结构开发，管理员无需安装额外的控制软件，就可以在任意一台计算机上轻松管理整个防毒体系，真正实现了“管理无处不在”。

★多种管理架构

可扩展的无限分级管理架构——使用主系统中心来集中管理数据，以实现以单个系统中心对多个系统中心、升级服务器及其他特殊防毒节点的集中管理。

混合云架构——借鉴 SaaS 的管理模式，采用物理与 SaaS 的虚拟混合云管理架构，支持账号和其管辖范围的绑定。有效减少服务器资源投入，并降低维护成本。

★高效的安装部署方式

多种安装方式，包括《邮件通知》、《网站发布》、《远程安装》、《脚本安装》。管理员可以根据企业网络环境采用合适的安装方式，

★领先的云引擎

毒霸防病毒系统网络版 V9.0 将猎鹰安全多年运营与积累的核心云安全技术全面整合到产品当中，依托金山公有云的业内领先优势，为企业提供数倍于传统企业杀毒软件的能力的同时，终端资源占用相对于传统本地库的杀毒软件大为降低。

★多样式的账户管理设置

默认可分配三种管理员权限，系统管理员、安全管理员、审计管理员，可适应企业不同人员权限的划分设置，以保证灵活与安全。

★报警

管理员可以通过 Email 方式接收病毒事件报警，以保证及时应对病毒疫情。

★云查杀

病毒查杀

云引擎鉴定

云查杀设置

★终端管理

组管理

终端设置

查杀白名单

单点维护

★报表管理

毒霸防病毒系统网络版 V9.0 支持对终端病毒日志、安全日志、僵尸病毒、文件及应用升级日志、终端事件告警、管理员日志等信息进行报表统计。

◎客户端功能

★病毒查杀

①快速扫描（默认查杀方式）——此模式只对电脑中的系统文件夹等敏感区域进行独立扫描。

②全盘查杀——此模式将对电脑的全部磁盘文件系统进行完整扫描。

③自定义查杀：——此模式将只对您指定的文件支持右键调起查杀。

★设置

①文件信任，设置信任文件及文件夹。

②系统保护，默认选定开机时是启动文件系统保护。

隔离区文件，对已经处理的威胁文件进行隔离区备份，可进行恢复、删除等操作。

★日志管理器

毒霸防病毒系统网络版 V9.0 日志管理器包含有病毒查杀日志、产品升级日志、系统防御日志、挂马拦截日志。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106232011

★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：猎鹰安全

发布时间：2023 年 6 月

产品适用领域：政府、军工、企事业单位等专用平台网络环境

产品照片：



产品咨询邮箱：wangzhiyong@ejinshan.net



产品咨询二维码

产品名称：猎鹰终端安全管理系统 V9.0**产品概述**

猎鹰终端安全管理系统 V9.0（以下简称终端安全系统 V9）是专门为政府、军工、能源、教育、医疗及集团化企业设计的终端安全管理平台，是根据多年来市场需求及安全威胁的不断快速迭代，在 V8.5 基础上的全面升级，全面统管终端安全。系统集成恶意代码快速查杀、安全攻击实时防护、全方位桌面管理、丰富的运维支撑、灵活的漏洞补丁管理、细粒度的外设管控以及多维度的日志审计回溯等功能，增强了包括从异常检测、行为安全管控、安全加固、安全运维及安全事件回溯等维度实现终端整体安全防护，是一款一站式终端安全管理 EDR 产品。

支持与猎鹰防毒墙、安全一体化平台、猎鹰安全系统、深度威胁分析平台等猎鹰安全设备以及第三方安全系统联动，协助企业构建高效的主动式的统一安全保障体系。

功能特点**◎控制台功能**

1. 可移动的 Web 管理控制台

控制台基于 WEB 结构开发，管理员无需安装额外的控制软件，就可以在任意一台计算机上轻松管理整个防毒体系，真正实现了“管理无处不在”。

2. 多种管理架构

★可扩展的无限分级管理架构

★混合云架构

3. 高效的安装部署方式

多种安装方式，包括《邮件通知》、《网站发布》、《远程安装》、《脚本安装》。管理员可以根据企业网络环境采用合适的安装方式。

4. 领先的云引擎

5. 多样式的账户管理设置

默认可分配三种管理员权限，普通管理员、配置管理员、审计管理员，可适应企业不同人员权限的划分设置，以保证灵活与安全。

6. 报警

管理员可以通过 Email 方式接收病毒事件报警，以保证及时应对病毒疫情。

7. 云查杀

★病毒查杀

★云引擎鉴定

★云查杀设置

8. 漏洞修复

★修复详情

★修复设置

9. 终端管理

★组管理

★终端设置

★查杀白名单

★USB 设置

★单点维护

10. 边界管理

边界管理克服传统杀毒软件弊端，在程序和文件进入企业终端之前划定一条严格的界限，当病毒文件通过边界进入企业终端时，直接先将文件传送到系统中心进行分析判断，并由系统中心统一监控、检查，在病毒尚未运行时即可被判定为安全或不安全，让病毒无可乘之机，实现前置主动预防。

11. 软件管理

猎鹰终端安全管理系统 V9.0 独有的企业软件管家功能不但能够统计全网终端的软件部署情况，还可以根据企业不同部门进行终端分组，并对不同分组分发不同软件，实现远程部署、远程通知安装等方式。

12. 报表管理

支持对终端病毒日志、安全日志、漏洞修复、僵尸病毒、文件及应用升级日志、终端事件告警、管理员日志等信息进行报表统计。

◎客户端功能

1. 病毒查杀

★一键云查杀（默认查杀方式）

★全盘查杀

★自定义查杀

2. 铠甲防御系统

铠甲防御技术是一款完美的结合猎鹰云引擎的终端云主动防御技术，铠甲防御技术中的行为拦截模式，是基于多步行为的综合判定，是拥有广谱特征匹配的启发式行为判定。

3. 漏洞修复

漏洞扫描其实是一键设计的，点击《漏洞扫描》，猎鹰终端安全管理系统便进行漏洞扫描。

4. 边界防御

“边界防御”是猎鹰终端安全管理系统率先提出的防病毒技术理念，在病毒尚未被运行时即可被判定为安全或不安全，从而最大限度地保障对本地计算机的安全防护。

5. 系统优化

6. 垃圾清理

7. 设置

★文件信任

★系统保护

8. 日志管理器

猎鹰终端安全管理系统 V9.0 日志管理器包含有病毒查杀日志、产品升级日志、系统防御日志、挂马拦截日志。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：国家计算机病毒应急处理中心计算机病毒防治产品检验实验室

★证书编号：24BD00521-A

★有效期：2024 年 4 月 26 日至 2026 年 4 月 26 日

所属品牌：猎鹰安全

发布时间：2022 年 5 月

产品适用领域：政府、军工、能源、教育、医疗及集团化企业等

产品照片：



产品咨询邮箱：wangzhiyong@ejinshan.net



产品咨询二维码

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISASecure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 6000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.winicssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特终端检测与响应系统（防病毒）

产品概述

威努特终端检测与响应系统以威胁检测与响应技术为核心，实时检测未知威胁并快速响应。终端检测与响应系统目前运用于各行业终端操作系统中，其优良的用户体验效果和兼容性让终端检测与响应系统在各行业中深入使用，管理强度深入到硬件驱动层，有力的保护了终端系统的安全。

功能特点

◎未知威胁有效防范

终端检测与响应系统对基于威胁诱捕、人工智能威胁检测引擎，可快速识别未知安全威胁，帮助用户构建未知威胁防御能力。

◎威胁事件快速响应，精准溯源

终端检测与响应系统支持文件隔离、文件修复、终端隔离、全局威胁处置、威胁情报全网同步等能力，可有效支撑威胁快速处置，并实时记录系统内部动态行为，全面梳理安全事件，

精准还原威胁过程，方便用户快速开展威胁溯源定位。

◎轻量化部署和应用

与传统主机防护软件相比，终端检测与响应系统部署快捷，方便易用，部署后可立即投入使用，客户端对终端性能占用小，保留轻载的病毒查杀、外设管控等模块，重载的威胁分析模块由终端检测响应平台管理，不会对系统软件的正常使用造成任何影响。

◎ 身安全防护

终端检测与响应系统可对自身进行安全性保护，包括防止非法卸载、停止本软件的应用程序、服务及驱动，并对执行此类操作的行为进行防护，从而有效保障服务器和终端的安全。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106232090

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：威努特

发布时间：2023 年 2 月 20 日

产品适用领域：电力、石油石化、轨道交通、钢铁、市政、烟草、
智能制造等

产品照片：



产品咨询二维码

产品咨询邮箱：support@winicssec.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业收入总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信天擎终端安全管理系统

产品概述

奇安信天擎终端安全管理系统（简称“天擎”）是注重实效的一体化终端安全解决方案，通过“体系化防御、数字化运营”方法，帮助政企客户准确识别、保护和监管终端，并确保这些终端在任何时候都能可信、安全、合规地访问数据和业务。天擎基于奇安信全新的“川陀”终端安全平台构建，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析 and 安全可视化等创新技术，通过系统合规与加固、威胁防御与检测、运维管控与审计、终端数据防泄漏、统一管理 with 运营等功能，帮助政企客户构建持续有效的终端安全能力。

功能特点

◎系统合规与加固

对操作系统的安全配置、漏洞补丁、软件安装合规性等方面进行检查和修复，通过契合的安全基线核查、有效的漏洞补丁管理、统一的软件管理，及时进行系统加固，达到收缩暴露面、

“强身健体”的目的。

◎威胁防御与检测

集成多个防护引擎，再结合奇安信强大的攻防研究能力及丰富的规则库储备及生产能力，实现对可疑行为、已知病毒、未知病毒和各类攻击的实时拦截、高效检测、准确定位、完整溯源，并有效防御针对服务器系统的漏洞利用攻击，确保终端始终安全。

◎终端管控与审计

通过对终端的管控、运维、审计，构建完善的主机管控与行为审计体系，实现对终端的外接设备、移动存储设备、系统行为、网络行为、应用进程等多层次的管控与审计。

◎终端数据防泄漏

根据预先定义的策略，实时扫描存储和传输中的数据，评估数据是否违反预先定义的策略，并根据预设自动采取诸如警告、隔离甚至阻断等保护动作；集成资产管理、文件追踪、通道管控等功能，通过资产管控和安全水印等安全措施，实现终端数据防泄漏及泄露追踪。

◎管理与安全运营

通过管理中心实现全网终端的统一管理及策略、任务的统一下发，同时可利用其配套的安全管理平台实现基于量化指标的数字化安全运营。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：国家计算机病毒应急处理中心

★证书编号：24BD01391-A

★有效期：2024年09月20日至2026年09月20日

所属品牌：奇安信网神

发布时间：2015年8月

产品适用领域：全行业

产品照片：

产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

三六零数字安全科技集团有限公司

360 数字安全集团 (三六零数字安全科技集团有限公司) 是数字安全的领导者, 秉持“上山下海助小微”战略方针, 以“安全即服务”为核心发展理念全面升级“360 安全云”, 将十多年被行业反复验证成功的数字安全运营体系框架, 以云化服务化方式为国家、城市、大型企业、中小微企业构建应对数字时代复杂威胁的完整数字安全能力。

网址: <https://360.net/>

电话: 400-0309-360

地址: 北京市朝阳区县 (区、市、旗) 酒仙桥路甲 10 号 3 号楼 17 层 1773 号

产品名称: 360 终端安全管理系统 V12.0

产品概述

360 终端安全管理系统是在 360 安全大脑极致赋能下, 以云计算、大数据、人工智能等新技术为支撑, 以可靠服务为保障, 集高级威胁发现 (EDR)、防病毒、漏洞防护、停机加固、终端合规管控、终端准入 (NAC)、终端审计、数据安全、主机加固 (CWPP) 管理于一体的企业级安全产品, 能同时兼容传统与信创终端统一管理、全面保障政企终端安全。

功能特点

◎勒索挖矿防护

挖矿木马和勒索病毒的肆虐, 对终端资源的榨取已经到了无以复加的地步。如何有效守护合法拥有的计算资源、数据资源, 是广大政企用户必须要重视的问题。终端作为网络攻防的主战场, 将持续聚焦攻防视角下的端点安全防护痛点与难点, 围绕构建有效的查、杀、防体系, 坚强守护端点安全防线, 提供动态化、持续化、高效化的安全防护能力。

◎高级威胁检测与响应 (EDR)

如今的网络威胁已经由简单的个体炫技演变为有组织的网络犯罪和有国家情报支持的高级网络攻击。攻击者掌握了更隐蔽, 持续性更强的攻击手段, 使得企业和组织乃至国家不得不面临更复杂的高级威胁。

在这种情况下, 传统被动式的反病毒软件 (AV) 已经无法满足需求, 而端点检测与响应 (Endpoint Detection & Response, EDR) 被认为是一种面向未来的终端安全解决方案。

通过不同于传统的签名检测或启发式技术, EDR 专为检测终端上的可疑行为而设计, 能够在现有基础上为企业提供更深层、细化的端点数据, 通过持续监测终端活动行为、检测安全风险、对于威胁风险进行深度调查、提供补救响应手段的方式, 补充了传统终端安全产品防御高

级威胁能力的不足，在对抗高级威胁中获得更好的效果与更快的效率，尽可能压缩攻击者的攻击时间，减少高级威胁最终达到目的可能性。

◎ 停服加固

2020 年 1 月 14 日，微软正式宣告 Windows7 操作系统停止更新，官方停止技术支持、软件更新和安全问题的修复，这意味着数以亿计仍在运行 Win7 系统的计算机失去官方修复风险的可能。受此影响，包含 Win7 系统在内的微软停服系统都将暴露在各种网络威胁之中，机密信息、业务的正常运行都将受到严重威胁，一旦这些威胁发生，将产生难以估量的灾难性后果。

◎ 合规管控

应等保合规 2.0 相关终端安全管理要求，从恶意代码防护、桌面标准化、终端外联、介质使用、系统加固、终端准入、终端审计等层面符合监管要求，满足本单位网络安全建设规范，确保终端安全建设合法合规。

◎ 数据安全

终端数据外泄方式多样化，越来越难以防控，且数据安全法及等保 2.0 中关于数据安全已经提出了关于数据安全的相关要求。为加强终端数据安全防护，需要建立敏感数据检测、敏感数据外发拦截、终端行为审计等全面的安全防护措施，加强数据安全防护能力。

技术指标

类别	功能名称
部署架构	部署模式、灵活授权、系统兼容性 数据开放 API、模块化部署
基础管理	高危操作验证、客户端自我保护 终端反馈、账号锁定、账号登录白名单 角色管理、任务管理、syslog 外发 LDAP 联动、虚拟化管理、客户端迁移
资产管理	硬件资产、软件资产、资产采集 资产风险、终端发现、资产登记 实名认证、资产同步、终端资源监控、功能定制
防病毒相关	反病毒引擎、扫描策略、防感染模式 杀毒资源占用、系统修复、安全区 病毒库升级、办公文档智能备份、勒索防护、 勒索响应、勒索解密、宏病毒查杀、威胁详情订阅服务 病毒团伙/家族情报、系统风险防御、上网风险防御、入口风险防御、高级 威胁防御、勒索风险防御 系统登陆二次认证、威胁自查、云脑情报
漏洞与补丁管理	漏洞修复、停服系统统计 Windows 补丁管理、灰度发布
终端管控	桌面加固、外联管控、外设管控、服务管控、 进程管理、主机防火墙软件卸载、文件分发、远程控制
无补丁漏洞免疫	系统核心防护、微补丁漏洞免疫

类别	功能名称
移动存储管控	注册管理、加密 U 盘注册 U 盘注销、注册申请、授权管理
桌面优化	优化工具、系统工具、文件粉碎机 查找重复文件、桌面助手、自定义工具
安全检查	隔离沙箱、流量管理、安全检查
终端审计	文件审计、终端打印审计 网络连接访问审计、终端开关机审计 系统账户审计、外设使用审计
水印策略	屏幕水印、屏幕显形、打印水印 应用水印 - 进程水印、应用水印 - 网页水印
数据安全	敏感信息扫描、敏感信息库、OCR 识别、 文件外发防护、外发白名单、文件外发审批
能耗管理	能耗总览、资源占用监控、终端运行资源告警 单点终端性能监控驾驶舱、开关机审计、 工作时间外开机审计、节能配置、能耗统计
智能隔离	智能隔离
屏摄追踪	取证管理
软件管家	软件市场、软件使用分析、软件管理策略 软件定制、下载空间管理、下载安装统计 软件管家离线工具、软件分发、文件分发 软件防卸载、软件防安装、软件防启用 操作系统正版化检测、应用程序检查
安全 U 盘	外出权限控制、安全登录 密码找回、系统兼容 离线审计、多分区
终端检测响应 EDR	Windows 异常行为捕获、Linux 异常行为捕获 Windows 终端 APT 扫描和响应 Windows 终端专项检测响应 文件检测、检测性能 告警规则管理、响应处置 APT 情报、APT 失陷检测
Mac 终端防病毒	Mac 安全防护、MAC 资产登记
外联靶机	外联靶机、靶机管理
终端安全可视化	终端安全综合治理结果可视化展示 病毒处置结果可视化、漏洞修复结果可视化

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：网络安全专用产品安全检测证书

★证书编号：24BD00027-A

★有效期：2024 年 1 月 26 日至 2025 年 6 月 30 日

所属品牌：360

发布时间：2023 年 8 月 10 日

产品适用领域：党政军、公检法司、金融、能源、央企、教育、医疗、企业等全行业客户

产品照片：



产品咨询邮箱：lideyang@360.cn

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：统一端点安全管理系统（aES）

产品概述

深信服统一端点安全管理系统由管理平台与客户端组成，管理平台支持统一的终端资产管理、终端安全体检、终端合规检查。全面采集终端侧系统层、应用层行为数据，本地分层上报至平台关联分析，对攻击事件精准研判。最终以可视化的攻击进程链形还原攻击故事。威胁狩猎则可基于全面采集到的数据，细粒度对全网终端做狩猎查杀，猎捕残余攻击。微隔离的访问控制策略统一管理，支持对安全事件的一键隔离处置。端点软件支持防病毒功能、入侵防御功能、防火墙隔离功能、数据信息采集上报、安全事件的一键处置等。深信服的 aES 产品也支持与自家网络侧安全产品如 NGAF、AC、SIP，以及 XDR 平台形成深度联动，打通网端数据，让网端安全产品协同，促进安全事件彻底闭环。形成新一代的联动防护体系。

功能特点

◎终端资产的全面管理：全网终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、资产位置等。每

一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

◎**终端安全的合规检查**：每一个组织都有自己的终端安全合规要求，特别是等级保护的合规要求，对主机的安全要求。终端安全合规审查依据等级保护的主机安全要求进行设计，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等策略进行合规性审查，满足企业建设等级保护系统的主机安全要求。

◎**勒索病毒的实时防御**：勒索病毒通过加密文件的方式，要求中招者支持一定数额的赎金。需要对最新的勒索软件进行有效的查杀，防止用户感染最新的勒索软件。

◎**入侵攻击的主动检测**：针对 Web 安全攻击行为，则主动检测 Web 后门的文件。针对僵尸网络的攻击，则根据僵尸网络的活跃行为，快速定位僵尸网络文件，并进行一键查杀。

◎**访问关系的策略控制**：当前各种感染性病毒大部分都是通过网络进行传播，从而导致大范围内的终端中招，影响范围较广。需要对网络访问关系策略进行配置，可以实现业务域之间或者终端之间的网络隔离，从源头上杜绝病毒的传播，减少用户的损失，进一步保证终端的安全。

技术指标

◎**资产清点**：支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和终端账户，支持从资产和终端两个视角进行统计和展示操作系统和监听端口。

◎**策略管理**：支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录。

◎**终端自保护**：针对 Windows 系统，支持实时监控所有非授信驱动及黑客工具的装载、运行等行为，发现风险行为时进行提示和拦截，同时支持设置敏感时间段，监控敏感时段内可疑驱动的装载、运行等行为，发现风险行为时进行提示和拦截。

◎**暴力破解**：统计单个攻击源及分布式攻击源的暴力破解检测，支持按照 RDP、SMB 和 MSSQL 类型进行封堵并自定义爆破阈值，可对封停时间进行自设置。

◎**威胁检测**：具备基于本地缓存信誉检测与全网信誉检测，构建企业全网信誉库的检测引擎，做到企业内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率。

◎**屏幕水印**：支持 windows 系统屏幕水印功能，灵活定义屏幕水印内容，可设置不透明度、生效范围和生效时间段等，如有敏感信息泄露可以通过水印信息辅助做溯源。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0503232104

★有效期：2023 年 06 月 30 日至 2025 年 06 月 30 日

所属品牌：深信服科技股份有限公司

发布时间：2018 年 04 月 07 日

产品适用领域：交通、公安、能源、金融、医疗、媒体、政府、
教育等

产品咨询邮箱：market@sangfor.com.cn



产品咨询二维码

深圳市联软科技股份有限公司

深圳市联软科技股份有限公司创立于 2004 年，专注于企业级网络安全市场，为政企客户提供网络安全产品和服务。深耕金融行业，产品已在银行、保险、证券等金融各细分领域得到广泛应用，在端点安全产品在金融领域市场份额居行业前列，并在制造业、运营商、党政军、医疗、能源和交通等行业构建了较强的市场影响力，已服务超过 3000 家高端行业客户。17 年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、并成为国内率先落地基于“零信任安全”产品的厂商之一。2019 年，联软科技并购魔方安全，获得了以攻击者视角对全网暴露面进行主动持续监控与管理的能力。近 5 年来，联软科技营收以超过 50% 的平均增速在网络安全行业高速增长，并在 2020 年引入中网投、高新投战略投资，正式成为网络安全“国家队”。

网址：<https://www.leagsoft.com/>

电话：0755-86219298

地址：深圳市南山区粤海街道科技园社区科苑路 15 号科兴科学园 A 栋 A2-901

产品名称：联软 UniEDR 终端检测与响应系统（防病毒）

产品概述

联软 UniAV 防病毒系统是联软面向企业客户的端点综合安全防护软件，其内置下一代威胁检测引擎，为各类端点场景提供多层次、全周期的动态防护能力。

UniAV 支持不同网络环境（互联网 / 隔离网 / 混合网络等）的快速部署，并且可以与网络内其他安全设备进行联动，同时支持端点场景全要素采集以支撑态势感知系统。

功能特点

◎病毒检测查杀

采用动态模拟检测技术，提前预判恶意行为，基于海量样本的全体系支撑，后台云计算平台提供病毒 DNA 解析大数据处理，支持智能打击恶意病毒。

支持对木马、病毒、蠕虫、漏洞攻击类、危险程序、勒索程序、挖矿木马、广告程序、恶作剧类程序、后门程序、病毒生成器、木马释放器、黑客程序、可疑加壳的程序等多种病毒类型的查杀。

◎文件实时防护

支持对网页访问、程序下载、文件拷贝等敏感系统边界入口主动发起检测，精准拦截危险文件的落地，将风险隔绝在系统之外。出现病毒威胁时，会根据设置，自动删除病毒文件，或

者锁定病毒文件禁止其运行，等待处理。

支持主动检测外部输入文件，来源包括接入终端设备的 U 盘、网络磁盘、共享网盘、浏览器下载文件、即时通讯下载文件、邮件附件等文件进行主动查杀。

◎专项勒索防护

联软对勒索软件展开了研究，并持续分析大量的、多类型勒索软件样本，最早形成勒索软件相关防护能力。基于勒索软件的原理分析和防御研究，UniAV 建立了针对勒索软件专属的病毒特征库和行为特征库，以海量数据情报和成熟防御模型为基础，推出了“防入侵 - 快速发现 - 应急响应”的防护方案，可以终端设备获得有效的防勒索能力。

◎威胁主动防御（可选）

支持对系统日志、进程行为、系统运行、网络连接等数据进行全方位、细粒度采集；

基于丰富的攻击行为特征库和领先的分析引擎，覆盖 ATT&CK 威胁框架的常见攻击手法，快速发现各种异常行为，同时支持自动化威胁响应机制，实现对高级威胁的有效防护。

◎黑白名单管理

支持文件与目录自定义黑白名单的方式来管理全网终端的文件；

文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；

◎病毒库升级

支持在线 / 离线方式升级服务器 / 终端病毒库。

支持按时升级和流量限速分流，保障网络带宽的正常使用。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106230825

★有效期：2023 年 4 月 14 日至 2025 年 4 月 14 日

所属品牌：联软科技

发布时间：2020 年 5 月 8 日

产品适用领域：制造业、金融业、物流行业。

产品咨询邮箱：Lrkjzjzc@leagsoft.com



产品咨询二维码

沈阳东软系统集成工程有限公司

沈阳东软系统集成工程有限公司 1997 年 3 月 6 日成立，注册资金 7500 万元。公司秉承“超越技术的应用智慧”的经营理念，为客户提供优秀的计算机系统集成解决方案为核心业务方向，以客户为中心，面向政府、公检法和企业的信息基础设施建设，围绕客户的核心业务，提供软件和安全解决方案。业务范围包括：计算机信息系统软件开发、硬件系统安装调试、面向客户的 IT 信息系统规划和建设方案、IT 设施运营维护、技术培训、建筑智能化设计与施工、信息安全服务、商用密码产品的生产及销售等。近年来，在政府、通信、医疗卫生、交通、税务、教育、电力、安全等领域，保持领先地位，市场遍布全国十几个省市地区。

网址：<http://www.neusoft.com>

电话：010-57080489

地址：辽宁省沈阳市浑南区创新路 175-3 号 501、502、503、504、510 室

产品名称：东软 NetEye 终端安全管理系统

产品概述

终端安全往往被理解为杀毒软件，于是公司企业从终端安全厂商那里买来软件，然后让 IT 运营员工负责照管这些杀毒软件——任务完成，终端安全！

但刚刚过去的几年里，这一情况发生了很大改变。因为出现了针对性攻击、无文件恶意软件和勒索软件，传统基于签名特征来防护的产品难以发挥作用，取而代之需要以威胁预防、检测和响应上的新技术来满足不断变化的企业安全需求。

东软 NetEye 适时推出面向泛终端安全防护产品——东软 NetEye 终端安全管理系统（东软 EDR），帮助用户解决多形态 IT 资产一体化安全防护需求。

功能特点

东软 NetEye 终端安全管理系统以 PPDR 安全模型动态安全体系为基础，以 AI 大数据技术为支撑、通过云网端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建下一代终端安全系统，能够精确检测已知病毒木马、未知恶意威胁，有效防御 APT 攻击，勒索病毒，并提供终端资产管理、漏洞补丁管理、安全运维管控、软件管控等多功能。

◎终端资产统一盘点

终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端，虚拟机，云端服务器，工控机，云桌面等。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、资产位置等。每一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

◎多维度恶意软件检测

传统的终端防病毒检测技术使用特征匹配，使得病毒特征库越来越大，运行所占资源也越来越多。东软终端安全产品使用多维度轻量级的多特征检测技术，包含 AI 技术引擎、行为引擎、云查引擎、全网信誉库等，检测更智能、更精准，响应更快速，资源占用更低消耗。

◎勒索病毒防御

通过加密文件索要赎金的勒索病毒攻击方式越来越流行，东软终端能够非常精准的识别不同的勒索软件家族，并通过专业分析识别出种种勒索病毒感染行为和加密特征，对最新的勒索软件进行有效的查杀，防止用户感染最新的勒索软件。

◎微隔离技术

传统的安全设备无法管控东西向流量，内网威胁传播路径无法可视化，东软终端安全产品提供基于代理形式的微隔离方案，使得端点安全可视可控，精细化微隔离，简单落地，高效运维大大降低威胁影响范围。

◎多产品安全协同

该产品能与东软安全网关，东软安全运营管理平台，东软日志审计系统，上网行为管理等产品进行产品进行协同联动响应，关联在线数安全设备的反馈威胁情报数据，智能分析精准研判，超越传统的黑白名单和静态特征库，为已知未知威胁检测提供有力支持。

技术指标

支持最大终端数 1000 个。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106231999

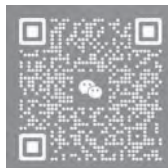
★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：东软 NetEye

发布时间：2020 年 9 月

产品适用领域：电力、医院、政府，等

产品照片：



产品咨询二维码

产品咨询邮箱：cuijin@neusoft.com

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：腾讯 iOA- 网络防病毒系统

产品概述

产品通过终端安全、身份安全、链路安全与零信任策略中心联动构建完整的零信任办公体系，对业务访问的整个过程进行持续的权限控制和安全检查，实现终端在任意网络环境中安全、稳定、高效的访问企业资源。

终端的管控是企业的核心需求之一，也是 iOA 产品的核心技术点之一。基础平台构建好之后，针对信创平台 iOA 基于零信任安全理念，高优先级需要支持设备安全。终端管理是设备安全中不可缺少的核心部分。企业通过终端管理实现企业安全基线的一致性，设备的统一性。

功能特点

◎可信身份验证

在对用户授予企业应用的访问权限之前，提供包括企业微信扫码、Token 双因子认证在内的多种身份验证方式，验证所有用户的身份，以防止网络钓鱼和其他访问威胁。

◎可信设备安全

在设备接入内网之前以及接入运行后，通过终端安全管理模块，持续检查设备安全状态，更好地透视与管控企业内网环境，限制任何不符合安全要求的设备对内网的访问。

◎可信应用访问

根据特定用户 / 用户组的职能以及需求授予访问权限，确保用户在接入内网后只能访问到权限内的应用和数据，实行最小权限原则，更好地保护敏感生产环境的访问安全。

◎高级威胁检测与告警

透视全网终端安全态势，秒级发现入侵隐患，云端联动最新威胁情报，对于高级威胁事件即时产生告警、快速响应并极速处置收敛风险。

◎多维度狙击信息泄露

从外设、文件、存储等多维度多层面保护企业敏感数据资产，对终端用户的泄密行为进行记录、告警、阻断，并对终端用户行为进行审计，提高员工保密意识。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：国家计算机病毒应急处理中心计算机病毒防治产品检验实验室

★证书编号：24BD00299-A

★有效期：2024年03月08日至2026年03月08日

所属品牌：腾讯安全

发布时间：2020年5月15日

产品适用领域：泛互、金融、政府等

产品照片：



产品咨询邮箱：amerlinwang@tencent.com



产品咨询二维码

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信终端威胁防御系统

产品概述

天融信终端威胁防御系统（TopEDR）是天融信依托Gartner提出的EDR技术理念，面向企业级客户设计的一款终端安全检测与响应产品。产品基于预防、防御、检测、响应一体化的安全体系赋予终端威胁防御能力，提供持续的检测分析，采用基因识别、虚拟沙盒、动态启发扫描、主动防御、微隔离等技术实时动态感知威胁行为，精准识别各种已知威胁和未知威胁，有效预防、抵御各类流行病毒以及勒索软件对终端的入侵，洞察威胁本质，帮助客户快速检测、响应终端安全问题，全面提升终端安全防护能力。

功能特点

◎基因识别

天融信终端威胁防御系统采用的基因识别技术快速解决变种病毒，它基于病毒种族的核心理基因特征，区别于传统引擎的特征一一匹配方式，通过核心理基因特征信息提取对病毒种族进行识别，病毒归属于该种族范围内，核心理基因就不会发生变化，因而可以对病毒变种进行查杀

防护。

◎虚拟沙盒

天融信终端威胁防御系统采用领先的虚拟沙盒技术，该技术设计了完备的操作系统环境仿真，模拟超过 5000 个 API，涵盖了绝大多数操作系统的核心机制，包括但不限于：

★文件系统：存储着核心系统文件，并可以跟踪虚拟沙盒内进程执行时创建和修改的文件，反病毒引擎在并发扫描时，不同虚拟进程拥有隔离的文件系统视图；

★进程、线程、同步对象、调度、时钟：虚拟沙盒仿真完备的进程、线程对象，并根据虚拟时钟及调度逻辑对线程进行调度，可以有效地“跑开”Themida 等多线程解码的壳；

★窗口系统：虚拟沙盒还实现了复杂、庞大的窗口系统，以及多中窗口控件，著名的 TrojanDownloader/Upatre 家族混淆器即通过 Edit/RichEdit 控件的各种消息和窗口特性来作为反虚拟机的手段。

◎脱壳

虚拟沙盒反病毒引擎通过指导脱壳技术和通用脱壳技术来解决恶意代码加壳问题。

指导脱壳：通过虚拟机的调试接口，模拟调试的过程动态还原原始代码和数据。

★可跨平台；

★控制逻辑编写简单；

★可以控制精确定位到原始入口点；

★编写控制逻辑的复杂度和时间成本远远低于静态脱壳。

通用脱壳：不对壳进行识别，通过虚拟机动态执行带脱壳程序，通过启发式分析判断停止条件。

★可跨平台；

★无需编写任何控制逻辑；

★可以脱未知壳（包括各种自定义壳和混淆器）。

◎行为分析

虚拟沙盒行为分析通过虚拟机执行引擎来实现，可以跟踪和记录运行在其中程序的行为，反病毒引擎通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估。

虚拟机化执行引擎负责实现指令集仿真，虚拟沙盒实现了两个执行引擎：

★虚拟化执行引擎

通过虚拟化技术，为目标代码划分独立的地址空间，并通过接管中断和异常为目标代码分配私有时间片，从而使目标代码得以受控执行。执行效率几乎可以达到与真实机相当，仅执行环境切换带来微量开销；

★动态翻译执行引擎

通过对目标代码进行分析并可控地翻译成本地代码执行的技术称为动态翻译，虚拟沙盒通过动态翻译执行引擎实现对目标代码的细粒度控制。

前期在脱壳过程中已通过启发式分析算法对调用函数和库文件进行初步评估，对于调用对系统没有危害的函数和库的文件，通过虚拟化执行引擎进行浅层执行，速度快，效率高；对于调用对系统可能有危害的函数和库的文件执行动态翻译，细粒度分析，跟踪行为序列判断是否对系统有破坏。

技术指标

系统部署采用 C/S 架构，管理采用 B/S 架构，管理员只需通过浏览器登录管理中心，即可对系统进行管理。

CentOS7.6 及以上版本、欧拉 64 位，采用 Docker 部署方式，能够快速恢复，横向扩展，可移植性强。

客户端至少支持 WindowsXP、Windows 7、Windows 8、Windows 10、Windows 11 等 32 位 /64 位终端操作系统，支持 Windows server 2003、Windows server2008、Windows server 2012、Windows server 2016、Windows server 2019 等 32 位 /64 位服务器操作系统。

Red Hat Linux、Ubuntu Linux、SuSE Linux、CentOS、Debian

支持中标麒麟、银河麒麟、中科方德、深度、UOS 等国产操作系统。

客户端安装后至多占用 50M 硬盘资源，日常内存占用不到 30M，有效节省 PC/Server 资源。

支持动态认证，根据终端用户的 IP、计算机名、部门等条件设置终端动态认证策略，配置动态认证策略可以在用户登录系统时进行口令认证，确保终端用户间的安全访问。支持一键启用、一键禁用、一键重置口令。

设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。

支持文档检测功能，针对终端存储的 word、pdf、ppt、Excel、rtf、txt 等文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。

支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读_运行）和启用读写、启用（读写_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外 USB 设备。

产品安全认证或安全检测结果证明等

(1) 计算机信息系统安全专用产品销售许可证

★证书编号：0106231302

★有效期：2023 年 6 月 2 日至 2025 年 6 月 2 日

(2) 计算机信息系统安全专用产品销售许可证

★证书编号：0106231681

★有效期：2023 年 6 月 16 日至 2025 年 6 月 16 日

所属品牌：天融信

发布时间：2017 年 4 月

产品适用领域：政府、教育、医疗、企业、交通、公检法、能源等

产品照片：



产品咨询二维码

产品咨询：feng_chong@topsec.com.cn

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，国有资本占股近 50%。

基于“安全协同·AI 赋能”的战略理念，公司在工业互联网安全领域持续深耕，团队核心成员是中国工业互联网安全事业的第一批践行者。

长扬科技在业界开创了“智能工业安全大脑”的产品理念，以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了 60 余款产品，面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉 AI 安全分析、工业零信任安全、工业数据安全和工业数据通信等多维度产品，构建覆盖工业互联网安全产业完整生命周期的安全保障体系。

公司总部位于北京，并在西安、武汉、郑州、成都、上海、广州等全国近 30 个城市建有研发中心及服务分支机构，形成了覆盖全国的“网状战略布局”，可为客户提供强有力的本地化服务。长扬科技积累了超过 32 个行业细分领域、4000 余家工业企业的安全服务经验，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，提供 4 大类、27 项标准化服务，致力于为工业企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：<https://www.cy-tech.net/>

电话：010-82194186

地址：北京市海淀区闵庄路 3 号四季慧谷·国家网络安全产业园 2 期 15 号楼

产品名称：长扬防勒索软件 V2.0

产品概述

长扬科技基于对工业互联网的深刻理解和实践经验，以数据保护为核心，推出工业数据防勒索解决方案，从评估加固、攻击检测、备份容灾方面对数据存储过程中的勒索攻击进行防御，建立业务不停、网络不断、数据不丢的工业数据安全防护体系。

长扬防勒索软件产品具有检测、防护、备份恢复三大功能，可以对勒索攻击进行精准阻击，帮助工业企业提升业务系统自身免疫力，保护核心数据及业务环境，降低勒索攻击发生几率。同时结合网络安全保险，还可以降低客户在勒索攻击发生后的经济损失。

功能特点

◎以数据保护为核心，融合多重检测技术

长扬防勒索软件产品从评估加固、攻击检测、备份容灾、网络安全保险等多方面建立数据

存储、使用过程中的勒索攻击主动防御体系。

事前：评估风险，加固系统，减少网络暴露面，阻断传播途径。

事中：实时检测攻击，精准识别已知和未知勒索攻击。

事后：核心数据备份、系统容灾、保险理赔，保障业务不间断持续运行。

◎全网持续监测，第一时间发现勒索攻击

长扬防勒索软件采用数据访问基线为核心的智能分析与识别技术，识别和阻断文件遍历、文件加密等数据异常访问行为，高效识别各类已知与未知的勒索攻击。

数据访问基线：深度学习 + 动态行为分析，频繁读写、进程终止、文件加密、备份删除等可疑行为，阻断访问，隔离可疑程序。

勒索病毒检测：专业勒索病毒查杀引擎，轻量化病毒库；已知病毒、加壳病毒；资源占用小，误报率低。

勒索攻击诱捕：模拟生产成数据库文件、工艺图纸、代码等高价值数据，诱使勒索软件来访问，主动发现勒索行为。

◎系统级容灾备份，分钟级恢复核心数据和业务环境

在遭受攻击后，通过长扬防勒索方案的数据备份还原与容灾恢复机制，可以分钟级恢复核心数据和业务环境，保证业务的连续性。

文件保险箱：在本地磁盘划分出安全空间用于备份重要数据，对其中的数据进行加密保护，并且安全空间内的数据只有可信的进程才能访问，攻击后快速从安全空间恢复数据。

系统级容灾：采用实时复制、介质同步技术，对应用系统和数据实时备份、本地高可用、一体化集成保护、异地业务持续性容灾。

更高备份效率、更短恢复时间、更小数据丢失量。

◎结合网络安全保险，降低攻击后经济损失

通过将保险与网络安全产品进行有机结合，长扬科技针对勒索攻击提供数据安全专项保险服务，帮助客户减少勒索攻击带来的经济损失。

营业中断损失：因勒索攻击造成被营业中断而产生的经济损失和必要且合理的维持费用。

网络安全防御费用：因发生攻击事件，为避免和减少损失扩大，对系统、软件进行防御、修复、升级所发生的必要且合理的费用和支出。

数据恢复费用：因攻击事件造成数据丢失、损毁、修改、损坏、删除后，为恢复数据所发生的合理费用及支出。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：国家计算机病毒应急处理中心计算机病毒防治产品检验实验室

★证书编号：23BD00097-A

★有效期：2023年9月22日至2025年9月22日

所属品牌：长扬科技

发布时间：2023 年 9 月 23 日

产品适用领域：能源、石油石化、轨道交通、智能制造等工业企业

产品照片：



产品咨询二维码

产品咨询: guodong.zhang@cy-tech.net

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望高级威胁检测系统

产品概述

远望高级威胁检测系统采用了创新的应用级沙箱和环境感知技术，集成 AV 和 IDS 辅助检测模块，并引入威胁情报体系，构成分层检测架构，有效地弥补了传统的特征检测技术以及传统沙箱技术的不足，能够高效地感知和防御 APT 攻击。

功能特点

◎强大的 APT 检测功能

远望高级威胁检测系统的 IDS 模块可以有效检测溢出攻击、恶意木马、跨站攻击等已知威胁；AV 模块能够检测各类已知病毒样本，且可以提高沙箱检测性能；沙箱模块支持各类 Windows 和 Android 系统，可以追踪样本对系统进程、内存、注册表等各类交互行为，是检测未知漏洞的利器；威胁情报模块可以针对恶意 IP、恶意 URL、恶意域名、恶意 Email 等提供预检测能力；自定义策略可以基于 Email、Web 访问、远程控制、文件传输、端口检测等内容，为用户提供了灵活的威胁检测能力。

◎完整的威胁情报体系

全面：与知名威胁情报平台实现情报及时共享

准确：从沙箱检测到的恶意样本中提取威胁情报，形成准确的内部威胁信息

及时：本地威胁情报与云端威胁情报最快可以实现分钟级同步

◎清晰的威胁可视化

面向决策者提供简洁、直观的威胁呈现界面，如全网安全态势、攻击路径、威胁趋势等综合统计信息，协助决策者制定下一步安全防御策略。

面向分析人员提供专业、详尽的威胁信息展示，基于交互式可视化分析技术，协助安全运维人员快速定位攻击来源、攻击组织、攻击手段以及受损主机等，方便快捷地进行溯源取证和责任判定。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0108230118

★有效期：2023 年 01 月 20 日至 2025 年 01 月 20 日

所属品牌：远望

发布时间：2018 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询：mail@chinayuanwang.com



产品咨询二维码



安全操作系统

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 10000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.wincssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特工控主机卫士

产品概述

威努特工控主机卫士产品（以下简称“工控主机卫士”）是国内首款针对操作员站、工程师站、数据服务器等工业现场主机进行安全加固的软件产品。产品颠覆了传统防病毒软件的“黑名单”思想，采用与其相反的轻量级“白名单”机制，可以有效阻止包括震网病毒、Flame、Havex、BlackEnergy 等在内的工控恶意程序或代码在工控主机上的感染、执行和扩散。

产品包括单机版和集中管理版两种形态，其中集中管理版可以对分布安装的工控主机卫士执行统一的管理，包括软件配置、策略制定与下发、日志管理等。

工控主机卫士目前运用于各行业主机操作系统中，其优良的用户体验效果和兼容性让工控主机卫士在众多工控企业中深入使用，管理强度深入到硬件驱动层，有力的保护了主机系统的安全。

功能特点

◎“四重锁定，两个中心”构建工业主机安全计算环境

★应用锁定

采用“白名单”防护机制，锁定工业主机上应用程序的运行，阻止任何白名单外的程序运行，避免恶意代码、非法程序的运行，最大限度保障工程师站、操作员站以及服务器等重要设备安全稳定运行。

★系统锁定

通过安全基线管理和强制访问控制功能，锁定工业主机运行环境和资源，确保工业主机上的设置符合安全基线策略要求，并按照设定的主客体制定读写访问控制策略进行访问。

★网络锁定

锁定工业主机的网络访问环境，只允许工业主机和特定的服务器之间进行通信，控制恶意代码的在网络内部的传播、扩散。

★外设锁定

锁定外接输入设备的使用，只有经过认证的安全可信的 USB 设备且经过病毒查杀才可以在工业主机上运行，防止通过 U 盘等外接输入设备引入恶意程序，导致感染病毒和泄露敏感数据。

★管理中心和监测中心

通过管理中心实现对网络中部署客户端的状态监测、集中管理，统一策略配置，通过安全日志中心可以实现对安全事件和实时告警的统一收集和分析，动态评估工业主机的安全状态和风险级别。

◎兼容性强，适用各种业务场景

★支持 Windows、Linux 平台，应用程序白名单、主机加固功能二合一的工业主机安全产品

★已适配 70 个 Linux 发行版本，34 个 Windows build 版本，针对操作系统 Build 版本号，内核版本进行兼容性适配并已在多个行业数万台终端上现网应用

★支持大点位工控主机卫士在线管理，满足大规模场景的部署应用

★完美兼容银河麒麟、中标麒麟，统信桌面版和服务器版，凝思、麒麟信安等国产操作系统

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0403231321

★有效期：2023 年 06 月 02 日至 2025 年 06 月 02 日

所属品牌：威努特

发布时间：2019 年 5 月 20 日

产品适用领域：电力、石油石化、轨道交通、钢铁、市政、烟草、智能制造等

产品照片：



产品咨询二维码



产品咨询邮箱：support@winicssec.com

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等 70 余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

产品名称：绿盟主机卫士

产品概述

绿盟主机卫士是一款面向工业控制系统中的监控主机、工程师站、操作站、数据服务器等设备进行安全加固的终端安全防护产品。针对工控终端业务环境相对固定、稳定第一的特点，系统采用了白名单机制，拦截一切未知程序和脚本的执行，既可有效抵御已知和未知的恶意代码，又规避了传统杀毒软件病毒库更新不及时的问题，从根本上保障主机运行环境的安全。

绿盟主机卫士支持全系列 Windows 操作系统和主流 Linux 操作系统，产品适用于 SCADA、DCS、PCS、PLC 等工业控制系统中的各类终端设备，已被广泛的应用到石油石化、天然气、电力、智能制造、水利、铁路、城市轨道交通、城市市政以及其他与国计民生紧密相关领域的工业控制系统。

功能特点

◎应用程序白名单防护

应用程序白名单：禁止白名单以外的非法进程运行，产生安全事件

程序完整性检查：通过证书、校验值等确认程序的完整性，从而阻止被病毒感染、篡改的程序运行。

◎脚本白名单防护

支持常见的 .bat,.cmd,.vbs 等脚本格式。

白名单之外的脚本文件被禁止执行。

USB 设备白名单防护

USB 设备识别：支持通用 USB 设备识别。

USB 设备授权：提供 USB 存储设备的多种操作权限授予：读写、禁止使用。

USB 设备白名单：禁止白名单以外的非法 USB 设备连接，产生安全事件。

USB 设备审计：提供 USB 存储设备的操作记录，此记录不可删除、不可篡改。

安全 U 盘

数据分区存储：安全 U 盘有两个分区：公共区和加密区。公共区数据明文存储，可被所有机器存取，该区用于与外网交换数据；加密区数据加密存储，只能被装有卫士的机器存取，实现专区专用。

分区策略单独配置：可以对安全 U 盘的两个分区单独配置使用策略，可配置的策略有：自由使用、禁用、只读（禁止向 U 盘拷贝数据）。管理员可根据工控主机的不同密级要求灵活配置安全 U 盘的使用策略。

自动挂载：安全 U 盘插入装有卫士的机器后加密区会被自动挂载，无需用户其他操作，即插即用。

透明加解密：加密区在数据写入时自动加密，在数据读取时自动解密，用户无感知，不改变用户使用习惯。

硬件加密：加密区数据采用专有硬件加密芯片，加解密速度快，加密算法采用高强度的 sha256 有效防止暴力破解导致的数据泄密。

客户私有 ID 配置：每个安全 U 盘都配置有客户专属的 ID，此 ID 只能被卫士读取，从而保证安全 U 盘的加密分区只能被装有卫士的机器挂载，不同客户的安全 U 盘也无法混用。

◎主机加固

自定义文件保护：支持用户对系统的关键文件、目录进行保护，被保护的文件无法被修改或删除。

自定义注册表保护：支持用户对自定义的注册表关键路径进行保护，被保护的注册表路径无法被修改或删除。

自定义进程保护：支持对重要业务进程进行保护，防止被恶意程序杀死。

安全策略配置：支持对操作系统的密码策略、审核策略、默认共享等安全策略进行统一配置。

◎白名单管理

白名单生成：通过一键固化，自动扫描功能，建立白名单；

白名单导入导出：提供白名单的导入导出功能

白名单的手动更新：支持告警程序的一键加白；支持基于目录的程序扫描追加；

手动软件更新：支持本地手动安装软件，并追加更新的程序到白名单库中；

软件智能更新：支持基于软件更新平台的自动化软件更新和基于信任软件库的软件更新场景下的更新程序自动追踪，并添加到白名单中，不影响更新后软件的使用；

补丁智能更新：支持操作系统的补丁更新，系统后台智能跟踪更新过程，并将更新文件追加到白名单库中。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00382-A

★有效期：2024年3月29日至2026年3月29日

所属品牌：绿盟科技

发布时间：2020年

产品适用领域：电力、水利、智能制造、石油石化、化工、冶金、有色、市政、交通、烟草、机械加工等

产品照片：





公钥基础设施

北京数字认证股份有限公司

北京数字认证股份有限公司（简称“数字认证”）是国内领先的网络信任与数字安全服务提供商，公司成立于 2001 年 2 月，是首批获得电子认证服务许可资质的大型国有控股企业。公司 2016 年在深交所上市，被誉为“中国电子认证第一股”（股票代码：300579）。经过近 20 年的发展，公司以密码技术为核心，形成了网络信任服务、数字资产保护、网络安全服务的业务格局，应用覆盖政务、医疗、金融、教育、交通、电信等多个行业，为近千万企业用户和数亿个人用户提供网络安全服务。

网址：<https://www.bjca.cn/>

电话：4009-197-888

地址：北京市海淀区北四环西路 68 号（左岸工社）15 层（100080）

产品名称：密钥管理系统

产品概述

密钥管理系统产品由北京数字认证股份有限公司（简称：数字认证）自主研发，面向电子政务、金融、电力、交通、医疗等各个领域，为用户提供密钥的全生命周期管理、以及数据加解密服务。产品提供应用密钥、加密密钥、分散密钥、设备密钥等多种密钥类型，支持各种密码应用场景，并对外提供密钥 API 服务，包括密钥申请、密钥更新、密钥归档、密钥注销、密钥加解密等接口。

另外，产品支持分布式部署，使用密码设备存储密钥及密钥运算，支持管理员行为、接口事件等安全审计日志，支持密钥数据备份和恢复，并遵循《信息安全技术 SM4 分组密码算法》、《信息安全技术 SM3 密码杂凑算法》、《SM2 密码算法使用规范》、《SM2 密码算法加密签名消息语法》等标准规范，是国密局认可的商密产品。

功能特点

◎符合国家标准规范：符合国家密码管理局、工业和信息化部等国家有关标准规范要求，获得商用密码产品认证证书，并入围国家信创目录。

◎支持多种类型密钥和模板：包括加密密钥、分散密钥、应用密钥、设备密钥等，并且支持产生和配置多种密钥模板。

系统的灵活配置：系统具有可视化的配置界面，提供灵活的各种配置菜单，可以根据用户的需要，对系统关键参数、密钥模板进行配置，并实时生效。

◎支持多种加密设备：为密码设备提供扩展机制，对符合国家密码管理局规范的密码设备，通过统一接入规范即可统一注册管理。

◎产品的开放性：提供完整的开发套件，与应用系统进行接口对接，可为应用系统提供密钥全生命周期管理服务，支持 KMIP 协议。

技术指标

产品型号	KMS	KMS-A8001
产品商密型号	SYT1925	SYT1812-G
支持算法	SM2、SM3、SM4、AES、RSA2048、SHA256 等	SM2、SM3、SM4 等
	操作系统： CentOS、RedHat 等	操作系统：中标麒麟、银河麒麟、统信等 CPU：飞腾、龙芯、鲲鹏等
	数据库： Mysql、Oracle 等	数据库：人大金仓、南大通用、达梦、神通等
	中间件：Tomcat 等	中间件：东方通、金蝶、宝兰德、中创等
	密码机：数字认证、卫士通、兴唐、三未信安、得安、奥联、国泰网信、数盾等	密码机：数字认证、三未信安
密钥容量	千万级	
系统性能	SM2 解密 >8000TPS、SM2 签名 >8000TPS RSA2048 解密 >4500TPS RSA2048 签名 >3000 TPS SM4 加密速率 >10000TPS SM4 解密速率 >10000TPS SM4 产生速率 >4000TPS	
并发访问	支持 1000 个并发连接访问	

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00152-A

★有效期：2023 年 10 月 13 日至 2025 年 10 月 13 日

所属品牌：数字认证

发布时间：2023 年 10 月 13 日

产品适用领域：政务、医疗、金融、交通、教育、企业

产品照片：



产品咨询邮箱：marketing@bjca.org.cn



产品咨询二维码

北京天威诚信电子商务服务有限公司

北京天威诚信电子商务服务有限公司（以下简称：天威诚信）于 2000 年 9 月在北京成立，2005 年获得首批国家密码管理局颁发的《电子认证服务使用密码许可证》、工业和信息化部颁发的《电子认证服务许可证》。

天威诚信致力于成为数字时代安全可信支撑体系的核心力量。以法律为标准，以电子认证行政许可为依托，以数字化技术为手段，支撑构建安全可信的数字应用生态，推动数字经济安全、合规发展。运用密码、区块链、大数据、人工智能、云计算等技术，将立法标准、司法实务标准与密码应用规范、电子认证业务规范相融合，构建完整的法律科技服务体系，为数字世界中的人、事、物、时、空提供真实性证明服务，为数字世界法治生态建设提供支撑保障，守护数字世界秩序。

北京天诚安信科技有限公司（以下简称：天诚安信）作为天威诚信的全资子公司，成立于 2011 年 5 月，是一家集自主研发、生产、销售、服务为一体的高新技术企业，专业从事拥有自主知识产权的数字身份标识、身份管理、安全认证系统和密码安全产品的应用开发及客户服务。

天诚安信核心技术团队始于 2000 年原信息产业部（现工业和信息化部）商业数字认证（PKI）国际合作技术开发项目，是国家认可的第一支纯商用 PKI 技术团队，主导建设了北京天威诚信数字认证中心。

网址：<https://www.itrus.com.cn/>

电话：4006663999

地址：北京市海淀区上地八街 4 号院 401

产品名称：密码服务管理平台

产品概述

密码服务管理平台是北京天威诚信电子商务服务有限公司（简称：天威诚信）自主研发，面向政务、集团企业、教育、交通等各个领域，为用户提供一站式的安全密码服务。产品可提供身份认证、数字证书、数据加密、密钥管理、协同签名、电子签章等密码服务可满足各种密码应用场景需求，提供安卓、IOS、鸿蒙、JavaScript、Java、C 等技术语言的 API 接口和 SDK 便于各种类业务应用的安全集成需求，提供一体化的管理可实现硬件密码设备管理、密码服务管理、租户管理、应用接入及授权等管理功能降低客户管理成本，提供可视化数字大屏便于客户运营人员实时观察密码服务运行情况和各应用密码使用情况等。

功能特点

统一应用接入授权能力：对可接入的业务应用统一授权，有效抵御非法应用攻击。

密码设备统一管理能力：提供多个厂商多种种类及形态的密码设备接入能力，实现密码资产的统一接入、集中管理、统一配置管理能力。

密码服务统一管理能力：提供身份认证类、签名验签类、数据加解密类、发证服务类管理能力，实现部署包统一管理、统一配置、统一发布、制定服务启停能力。

不同密钥统一管理能力：提供主密钥、密钥加密密钥、数据加密三级密钥体系，实现不同类型不同算法、不同密钥长度密钥统一管理能力。

技术指标

产品型号：TopCSP

支持算法：支持国密 SM1、SM2、SM3、SM4 等算法和国密 AES、SHA256、RSA2048、RSA3072、RSA4096 等算法。

操作系统：LinuxCentOS、Ubuntu、统信 UOS、麒麟、龙芯等。

数据库：MySQL、人大金仓、瀚高、达梦等。

中间件：宝蓝德、东方通、中创等。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01635-A

★有效期：2024 年 11 月 08 日至 2026 年 11 月 08 日

所属品牌：天威诚信

发布时间：2023 年 3 月 28 日

产品适用领域：集团企业、政务、教育、交通、工业互联网、物联网等领域

产品照片：



产品咨询二维码

产品咨询邮箱：marketing@itrus.com.cn

北京信安世纪科技股份有限公司

北京信安世纪科技股份有限公司（股票代码：688201）成立于 2001 年 8 月，是科技创新型的信息安全产品和解决方案提供商。公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全、通信安全等基础性安全问题，为金融、政府、企业、军队等重要领域的核心业务系统提供先进的网络安全产品与安全解决方案。

网址：www.infosec.com.cn

电话：010-68025518/400-670-5518

地址：北京市海淀区建枫路（南延）6 号院金隅西三旗科技园 2 号楼信安大厦

产品名称：NetSign 签名验签服务器

产品概述

信安 NetSign 签名验签服务器，由提供独立签名运算的服务器设备 (NetSign Server)、应用开发 API (NetSign Agent) 和客户端签名组件组成，为关键业务提供了一套基于 PKI 系统架构、支持不同应用的完整且独立运行的电子签名解决方案，从而保证关键业务应用中交易过程的机密性、信息完整性、不可否认性和事后追溯性。本产品适用于网上银行、支付清算、财务管理、电子政务、网上审批等需要支持等保要求或强审计要求的业务应用，可支持信创部署要求。

功能特点

◎ PKI 和密码功能

- ★支持 PKCS#1、PKCS#7、CMS、GB/T 35275 规范标准的签名验签
- ★支持 RAW，Attach、Detach 格式的签名验签
- ★支持 PDF 签名验签
- ★支持密数字信封，带签名数字信封加解密
- ★支持产生随机数，对称、非对称加解密，Hash 和 Mac 运算

◎管理功能

- ★证书申请、导入、备份、恢复等管理功能
- ★对称密钥、非对称密钥、公钥证书的产生、删除等管理功能
- ★系统备份、恢复、升级等管理功能

◎监控功能

- ★支持监控系统资源使用情况，根据 CPU 使用率，风扇转速，CPU 温度等控制指示灯状态
- ★支持签名服务监控，包括对 NetSign、DownLoadCRL 等服务的监控

★支持对接 SNMP 监控，支持 v1v2 协议，支持自定义 Trap 规则

★支持配置远程 Syslog 服务器

◎信创适配

★可提供海光、飞腾、兆芯的服务器设备

★可提供支持多种信创环境的客户端组件

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01612-A

★有效期：2024 年 11 月 01 日至 2026 年 11 月 01 日

所属品牌：信安世纪

发布时间：2023 年 5 月

产品适用领域：金融、电力、交通、人社、财政、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：market@infosec.com.cn

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神国密安全密码应用中间件

产品概述

奇安信网神国密安全密码应用中间件，将“密改集成、密钥管理、资源调度、运行感知”融为一体，将集约化经验赋能客户的业务系统，降低前期改造及后期管理成本，同时，还具备免代码改造的数据库加密能力，业务系统仅需“复制插件+修改配置”即可完成数据存储机密性、完整性改造，精确到字段级加密，“一字段一密钥”，精细化管理加密策略，让客户更便捷地享受合规的商密赋能。奇安信网神国密安全密码应用中间件同时支持本地私有化部署，以及基于云场景多租户 VPC 隔离的部署模式，使密钥管理更加安全。

功能特点

◎统一密码服务接口功能

统一密码服务接口模块能够屏蔽底层密码设备的差异，这些密码设备可能提供诸如 P11、JCE、SDF、SKF 等多种多样的密码服务接口，导致信息系统集成工作复杂度高、工作量大。统

一密码服务接口能够对上提供统一的数据 / 文件加密解密、数据库透明加解密、签名验签、杂凑运算、消息认证码运算、时间戳、数字证书、数字信封等密码服务接口，方便业务应用集成密码。

◎密钥管理功能

密钥管理模块能具备国密算法的密钥管理能力，可通过密钥分散技术进行密钥的生成、更新、备份；同时支持对接具有商密产品认证资质的密钥管理系统的能力。提供完整的密钥生命周期，保障密钥安全。

密钥管理模块能够在一定程度上替代外部协同工作的密钥管理系统，使信息系统不用购买部署密钥管理系统也能够先期进行密码应用的开发。

◎密码设备管理功能

密码设备管理模块能够兼容不同厂商的各类异构密码设备。由于密码设备与信息系统深度绑定，品牌、种类不同的密码设备难以做到互相兼容，密码设备管理模块以统一的连接器模式管理，对上层信息系统屏蔽密码设备间差异，达到密码设备统一注册、监控、告警等管理目标。

◎密码计算资源调度功能

密码计算资源调度模块能够以会话的模式管理计算资源，以科学高效的算法调度，从而最大程度地利用好这些算力资源，避免算力浪费，提升上层应用计算体验。

◎密码设备模拟器功能

密码设备模拟器模块可以模拟真实的物理服务器密码机、签名验签服务器、时间戳服务器等常见密码设备，对信息系统提供相同的符合《GMT0018-2012 密码设备应用接口规范》的标准 SDF 密码服务接口与密码计算能力。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00177-A

★有效期：2023 年 10 月 20 日至 2025 年 10 月 20 日

所属品牌：奇安信网神

发布时间：2022 年 6 月

产品适用领域：政府、医疗、教育、交通、能源、金融等

产品照片：



产品咨询二维码

产品咨询邮箱：kefu@qianxin.com

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：密钥管理系统

产品概述

密钥管理系统是一款安全管理类服务，可以帮助用户轻松创建和管理密钥，保护密钥的保密性、完整性和可用性，满足用户多应用多业务的密钥管理需求。

功能特点

◎安全合规

密钥管理系统基于经过第三方认证的硬件安全模块（HSM）来生成和保护密钥。

丰富功能：密钥管理系统支持对称加密以及非对称加密算法，为您提供了丰富的管理功能，包括密钥创建、启用、禁用、归档、轮换、导入等密钥的全生命周期管理功能。

支持外部密钥导入：允许用户在腾讯云架构上使用您自有的密钥材料进行敏感数据加解密服务，即在腾讯云上实施 BYOK（Bring Your Own Key）方案。

◎稳定容灾

采用多机房分布式集群化的业务部署和热备份，底层 HSM 设备采用双机房冷备份部署，确保密钥管理系统的高可用性。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405232056

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：腾讯安全

发布时间：2019 年 01 月 18 日

产品适用领域：金融、出行、医疗、零售

产品照片：



产品咨询二维码

产品咨询邮箱：jessejcchen@tencent.com

长春吉大正元信息技术股份有限公司

长春吉大正元信息技术股份有限公司是中国领先的数字安全综合服务商，1999年成立，2020年在深交所挂牌上市，是国家网络空间安全及数字安全建设引领者，我国密码安全、电子认证、身份信任等领域领军企业，国内最大的公钥基础设施（PKI）产品供应商之一，国家数字安全科研项目、标准建设的主要参与者，国家重大活动的安全保障参与者。

吉大正元坚持技术创新，以密码技术为核心打造了密码安全、身份信任、数据安全、系统安全、网络安全、应用安全、业务安全等完整的数字安全产品体系、解决方案和服务能力，以及新一代数字安全体系“元安全”，涵盖数字安全防护设施与智能操作系统，提供数字经济安全运行环境，为数字经济发展和数字中国建设中的各行各业关键信息基础设施提供安全支撑与保障。

公司资质体系完善，服务覆盖政务、金融、能源等多行业客户，广泛参与建设国家金字工程，保障全国两会、载人航天、北京奥运会等重大社会、政治活动。据权威机构统计，公司在身份管理和访问控制软件市场的占有率连续多年稳居行业第一。

公司未来将持续探索数字安全与应用和数字经济产品技术，不断为用户提供领先的数字安全产品、服务和全方位数字安全解决方案，全面护航数字经济发展，夯实数字中国安全基石。

网址：www.jit.com.cn

电话：010-62618866

地址：北京市石景山区给古城街道中海时代广场B座16、17层

产品名称：吉大正元密码服务管理平台

产品概述

密码服务管理平台面向应用提供统一密码服务的解决方案，可以为用户提供集中的密码设备资源管理、密码服务管理、应用密钥管理功能，为业务系统提供统一的密码服务功能。密码服务平台主要从密码资源池、业务规划、数据分析、可扩展性等多个维度为用户业务赋能，帮助用户建立综合的密码技术应用能力，支撑用户各种业务系统在等级保护、密码测评等领域的密码合规应用需求。

功能特点

提供按需部署多服务节点，增强平台服务的可靠性及吞吐性能。

提供数据分析总览大屏，大屏提供多维度数据态势分析，提供平台内设备、服务、应用、密钥等的总量展示，提供设备、服务的分类统计展示，提供服务调用的应用排名展示。

具备网关产品集成规范，并提供集成身份认证网关，提供基于证书的身份认证服务。

具备云密码机集成规范，并提供集成多品牌云密码机，支撑虚拟密码机创建、管理、服务启停等管理，提供密码计算服务。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230179

★有效期：2023 年 2 月 3 日至 2025 年 2 月 3 日

所属品牌：吉大正元

发布时间：2020 年 4 月 30 日

产品适用领域：能源、金融、政务、医疗、教育等

产品照片：



产品咨询邮箱：marketing@jit.com.cn

中移互联网有限公司

中移互联网有限公司是中国移动面向互联网领域设立的专业子公司，前身是中国移动互联网基地，2015 年 10 月 30 日在广州注册成立，2022 年 3 月正式入围国资委“科改企业”名单。

公司聚焦“信息+互联网”，胸怀国之大者，勇当信息服务科技创新公司排头兵，成为移动互联网产品创新主力军，利用中国移动的规模、能力、体系优势，与中国移动的网络、技术、数据相融合，面向算力、大数据、人工智能等“9+6”科创战新领域布局，推动“号、卡、云、消息、通话”快速跃迁为新型信息基础设施，并融合打造个人云服务基座、信创安全基座、超大 AI 应用基座，不断延展生态新边界，拓展信息服务新空间，激发 CHBN 价值增长新动能，为两个“做强做优做大”贡献更大力量。目前，中移互联已形成有特色、有规模、有前景的产品体系，6 个产品规模过亿，3 个产品进入行业第一阵营，聚焦互联网、电商物流、金融、党政等重点行业深度开展业务合作，2023 年收入破百亿。作为高新技术企业，公司已累计获得专利 163 项、软著 290 个，拥有 CMMI4 等资质 10 余项，参与了多个国家级项目，并发挥产学研用价值，与国家超算中心、省政数局、高校院士团队等多家单位开展科研合作。

网址：<https://dev.10086.cn/superSIM/portal-main/securityProduct>

电话：020-66600008

地址：广州市天河区高唐路 323 号中国移动南方基地智汇中心 B 栋

产品名称：超级 SIM 量子国密资源池

产品概述

超级 SIM 量子国密资源池以超级 SIM 卡为密钥安全载体，融合国密及量子技术，提供端到端全流程“国密+量子”双密码服务体系，保障安全身份认证、数据加密传输、数字资产保护等场景国密应用合规性、有效性，助力政企快速通过密评密改，还可为各场景叠加量子安全能力，保障网络信息安全。

功能特点

◎融合国密与量子技术，保障合规与安全

超级 SIM 量子国密资源池融合了国密和量子密码服务，提供安全合规的国密应用服务以及量子增强安全服务，满足密评需求的同时，借助新兴量子技术保障系统的安全性。

◎超级 SIM 卡提供硬件级密钥安全

超级 SIM 卡作为客户端侧的密钥硬件载体，提供常用的 SM2/SM3/SM4 国密算法密码服务，具有比密码软模块更高的安全性。每次通信都通过硬件级的加密方式，确保密钥的安全性与保

密性。

◎一次一密，量子密钥协商保障通信安全

量子超级 SIM 卡通过预灌注量子一级密钥 QK，并利用 QK 进行二级会话密钥协商。每次会话都使用唯一密钥，确保每次通信的安全性，优于其他竞品的常规密钥管理方式。

◎全生命周期管理，保障量子密钥的安全性

超级 SIM 量子国密资源池提供量子密钥的统一管理，涵盖密钥的生成、分发、存储及充注。通过全生命周期的密钥管理，确保密钥的完整性和管理的高效性，提升系统的安全性与可靠性。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00822-A

★有效期：2024 年 06 月 14 日至 2026 年 06 月 14 日

所属品牌：中移互联网

发布时间：2022 年 11 月 17 日

产品适用领域：通信、党政、军警司法、金融、医疗、工业能源、央企等

产品照片：



产品咨询二维码



产品咨询邮箱：dengchong9416@139.com



网络安全态势感知产品

安天科技集团股份有限公司

安天是引领威胁检测与防御能力发展的网络安全国家队，依托自主先进核心技术与安全理念，致力于为网信主管部门、军队、部委、保密和关键信息基础设施等高安全需求客户提供整体安全解决方案。安天产品和服务为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等基础能力，建设实战化的态势感知体系，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，赋能客户筑起可对抗高级威胁的网络安全防线。

安天为全球超过一百三十万台网络设备和网络安全设备、超过三十亿部智能终端设备提供安全检测能力；安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑，多次收到相关部门的感谢信。

安天已发展成为以哈尔滨为总部基地，建有七地研发中心、九家控股子公司，拥有一个国家企业技术中心和三个省级重点实验室、工程技术研究中心和新型研发机构，参与一个国家工程实验室建设，建立一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

网址：<https://www.antiy.cn>

电话：010-82893723

地址：北京市海淀区闵庄路 3 号清华科技园玉泉慧谷一期 1 号楼

产品名称：安天可扩展威胁检测响应平台 XDR

产品概述

安天可扩展威胁检测响应 XDR 平台是面向重保、常态化攻防演练等威胁对抗及日常安全运营场景的安全管理平台。

平台能够统筹和调度安全设备与资源，将云/网/端/业务/身份数据融合分析，跨设备跨场景识别风险上下文，实现对网内威胁的智能发现、识别和关联溯源；结合多来源情报信息，对网内威胁对象进行持续检测和监控，形成高置信告警；可快速发现和梳理网内资产并持续监测全网资产及其环境动态，全面排查资产脆弱性、暴露面；自动化研判响应各类风险并提供设备策略管理、智能下发以及验证能力，在提高安全运营效率的同时，保障准确性和可验证性。

安天可扩展威胁检测响应 XDR 平台以全面数据监控、精准威胁发现、高效处置编排、安全能力扩展，构筑闭环安全防线，为用户提供高效易用的威胁持续检测和对抗能力，提升安全管理水平和效率，帮助用户节省时间成本，释放人员精力。

功能特点

◎场景化威胁及异常检测

平台能够融合流量、端点、业务数据进行实时特征、异常指标和上下文关联等场景化分析检测，面向各类安全场景形成了近千条检测规则，涵盖：虚拟专用网异常行为检测、邮件异常行为检测、供应链威胁行为检测、服务器场景检测，漏洞检测等。

◎内外部情报运营检测

平台能够结合威胁监测响应知识和经验固化形成具有强针对性、高命中率、高客户价值的本地运营情报。支持接入外部情报，通过融合内外部情报，对网内发现的 IP、域名、URL、文件等风险对象进行持续检测，形成高置信 / 高风险告警，有效提升网空威胁感知能力。

◎安全编排与自动化响应

平台具备开箱即用、轻量化参数配置的案例式脚本、常用剧本。支持自定义编辑导入脚本、可根据业务场景灵活编排处置剧本。通过策略配置为告警自动匹配剧本，从而自动化处理高置信度风险告警。

◎多手段资产感知与清点

通过主动扫描与被动识别相结合的形式，对资产数据进行有效地快速整合与同步。通过应用检测模块和漏扫数据关联识别资产应用，通过全要素网络信息或可用性扫描信息监测资产在线情况。对漏洞、弱口令扫描结果进行统一管理，对资产暴露的服务、端口进行识别。

技术指标

风险分类覆盖《GB/Z 20986—2023 信息安全技术网络安全事件分类分级指南》中定义的所有风险类型。

支持身份风险检测，包括但不限于：弱口令登录、异地登录、境外登录、暴力破解。

支持将检测结果涉及的 IP 和域名能够自动化的关联终端资产、网站资产以及网络 / 安全设备。

支持资产及 IP 地理位置的可视化呈现，资产定位支持向上级联继承归属分组的定位。

支持通过平台内置扫描组件，探测发现网站类型资产，能够识别主页地址、部署终端、网页 title 等信息，支持获取主页页面元素并生成网页快照。

系统能够自动验证证书的一致性和有效性，能够标记证书过期状态，包含已过期、临近过期和正常。系统能够自动对已过期的网站发送邮件、短信等通知预警。

支持通过告警分析模型，支持根据风险的不同提取不同的要素，形成对象化语义化的告警。

支持自动生成风险画像，以与威胁攻击或受害相关的 IP、资产、网站域名视角形成画像。

支持 ATT&CK 技战术的可视化分析，能够自动关联最近活跃的告警情况并形成地理空间和网络攻击的图示关系链条。

支持对预置和自定义剧本进行管理，包括新建、编辑、删除、导入、导出、有效性验证、执行历史查看、配置自动化等，支持剧本模板，能够基于任意剧本作为模板快速创建新剧本。内置响应处置剧本，包括文件隔离、进程终止、IP/DNS 封堵、主机隔离、失陷断网等常见场景下的快速响应处置剧本。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0503231760

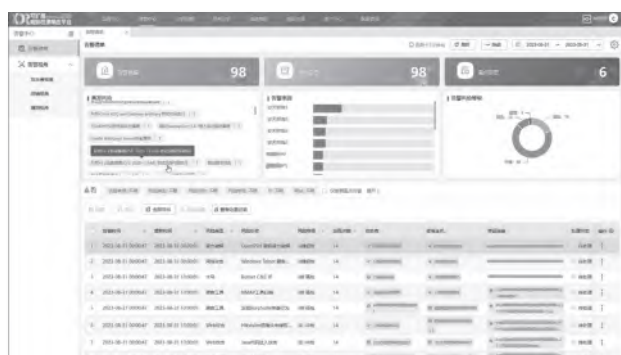
★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：安天

发布时间：2023 年 06 月 30 日

产品适用领域：金融、教育、军工、政府、能源电力

产品照片：



产品咨询二维码

产品咨询邮箱：support@antiy.cn

北京百度网讯科技有限公司

百度是拥有强大互联网基础的领先 AI 公司。是全球为数不多的提供 AI 芯片、软件架构和应用程序等全栈 AI 技术的公司之一，被国际机构评为全球四大 AI 公司之一。百度以“用科技让复杂的世界更简单”为使命，坚持技术创新，致力于“成为最懂用户，并能帮助人们成长的全球顶级高科技公司”。

百度公司 2000 年 1 月 1 日创立于中关村，创始人李彦宏拥有“超链分析”技术专利，也使中国成为美国、俄罗斯和韩国之外，全球仅有的 4 个拥有搜索引擎核心技术的国家之一。百度每天响应来自 100 余个国家和地区的数十亿次搜索请求，是网民获取中文信息和服务的最主要入口，服务 10 亿互联网用户。

基于搜索引擎，百度演化出语音、图像、知识图谱、自然语言处理等人工智能技术；最近 10 年，百度在深度学习、对话式人工智能操作系统、自动驾驶、AI 芯片等前沿领域投资，使得百度成为一个拥有强大互联网基础的领先 AI 公司。

网址：<https://home.baidu.com/home/index>

电话：010 - 59928888

地址：北京市海淀区上地十街 10 号百度大厦 2 层

产品名称：主机安全

产品概述

主机安全（Hosteye）产品是为客户的各类云资产提供全方位安全防护的一站式运营中心。旨在通过整合多种安全功能和服务，为客户的云工作负载、应用程序和数据等资产提供综合性保护，以应对不断演变的安全威胁和风险。

功能特点

资产清点。帮助用户对云服务器内的信息资产进行梳理，杜绝未知资产，便于对客户资产进行有效防护。

病毒查杀。具备 300W+ 的本地病毒特征库，支持对恶意进程 / 恶意文件进行快速扫描、全盘扫描、自定义扫描查杀与隔离处置。

漏洞扫描。具备 25 万 + 的漏洞特征库，支持对 Linux 系统漏洞进行扫描，并提供修复建议

基线核查。根据 CIS 与等保三级的基线检查要求，帮助客户快速进行云服务器的安全基线检查并给出修复建议，支持客户自定义基线检查模板。

异常检测。支持多种异常行为检测，包括反弹 shell 检测、文件异常检测、进程提权检测、文件提权检测。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0503230584

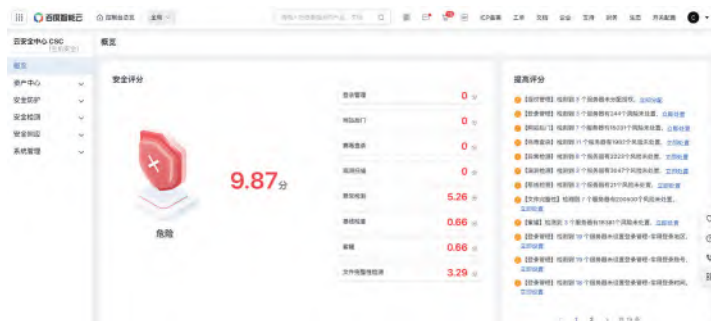
★有效期：2023 年 3 月 24 日至 2025 年 3 月 24 日

所属品牌：百度

发布时间：2024 年 7 月 1 日

产品适用领域：金融、网络技术、互联网、智能制造等

产品照片：



产品咨询二维码

产品咨询邮箱：yuhuan08@baidu.com

北京观成科技有限公司

北京观成科技有限公司成立于 2018 年 8 月，是一家以加密流量检测为核心技术的创新型网络安全公司。自成立以来，荣获“国家高新和中关村高新技术企业”、北京市“专精特新”企业称号，始终坚持“自主研发、持续创新”的技术理念，并已申请 50 余篇加密流量检测相关国家发明专利，拥有基于人工智能的加密流量检测与分析技术、基于可计算机引擎的加密数据研判与筛选技术、面向密码对抗的加密业务态势监测技术、面向攻防博弈的加密类 APT 跟踪分析技术等四大核心技术能力，陆续推出了观成瞰云（ENS）- 加密威胁智能检测系统、瞰峰（ESA）- 加密业务态势感知平台、瞰雾（ETI）- 加密威胁情报平台三款核心产品。其中，瞰云（ENS）荣获 CCIA 2021 创新产品冠军。

公司坚持“重客户，讲诚信，勇创新，敢担当”为企业价值观，利用先进的服务水平和可靠的技术性能，为产品及客户提供全面、优质、高效益的售后服务。同时，为了更好地服务用户，已经建立起了完善的本地化服务支持体系，方便为用户提供 7*24 小时优质、迅速、及时的售后服务和技术支持。

网址：<https://www.viewintech.com/>

电话：010-60608185

地址：北京市海淀区东北旺西路 8 号中关村软件园 17 号楼 2 层 B205 室

产品名称：观成瞰峰（ESA）- 加密业务态势感知平台

产品概述

观成瞰峰 - 加密业务态势感知平台 ESA（Encrypted-network Situational Awareness）是观成科技依托加密流量检测分析以及人工智能等核心技术构建的加密业务态势感知平台，平台集成流量、资产、业务、风险、威胁五大态势，实现加密业务“可感知、可监测、可预警、可追溯”，支撑涉及加密业务的网络空间安全综合管控决策。

该产品以加密流量分析为基础，综合分析流量、业务、资产、风险和威胁等多角度态势信息，构建加密网络空间态势感知能力。产品使用丰富的可视化效果对各类加密资产状态予以呈现，可直观反映加密资产态势信息，自动生成加密资产业务拓扑和物理拓扑，直观展示各类加密资产互连情况。且拓扑图支持自定义增删修改，体现安全投入价值，同时提升响应与处置效率。

功能特点

◎功能

★赋能加密网络空间态势感知

以加密流量分析为基础，综合分析流量、业务、资产、风险和威胁等多角度态势信息，构建加密网络空间态势感知能力。

★支撑关键加密资产识别梳理

针对加密资产进行细粒度识别，提取加密数据、协议、证书等要素，提高加密资产运维效率，降低成本。

基于资产加密要素，有效识别并关联潜在攻击威胁与风险异常，满足重点时期高烈度攻防防护需求。

★聚焦资产视角的加密业务分析

加密资产业务、风险和威胁实时分析与感知，统计和梳理加密应用在网络中的使用情况以加密业务风险、加密威胁和加密流量（流量大小、协议、证书、通联）等多维度统计、分析和检测，辅助决策。

★实时呈现加密资产综合状态

类加密资产状态使用丰富的可视化效果予以呈现，可直观反映加密资产态势信息，体现安全投入价值，同时提升响应与处置效率自动生成加密资产业务拓扑和物理拓扑，直观展示各类加密资产互连情况。拓扑图支持自定义增删修改。

◎特点

★主被动相结合的加密资产识别与拓扑绘制

基于加密要素的加密资产、加密服务识别与分析、基于加密资产信息、网管协议和路由协议分析的加密资产拓扑还原。

★基于加密资产视角的加密网络空间态势分析

掌握加密资产的流量态势、业务态势、风险态势、合规态势、威胁态势加密资产和业务可管、可控。

★全面丰富且支持定制的加密业务态势可视化呈现

多维度、多角度大屏呈现，各类态势一目了然，方便展示、运维，支持定制化展示呈现，安全投入看得见。

★多类型多协议的日志报告上报和纳管能力

支持多种类型、多种协议的高度定制化日志上报。

支持纳管其他流量产品或探针的各类日志数据。

技术指标

◎基于人工智能的加密流量检测与分析技术

机器学习、深度学习，融合规则检测、行为分析等方法，从单流、多流和宏观通联等多维度综合检测与分析。

◎面向密码对抗的加密业务态势监测技术

深度挖掘、加密流量的多维度行为建模，加密业务可感知、可识别、可监测，可关联、可预警，可追溯。

◎分布式实时计算引擎

相对于传统的离线计算会存在数据反馈不及时的问题，很难满足急需实时数据做决策的场景。分布式实时计算引擎，支持实时流 stream 处理和批 batch 处理，有界数据和无界数据进行有状态计算，纯流式处理模式，保证了低延迟。

◎分布式消息队列处理

支持分布式、高可用的部署，消息持久化，并且对一个大的队列分成多个 Partition(分区)，来提高消息入队的吞吐量，分而治之的思想。消费能够支持多个客户端消费同一个队列，并且一个 group 中可以增加 Consumer 的数量来扩展消费的处理量。系统采用的是生产者消费者模型。

◎OLAP 类存储分析引擎

适合场景：适合响应时间要求高的分析场景。

存储引擎的特点：

★完备的 DBMS 功能

拥有 DBMS 完备的管理功能，但它不仅仅是一个数据库。作为 DBMS，它具备以下基本功能。

DDL（数据定义语言）：可以动态地创建、修改删除数据库、表和视图，而无须重启服务。

DML（数据操作语言）：可以动态查询、插入、修改或者删除数据。

权限控制：可以按照用户粒度设置数据库或者表的操作权限，保障数据的安全性。数据备份与恢复：提供了数据备份导出与导入恢复机制，满足生产环境的要求。分布式管理：提供集群模式，能够自动管理多个数据库节点。

★列式存储

相比于行式存储，列式存储有如下优点：

我们在做统计某些指标的聚合值时，往往需要查询海量的行，仅仅需要少量的列。在列式存储的模式下，只需要读取与计算有关的列即可，极大的减少的数据的 IO 操作，加快了查询速度。

同一列的数据类型相同，压缩比高，能够减少大量的存储空间；更高的压缩比，意味着从磁盘中读取数据更加省时。

自由的压缩比算法，不同的列可以选用不同的压缩算法。这样可以根据不同列的类型，选择最合适的压缩算法。

★数据的有序存储

可以指定数据按某些列进行排序。排序后，这些 sort key 相同的数据会分布在磁盘的连续空间上。这样在查询数据的时候，命中率就非常高。

★主键索引

支持主键索引，它将每列数据按照 index granularity（默认 8192 行）进行划分，每个 index granularity 的开头第一行被称为一个 mark 行。主键索引存储该 mark 行对应的 primary key 的值。

对于 where 条件中含有 primary key 的查询，通过对主键索引进行二分查找，能够直接定位到对应的 index granularity，避免了全表扫描从而加速查询。

★高吞吐写入能力

数据存储采用类 LSM 树的结构，数据写入后定期在后台 Compaction。顺序写的模式将数据追加到文件中。顺序写的特性，充分利用了磁盘的吞吐能力，我们知道顺序写和向内存中写入数据的效果差不多。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS023-674

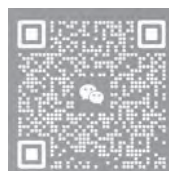
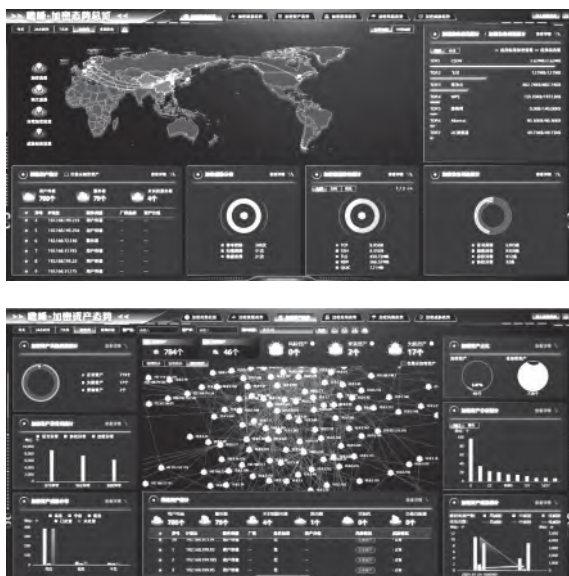
★有效期：2024 年 03 月 05 日至 2029 年 03 月 04 日

所属品牌：观成瞰峰

发布时间：2023 年

产品适用领域：金融、军工、政企、能源等

产品照片：



产品咨询二维码

产品咨询邮箱：xiongjingjing@viewintech.com

北京国舜科技股份有限公司

国舜股份是一家面向政企、金融、通信、能源、交通等关键行业的专业化信息安全产品及整体解决方案咨询服务商。作为国家高新技术企业、国家专精特新“小巨人”、北京市企业技术中心，国舜股份始终坚持自主创新，通过将 AI、大数据、UEBA 等技术融入安全攻防技术，以丰富的产品体系及安全服务资质助力用户在开发安全自动化管理、风控反欺诈、XDR、安全运营、态势感知、Web 应用安全等方面的痛点突破，已助力百余家银行及上千家企事业单位信息安全保障能力与网络安全防护能力的提升。

网址：www.unisguard.com

电话：010-82838085

地址：北京市海淀区上地信息路 7 号弘源首著大厦

产品名称：北斗网络安全运营平台

产品概述

北斗网络安全运营平台是国舜自研的统一安全运营与管理平台，通过搜集所有网内资产的安全信息，对收集到的各种安全事件进行深层的过滤、分析、统计、关联和存储。提供资产自动化盘点、网络攻击面测绘、流量威胁感知、漏洞闭环管理、攻击链还原、威胁情报管理、日志审计与检索调查、安全编排与自动化响应及安全可视化等能力，及时发现反映被管理资产的安全情况，定位安全风险，并提供处理方法和建议。帮助用户实现事前安全预防，事中事件监测与威胁检测，事后快速响应处置的一站式、可视化、自动化的安全运营管理。

功能特点

◎**面向业务安全管理**：系统内置业务建模工具，反映业务支撑系统的资产构成，并自动构建业务健康指标体系，从业务的性能与可用性、业务的脆弱性和业务的威胁三个维度分析业务的健康度，协助用户从业务的角度去分析业务可用性、业务安全事件和业务告警。

◎**集成多种安全产品统一进行安全理解，增强检测和响应能力**：通过在组件安全产品之间共享本地威胁情报来提高保护能力，从而在所有组件之间提供有效的威胁屏蔽；此外，通过自动关联和确定报警来减少漏报；集成相关数据，进行更快、更准确的报警分类。

◎**智能的安全能力网关**：系统提供的安全能力网关支持通过系统配置的方式，快速提供安全产品、平台的接入（例如：沙箱、CMDB 系统等），将其外部的安全能力和系统能力通过配置的方式快速集成到 SOAR 引擎，丰富 SOAR 剧本安全能力，实现安全能力投资的对外赋能和复用，提升企业整体的安全基线。

◎**从实战出发的调查取证和自动化处置**：平台支持利用 SOAR 引擎提供的剧本能力实现自

动化取证能力，并提供取证工具可线上或线下辅助安全运营人员完成取证工作，并通过系统系统的分析研判工作台完成证据链梳理，线索拓线、溯源分析，提升安全运营人员分析研判效率，并借助 SOAR 剧本引擎实现自动处置实现快速止损。将应急响应中告警分析研判周期由天级压缩至分钟级，将告警的响应处置周期由小时级压缩至秒级。全面提升安全运营的分析研判和处置响应效率。

◎降低安全运营的复杂度，提高安全运营人员的效率：客户能够统一收集来自网络中 IT 资产的运行信息和日志信息，通过分析这些数据，识别各类性能故障、非法访问控制、不当操作、恶意代码、攻击入侵，以及违规与信息泄露等行为，协助客户安全运维人员进行安全监视、审计追踪、调查取证、自动化应急响应和处置、生成各类报表报告，提高客户日常安全运营效率。

◎丰富多维的安全态势：通过对数据的综合利用，包含安全事件、漏洞脆弱性、告警、资产信息、外部威胁情报等各类安全数据，使用户把控宏观安全及风险态势，了解当前遭受的攻击态势，综合掌握网络中资产及业务的安全隐患，识别被防护对象受到的威胁态势，掌握攻击规律趋势，定位攻击源头并预警潜在威胁。其目标是通过安全信息的集中整合分析，使用户从资产态势、漏洞态势、风险态势、攻击态势等多维度掌握风险威胁态势，把握威胁的发生、发展、危害范围，提升整体资产及业务的防护能力。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01650-A

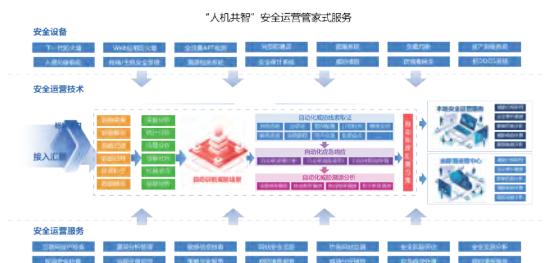
★有效期：2024 年 11 月 8 日至 2026 年 11 月 8 日

所属品牌：国舜

发布时间：2021 年

产品适用领域：金融、政企、运营商等

产品照片：



产品咨询二维码

产品咨询邮箱：yuweijie@unisguard.com

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家级专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区昆明湖南路 47 号国防教育基地二层

产品名称：工业安全管理与态势分析系统

产品概述

工业安全管理与态势分析系统是对工业企业的生产与办公网络全维度安全数据进行采集、分析、预测、响应的综合性分析决策平台。平台通过大数据分析、机器学习等技术对工控业务安全数据进行分析 and 建模，对威胁和攻击行为进行预测、响应和溯源，通过多维度可视化技术展示，使整体安全状态可感知，安全态势可预测，为企业的安全运营体系提供安全决策的数据支持。

功能特点

◎全面的资产管理

支持对工业资产自动精准识别和动态感知，构建细粒度资产信息。辅助手动编辑工控网络拓扑和网络区域层级，实现工控企业网络中的工控资产和网络拓扑可视化。

◎全面的流量分析

对生产控制网和生产管理网的网络流量状况进行实时采集和分析，可分析出主流的网络协议、工业协议；识别出网络攻击流量和网络攻击行为；同时具备网络流量统计、网络性能分析、网络故障定位能力。

◎全方位的威胁感知

系统基于大数据存储技术，采集海量业务流量、安全日志等数据，叠加内置的各类知识库、规则库；采用各类分析引擎、机器学习算法以及基于特征、行为和时序的异常检测算法，可精准检测出各类漏洞、威胁、安全事件和异常行为等。

◎深度溯源分析

利用大数据存储技术，完整保留网络流量、安全日志数据等，采用大数据分析技术，将安全事件与该事件所针对的目标资产信息进行关联，找到源头，逐层分析，找出攻击链条，还原攻击路径，实现对任意风险事件的溯源分析。

◎可量化风险评估

对工业网络、关键基础设施上的恶意代码、漏洞、攻击方法等进行搜集、整理和分析，结合资产价值和威胁信息等因素给出安全风险量化评估结果，并进行安全风险预警与预测。

◎安全态势可视化

系统提供大屏、安全报表等方式展示安全综合态势图，可直观的了解系统整体安全状态以及安全风险分布趋势，通过数据下钻技术，可以进一步了解安全风险细节信息，精确定位全网脆弱节点。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231090

★有效期：2023 年 5 月 12 日至 2025 年 5 月 12 日

所属品牌：珞安科技

发布时间：2017 年 11 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业。

产品照片：



产品咨询二维码

产品咨询邮箱：liss@icssla.com

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 6000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.winicssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特态势分析与安全运营管理平台

产品概述

态势分析与安全运营管理平台（简称态势感知）是企业的安全大脑，主要服务于企业日常安全运营，一方面提供系统资产态势、运行态势、攻击态势、脆弱性态势、事件态势等各类宏观数据的分析和展示；另一方面统一安全管理入口，实现多设备集中运维、安全策略集中配置和下发、日志集中收集和分析、设备操作集中审计。实现了含资产管理、策略管理、监测预警、攻击溯源、漏洞管理、风险评估、合规评估、趋势预测、协同联动于一体的一站式安全运营。

功能特点

◎态势分析大屏

通过可视化场景，综合安全态势、资产态势、运行态势、脆弱性态势、网络攻击态势、横向威胁态势、安全事件态势等，实现安全风险可视化，形成一体化工业安全运营分析中心。

◎资产全生命周期管理

基于设备指纹自动识别系统内的设备和系统，支持 3000+ 网络设备指纹、500+ 控设备指纹、300+ 视频监控设备指纹、1500+ 打印机指纹、200+ 安全设备指纹、100+ 种工控应用指纹，识别准确率可达 90%。以资产为核心，将漏扫设备、配置核查设备、安全设备数据进行整合，将资产运行信息、链路状态、资产漏洞、风险、操作系统、服务和端口等信息进行结构化整合，从底层硬件、操作系统、应用程序、安全风险多层次对资产情况进行全面刻画。

◎组态化拓扑

创新性的引入基于业务、基于工艺、基于拓扑的安全监测模式，以可视化拓扑方式实时展示网络安全问题。安全监测不再是安全设备本身的监测，而是基于网络内所有资产的监测，如主机、网络设备、服务器甚至“网线连通状态”，从单纯的安全监测提升到业务安全监测。

◎自动化风险评估和合规评估

内置等保 2.0 知识库，自动对系统合规情况进行检查，提供不合规项整改报告，量化合规指标，帮助安全管理员定期进行安全合规情况检查，让合规建设工作开展有序。

◎工业场景典型威胁分析

工业环境通常不允许使用 WEB 服务，所以常规的 SQL 注入、XSS 跨站、DDOS 攻击等 IT 事件在工业环境非常少见，但工业环境中的 U 盘滥用、非法设备接入、非法外联、非法软件安装、非法远程访问、非法命令操作、工业协议关键事件、跨区通信等行为比较多见，得益于我司在工业协议解析和工控主机安全防护方面的经验积累，我司产品在上述工业典型威胁的监测和分析中优势明显。

◎多源异构数据采集

灵活可扩展规则库，支持多种设备、多种协议、多种格式的日志的采集和标准化处理，包含 7 大类 300+ 设备日志采集，内置 900+ 日志解析规则，涵盖国内外主流厂商的安全设备、网络设备、中间件、数据库、主机、应用及服务日志。

◎一站式安全运维

作为安全管理的统一入口，实现从设备状态监控、安全策略配置和下发、软件升级和授权、安全事件收集和处置，支持内网多区域管理及跨地域级联管理，解决多种安全设备带来的安全管理分散问题，显著提升日常安全运维效率。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231266

★有效期：2023 年 06 月 02 日至 2025 年 06 月 02 日

所属品牌：威努特

发布时间：2021 年 9 月 20 日

产品适用领域：电力、石油石化、轨道交通、钢铁、市政、烟草、智能制造等

产品照片：



产品咨询二维码

产品咨询邮箱：support@winicssec.com

北京长亭科技有限公司

长亭科技是国际顶尖的技术驱动型安全公司，全球首发基于智能语义分析的下一代 Web 应用防火墙产品，成为中国 WAF 市场份额占有率增速最快的下一代网络安全公司。目前，公司已发布 10 余款自研技术驱动产品，形成以攻（安全评估系统）、防（下一代 Web 应用防火墙、高级威胁分析预警系统）、知（安全分析与管理平台、攻击面管理运营平台）、查（主机安全管理平台）、抓（伪装欺骗系统）为核心的新一代安全防护体系，并提供优质的安全测试及咨询服务，为企业级客户带来智能的全新安全防护思路。

网址：www.chaitin.cn

电话：4000-327-707

地址：北京市朝阳区北辰东路 7 号楼 -2 至 8 层 101 内北区 6 层 602 室

产品名称：长亭万象（Cosmos）安全分析与运营管理平台 CM V1.0

产品概述

基于多年安全实战经验，长亭科技发布万象 (COSMOS) 安全分析与管理平台，汇聚多源数据，驱动安全建设，提升企业安全水平。结合【人+平台】整体解决方案，万象 (COSMOS) 基于更专业的安全人员来启动、调优和护航，具备更贴近于企业安全场景的风险分析业务能力，助力企业逐步实现信息安全大数据态势感知。

万象安全分析与管理平台的产品定位包括：

①应对层出不穷的新型威胁，提供更专业的攻防经验支撑、威胁情报数据支撑及安服团队支撑的整体感知与运营方案。

②汇聚多源异构的安全类数据（安全设备日志、安全合规日志、操作日志、安全运行日志）、基础 IT 类数据（用户数据、资产数据）、威胁情报数据、流量数据等的安全数据中心。

③基于长亭安全攻防实战及风险分析经验，针对丰富融合的各类多层次安全数据，提供多种角度深度分析的安全风险数据分析平台。

④贴合不同企业业务，提供灵活可配置的安全数据处理及可视化分析的安全策略分析工具

⑤贯穿企业安全运营体系建设，逐步建立数据分析、风险发现、风险处置、处置反馈/复查的安全风险闭环流程，串联实际安全工作，形成企业安全运营管理机制。

⑥企业综合安全多维度大屏呈现，风险分析场景可视化展现。

功能特点

◎全面汇聚各类安全数据

★覆盖企业安全数据

基于数据驱动安全的理念，万象 (COSMOS) 能够融合多源异构数据，建立更贴合业务需求的安全数据中心。平台支持接入 4 大维度企业网络安全数据：安全类数据基础 IT 类数据、全流量数据、系统配置和用户管理数据，共 8 大类 90 小类：WAFIPS/IDS、漏扫、DDoS、APT、应用系统等。同时，万象 (COSMOS) 数据中心支持多种存储数据结构的维护管理、扩展编辑，可持续扩展接入数据的管理结构。

★数据接入和泛化

兼容主动、被动的主流数据获取方式，包括：Syslog、文件 FTP/SFTP、数据库、全流量镜像等，支持接入监控并管理设备，及时发现设备数据是否接入、是否成功泛化，内置 50+ 主流安全系统自动化解析能力，可直接接入标准化日志，同时支持零基础数据泛化，可快速接入 JSON、XML、键值对，并提供正则模式。

◎多源风险场景智能分析

万象 (COSMOS) 内置实时流式分析、离线周期分析和离线手动分析三大分析引擎，帮助用户在理解数据的基础上快速获取风险分析能力，高效应对不断迭代的风险问题，输出高可信告警。

在实际业务中，由于安全建设背景、运维思路以及网络环境等都不尽相同，安全人员很难利用内置的安全规则直接输出贴合业务需求的告警，需要根据不同风险需求、告警数据量、数据内容、业务情况等调整阈值，修正分析数据。

万象 (COSMOS) 针对多源数据提供交互式功能，可以灵活配置统计、选、关联、基线等分析策略，学习成本更低，并支持通过 SOL 补充多种复杂分析要求，同时可循环引用分析结果数据，输出态势风险告警

◎高效安全运营管控

万象 (COSMOS) 结合实际安全运营需求，串联多种自动化安全分析及处置手段，覆盖重大活动保障和日常安全管控工作场景，降低运营管理成本。

★安全编排、自动化响应

平台支持灵活可配置的安全编排及自动化响应功能，按照定义的标准工作流程自动执行安全风险协同响应工作，串联规范化和流程化的安全管控，降低安全运营成本。

★风险研判处置

平台内置风险告警研判中心，面向多个安全运营角色，包括告警监控角色、研判分析角色及风险处置角色，能够串联安全运维及处置流程，并支持按需扩展和建设。

技术指标

模块	功能模块	功能参数
态势可视	大屏 & 可视化分析场景	支持多种大屏、可视化分析场景呈现。
	自定义仪表盘	支持内置多种可视化视图，并可自定义视图呈现、数据源筛选，并可自定义仪表盘风格、逻辑来统一构建仪表盘，并支持发布应用为可视化分析场景。
	报告中心	支持多种报告类型，并支持自定义报告模板。
安全告警	告警列表 & 聚合	支持告警列表模式呈现，展现告警等级、分类、处置建议等信息，分析过程支持从关联安全日志、关联资产、关联命中情报、安全域等维度进行分析，并针对告警进行分析研判，通过人工手动、自动化策略 2 种方式，建立告警研判 + 处置流程闭环；
	告警处置	支持人工手动、自动化策略 2 种方式进行告警处置，针对高频、高效场景抽象边界拦截、主机隔离场景，MTTR 从小时 / 分钟级降低到秒级；
资产中心	资产管理	支持面向多源资产实现 IP 资产、应用资产的资产管理能力，管理资产名称、责任人、组织机构、安全域等信息，并支持确认资产、未知资产 2 种维度进行资产管理；
	脆弱性管理	支持面向第三方厂商、长亭自研漏扫的接入、管理，统一驱动并管理漏洞扫描任务，通过扫描器视角、扫描任务双视角进行集中扫描管理
智能分析	检索分析	支持多种筛选模式：条件筛选、高级筛选、SQL 筛选，可将日常运营常用的检索条件进行保存管理
	关联分析	支持图形化交互、SQL 分析，抽象安全日志、告警、资产、脆弱性、行为、情报等数据，内置离线周期、实时流式 2 大能力引擎
	基线分析	支持离线周期、实时流式模式下针对历史或实时数据构建基线学习规则，通过学习数据针对网络异常行为、风险攻击趋势等场景进行分析，输出基线数值，并支持从阈值、极值等多方面对学习过程及结果进行分析描述。
	自然语境	支持面向自然语境习惯构建场景化分析能力
运营工具	SOAR	支持拖拽方式自定义编排剧本流程，细粒度控制 SOAR 剧本的触发条件（动作、参数）和触发模式（一次 / 多次，自动化、人工触发），能够在一条分析规则中进行复杂分析场景及剧本触发的多层级组合、嵌套配置，可实现精细化剧本触发，并支持针对编排流程进行统一管理；
	工单管理	支持内置工单引擎，通过手动拖拽方式自定义构建工单模板和工单流程（如普通工单、告警工单等）
	拓扑自定义	支持可视化拓扑管理及自定义配置，并发布为大屏进行统一呈现（拓扑架构、设备安全日志、万象告警、设备监控告警）。
威胁情报	IP 情报	支持内置、接入第三方威胁情报源，统一管理威胁 IP 类情报，并可支持检索及关联情报命中分析等场景。

模块	功能模块	功能参数
数据 ETL& 管理	数据采集 & 处理	平台支持主动与被动相结合的方式获取多源异构数据，数据获取方式包括但不限于：Syslog、Kafka 采集、NSQ、FTP/SFTP、数据库采集（MySQL、PostgreSQL）、SNMP 等；
	数据管理	支持新增定义数据字段满足新数据接入要求，支持管理安全日志、资产数据、情报数据、脆弱性数据、用户定义数据等
平台配置 管理	多种部署模式	支持二级（二级平台模式、一级平台二级采集探针模式）级联部署
	设备管理 & 监控	平台支持对接入设备进行集中管理，并支持对各类设备进行状态监控
行业化 属性	证券行业数据 上报	支持证券行业数据上报功能模块（报送统计、报送数据管理、报送任务管理、数据处理策略等）；

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

- ★安全认证机构名称：中国网络安全审查技术与认证中心
- ★证书编号：CCRC-2024-CS023-615
- ★有效期：2024 年 1 月 2 日至 2029 年 1 月 1 日

所属品牌：长亭科技

发布时间：2021 年 9 月

产品适用领域：金融、电力、能源、政府

产品照片：



产品咨询二维码

产品咨询邮箱：info@chaitin.com

福建省海峡信息技术有限公司

福建省海峡信息技术有限公司是国内最早专业从事网络安全自主研发、产品销售及安全服务的公司之一。2022年4月，海峡信息正式成为福建广电网络集团直属单位。海峡信息是国有控股高新技术企业、国家“专精特新”小巨人企业、福建省创新型研发机构、行业领先的网络安全整体解决方案提供商，是福建省唯一通过国家信息安全服务资质安全运营认证、信息安全服务资质二级认证（安全工程/风险评估）的企业，2022年入选福建省重点上市后备企业，在江西、四川、湖北、湖南等地设有办事处及技术支撑机构。

在技术探索领域，海峡信息成立了“两大实验室”和“一中心”，在过去的二十多年里，一直专注于网络安全产品与服务领域。以创新研发和实战攻防为核心，致力于探索网络安全的最新前沿方向。

在科研成果方面，累计获得了福建省、市科学技术进步奖8项；发明专利授权10项；拥有软件著作权100多项。海峡信息独立承担的福建省高新技术重点项目、火炬计划项目及福建省重大招标项目。所有产品均以创新研发和实战攻防为核心，构建了一个基于主动防御、动态防御、精准防护、整体防护的综合防控体系，广泛应用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域。

网址：<https://www.si.net.cn>

电话：0591-87303711

地址：福建省福州市鼓楼区北二环中路61号2号楼

产品名称：黑盾安全感知与运营管理平台

产品概述

内置综合日志采集引擎、资产发现与管理引擎、漏洞检测与管理引擎。在内网部署黑盾安全感知与运营管理平台，对各节点态势感知探针的数据进行收集，并通过可视化的形式为用户呈现业务资产及针对关键业务资产的攻击与潜在威胁；并通过该平台联动安全防护设备进行攻击封堵。

黑盾安全感知与运营管理平台作为客户环境中的安全大脑，在事前预警、事中响应、事后优化不同阶段发挥着作用，通过安全大数据分析，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力。

功能特点

黑盾安全感知与运营管理平台参与下的企业安全建设，从原来的单点作战转变成了多点防御。通过一个综合平台，打通安全设备之间的循环赋能，提升对事中甚至事前的攻击感知敏感

度，为企业构建起“摸清家底、感知脆弱、认清风险、运营处置、溯源分析”的主动安全防御体系。

◎打破数据孤岛，统一收集和处理数据

对多源异构日志的自动化解析和标准化处理，同时具备对不同类型流量探针的适配，协助用户进行安全日志管理。

◎资产治理赋能，全景化资产风险安全评估

通过全面探测资产，清晰梳理资产台账。同时结合指纹信息、业务信息、漏洞信息、告警信息等进行风险研判，实现全面资产安全评估以及深度资产溯源分析，全方位守护资产安全。

◎大数据关联分析，多维分析精准定位威胁

结合机器学习、大数据关联分析、云端赋能等多维度能力，快速定位到隐蔽的威胁行为，精准捕获精准告警。智能压缩告警，提炼关键事件，威胁情报碰撞，让安全更简单也更准确。

◎安全编排与响应，威胁自动响应

结合多种业务场景和处置经验，内置安全编排剧本，自动化启动安全运营流程，联动预警通报流程、安全处置设备等，即使无人值守也能对恶意攻击精准封堵，提升安全防护能力和安全运营效率。

◎可视化展示，直观呈现全局态势视图

将复杂的信息和数据转换成直观图形的过程，在攻防过程中发挥挂图指挥的作用，以大屏形式有效呈现各维度信息，辅助管理者做出更好决策。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00817-A

★有效期：2024年6月14日至2026年6月14日

所属品牌：黑盾

发布时间：2020年1月15日

产品适用领域：适用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域

产品照片：



产品咨询二维码

产品咨询邮箱：chenxf@heidun.net

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：先知威胁感知大数据平台

产品概述

迪普科技先知威胁感知大数据平台是一款帮助用户发现 APT 攻击、失陷主机、僵尸蠕传播等安全威胁，实现精准溯源及应急处置的产品。平台以安全大数据+AI 智能分析技术为核心，结合主/被动检测、威胁情报、UEBA、攻击行为建模、失陷主机检测等技术，实现安全事件可视化、全网威胁可视化、全网流量可视化、资产及脆弱性可视化等，帮助客户评估安全状态并决策处置。同时平台设计遵循《GB/T 20984-2022- 信息安全技术信息安全风险评估》《GB/T 42453-2023- 信息安全技术网络安全态势感知通用技术要求》及等保 2.0 等相关要求，全面满足合规性需求。

功能特点

◎安全可视化

基于先进的安全可视化技术，平台通过安全总览、威胁分析等不同分析维度为用户实时呈现网络安全状况，帮助用户快速识别网络异常入侵行为，及时把握网络安全事件发展趋势，为用户营造全新安全管理体验。

◎安全威胁态势感知

平台系统提供全面的网络威胁入侵检测能力，同时具备丰富的安全特性：支持信息资产的识别，可对资产进行长期监控；支持对僵尸、木马、蠕虫等系统类攻击，SQL 注入、网络爬虫等 Web 类攻击，HTTP Flood、ACK Flood 等 DDoS 类攻击进行态势感知。平台从全网整体安全监测入手，再细化到信息资产以及安全数据的监测，实现全方位安全的态势感知。

◎大数据引擎技术

该引擎技术作为态势感知的“大脑”，能够对海量数据日志进行存储、特征提取以及挖掘分析。其通过机器学习的特征积累方式来不断优化平台的处理精度，以及通过对历史日志信息进行关联、回溯等手段，帮助用户发现潜在的安全威胁，进而实现对未来安全威胁趋势的科学预测。

◎虚拟探针技术

平台通过软件实现方式，将用户现网中的安全设备虚拟化成不同区域的采集探针，同时可以和迪普安全云进行威胁情报的联动，使得态势感知平台可以将各种安全设备日志、威胁情报等数据进行整理和汇总，从而保障用户自身安全设备数据能发挥出最大的利用价值。

◎攻击事件还原

平台会从采集的日志中整理攻击事件，对攻击事件进行时间线还原，绘制攻击者从开始到结束的每个具体攻击动作，从而帮助用户实现对攻击行为的还原追溯。

◎被攻击主机分析

平台对被攻击主机进行统计，基于被攻击主机的端口、攻击源 IP 及地理分布、攻击方式、攻击数量趋势等多个维度进行深入分析，检测该 IP 主机上是否有 WebShell、病毒、木马等，帮助用户判断此主机是否被入侵提供线索。

◎安全策略优化

摆脱过去单兵作战的防护模式，每个安全设备都只作为整个安全防护网的一个节点，设备间进行信息共享，安全策略通过态势感知平台不断的进行优化调整。

技术指标

◎在海量资产场景实现大规模消除攻击误报及事件分级

网络安全空间的海量告警远远超过人力能够处理的范畴。因此通过平台首要实现的是减少无用告警、生成需关注和处理的关键事件、有效减少误报。同时，统一报警分级标准，如最高

级别的警报事件，可能存在拒绝服务、系统控制、数据泄漏等情况。随后是处置、追溯、修复、优化等一系列过程，这些后续过程不可避免地需要大量的人工干预。为了避免人工成为整个过程的瓶颈，需要对需要处理的事件进行优先级排序，形成时、日、周、月的处理梯队，使不同类型的安全事件能够及时解决，兼顾全局。

◎建立高级威胁感知及溯源能力

利用平台去除大量误报和无实质性影响的告警，同时对事件进行整合和提炼，实现对监测数据的进一步加工，通过关联挖掘出新的事件。在此过程中：（1）还原和定位单体事件在渗透和攻击链中的所处阶段，结合溯源分析，进一步形成完整的证据链，有利于全面评估损失和安全风险；（2）深度挖掘异常行为，对于外部已发生但本地仍未知的高级威胁，通过引入威胁情报来补充，并与自身安全技术体系有机结合，具备更全面的检测和防护能力。

◎以数据驱动智能安全运营延伸发展

安全运营是网络攻防、事件处置等传统基础安全工作的集中和升华，成为安全治理的主体工作。安全运营建设既离不开人、财、物的投入和机制建设，更需要安全运营平台和团队人员技术能力的双向提升。利用平台加快了针对不同安全威胁的分析速度，快速分发防护和响应策略，节约人工成本，有效提升安全运营效率和规模，并实现运营工作自动化。

随着网络安全智能技术的不断成熟和发展，安全运营和治理的效果也将显著提升，有助于实现各行业用户网络的未来安全战略，更好地保障各行业网络的安全稳定运行。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230025

★有效期：2023 年 1 月 13 日至 2025 年 1 月 13 日

所属品牌：迪普科技

发布时间：2018 年

产品适用领域：公安、电力、政府、金融、电力能源、科教文卫、
大企业、检法司、运营商

产品照片：



产品咨询二维码

产品咨询邮箱：liandonghai@dpotech.com

杭州美创科技股份有限公司

杭州美创科技股份有限公司（简称：美创科技）成立于 2005 年，中国专业数据安全头部企业，拥有数据安全、运行安全、数据流动、安全运维服务四大业务，累计服务客户数超 16000 家。

深耕数据安全近 20 年，美创数据安全管理平台、数据安全分类分级、数据库审计、数据脱敏、容灾备份等产品持续保持市场领先。基于数字化时代安全诉求，美创创新提出韧性安全框架，研发推出适应多云环境，具备数字化、弹性、云化、自适应进化、可观测为特点的新一代数据安全管理平台、新一代灾备一体化平台和数据流动平台。

作为数据安全中坚力量，美创已参与 30 余项国家行业标准制定，深入推进产学研合作，布局信创、关基保护领域，不断以更全面创新的产品方案与服务，护航数字经济发展。

网址：<http://www.mchz.com.cn/>

电话：400-811-3777

地址：浙江省杭州市余杭区五常街道中福未来星辰金座 4 幢 3 层 301 室

产品名称：美创诺亚防勒索主机防护系统

产品概述

美创诺亚防勒索主机防护系统是一款以数据资产防护为核心的、以零信任为基础的勒索病毒防护软件。产品以知白守黑、不阻断无安全为核心理念，集合内核级别防护机制、主机防护、基线防护、威胁情报、诱捕机制、智能模型等创新技术，实时监控各类进程对数据文件的读写操作，快速识别、阻断非法进程的入侵行为，旨在通过严密的防御机制，主动抵御政企事业单位机构中面临的各类病毒的侵袭。

功能特点

◎有效防止病毒攻击

诺亚防勒索基于美创安全实验室的防病毒引擎，结合访问控制引擎、诱捕引擎，来判断访问保护对象的程序是否为病毒、恶意软件，从而抵制已知、未知病毒攻击。

◎可视化溯源分析

防勒索终端可以采集终端上所有进程的访问行为、所有保护资产的被访问行为，这些访问关系及访问结果会汇聚到服务端的控制中心，让安全运营人员能够及时了解网内所有终端设备的资产访问情况，对异常访问行为可以进行溯源分析，同时，对高危访问行为能够快速设置防护策略，时刻掌握网内终端设备的安全动态并及时响应。

◎建立终端防护体系

诺亚防勒索具备访问控制引擎、诱捕机制、主机入侵检测、病毒库、白名单、防泄漏等多种防护机制，从诱捕、入侵、访问控制、病毒检测、数据泄露等多方位，层层防护，重重加码，为终端安全建立起了一整套安全防护网，从而保障终端安全。

◎终端统一管理

防勒索控制中心为安全运营人员提供统一终端管理、统一策略下发、统一日志收集等多种管理功能，安全运营人员可以对网内所有终端进行统一管理，确保网内终端设备的安全可管、可视、可控。

技术指标

诺亚防勒索主要包括控制中心、客户端两个核心部分，控制中心部分采用 B/S 架构，完成管理员的所有管理需求；客户端部分是一个独立的本地可执行程序，完成管理员下发。

◎控制中心

控制中心部署在 mcos 系统上，可以管理终端，汇总统计所有安全事件，策略配置下发等功能。控制中心采用的是 B/S 架构，用户可以通过不同的浏览器进行访问，同时根据不同的权限分配限定用户的访问范围，做到安全访问。控制中心主要包括策略管理、下发，终端状态查看、管理，终端风险日志、操作运行日志等安全信息管理检索，告警管理，事件报表统计、可视化报表生成，证书管理，分组管理，应用地图等模块功能。

◎客户端

防勒索客户端是部署在 Windows/Linux 系统上的客户端程序，主要有 Policyagent，内核模块（LKM/Enforcer），交互模块（命令行/UI 界面）3 部分组成。其中 Policyagent 以系统服务形式存在，内核模块以系统驱动形式存在。其中内核模块拦截操作系统事件，例如文件事件，进程事件等，然后交由 Policyagent 做策略计算，然后返回结果给内核模块。交互模块可以显示防勒索客户端的信息，例如策略，日志等信息。同时客户端会跟控制中心进行状态同步以及信息上报等。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01737-A

★有效期：2024 年 11 月 22 日至 2026 年 11 月 22 日

所属品牌：杭州美创科技股份有限公司

发布时间：2017 年 11 月

产品适用领域：全行业

产品照片：



产品咨询二维码

产品咨询邮箱：marketing@mchz.com.cn

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于2000年4月，总部位于北京。公司于2014年1月29日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有50余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等70余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路4号益泰大厦3层

产品名称：绿盟智能安全运营管理平台

产品概述

绿盟智能安全运营管理平台（态势感知）是遵循绿盟智慧安全3.0理念，以“实战化安全运营”为主旨，以资产为核心，基于大数据架构自主构建，面向政企客户的可信任、全场景的安全管理平台。平台通过统一全网流量和异构日志数据，融合威胁情报进行实时分析、智能决策，实现资产管理、漏洞管理的全周期管控，实现威胁事件调查分析溯源和取证响应等闭环处置，辅助安全编排和异常行为分析帮助客户落地布局安全中心，为安全运营（管理、分析、响应）提供有效支撑，实现全域安全态势感知和协同指挥，促进企业安全防护良性生态体系的建立。

功能特点

◎数据接入及数据湖建立

平台将框架、解析插件、存储分类设计，可选择kafka、syslog、ftp等多种通道接入数据，已支持多达上千种安全产品的日志接入。接入过程中，按照统一的基准，实现数据的资产信息、

威胁情报、地理位置等富化增强，建立覆盖各分析层级的安全数据湖。

◎ 威胁识别与攻击者画像

平台基于安全检测、防护策略、身份认证等各类数据，结合终端 EDR、蜜罐诱捕等技术，配合绿盟威胁情报，以绿盟独创的威胁分析建模引擎、异常行为分析引擎、安全治理分析引擎进行深度威胁关联分析，实现已知、未知和灰度行为的检测与分析。同时借助 ATT&CK 矩阵中攻击方式的依赖，能关联高度复杂、事件跨度大的攻击行为，精准、详细、真实的描绘攻击者行为，形成可视化攻击图谱，并且实现后续攻击的预测。

◎ 威胁狩猎与溯源取证

基于 XDR 中丰富的数据，平台支持从多个角度开展威胁狩猎工作，重建攻击路径图，还原攻击轨迹，定位威胁发生的根本原因。同时基于全流量存储，在样本披露发生时，可对热点事件进行自定义规则并查询回溯，也可基于探针实时采集的 PCAP 全量存储包进行溯源取证。

◎ 事件分诊及响应处置机制

事件分诊可帮助用户快速分析其最关注、最具价值的事件，通过多种关联分析、行为分析、人工智能等手段检测威胁事件，依据 SOAR 技术手段配置自动化响应剧本，以自动化、高效率的方式对网络侧、终端侧进行实时阻断，并结合多种通报预警方式（钉钉、微信、短信和邮件等）及时通告安全信息，实现全自动检测响应处置，提升安全运营效率。

◎ 资产发现与资产管理

在资产识别方面，ISOP 可通过日志 & 流量 & 终端式被动发现、情报 & 评估探针式主动发现等多方式实现内部与外部网络的全类型资产测绘，梳理暴露面，发现资产死角，帮助企业建立安全资产台账，消除资产管理中的信息孤岛。

◎ 脆弱性检测与合规评估

平台提供覆盖系统漏洞、网站漏洞、配置基线、弱口令、渗透测试、合规审计等综合脆弱性管理，配合绿盟自主原创的“优先化”模型算法和漏洞威胁闭环管理框架辅助漏洞管理运营与量化分析，帮助企业安全管理者快速了解企业物理环境、通信网络、制度管理的等保合规情况。

◎ 态势感知呈现

平台基于可视化技术可以从不同运维角度对网络安全态势进行呈现。平台内置了综合态势、环境感知态势、威胁态势、运维响应态势、脆弱性态势、日志审计态势、5GC 威胁态势和扩展分析响应态势八大主流维度的态势感知界面。平台可以针对整体范围或某一特定时间与环境进行因素理解与分析，最终形成历史的整体态势以及对未来短期的预测，洞察企业内部整体安全状态。

技术指标

◎ 精准的威胁检测与研判能力

平台依托 XDR 能力重点关注威胁检测和响应，将端侧、网络侧的多源遥测数据收集，结合

高级威胁检测模型、广泛的上下文视图、多个组件的关联分析，将多源弱信号聚合为事件，提升检测深度。平台突出的安全分析和 XDR 能力荣获国际咨询机构 Forrester 的认可。

◎高效的闭环响应机制

平台可基于安全分析产生的运维事件，进行运维模型的构建，结合响应事件类型来分析攻击类型趋势，针对不同的攻击类型及时调整防御策略，从而确定自动化执行防护策略，针对各类应急事件，可自动化完成检测、通报、处置流程，保障业务连续性，提升闭环处置效率。

◎丰富的联动编排响应手段

平台具备灵活的开箱即用能力与自动化编排能力，可提供端到端的安全编排能力，覆盖从威胁检测、威胁分析到自动化协同响应的闭环解决方案。同时，平台支持多种响应处置动作与告警通知方式。在国际权威咨询机构 Gartner 报告中，绿盟科技凭借其平台优异的能力表现，被列为 SOAR 市场代表供应商；2020-2022 连续三年获得 IDC 响应和编排市场销售第一。

◎高价值威胁情报积累

平台依托绿盟威胁情报中心（NTI）支撑，覆盖挖矿、勒索、APT、C2、攻防演练等专项场景的 100T+ 高价值威胁情报，帮助用户及时洞悉资产面临的安全威胁，并实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握威胁态势，准确地进行威胁追踪和攻击溯源。

◎智能化安全运营体系

平台结合 AISecOps 技术体系，针对大规模运营事件，可结合自动化的基线告警收敛与告警分诊，已成功应用于多个企业级的安全运营实战，大幅降低对安全专家资源的依赖。绿盟科技智能化安全运营解决方案 2017-2019 连续两年获得 IDC AIRO 市场销售排名第一。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00309-A

★有效期：2023 年 11 月 17 日至 2025 年 11 月 17 日

所属品牌：绿盟科技

发布时间：2016 年

产品适用领域：运营商、金融、政府、
能源、企业、交通、医疗、教育

产品照片：



南京聚铭网络科技有限公司

聚铭网络是由腾讯、国家中小企业发展子基金、江苏高投毅达宁海创业投资基金等投资的国内领先的安全运营商。

公司先后荣获了“高新技术企业”、“江苏省专精特新企业”、“江苏省规划布局内重点软件企业”、“江苏省软件企业技术中心认定企业”、“南京市工程技术研究中心认定企业”、“双软企业”、“创新型企业企业家培育企业”、“创业南京高层次创业人才引进企业”、“国家信息安全漏洞库CNNVD技术支撑单位”、“数据安全10强企业”等荣誉，公司专注于网络安全智能分析和检测，提供全面的信息安全防护，为达成“让安全更简单”的使命而不懈努力。

公司每年投入大量的科研经费用于产品研发和人才培养引进，先成立了“聚铭安全攻防实验室”，后又与南京大学联合成立了“数据科学联合实验室”，两大实验室用于网络安全前沿技术的预研。目前公司产品荣获了江苏省软件产品金慧奖、江苏省重点推广应用新技术新产品、南京市新兴产业重点推广应用新产品等荣誉。

凭借先进的技术和优质的服务，目前公司产品已服务教育、医疗、政府、电信、能源、金融等行业超10000家政企客户，云端托管客户超6500家。公司在北京、南京成立了双总部中心，同时在各地设有分支机构，业务覆盖全国31个省市及香港地区。

网址：<https://www.juminfo.com/>

电话：400-1158-400；025-52205520

南京总部：南京市雨花台区软件大道180号大数据产业基地7栋4层

产品名称：聚铭下一代智慧安全运营中心

产品概述

在数字化转型的浪潮中，用户购置大量安全设备，如何构建高效、智能、全面的安全防御体系成为用户亟需解决的问题。聚铭网络作为国内领先的安全运营商，着力组织安全顶层规划推出下一代智慧安全运营中心，体系化构建五大中心——全域数据采集分析中心、全域安全监控中心、安全运维承载中心、整网安全管控中心及安全可视化中心，旨在为企事业单位提供一站式安全运营管理解决方案。

方案依照等级保护、网络安全法、数据安全法等政策法规，ITIL、ISO27001等技术标准，整合各行业制度规范、技术平台、管理流程、人员组织，实现信息中心、网络出口的安全风险的集中监控、安全事件的集中处置、安全策略的合规检查、安全态势的统一展示，将信息安全

管理和技术有机结合，健全信息安全保障体系。

功能特点

◎全域数据采集分析中心

1、全域数据采集专利技术，构建用户数据仓储底座。

★设备日志采集：统一采集各类安全设备、网络设备、终端等告警信息。

★网络流量采集：各区域部署流量探针，基于平台分析溯源全域威胁。

★脆弱性数据采集：内置检测引擎，主动扫描整个网络存在的脆弱性风险。

2、全域数据分析，用户安全的隐形护盾。

平台不仅具备被动监测安全防御能力，更具备主动出击，全面扫描并消除各类潜在的脆弱性风险，全方位护航用户网络安全。

★自动化主动体检，挖掘潜在安全隐患：漏洞扫描、弱口令扫描、基线扫描。

★智能化被动防御，实时监测网络攻击：高级威胁模型、异常行为模型、关联分析模型、ATT&CK 战术模型、统计离散模型、多源威胁情报。

平台依托专利安全告警归并技术，实现数据包级自动研判降噪。

★智能降噪：对于三方告警数据，平台采取“摄像头监控”方式，抓取产生告警时的快照信息结合人+机器，对快照进行智能研判，减少大量误报。

★云端赋能：支持将告警及快照信息自动上报到云端，云端专家进行精准研判，并下发研判规则至本地，形成云到本地的持续赋能。

◎全域安全监控中心

全域安全监控专利技术，组织安全的全景视图。

★全局视角，实时监控组织安全：全方位 7*24 小时实时监控，精准捕捉任何异常活动或潜在的威胁迹象。

★即时预警，确保信息畅通无阻：通过人机协同方式，将详细的告警信息通过多种渠道发送给相关人员，确保信息畅通无阻。

★跨部门协同，形成合力应对威胁：构建一个高效的协作平台，促进组织内部各部门之间的紧密合作。

◎安全运维承载中心

全能运维中枢，赋能无限可能。

★资产梳理：整网资产梳理及动态管理维护。

★策略制定：制定组织及下属机构专属安全策略。

★安全检查：资产暴露面测绘、设备状态监测等场景。

★应急响应：围绕平台开展安全演练、HVV 等应急场景。

◎整网安全管控中心

全面管控，化繁为简。

★设备状态管控：各类设备运行状况实时监测和全面管理，确保设备始终处于最佳工作状态。

★设备告警管控：全网数据多维融合，动态管控安全事件，为事中威胁检测、事后溯源取证提供有力依据。

★安全策略管控：所有安全策略保持一致性和有效性，减少管理复杂性、提高效率，并确保遵循相同安全标准。

★万能联动响应：自主研发万能联动技术不依赖 API 基础上实现第三方安全设备、网络设备 etc 联动，适配快捷稳定。

◎安全可视化中心

全局掌控，安全效能。

全息大屏感知多场景业务动态，囊括全局安全可视化大屏、设备状态可视化大屏、业务运行可视化大屏、工作开展可视化大屏等展示界面，助力用户打造可视化运营中心。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS023-784

★有效期：2024 年 5 月 23 日至 2029 年 5 月 22 日

所属品牌：聚铭网络

发布时间：2019.01.01

产品适用领域：政府、教育、医疗、金融、电信、能源

产品照片：



产品咨询二维码

产品咨询邮箱：yangping@juminfo.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信态势感知与安全运营平台（NGSOC）

产品概述

奇安信态势感知与安全运营平台（NGSOC）秉持“专业品牌、专业技术、专业知识、专业服务”的产品理念，通过可靠的安全领军品牌、先进的安全技术、一流的专家知识、专业的服务体验，为全球安全运营中心（SOC）提供专业的产品及服务。奇安信 NGSOC 能够快速整合现有安全工具和能力，自动消除来自多种设备的告警噪声，精准检测边界、网络、端点、身份、应用和云等六大维度的网络威胁，提供跨数据源的全局威胁可视性，开箱即用的安全内容包，可覆盖 354 项 MITRE ATT&CK 攻击者技战术，搭配专业的驻场运营服务和远程运营服务（MSS），帮助用户轻松驾驭威胁检测、分诊、调查、响应（TDIR）的各个环节，让真实威胁无处遁形，让攻击者无法隐藏。

NGSOC 上市以来，已在数千家大中小政企机构落地实践。在北京 2022 年冬奥会和冬残奥会中，NGSOC 作为冬奥安全运营中心核心安全监测平台，为保障北京冬奥会网络安全“零事

故”发挥了核心作用。在 2022 年北京冬奥会期间，7*24 小时“零事故”安全稳定运行。此外，作为奇安信集团的核心产品之一，NGSOC 连续 4 年在态势感知与安全运营领域市场份额第一，拥有 74 家世界 500 强企业及中央部委头部客户，相关技术参与或牵头 10 项国家 / 行业态势感知与安全运营领域标准制定中。

功能特点

◎数据采集

数据采集功能是对接入的采集组件、数据的解析规则和处理策略提供统一的管理，同时对数据源采集状态、采集速率和趋势、NGSOC 系统的安全状态、集群节点数和健康状态进行实时监控。

◎资产风险

资产风险模块对资产和资产组进行风险数值的量化，给出具体的评分指标，能够有效的反映出当前网络的安全风险状态，安全管理人员能够宏观了解全网安全态势，给管理者提供有力的辅助决策支撑。

◎资产管理

NGSOC 系统提供完善的资产管理功能，包括主机资产和网站资产。IT 人员或安全管理人员能够建立资产信息、资产分组信息。

◎脆弱性管理

NGSOC 的脆弱性管理模块，实现了对重要资产的漏洞、弱口令、配置核查和 Web 漏洞的收集和管理，并将漏洞、弱口令和配置核查的结果自动同步到风险模块中，参与风险计算。

◎威胁分析

NGSOC 提供了丰富的告警分析和场景化分析能力，从多维度多视角进行分析并采用可视化技术进行展现，安全运营人员经过简单分析后即可判断异常事件中包含潜在威胁。

◎威胁检测

NGSOC 系统的关联分析引擎能够在大数据量级下对多维度安全数据进行实时关联分析，发现更复杂的、更具价值的威胁事件。

◎事件管理

事件管理为用户提供了快捷高效的事件调查和响应的闭环跟踪管理工具。安全分析师通过对威胁告警的综合分析研判，将一条或多条可能对企业产生威胁的告警合并生成一个事件。

◎处置响应

在事件响应各个阶段，均可生成当前阶段的响应报告，报告中详细记录了事件属性、受影响的资产、对攻击者的分析信息、研判证据和当前事件的处置建议。

◎监控和报表

安全概览将系统综合风险、风险资产、待处置的问题一一呈现，帮助用户了解系统整体情况和后续需要运营处理的问题。

◎态势可视化

NGSOC 系统支持企业管理者对安全工作的监控和管理。提供以下工作入口以帮助企业管理者对信息安全状况和安全运营工作进行监控和管理。

◎攻防演练

攻防演练行动，又称红蓝对抗，是目前安全行业的重点活动，NGSOC 提供了攻防演练相关功能来支撑该活动的管理与运营。

◎安全管理

NGSOC 提供等保管理功能，围绕我国信息系统安全等级保护相关政策和基本要求，实现对等保信息系统的定级备案管理、等保信息系统的自我评价、等保信息系统等保测评管理。

◎系统管理

NGSOC 支持用户进行安全知识的积累和集中管理，提供知识库、失陷 IOC 情报库。针对用户对安全部署和权限控制的管理要求，提供权限管理、升级管理、系统审计等功能。

技术指标

◎实时关联分析技术

奇安信 NGSOC 的关联分析引擎（Sabre）基于流式大数据处理框架进行设计，能够在大数据量级下实现对跨网、端、云、应用等多维数据源的实时关联分析，发现更深层、更具价值的复杂威胁事件。分析性能可扩展至数十台集群规模，性能可达数十万 EPS。预置 1200+ 关联分析规则，可开箱即用，在国际通用的攻击者技战术框架中（MITRE ATT&CK），已覆盖了 354 项敌方技战术，位居业界第一。

◎智能告警分诊技术

奇安信 NGSOC 智能分诊专利技术由专家经验模型和人工智能模型共同驱动，预置分诊模型可消除 80% 以上的告警噪声，同时支持用户自主构建结合自身业务的分诊模型，持续运营后可达 99% 的分诊率，解除分析师告警疲劳，大幅缩减平均检出时长（MTTD）。

◎高级情报分析技术

奇安信 NGSOC 采用了多维度威胁情报检测机制，与奇安信云端威胁情报中心（TI）、本地威胁情报中心（TI Inside）、独立威胁情报平台（TIP）均可对接实时情报检测，可对各种日志来源的数据进行实时的情报检测。

◎异常行为分析技术

奇安信 NGSOC 可实时计算网络实体的个体及群体基线，并找到偏离基线的异常实体，不同于特征检测模式，它可以帮助分析师及时发现隐蔽威胁和网络活动中细微的异常变化，是检测新型、未知威胁的关键技术手段。

◎事件自动调查技术

奇安信 NGSOC 可将相关告警自动汇聚形成完整事件卷宗，并自动补充上下文证据，映射 MITRE ATT&CK 攻击者战术和技术，自动解读攻击者意图、自动识别关键攻击痕迹、自动评

估影响面并计算处置对象，即使是复杂事件，也能轻松看懂事件的来龙去脉和完整信息。

◎综合风险评估技术

奇安信 NGSOC 使用动态计算方法将资产价值（机密性、完整性、可用性）、脆弱性和资产威胁三大属性进行加权计算，形成具有指导性的、以百分制为主要输出标准的风险评估模型。

◎生成式人工智能技术

奇安信 NGSOC 可集成奇安信自主研发的安全行业垂直大模型（Q-GPT），通过简单的对话，轻松完成安全运营。AI 智能助理是 NGSOC 借助本地 AI 模型和 Q-GPT 大模型组合开发的一款面向安全运营人员的智能助理，可以协助分析师完成数据查询、任务下发、查询情报等基础分析工作，大幅度提升安全分析师的工作效率。

◎高级交互式分析语言

奇安信安全数据分析语言（QAL），是奇安信 NGSOC 团队的多年研发成果，是一种数据分析层的专用语言。QAL 内置向量化执行引擎，支持多种复杂处理逻辑，提供多种实用的机器学习算法，用于对安全数据的深度挖掘。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS0375-A

★有效期：2023 年 12 月 01 日至 2025 年 5 月 5 日

所属品牌：奇安信网神

发布时间：2016 年 9 月

产品适用领域：电力、石油、煤炭、新能源、智能制造、水利、交通、

教育、医疗、科研、政府、公检法司、民航、物流、金融等

产品照片：



产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

集团总部位于北京市中关村软件园启明星辰大厦，DT（数据时代）总部位于杭州高新区（滨江），全国云安全总部位于苏州高新区，在全国各省、市、自治区设立了分支机构，拥有覆盖全国的渠道和服务体系，为用户提供网络安全产品、服务和解决方案。

网址：<https://www.venustech.com.cn/>

电话：400-624-3900

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：安全管理与态势感知平台

产品概述

安全管理与态势感知平台是一套以场景化为基础，以满足实战化为目的，以威胁为驱动手段，帮助用户建立监测预警、态势评估、响应处置的安全运营平台，定位为可支撑用户“攻防实战，协同指挥，智慧运营”的平台，在传统的“监测，审计，运维，管理”维度上强化“威胁可视、智能响应”，提供集成的预测、阻止、检测和响应能力。

功能特点

平台能力方面采用统一的 THDK 开发框架进行开发，融合业界主流的大数据技术，采用 THBD 数据库，结合 SQL、NewSQL 和 NoSQL 技术，实现对多元、异构、海量安全数据的高效采集检索、可靠存储和负责计算。通过构建 THStore 体系，减少模块的耦合，形成高内聚，低耦合的货架式功能 APP，从底层技术架构层面解决海量资产，数据分权分域，以及高性能日志处理问题。

业务能力方面提供智能化关联分析、自动化编排技术、基于机器学习的行为分析，流安全分析技术，内建主动安全管理机制，通过主动的漏洞扫描和安全配置核查，及时发现业务系统隐患，并进行事前预警；结合内外部情报，提供更加准确和及时的安全分析。同时引入攻击链模型和 ATT&CK 模型分析从侦查、渗透、攻陷、控制、破坏一整套攻击流程进行事中监测，威胁定位；利用流量日志融合，提供更多攻击上下文信息，在调查和攻击溯源方面进行事后取证，案例总结。同时提供宏观视角，中观视角，微观视角为不同角色的用户提供直观的、多维度的可视化呈现。帮助用户掌控实时安全态势，动态感知隐患与威胁，为安全分析师和决策层提供强有力的支撑。

平台在技术上采用新一代分布式计算技术架构和具有自主知识产权的非关系型数据库 (NoSQL/NewSQL) 技术——THDB，具有分布式、全文索引、水平弹性扩展、实时格式化数据搜索和原始数据关键字全文搜索、高可靠性等特点，同时系统采用开放平台架构设计，遵循业界通行的应用接口和管理接口，功能部件都实现了模块化装配，客户可以自由选择，并能够与客户的应用和管理环境实现良好的对接与整合。

技术指标

管理中心在单 Intel 酷睿 16 核 CPU，128GB 内存，64 位操作系统，内置数据库下，采用单一部署模式时，事件处理性能可达平均 20000EPS。

日志采集器在双 Intel 至强 8 核 CPU，32GB 内存，64 位操作系统下，事件处理性能可达平均 15000EPS。

事件存储量仅取决于系统可用存储空间大小。

日志采集器对于所在主机和服务器的 CPU 利用率占用值小于 2%。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405230276

★有效期：2023 年 02 月 10 日至 2025 年 02 月 10 日

所属品牌：启明星辰、网御星云

发布时间：2021 年 9 月

产品适用领域：系统具有国内最广泛的应用范围和客户群，在政府、能源、电信、军队、军工、公检法司、企业、交通、媒体、金融、烟草、卫生医疗、教育、党务等多行业均有成功的应用，已经 13 年位居国内市场销量第一。



产品咨询二维码

产品照片：



产品咨询邮箱：support@venustech.com.cn

产品名称：安全数据中心系统

产品概述

为解决各安全平台及安全数据的烟囱式管理、数据标准不一、整体质量参差不齐，从而导致集中治理、统筹分析、共享能力欠缺的问题，需建设安全数据中心。安全数据中心是以安全数据集中运营、内部共享为目标，以大数据平台为底层基座的技术支撑，统一各安全支撑系统、安全设备的标准化数据采集架构，实现安全数据的集中化管理、强化数据内部关联，支撑数据分析应用的内部共享，为前端各安全平台提供高质量的安全数据服务。

安全数据中心是安全数据的统一采集与汇聚平台，将制定统一的采集标准化和采集架构。

安全数据中心是安全数据的集中治理管理平台，对结构化、半结构化等异构数据进行组织和加工，对安全数据的质量进行把关，为安全数据治理和共享提供基础保障。

安全数据中心是一个“开放式”的安全分析平台，为上层各安全平台和自有安全专业人员提供开放式使用能力，支撑各类安全业务场景在安全数据中心进行开发、分析实现。

安全数据中心旨在解耦安全数据和安全业务应用的分离，通过落实安全数据的标准化工作，使上层安全业务场景的建设更加迅速、灵活、丰富。

安全数据中心 SDC 以安全数据集中运营、内部共享为目标，以大数据平台为底层基座的技术支撑，统一各安全支撑系统、安全设备的标准化数据采集架构，实现安全数据的集中化管理、强化数据内部关联，支撑数据分析应用的内部共享，为各安全平台提供高质量的安全数据。

安全数据中心为软件两种形态，主要采用集群部署，通过数据采集、预处理、存储、治理、

共享服务提供标准化、精细化、定制化的数据服务。

功能特点

安全数据中心主要包含：数据采集层、数据预处理、数据存储计算、数据开发、数据治理、数据集市和数据共享服务等。

◎安全数据采集与数据同步

提供可视化的数据集成组件，基于常见的业务场景提取业务流程进行可视化封装，简单配置接入数据，支持多种接口数据采集。数据采集层可对复杂数据源、大规模数据量、实时数据流提供统一数据接入能力，支持多协议、多方式的数据采集，并支持数据同步，满足安全数据中心数据统一采集的要求。

◎安全数据预处理

安全数据预处理功能主要通过对采集后的原始数据进行解析、过滤、清洗，关联、标签、脱敏，通过对数据归一化、格式化，并按照要求进行数据的补全的一系列初步加工，为用户提供可靠的数据处理，并形成统一的数据存储结构。

◎安全数据存储计算管理

存储包含 Kafka、pulsar 等实时消息队列，ES、HDFS 等分布式存储和关系型数据库。同时提供实时数仓服务，提供安全原始数据的存储；计算引擎包括：Flink、Python 等计算引擎，可以接收上层安全平台计算任务，实现对安全数据进行聚合，关联。

◎安全数据开发

数据开发是完成数据统计、计算或数据挖掘的计算逻辑的一站式过程，需要支持的任务类型包括，如：机器学习、融合建模、可视化建模、函数开发、自定义算法模型等任务类型。底层的机器学习引擎支持 sklearn 框架。

◎安全数据治理

安全数据治理是安全数据场景分析和深度挖掘的基础，其中治理方式不限如下方法：数据标准管理元数据管理、主数据管理、数据质量管理、安全数据管理、数据模型管理。元数据管理提供元数据采集，元数据变更管理。安全数据资产管理视图汇聚系统内所有数据的元数据，提供统一的数据视图，方便用户查询。数据生命周期管理提供定时数据清理、归档的等功能。同时，提供全链路的数据质量方案，包括数据规则配置以及质量监控等功能。

◎安全数据集市

数据开发人员可根据安全业务平台的需要对已存储的用户帐号类数据，配置类数据，运行类数据，安全告警数据，情报漏洞数据，审计日志集市等进行数据开发，数据开发生成的数据形成不同类别的数据集市。

◎安全数据共享

通过构建服务共享模块和开放共享引擎，基于上层安全业务诉求构造各类型数据集市，面向业务统一数据出口。

数据共享模块包括数据服务目录管理、数据服务配置、共享服务监控、实时消费数据、SQL 交互查询。

技术指标

◎数据采集与预处理：

★支持主动采集日志，支持定制日志：支持文本格式日志和目录下文本格式日志采集，文件采集方式包括本地文件采集、共享远程文件、FTP 远程文件、SFTP 远程文件；支持数据库格式日志采集，支持 oracle、sqlserver、mysql、db2、sybase、postgresql、informix；

★数据预处理任务支持页面配置流程图方式，并可自定义编排流程。可在采集、解析、关联补全、过滤归并、转发或入库的全阶段全流程查看数据上行下行的数据质量与数据量 EPS 情况。

★采集算子支持接收 UDP\ 接收 KAFKA\ 接收 UDP\ 接收 SNMP 等

★解析算子支持正则解析、JSON 解析、CSV 解析、key-value 等，解析规则支持划词匹配，智能匹配和智能校验，解析规则支持二次拼接，拼接类型包括样本值和值转换两种。

★富化算子包括静态补全、动态补全、地址补全、资产补全、账号补全、内外网补全、关联补全；

★规则算子支持引用过滤器、合并规则、数据质量规则、数据脱敏规则；

★数据输出算子支持发送 kafka、TCP SYSLOG、UDP SYSLOG、管理中心、pulsar、存储索引节点、内部存储、内部缓存、目标库、hive、ES、HDFS 等；

◎数据查询

★提供交互式数据分析模式，支持自定义查询过滤条件，自定义过滤条件支持基于日志字段进行查询，查询过滤条件可以无限叠加，逐层筛选，任意回退，且支持将用户的查询条件保存为策略；

◎数据治理、数据开发、数据集市与共享

★支持日志元数据、告警元数据、账户元数据、资产元数据管理，支持可通过配置元数据的字段名、字段类型、标签来新增元数据，支持导入元数据以及通过数据开发方式生成元数据；

★内置元数据字典：包括日志等级、日志分类、日志类型、应用协议、网络协议、攻击阶段、TCP 标志位、操作系统、采集类型；

★支持数据质量监控，包括每天、每月、每周采集统计，完整性问题、有效性问题、重复性问题 TOP 分析，支持对质量问题总数以及同步、环比变化分析；

★支持对多种数据集市进行对外发布管理；数据服务配置中支持设定接口类型，接口类型包括 HDFS、KAFKA、MariaDB 等。

◎性能指标

★采集器采集性能指标

单台（CPU 8 核，内存 16G，磁盘 1T 物理主机）配置下，10 种日志样例，配置正则解析和地址补全情况下，接收 udp syslog 采集性能为 8W eps，带宽占用 141Mbps。

★集群入库性能指标

三台物理设备，管理中心、两台存储节点，配置均为 CPU 2*12 核，内存 256G，磁盘 4*4T。入库性能为 6W eps。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405230276

★有效期：2023 年 02 月 10 日至 2025 年 02 月 10 日

所属品牌：启明星辰 网御星云

发布时间：2023 年

产品适用领域：运营商、政府、企业、金融、能源等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

产品名称：飞象大数据可视化分析平台

产品概述

飞象大数据可视化分析平台是一款用于实时数据和流数据处理、大数据分析和数据可视化的软件。可以无缝对接数据源，能将大数据可视化并加以分析和展示，并进行快速开发、部署和培训上手，适合党政机关、企业事业单位和其他组织的管理者、决策者、分析师进行数据监控、分析和展示。

飞象大数据可视化分析平台融合了数据整合、大数据分析挖掘、数据可视化展示、系统管理等技术，构建了一个从数据收集到模型构建，再到可视化展示都一应俱全的一站式大数据敏捷分析系统。基于它可以构建各类数据分析模型，各类态势感知系统，各类监测预警系统，各类数据大屏，甚至是应用、产品。

功能特点

◎ FEA 降低了大数据分析系统的使用难度，无需复杂编程即可快速实现大数据分析，即使缺乏相关行业背景和技术的人才，也能进行大数据分析。

◎ FEA 集成大数据分析的全流程，覆盖大 / 中 / 小 / 流数据，真正做到一站式和敏捷分析，贯穿于数据分析生命周期的全过程，并不断变更、迭代，直至完善。

◎ FEA 完美兼容各类大数据平台。系统向下可采集文本文件、数据库、ES、HADOOP、华为、GP、阿里 ODPS/OSS/ADB、Amazon 等数据，向上可嵌入各类图表、面板、GIS 等交互应用，与 Hadoop、Spark、华为、浪潮、ODPS 等大数据平台完美融合的开放式生态圈，具备分布式处理的优点，可提供完善的各种分析功能，确保分析与应用的完美衔接。

◎ FEA 解决了多元化团队作战造成实施成本高、需求变化快按时交付难、开放性差难以扩展等问题。

◎ FEA 综合 AI（人工智能）与 BI（商业智能）功能，打造了分析与应用的中件间，深入地融合 AI 技术，全面地支持人工智能。

◎ FEA 对机器学习算法的支持范围较广。包括决策树、逻辑回归、朴素贝叶斯分类、KNN、支持向量机 SVM、KMeans 聚类、层次聚类、均值漂移聚类、谱聚类、传播聚类、综合层次聚类（自动聚类）、dbscan（密度聚类）和主成份降维分析、tsne 降维可视化等算法。

技术指标

◎ 支持基于内存计算的交互式编程语言。支持 40 余种基础语法，120 余种自定义函数，以及包含分类、回归、聚类、降维、关联分析、模型处理、预测等在内的 40 余种机器学习函数。

◎ 支持机器学习算法，回归、聚类、降维等。

◎ 支持通过正则表达式、Lambda 函数、字符处理函数、矢量运算，去除噪音数据。

◎ 支持通过原语将数据进行文件类型、大数据类型、内存数据库、关系数据库等形式的存储，系统可以根据不同的存储需求合理安排数据存储策略。

◎ 支持 FEA 原语调试以及脚本运行，以四叶窗口的形式来展示，包括：脚本运行区，展示区，结果区和文件加载区四个部分。

◎ 支持提供分析操作控制台中心，其可直接输入脚本语句执行，显示结果。执行一条输出一个结果。同时可灵活组合多种执行语句，将复杂的数据分析场景简单化。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405230276

★有效期：2023 年 02 月 10 日至 2025 年 02 月 10 日

所属品牌：启明星辰 网御星云

发布时间：2021 年 4 月

产品适用领域：运营商、政府、企业、金融、能源、烟草等。

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

三六零数字安全科技集团有限公司

360 数字安全集团 (三六零数字安全科技集团有限公司) 是数字安全的领导者, 秉持“上山下海助小微”战略方针, 以“安全即服务”为核心发展理念全面升级“360 安全云”, 将十多年被行业反复验证成功的数字安全运营体系框架, 以云化服务化方式为国家、城市、大型企业、中小微企业构建应对数字时代复杂威胁的完整数字安全能力。

网址: <https://360.net/>

电话: 400-0309-360

地址: 北京市朝阳区县 (区、市、旗) 酒仙桥路甲 10 号 3 号楼 17 层 1773 号

产品名称: 360 本地安全大脑分析响应系统

产品概述

本地安全大脑是在 360 长期对抗中沉淀的攻防知识图谱指导下, 基于 XDR 架构设计的安全运营平台级产品, 将 360 全网数字大脑为核心能力本地化的开放式智能分析、研判、预警、响应、评估的统一安全运营平台。可视化、自动化、智能化地形成安全态势感知、高级威胁检测、自动化响应处置、应急作战指挥和 BAS 抗攻击评估等运营能力, 体系化提升客户主动防御效能。

功能特点

以 360 云端全网攻防视野, 赋能本地化安全能力建设。将 360 云端大网数据、攻防知识以及专家能力进行服务化赋能, 提高客户本地“看见+处置”的广度、深度和准度, 解决本地安全视野局限、安全能力上限低的问题。

以广兼容、可扩展的安全大数据底座, 支撑海量数据治理及价值输出。从兼容性、开放性、伸缩性、延展性综合平衡, 提供可大可小, 快速调整, 效果不变的安全大数据平台, 解决安全运营平台建设中接入难、使用慢、弹性弱、成本高等问题。

以融合式分析机制深度降噪、收敛、聚合, 提升威胁分析研判效率。提供自动化告警降噪收敛、智能化关键信息聚合、交互式图谱拓线的威胁分析功能体系, 解决告警风暴难处理、告警误报难消除、高级威胁难发现、分析研判门槛高等问题。

以体系化的协同响应功能, 增强响应处置人机协同、人人协同的灵活性、及时性。协同响应功能体系贯穿响应处置整个工作流程, 一站式实现指挥统筹、协同流转、自动化响应、流程化闭环, 解决传统响应处置不连贯、不协同、难流转的问题。

以实战化、自动化、常态化的自评估机制, 助力企业持续发现防御短板、改进优化。国内

最早研制 BAS 技术，率先完成诸多行业头部客户落地实践，依托 360 云端海量且真实的攻击积累，输出高质量评估验证能力，解决防御短板难发现、安全规划缺度量的问题。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230020

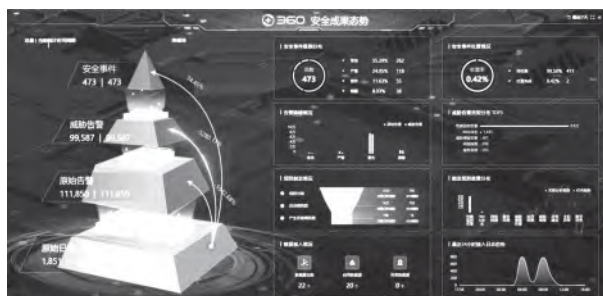
★有效期：2023 年 1 月 6 日至 2025 年 1 月 6 日

所属品牌：360

发布时间：2020 年 9 月

产品适用领域：政府、金融、教育、运营商、国央企、民营企业、
交通、医疗等行业

产品照片：



产品咨询邮箱：service-tech@360.cn



产品咨询二维码

山东云天安全技术有限公司

山东云天安全技术有限公司成立于 2016 年，专注网络信息安全产品的研发、生产及销售，大力推进网络安全技术创新和产品服务创新，为政府企事业单位提供体系化的独立第三方网络空间安全运营服务。

云天安全通过了高新技术企业认定、软件企业认定、大数据企业认定，信息系统安全集成、安全运维、风险评估、应急处理服务资质认证及多项 ISO 体系认证。自主研发的安全产品获得知识产权证书百余项。公司董事长被评为泉城产业领军人才，公司被评为省市级瞪羚企业，省市级“专精特新”企业、省重点上市后备企业、省大数据 50 强企业、省网络安全重点企业、省软件工程技术中心、省市级工业企业“一企一技术”研发中心、市工程研究中心、市企业技术中心等。公司已成长为山东本土最大的安全厂商，也是国内石化行业最核心的安全厂商之一。

网址: <https://www.cloudskysec.com/>

电话: 0531-58677600

地址: 山东省济南市历下区经十路 12111 号中润世纪中心 1 号楼 38 层

产品名称：昊天融合安全数据采集与监控系统

产品概述

昊天融合安全数据采集与监控系统（超融合探针）是一套集探测、采集、监测、分析及展示于一体的超融合系统。系统能够实时地对采集到的不同类型的信息进行标准化处理和实时关联分析，协助安全管理人员从海量日志中迅速准确地识别安全事故，同时提供安全事件的详细攻击路径、终端指纹和行为特征，实现全面取证，精准溯源。

通过收集资产的日志、巡检信息、配置信息等数据，对资产进行实时的安全行为监测及分析；体系化、集中化的漏洞扫描、安全状态监控、威胁情报告警、全流量监测，对安全态势实时感知、综合分析，实现风险预警、安全可视化，帮助用户及时了解安全风险状况，大幅提升组织安全防护能力。

功能特点

- ◎资产扫描任务：对指定网段进行扫描发现网段内资产。
- ◎弱口令扫描任务：对指定网段内资产进行扫描，发现存在的弱口令。
- ◎漏洞扫描任务：对指定网段配置漏洞扫描任务，发现资产漏洞。
- ◎入侵事件：平台探针结合流量规则库对恶意行为进行告警发现，查看事件趋势、数量并呈现。
- ◎流量弱口令：通过对网络流量监听发现弱口令信息。

◎攻击威胁情报：管理所有通过威胁情报比对发现的攻击威胁告警记录。

◎外联威胁情报：管理所有通过威胁情报比对发现的外联威胁告警记录。

◎自动化报告生成：根据设置自动输出报告。

技术指标

◎硬件参数：

2U 机架式工控机、8 核心处理器；

64G 内存、1T+4T 存储（可扩展）；

4 个千兆 RJ45 电口（可选 SFP+ 光口）；

2 个 USB 口，1 个 Console 口，交流冗余电源。

◎性能参数：

网络吞吐量 $\geq 1\text{Gb}$ ；

原始数据并发采集能力 ≥ 20000 条 /s；

事件分析处理能力 ≥ 10000 条 /s；

告警类数据支持 30 天跨度查询，页面查询响应速度 $\leq 2\text{s}$ ；

审计类数据支持 7 天跨度查询，查询响应速度 $\leq 2\text{s}$ 。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00378-A

★有效期：2023 年 12 月 1 日至 2025 年 12 月 1 日

所属品牌：云天安全

发布时间：2023 年 12 月 1 日

产品适用领域：制造业、石油化工、能源、水处理、航旅、交通运输、医疗等领域。

产品照片：



产品咨询二维码

产品咨询邮箱：shichang@cloudskysec.com

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：深信服安全感知管理平台

产品概述

以安全可视和协同防御为核心，深信服安全感知管理平台 (SIP) 旨在构建智能化、精准化、具备协同联动防御及人工专家应急能力的大数据安全分析平台和统一运营中心，对威胁进行实时监测、预警处置，让安全可感知、易运营，以便应对日趋复杂的业务网络安全环境。

深信服 SIP 产品架构以全流量分析为基础，通过探针、深信服自有安全设备及第三方安全设备等安全组件采集全网关键数据，以安全感知管理平台为安全大脑核心，结合威胁情报、行为分析、UEBA、机器学习、大数据关联分析、可视化等先进技术实现全网业务可视和威胁感知，从而实现全面发现各种潜伏威胁。同时，SIP 提供易运营的支撑体系，便于安全服务专家或相关运维体系介入与应急响应，提高事件响应的速度和高级威胁发现能力。

功能特点

全局安全可视：通过全流量分析、多维度的有效数据采集和智能分析能力，实时监控全网的安全态势、内部横向威胁态势、业务外连风险和服务器风险漏洞等，让管理员可以清楚的感

知全网是否安全、哪里不安全、具体薄弱点、攻击入口点等，围绕攻击链来形成一套基于“事前检查、事中分析、事后检测”的安全能力，看清全网威胁，从而辅助决策。

◎**大数据分析、检索能力**：深信服安全感知管理平台基于大数据框架，结合 Elastic-Search 引擎进行设计，产品默认具备 TB 级别的海量数据存储、关联分析能力，并可通过集群等方式进行扩充。同时，应用深信服数据分析团队在大数据性能优化方向多年的研发能力积累，让安全感知平台具备万亿级数据的超大规模数据管理和秒级查询能力。

◎**智能分析能力，应对未知威胁**：深信服安全感知管理平台具备智能分析技术，利用机器学习、关联分析、UEBA 等新技术，能够检测 APT 攻击、网络内部的潜伏威胁等高级威胁，无需更新检测规则亦能发现最新威胁。

◎**实时监测，精准预警**：深信服安全感知管理平台通过对全网流量、主机日志和第三方日志的采集分析，实现对已知威胁（僵尸蠕毒、异常流量、业务漏洞等）和未知威胁（网络僵尸、APT、0day 漏洞等）的全天候实时监测，同时结合智能分析和人工干预的便捷运营支撑，对已发现的威胁进行精准化预警，简化运维，有效进行通报预警。

◎**高效协同响应，阻断风险扩散，辅助闭环**：深信服安全感知管理平台可联动深信服自有安全设备和第三方安全设备，当发生重要安全事件或风险在内部传播时，可通过联动进行阻断、控制，避免影响扩大，联动方式涉及到网络阻断、上网提醒、一键查杀等，可有效辅助管理员进行问题闭环。

◎**威胁举证与影响面评估**：深信服安全感知管理平台可将 IP 自动化地进行资产类型划分，以业务安全及终端安全的维度实现不同类型受损情况展示，聚焦运维人员对业务资产的关注点。同时，结合详细攻击内容举证、多维度潜伏威胁、基于流量可视威胁黄金眼，可清晰直观看清威胁影响面，评估受损情况。

◎**追踪溯源**：深信服安全感知管理平台基于全流量和第三方日志（中间件、操作系统、安全设备等）的有效数据提取能力，实时提取有助于威胁分析和追踪溯源的关键元数据，结合 TB 级别的超大存储空间及集群部署能力，可存储至少 1 年以上的元数据。同时，利用可视化技术形成以流量可视、潜伏威胁黄金眼、威胁攻击链可视、统一检索及大数据能力等技术为主的追踪溯源支撑体系，为安全专家的溯源分析提供有力支撑。

技术指标

◎**大屏可视化**：支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，产品内置综合态势大屏、分支安全态势、安全事件态势、通报预警态势大屏、物联网安全态势大屏、全球网络攻击态势、资产态势、外联风险监控态势等；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置。

◎**资产识别**：支持主机类资产识别，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基线异常、操作系统等，支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性并重新识别补齐缺失字段，支持跨三层取 MAC 地址，识别资产 MAC 地址。

◎**脆弱性分析**：支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web 明文传输、可用性风险），支持第三方漏扫报告导入和解析，可按资产组分类上传，支持上传文件。

◎**威胁专项分析**：支持勒索专项检测，帮助客户更好的应对日益严峻的勒索风险，支持对勒索主题的安全告警进行统一展示和管理；支持挖矿专项检测，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果。

◎**联动响应**：支持与同品牌防火墙、行为管理、超融合、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等，并可联动超融合进行关机、挂起等；支持联动第三方应用进行处置；

◎**安全风险报告**：支持综合安全风险、主机安全风险、脆弱性感知、外部威胁感知、工单报告、摘要报告、处置报告多种方式呈现，可快速生成月度、季度、年度报表，摘要报告支持至少三种导出方式，至少包含 ppt、pdf、doc，满足客户不同场景的汇报需求。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：23SS00116-A

★有效期：2023 年 09 月 28 日至 2025 年 09 月 28 日

所属品牌：深信服科技股份有限公司

发布时间：2016 年 9 月

产品适用领域：交通、公安、能源、金融、医疗、媒体、政府、教育等

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn

产品名称：深信服可扩展威胁检测响应平台 XDR

产品概述

深信服可扩展威胁检测响应平台 XDR 是一种通过对多源遥测数据进行数据采集，实现数据编织、威胁检测、事件调查、威胁狩猎、响应处理功能的安全产品。通过 E+N 聚合分析引擎、上下文关联分析，实现攻击故事线还原、海量告警降噪的效果。内置 SOAR 功能模块，具备剧本化事件响应的能力，结合 MDR 服务提供事件分析与响应服务，释放运营人员精力，带来实战对抗能力增强、运营效率大幅提升的效果体验。

功能特点

◎**第三方数据质量分析**：支持将接入的第三方设备进行数据质量效果评级，最高三级。并将第三方设备产生的每个级别的数据（日志，告警，事件）进行统计，直观的看出每个设备的数据使用情况。

◎**基础分析检测能力**：支持威胁复测，平台支持对来自第三方网络和终端组件的安全告警和审计日志进行二次检测，从而发现组件中误报、漏报，并给出更新后的检测结果

◎**安全告警分析与展示**：支持告警智能定性分析，可以将告警诊断定性为定向攻击、攻防演练、内部测试、监管通报、病毒、扫描器攻击、脆弱性风险、业务不规范与其他威胁等。

◎**安全事件分析**：支持攻击链、入口点、父子进程、影响面的还原，可支持进程树纵向拓展至 10 个及以上层级，横向拓展至 15 个及以上层级，以对风险资产的复杂威胁提供更全面细颗粒度的展现视角。

技术指标

◎**数据采集层**：检测效果取决于高质量的数据采集能力，过往基于单一来源数据的检测设备难以有效检出高级威胁与未知威胁。深信服 XDR 遥测数据采集的类型分为三种，分别为网络侧遥测数据，终端侧遥测数据以及第三方数据，采集的数据以 JSON 或文件的格式上报。

◎**检测能力层**：深信服 XDR 平台的安全检测能力主要围绕“能力三叉戟”——威胁检测能力、关联分析能力、应急处置能力。通过对三个能力的深度覆盖，带来面对多种安全场景下的完整安全闭环的价值。除此之外，还具备对风险的检测、融合、以及分析能力。

◎**资产中心**：资产管理是安全运营工作的核心，安全问题都是以资产为基础开展响应闭环。通过资产管理模块，可以解决资产分散、指纹模糊、定位困难等一系列管理问题，为后续的资产风险识别、威胁事件响应、流程工单协作建立基础。

◎**脆弱性管理**：深信服 XDR 平台结合网络侧（云镜）以及端点侧识别（EDR/CWPP）漏洞检测，能够全面的了解用户设备的真实漏洞情况。

◎**智能对抗**：基于安全运营该现状，深信服 XDR 提供智能对抗用于解决大量病毒、挖矿等安全事件的处置闭环，针对一些置信度高的事件，进行自动封禁处置，将安全运营工程精力释

放出来，用于面对高级威胁事件研判分析处置。

◎ SOAR：深信服 XDR 平台提供了可视化的流程编排工具，可通过剧本的方式编排响应处置流程，一旦发现安全问题就立即启动预定义的剧本，快速将安全事件进行闭环，实现了根据不同类型的风险自动化执行不同的处置流程。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0503230561

★有效期：2023 年 3 月 17 日至 2025 年 3 月 17 日

所属品牌：深信服科技股份有限公司

发布时间：2022 年 5 月

产品适用领域：政府、教育、医疗、企业、金融等行业

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn

神州灵云（北京）科技有限公司

神州灵云（北京）科技有限公司，成立于2016年，是基于大数据分析平台和人工智能技术，提供网络全流量实时分析和应用业务数据融合解决方案的高科技公司，是国内性能管理和全流量安全的开拓者。神州灵云独创地将全流量实时分析与应用代码级监控技术通过智能综合运维大数据平台进行融合，对网络、应用和业务数据进行建模分析，实现全链路一体化性能可观测。助力客户秒级定位故障位置，查找问题根因，并留存网络原始数据，加速向新一代智能运维 AIOps 转型，重塑 IT 服务价值。

网址：<http://www.dclingcloud.com>

电话：400-058-0958

地址：北京市朝阳区望京阜通东大街6号方恒国际中心A座2002室

产品名称：神州灵云 APT 威胁监测系统

产品概述

神州灵云 APT 威胁监测系统是一套由神州灵云完全自主设计研发的软硬件一体化网络安全检测产品，主要部署在客户环境的网络出口、核心枢纽等关键网络位置，主要以分光接入或交换机镜像接入等旁路的方式接入实时流量数据进行分析，也可以部署在其他工作开展方便的网络环境，主要进行离线网络流量的分析。

产品基于先进的自研流量分析处理引擎以及完善的安全架构规范打造实现，集成了网络威胁检测、脆弱性检测、数据泄露检测、溯源取证、全流量分析、网络审计、响应处置等全维度网络流量测安全能力。其中，安全能力的“融合”是本产品的核心设计理念，产品内部的所有安全检测和流量分析功能均能够较好的进行便捷、直接的关联，保证用户在流量层面灵活、完整的安全分析和把控，以实现在保证局部安全能力的同时，保证产品整体的实战应用能力。

功能特点

神州灵云 APT 威胁监测系统主要功能：

◎完整准确的的底层数据构建能力

底层基于完全自研的流量处理框架进行流量的基础分析处理，在流量重组、协议解析、功能编排等层面具备业内领先的功能稳定性。

◎全面的异常发现能力

充分考虑高级威胁、未知威胁场景，难以直接发现威胁过程的特点，设计了很多高级威胁行为难以绕开的协议异常、行为异常、数据异常、网址异常等异常检测策略，及时发现相关安

全线索，为面向高级威胁、未知威胁的分析研判提供更多的线索和入口。

◎灵活的迭代分析能力

充分考虑流量安全分析场景的不确定性进行设计，支持以留存的原始实时流量、上传或其他方式接入的离线流量为数据源，进行不限次数的迭代分析检测，支持自由设定每轮流量分析的配置策略，独立保存每轮的流量分析结果，为策略验证、研判思路验证以及更有深度的流量分析提供良好的支持。

◎灵活的功能定制能力

产品技术架构基于通用、完整、可拓展的思路进行搭建，从流量分析处理的最底层到数据功能呈现的最前端都支持灵活的功能调整和面向不同业务场景的拓展，为流量分析检测相关技术的演进变化以及面向不同业务需要奠定了良好的基础。

◎灵活的分析配置能力

友好支持专业级流量安全分析人员使用，在流量分析的配置环节，支持功能开启、数据过滤、协议识别、应用服务识别、异常检测、威胁检测规则及威胁情报、敏感数据检测、行为模型检测、脆弱性特征、敏感数据等等进行非常灵活的自定义配置，实现完全自由且按需进行的流量分析能力。

◎全面的数据关联能力

始终强调针对数据结果进一步的研判分析能力的支持，因此提供了立体化的全维度数据关联能力，支持在数据结果页面直接关联多维的结果，同时提供指定特定条件的关联数据页面跳转，为研判场景的融合分析提供了良好的支持。

◎超高的分析处理性能

全局的流量分析处理性能是产品的核心技术要求，目前产品支持 20Gbps 通用流量场景的完整功能支持能力，对于特殊需求场景，可以针对性地进行技术调整，拓展到 40Gbps 的流量处理能力。

技术指标

◎流量接入

- ★支持对实时流量接入的采集网口进行自由的选择配置；
- ★支持配置需要分析的流量的时间范围；
- ★支持配置 BPF 格式的流量过滤规则进行流量分析的过滤；

◎流量统计

- ★支持对原始流量的实时流速、实时包速、实时连接建立速率、实时并发会话数进行统计；
- ★支持展示接入流量的 TCP 完整度，反映接入流量的完整性；
- ★支持对原始流量的历史累计趋势进行统计；
- ★支持对 TCP、UDP 的端口占比情况进行排序展示；

- ★支持对应用层协议的占比情况进行排序展示；

◎流量识别

★支持自定义协议或服务识别规则对流量进行识别，支持的规则配置项包括但不限于：IP、传输协议、端口、负载等特征的组合。

- ★支持配置多包交互数据特征的协议和服务识别规则；

◎威胁检测

★支持包含 Nessus、绿盟 NSFOCUS、安恒明鉴、华云安灵鉴、洞悉、云镜、Nmap、UnicornsCan、Xray、SQLmap、Masscan、Nexpose、Zmap、Metasploit、Netcat、Nikto 等工具在内发起的漏洞扫描行为检测；

★支持 SQL 注入、缓冲区溢出、代码执行、跨站攻击、未授权访问等多种类型的漏洞攻击进行检测，具备 0day 漏洞利用攻击的检测能力，具备包含摄像头漏洞、网络设备漏洞、信创系统漏洞在内的多场景漏洞利用检测能力；

★支持 WebShell、木马、病毒等多种恶意文件进行检测，支持的 WebShell 类型包括 PHP、JSP、ASP、ASPX 等，支持针对邮件附件中的恶意文件进行检测；

★支持对目标失陷后的各类心跳连接、DGA 域名、命令控制、系统控制、WebShell 连接、横向移动等恶意行为进行检测，支持各种变形的 WebShell 连接检测；

★支持 CobaltStrike、nmap、sqlmap、awvs、OpenVAS、zgrab、Nessus、菜刀、蚁剑、冰蝎、哥斯拉等三十余种恶意工具的相关恶意行为检测识别；

- ★支持对 APT 威胁的 APT 组织、APT 方向进行解读；

- ★支持基于 KillChain 模型对 APT 威胁进行威胁阶段的解读；

★支持对漏洞攻击相关的漏洞编号、漏洞描述、漏洞等级、影响组件和攻击状态进行检测识别；

- ★支持对网络威胁进行区分于攻击前、攻击中、攻击后的阶段识别；

- ★支持基于 ATT&CK 框架对威胁结果进行战术和技术的解读。

- ★支持基于流量原始时间戳进行规则的时效性的匹配性检测；

★支持添加或导入至少包含黑 IP、黑域名在内的威胁情报进行威胁检测，支持配置威胁情报的失效时间；

★支持提供可拓展的威胁检测规则配置入口，实现包含 IP、传输协议、端口和负载特征组合条件的检测配置能力；

- ★支持配置多包交互数据特征的威胁检测规则；

◎敏感数据检测

- ★支持针对自定义的敏感数据进行检测；

- ★支持对敏感数据进行分组、分级配置；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0108230137

★有效期：2023 年 1 月 20 日至 2025 年 1 月 20 日

所属品牌：神州灵云

发布时间：2020 年

产品适用领域：能源、政府、金融、医疗、军工

产品照片：



神州灵云
DCLINGCLOUD

产品咨询邮箱：support@dclingcloud.com



产品咨询二维码

沈阳东软系统集成工程有限公司

沈阳东软系统集成工程有限公司 1997 年 3 月 6 日成立，注册资金 7500 万元。公司秉承“超越技术的应用智慧”的经营理念，为客户提供优秀的计算机系统集成解决方案为核心业务方向，以客户为中心，面向政府、公检法和企业的信息基础设施建设，围绕客户的核心业务，提供软件和安全解决方案。业务范围包括：计算机信息系统软件开发、硬件系统安装调试、面向客户的 IT 信息系统规划和建设方案、IT 设施运营维护、技术培训、建筑智能化设计与施工、信息安全服务、商用密码产品的生产及销售等。近年来，在政府、通信、医疗卫生、交通、税务、教育、电力、安全等领域，保持领先地位，市场遍布全国十几个省市地区。

网址：<http://www.neusoft.com>

电话：010-57080489

地址：辽宁省沈阳市浑南区创新路 175-3 号 501、502、503、504、510 室

产品名称：东软 NetEyeSOC 网络安全管理系统 V5.0

产品概述

随着态势感知产品形态的发展，现有产品已经不能够完全满足市场需求。随着大数据时代、人工智能时代的来临，态势产品应该全面进入基于日志大数据分析的人工智能态势感知时代。为了紧密结合态势感知产品的发展趋势，产品考虑以下的设计理念：

采用前后端分离技术，将前端独立出来。拥抱前端技术发展的红利，使用更先进的前端渲染技术，为用户提供操作更流程、响应更及时、效果更丰富的前端展示页面。以用户体验为中心，优化页面操作设计。

后端将系统按照逻辑关系划分模块，定义模块与模块之间的接口。模块设计基于设计模式的六大原则。实现后端平台建设的灵活性和可扩展性。

架构设计的底层支撑平台经平台功能从业务功能中抽离出来，让业务研发更加专注于业务处理，其他的平台级别的功能通过一些技术手段隐形的织入业务处理的流程中。做到平台与业务分离，简化业务研发成本。

随着数据量的不断提升，架构需要采取分布式架构的技术路线。根据基础设备的性能实现动态的缩扩容，全方位的使用基础设备性能。保证对大数据的高吞吐、低延迟计算，对数据处理要具备准确性，支持 exactly-once 语义。

整体架构要对云端微服务做技术储备，支持最小投入可微服务化的分层设计，明确业务边界。

功能特点

支持单机部署，支持集群分布式部署。支持三级组织架构部署，支持分域、分级、分权管理。

SOAR 剧本模板支持与防火墙，EDR，工单，邮件、短信方式告警、执行动作联动。支持综合安全态势感知、资产安全态势感知、外部攻击态势感知、内网安全态势感知、流量态势感知、异常行为态势感知、脆弱性态势感知、威胁事件态势感知等。

支持 UEBA 检测：UEBA 检测引擎支持从统计分析、机器学习两种模式建立数学模型分析、检测。支持建立单体模式基线和组模式基线。支持模型编辑、新建。支持对用户行为，包括流量、连接、应用等行为特征建模，能够分析、预测用户行为异常。进行用户、用户组的时域、空域特征比对，结合用户、资产的属性，将异常分析由单点拓展至组特征，实现 30 余种异常行为告警。

支持拓扑管理，支持拓扑编辑器，支持拓扑对象节点的矢量化，支持多层拓扑，区域、组拓扑节点支持收起、展开；支持拓扑连线的多维属性配置。

支持基于资产 IP 维度绘制全网连接关系全景图，全景图支持全网资产 IP 连接按照流量、连接数选择 TOP10、TOP20、TOP50 等筛选，支持配置协议筛选、流量大小、连接数数量筛选；支持单个资产绘制连接关系图，支持按照该资产的流量、连接数选择 TOP10、TOP20、TOP50 等筛选，支持配置协议筛选、流量大小、连接数数量筛选；支持选择协议、端口进行筛选。

支持对市场主流厂商的路由器、交换机、防火墙、WEB 应用防火墙（WAF）、VPN 设备、上网行为管理设备、入侵检测 / 防护系统等网络和安全设备的基本信息、操作日志、访问日志、安全日志、告警日志等系统日志进行采集。已支持的设备数量 200 余种。支持对 WINDOWS、LINUX 等主流服务器操作系统的基本信息、登录日志、运行日志、告警日志等进行采集。支持对中间件软件（IIS、Websphere / Weblogic、Apache、Tomcat、Ngnix）日志信息的收集，包括状态会话、应用进程、HTTP/HTTPS 访问记录等信息。支持对网管平台（包括锐捷、华为 esight 等）的数据进行采集，采集的数据包括：基本信息、操作日志、访问日志、安全日志、告警日志等系统日志。支持对 SQL Server、Oracle、mongodb、MySQL 等主流数据库系统日志进行采集。

技术指标

秉承“业务驱动安全”理念，本产品从以下几方面实现“业务驱动安全”的理念：

◎全面的可视性：理清企业目前业务和资产是怎样的状态，有哪些风险，有哪些核心资产。

◎智能的实时态势：清晰地呈现 IT 或业务架构，当出现网络攻击时更加容易地定位问题。

◎灵活的分析：一旦发生泄密，有相应的工具或平台能够快速定位问题、分析问题。

◎公司治理与合规：执行标准包括 GDPR、ISO27000、等级保护、关键基础设施保护等。

强大的设备兼容性，本产品可以无缝解析 14 大类，接近 300 余种设备的日志，对于不支持

的日志格式，提供可视化的规则设计器，通过简单的设置支持逗号分隔串、JSON 串等解析；同时，产品研发团队定期升级内置的解析规则，紧跟主流安全设备的日志格式变化。另外，平台还通过 API 调用等方式，实现了与市场主流防火墙、漏洞扫描设备的联动，当发生攻击威胁时，实现自动阻断，并识别潜在的受攻击资产。

领先的智能分析能力，本产品内置几十种安全分析场景，提供可视化的策略编辑器，包括聚合策略、关联分析策略、UEBA 策略、SOAR 策略，全面提升安全检测、分析、响应的精细化操作、自动化程度，同时由专业的安服团队定期更新分析场景。

领先的威胁情报作为国家网络安全应急服务支撑单位、国家安全漏洞库 CNVD 核心提供者，东软一直致力于网络威胁情报的挖掘、积累和交换共享。2018 年，东软与国际知名网络安全厂商 Fortinet 联合组建东软成都学院网络安全实验室，进一步提升了威胁情报的应用能力和水平，突出的交付能力，东软集团作为国内首家通过 CMMI5 级认证的软件企业，遵循着一套完整、严谨的交付流程体系，自 2015 年以来成功交付国家环保部、宁波市经济和信息化委员会、国家电力投资集团、华夏银行等多个千万级大型项目，涉及行业专网、政务外网和企业内网的预警监测、态势感知和处置服务。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231045

★有效期：2023 年 05 月 05 日至 2025 年 05 月 06 日

所属品牌：东软 Neteye

发布时间：2023 年 4 月 30 日

产品适用领域：学校，政府，医院，石油等。

产品照片：



前面板



后面板



产品咨询二维码

产品咨询邮箱：zhaohcp@neusoft.com

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：腾讯 T-Sec 安全运营管理平台

产品概述

腾讯安全面向政府、金融、制造业、医疗、教育等大中型企事业单位推出的智能化安全运营平台。以云原生技术为基础，仓湖一体化大数据平台为底座，MITRE ATT&CK 技战术框架为指导，结合腾讯领先的威胁情报能力、AI 和可视化技术，聚焦 TDIR（Threat Detection, Investigation and Response）威胁运营，打造智能化安全运营平台，提升企业安全运营效率，实现企业全网安全态势可知、可见、可控的闭环。

功能特点

◎数据接入

数据采集支持不同来源、不同类型、不同格式的数据聚合。输入来源包括但不限于流量探针的流量日志数据，来自第三方网络设备和安全设备的同步日志或事件信息日志。

◎数据处理

产品内置大量设备的解析策略，覆盖市场上大部分的设备类型与型号，达到开箱即用。针对未覆盖设备平台支持多种快速解析的方案，强大且易用的解析配置能力，支持多种解析方式，同时平台内置脚本解析引擎，方便扩展定制化的解析需求。

◎安全检测

将接收的来自第三方安全设备、系统、应用日志归一化后的日志，通过多源日志关联、日

志与漏洞信息关联匹配，生成高确信安全告警。

◎调查分析

提供了图形化交互的搜索工具，展开人工主动威胁调查或狩猎，根据需要对本系统存储的基础安全数据进行检索，并可将检索出的数据生成十六种不同特点的日志统计图表，实现安全威胁的调查与分析。

◎联动响应

平台支持对告警、漏洞、设备、用户等风险对象发起响应动作，动作类型包括：安全工单、通知策略和联动策略三类。支持用户直接从各个功能模块快速发起响应动作，也可以从响应中心自定义创建响应工单或策略。

◎资产管理

通过对资产可视化管理，支撑安全管理人员从资产的角度了解安全态势。

◎漏洞管理

聚合多种来源产生的漏洞事件，展示漏洞相关信息，为漏洞修复和资产风险管理提供支持。

◎安全可视

平台为各层次用户提供可视安全，让安全看得见可评价。安全 BI 支持安全分析人员创建监测仪表盘进行实时监控。统计报表为安全管理人员提供统计分析工具，定期对安全运营各维度指标进行复盘。3D 态势大屏为安全管理领导层宏观呈现全局安全态势，为其对业务安全的持续改进和决策提供全局视角。

技术指标

◎数据遥测

支持 200 多种网络设备、安全设备、主机系统、数据库等主流产品的数据归一化解析能力，支持对个性化日志进行自定义解析模板配置。接入多种接入方式，包括：udp、tcp、syslog、kafka、nsq、jdbc、ES、beats 等方式。

◎多源关联分析引擎

SOC 关联分析引擎支持简单规则、无序规则和有序规则三大类检测逻辑，可覆盖绝大部分威胁场景的检测与识别，并可将每日百万级告警日志数量收敛到千百级人工可处置的量级。

系统内置开箱即用的告警策略 700+，覆盖 47 类重保安全场景和 67 类通用安全场景，ATT&CK 技战术框架覆盖度 74%。同时支持用户自定义告警策略，并提供交互向导模式和高级编辑器模式，满足使用习惯的安全运营人员使用。

◎腾讯海量高精度威胁情报库

腾讯威胁情报中心拥有海量基础安全大数据，和高质量威胁情报数据及应用，包括百亿级恶意文件、木马病毒样本库；数亿级 IP 信誉库、域名信誉库；数千万级恶意网址、数百万级核心 IOC 情报数据；全球部署 1000+ 蜜罐、2000+ 沙箱；识别近百个全球 APT 组织、上万个暗网

& 深网入口。

◎ UEBA 异常行为违规风险检测

通过自动回溯、故事线串联全方位、多维度的告警日志、行为信息、用户和资产等数据，进行行为基线学习和群体异常检测分析。内置规则引擎、画像分析引擎、智能 AI 引擎，覆盖已知威胁聚焦风险行为，通过自研风险量化算法智能评分。能够自动识别高风险得分用户和设备。通过时间线查看异常行为的上下文信息，极大提升风险定位和详情调查以及处置响应的效率。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231932

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：腾讯安全

发布时间：2018 年 06 月 28 日

产品适用领域：金融、政务、政企事业单位、能源、交通、出行、制造业、物流、互联网、医疗、教育、农文旅、传媒等

产品照片：



产品咨询二维码

产品咨询邮箱：secwwang@tencent.com、invokerdu@tencent.com、herryqi@tencent.com

亚信安全科技有限公司

亚信安全是中国网络安全软件领域的领跑者，是业内“懂网、懂云”的网络安全公司。承继亚信 30 年互联网建设经验，肩负守护互联网之使命，亚信安全于 2015 年正式启航，目前已成为建设中国网络安全的重要力量。不负使命，成功执行建党 100 周年、历年两会等国家重要网络安全保障任务 30 余次。

依托互联网建设能力，让亚信安全具备强大的“懂网”业务能力与资源优势；深耕网络安全高精技术，让亚信安全拥有优异的“懂云”技术基因。亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理及 5G 安全等领域突破核心技术，用实力筑牢云、网、边、端之安全防线。

亚信安全在中国网络安全电信行业细分市场份额占比第一，连续五年蝉联身份安全中国市场份额第一，终端安全中国市场份额占比第二，在威胁情报、EDR、XDR 等细分技术领域均居于领导者象限，是中国网络安全企业 10 强。

网址：www.asiainfo-sec.com

电话：400-820-8876

地址：江苏省南京市雨花台区花神大道 98 号东久创新中心 1 号楼、2 号楼 3 楼

产品名称：亚信安全信舵安全管理与分析平台

产品概述

信舵安全管理与分析平台采用先进的大数据架构，通过采集企业内所有网络安全数据，包括全网资产信息、脆弱性信息、攻击行为信息、情报信息、异常流量信息等，利用智能引擎对安全数据进行融合分析，实现对网络攻击行为、安全威胁事件等网络安全问题的发现和追溯。

信舵安全管理与分析平台采用了独创的“1+3+1+S”的战略生态模式，即 1 个平台 +3 类探针 +1 个威胁情报引擎 + 安全编排与自动化响应系统（SOAR）。打造监测、发现、分析、处置的安全运营流程，通过内置的各种引擎，运用规则模型、聚类统计、关联分析、情报碰撞等实现对网络安全事件的发现和处置。

平台具备安全监测中心、安全分析中心、安全响应中心、安全资产中心、知识情报中心等能力中心，部署在用户信息系统网络之中，实现实时安全告警分析、多视角态势监测感知与自动化处置。

功能特点

平台的功能架构包括首页门户、安全能力中心、安全数据中心、技术引擎、平台管理几部分：

◎**首页门户**：采用可视化方式，从威胁、资产、响应等多个维度全面展示全网安全态势和安全运营情况；

◎**安全能力中心**：提供了全面的安全监测、分析、响应能力，包括监测中心、分析中心、响应中心、脆弱性中心、资产中心、情报中心等模块；

◎**安全数据中心**：实现安全数据的聚合及处理，形成稳固的大数据底座，包含数据采集、数据处理、数据解析、数据管理和数据存储等功能；

◎**技术引擎**：包含多种亚信安全自主研发的处理引擎，提供多种基础能力，能够显著提高平台的处理性能；

◎**平台管理**：作为统一的运维管理中心，实现平台的可视化管理、流程管理、统一权限、统一配置和统一监控等功能。

技术指标

◎强大的数据处理性能

采用基于大数据的处理架构和存储框架，保障平台的数据处理的实效性和准确性。

◎灵活弹性的服务架构

平台采用微服务架构，将业务模块微服务化，服务之间互相协调配合，提高了服务灵活性。

◎稳健的数字底座支撑

采用大数据技术，具备数据采集、数据标准化、数据关联补齐和数据存储服务。

◎强大的关联分析能力

采用自研的安全事件关联分析引擎，实现多源日志关联分析能力，能够实时对范式化后的日志流进行关联分析。

◎智能 AI 辅助研判

采用国内首创的机器学习模型与人工标注结合的方法，引入 AI 推理引擎，实现人机互动，有效减少安全告警误报率、提高安全告警的准确性。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230705

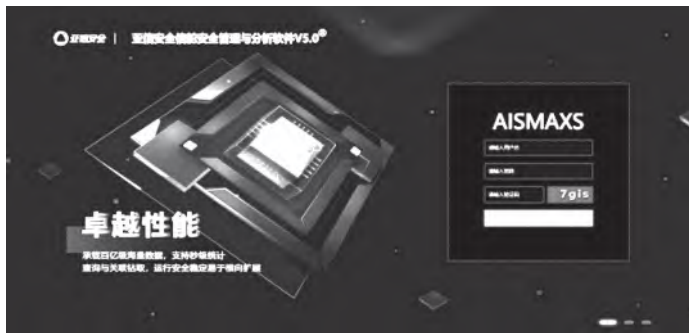
★有效期：2023 年 03 月 31 日至 2025 年 03 月 31 日

所属品牌：亚信安全

发布时间：2022 年

产品适用领域：金融、企业、政府、电力、交通、医疗、运营商等

产品照片：



产品咨询二维码

产品咨询邮箱：sec-business@asiainfo-sec.com

远江盛邦（北京）网络安全科技股份有限公司

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全，股票代码：688651）成立于 2010 年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为用户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。公司秉持精准识别、精确防御、深入场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图等领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能各行业用户的数字化安全转型，护航国家网络空间安全战略实施落地。

网址：www.webray.com.cn

电话：4006-911-199

地址：北京市海淀区上地九街 9 号 2 层 209 号

产品名称：综合日志分析与风险感知平台（RayThink）

产品概述

综合日志分析与风险感知平台（RayThink）是盛邦安全推出的，集感知、分析、研判、预测和处置于一体，能够对海量网络安全事件数据进行采集、存储与关联分析的系统，它通过构建安全模型实现风险预测，全面感知综合风险态势和资产安全状态，并结合通报预警和应急处置流程形成闭环的安全指挥体系，适用于企业内部网络安全整体监控、垂直单位安全事件监管报送等多种行业应用场景。

功能特点

◎海量事件数据采集与分析

数据采集并对安全事件日志进行统一格式化处理和智能分析去重，采用 Elasticsearch 数据库实时快速地对海量数据进行存储、搜索和分析。

◎通报预警流程闭环管理

通报预警流程实现从建立、流转、审批到处置的闭环管理，支持预警处理和事件处置等流程的类型及紧急程度的自定义可指定责任人和监督人对流程处置的时效进行管理。

◎丰富的数据统计分析

可进行安全事件历史追溯，原始数据钻取，并形成合理的处置建议，多种维度的态势数据统计与分析，包括但不限于日环比分析、周环比分析、事件进度分析、安全趋势分析、资产健康度排名以及事件类型分布统计和地域分布统计等。

◎多维度可视化态势管控

多维度态势感知可视化大屏展示，包括安全事件实时播报、内网威胁态势、外网攻击态势、风险备案、威胁地域分布、事件和漏分布、值班状态、事件进度及设备运行状态等，并可以通过大屏便捷下发处置工单、封禁指令、误报删除和白名单等操作命令。

技术指标

◎安全事件数据的智能处理技术

数据解析支持识别所接收的数据格式，并识别数据类型，解析出标准化信息。还支持根据具体要求识别出特定的非标准化数据，当数据字段不完善或不符合标准时，支持对缺少的数据字段进行智能补全，并将不符合标注的数据字段进行标准化。

支持用户对所监测设备的数据过滤内容进行设定，包括日志类型及日志等级，当系统的数据解析引擎识别到日志信息符合用户所设定过滤条件时，系统会智能舍弃此类数据，过滤废弃数据。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231032

★有效期：2023 年 05 月 05 日至 2025 年 5 月 5 日

所属品牌：远江盛邦（北京）网络安全科技股份有限公司

发布时间：2020 年 12 月 25 日

产品适用领域：电力能源、通信、政府、金融、教育、交通、医疗等

产品照片：



产品咨询邮箱：support@webray.com.cn



产品咨询二维码

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，国有资本占股近50%。

基于“安全协同·AI赋能”的战略理念，公司在工业互联网安全领域持续深耕，团队核心成员是中国工业互联网安全事业的第一批践行者。

长扬科技在业界开创了“智能工业安全大脑”的产品理念，以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了60余款产品，面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉AI安全分析、工业零信任安全、工业数据安全和工业数据通信等多维度产品，构建覆盖工业互联网安全产业完整生命周期的安全保障体系。

公司总部位于北京，并在西安、武汉、郑州、成都、上海、广州等全国近30个城市建有研发中心及服务分支机构，形成了覆盖全国的“网状战略布局”，可为客户提供强有力的本地化服务。长扬科技积累了超过32个行业细分领域、4000余家工业企业的安全服务经验，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，提供4大类、27项标准化服务，致力于为工业企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：<https://www.cy-tech.net/>

电话：010-82194186

地址：北京市海淀区闵庄路3号四季慧谷·国家网络安全产业园2期15号楼

产品名称：工业互联网安全态势感知与智能运营平台 CG-N-INSSA/V3.0

产品概述

工业互联网安全态势感知与智能运营平台以网络安全数据、新基建关键基础设施行业数据为基础，以资产指纹、漏洞信息、威胁情报、网络模型等海量数据为资源支撑，运用大数据、人工智能及云技术，帮助企业精准识别网络威胁，提升风险评估、态势感知、监测预警及智能运营一体化的能力。

该平台融合大数据和云架构设计，具有多要素采集、多引擎安全分析、多方位态势感知、多层次开放连接、多维度安全可视化的技术特色。平台采用ElasticSearch全文检索分析引擎支持PB级的结构化和非结构化海量数据的处理，采用Spark流式计算引擎用于历史数据和实时数据联合分析。支持全方位工控安全数据采集、数据预处理、数据存储与分析、功能呈现以及向上级监管单位上报相关数据等功能。

功能特点

安全大数据分析能力：系统采用大数据的分布式存储、分布式计算框架，充分利用大数据挖掘、机器学习、复杂数据关联、大数据检索等技术手段，从海量网络事件中发掘未知的异常，如 APT 攻击，提升事件检测能力及准确性。利用大数据存储技术，完整保留了网络运行行为 PCAP 包数据，从而实现告警事件到异常行为的完整追溯。

深度分析及预测能力：平台集成先进的 ATT&CK 框架，规则库中关联攻击阶段及攻击技术，增强安全分析能力，同时基于已发生告警事件数据，预测短时间内攻击技术的走向。

平台同时提供网络攻击、异常行为统计功能，查看其在组织机构的分布情况，同时提供基于资产详情 -> 安全基线 -> 通联分析 -> 安全事件、病毒、情报、UEBA 等溯源分析能力。

基于 SOAR 的安全运营能力：平台将 SOAR 作为安全运营核心技术手段，内置全面的场景化剧本，支持灵活地、可视化地、自动化地编排模式，将多维度安全分析、研判、响应处置等多种能力进行串联，形成一整套场景化安全运营自动化响应处置方案。

为企业准确高效的安全运营起到推动作用，为安全运营人员提供自动化处置、移动端处置等多种处置方式，用户可根据特定需求灵活选择。提升企业的自动化安全运营能力降低人员依赖、进一步提高安全响应效率、提升工作效率减少运营成本，保障响应处置质量。

资产台账梳理及风险评估能力：系统采用主被动结合的资产发现方式，协助企业梳理资产台账，解决企业资产不清或台账不准确等问题。同时系统参照《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）相关标准的要求，从资产运行、安全事件、脆弱性告警与事件、主机配置数据为基础，科学评估资产风险状态，对全网资产进行全面的安全监测；助力企业在摸清资产家底的同时，主动及时掌握资产安全动态，实现风险的资产进行闭环处置。

集中设备运维管理能力：通过流量、日志、SNMP 等多种方式全面采集，并通过可视化的方式实时感知系统的运行状态、性能指标、异常情况等信息，最终帮助用户提前感知问题，预防故障发生，实现运维效率提升。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00254-A

★有效期：2024 年 3 月 01 日至 2026 年 3 月 01 日

所属品牌：长扬科技

发布时间：2020 年 3 月 12 日

产品适用领域：电力、能源、化工、石油石化、智能制造、水利水务等

产品照片：



产品咨询二维码

产品咨询邮箱：jing.zhang@cy-tech.net

浙江木链物联网科技有限公司

浙江木链物联网科技有限公司（简称：木链科技）受陈纯院士技术指导，成立于2017年，为工业互联网安全、工控网络安全代表企业。公司面向工业企业及关基单位提供安全合规整改、安全运营中心建设、网络安全实验室规划、安全业务创新及专业安全服务，并助力推动关键领域信息安全产品的高水平国产化替代。

目前公司已在军工、电力能源、石油石化、轨道交通、智能制造等重要领域部署产品、落地项目，包括某装备制造关基单位关基系统安全防护集成项目，中石油下属某储气库多维安全生产智慧化管控平台建设项目，核能行业某研究设计院网络安全靶场项目，核能行业燃料企业工控系统安全建设项目，大唐集团智慧电厂国产化替换升级采购项目等，多维度、多层次积极推动工业网络与信息安全发展和关键信息基础设施安全防护体系建设，为工业企业信息化数字化转型夯实安全基座。

“十四五”规划开局起步，数字化转型全面铺开推动网络安全加速发展。木链科技锚定网络强国、制造强国和数字中国建设目标，针对新技术下产生的工业新业态、新业务和新场景，为客户提供全面、有效、可持续的工业互联网安全建设方案。

网址：boolean.com.cn

电话：400-0571-950

地址：杭州市余杭区五常街道联创街188号贝达梦工场C座10楼

产品名称：BooleanGuard 工业互联网安全运营平台

产品概述

BooleanGuard 工业互联网安全运营平台以建立完整的工业互联网安全技术和管理体系为目的，融合多种信息安全技术和管理理念，充分实现组织、管理、技术三个体系的合理调配，帮助用户从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个环节实现对业务信息系统的统一安全保障。为用户提供安全合规，实时监测，智能分析，安全可视，追溯溯源，高效协同等价值体验。

功能特点

◎分布采集，统一处理：分布式部署探针采集数据，针对于不同网络环境，在边缘端通过探针获取和解析数据，统一发送到中央处理服务器做大数据分析和响应。覆盖工业领域全场景，支持工业流量、组态软件、工控设备、工业互联网平台等多维度的数据采集。

◎安全监测，风险可控：全面采集工控网络中的安全事件信息、资产流量数据、工控操作

指令等。结合 CNVD、CNNVD、CVE 等工控威胁特征库，对目标区域资产进行智能分析和综合评估，及时识别安全风险，采取相应的安全策略完成闭环处置。

◎全面感知，主动防护：平台集成各类安全信息感知模块，实现安全态势问题全面监控和快速发现，支持场景化分析，自动化分析，精准捕捉网络威胁，实现主动防护，提供丰富的攻击，资产和用户画像，挖掘海量安全数据背后的真正价值。

◎数据可视，概况总览：平台提供多种全局安全态势大屏界面，如安全态势、运营态势、资产态势，流量态势，3D 生产模型，溯源视图等。满足客户整体安全态势感知需求，实现对安全运营的有效支撑。

◎生产安全，行业定制：基于木链科技自身对安全和工控领域的的能力积累，平台可以根据用户实际需求，按照行业进行定制化开发，深入业务生产，利用安全与信息技术，赋能传统工业，加强安全管控，节能降耗，提升经济稳定运营能力，探索行业高质量发展路径，使工业生产环境可知，可管。

技术指标

数据处理能力：10000EPS（支持线性扩展）

数据查询能力：亿级数据秒查

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00464-A

★有效期：2023 年 12 月 22 日至 2025 年 12 月 22 日

所属品牌：BooleanGuard®

发布时间：2020 年 09 月 05 日

产品适用领域：工业互联网安全运营平台产品适用领域广泛，当前主要应用领域为政府单位、集团体系、工业企业、生产工厂等安全运营和保障需求。

产品照片：



产品咨询邮箱：info@boolean.com.cn



产品咨询二维码



信息系统安全管理平台

北京安博通科技股份有限公司

始创 2011 年,以“看透安全,体验价值”理念为核心,是可视化网络安全专用核心系统产品与安全服务提供商。其自主研发的 ABTSPOS 可视化网络安全系统平台,已成为众多一线厂商与大型解决方案集成商广泛搭载的网络安全系统套件,是国内众多部委与央企安全态势感知平台的核心组件与数据引擎。重研发投入和工程师文化,在北京、武汉设有研发中心,专注核心技术。作为国家高新技术企业,安博通及全资子公司获得和申请的专利软著超过 350 项,并保持每年 20% 以上的增速。已拥有 100 多家战略合作伙伴,50000 多个企业级客户,在网运行 SPOS 系统约 150000 多套。形成了以深度安全网关、数据分析与综合运维平台等产品系列组合,面向政府、金融、运营商、军队、企业、教育等客户业务场景。

网址: <http://www.abtnetworks.com/>

电话: 010-80699886

地址: 北京市西城区裕民路 18 号北环中心 2603

产品名称: 安博通 SPOS-Trace 网络安全管理平台

产品概述

安博通 SPOS-Trace 网络安全管理平台通过对全网防火墙、路由交换等访问控制类设备的安全策略数据进行自动采集与解析,基于大数据分析 with 人工智能算法,提供策略优化清理、策略合规审计、逻辑拓扑可视、安全路径可视、网络攻击面可视、策略应急封堵以及策略自动开通等功能,从而实现全网安全策略的集中可视化管理与智能化运维,提升全行网络运维自动化水平以及网络安全防护保障能力。

功能特点

◎异构设备安全策略集中管理

实现对全网防火墙、路由交换、负载均衡、VPN 等异构品牌、异构型号的网络安全设备的安全策略进行统一集中可视化展示、管理和控制,包括策略采集、策略解析、策略历史、策略变更监控、策略查询、策略清理、策略开通、策略风险分析等相关功能。

◎安全策略配置检查

安全策略配置检查通过对标准化的策略数据进行计算,检查策略规则之间的相互关系,从而发现隐藏策略、冗余策略、过期策略、可合并策略等问题策略,以及空对象、未被引用对象等问题对象;并且通过某些字段的分析发现空策略、含 ANY 策略、过期策略,实现垃圾策略与风险策略的检查,并提供处置建议,优化策略规则。

◎访问控制策略收敛分析

对进出防火墙设备的流量会话数据监控和统计，针对每条安全控制策略统计会话命中数据，并支持源地址、目的地址、目的端口等维度对安全策略利用率进行分析，挖掘宽松与长期无用策略，实现对僵死策略（长期不命中）的清理，以及对 ANY 或大段宽松策略的逐步收敛和收紧，最终实现策略配置最小化。

◎域间策略基线与风险管理

通过建立和维护全网安全域间访问控制基线矩阵，实现访问控制策略的事前和事后合规检测，从而提前告警策略开通违规风险，定期输出域间违规策略报告，提升全行防火墙策略安全合规审计水平

◎安全基础架构可视化

实现防火墙、路由器、交换机设备安全策略信息的自动提取与解析管理，其中包括对数据安全产生影响的路由信息、访问控制、NAT 策略，并运用可视化技术，实现全网安全域基础架构的可视化展示。实现根据等保规范划分安全域，对安全拓扑中相关网络资产设备分组并使用能够标记安全域，能够自定义用户业务规则，实现用户对于安全管理的可视化，实现从安全视角的安全合规可视化分析。

◎安全路径可视化

结合业务流程、应用架构、数据架构等现状，实现在安全基础架构图层上查询与展示安全路径，能够基于源地址、目的地址、常用协议、端口等条件过滤的路径查询与展示，能够显示此路径上的网络与安全节点，能够实现对源到目的多条网络路径可视化，并能够列出影响此路径的相关策略，对网络路径风险处置提供依据。

◎访问控制策略应急封堵

支持指定防火墙和自动定位防火墙两种模式下发五元组封堵 / 解封安全策略，支持对防火墙、路由器、三层交换机下发 IPv4 和 IPv6 黑洞路由，从而实现针对恶意 IP 或域名的快速封堵，并支持与第三方平台对接。

◎策略自动开通

全面实现全网访问控制与安全策略运维管理自动化和可视化，包括开通业务请求服务化、模拟仿真分析、开通选路建议、策略风险分析、策略配置自动生成以及策略开通验证等功能，协助网络安全运维人员能快速、有效的完成策略变更，并确保变更内容准确，提升智能化运维水平。

技术指标

序号	功能模块	功能 / 规格描述
1	设备管理	支持对异构品牌型号的防火墙设备的安全策略进行中集中可视化展示、分析、管理与运维
2	配置管理	支持防火墙策略配置的备份，归一化解析，策略变更监控，策略配置对比等功能；
3	策略分析	支持对防火墙策略明细的可视化展示，查询分析等功能；

序号	功能模块	功能 / 规格描述
4	策略检查	支持对安全策略配置检查，发现各种隐藏策略、冗余策略、过期策略、可合并策略等问题策略，以及空对象、未被引用对象等问题对象；
5	策略合规	支持自定义合规规则，例如高危端口、宽松策略、跨区访问等，并定时进行策略合规检查，输出策略合规审计报告；
6	拓扑路径	包括逻辑拓扑展示，以及全网端到端路径查询分析等功能；
7	策略运维	全网访问控制与安全策略运维管理自动化和可视化，包括开通业务请求服务化、模拟仿真分析、开通选路建议、策略风险分析、策略配置自动生成以及策略开通验证等功能；
8	应急封堵	支持指定防火墙和自动定位防火墙两种模式下发五元组封堵 / 解封安全策略，支持对防火墙、路由器、三层交换机下发 IPv4 和 IPv6 黑洞路由，从而实现针对恶意 IP 或域名的快速封堵。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405231556

★有效期：2023 年 6 月 9 日至 2025 年 6 月 9 日

所属品牌：安博通

发布时间：2017 年

产品适用领域：金融、运营商、能源、政府、企业

产品照片：



产品咨询二维码

产品咨询邮箱：sunxiangming@abtnetworks.com

产品名称：安博通数据监测溯源与安全管理平台

产品概述

数据安全平台通过专利手段，系统性融合数据防泄漏技术、云应用代理安全技术、用户及实体行为分析技术、及大数据分析技术为一体，结合分布式边缘计算、集群式统一分析，创造性的实现了对网络中流动的数据资产实现了实时监控、预警、溯源的能力，实时发现网络中结构化、半结构化、非结构化数据，实现统一分类分级，对其流转路径进行监测、持续不断的对数据行为进行全面刻画，重构数据与用户、设备、业务系统、API 等内在关联关系，呈现敏感数据的关联安全态势，发现数据违规、数据泄露、数据滥用等风险行为，提供强大的数据溯源能力，为事件调查取证提供全面的证据链，快速界责。

功能特点

◎**数据安全态势**：平台通过丰富的数据采集能力，实时捕获网络中流动的结构化、非结构化、半结构化数据，实时监控、关联、呈现网络中流动数据资产的全貌，展示数据资产分布、重要数据、敏感数据分布及流转路径、敏感数据分级占比，数据分类分级、数据安全事件及处置状态以及近期或自定义时间段内各类敏感数据总量，呈现数据流转及其风险的宏观态势。

◎**数据资产分类分级**：支持数据分类，建立统一、准确、完善的数据治理基础。

◎**数据资产测绘**：对目标环境内数据资产载体进行探测发现、并对数据资产载体（如数据库）内部的敏感数据的类型、分布、数量进行识别鉴定，对数据载体如数据库内部的账号及权限情况进行梳理，形成静态数据资产目录。

◎**数据溯源**：回溯和审计任意时间段数据行为的能力，对任何流动数据的当前和历史状况进行追溯，还原数据流转的路径及流转的范围，数据使用的访问者、发生的时间、使用设备、IP 地址、访问行为、涉及的应用 /API 等详细信息，提供完整数据轨迹和证据链。

◎**数据合规检测**：从数据出境、跨域、脱敏审计、加密审计等方面提供监测能力。可以根据具体应用场景配置规则，通过定时的监测进程，实现对违规的发现并生成报告。包括个人信息出境合规、身份证跨区域脱敏合规、加密审计、重要数据跨安全域场景。

◎**数据事件告警**：通过实时捕获网络中各种流动的数据，基于规则的用户违规告警、基于行为分析的异常告警、来自数据源访问的安全事件、来自 API 风险的告警。

◎**资产可视化**：为用户构建宏观的自上而下整体数据资产视图，系统通过各种技术和特征码，支持自动抓取和识别网络中的各种应用，内置应用分类模版或用户自定义分类模版，将网络中的各种应用（互联网应用和内部应用）进行统一的分类，自动入库，并通过目录树结构呈现。

◎**结构数据审计**：实时监控业务系统和管理员对业务数据库的所有访问，根据多种安全策略判定访问操作的风险等级，并根据风险等级选择性的报警，从而实现完全独立于数据库的审计功能。

◎应用资产梳理：当业务访问流量接入后，系统须支持基于网络流量协议解析技术智能化识别接入流量中的应用资产信息，辅助用户整理应用资产清单，并根据用户需求将需要监测的应用系统配置纳入系统监测范围。

◎数据防泄漏：集边缘计算与大数据分析为一体的综合数据安全管理系统，实现数据安全风险感知、数据资产测绘、合规监测、数据溯源、数据泄露、聚类分析、违规告警、行为异常分析等功能。

技术指标

分析平台支持集群部署，支持分布式数据采集器部署。

平台支持多种数据采集能力，可无缝接入网络流量数据、API 及应用交互数据、数据库交互数据、终端交互数据以及静态数据源数据采集，可以按不同的地理位置、网段、业务目标进行数据采集。

“实现结构数据、非结构数据和半结构数据的统一数据分类分级管理、统一数据态势展示管理、统一数据深度分析、统一数据风险告警、统一数据安全设备监控管理

同一个分类分级策略，同时应用到不同数据源，不同结构的数据（文件、邮件、API），实现统一的分类结果”

平台以数据、人员、设备、应用进行深度关联分析，支持网络流量数据源、API 数据源、数据库数据源、邮件数据源、终端 agent 数据源的关联分析，实现对敏感数据的深度过程追踪与跨系统、跨人员交互溯源。

平台具有异构数据安全系统管理能力，支持审计类、脱敏类、加密类、数据访问控制类等多种数据安全系统的集中管理、策略管理、安全事件管理、业务日志管理。

平台数据采集与分析能力不低于 600 个业务应用、300 个数据库、30Gb 业务流量的全量融合数据分析。

数据分析能力：邮件（SMTP、POP3、IMAP、Webmail）、Web（HTTP）、Web（HTTPS）、MySQL、Oracle、TDS、FTP、SMB、NFS；加密应用（SMTP/SMTPS、POP3/POP3S、IMAP/IMAPS、Webmail）、Web（HTTP）、Web（HTTPS）、云盘；关系型数据库：Oracle、SQLserver、MySQL、DB2、Sybase、Informix、Postgresql、Gbase、Teradata、Cache、CacheWeb、tibero；国产关系型数据库：DM7、人大金仓（KingbaseES）、神通、浪潮 KDB、湖南上容、HighGo（瀚高）；非关系型数据库：MongoDB、Hive、HDFS 文件系统、Hana、HWMPP、Hbase、ES、Solr、Redis、SSDB、KingbaseAnalyticsDB。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230210

★有效期：2023 年 2 月 3 日至 2025 年 2 月 3 日

所属品牌：元溯

发布时间：2022 年 2 月

产品适用领域：产品适用广泛，适用于关键基础设施行业单位及有重要数据、敏感数据保护的多个行业如：采矿业、制造业、电力、热力、燃气及水生产和供应业、交通运输、仓储和邮政业、住宿和餐饮业、信息传输、软件和信息技术服务业、金融业、科学研究和技术服务业、水利、环境和公共设施管理业、教育、卫生和社会工作、公共管理、社会保障和社会组织

产品照片：



产品咨询邮箱：wangxiaosong@abtnetworks.com



产品咨询二维码

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家级专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区昆明湖南路 47 号国防教育基地二层

产品名称：工控集中安全管理系统

产品概述

工控集中安全管理系统是对工控网络中各种安全产品进行统一管理、配置、授权和监控的管控平台。通过对安全设备统一管理、安全策略统一配置、安全日志集中采集、业务安全综合分析、安全风险集中监测，从而消除工控网络安全信息孤岛，简化企业网络安全管理模式，降低企业安全运维成本，提高工控系统整体安全防御能力。

功能特点

◎安全设备统一管理

可集中管理全系列工控安全产品，支持对工控网络内所有安全设备进行设备信息维护、设备状态监测、安全策略配置、设备日志采集，实现网络安全状态可视、策略可管、威胁可控。

◎工控网络拓扑可视化

可主动或被动识别网络资产，支持自定义编辑网络节点和网络层级，实现工控网络拓扑可视化。

◎灵活多样的策略配置

可对各类安全设备的安全策略进行灵活配置，支持单点配置、批量应用、模板化管理，并

支持通过安全域划分进行差异化安全策略配置。系统可基于对工控网络安全状况的检测和评估结果，提供安全策略配置建议。

◎丰富的安全策略知识库

系统内置丰富的风险知识库和安全策略规则，可自定义配置各类安全事件指标的阈值、风险等级、关键字等条件，建立贴合企业安全管理要求的工控安全风险管理体系。

◎用户分权分域管理

系统支持自定义用户角色，可根据需要配置不同角色的功能使用权限，实现用户分权管理；系统支持安全域管理，可按照企业的组织架构划分不同的安全域，不同用户具备不同安全域内的安全设备访问权限，实现用户分域权限管理。

◎支持多级级联管理

支持多级级联配置，用户可以从中心平台对任意下级平台以及末端的安全设备进行集中配置，实现整体安全业务统一管理。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00481-A

★有效期：2023 年 12 月 29 日至 2025 年 12 月 29 日

所属品牌：珞安科技

发布时间：2017 年 11 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业。

产品照片：



产品咨询邮箱：liss@icssla.com



产品咨询二维码

北京天地和兴科技有限公司

北京天地和兴科技有限公司是国内专业从事工业网络安全的领军企业。公司总部位于北京，在全国 31 个省级行政区域设置了分公司或办事机构，用户覆盖电力、石油石化、轨道交通、智能制造、钢铁冶金和军工等多个国家关键信息基础设施行业。作为国家高新技术企业、国家级专精特新“小巨人”企业，天地和兴高度重视研发投入与核心能力建设，是国内首家获得 IEC62443 国际安全标准认证的工业网络安全企业，打造的“天堰”、“地盾”、“和睿”、“兴邦”四大产品系列，覆盖检测评估、防护隔离、审计分析、平台管理等全域工业网络安全需求，具备安全风险管控、渗透测试、攻防演练、安全培训、安全测评、应急响应等全方位的工业网络安全服务能力。

网址：<http://www.tdhx.com>

电话：010-56380988

地址：北京市海淀区西北旺东路 10 号院 7 号楼博彦科技大厦 C 座 6 层

产品名称：天地和兴安全管理平台

产品概述

天地和兴安全管理平台（等保一体机）HX-GPM 产品是天地和兴根据对当前信息安全等级保护建设要求的问题调研，及多年在对安全领域的研究与经验积累，结合公司全线安全产品资源，打造的专门针对当前现状的网络安全产品，旨在帮助用户解决网络安全问题，建设符合信息安全等级保护要求的信息安全网络。

功能特点

◎统一管理

在传统安全应用中，安全产品通常相互独立，大大增大了客户的运维成本。天地和兴安全管理平台可以实现安全产品的统一管理，统一引流，为客户提供统一管理平台。

◎统一分析

天地和兴安全管理平台提供统一的安全数据、日志的收集、存储、解析、分析的及展示的大数据平台模块。为客户从不同维度最大化的挖掘安全数据的价值。

◎等保合规

等级保护是我国推行最广的一套安全标准，天地和兴安全管理平台为客户提供云等保所需要的各种安全产品及安全服务，并为客户提供等级保护评估能力。

◎安全可视化

天地和兴安全管理平台能够全局观察整个云平台的安全态势，实现安全拓扑、业务风险、安全合规等可视化管理，让安全运维管理变得更加简单。

◎安全资源灵活分配

天地和兴安全管理平台为客户提供灵活的安全服务选择方式，用户可以通过简单的鼠标操作，灵活的为不同的保护对象提供不同的安全服务。

◎弹性扩容，提高资源利用率

- ★当安全虚拟机资源不够时可以动态添加 CPU、内存、硬盘、网卡。
- ★当服务器资源不够时可以动态的横向扩展。
- ★降低成本提供资源利用率。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心（公安部第三研究所）

★证书编号：24SS01688-A

★有效期：2024 年 11 月 15 日至 2026 年 11 月 15 日

所属品牌：天地和兴

发布时间：2020 年

产品适用领域：电力、新能源、石油石化、市政水务、轨交等关键信息基础设施行业

产品照片：



产品咨询邮箱：tdhx@tdhx.com



产品咨询二维码

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 6000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.winicssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特统一安全管理平台

产品概述

统一安全管理平台具备企业资产的集中管理、安全策略的集中管控、安全事件的集中分析，可解决企业资产和安全运营可视的难题。统一安全管理平台可管理的安全设备，包括但不限于：工业防火墙、工控安全监测与审计平台、工控主机卫士、工业互联防火墙、安全运维管理系统、入侵检测系统、日志审计与分析系统、安全隔离与信息交换系统等。

功能特点

◎便捷的策略统一管理

统一安全管理平台作为一种集中的安全管理形式，它能够将众多的安全设备集中管理起来，能够对安全设备的安全策略统一管理，包括：安全策略模板配置、安全策略统一下发、安全策略变更可视等。安全策略的统一管理极大地提升了企业安全运维的效率。

◎全面的安全数据采集

统一安全管理平台将工业网络中的区域边界、网络通信和计算环境作为安全对象，进行安全事件、系统日志和网络流量等安全数据的采集。系统拥有强大的日志范化引擎，可采集主机、

数据库、网络设备、安全设备、中间件等几百种类型的安全日志，并且支持用户自定义日志范化策略。

◎智能的事件关联分析

统一安全管理平台，拥有智能的事件关联分析引擎。事件关联分析引擎将多种类型的事件通过基于与或非的逻辑运算进行关联，将单个事件通过字段条件判断进行筛选，从而将安全专家的事件分析结果固化到规则引擎中，在事件接入后迅速分析出安全告警。

统一安全管理平台，拥有智能的攻击路径分析引擎，具备基于图形计算算法的关联分析能力。攻击路径分析引擎采用了图数据库，将设备 IP 作为图中的节点，将安全事件作为有向图中节点的连接关系，自动绘制攻击图；在查找经过某个节点的攻击路径时，基于安全事件的权重和时间的先后顺序，自动计算攻击路径。

◎强大的安全数据可视

统一安全管理平台，拥有强大的资产可视能力。系统可自动识别西门子、施耐德、罗克韦尔、ABB、霍尼韦尔、GE 等超过 500 种国内外主流自动化厂商的工控设备。

统一安全管理平台，拥有强大的漏洞可视能力。系统内置 3000 多个工控漏洞，覆盖 CVE、CNVD、CNNVD 等国内外主流漏洞库。系统具备工控漏洞自动发现的能力，并提供专业的漏洞描述和漏洞修补建议。

统一安全管理平台，拥有强大的流量可视能力。系统可自动识别 S7、MODBUS、IEC61850、OPC、DNP3 等超过 20 种工控协议，自动识别组态下装、CPU 停止等控制指令，自动识别基于工控协议的攻击行为。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231319

★有效期：2023 年 06 月 02 日至 2025 年 06 月 02 日

所属品牌：威努特

发布时间：2019 年 4 月 30 日

产品适用领域：电力、石油石化、轨道交通、钢铁、烟草、智能制造等

产品照片：



产品咨询二维码

产品咨询邮箱：support@winicssec.com

福建中信网安信息科技有限公司

福建中信网安信息科技有限公司以数据安全守护者为使命，致力于网络与数据安全领域，是一家集研发、生产、销售和服务于一体的高新技术企业。中信网安在国内首家提出基于时空网格技术的“云、网、端、数”多维度动态安全监管技术体系，公司依托领先的技术研发与创新能力，先后荣获国家级专精特新“小巨人”企业、国家高新技术企业、工业和信息化部 5G 应用安全创新推广中心、工业和信息化部重点实验室“商用密码应用工作组”及“大数据安全工作组”成员单位、国家知识产权优势企业、福建省级新型研发机构、福建省产业领军团队等多项荣誉，服务用户数量超过 2000 家，并在北京冬奥会、第四十四届世界遗产大会、世界航海装备大会、中国侨智发展大会、历届数字中国建设峰会等大型活动的安保实践中勇担重任，以专业的技术、可靠的服务成为客户心中最信赖的网络与数据安全领军企业。

网址: <https://www.cicisp.com/>

电话: 0591-87895020

地址: 福建省福州市晋安区鼓山镇福光路 318 号 2 号楼 8 层

产品名称：华安星安全管理平台

产品概述

华安星安全管理平台是一款聚焦于等级保护的合规产品。它基于通用硬件和虚拟化技术，实现安全能力快速部署和弹性扩展，协助用户快速满足等级合规要求。

华安星安全管理平台在安全防护方面采用“一个中心，三层防护”的设计思想，整合各种安全能力，并融入合规自查、持续监测等特色，帮助用户围绕等保技术体系的安全控制项进行快速合规检测、定位合规风险并持续性监控。在管理方面内置管理能力作为支撑，并从等保工作的定级、备案、建设整改、等级测评等全过程进行管理，规范等保建设流程，促进安全管理工作常态化。

功能特点

◎系统监控

通过统一管理界面对各个安全设备运行状态的监测，包括各安全设备的内存、Cpu、存储、健康度等进行监控。

◎系统管理

a、内置数据库安全审计或数据资产分析系统等数据安全产品，支持对其他安全设备进行添加、删除等操作；

b、身份鉴别：平台对各安全设备的管理采用静态口令鉴别机制进行远程管理，静态口令支持修改。

c、远程管理：平台支持对各安全设备进行重启、关闭、跳转登录等配置。

d、策略配置：支持对数据库安全审计或数据资产分析系统等数据安全产品的策略配置操作。

e、系统日志：平台支持记录平台登录成功、失败、修改密码等日志记录；同时支持对日志的导出、删除等操作。

◎安全审计

a、日志收集：支持对数据资产分析系统、数据库审计等日志进行收集。

b、事件审计：支持对数据库行为等各种日志进行统一审计，审计内容包括时间名称、事件类型、事件级别、发生时间、设备 ip、设备类型、来源 IP、目的 IP 等。

c、事件查询：支持时间范围、事件级别、设备类型、事件类型等组合条件查询。

◎安全管理

a、管理员身份鉴别：平台支持采用用户名和静态口令鉴别机制进行登录，并可进行设置密码口令的复杂难度和有效期进行定期提示变更密码。

b、鉴别失败处理：平台支持设置账号密码锁定策略，当账号密码口令失败次数符合锁定策略时，进行强制锁定该用户。

c、管理员分级：平台内置安全管理员、审计管理员、系统管理员三种等级账户。

技术指标

◎等保态势

平台帮助用户单位全面掌握信息系统综合安全运行状态，包括漏洞、安全工作运转状态、等保合规状态、指标自评趋势等。同时对以信息系统为中心的各类资产的安全进行监控与审计，帮助用户单位及时掌握网络安全风险状况。

◎统一管理

平台能对内置的各类安全能力进行统一的管理，包括对各安全能力的镜像进行配置、管理，并由统一管理平台进行调度。在日常应用方面，针对各类安全能力提供统一的入口、策略配置，并对各类日志进行集中审计、分析。

◎合规管理

对基本信息、定级、备案、自评、等级测评、监督检查等全过程进行管理，同时在技术层面与各类安全组件对接，实时进行合规性检测与评估。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS024-866

★有效期：2024 年 7 月 29 日至 2029 年 7 月 28 日

所属品牌：华安星

发布时间：2018 年 4 月

产品适用领域：医疗、政府、教育、电力

产品照片：



产品咨询二维码

产品咨询邮箱：zxwa@cicisp.com

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

作为行业领导者，安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

2020 年 11 月 23 日，安恒信息正式成为 2022 年杭州第 19 届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

网址：<https://www.dbappsecurity.com.cn/>

电话：0571-28860999

地址：杭州市滨江区联慧街 188 号安恒大厦

产品名称：安恒工业安全管理平台

产品概述

产品采用 8+3+5 的架构，以大数据分析为基础，以工业资产为核心，以安全生产为服务目标，实现工业资产集中管理、风险集中管控，依托大数据安全分析能力，通过采集工业环境各类数据，并将技术指标与安全生产指标相结合，提供可视化安全态势感知与安全技术分析能力，及时预判工业互联网环境的安全趋势，为应急响应提供决策分析支撑，构建工业互联网智能化网络安全运营管理体系。

◎工业安全引擎：负责采集各类工业互联网环境的安全数据，包括网络空间测绘数据、威胁检测数据、云安全监测数据、威胁情报数据、安全检测数据等，数据覆盖线上、线下采集，满足在工业云、工业互联网平台、工业网络等多种场景的数据采集。

◎数据中台：提供大数据安全服务能力：

◎安全数据中台：提供数据采集治理、威胁情报碰撞、大数据智能分析、工业威胁建模、UEBA 分析服务。

◎安全能力中台：将安全设备能力 API 化，为策略下发及自动化提供支撑服务。

◎安全业务中台：安全业务应用解耦，适应快速定制，灵活开发升级。

◎业务应用：以管资产、管设备、管人和管事的角度引入安全运营管理理念，通过资产中心、监测中心、安全分析、应急响应、联动防控、安全运营和安全可视化七大业务应用，建立

一体化工业安全运营管理体系。

功能特点

◎工业安全大数据分析

基于大数据分析技术和人工智能算法，将工业安全技术指标与安全生产指标进行进行分析挖掘，提供工业场景下的威胁建模能力，持续监测工业网络安全状态，提供精准的安全告警、趋势分析与预测能力，为工业网络安全决策提供支撑。

◎SOAR 自动化响应编排

在工业环境中，需要关注很多安全生产指标，通过将工业安全技术指标与安全生产指标做映射关系，再利用 SOAR 自动化响应编排技术，将管理、技术、人结合在一起，能够自动分析并处置大量重复的安全事件，将安全管理人员从日常枯燥的安全运维工作中解放出来，大幅提升安全运维效率。

◎开放的安全能力整合

高度兼容多种主流安全设备，采用专利技术提高协议解析的精准性，并提供丰富的第三方系统对接 API，将安全分析能力赋能给传统安全设备；可以高效整合用户现有网内安全能力，构建一体化的安全防护体系，最大限度减少重复建设的成本。

◎超大规模的存储与检索

解决大规模数据存储难题，满足客户长时间的日志存储需求，采用高效的压缩存储技术，节省大量存储资源；具备高效的查询能力，能够在秒级内从数万亿条规模的结构化和非结构化大数据中查询出用户所需数据，极大地提高工作效率。

◎稳定可靠的处理性能

采用多核处理技术、多线程应用系统，处理能力可达 10WEPS，节省用户成本；支持分布式部署模式和数据并行处理能力，兼顾未来系统扩大化建设的需求。

技术指标

◎预置工业威胁模型

结合 IT/OT 应用场景，内置 1300 多种安全分析模型，包括 180 多种扫描探查检测类模型、740 多种渗透攻击检测类模型、20 多种获取权限检测类模型、210 多种命令控制检测类模型和 30 多种资产破坏类检测模型，覆盖 Intrusion Kill Chain 的各个维度。

◎自定义工业安全分析模型

支持根据网络实际环境自定义规则模型、统计模型、情报模型、关联模型和 AI 模型等安全分析场景。

◎威胁情报碰撞

平台具备情报收集（内部 + 外部各类情报源）、多源情报关联分析、情报检索验证与攻击溯源、情报更新维护、关联下游产品。

◎工业控制场景实体行为分析

对实识设备、工业通信指令进行智能 AI 学习或进行基线设置，构建出用户在不同场景中的基线状态。及时发现用户、系统和设备存在的可疑行为。

◎工业资产画像分析

通过安全建模分析，提供可视化工业资产画像，主要包括：资产基本信息、风险信息、访问关系、行为画像、服务端口、访问端口、脆弱性等。

◎溯源分析

结合大数据关联技术能够实现对安全告警事件和攻击者的追踪与取证，并提供溯源报表的一键智能下载。

◎调查取证分析

通过搜索、聚合、关联等调查取证手段，提供攻击事件数据包、攻击者设备指纹等举证信息。支持基于源、目的、事件名、攻击意图等多种聚合调查方式。可以关联资产信息、威胁情报、弱点详情、安全事件、处置方式等多维数据进行调查取证。

◎可视化安全态势感知

提供场景化安全态势感知，支持组态化管理，支持通过自定义的方式对大屏进行编辑，可以通过调用平台的分析指标，或通过 Rest API，SQL 等方式直接调用第三方数据源作为大屏展示的数据源。可视化组件超过 80 种，满足自定义态势感知大屏的需求。

◎资产管理

提供全面的资产能力图谱，涵盖组织、网络、系统、IP、设备、应用等不同类型的资产，同时支持多协议、多场景的工业资产属性管理，支持将资产与安全监测进行关联展示，支持流量自发现和人工录入等方式丰富资产图谱，支持将资产通过自定义方式进行网络拓扑关联。

◎通报预警

当监测到风险隐患或安全事件时，通过平台进行通报预警，并根踪反馈。平台具备多种通报方式，包括钉钉、微信小程序、短信、电话和邮件等。

支持工单处置、支持从数据接入到策略执行的 SOAR 自动化响应全流程拖拽式交互编排，实现安全事件的告警聚合、关联验证和联动阻断。支持策略下发并生成跟踪任务，任务执行过程中可加入人工核验环节进行控制。

◎集中管控

设备集中管控包括对工业安全审计、工业防火墙、工业网闸、工业安全主机等探针进行策略管控，支持策略下发、任务创建、对象管理等，创建策略任务后联动的探针设备能够即刻生效。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231231

★有效期：2023 年 05 月 26 日至 2025 年 05 月 26 日

所属品牌：安恒

发布时间：2017 年

产品适用领域：电力、水利、智能制造、石油化工等

产品照片：



产品咨询邮箱：walker.bai@dbappsecurity.com.cn

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：网络安全风险管控平台

产品概述

迪普科技网络安全风险管控平台是一款帮助用户实现资产测绘、漏洞感知及运营管理的产物。平台以安全大数据分析技术为基础，通过主动探测机制，依托可视化技术实现网络安全风险的预警及信息通报，落实网络安全监管主体责任，实现网络安全管理闭环。

功能特点

迪普科技网络安全风险管控平台是一款帮助用户实现资产测绘、漏洞感知及运营管理的产物。平台以安全大数据分析技术为基础，通过主动探测机制，依托可视化技术实现网络安全风险的预警及信息通报，落实网络安全监管主体责任，实现网络安全管理闭环。

针对资产与漏洞的管理与维护工作中存在的难点和痛点，风险管控平台产品应具备以下要素：

◎原始数据采集的检测装置：采集资产信息完成资产测绘，扫描漏洞等脆弱性信息完成；

◎对检测装置进行集中管理的控制模块：实现对检测装置的运行状况监控、功能的远程升级、扫描策略配置、检测任务下发等；

◎大数据系统：历史、实时数据的交互、存储、处理，多维度数据支撑，原始数据的分析、呈现；

◎基于应用场景实现业务的功能模块：包括安全预警、结果分析、流程跟踪、整改修复、加固策略等。

平台由资产管理、漏洞管理、检测管理、情报管理、安全通报、风险处置、对比分析等业务模块组成。形成安全风险监测、安全运营管理两大体系。实现三个核心管理目标：动态资产核查及异常监控、多维资产脆弱性风险评估、全流程安全风险闭环管理。

技术指标

网络安全风险管控方案主要包括慧眼安全检测平台及安全风险管控平台。部署慧眼安全检测平台，通过主动探测机制结合自身的海量资产指纹库精准识别各类资产，包括信创资产、各类业务系统、物联网终端、行业特有装置等；基于零信任安全理念，借助实时采集技术监控资产上下线状态，确保只有可信资产接入网络。针对各类资产，进一步结合完全自主可控的漏洞发现引擎识别各类信创资产漏洞、系统漏洞、中间件漏洞、数据库漏洞、Web 漏洞及云平台漏洞等，并采用模拟人工渗透的方式对漏洞进行自动化验证。慧眼安全检测平台采集的数据，实时同步到安全风险管控平台。安全风险管控平台具备完善的网络风险运营管理体系，以宏观视角全局监测网络空间各类资产及风险态势，资产风险信息关联到具体组织机构及责任人，实现可疑资产通报、漏洞整改通报、行业违规通报、高危预警、远程安全加固等，落实网络安全监管主体责任。除此之外通过在安全风险管控平台结合“技术+人员+管理”的体系，对资产风险进行统一排查，提高排查效率和风险排查准确性。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230025

★有效期：2023 年 01 月 13 日至 2025 年 01 月 13 日

所属品牌：杭州迪普科技股份有限公司

发布时间：2020 年 6 月 18 日

产品适用领域：全行业

产品照片：



迪普订阅号



迪普服务号

产品咨询邮箱：wuguangbo@dpotech.com

杭州美创科技股份有限公司

杭州美创科技股份有限公司（简称：美创科技）成立于 2005 年，中国专业数据安全头部企业，拥有数据安全、运行安全、数据流动、安全运维服务四大业务，累计服务客户数超 16000 家。

深耕数据安全近 20 年，美创数据安全管理平台、数据安全分类分级、数据库审计、数据脱敏、容灾备份等产品持续保持市场领先。基于数字化时代安全诉求，美创创新提出韧性安全框架，研发推出适应多云环境，具备数字化、弹性、云化、自适应进化、可观测为特点的新一代数据安全管理平台、新一代灾备一体化平台和数据流动平台。

作为数据安全中坚力量，美创已参与 30 余项国家行业标准制定，深入推进产学研合作，布局信创、关基保护领域，不断以更全面创新的产品方案与服务，护航数字经济发展。

网址：<http://www.mchz.com.cn/>

电话：400-811-3777

地址：浙江省杭州市余杭区五常街道中福未来星辰金座 4 幢 3 层 301 室

产品名称：美创数据安全管理平台

产品概述

美创数据安全管理平台突破传统数据安全理念，引用韧性数据安全体系，将各数据安全防护、数据安全治理、数据安全运营等安全能力，通过一套技术架构收敛至一个平台、一个入口，同时，其天然具备的横向扩容、纵向订阅以及多租户 / 数据隔离能力，有效应对当前多云 / 混合云场景下，复杂的数据资产安全管理、数据流动安全管控、数据安全风险监测等数据安全需求。

功能特点

- ★全域数据资产治理
- ★风险实时智能监测
- ★安全风险告警与处置
- ★全域事件追踪溯源
- ★丰富多样的分析报表
- ★来访身份动态治理
- ★合规评估引导安全建设
- ★安全风险防护管控
- ★安全态势可观测

技术指标

◎多云、海量资产全面纳管

突破传统静态管理模式，数据安全治理平台的云端技术架构天然具备应对多元混合生长和

海量数据增长之后的安全资产管理问题。

◎海量资产自适应防护

安全策略 AI、端云闭环、动态防护等能力，可快速应对海量数据增长和流动使用场景爆炸之后的闭环安全防护。

◎数据安全保障能力全面融合

通过一个平台，全面融合数据安全治理、数据安全能力、数据安全可视化，实现数据安全可持续运营。

◎安全防护标准全面统一

统一分类分级防护、统一身份管理、统一安全策略配置入口和分发、统一事件处置，确保多云环境遵循相同的数据安全标准。

◎弹性、灵活的防护机制

集群、云端架构、集中纳管、存算分离等机制，可应对海量数据增长和流动加速带来的散乱未知的安全风险监测和防护。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231095

★有效期：2023 年 5 月 12 日至 2025 年 5 月 12 日

所属品牌：杭州美创科技股份有限公司

发布时间：2021 年 11 月

产品适用领域：全行业

产品照片：



产品咨询二维码

产品咨询邮箱：marketing@mchz.com.cn

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等 70 余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

产品名称：绿盟威胁和漏洞安全管理平台

产品概述

绿盟威胁和漏洞安全管理平台结合企业漏洞管理现状，引入漏洞威胁情报，激活传统企业漏洞等工具，为企业客户提供基于以威胁为中心的风险自适应管理解决方案，帮助客户整合多源脆弱性数据，聚焦关键风险，可视化和量化分析风险管理指标，建立快速漏洞预警响应机制，提供漏洞管理的过程支撑，及时有效建立和完善漏洞管理补偿体系。

功能特点

◎基于威胁的漏洞管理

利用外部漏洞威胁情报定位关键风险点，重新定义漏洞处置优先级，优先处理被攻击者或恶意软件利用的漏洞。

◎基于情报的应急响应

实时跟踪热点漏洞，对需要紧急处理的漏洞快速定位到影响资产，向运维人员发出漏洞预

警快速进入内部漏洞管理流程，形成完善的基于情报的漏洞应急响应。

◎全网资产持续监控

对全网所属资产进行全面普查，确定系统内合法存在的资产，建立资产基线，通过持续监控及时发现资产新增、减少、变化情况，及时通报安全责任人，协助制度的有效执行。

◎漏洞运维全过程管控

为漏洞运维提供漏洞预警、漏洞扫描、漏洞处置、资产稽查、优先级分析等能力支持，对管理过程跟踪度量，协助流程优化。

技术指标

◎专业的云端情报支撑

依托绿盟威胁情报中心（NTI）多年的威胁情报运营，第一时间跟踪到紧急漏洞的爆发，快速预警处置。

◎创新的漏洞处置优先级算法

基于威胁的多维度（热度、POC、恶意软件），基于业务的多维度（重要性、级别、是否防护）结合领先的算法重新定义漏洞处置优先级。

◎多源漏洞融合

支持各类异构厂商的扫描结果漏洞、渗透测试漏洞、外部通报、漏洞情报等多个维度的漏洞统一接入、融合分析、集中处置。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231877

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：绿盟科技

发布时间：2016 年

产品适用领域：政府、企业、交通、运营商、医疗、高校、能源等
全行业适用

产品照片：



产品咨询二维码

南京众智维信息科技有限公司

南京众智维信息科技有限公司于 2015 年 2 月成立于南京，是以国内知名的麒麟安全实验室（原 OPENX 实验室）为基础建立的网络安全软件研发创新型企业。公司坚持“众智创新重塑安全生态、AI 运营赋能网信安全”，是新一代人工智能 + 机器学习驱动的网络安全攻防运营（AISecOps）解决方案商。两年内相继获得南京市政府、国资背景、市场化基金过亿元融资。

公司立足对安全厂商产品生态体系的持续投入，目前已实现 500+ 国内外厂商（APP）的对接，近 1500 款安全动作集成并平滑联调。与 200+ 高质量客户达成合作与签约，覆盖金融、政务、运营商、能源、军工等行业龙头客户。目前众智维科技与南京市大数据集团合资成立了国有平台南京大数据安全技术有限公司，持续聚焦数据安全运营领域的创新探索。

公司拥有 20+ 核心专利，40 余项软件著作权。公司拥有国家高新技术企业、国家信息安全漏洞共享平台 CNVD 支撑组单位、国家信息安全漏洞库 CNNVD 技术支撑单位、国家工业信息安全监测应急支撑单位、国家 242 信息安全专项合作单位、CNCERT 网络安全应急服务支撑单位（省级）、江苏省“数动未来”融合创新中心、江苏省网络安全技术支撑机构、江苏省通信管理局网络和数据安全技术支撑单位、山东省网络安全应急服务支撑单位等资质荣誉。

网址：www.openxorg.com

电话：400-0133-123

地址：江苏省南京市江宁区徽商大厦 B-1 栋 601

产品名称：红鲸 RedOps 安全协同响应平台

产品概述

RedOps 红鲸安全协同响应平台（以下简称“RedOps 红鲸平台”），以自主研发的安全自动化编排技术为核心，基于国内最大的安全运营自动化协同响应知识库，通过 AI+ 自动化协同安全响应平台 + 实战对抗网格的创新模式，通过安全运营辅助决策全面提升企业的网络安全运营自动化水平。系统采用分布式架构部署，拥有很强的告警综合管理分析能力，并通过图计算决策协同 + 安全编排自动化及响应能力，实现企业网络安全运营自动、剧本开箱即用、安全生态集成的体系化能力。

RedOps 红鲸平台，基于 NLP 和语义分析的知识图谱关键技术，内置协同作战室、AI 机器人进行智能匹配和推荐。针对应急事件能够快速获取与该事件相关的部门、人员和处置步骤，用作战室的方式进行协同应急工作，实现高效率、低成本的响应处置。平台提供智能化特征识别，快速精准匹配合理的 SOAR 剧本，形成完整的应急响应知识库，将企业宝贵的安全运营人员从低技术劳动中彻底解放出来，提升人、机器、设备高效协作与自动化安全运维。

功能特点

◎**自动化编排攻防处置策略**：通过落地 SOAR 安全编排自动化技术，将原本需要多人多设备协同参与处置的安全事件，按照预定义的安全剧本（事件处置流程）进行应急响应，将重复的、常规的、确定的部分交给机器完成，将新的、复杂的、不确定的交给人工研判处置。分解运营流程中的任务，抽象成不同类型和粒度的自动或手动触发的剧本，从而全面加速操作过程，减少人工等待，提升安全响应的速度和效率。

◎**AI 安全运营协同作战室**：采用网络安全作战室语义算法技术，构建专家系统对话机器人（AI），提高结果的准确性，调度剧本引擎实现对网络安全事件触发，当后续类似攻击发生时，实现精准推送，充分利用自动化技术手段，将人、技术和流程高度协同。同时，系统支持基于安全事件的特点和行业已有的成熟解决剧本方案，使用协同过滤算法，在行业级的知识库中进行事件关联度特征匹配，实现另一个维度的协同工作。当安全事件触发后，网络安全作战室依据安全日志等进行数据分析，生成分析报告，作战室的相关人员，如总指挥、作战参谋和事件处置人员等做出指令决策。根据这些信息，将数据进行标准化处理，为 NLP 模型读取数据打好基础。相关数据读入推荐算法模型后，参考网络安全事件的知识库，推荐出一个或多个可施行的剧本来完成相应的工作流程。

◎**“挂图作战”降低全局风险**：依托“挂图作战”战术思想，完整地把安全事件响应的全流程信息和操作关联起来，无论是分析研判所涉及的多源关联日志，还是多人协作过程中产生的阶段信息，以及可用的人力/工具/剧本都能在“全局作战图”上实现可关联、可观测、可操作，平台采用“行为力导图”“攻击路径图”“对抗指导图”等图形化方式作为核心策略。

◎**安全集成生态架构开放化**：适配兼容各类安全系统及工具，通过专用的 API 接口和其他通讯方式扩展指标级的采集功能，借助系统内置的安全应用超市功能，可以将所有与外部安全设施和运营相关的各种系统和功能映射为内部可识别的 APP 应用，每个应用都是特定安全能力的服务化封装，实现了对内外部应用及其动作和实例的统一化管理。系统内置基本的应用，包括主流的主机设备、安全设备、协同软件，以及云端应用（如威胁情报），也包括通用的 Syslog、REST 等应用，内置 150+ 种应用，包含 400+ 动作。

◎**智能化大屏赋能安全运维**：自动化运营大屏通过大规模的数据处理性能、灵活的视图展示、智能监控的能力，可以对采集到的指标进行视图/报表展示，提高监控的及时性、准确性、智能化，支持以短信、邮件等多种方式进行告警通知，为在线业务保驾护航。

◎**多维度入侵感知**：对攻击路径每个节点深入监控，提供了多平台、多系统的全方位、高实时的攻击监控，做到全方位实时监控；同时，提供包括自动封禁、手动隔离、黑/白名单和自定义处理任务等多种响应能力，让响应高效化。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230190

★有效期：2023 年 2 月 3 日至 2025 年 2 月 3 日

所属品牌：众智维科技

发布时间：2021 年 3 月

产品适用领域：金融、政府、能源、工业等

产品照片：



产品咨询二维码

产品咨询邮箱：market@openxorg.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟（CCIA）发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神 API 安全分析与管理系统

产品概述

奇安信网神 API 安全分析与管理系统与 API 安全检测系统、API 安全防护系统两个产品一起组成的 API 安全防护方案，可通过分布式部署，实现 API 资产识别、API 漏洞的攻击检测与防护、API 数据泄露检测以及 API 管控等 API 安全防护措施，以解决现有安全产品无法应对的 API 安全问题、敏感数据泄露无感知问题。

功能特点

◎ API 资产管理

通过自动标记公共组件 API，并支持用户手动标注 API 的应用属性和所属应用系统。系统还支持手动导入已有 API，并允许用户逐项添加特定 API 已识别标注和未打标签的 API 会以图形化列表方式展示，包括 API 所属主机、路径、业务应用以及发现时间和最近活跃时间。此外，该系统与代码卫士联动，实现源代码侧静态 API 与流量侧动态 API 的全状态监测，有效发现活

跃、失活、僵尸和下线的 API，从而缩小 API 暴露面。

◎异常行为分析

内置高频访问、非工作时间访问、敏感数据过度下载等 20 余个异常行为检测模型，通过对 API 安全检测系统上送的业务访问日志以及涉敏日志进行关联分析，发现异常高频访问、文件批量下载、敏感数据批量爬取、以及接口参数遍历等 API 异常访问行为，发现潜在的 API 安全风险，将风险前置。同时可根据业务情况的不同自定义异常行为分析引擎，自定义维度包括但不限于学习时长、学习窗口、阈值以及敏感数据类型等，配置完成后自动更新到对应的模型中，做到动态更新 API 异常行为分析模型，减少低价值的告警、提高异常行为告警可信度、准确度。

◎敏感数据传输分析

通过集中存储和大数据分析的优势，跨长时间维度分析对其传输内容进行分析来达到“谁通过什么方式的 API，传输了什么类型的敏感数据，传输了多少”的效果，实现敏感信息的数据传输分析。

◎威胁事件分析

通过大数据分析组件的关联分析能力还原基于 API 的供给链过程，清晰展示“什么人（攻击者）通过哪个接口，什么攻击方式手法，攻击了谁（受害者），攻击结果是什么”的效果，极大缩小运营人员的分析效率。

◎风险 API 分析

基于 API 的脆弱性关联 API 的异常访问行为、API 的敏感数据传输、API 的威胁事件分析等维度进行多维关联分析，使风险 API 具象化，为运营人员对风险 API 的处置提供依据。

技术指标

本系统的设计将遵循以下原则：

◎可靠性原则

产品服务端软件自身具备较高的安全性和可靠性。在总体架构上支持数据分布式存储及计算架构，可以总体上提升系统的组件和接口冗余度，保证在个别单元异常的情况下系统仍旧能够正常运行。

◎开放性原则

满足国际和国内的相关标准，采用通用技术，遵守国家相关信息化和安全规定。

◎先进性原则

系统建设充分考虑采用先进而成熟的技术、先进的体系结构，既保证实用成熟，又能够适应未来的业务发展和技术的更新要求。

采用自然语言处理、大数据关联、机器学习等技术，保证了奇安信网神 API 安全分析与管理系统更好的实现 API 安全风险管理的功能。

◎安全性原则

系统间的通讯采用加密机制，保证网络通讯的安全。

◎适应性原则

支持系统和策略的灵活配置，以便适应各种业务场景，方便管理、使用和维护。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231084

★有效期：2023 年 5 月 5 日至 2025 年 5 月 5 日

所属品牌：奇安信网神

发布时间：2021 年 4 月

产品适用领域：银行、电力、证券、保险、央企、教育以及医疗等行业。

产品照片：



产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

集团总部位于北京市中关村软件园启明星辰大厦，DT（数据时代）总部位于杭州高新区（滨江），全国云安全总部位于苏州高新区，在全国各省、市、自治区设立了分支机构，拥有覆盖全国的渠道和服务体系，为用户提供网络安全产品、服务和解决方案。

网址：<https://www.venustech.com.cn/>

电话：400-624-3900

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：安全管理平台

产品概述

安全管理平台系统是一套面向客户业务信息系统的，以 IT 资产为基础，以业务为核心保障目标，融合业界流行的大数据技术，针对高速信息进行采集，融合多源异构数据，结合 SQL、NewSQL 和 NoSQL 技术，实现异构海量安全数据的高效可靠存储，并以安全数据为驱动，提供智能化关联分析技术和基于机器学习的行为分析技术，流安全分析技术和态势感知。系统内建主动安全管理机制，通过主动的漏洞扫描和安全配置核查，及时发现业务信息系统中存在的隐患和风险，并进行事前预警；结合内外部情报协作，提供更加准确和及时的安全分析；融合多种信息安全技术和管理理念，充分实现组织、过程和技术三个体系的合理调配，帮助用户从监控、审计、风险、运维四个维度实现对业务信息系统的统一安全保障。

功能特点

系统采用新一代基于 Clickhouse 列式存储技术架构和自主知识产权的非关系型数据库 (NoSQL/NewSQL) 技术——CupidDB，具有全文索引、水平弹性扩展、实时格式化数据搜索和

原始数据关键字全文搜索、智能、机器学习、集成威胁情报和高可靠性等特点，同时还提供一套可视化的数据分析工具，借助于可视化人机界面，安全分析师可灵活调整分析过程，发现数据价值。系统采用开放平台架构设计，遵循业界通行的应用接口和管理接口，功能部件都实现了模块化装配，客户可以自由选择，并能够与客户的应用和管理环境实现良好的对接与整合

系统采用开放平台架构设计，遵循业界通行的应用接口和管理接口，功能部件都实现了模块化装配，客户可以自由选择，并能够与客户的应用和管理环境实现良好的对接与整合。

技术指标

管理中心在单 Intel 酷睿 4 核 CPU，16GB 内存，64 位操作系统，内置数据库下，采用单一部署模式时，事件处理性能可达平均 46000EPS。

日志采集器在双 Intel 至强 4 核 CPU，8GB 内存，64 位操作系统下，事件处理性能可达平均 6000EPS。

事件存储量仅取决于系统可用存储空间大小。

日志采集器对于所在主机和服务器的 CPU 利用率占用值小于 2%。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405230276

★有效期：2023 年 02 月 10 日至 2025 年 02 月 10 日

所属品牌：启明星辰、网御星云

发布时间：2015 年 6 月

产品适用领域：系统具有国内最广泛的应用范围和客户群，在政府、能源、电信、军队、军工、公检法司、企业、交通、媒体、金融、烟草、卫生医疗、教育、党务等多行业均有成功的应用，已经连续 11 年位居国内市场销量第一。

产品照片：

产品咨询邮箱：

support@venustech.com.cn



产品咨询二维码

产品名称：工控安全管理平台

产品概述

工控安全管理平台是一套以场景化为基础，以满足实战化为目的，以威胁为驱动手段，帮助用户建立监测预警、态势评估、响应处置的安全运营平台，定位为可支撑用户“攻防实战，协同指挥，智慧运营”的平台，在传统的“监测，审计，运维，管理”维度上强化“威胁可视、智能响应”，提供集成的预测、阻止、检测和响应能力。

功能特点

平台能力升级大幅提升平台数据采集与处理能力，业务能力升级全面匹配攻防实战的使用场景，智能驱动安全运营。

平台能力升级：采用统一的 THDK 开发框架进行开发，融合业界主流的大数据技术，采用 THBD 数据库，结合 SQL、NewSQL 和 NoSQL 技术，实现对多元、异构、海量安全数据的高效采集检索、可靠存储和负责计算。通过构建 THStore 体系，减少模块的耦合，形成高内聚，低耦合的货架式功能 APP，从底层技术架构层面解决海量资产，数据分权分域，以及高性能日志处理问题。

技术指标

业务能力升级：提供智能化关联分析、自动化或半自动化编排技术、基于机器学习的行为分析，流安全分析技术，内建主动安全管理机制，通过主动的漏洞扫描和安全配置核查，及时发现业务系统隐患，并进行事前预警；结合内外部情报，提供更加准确和及时的安全分析。同时引入攻击链模型和 ATT&CK 模型分析从侦查、渗透、攻陷、控制、破坏一整套攻击流程进行事中监测，威胁定位；利用流量日志融合，提供更多攻击上下文信息，在调查和攻击溯源方面进行事后取证，案例总结。同时提供宏观视角，中观视角，微观视角为不同角色的用户提供直观的、多维度的可视化呈现。帮助用户掌控实时安全态势，动态感知隐患与威胁，为安全分析师和决策层提供强有力的支撑

网络安全专用产品安全认证或安全检测结果证明

(1) 网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00192-A

★有效期：2024 年 2 月 8 日至 2025 年 5 月 5 日

(2) 网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00195-A

★有效期：2024 年 2 月 8 日至 2025 年 5 月 5 日

所属品牌：启明星辰、网御星云

发布时间：2015 年 6 月

产品适用领域：系统具有国内最广泛的应用范围和客户群，在政府、能源、电信、军队、军工、公检法司、企业、交通、媒体、金融、烟草、卫生医疗、教育、党务等多行业均有成功的应用。

产品照片：



产品咨询二维码

产品咨询邮箱：

support@venustech.com.cn



产品名称：天榕数据安全平台

产品概述

数据安全平台（DSMP）数据安全治理管控系统（DSMP）是“以数据和身份为中心，元数据驱动，基于场景化的思路”进行设计，在对数据资产自动发现并分级分类的基础上，根据不同场景的安全需求和安全风险，统一制定安全策略并调配底层能力组件，实现数据全生命周期管理。

数据安全平台（DSMP）是数据安全保障的作战指挥系统，在整个数据安全治理体系中处于核心的枢纽地位：向上承接各类制度规范的拆分和解读，使之成为具体可落地、可执行的安全策略；向下基于统一的、全局的安全策略驱动和调度各种能力组件（数据安全产品）执行各种安全策略。数据安全平台（DSMP）同时提供对安全运营服务的支撑，使得制度、规范、流程、风险评估、安全能力、安全策略形成闭环，从而为数据安全构建起一套综合的防护体系。

功能特点

◎安全策略统一管理

以分类分级结果为基础，以数据为中心来制定安全策略，通过安全策略下发形成数据安全平台与各能力组件的策略协同联动，实现数据资产的可视、可控、可管。安全策略包括敏感数据发现策略、脱敏策略、加密策略、水印策略、访问控制策略、传输策略等。

◎全生命周期管理

依托场景化的解决思路，从数据采集、数据传输、数据存储、数据处理、数据共享、数据销毁等阶段对数据资产进行全生命周期管理，对各个阶段的数据、事件、防护、合规进行全方位监测和管理，可以根据实际业务场景需求，自由定制全生命周期管控能力。

◎数据资产自动发现和识别

通过自动发现、手动配置和外部导入方式发现数据源，对不同存储位置、不同数据类型的数据源进行统一管理。同时基于分词、基于 NER、机器学习等核心技术，提供全网敏感数据进行自动扫描发现能力，自动识别出核心重要数据。

◎数据分类分级

精准识别资产设备和资产类型，自动识别敏感数据，根据客户相关行业规范对数据资产分级分类，实现敏感数据的可发现、可展示、可稽核，全面掌控数据核心资产。

◎数据脱敏

内置差分隐私、数据遮蔽、固定值映射、随机脱敏、加密算法、乱序脱敏等丰富的数据脱敏算法，能够对各类数据库和文件服务器数据脱敏处理，全自动化将字段类型进行映射和转换。

◎水印溯源

支持对数据库和结构化文件添加数据水印，支持从一种数据到另外一种数据的异构方式对数据进行添加数据水印信息。数据水印过程自动化，可根据不同数据库、文件打不同的水印信息，方便后续数据溯源，精准定位。

◎数据流转监测

以数据视角和用户视角展示业务过程的数据实时流转情况，将敏感数据和用户、应用、API、数据库进行关联，并展现流转过程中形成的风险事件。

◎数据风险监测

数据风险监测主要围绕数据安全的风险分析，通过行为画像、高频访问、越权访问、高风险指令、敏感数据外发、异常访问、暴力破解等审计分析模型完成数据流转、数据异常行为的已知威胁和未知威胁，并形成事件进行告警。

◎DSMM 能力合规评估

数据安全平台基于以数据为中心的管理思路，从组织机构业务范围内的数据生命周期（采集、存储、传输、处理、交换、销毁）的角度出发，提出对组织机构的数据安全能力成熟度的分级评估方法，衡量组织机构的数据安全能力，促进组织机构了解并提升自身的数据安全水平。

技术指标

分类分级规范管理：内置运营商、金融、证券等行业 20+ 个数据分类分级规范。支持同时启用多套分类分级规范，并设置默认分类分级规范，支持文件类型数据自动生成文件摘要，并提取文件关键字，辅助人工复核分类分级结果；

数据类型和识别规则管理：系统内置 300+ 数据识别规则，60+ 数据字典；

数据采集监管：支持数据库采集、API 采集、文件采集、应用系统采集四种采集方式的管理，支持图形化方式以时间、数据分级、采集方式等维度进行统计分析，并支持数据采集阶段能力组件、安全策略统计分析；

数据生命周期监管：支持自定义数据全生命周期采集、传输、存储、共享、使用、销毁阶段的应用场景，同时开启全生命周期各阶段安全监测等功能；

运营工作台：支持将风险事件、风险评估、合规检查、分类分级复核等工作指派给其他管理员处置，也支持管理员进行人工处置和工单处置；

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00751-A

★有效期：2024 年 05 月 31 日至 2026 年 05 月 31 日

所属品牌：启明星辰

发布时间：2021 年

产品适用领域：运营商、政府、电力、金融、交通、政法、卫生医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

产品名称：云安全管理平台

产品概述

云安全管理平台由安全资源池和安全能力中台以及安全应用层组成，其中安全资源池通过底层虚拟化技术将安全组件进行软件化，并以池化方式将各类安全组件进行集中化管控，通过网络调度技术实现对安全组件的服务编排能力，从而实现软件定义安全。

◎安全应用层：安全应用层作为安全运营人员和租户人员的统一管理入口，可为客户提供安全运营门户和租户安全门户。基于系统下层安全要素的采集和分析，负责向运营方和租户方呈现态势感知能力，根据安全防护和宏观监测的重要维度，包含总体安全态势、租户安全态势、资产态势、攻击态势等，使用户能够感知和把握网络安全整体态势。

◎安全能力中台：安全能力中台是云安全管理平台的底座，提供大数据平台、安全数据能力中台和安全业务能力中台，为上层安全应用层提供技术和引擎支撑。平台采用微服务架构，功能模块可弹性扩展，各模块之间互相隔离、互不影响，各模块之间的重启、重载不影响主进程的活动。

◎安全资源池：安全资源池底层基于虚拟化技术将物理服务器整合形成逻辑集群池，从而提供安全能力集成、安全能力编排、安全路径隔离、安全能力执行等功能，来满足业务系统的安全需求。

功能特点

◎统一安全门户：为满足政务云、行业云、安全运营等场景，满足等保合规要求，实现平台数据与业务数据的隔离，系统管理员无法查看业务数据和租户数据，仅监控、检测与平台相关的运行状态、资源占比、事件告警、安全风险、订单详情等内容；租户管理员通过门户页面查看本租户相关的安全告警、安全趋势、资源占比、授权状态、日志信息等内容。

◎多云安全管理：通过多云对接、多安全资源池统一管理和分级管理能力，实现多云平台安全能力资源化、安全资源服务化，云安全管理平台对接各类云平台，为多云平台场景打造整体的综合性云安全解决方案。

◎安全流量编排：业务系统以安全域为单位，在不同安全域之间进行业务访问的过程中，需根据安全防护要求配置不同的安全防护措施。

云安全管理平台支持流量编排功能，能够以安全域为对象下发安全服务链，在安全服务链中设置安全节点的数量，分配每个安全节点的安全类型，设置服务链的主备模式，设置服务链的监控模式以及安全节点的监控模式。

◎云安全运营：云安全管理平台通过融合态势感知与 SOAR（安全编排自动化与响应），提供面向多租户云环境的态势感知能力和安全编排自动化与响应能力；其中态势感知呈现包含总体安全态势、租户安全态势、资产态势、攻击态势等；SOAR 提供了灵活的安全编排能力，实现自动化、半自动化的事件分析和分类过程，通过定义的工作流确定优先级并进一步推动安全

人员快速处置，提升整体响应处置效率，为用户构建宏观监控、急速响应的安全运营中心。

◎日志集中管理：云安全管理平台支持对日志进行统一管理，通过收集虚拟安全产品的所有安全事件信息，对安全日志进行统一展示、统一归并、统一外发、统一归档。系统管理员可以集中配置日志策略，对日志类型、事件类型、时间周期进行设置，仅展示管理员关注的日志信息、展示特定时间段内的时间信息、设置日志归档周期。

网络安全专用产品安全认证或安全检测结果证明

（1）网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00279-A

★有效期：2023 年 11 月 10 日至 2025 年 11 月 10 日

（2）网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00280-A

★有效期：2023 年 11 月 10 日至 2025 年 11 月 10 日

所属品牌：启明星辰 / 网御星云

发布时间：2017 年 4 月

产品适用领域：运营商、政府、企业、电力、公安等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信安全管理系统

产品概述

天融信安全管理系统基于大数据架构，联合多种探针设备，运用主被动采集方式，实现多源异构的安全数据采集；结合安全数据进行资产风险分析；对日志、漏洞、性能进行实时监测及告警，并基于工单及安全设备集中配置、快速联动，实现协同化、高效化的安全处置；结合安全服务的最佳实践，以资产管理为基础，以风险管理为核心，以日志管理为主线、以等保管理为抓手，最终实现对全网资产的风险、告警管理和集中处理。

功能特点

◎特点1：集中资产管理与风险管理

通过对关键资产性能的实时监控，以及对探针上报的安全日志进行风险分析和处理，从而维护企业和组织的资产安全。通过多维度资产视图，查看资产的软硬件信息、漏洞补丁列表、物理位置信息，全面了解资产基本状况。结合资产风险曲线图、资产温度计了解资产风险情况。

◎特点 2：等保自测评全过程管理

紧密贴合我国网络安全等级保护政策，实现对信息安全工作中定级备案、安全建设整改、等保测评等各个工作环节的信息与数据集中管理和工作流程管理。提供等保概览、定级备案、等保检查，实现等保自测评全过程管理，全网等保测评进度可视化呈现。

◎特点 3：多厂家探针灵活接入

采用 syslog、snmp、wmi、JMS、NetFlow 等主被动采集方式，实现多厂商多探针的多源异构安全数据接入，接入设备类型包括防火墙、僵尸蠕、EDR、系统漏扫、Web 漏扫、蜜罐、入侵检测、Web 攻击检测、DDoS 检测、数据库审计、网络审计。客户可根据实际网络、预算情况灵活选择所需探针，选择不同类型的探针进行组合不影响系统运行。

◎特点 4：海量数据处理性能

海量数据存储与分析能力能够解决用户数据分析慢、安全数据无法长期存储的问题，是态势感知系统面向大数据分析场景的基础能力，尤其在设备多、网络环境复杂的用户环境下优势更为明显。分布式存储能力：系统支持分布式存储能力，通过横向扩展部署服务，实现数据的分布式多节点存储；快速分析能力：通过系统特有多节点调度技术提升了数据分析能力，实现安全数据的快速关联碰撞分析，及时发现威胁。

◎特点 5：多维态势支撑决策

多维安全态势对组织机构的安全数据按各种场景分析之后提供多维度态势展示，并支持安全态势的大屏展示。态势分析维度包括全网分析、攻击态势、安全处置态势等态势，辅助决策者做到态势全局掌控，可满足不同行业实时态势感知、准确安全监测、及时应急处置等目标，进而提升风险识别效率和快速处置能力。

◎特点 6：全方位集中管控

集中管控可实现对安全设备的统一管理能力，极大方便了安全运营处置工作和安全设备状态监控工作。设备管控能力：基于现实场景出发，系统采用集中管控安全设备的思路，实现诸如防火墙、僵尸蠕、EDR、漏扫等设备的集中管控能力；状态监控能力：能够实时监控设备状态，动态了解安全设备自身健康情况；设备配置备份：能够实现设备策略备份及自动化对比配置差异，快速掌握安全设备配置变更情况；设备策略管理：能够实现设备策略配置下发，提升安全运营效率。

技术指标

性能：数据采集性能 20000EPS

◎参数指标：

- ★支持大屏展示综合分析，包括全网分析、攻击态势、安全处置
- ★支持告警统计，告警处置统计，实时告警滚动显示
- ★支持告警工单处置人、告警处置结果、未处置状态统计并支持下钻详情；
- ★支持日志实时监视、日志采集配置，支持对接同品牌及第三方安全设备的日志

- ★支持漏洞监测功能，支持联动漏扫设备
- ★支持资产性能监测支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示等，支持性能监测任务新建、删除、启用和禁用等操作管理，支持对已有监测任务进行分类查询、查看、编辑等操作
- ★支持告警处置、漏洞处置功能
- ★支持对日志检索结果进行展示，支持日志检索、通连关系和聚合检索三种展示模式；支持日志溯源的攻击关系展示；
- ★支持生成安全报告，支持报告任务管理，包括新增、删除、暂停、查看，支持报告执行方式管理；
- ★支持资产管理功能，支持资产新增、修改、删除，支持自定义资产信息；支持备库管理；资产探测任务管理、多视角全网拓扑管理
- ★支持等保管理功能支持对业务系统进行等保定级备案，支持新建、删除、查询等
- ★支持策略管控、策略下发，包括防火墙、僵木蠕、EDR 等
- ★支持威胁情报管理，支持系统使用云端情报和离线情报。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：405231437

★有效期：2023 年 06 月 09 日至 2025 年 06 月 09 日

所属品牌：天融信

发布时间：2012 年 12 月 01 日

产品适用领域：政府、金融、交通、电力、教育、卫生、公检法、

运营商等

产品照片：



产品咨询二维码

产品咨询邮箱：feng_chong@topsec.com.cn

产品名称：天融信安全控制管理系统

产品概述

天融信安全 SD-WAN 解决方案由两部分组成：1、天融信安全控制管理系统（以下简称 WSC）。2、天融信边缘安全路由网关系统（以下简称 CPE）。其中 CPE 作为边缘接入网关部署在小分支机构的网络边缘侧以及总部网络出口，保障企业分支与分支之间、分支与总部之间、分支与数据中心之间的业务稳定，并提供高等级的安全防护功能，WSC 作为控制器部署在企业总部或者数据中心，负责对 CPE 进行统一管理，统一日志上报与统一用户控制。

天融信安全 SD-WAN 是天融信第一款自主研发的软件定义广域网产品，产品实现了多线路融合，智能 QoS，智能选路，应用识别，加速优化，用户认证，网络安全，集中管理等多项核心功能，并且针对分支机构做到了零配置上线，分支到总部无感知 VPN 互联，链路状态自动检测与链路自动切换，实现在不增加带宽与专线的前提下，极大优化出口流量，保障分支机构核心业务稳定。

功能特点

“安全可视化”一直以来都是天融信安全 SD-WAN 的重点研究方向，在设备本身实现应用层流量“可视”，从而让用户更加直观、更加全面的掌握安全风险，比如在报表中可以充分展现威胁监控信息，包括威胁类型排名、攻击者排名、受害者排名、威胁总数排名等，同时也可将威胁所触发的 CVE 漏洞信息进行充分展现，包括 CVE ID、风险等级、应用类型、漏洞描述等信息。通过 SD-WAN 设备本地“可视”，为用户提供了对攻击行为的追溯能力。

为了协助用户实现对网络的有效运维及管理，天融信安全控制管理系统为用户提供了安全可视化功能，实现对设备各种状态的实时监控，从而有效掌握整网设备运行情况及安全态势。

天融信安全控制管理系统具有专门的监控和数据中心功能模块，管理员通过监控面板可以快速地查看设备的流量统计信息和了解设备当前的运行情况。可以根据接口、应用、用户、用户组、服务器、IPSec VPN 查看设备的流量统计信息，查看设备受到的威胁信息，查看设备的 IPv4 和 IPv6 连接信息，查看在线的用户信息。数据中心主要实现对安全防护平台中的信息做统计，包括对网络事件的汇总和归档，相关数据的管理和日志的查看，并根据需要实现报告的生成和数据导出。

技术指标

指标项	详细要求
设备性能	默认包含 5 个授权点数，最多可管理设备数量为 10000 台
设备部署	支持旁路模式部署 支持配置 IPv6 地址

指标项	详细要求
登录安全	支持密码规则自定义 支持自定义登录规则，支持统计规则命中次数 内置三员管理员，包括系统管理员、安全管理员、安全审计员 支持外部服务器认证 支持双因子认证
系统管理	支持 NTP 时间同步、控制器与设备预共享密钥设置、SNMP 设置与页面关机 / 重启 支持系统告警，配置控制器 CPU、内存、磁盘告警阈值 支持审计数据转存，自动备份审计数据 支持审计数据按照磁盘阈值，保存周期进行自动清理
零配置上线	支持通过 Excel 表格导入的方式批量生成多分支上线配置 支持根据用户 WAN、LAN 信息自动生成隧道配置信息 边缘网关设备支持离线状态下，根据零配置上线信息自动生成 VPN 隧道配置 支持将设备初始化配置及上线指南发送到指定邮箱 支持 U 盘零配置上线
设备管理	支持对无公网地址的设备进行单点登录管理 支持命令行登录模式的远程协助，多个管理员共享操作屏幕 支持对命令行方式操作进行指令记录和录屏 支持配置设备基本信息
策略管理	支持策略模板管理 支持制定策略下发任务，支持定时任务和周期任务。 支持设备策略和配置的版本对比功能
配置管理	支持设备配置手动、定时、周期备份 支持设备配置查看、下载 支持对设备配置进行恢复 支持设备不同版本的配置、不同设备间配置进行对比
账号管理	支持设备管理员账号抽取、推送 支持对设备上管理员账号进行巡检，支持一键修复 支持账号追溯功能 支持设备密码维护
设备巡检	内置巡检模板 支持手动巡检、自动巡检
远程升级	支持手动升级、自动任务升级 支持系统版本、病毒库、IPS 库等类型升级 支持升级包 MD5 校验
任务编排	支持手动下发任务编排 支持自动下发任务编排 支持编排脚本的在线编辑和上传文件
系统数据展示	展示控制器系统信息、设备统计信息、Top 统计图、告警统计图 支持以离线地图模式展示设备在不同区域的分布情况和设备状态 支持隧道连接状态统计 支持大屏展示
设备状态展示	支持单台设备的状态信息查看，支持自定义展示范围。

指标项	详细要求
业务状态展示	支持以分组拓扑形式展示设备组网情况 支持在隧道列表展示全网隧道状态、隧道流速，支持查看隧道流量趋势图、隧道质量趋势图 支持以时延、抖动、丢包率维度查看隧道质量 支持隧道业务断开告警
安全监控	支持监控图表 支持集中显示隧道异常告警日志
报表展示	支持分支设备 CPU、内存、磁盘利用率 TOP10 生成报表 支持分支设备上下行流量 TOP10 生成报表
系统日志	支持系统硬件日志记录 支持系统操作日志记录

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230645

★有效期：2023 年 3 月 31 日至 2025 年 3 月 31 日

所属品牌：天融信

发布时间：2020 年

产品适用领域：政府、运营商、卫生、人社医保、企业、交通等

产品照片：



产品咨询二维码

产品咨询邮箱：feng_chong@topsec.com.cn

产品名称：天融信工控安全集中管理系统

产品概述

天融信工控安全集中管理系统依托天融信在工业安全领域多年研究的技术优势，结合工业安全产品特点进而设计的一款安全管理类产品。系统支持对工控防火墙、工控入侵检测与审计、工控安全监测审计、工控主机卫士、工控网闸、工控漏扫等产品进行统一配置、管理，以全局视角实现工业网络流量监控、工业资产统一管理和工业安全事件集中处置。为工业网络安全运营提供决策支持，加强安全事件响应速度与安全运维感知能力，提升整体工业网络信息安全水平。

功能特点

◎统一管理安全设备

天融信工控安全集中管理系统支持对工控防火墙、工控安全监测审计、工控主机卫士等工业安全设备集中管理，统一监控，安全策略批量下发，同时提供标准接口，支持对第三方设备进行实时监控，实现安全管理的集中化、便捷化。

◎全面收集安全日志

天融信工控安全集中管理系统支持对安全日志进行统一收集与归一化处理，内置大数据分析引擎，提供强大的数据查询处理能力，对海量安全日志进行快速处理与存储，满足存储合规要求，同时为进一步安全分析提供有力的数据支撑。

◎智能预警安全事件

天融信工控安全集中管理系统内置安全分析引擎，通过建立业务安全基线，及时发现异常行为与安全风险；同时支持安全规则自定义，基于业务自身特点定制完善的安全规则。系统提供 WEB、邮件、短信等多种告警方式，快速通告安全问题，提升安全事件响应速度。

◎集中下发安全策略

天融信工控安全集中管理系统支持安全策略下发，对业务基线模型、工控协议规则等通用策略进行批量配置，实现对分散的安全设备进行快速集中管理，同时支持单点设备管理，既减少设备运维工作量，又满足了设备个性化配置，全面提升管理效率。

◎精准识别安全威胁

天融信工控安全集中管理系统通过与工控漏扫实时高效联动，结合 CNVD、CNNVD、CVE 等工控漏洞库，对工业资产进行识别分析与综合评估，从多维度发现资产的脆弱性，并为客户提供详实的风险描述信息和漏洞解决方案。

功能指标

支持 1000 个终端同时在线；

支持工控安全设备管理，包括但不限于工控防火墙、工控审计、工控入侵、工控主机卫士等，提供策略的统一下发、日志的统一收集分析和设备状态信息的统一监控；

支持以网络拓扑方式展示网络环境及各设备的运行状态和安全状态；

支持通过 syslog、SNMP、FTP、webservice 等多种方式采集工控安全设备、网络设备、主机设备、业务系统、控制设备日志信息；

系统内置强大的工控安全分析引擎，通过对工控安全设备及应用日志的关联分析，可准确识别各类恶意攻击及异常行为；

支持生成工业资产、安全事件、安全告警、安全运维等维度的统计报表。

性能指标

事件采集能力 ≥ 8000 条 / 秒；

事件处理能力 ≥ 5000 条 / 秒；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231496

★有效期：2023 年 6 月 9 日至 2025 年 6 月 9 日

所属品牌：天融信

发布时间：2019 年 8 月 1 日

产品适用领域：可广泛应用于轨道交通、电力、冶金、煤炭、石油化工、
市政、汽车、烟草、智能制造、核电等行业。

产品照片：



产品咨询邮箱：
feng_chong@topsec.com.cn



产品咨询二维码

产品名称：天融信工业互联网态势分析与安全管理系统

产品概述

天融信工业互联网态势分析与安全管理系统是企业 and 组织对自有工业生产控制内网进行态势感知的系统。系统采集网络中的资产、流量、日志、设备运行状态等相关安全数据，经过存储、处理、分析后形成安全态势及告警，辅助用户了解所管辖工业网络安全态势并对告警进行协同处置。利用现有安全系统、安全设备，逐步演进为“工业安全数据集中存储、工业态势感知场景丰富、安全动态建模分析及工控可视化综合展示”的高价值安全信息存储及分析系统，加快对安全威胁认知及有效预警。

系统按照一体化、标准化、智能化、可视化要求进行建设。实现对网络安全态势觉察、跟踪、预测和预警，全面、实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患，及时监测漏洞、病毒木马、网络攻击情况，发现网络安全事件线索、预警通报重大网络安全威胁、处置安全事件，有效防范和打击网络攻击等违法犯罪活动，达到实时态势感知、准确安全监测、

及时应急处置等目标，提升企业等组织的风险发现能力，加快风险解决速度。

功能特点

◎强大的数据处理能力

采用大数据分析引擎，利用分布式文件存储及检索技术，可支持高达 PB 级的数据存储及检索，支持十亿级别数据秒级检索响应，同时具有横向扩展特性，客户可以根据实际使用需求，动态的增加系统的存储与计算性能。

◎全面的安全分析技术

支持汇总各类安全数据，运用关联分析、用户画像、业务安全基线、模型分析、威胁情报等安全技术，有效发现各类安全事件与风险隐患，识别漏报与误报的行为，提升安全运维工作效率，形成安全联动、动态感知的整体安全分析能力。

◎灵活的部署安全探针

支持丰富的探针类型，包括工控漏扫、工控防火墙、工控网闸、工控入侵检测与审计、工控监测审计、工控主机卫士等，同时支持第三方设备数据接入，客户可根据实际网络、预算情况选择安全探针进行部署，灵活组合不同类型的探针。

◎智能的识别工业资产

通过工业资产指纹识别技术，全面发现工业互联网资产，从工业设备、主机、应用、业务等多个维度构建资产库，对网内资产进行实时安全监控，呈现网络的风险、脆弱性等安全信息，为客户提供强大的资产管理与安全监控手段。

◎完备的安全知识大脑

以工业互联网安全知识大脑为核心，包括工业资产指纹库、工业协议库、工业漏洞库、工业威胁特征库和工业设备库等，提供威胁情报、联动分析、合规分析、威胁追溯等安全分析服务，为客户持续输送安全能力。

◎全维度安全态势感知

从风险、攻击、资产等多个通用维度进行基本态势展示，从探针、追踪溯源等多个专项维度进行专项态势展示，并支持自定义态势展示。通过多种可视化态势感知技术，为客户提供友好易用的安全监控手段，进一步提升安全运维工作效率。

功能指标

支持全网态势、威胁态势、资产态势、漏洞态势、攻击态势、运行态势等态势大屏，同时支持态势大屏中相关信息下钻到对应的详细页面；

支持通过大数据分析技术对各类探针系统及业务系统的日志进行 7*24 小时实时威胁风险预警及展示；

支持接入第三方各种类型安全设备的日志采集、归一、关联分析并按照安全事件进行分类展示；

支持内置调查分析引擎对全网流量和日志进行深度安全场景分析，安全分析场景包括但不限于：追踪溯源、威胁画像、资产画像；

支持全网流量进行综合分析，并对接入的流量设备进行综合分析后按照设备概况、流量关系图、流量趋势进行动态监控展示；

支持按照资产管理、安全域管理、业务系统、软件管理、硬件管理多个视角对资产进行不同维度进行统计分析和展示；

支持基于多源安全设备策略管理，可通过策略下发接口下发安全设备策略采集命令，接收安全策略数据，并完成相关安全设备管理、策略抽取、命令下发。

性能指标

事件采集能力 ≥ 20000 条 / 秒；

事件处理能力 ≥ 20000 条 / 秒；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230685

★有效期：2023 年 3 月 31 日至 2025 年 3 月 31 日

所属品牌：天融信

发布时间：2020 年 7 月 20 日

产品适用领域：可广泛应用于轨道交通、电力、冶金、煤炭、石油化工、市政、汽车、烟草、智能制造、核电等行业。

产品照片：



产品咨询邮箱：

feng_chong@topsec.com.cn



产品咨询二维码



网络型流量控制产品

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：深信服流量控制系统

产品概述

深信服流量控制系统 BM 是一款先进的网络流量可视化解决方案，它的出现旨在帮助 IT 管理员更加高效地管理和优化网络带宽资源。在现代企业中，网络的重要性不言而喻，而如何合理利用和管理网络资源，以保证网络运行的稳定性和性能，成为了 IT 管理员面临的一大挑战。BM 解决方案正是针对这一挑战，提供了一系列实用且直观的功能，助力管理员轻松掌握网络运行状况。

BM 解决方案通过出口流量曲线图，让 IT 管理员能够清晰地了解到网络出口的流量变化情况。这有助于管理员及时发现并解决网络带宽瓶颈，从而提高网络运行效率。此外，曲线图还可以作为预测网络流量需求的参考，为网络资源的规划提供数据支持。

总之，BM 网络流量可视化解决方案为 IT 管理员提供了一站式的网络管理和优化服务。通过直观的数据展示和实用的功能，BM 解决方案有助于管理员更好地监控和管理网络流量，提高网络运行性能，防范网络攻击，确保网络安全。在我国，随着信息化进程的不断推进，网络管理的重要性日益凸显，BM 解决方案的应用将有助于企业提升网络管理水平，为企业的可持续发展

展创造价值。

功能特点

BM 解决方案在现代企业网络管理中发挥着重要作用，它具有实时监测网络异常状况的能力，包括异常流量波动、网络攻击等情况。通过及时发出预警，BM 解决方案助力 IT 管理员迅速响应和处理网络故障，确保网络的正常运行。在这个基础上，BM 解决方案还能提供针对网络攻击的防范建议，降低企业网络风险，守护网络安全。

为了让 IT 管理员更加便捷地掌握用户网络行为分布和带宽资源使用情况，BM 解决方案还具备自动形成报表文档的功能。这些报表会定时发送到指定邮箱，使管理员能够轻松了解流控策略效果，并为带宽管理的决策提供准确依据。

总之，BM 解决方案不仅具备实时监测网络异常、预警提醒等功能，还能提供网络攻击防范建议，降低企业网络风险。同时，通过记录和审计内网用户网络行为，生成直观的报表，BM 解决方案使 IT 管理员能够更加轻松地管理带宽资源，提高网络运行效率。BM 解决方案在保障网络安全、优化网络性能方面具有重要意义，值得企业在网络管理中广泛应用。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：404231350

★有效期：2023 年 6 月 2 日至 2025 年 6 月 2 日

所属品牌：深信服科技股份有限公司

发布时间：2021 年 10 月 11 日

产品适用领域：政府、教育、医疗、企业、金融等行业

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn



负载均衡产品

北京信安世纪科技股份有限公司

北京信安世纪科技股份有限公司（股票代码：688201）成立于 2001 年 8 月，是科技创新型的信息安全产品和解决方案提供商。公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全、通信安全等基础性安全问题，为金融、政府、企业、军队等重要领域的核心业务系统提供先进的网络安全产品与安全解决方案。

网址：www.infosec.com.cn

电话：010-68025518/400-670-5518

地址：北京市海淀区建枫路（南延）6 号院金隅西三旗科技园 2 号楼信安大厦

产品名称：APV 应用交付系统

产品概述

APV（信创系列）应用交付系统基于国产硬件和国产操作系统，实现应用交付的自主创新。APV 系列是下一代应用交付控制器（ADC），作为一个为企业级应用服务设计的应用交付解决方案，APV 代表了新一代的应用负载均衡和性能优化产品，仅仅通过一个功能强大的系统，即可提供高度集成的应用交付功能。

APV 应用交付系统，搭载国产多核 CPU 处理器，适配国产操作系统，在可用性、加速和安全功能上有一系列优异表现，提供应用交付在自主创新领域的高性能，为客户带来极高的整体价值。APV 硬件设备，采用自主创新认证的硬件加速和节能组件，提供高性能保证。APV 致力于提升现代数据中心的应用性能，加速服务提供商、企业和公共组织机构的投资回报。

功能特点

◎多重负载均衡机制

APV 应用交付系统同时支持 OSI L2-L7 层的服务器负载均衡，链路负载均衡，全局负载均衡，可适用于多种负载均衡场景。

多重服务器负载均衡算法将所有流量均衡的分配到各个服务器，充分利用所有的服务器资源，确保业务的稳定运行。

支持出入向的链路负载均衡的同时，拥有丰富的链路负载均衡算法，满足多链路互联网接入、多分支机构网络等多种应用场景。

超高 DNS 查询响应性能（RPS），通过自研技术架构、多核处理等方式，显著提高权威 DNS 性能。同时支持智能 DNS 解析、全域名解析及 DNS 防护策略，为用户提供最佳的应用体验。

◎强大的 SSL 安全功能

身份鉴别高安全性，支持 SSL/TLS 协议族，支持单、双向身份认证，支持高强度加密算法，为应用提供可靠的身份认证方案，支持多种证书状态验证模式，包括 CRL（支持 LDAP、FTP、HTTP 协议）、OCSP 方式；

支持标准的 PKCS#10 证书请求、X509V3 证书，支持国内外各大证书运营商的证书；

支持多种网络通信协议，与多种网络应用系统无缝集成，支持所有基于 TCP 协议之上的应用，包括 HTTP、FTP 等多种常用协议；

支持应用重定向功能，能根据用户证书属性进行应用重定向，限制或允许特定证书对应用的访问。

◎IPV6 支持

APV IPV6 解决方案为客户的应用交付提供了 IPV6-to-IPV4 和 IPV4-to-IPV6 转换技术，帮助客户将应用业务平滑和无缝迁移到 IPV6 网络，解决 IPV6 升级改造过程中遇到的“IPV6 天窗”等问题，提供与 IPV4 应用交付一致的性能、稳定性和高可用性，为用户提供最佳的应用体验。

◎支持国密标准

支持国家密码管理局颁布的规范《GMT 0024-2014 SSL VPN 技术规范》《GMT 0025-2014 SSL VPN 产品规范》；

支持国际标准算法，支持国家密码管理局提供的国密 SM2/SM3/SM4 算法；

具有国家密码管理局颁发的商用密码型号证书，产品完全自主可控。

◎可维护性

APV 支持多种语言管理界面，提供快速配置功能，可通过 Web 图形管理界面或简单易用的命令行界面，进行直观的配置和管理，实时监控图表，为排查问题、决策分析等提

强大的审计功能，提供包括系统、操作、访问和调试的详细日志记录，可帮助管理员进行迅速的故障排查；

支持 SNMP、SYSLOG、RMON 和 Email 告警等功能，便于第三方网络管理软件集成，保障系统稳定运行；

具有按需定购的灵活性，能在不升级硬件的情况下增加负载均衡模块，具有高度灵活性和可扩展性；

支持 epolicy 七层应用脚本与 eroute 四层路由功能提供定制的应用流量控制，通过高性能的内核级七层策略引擎实现定制化流量管理，且性能和扩展性不受影响；

系统部署对应用系统无影响，无需变更应用系统和网络架构；

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS026-622

★有效期：2024 年 1 月 9 日至 2029 年 1 月 8 日

所属品牌：信安世纪

发布时间：2011 年 8 月 23 日

产品适用领域：金融、电力、石油、烟草、运营商、教育、政企、电商、
交通、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：market@infosec.com.cn

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：迪普应用交付平台

产品概述

IT 系统的建设就是为了更精细的实现业务系统“加速”、“安全”、“可靠”的本质需求，从而应用交付产品在市场上诞生了，并且迅速得到用户的广泛认可。

为了解决深度包检测对业务系统性能影响，迪普科技基于自身领先的 APP-X 硬件平台、ConPlat 软件平台和 APP-ID 应用识别与检测技术，研制的 ADX 应用交付平台系列产品，完美的解决了这一矛盾。可为业务系统的信息化建设提供如下能力：

◎确保业务系统永续

迪普科技 ADX 产品利用健康监测，智能调度算法，AD_Rules 脚本语言，虚拟化技术等针对业务系统的服务器、链路和业务扩容能力等三个方面进行优化，让业务系统永续成为可能。

◎保障业务安全

迪普科技 ADX 具备安全防御能力尤其是针对 DoS/DDoS 这类等对业务系统危害巨大的攻

击，实现业务系统的多层次安全防护。

◎提升用户体验

ADX 通过众多的 SSL 加速、HTTP 压缩、Cache 等功能，不仅提升服务器工作能力，而且提高用户的访问速度和应用体验。

ADX 也全面支持 IPv4/IPv6 协议及 IPv4/IPv6 过渡技术，兼容现有不同的网络技术。

ADX 是业界第一款 3.2T 应用交付平台^{*}，具有处理能力强、应用交付能力全面、接口密度丰富等优点，可应用于各行业和运营商的数据中心和网络出口，提供服务的可靠性、提高服务的响应速度、方便业务灵活扩展等最佳的业务价值。

功能特点

◎电信级高可靠

关键部件冗余设计、数据平面与控制平面相分离、N:M 虚拟化、双机热备、VRRP、N+M 集群等技术，可有效降低单点故障。设备发生故障后确保原有的网络连接不会中断，做到真正的无缝切换，实现电信级的网络高可靠性。

◎首款 3.2T 应用交付平台

基于高性能硬件架构 APP-X，可提供超过 3.2T 单设备性能，并可通过 N:M 虚拟化进行性能聚合，实现性能的倍增。

◎个性化编程

AD_Rules 可快速适配用户在网络出口、服务器、数据中心场景下的个性化需求。广泛运用于政府、运营商、电力、金融等行业。

◎多功能融合

集成链路、服务器及全局负载均衡功能，并支持 SSL 加速、HTTP 缓存、HTTP 压缩、抗 DDoS 等应用优化与安全防护功能，确保应用的快速、安全、可用。

◎丰富的网络特性

支持 IPv4/IPv6、OSPF、RIP、MPLS 等协议，满足复杂网络环境的组网要求。

◎全面检测，智能调度

支持 30 余种健康检测算法，20 余种调度算法，并且支持根据业务模型自定义，从网络层、应用层全方位的探测、检查服务器和链路的运行状态，以便快速的选择最合适的服务器或出口链路，从而实现高效的负载分担。

◎部署方式灵活

支持串接、旁路、三明治等多种部署方式，并支持高密千兆及万兆接口，能满足各种复杂应用环境的需要。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00068-A

★有效期：2023 年 09 月 15 日至 2025 年 09 月 15 日

所属品牌：杭州迪普科技股份有限公司

发布时间：2010 年 6 月 18 日

产品适用领域：运营商 - 中国移动，中国电信，中国联通，吉视传媒等；

电力能源 - 国家电网，中国南方电网，中国石油，中国石化等；

政府 - 国家信息中心，公安部，国家发改委等；

教育 - 复旦大学，山东大学，北京航空航天大学等；

大企业 - 中国铁路总公司，中国烟草，中国建筑总公司等；

交通运输 - 吉祥航空，东方航空，南方航空等；

金融 - 中国工商银行，中国交通银行，中国银行等

产品照片：



产品咨询邮箱：zhangjunkai@dpotech.com



迪普订阅号



迪普服务号

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等 70 余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

产品名称：绿盟负载均衡系统

产品概述

绿盟负载均衡系统 ADC，是一款专业的应用交付产品。支持完善的负载均衡功能，包括链路负载均衡（LLB）、服务器负载均衡（SLB）和全局负载均衡（GSLB）。支持应用、服务器和链路的健康检查、SSL 卸载、缓存加速等应用优化的特性，大大提高了客户业务系统、网络的可用性和可扩展性，有效提升了企业数据中心的运营效率。

功能特点

◎ 绿盟负载均衡技术特点

负载均衡提供了一种廉价、有效、透明的方法扩展网络设备和服务器的带宽、增加吞吐量、增强网络数据处理能力，提高网络的灵活性和可用性。

负载均衡技术具有如下特点：

高性能：通过调度算法，将客户端请求合理地均衡到后端各台服务器上，消除系统可能存在的性能瓶颈。

可扩展性：当业务的负载增长时，系统能被扩展来满足需求，且不降低服务质量。

高可用性：通过健康检测功能，能实时监测应用服务器的状态，保证在部分硬件和软件发生故障的情况下，整个系统的服务仍然可用。

透明性：将多个独立计算机组成的松耦合的服务系统构成一个虚服务器；客户端应用程序与服务系统交互时，就像与一台高性能、高可用的服务器交互一样。客户端无须作任何修改。部分服务器的切入和切出不会中断服务，而用户觉察不到这些变化。

◎绿盟绿盟负载均衡产品优势

负载均衡技术发展至今已经十分成熟，各个厂商之间基本上都是大同小异，但是侧重点会有所不同。绿盟负载均衡产品致力于提供快速、安全、稳定的应用交付解决方案。其优势如下：

完善的服务器负载均衡功能 — 超过 20 种负载均衡算法；多维度的健康检测机制，支持脚本健康检测，能够对业务健康状况进行深入检查。

强大的链路负载均衡能力 — 多种流量调度机制，如基于 ISP 选路、应用选路、URL 选路、及动态就近性选路

丰富的应用优化手段 — 通过各种应用加速功能，如 TCP 协议优化、TCP 连接复用、Web 缓存、压缩技术、SSL 卸载，实现业务系统的快速交付。

领先的虚拟化技术 — 支持多种虚拟化技术：完美适配云环境下的多租户场景。

稳定的硬件平台 — 所有硬件产品型号，易损件（电源、硬盘、风扇）支持冗余，且电源支持热插拔，真正做到业务永远在线。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00158-A

★有效期：2024 年 02 月 02 日至 2026 年 02 月 02 日

所属品牌：绿盟负载均衡系统 ADC

发布时间：2021 年

产品适用领域：全行业适用

产品照片：



产品咨询邮箱：support@nsfocus.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

集团总部位于北京市中关村软件园启明星辰大厦，DT（数据时代）总部位于杭州高新区（滨江），全国云安全总部位于苏州高新区，在全国各省、市、自治区设立了分支机构，拥有覆盖全国的渠道和服务体系，为用户提供网络安全产品、服务和解决方案。

网址：www.venustech.com.cn

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：天清应用交付控制系统

产品概述

天清应用交付控制系统（简称天清 ADC），是在传统的负载均衡产品基础上进行全面升级后的新一代应用交付产品。产品集链路负载、服务器负载、全局负载等功能为一体，突出了应用安全防护、应用加速和内容分发等技术，可以确保用户的业务应用能够快速、安全、可靠地的交付。目前天清 ADC 产品和解决方案已成功运用在政府、公检法司、企业、教育、医疗、能源、交通、金融等数千用户。

功能特点

◎**多功能融合**：集成服务器负载、链路负载、全局负载、SSL 加速、HTTP 压缩、Cache、VPN、DDOS 等功能，ALL-IN-ONE 设计；

◎**应用选路**：内置应用检测引擎，可有效识别在线视频、P2P 下载、视频会议等 20 大类，上千种主流应用，可根据业务优先等级进行流量牵引和 QOS；

◎智能流量编排：安全设备池化接入，对不同属性用户流量进行编排，SSL 流量可视化，安全设备之间松耦合；

◎个性化编程：基于 TCL、Python 语言的 tRules 可满足 IT 业务的个性化需求；

◎安全防护：集成四七层防火墙、DDOS 防护、DNS 防护、WEB 防护、黑白名单等一系列安全功能。

技术指标

◎具备负载均衡功能，包括链路负载、服务器负载和全局负载。

◎具备链路和服务器状态检查功能。

◎具备优化加速功能，包括 TCP 连接复用、SSL 加速、ram 缓存、http 压缩。

◎具备设备访问控制功能。

◎具备 HA 高可用性功能。

◎具备鉴别、管理、日志等自身安全功能。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00427-A

★有效期：2023 年 12 月 15 日至 2025 年 12 月 15 日

所属品牌：启明星辰

发布时间：2013 年

产品适用领域：政府、公检法司、金融、运营商、电力、交通、企业等

产品照片：



产品咨询二维码

产品咨询邮箱：du_delong@venusgroup.com.cn

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址: www.sangfor.com.cn

电话: 400-806-6868

地址: 深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称: 深信服应用交付网关 AD-1000 V7.0

产品概述

深信服 AD 产品作为专业的应用交付设备，能够为用户的应用发布提供包括多数据中心负载均衡、多链路负载均衡、服务器负载均衡以及 SSLO 流量编排的全方位解决方案。配合性能优化、单边加速以及多重智能管理等技术，实现对各个数据中心、链路以及服务器状态的实时监控，同时根据预设规则将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。不仅扩展应用系统的整体处理能力，提高其稳定性，更可切实改善用户的访问体验，降低组织的 IT 投资成本。

功能特点

◎服务器负载均衡：运用多台服务器集群的机制，深信服 AD 应用交付设备能将所有真实服务器配置成虚拟服务来实现负载均衡，对外直接发布一个虚拟服务 IP。当用户请求到达应用交付设备的时候，根据预先设定的基于多重四、七层负载均衡算法的调度策略，能够合理的将每个连接快速的分配到相应的服务器，从而合理利用服务器资源。不仅在减少硬件投资成本情

况下解决单台服务器性能瓶颈，同时方便后续扩容，为大并发访问量的系统提供性能保障。通过对服务器健康状况的全面监控，深信服 AD 应用交付设备能实时地发现故障服务器，并及时将用户的访问请求切换到其他正常服务器之上，实现多台服务器之间冗余。从而保证关键应用系统的稳定性，不会由于某台服务器故障，造成应用系统的局部访问中断。

◎**链路负载均衡**：深信服 AD 应用交付设备集成智能路由、DNS 透明代理和智能 DNS 解析等技术，通过轮询、加权轮询、静态就近性、动态就近性等算法，解决多链路网络环境中流量分担的问题，充分提高多链路的带宽利用率，节约企事业单位对通信链路的投资；并且通过为用户分配最佳的通信线路，使用户获得绝佳的访问体验。此外，深信服 AD 应用交付设备还利用链路健康检查及会话保持技术，实现了在某条链路中断的情况下任然可以提供访问链接能力，充分利用了多条链路带来的可靠性保障，使对于用户的访问达到了最全面的支持。

◎**全局负载均衡**：深信服全局负载均衡解决方案能够帮助组织将相同应用系统的服务内容部署在不同地理位置之上，保证承载应用系统的多数据中心能够具备更高的持续性和可用性以及快速性，使得用户不管身处全球任何位置都能获得更快速、更稳定的访问体验。通过全面的健康检查机制，AD 设备能够实时的监控各个数据中心的运行状况，及时发现出现故障的数据中心或者其内部服务器，从而保证将用户后续访问请求都分配到其他的正常数据中心或者服务器之上。不但使多站点之间形成冗余，保障用户访问稳定，还提升了各站点的资源利用率。

◎**单边加速功能**：独一无二的单边加速功能，用户客户端无需安装任何插件或软件即可提升访问速度。打造稳定智能的业务发布平台，使得用户可以更快更稳定地访问发布内容。

◎**智能优化技术**：DNS 透明代理、链路 / 服务器拥塞繁忙保护、智能路由、邮件智能告警技术进一步提升各类资源的利用率，增强用户的访问体验。

技术指标

深信服应用交付产品覆盖的性能档次比较全，吞吐量从最低端的 2G 到最高端的 160G。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00303-A

★有效期：2024 年 03 月 21 日至 2025 年 05 月 12 日

所属品牌：深信服

发布时间：2009 年

产品适用领域：政府、金融、交通、电力、医疗、运营商、教育等

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信负载均衡系统

产品概述

天融信负载均衡系统（以下简称TopAPP产品）为客户提供高可靠的数据中心解决方案，包括链路负载均衡解决方案、服务器负载均衡解决方案、全局负载均衡解决方案。TopApp产品集成了压缩、缓存、SSL卸载等网络优化技术，加速业务系统提升系统效率。同时结合Web应用防火墙、DNS防火墙、DDoS攻击防护及漏洞扫描功能形成全方位的网络安全防护，为客户业务系统安全保驾护航。

功能特点

◎高性能

TopApp基于天融信新一代安全系统NGTOS平台设计和开发，凭借NGTOS平台高性能的优势，单主控板硬件设备吞吐能力高达120Gbps，上亿级并发连接数，百万级新建处理能力，设备性能已经达到国内市场的巅峰。

◎安全防护

TopApp 产品还继承了天融信 NGTOS 平台的安全基因，具有完备的安全技术手段，集成了 4-7 层的访问控制、DDoS 攻击防护、DNS 攻击防护、Web 安全防护、数据库安全防护、漏洞扫描等一系列安全功能，为客户提供紧贴应用的安全防线。

◎编程调度

TopApp 产品可编程技术灵活调度用户需求，处理应用和网络事件。TopApp 产品支持流量调度策略和会话保持等功能，提高业务灵活性，完成一些个性化需求，具有低工作量、低成本、高效率的特点，保证业务快速稳定上线。

◎双栈接入

TopApp 产品支持双栈接入和 IPv4 与 IPv6 地址转换功能，支持 IPv6 环境下的 SSL 商用卸载和国密卸载，同时 TopApp 产品支持双栈接入下的访问控制、DDoS、Web 安全、数据库安全、DNSSec 等一系列安全防护。

◎应用监控

TopApp 产品具备丰富的实时以及历史报表，用户能够清晰的看到虚拟服务器、链路、服务器节点的健康状态、服务分布、流量走势、带宽占用、故障分类等信息，从而帮助用户深入了解自己的网络运行状态。同时支持细粒度定制化报表，进一步提升用户的可视化体验。

技术指标

指标项	详细要求
设备形态	标准机架式设备，独立硬件平台，高性能系统架构，非任何插卡扩展形态的负载均衡设备。
部署模式	支持串行、旁路、三角传输部署模式。
高可用性	链路负载均衡和服务器负载部署支持 AS/AA 模式，同步配置实现无缝故障切换。
双栈接入	支持主备之间会话同步，支持 IPV6/IPV4 双栈，支持 NAT66、NAT64、NAT46、DNS64 可对过渡型网络进行负载均衡。
多功能合一	支持多功能合一同时支持链路负载均衡、服务器负载均衡和全局负载均衡的功能，无需额外购买相应授权。此外设备集成 TCP 协议优化、WEB 压缩缓存、页面加速、SSL 卸载、网络防火墙、Web 应用防火墙、DNS 防火墙、漏洞扫描、四七层 DDoS 攻击防护等功能。
安全防护	提供网络防火墙功能，支持基于五元组进行访问控制；提供 Web 应用防火墙功能。提供 DNS 防火墙功能；支持提供四七层抗 DDoS 攻击功能；提供数据库安全功能；提供漏洞扫描功能。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00052-A

★有效期：2023 年 9 月 1 日至 2025 年 9 月 1 日

所属品牌：天融信

发布时间：2013 年 1 月 4 日

产品适用领域：政府、运营商、金融、能源、企业等

产品照片：



产品咨询二维码

产品咨询邮箱：feng_chong@topsec.com.cn



抗拒绝服务攻击产品

北京百度网讯科技有限公司

百度是拥有强大互联网基础的领先 AI 公司。是全球为数不多的提供 AI 芯片、软件架构和应用程序等全栈 AI 技术的公司之一，被国际机构评为全球四大 AI 公司之一。百度以“用科技让复杂的世界更简单”为使命，坚持技术创新，致力于“成为最懂用户，并能帮助人们成长的全球顶级高科技公司”。

百度公司 2000 年 1 月 1 日创立于中关村，创始人李彦宏拥有“超链分析”技术专利，也使中国成为美国、俄罗斯和韩国之外，全球仅有的 4 个拥有搜索引擎核心技术的国家之一。百度每天响应来自 100 余个国家和地区的数十亿次搜索请求，是网民获取中文信息和服务的最主要入口，服务 10 亿互联网用户。

基于搜索引擎，百度演化出语音、图像、知识图谱、自然语言处理等人工智能技术；最近 10 年，百度在深度学习、对话式人工智能操作系统、自动驾驶、AI 芯片等前沿领域投资，使得百度成为一个拥有强大互联网基础的领先 AI 公司。

网址：<https://home.baidu.com/home/index>

电话：010 - 59928888

地址：北京市海淀区上地十街 10 号百度大厦 2 层

产品名称：DDoS 防护服务

产品概述

DDoS（Distributed Denial of Service）分布式拒绝服务攻击，是网络攻击中最常见的攻击方式。这种攻击方式在进行攻击的时候，会组织不同地点的大量计算机同时进行，攻击的数据包各式各样，其目的主要是对目标造成无法提供服务的故障，给开放服务带来巨大损失。这类攻击成功的表现形式可能是应用服务迟钝、系统设备宕机、网络带宽拥塞等等。

DDoS 防护服务提供 T 级云防、定制端防和运营商联防等能力，能有效抵御网络层和应用层 DDoS 攻击。通过 IP 或 DNS 解析的方式接入，支持 TCP、UDP、HTTP、HTTPS、WEBSOCKET、WEBSOCKETS 等协议，广泛适用于各种业务场景。同时采用了 BGP 线路，天然具有更强的灾备能力、线路更稳定、访问速度更快。



产品架构图

功能特点

功能	说明
极速攻击预警	基于对流量的分析、学习和预测，建立起业务流量模型。DDoS 攻击开始的数秒钟内，即可实现攻击发现、防护启动、通知预警等，真正做到秒级防护。
4 层流量攻击防御	替身式服务，源站隐藏于 T 级带宽云防节点之后，有效防御 SYN Flood、SYN ACK Flood、UDP Flood、TCP Flood 在内的 40+ 种类型流量攻击。
7 层 CC 攻击防御	基于对被保护业务的基线学习，结合黑白灰安全模型，能够准确快速鉴别出应用层攻击的攻击特征，实施精准防御。
多维度数据报表	多项数据报表，从流量、报文等多个维度全面诠释攻击情况。

技术指标

◎**实时监测秒级防御**：基于独有智能高敏数据包比例模型算法，最快 100ms 发现流量攻击，秒级执行防御。

◎**高效联动防御**：弹性公网 IP 等百度云资源或私有化本地部署防御系统，在检测到超量攻击后自动联动云防防御。

◎**更聪明更智能**：特有智能分析系统，实时提取攻击特征，辅助全网 IP 威胁库、攻击 IP 进行恶意请求拦截，多维度精确缓解 CC 攻击。

◎**更快更强更高效**：总计 T 级的 DDoS 防护带宽，30+ 线路 BGP，速度更快，延迟更小，线路更稳定。

◎**专业可信赖**：百度安全专业团队提供技术支持，拥有多年百度实战经验，值得信赖。

网络安全专用产品安全认证或安全检测结果证明

(1) 网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检测中心

★证书编号：24SS00904-A

★有效期：2024 年 6 月 28 日至 2026 年 6 月 28 日

(2) 计算机信息系统安全专用产品销售许可证

★证书编号：0402231372

★有效期：2023 年 6 月 2 日至 2025 年 6 月 2 日

所属品牌：百度

发布时间：2019 年

产品适用领域：金融、网络技术、互联网、智能制造等有互联网业务的客户

产品照片：



产品咨询二维码

产品咨询邮箱：dun-bd@baidu.com

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：异常流量检测与清洗系统

产品概述

迪普科技异常流量检测 / 清洗系列产品是专业的抗 DDoS 攻击防护设备，包括：异常流量检测产品 Probe3000、异常流量清洗产品 Guard3000 以及业务管理平台，能够及时发现网络中的各类 DDoS 攻击并实现对攻击流量的快速过滤。此外，迪普科技异常流量检测与清洗系统还可为用户提供安全可视化服务，帮助用户直观了解现网安全状况，及时消除安全隐患。

功能特点

◎全面防护各类 DDoS 攻击

迪普科技异常流量检测 / 清洗系统采用独创的四大检测引擎：多级特征检测引擎、流量智能调度引擎、智能指纹提取引擎和行为探测防护引擎，凭借多重安全引擎的加持，可以实现流量型 DDoS 攻击和应用型 DDoS 攻击的深度检测和防御，可以有效防范当前主流的 DDoS 攻击，如 SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、CC、DNS Flood、DNS 反射攻击、NTP 反射攻击等。

◎双向攻击检测防护

常规的 DDOS 攻击流量清洗是针对固定的防护目标，清洗入方向的异常流量。对于出方向的 DDOS 攻击流量，存在攻击目标不确定性。异常流量检测 / 清洗产品通过模糊攻击检测技术智能分析出向流量目的 IP，并开启全局清洗策略，实现近源清洗效果，满足特定场景下双向抗 DDoS 攻击防护需求。

◎攻击溯源分析

在实现 DDoS 攻击检测与清洗之外，迪普科技异常流量清洗产品集成了一套抓包溯源和攻击自动分析的工具，支持抓取清洗前、清洗后、清洗丢弃的报文进行分析；针对抓包文件可以进行攻击源 IP 溯源，并提取攻击报文中的攻击特征，简化防护策略配置难度。

◎复杂网络适应能力

迪普科技异常流量检测 / 清洗产品支持丰富的网络特性，可部署于 BGP、MPLS VPN 等复杂网络环境下。旁路部署模式下，支持通过 BGP 技术进行流量牵引，流量回注技术可使用策略路由、VLAN、GRE、MPLS 等技术，满足不同组网环境下的抗 DDoS 防护需要。

◎抗 DDoS 安全运营管理解决方案

为满足运维管理和抗 DDoS 服务运营需要，迪普科技可提供综合性的运营管理平台，遵循“护自己、护他人”的理念，在简化日常运维及攻击处置的同时可以为租户提供抗 DDoS 攻击防护服务，通过可视化平台全面提升租户感知能力和使用体验。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402231157

★有效期：2023 年 5 月 19 日至 2025 年 5 月 19 日

所属品牌：迪普科技

发布时间：2009 年

产品适用领域：运营商、金融、政府

产品照片：



产品咨询二维码

产品咨询邮箱：liandonghai@dptech.com

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等 70 余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web 应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路 4 号益泰大厦 3 层

产品名称：绿盟抗拒绝服务系统

产品概述

绿盟抗拒绝服务系统（NSFOCUS Anti-DDoS System，简称 NSFOCUS ADS）是一款专业的 DDoS 攻击防御产品。首款产品型号自 2001 年发布上市以来，坚持进行技术创新和产品研发，推出适配不同行业特点的 DDoS 防御功能和算法，及时发现背景流量中各类复杂的 DDoS 攻击事件并迅速进行清洗，保障业务的正常运行。产品具备灵活部署、全面监控、精准防护和数据丰富等特性，实现 DDoS 防护的完整闭环。NSFOCUS ADS 基于机器学习建模、交互式动态防护算法、大数据威胁情报等技术，在 IPv4、IPv6 及两者混合环境中，全面精准防护各类 DDoS 攻击。产品具备硬件和虚拟化形态，并可与其他产品能力组合可以形成自动牵引的三位一体解决方案，高效应对大流量 DDoS 攻击的云地混合防护，以及资源统筹调度的增值运营解决方案。

功能特点

序号	功能特点	具体描述
1	传输层 DDoS 防护	支持四种 SYN Flood 防护算法、三种 ACK Flood 防护模式、多种 ICMP 和 UDP 的防护策略来防御各类传输层 DDoS 攻击
2	应用层 DDoS 防护	支持九种 HTTP Get/POST 防护算法、HTTPS、HTTP/2、慢速攻击防护、四种 DNS Flood 防护算法对应用层进行精细化防护以及区分 PC 端 /APP 业务流量，进行精细防护。
3	流量过滤策略	支持基于黑白名单、ACL、正则规则、TCP/UDP 反射防护规则、模式匹配、GeoIP、云 IP 信誉等策略进行清洗防护。
4	产品可维护性	满足多任务的手动 / 自动抓包功能、一键故障收集、三方接口以及抓包可视化、智能策略关联等。

技术指标

◎支持对欺骗与非欺骗的 SYN Flood、ACK Flood、ICMP Flood、ICMP Fragment、UDP Flood、UDP Fragment、FIN/RST Flood、TCP Misuse、TCP Connection Flood、TCP Fragment、HTTP Flood、HTTP Slow Attack、HTTPS Flood、SIP Flood、DNS Query Flood、DNS Reply Flood、DNS Amplification、SSDP Amplification、NTP Amplification、Chargen Amplification、SNMP Amplification、Jenkins Amplification、WSDD Amplification、COAP Amplification、Memcache Amplification、ARMS Amplification、CLDAP Amplification、MS SQL Amplification 及混合类型攻击进行检测、告警并防护。

◎设备具备针对缓存 DNS 服务器及授权 DNS 服务器专用的 DNS 防护手段，至少 4 种。

◎设备具备正对 DNS 查询防护以及 DNS 响应防护的能力。

◎设备具备针对 HTTP Get Flood 攻击具备不少于 9 种专有防护手段，能够对 HTTP 进行解码。

◎设备具备针对 HTTP POST Flood 攻击专有防护算法。

◎支持肉鸡防护，通过对源 IP 的 URL 访问比例进行统计防护肉鸡攻击。

◎支持 TCP/UDP 反射规则防护。

◎设备具备对不同类型的 url 请求合法性进行验证，实行不同的防护策略，可防御 CC 及变种的能力。

◎设备具备对连接耗尽型攻击的防御能力。

◎设备提供过滤功能，支持白名单、群组黑名单、全局黑名单、群组 ACL、全局 ACL、正则表达（同时支持 TCP 和 UDP 协议）、GeoIP 功能。

◎设备提供 GeoIP 库，并且支持按照国家进行过滤，国内支持按省/直辖市/地区进行过滤。

◎支持 URL 访问控制规则等多种分组过滤方式。

◎支持基于 UDP 的 payload 长度和规律提供检查和防护。

◎UDP 防护支持多种检查和限速方式，包括最小包长、最大包长、源 IP+ 源端口限速、源 IP 限速、目的 IP+ 目的端口限速、目的 IP+ 源端口限速、目的 IP 限速。

◎可以根据 TCP 的标志位进行信任源 IP 限速。

◎支持对空连接进行检测和防护。

◎支持 SIP 防护。

网络安全专用产品安全认证或安全检测结果证明

（1）网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00498-A

★有效期：2023 年 12 月 29 日至 2025 年 12 月 29 日

（2）计算机信息系统安全专用产品销售许可证

★证书编号：402230684

★有效期：2023 年 03 月 31 日至 2025 年 03 月 31 日

所属品牌：绿盟科技

发布时间：2002 年

产品适用领域：全行业

产品照片：



奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址: www.qianxin.com

电话: 95015

地址: 北京市西城区西直门外南路 26 号院 1 号楼

产品名称: 网神 SecDDoS 3600 抗拒绝服务系统

产品概述

网神 SecDDoS 3600 抗拒绝服务系统主要职责就是抵御 DDoS 攻击行为，通过对流量的分析和识别，检测流量中的各种 DDoS 攻击行为，使用阈值限制，流量算法、识别验证等多种方式识别 DDoS 流量，高效的抵御 DDoS 攻击和保障用户网络的完整性和可靠性。

功能特点

◎阈值防护

抗拒绝服务系统也使用标准的“阈值”理论。针对 TCP、UDP、ICMP 等协议进行数据包流量限制。针对 HTTP 流量使用连接数阈值限制等流量限制方式进行 DDoS 攻击防御。

◎自动识别攻击

针对应用层的 CC 攻击时，使用切入页面防护手段进行防御。僵尸网络、CC 攻击器都是电脑系统，无法输入验证码、验证页面等手段来验证攻击行为，自识别僵尸网络、CC 攻击等威胁行为。

◎旁路协调防御

抗拒绝服务系统旁路部署与流量分析器实现联动，流量分析器对流量进行镜像分析。当发现攻击行为自动通过 BGP/OSPF 等路由协议牵引流量至抗拒绝服务系统进行流量分析。旁路分析与清洗实现协同防御理念是完全自动化。

技术指标

◎阈值限制

对流量限制和保障等多种限制机制抵御 DDoS 攻击。

◎验证识别

使用验证手段，抵御僵尸网络、攻击器的应用层 DDoS 攻击。

◎规则匹配

通过“正则分配”技术对流量的特征进行匹配过滤抵御 DDoS 攻击。

◎端口保护

对制定端口协议进行过滤和保障，抵御 DDoS 攻击行为

◎双协议栈

随着 IPv6 的高速普及，抗拒绝服务系统支持双协议栈过滤，通过对 IP 地址的识别，自动区分是 IPv4 还是 IPv6 协议，快速适应网络的高速发展需求和 DDoS 防御需求。

◎独立防护算法

抗拒绝服务系统具备独立防护算法，包含连接代理、数据转发、内核防护、数据挖掘等防护算法。防护算法主要是抵御来自网络层、应用层的 DDoS 攻击。

◎自识别攻击

针对应用层的 CC 攻击时，使用切入页面防护手段进行防御。僵尸网络、CC 攻击器都是电脑系统，无法输入验证码、验证页面等内容。采用 Web protection Based On Page Injection 即基于页面插入式 Web 防护算法。对于开启防护的 Web 服务器，防护模块会主动插入 Web 页面，客户端可无察觉的自动完成验证过程，已达到高效的防御 Web 类连接攻击的目的。

◎集群防御

抗拒绝服务系统支持扩展集群方式，针对流量不断扩展的同时，与老旧设备形成集群扩展部署方式，旧设备与新设备形成一个整体的防御体系。采用 Extensible Firewall Cluster Mode 即可扩展的集群模式，通过领先的数据分流技术，使得若干设备可组合形成更大的防护主体，提供海量攻击的防护解决方案。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402230940

★有效期：2023 年 4 月 28 日至 2025 年 4 月 28 日

所属品牌：奇安信网神

发布时间：2014 年

产品适用领域：全行业

产品照片：



产品咨询二维码

产品咨询邮箱：kefu@qianxin.com

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高速增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

网址：<https://www.venustech.com.cn/>

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号

产品名称：抗拒绝服务系统

产品概述

天清 ADM/网御 TAM 是启明星辰公司自主研发的抗拒绝服务系统，能够对分布式拒绝服务攻击（DDoS）实时有效地进行检测和防护，是互联网安全第一道防线！

天清 ADM/网御 TAM 包括有清洗（GUARD）、检测（DETECTOR）、管理（MANAGER）三个组件，即可单独使用，也可组合使用实现三位一体抗 DDoS：

清洗设备（GUARD）：串行部署或旁路部署，实现 DDoS 攻击过滤、异常流量清洗处理等功能，单机最大防护能力达 200G，并可通过集群无限扩容，是抗 D 产品最核心组件。

检测设备（DETECTOR）：旁路部署，通过收集 flow 数据实现异常流量检测，快速、自动地将异常流量牵引至清洗设备进行清洗。

管理设备（MANAGER）：可统一管理多台清洗（GUARD）设备和检测（DETECTOR）设备，实现策略下发、日志收集和报表分析等，简化了多台设备的管理配置，实现全网抗 DDoS 统一管理。

功能特点

◎抗拒绝服务系统能够对分布式拒绝服务攻击（DDoS）实时有效地进行检测和防护，是互联网安全第一道防线！

◎抗拒绝服务系统有清洗（GUARD）、检测（DETECTOR）、管理（MANAGER）三个组件，即可单独使用，也可组合使用实现三位一体抗 DDoS：

◎清洗设备（GUARD）：串行部署或旁路部署，实现 DDoS 攻击过滤、异常流量清洗处理等功能，单机最大防护能力达 200G，并可通过集群无限扩容，是抗 D 产品最核心组件。

◎检测设备（DETECTOR）：旁路部署，通过收集 flow 数据实现异常流量检测，快速、自动地将异常流量牵引至清洗设备进行清洗。

◎管理设备（MANAGER）：可统一管理多台清洗（GUARD）设备和检测（DETECTOR）设备，实现策略下发、日志收集和报表分析等，简化了多台设备的管理配置，实现全网抗 DDoS 统一管理。

技术指标

清洗设备从 1Gbps 到 200Gbps

检测设备从 8 万 fps 到 160 万 fps

网络安全专用产品安全认证或安全检测结果证明

（1）网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00080-A

★有效期：2024 年 1 月 19 日至 2026 年 1 月 19 日

（2）网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00079-A

★有效期：2024 年 1 月 19 日至 2026 年 1 月 19 日

所属品牌：启明星辰、网御星云

发布时间：2012 年、2007 年

产品适用领域：运营商、政府、企业、金融、公安等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<http://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信异常流量管理与抗拒绝服务系统

产品概述

天融信公司自主研发的天融信异常流量管理与抗拒绝服务系统（TopADS）是专业的抗拒绝服务攻击产品，它能够从纷杂的网络背景流量中精准地识别出各种已知和未知的拒绝服务攻击流量，并能够实时过滤和清洗，确保网络正常访问流量通畅，是保障服务器数据可用性、网络可达的安全产品。

TopADS 具有在线串接、旁路检测和旁路清洗三种工作模式，既可以单台设备在线串接方式部署，也可以两台设备分别进行检测和清洗工作。能够检测与防御流量型 DDOS 攻击（如 UDP Flood、TCP SYN Flood 等）、应用型 DDOS 攻击（如 CC、DNS Flood、慢速连接耗尽等）、DOS 攻击（如 Land、Teardrop、Smurf 等）、非法协议攻击（如 IP 流、TCP 无标记、无确认 FIN、圣诞树等）四大类拒绝服务攻击。TopADS 产品还具有流量牵引和回注、数据包过滤、攻击报文取证等功能，支持双机热备和集群，并提供了详尽的攻击事件记录、各种统计报表，并以可视化方式动态展示，实现实时的全网威胁监控，是适用于政企网、电商、网游、电信骨干网、IDC 网络和云计算中心的理想的抵御拒绝服务攻击的安全产品。

功能特点

◎超高清洗能力

TopADS 产品基于本地单台设备防护的基础上可灵活弹性扩容，为客户提供高达 T 级清洗性能，实现超高流量秒级响应，快速阻断 DDoS 攻击。同时 TopADS 产品支持形成“端 + 云”的联动防护，云防护能力加持，实现全自动云地清洗切换，从而专注于全域级大规模攻击流量的检测清洗和强制防御。

◎全面防护引擎

系统在传统的代理、探测、反弹、信誉机制及报文合规等标准技术上，对违反协议规则的攻击流量进行阻断。同时结合多模式源认证、七层应用分析及行为模式分析等多种特有的攻击智能分析与防护手段，深层次抵御网络层到应用层的各种 DDoS 攻击，为用户构建更完善、更安全的全方位保护屏障。

◎精细业务保障

系统精确到基于具体应用层协议的业务防护对象进行细粒度匹配，专注于增强业务的应用层保护。当流量流经产品后，依据策略防护原则优先匹配最为精细的业务防护对象，涵盖解决具体业务的应用层及关联网络层、传输层的能力，保障业务平稳运行。

技术指标

◎行业

性能参数：清洗性能：4Gbps，小包防御能力（64 字节 /pps）：592 万 pps，最大保护服务器数量：200 台，最大 flow 数据处理能力：300,000Flow/ 秒

◎国产

性能参数：清洗性能：10Gbps，整机网络层吞吐：19479Mbps（1518 字节），整机应用层吞吐：9600Mbps，整机 TCP 最大并发：1000W，整机 TCP 最大新建：25w/s

网络安全专用产品安全认证或安全检测结果证明

（1）网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00343-A

★有效期：2023 年 11 月 24 日至 2025 年 11 月 24 日

（2）计算机信息系统安全专用产品销售许可证

★证书编号：0402220882

★有效期：2022 年 06 月 09 日至 2024 年 06 月 09 日

所属品牌：北京天融信网络安全技术有限公司

发布时间：2013 年 1 月

产品适用领域：政府、运营商、企业集团等行业

产品照片：



产品咨询二维码



行业：TopADS V3



国产：TopADS(HG-B20)（万兆）V3

产品咨询邮箱：feng_chong@topsec.com.cn

网宿科技股份有限公司

网宿科技股份有限公司成立于 2000 年，2009 年于深交所创业板首批上市（300017），是全球领先的信息基础设施平台服务提供商，业务遍及全球 70 多个国家和地区。公司始终致力于助力产业数字化转型升级，满足用户随时随地、安全、可靠的数据处理及交互需求。

公司专注于边缘计算、云分发、云安全、云计算、云服务及绿色数据中心业务，帮助企业技术创新实践，是产业数字化转型升级值得信赖的合作伙伴。

公司现有员工 2300 余人，在厦门、深圳、韩国首尔、美国硅谷等四地设立研发中心，研发技术人员占比 55%。

网址：<https://www.wangsu.com/>

电话：400-010-0617

地址：上海市嘉定环城路 200 号

产品名称：网宿 DDoS 云清洗

产品概述

网宿 DDoS 云清洗（DDoS Mitigation Service，简称 DDOS 云清洗），依托 CDN 资源优势，结合大数据分析，自主研发防护算法，实时检测并清洗各类 DDoS 攻击（如 SYN Flood、UDP Flood、CC 等），保障基于 HTTP/HTTPS 的用户业务在遭遇大流量 DDoS 攻击时仍然能够稳定在线。

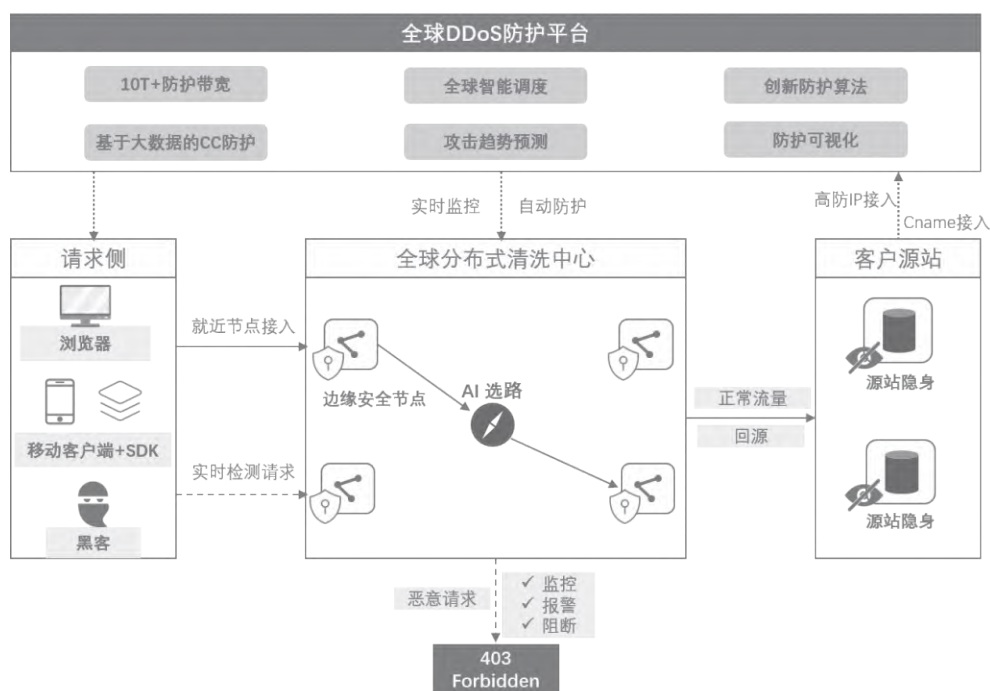
目前网宿 DDoS 云清洗单节点抗攻击能力可达 800Gbps，同时 DDOS 云清洗的智能调度中心能够根据攻击情况智能调度全网资源，总体抗攻击能力达到 15Tbps+。

功能特点

网宿 DDOS 云清洗依托全球部署的云安全节点联接形成云安全网络，并配以专有的攻击监控报警中心和智能调度中心，结合云端大数据分析平台，实时检测分析请求包，如发现异常请求则拦截，并根据攻击情况实时动态调整防护策略，有效保障用户平台安全。网宿 DDOS 云清洗产品架构如图所示：

◎网络层 DDoS 防御

网络层 DDoS 攻击是攻击者通过伪造大量 IP 地址向目标服务器发起大量数据包，耗尽网络带宽资源进而导致目标服务器无法响应正常的请求。常见的网络层 DDoS 攻击包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、各类反射攻击（如 NTP 反射、Memcache 反射、SSDP 反射）等。



网宿 DDoS 云清洗通过部署智能防火墙，实现对数据报文的实时检测和分析，在不影响正常数据报文访问的前提下，实时高效阻断攻击报文。DDoS 云清洗单节点防护容量达 800Gbps，平台总体防护能力达 15Tbps+。目前可有效防御 SYN Flood、UDP Flood、ICMP Flood、NTP 反射攻击、SSDP 反射攻击、Memcache 反射攻击等各类网络层 DDoS 攻击。

◎应用层 DDoS 防御

网宿 DDOS 云清洗通过威胁情报库、访问控制、日志自学习、人机校验等方式实现对请求包实时检测和分析，在不影响正常访问的前提下，实时高效阻断恶意请求，单机防护性能达 1000 万 QPS，平台总体防护能力达 10 亿 QPS。目前可防御 CC、HTTP Flood、慢攻击等各类常见的应用层 DDoS 攻击。

◎大数据驱动防护

通过端（客户端采集的数据）、网（边缘节点的接入流量数据）、云（网宿平台自生产的情报数据）为决策引擎提供了丰富的攻击数据基础。网宿平台服务了 8 成以上的全国网民，每日承载万亿级的请求数，每天攻击样本超过 30 亿，为中心智能引擎的攻击分析和决策提供丰富的数据基础。

实时行为模型和机器学习，能够快速识别动态变化的攻击模式，并相应地生成防护策略，使得平台能够更准确地检测和组织各类攻击。

通过统一、实时的汇聚的动态攻击数据，驱动云边（边缘 & 中心）双引擎协同防护和持续对抗，提升平台应对各类攻击威胁的防护水位。

技术指标

◎产品能够进行网络层 DDoS 防护

防护类型：能够防护常见的网络层 DDos 攻击包括 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、各类反射攻击（如 NTP 反射、Memcache 反射、SSDP 反射）等；

防护性能：单节点防护容量达 800Gbps，平台总体防护能力达 15Tbps+；

网络层攻击预警：网宿 DMS 为每个客户提供一组独立 IP 服务，因此能够以客户为粒度实时采集并统计客户对应服务 IP 的网络层攻击带宽，当网络层攻击到达客户设置的攻击带宽阈值时，将通过邮件 / 短信形式向客户报警，报警信息包括攻击时间、攻击峰值等；

◎产品能够进行应用层 DDos 防护

防护类型：能够防护常见的应用层 DDos 攻击包括 CC 攻击、HTTO Flood 攻击、慢连接攻击等；

防护性能：单节点防护性能达 1000 万 QPS，平台总体防护能力达 10 亿 QPS。

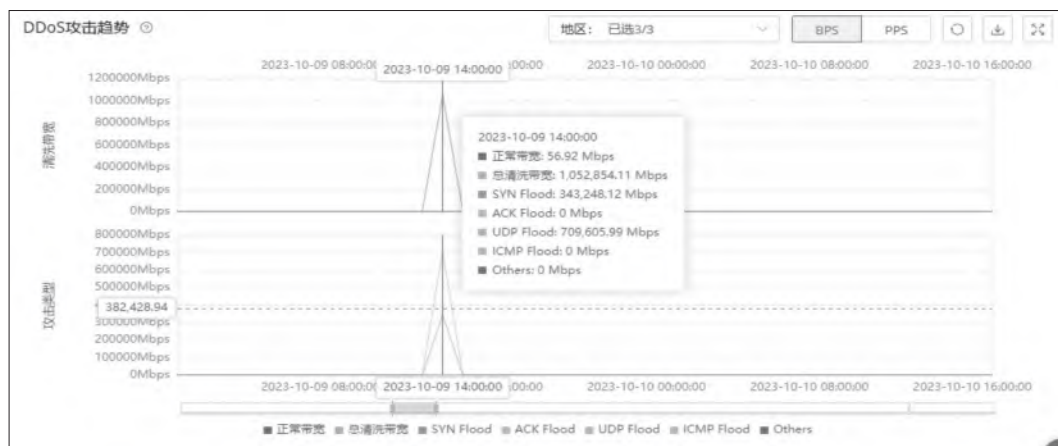
应用层攻击预警：网宿 DMS 各安全节点通过动态学习客户的历史访问日志（如客户每个资源的访问量、行为特征等），建立动态访问基线，当检测到异常访问时，根据报警规则（如 QPS 设置的阈值）通过邮件 / 短信形式向客户发送相应攻击报警。

◎防护数据可视化

1) 展示某段时间 DDos 攻击峰值，并实时展示清洗带宽和正常带宽；



2) 展示清洗流量类型



3) 曲线图形式展示 CC 攻击 QPS



4) 以攻击事件形式展示攻击 IP、所属区域、攻击时间、攻击域名等

攻击事件	状态	开始时间	结束时间	持续时间(min)	峰值时间	被攻击域名	攻击次数
1	清洗结束	2023-10-31 10:44:00	2023-10-31 10:46:00	2	2023-10-31 10:45:00		15,280
2	清洗结束	2023-10-31 10:08:00	2023-10-31 10:12:00	4	2023-10-31 10:10:00	www. .com	28,846
3	清洗结束	2023-10-31 05:26:00	2023-10-31 05:27:00	1	2023-10-31 05:26:00	.com	7,778
4	清洗结束	2023-10-31 04:50:00	2023-10-31 04:51:00	1	2023-10-31 04:50:00	www. .c...	6,274
5	清洗结束	2023-10-31 04:37:00	2023-10-31 04:39:00	2	2023-10-31 04:38:00	www. .com	15,508
6	清洗结束	2023-10-31 04:36:00	2023-10-31 04:38:00	2	2023-10-31 04:37:00	.com	16,607
7	清洗结束	2023-10-31 02:27:00	2023-10-31 02:28:00	1	2023-10-31 02:27:00	.com	6,576

5) 提供被拦截的 IP 详细信息, 包括 IP 所在地、攻击类型、攻击次数等, 以利于客户对后续对攻击者的处理;

2023-10-02 ~ 2023-10-31 域名: 已选564/564 查询

受攻击域名列表
受攻击URL列表
攻击源IP列表
触发策略统计

攻击源IP列表 提示: 默认按照缓解次数降序排列

攻击源IP 攻击地图

攻击IP	地理位置	请求次数	缓解次数	告警次数	缓解占比	告警占比
5...18	中国大陆 江苏	14,371	14,349	0	99.85%	0.00%
221...226	中国大陆 江苏	13,275	13,229	0	99.65%	0.00%
182.4...249	中国大陆 北京	11,220	11,220	0	100.00%	0.00%
115...197	中国大陆 湖北	11,444	10,653	0	93.09%	0.00%

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号: 0402230832

★有效期: 2023 年 4 月 21 日至 2025 年 4 月 20 日

所属品牌: 网宿安全

发布时间: 2012 年 12 月

产品适用领域: 政府、金融、制造业、能源、电商、企业等

产品照片:



网宿科技



网宿产品与服务

产品咨询邮箱: wengz1@wangsu.com

亚信安全科技股份有限公司

亚信安全是中国网络安全软件领域的领跑者，是业内“懂网、懂云”的网络安全公司。承继亚信 30 年互联网建设经验，肩负守护互联网之使命，亚信安全于 2015 年正式启航，目前已成为建设中国网络安全的重要力量。不负使命，成功执行建党 100 周年、历年两会等国家重要网络安全保障任务 30 余次。

依托互联网建设能力，让亚信安全具备强大的“懂网”业务能力与资源优势；深耕网络安全高精技术，让亚信安全拥有优异的“懂云”技术基因。亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理及 5G 安全等领域突破核心技术，用实力筑牢云、网、边、端之安全防线。

亚信安全在中国网络安全电信行业细分市场份额占比第一，连续五年蝉联身份安全中国市场份额第一，终端安全中国市场份额占比第二，在威胁情报、EDR、XDR 等细分技术领域均居于领导者象限，是中国网络安全企业 10 强。

秉承建网基因，坚守护网之责，亚信安全以护航产业互联为使命，以安全数字世界为愿景。

2020 年提出“安全定义边界”的发展理念，以身份安全为基础，以云网安全和端点安全为重心，以安全中台为枢纽，以威胁情报为支撑，构建“云化、联动、智能”的技术战略，守护亿万家庭和关键信息网络，建设全网安全免疫系统，为我国从网络大国向网络强国迈进保驾护航。

网址：www.asiainfo-sec.com

电话：400-820-8876

地址：江苏省南京市雨花台区花神大道 98 号东久创新中心 1 号楼

产品名称：亚信安全信舷抗拒绝服务系统

产品概述

亚信信舷抗拒绝服务系统（简称 AISADS）是一款专业的网络安全设备，旨在为帮助政企、运营商、金融机构等组织保护其网络基础设施免受分布式拒绝服务（DDoS）攻击的影响。

亚信信舷抗拒绝服务系统硬件基于 X86 多核平台，软件采用 DPDK 高性能架构，应用自主研发的抗拒绝服务攻击引擎，嵌入世界领先的数据流指纹检测技术；可全自动防御 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、IP Flood、混合攻击等各类 DDoS 攻击。亚信信舷抗拒绝服务系统集成 WEB、GAME、DNS、CT 等多种智能防御插件引擎，可轻松防御各类针对 HTTP、DNS、游戏业务等应用类攻击及 CC 攻击，结合可编程的特征码自定义策略，实现针对未知攻击的有效防御。

功能特点

◎智能防御 无需人工干预

系统内集成 SYN、UDP、ICMP、TCP、IP 攻击防御引擎。整合了公司 20 余年的防护经验，可防护互联网上 99.99% 的 DDOS 流量攻击。并且系统默认会对经过防火墙的每一个服务器自动开启全局防护，完全不需人工干预。

◎部署灵活 无场景限制

设备支持串联部署（透明部署）、旁路动态引流部署、旁路静态引流部署，支持等同模式无限制集群扩展；

串联部署：

组网简单，实施阻断攻击

部署在网关之后支持透明接入

旁路动态引流部署：

不影响原有网络架构，维护简单

只将攻击流量引到清洗设备清洗，避免大流量场景下，全流量处理耗费转发性能

逐包检测清洗，秒内响应攻击

旁路静态引流部署（旁路常住模式）：

静态引流回注，毫秒级攻击响应速度

静态引流可提高引流性能，尤其对于扫段攻击，防护效果显著

◎高效过滤 线速处理

抗拒绝服务系统采用 dpdk 架构设计，硬件搭配 intel 至强系列处理器，提供线速转发处理性能；防御引擎由《DataStreamFingerprintInspection》技术实现，具有攻击实时发现、零误判断、零穿透等诸多特性。

◎高可扩展 无限制集群

抗拒绝服务系统采用 x86 通用硬件，保证可计算平台的高性价比和易于升级的特性。

系统采用松耦合的模块化设计，在各层次上提供一个保障核心，很大程度的降低了系统的复杂度，提高了可维护性，稳定性，可扩展性。

核心模块，提供清洗设备核心网络处理模块，所有网络处理单元都以模块形式加载到主核心中，实现了高度的功能可扩展性。

服务层，基于面向对象原理实现了接口发布核心，所有功能以接口形式发布出来，并透明的实现本地访问和各种网络协议的接口访问。最大程度的实现了服务层的伸缩性。

WEB 层，为用户提供的 WEB 界面同样采用模块化得设计，每个模块一个发布包，易于升级和扩展。

技术指标

抗拒绝服务系统系统是一种网络安全产品，用于检测和清洗异常流量，防止网络攻击对系

统造成损害。以下是抗拒绝服务系统系统的典型产品架构：

◎清洗节点（Scrubbing Nodes）：具备强大的计算和网络处理能力，用于接收流量并进行深度分析和清洗操作。清洗节点通常采用分布式架构，可以水平扩展以处理大量的流量请求。

◎流量分析引擎（Traffic Analysis Engine）：负责对流量进行实时分析和检测，识别异常流量和攻击行为。流量分析引擎使用各种技术和算法，如行为分析、机器学习和规则引擎，以识别不同类型的攻击，如 DDoS、恶意请求、SQL 注入等。

◎清洗引擎（Scrubbing Engine）：当流量被标识为异常或恶意流量时，清洗引擎会对其进行清洗操作，过滤掉恶意内容或将流量重定向到安全环境进行进一步分析。清洗引擎可以采用多种技术，如包过滤、协议分析、反向代理等。

◎日志与报告模块（Logging and Reporting Module）：负责记录系统的运行日志和生成详细的报告。日志可以用于后续的分析和审计，报告则提供给管理员和安全团队以便查看系统的健康状况、检测到的攻击和采取的防御措施等信息。

◎管理与配置界面（Management and Configuration Interface）：提供用户界面用于配置和管理整个抗拒绝服务系统系统。管理员可以通过界面对系统进行监控、配置清洗规则、查看报告和日志等操作。

总体而言，抗拒绝服务系统系统的产品架构结合了分布式清洗节点、流量分析引擎、清洗引擎、日志与报告模块、管理与配置界面，形成一个完整的抗拒绝服务系统解决方案。该架构通过分布式的清洗节点和强大的流量分析引擎，能够高效地检测和清洗异常流量，保护网络系统的安全和可用性。

在实际部署中，可以根据具体需求和规模进行扩展和定制。例如，可以增加更多的清洗节点以处理更大的流量负载，或者将清洗节点部署在不同的地理位置以提高服务的可靠性和响应速度。另外，可以根据具体的安全需求定制流量分析规则和清洗策略，以适应不同类型的攻击和威胁。

抗拒绝服务系统系统的产品架构提供了全面的异常流量检测和清洗能力，并且可以与其他安全产品和系统进行集成，形成一个综合的安全防护体系。通过实时的流量分析和清洗操作，抗拒绝服务系统系统可以有效地保护网络系统免受各种网络攻击的威胁，提高网络的安全性和可靠性。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402231164

★有效期：2023 年 05 月 19 日至 2025 年 05 月 19 日

所属品牌：亚信安全

发布时间：2023 年 4 月 06 日

产品适用领域：政府、医疗、金融、电力、工业

产品照片：



产品咨询二维码

产品咨询邮箱：xu.yh@asiainfo-sec.com

远江盛邦（北京）网络安全科技股份有限公司

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全，股票代码：688651）成立于2010年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为用户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。公司秉持精准识别、精确防御、深入场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图等领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能各行业用户的数字化安全转型，护航国家网络空间安全战略实施落地。

网址：<https://www.webray.com.cn>

电话：4006-911-199

地址：北京市海淀区上地九街9号2层209

产品名称：异常流量清洗与抗拒绝服务系统（RayADS）

产品概述

异常流量清洗与抗拒绝服务系统（RayADS）是盛邦安全针对分布式拒绝服务攻击（DDoS）推出的专项防护产品。分布式拒绝服务攻击的主要目的是造成目标主机的TCP/IP协议层拥塞，导致应用层异常终止而形成拒绝服务的现象。强大的攻击工具批量出现，导致DDoS攻击数量更多、类型更加多样，更加难以识别。传统网络设备或者边界安全设备，诸如防火墙、入侵检测系统，都有各自的功能和性能瓶颈，无法做到对DDoS攻击的有效清洗防护。

异常流量清洗与抗拒绝服务系统（RayADS）基于自主研发的操作系统，采用全新的数据采集模型，对经过流量进行分发调配，并配合多核处理架构合理利用系统资源，提升自身处理和清洗能力。同时，通过多样的DDoS识别和二次验证算法，提升事件的检出能力和准确性。

功能特点

◎精确的攻击检测及防护

多种智能防护算法，30多种攻击类型，全面清洗各类DDoS攻击，快速应对未知的DDoS攻击类型，并内置多种策略模板，降低策略难度，提高运维效率。

◎全量逐包检测

异常流量清洗与抗拒绝服务系统从底层系统架构出发，对系统资源处理进行优化，创新性地采用了全量逐包检测引擎，直接对原始报文进行分析，记录完整行为，并将资源利用率控制在20%以下。在大型网络出口中可以合理分配自身性能，并更加精准的定位DDoS攻击。

◎多重验证算法

对于僵尸主机或恶意代码发出的页面请求或 GET/POST 包，异常流量清洗与抗拒绝服务系统可以通过反向验证算法及 HTTP 自身的 301 特性来组合判断请求发起者是否为正常主机，提升检出准确率。

◎流量限速

异常流量清洗与抗拒绝服务系统采用智能识别算法结合动态基线学习技术，从行为分析的角度出发，构建攻击模型，绘制流量基线模型，并根据报文状态自动调整，从而有效的过滤 DDoS 告警，减少误报。

◎双栈兼容防护

异常流量清洗与抗拒绝服务系统全面支持纯 IPV4、纯 IPV6 以及 IPV4 和 IPV6 混合的业务流量防护。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402220802

★有效期：2023 年 05 月 19 日至 2024 年 05 月 19 日

所属品牌：盛邦安全

发布时间：2022 年 05 月 19 日

产品适用领域：

电力能源、金融、运营商、医疗、教育、政府、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：support@webray.com.cn

中新网络信息安全股份有限公司

中新网络信息安全股份有限公司（以下简称“中新网安”）成立于 2002 年，总部设在合肥，是一家专注于网络安全技术研究、网络安全产品软硬件研发、网络安全服务的高科技企业。

中新网安以“致力于网络空间信息安全守护者”为企业愿景，定位信息安全守护者，重点围绕国家关键基础设施（通信、交通、能源等）；重要信息系统（金融、党政、财税等）；重要公众服务（互联网+政务、互联网+医疗、互联网+民生等）；重要监管单位（公安部、工信部、国家互联网应急响应中心、中国信息安全测评中心、等级保护测评中心等）为服务对象，秉承务实、正直、进取、创新的态度，为客户提供专业的信息安全一体化服务，与用户共创并享受安全、和谐、美好的网络空间。

网址：www.cnzxsoft.com

电话：0551-65178555

地址：安徽省合肥市高新区创新大道 2688 号中新网络安全研究中心

产品名称：中新金盾抗拒绝服务攻击系统 ZX-DMS V9.0

产品概述

中新金盾抗拒绝服务系列产品是中新网安核心的抗分布式拒绝服务攻击（DDoS）高性能解决方案。通过部署在网络边缘检测、阻挡并缓解多向量 DDoS 攻击。最新型的金盾抗拒绝服务系统端设备更可以和中新网安的金盾云清洗中心联动，是企业网络基础设施对抗流量型攻击的第一道防线。

功能特点

防御类型、应用层协议防护、CC 攻击防护、专业的 DNS 服务器防护能力、特定服务防护、算法调整、防护特性、端口过滤、内容过滤、自定义限制、连接跟踪、自动检测、黑白名单、分级设置、自动抓包、自动捕获、异常流量抓包、显示功能、统计功能、监控功能、牵引方式、回注方式、日志显示、日志保存、分级分权、管理方式、远程管理、统一管理、规则匹配、预定义、IP 访问、黑白名单、需求定制。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402230352

★有效期：2023 年 2 月 24 日至 2025 年 2 月 24 日

所属品牌：中新网安

发布时间：2015 年

产品适用领域：能源、政府、金融

产品照片：



产品咨询二维码

产品咨询邮箱：guoxiaoxi@cnzxsoft.com



终端接入控制产品

北京猎鹰安全科技有限公司

北京猎鹰安全科技有限公司（原金山安全）是猎豹移动、绿盟科技、安天科技等国内知名安全企业共同投资成立的国内领先的互联网安全技术与云安全平台解决方案提供商，是拥有完全自主知识产权的中国信息安全企业。北京猎鹰安全科技有限公司以“全面保障数字化环境安全”为企业使命，协助政府、军队、大型集团化企业和专用网络等企事业单位，构建专属的终端信息安全保障体系。

网址：www.ejinshan.net

电话：010-82663885

地址：北京市海淀区中关村大街 27 号中关村大厦 1112 室

产品名称：猎鹰安全 FNAC 网络准入系统 V9.0

产品概述

猎鹰安全 FNAC 网络准入系统 V9.0 是猎鹰安全自主开发的新一代集成化终端安全管理平台，是基于最先进的第三代准入控制技术的网络准入控制系统。

采用 B/S 架构，管理员通过 HTTPS 方式进行远程管理。授权用户连接网络时需进行身份鉴别，鉴别成功并且通过安全状态检查后，接入指定区域。该产品可实现接入用户控制、终端安全状态检查、响应方式控制、策略管理、终端用户管理和区域配置管理等功能。

功能特点

◎清晰的边界划分

猎鹰安全 FNAC 网络准入系统 V9.0 提供桥接、PBR (Policy-Based-Routing)、MVG (Multi-Vendor Gateway) 等各种准入技术实现方案。系统支持内置身份认证，外部 Email、Radius、LDAP、AD 域、短信、指纹、CA 系统、USB KEY 等多种认证方式。并且在认证基础上提供完善的角色、安全域、来宾权限管理，使终端具有清晰的网络边界。

◎广泛的网络适应

猎鹰安全 FNAC 网络准入系统 V9.0 兼容各种终端和网络设备，广泛适应异构系统、BYOD(Bring Your Own Device)、BYON(Bring Your Own Network) 的应用。采用先进的设备特征采集技术，能自动识别包括交换机、路由器、PC、智能终端等在内的多种设备，并对设备进行标示和固定。

◎安检策略丰富完善

猎鹰安全 FNAC 网络准入系统 V9.0 具备丰富的安全检查规范库。根据猎鹰安全科技多年来

在入网规范领域的经验总结，系统还提供了符合行业特征的安全规范，方便用户快速部署。

◎安全定位灵活多样

系统提供一个全网安全管理和展示的平台，能够对全网拓扑和设备状态进行展示。并提供快速定位网络设备或终端的手段。

◎安全功能持续扩展

猎鹰安全 FNAC 网络准入系统 V9.0 基于模块化的设计。客户可根据自身网络的需求，定制符合自己要求的功能或模块。

◎弹性化客户端

猎鹰安全 FNAC 网络准入系统 V9.0 提供弹性化的客户端，以满足不同客户的需求。客户可根据自己的需要，在自己网络内部署零客户端、自消融客户端、完全客户端等不同形式。

◎支持分布式部署

ASC（Access Standard Controller）适用于复杂网络或规模分支机构情况，可有效的分担核心设备的负荷，同时避免由于网络时延给终端用户带来的不愉快体验。

◎高可靠的自身安全性

猎鹰安全 FNAC 网络准入系统 V9.0 部署在自主开发的安全操作系统和高可靠性的硬件平台之上，并支持监控平台、自逃生、双机热备、Bypass（桥接模式下）等可靠性技术。

◎简单易用的用户操作

猎鹰安全 FNAC 网络准入系统 V9.0 服务器端提供友好的交互界面，系统设置、策略部署、日志统计全部在网页上进行。在终端用户侧，猎鹰安全 FNAC 网络准入系统 V9.0 采用自动安全检查和一键式修复，免除繁琐的操作培训。

◎完全支持智能终端

猎鹰安全 FNAC 网络准入系统 V9.0 支持包括 iOS、Android 在内的多种智能终端，让 BYOD 成为现实，让移动办公成为可能。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01582-A

★有效期：2024 年 10 月 25 日至 2026 年 10 月 25 日

所属品牌：猎鹰安全

发布时间：2024 年 10 月

产品适用领域：政府、军工、能源、金融、教育、医疗及企事业单位等

产品照片：



产品咨询二维码

产品咨询邮箱：wangzhiyong@ejinshan.net

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业 and 国家专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区上地东路 1 号院华控大厦 7 层

产品名称：网络接入控制系统

产品概述

网络接入控制系统基于先进的零信任理念即永不信任、始终验证原则，通过设备精准识别、准入认证、安全检查、信息自画像、行为可视化、安全告警、违规智能阻断、网络链路可视化等功能，实现对网络内终端主机、BYOD 设备、物联网设备、服务器、安全设备等各种资产进行准入控制，规范终端设备接入机制及流程，实现终端设备认证、权限及访问控制的一体化管理，从而确保接入网络终端设备合法、合规、可信。

功能特点

◎智能化设备识别与认证

采用被动监听、主动探测、行为建模等多种技术，构建智能化指纹特征采集引擎，利用少量特征信息，即可自动识别和控制各种接入终端。

◎全面的网络准入技术

准入技术依靠 DHCP、策略路由、透明网桥、802.1x 实现对网络的准入控制，支持基于企业当前网络和网络安全等级场景灵活部署合适的准入技术，从而大大提高网络适应性产品。

◎多维度终端网络边界管控

系统通过大数据分析算法和终端行为智能学习模型，自动创建终端访问网络边界规则库。基于终端行为智能学习模型分析结果，自动识别设备部署环境行业类型，并基于行业类型确定终端访问网络边界规则库颗粒度。

◎网络链路可视化管理

多种方式管理网络交换设备，不改变网络物理链路以及逻辑链路；快速生成可视化网络物理链路，以及网络逻辑链路；实现网络终端状态信息、物理链路信息、逻辑链路信息一目了然，告别网络链路手动更新时代。

◎无感知安全认证

针对工业场景的无交互界面终端设备，基于设备指纹识别、工控协议深度解析、自动识别通信业务，实现终端设备无感知安全接入认证。

◎智能联动阻断异常设备

智能分析网络通信数据，自动匹配终端访问网络边界规则库，阻断和告警终端违规网络边界行为；通过终端行为智能学习模型，自动识别和发现终端正常网络业务行为、异常网络行为以及未知可疑行为；发现异常行为或者未知可疑行为进行阻断和告警。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01731-A

★有效期：2024 年 11 月 22 日至 2026 年 11 月 22 日

所属品牌：珞安科技

发布时间：2020 年 9 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业

产品照片：



产品咨询邮箱：support@icssla.com



产品咨询二维码

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 10000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.wincsssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特网络准入系统

产品概述

网络准入系统采用标准机架式 1U/2U 硬件服务器，服务器采用 Linux 操作系统，支持 B/S，C/S 双重管理架构，便利易操作管理设计。网络准入系统在提供多样化的身份认证，保障准入网络人员合法性的同时，支持对设备的实名认证，保障了准入网络终端设备的合法性，从而加强内部网络的可控性，方便管理员对网络的统一管理。客户端系统运行在操作系统底层，对终端计算机网络、设备端口和系统安全配置提供一体化解决方案，同时提供高效的终端运维管理工具，从终端安全威胁源口到上应用操作进行全方位加固，从根本上解决终端计算机信息安全管理难题，保障终端计算机整体安全性。

功能特点

◎安全性高

★隔离阻断更严格

可以做到端口级、边界级阻断，可以做到网络链路层的管控，可以在准入位置第一时间进

行阻断，对比策略路由、透明网桥、端口镜像等网关型准入技术而言更安全；

★多级隔离阻断技术

采用特有的多级阻断技术，对违反安全要求的终端在链路层、网络层、应用层分别进行阻断，并可针对不同安全事件配置不同阻断技术组合，相对于单一阻断技术而言管控更加灵活和严格。

◎兼容性好

★兼容大型复杂网络

采用基于混合准入技术的解决方案，不同网络环境和需求灵活配置不同准入技术组合，无论是交换网还是路由网、交换机是否可网管都能够很好的兼容；

★兼容各种泛终端类型

准入技术不依赖于客户端软件，兼容各类泛终端类型，采用了独特的网络指纹识别技术，通过对泛终端多维指纹特征进行采集，自动生成指纹快照，快速指纹比对算法等技术，实时监测网络中存在的大量泛终端。

◎易用性好

★部署快速

系统几乎对网络零改动，可灵活的分区、分步实施并启用准入策略，部署简单快速。

★可视化管理

系统采用可视化 WEB 管理，屏蔽底层技术细节，对管理员技术门槛要求低。

★引导式入网

系统采用引导式准入理念，管理员无需人工参与入网过程，终端用户自己根据入网提示进行，极大的降低运维工作量。

★自动容灾

系统提供完备的容灾方案，具有无降级容灾、降级容灾等多层容灾技术，当准入系统异常宕机后对网络业务无影响。

◎灵活性好

★混合准入技术

威努特网络准入系统支持多种准入控制技术，比如支持 DHCP 准入控制技术、802.1X 准入控制技术、ARP 准入控制技术、SNMP 准入控制技术、Portal 准入控制技术等，并且支持多种准入技术的混合部署方案。

★无限维度管理

传统安全技术依赖传统的安全控制规则，传统模式下安全规则结构僵化、逻辑复杂，对于日常维护管理产生极大的难度。威努特特有的对象分组技术摆脱了过于单一化的目标定义方式，通过实现对象分组管理，使网络准入系统的入网策略设置更为灵活，逻辑更为清晰。

◎智能化强

在系统结构上，威努特网络准入系统有一个智能大脑模块，这个模块会汇集所有其他模块

提交上来的数据进行分析，就跟人的大脑一样，根据自己的知识库综合得出分析结果，然后再通知其它模块对网络终端做出相应的网络动作。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01362-A

★有效期：2024 年 9 月 13 日至 2026 年 9 月 13 日

所属品牌：威努特

发布时间：2020 年 5 月 30 日

产品适用领域：电力、石油石化、轨道交通、市政、烟草、智能制造等

产品照片：



产品咨询邮箱：support@winicssec.com



产品咨询二维码

福建省海峡信息技术有限公司

福建省海峡信息技术有限公司是国内最早专业从事网络安全自主研发、产品销售及安全服务的公司之一。2022 年 4 月，海峡信息正式成为福建广电网络集团直属单位。海峡信息是国有控股高新技术企业、国家“专精特新”小巨人企业、福建省创新型研发机构、行业领先的网络安全整体解决方案提供商，是福建省唯一通过国家信息安全服务资质安全运营认证、信息安全服务资质二级认证（安全工程 / 风险评估）的企业，2022 年入选福建省重点上市后备企业，在江西、四川、湖北、湖南等地设有办事处及技术支撑机构。

在技术探索领域，海峡信息成立了“两大实验室”和“一中心”，在过去的二十多年里，一直专注于网络安全产品与服务领域。以创新研发和实战攻防为核心，致力于探索网络安全的最新前沿方向。

在科研成果方面，累计获得了福建省、市科学技术进步奖 8 项；发明专利授权 10 项；拥有软件著作权 100 多项。海峡信息独立承担的福建省高新技术重点项目、火炬计划项目及福建省重大招标项目。所有产品均以创新研发和实战攻防为核心，构建了一个基于主动防御、动态防御、精准防护、整体防护的综合防控体系，广泛应用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域。

网址：<https://www.si.net.cn>

电话：0591-87303711

地址：福建省福州市鼓楼区北二环中路 61 号 2 号楼

产品名称：黑盾网络准入控制系统

产品概述

黑盾网络准入控制系统提供多样化的身份认证，杜绝一切非法、未知设备随意接入单位内部网络。保障接入网络人员合法性的同时，支持对设备的安全检查，保障了接入网络终端的合规性，从而加强内部网络的可控性，方便管理员对网络的统一管理。客户端系统运行在操作系统底层，对终端计算机网络、设备接口和系统安全配置提供一体化解决方案，同时提供高效的终端运维管理工具，从终端安全威胁源口到上应用操作进行全方位加固，从根本上解决终端计算机信息安全管理难题，保障终端计算机整体安全性。

功能特点

系统支持旁路、网桥、网关、软件安装服务端等多种部署方式，支持设备多级级联管理。产品兼容多网段、有线\无线 AP、跨 NAT 等复杂网络环境，设备部署过程中不改变原有网络结

构。支持独立或并行使用多种准入方式，独立部署准入控制服务器，单独管理特定网段，搭建网络边界级、端口级、应用级网络阻断控制应用效果。实时验证各种类型的接入终端身份合法性、主机合规性，只有符合入网策略的终端才可入网，构建入网规范化、自动化、流程化，实现“入网必可信、入网必合规”的安全态势。

支持 VARP 准入认证，通过 arp 欺骗原理，在 vlan 下预设虚拟地址，根据监听用户二层网络中的 arp 请求，根据入网规则判断设备是否合法，若为非法设备发起的 arp 请求该请求会被虚拟地址进行多次回复，达到欺骗的效果，终止其与真实目的 ip 的连接请求，从而达到准入控制的效果。

支持策略路由，一种基于终端认证及合规状态而动态进行路由选择的机制。部署时，管控区需要与访问区域处于不同网段，网关需更改原有路由配置，将报文转发至 NAC 设备，NAC 设备通过评估终端的认证及合规状态，选择是继续转发报文、重定向或丢弃，从而对网络内终端穿越边界行为进行管控。

支持镜像准入，流量欺骗或流量过滤的技术，对网络内终端穿越准入防护边界的流量进行检测与控制的方案，支持旁路镜像、策略路由两种设备部署方案，通过监听终端经过准入访问服务器的网络数据流，并做连接跟踪，对内网数据流进行合法性检测并对非法连接进行阻断和控制，保护核心区域访问的安全。它基于用户核心业务保护概念，对非法访问用户核心资源进行访问限制，确认身份的合法后才能正常访问。

系统提供图形可视化管理窗口，快速管理网络内交换机、IP 地址库及网络拓扑图，大屏展示全网资产设备实时状态，包含资产数据分析、资产分类、安全趋势、24 小时态势、关键设备态势及报警信息。支持图形化展现交换机信息，交换机面板显示各交换机端口详细信息，包含交换机品牌、型号、端口信息、VLAN 信息、IP 地址表、转发表、路由表和 ARP 表等细粒度管理。图形化管理全网 IP 地址资源，支持在线、离线、未使用、安全风险、安全阻断分类化显示，支持 IP 地址增加备注信息。结合网络设备不仅建立准入机制，还通过已有的终端与交换机端口对应关系，以视图的方式进行可视化呈现，建立终端快速定位平台，网络设备性能监控平台等功能，对各种进出网产生的安全事件，支持快速定位、可视定位。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01692-A

★有效期：2024 年 11 月 15 日至 2026 年 11 月 15 日

所属品牌：黑盾

发布时间：2021 年 1 月 18 日

产品适用领域：适用于智慧政务、医疗、教育、金融、部队、交通、水利
等关键领域

产品照片：



产品咨询邮箱：chenxf@heidun.net



产品咨询二维码

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟（CCIA）发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神网络安全准入系统

产品概述

奇安信网神网络安全准入系统 (NAC)，采用业界领先的软硬件架构，实现对终端从接入身份识别验证、安全合规评估到违规处置等全生命周期入网管控防护；支持对接入网络边界的发现与控制、避免私搭乱建。基于终端身份与合规结果等条件动态控制终端准入的网络权限，通过网络权限最小化原则，实现网络安全风险最小化。系统支持联动各类安全监测设备，实现对风险设备的有效阻断、隔离、修复等措施，实现全方位、立体的防御体系。。

功能特点

◎全面资产可视化能力

奇安信网神网络安全准入系统 (NAC) 可实现 IT、OT、IoT 全网终端资产发现、识别、全生命周期管理，具备完备的发现识别技术：通过 SNMP/ 广播探查 /nmap/ 流量分析等多种技术手段实现全量终端的发现与识别，内置终端识别指纹库，支持手动添加修改终端指纹库。

◎有 / 无代理合规检查

奇安信网神网络安全准入系统 (NAC) 通过在终端安装客户端实现 IT、OT 的合规检查、修复、通过无客户端扫描技术可实现对 IOT 终端的合规检查。产品支持 IOT 合规检测、联动天擎，实现全 day 病毒查杀后接入网络。

◎安全身份认证

奇安信网神网络安全准入系统 (NAC) 可实现实现员工、访客、驻场服务商等全人员身份的实名认证入网，杜绝非法用户访问。支持短信 / 二维码 / OTP / 证书 / 主机身份 / 双重认证 / 多因素认证等，支持 LDAP/AD/Email/ 企业微信 / 钉钉 / 派拉 / OAuth2/Email 等身份源。

◎全栈准入技术

奇安信网神网络安全准入系统 (NAC) 系统通过判定终端身份、人的身份、合规检查的合法性，判定终端是否可以入网；系统通过对接入网络边界的控制，防止边界非法外延，如私接小路由器。提供基于终端级（主机网络驱动）、交换机接口级（802.1x/MAB/portal）、边界级（旁路流量劫持、DHCP 准入等）、私网 NAT 级（流量水印穿透 NAT）全栈准入技术方案，根据不同场景提供梯次防御能力。

◎基于精细的网络微分段权限控制

奇安信网神网络安全准入系统 (NAC) 系统基于终端可信身份 / 人的身份实现动态的网络权限控制。支持通过 radius 协议下发 VLAN 给 NAS 设备，支持准入设备自身进行 ACL 策略实现网络权限精细控制。

◎协同联动、实现纵深防御

奇安信网神网络安全准入系统 (NAC) 系统联动天擎杀毒 / 零信任 / ICG 单点登录，联动 NGSOC / 攻击面检测 / SOAR / 天眼 / LAS 等实现纵深防御。系统提供用户下线 / 终端身份 / 用户身份等标准南向接口，提供实名入网日志、终端合规日志、资产数据等北向接口。

技术指标

本地用户认证上线（个 / 秒）	>= 1000
最大理论用户在线数（单台）	>=100000

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
- ★证书编号：23SS00321-A
- ★有效期：2023 年 11 月 17 日至 2025 年 11 月 17 日

所属品牌：奇安信网神

发布时间：2014 年 3 月

产品适用领域：全行业

产品照片：多种形态：1u/2u/3u 等，不同型号，性能不同，目前支持信创、非信创等近 30 款型号。部分型号产品照片如下图：



产品咨询二维码



产品咨询邮箱：kefu@qianxin.com

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：深信服全网行为管理系统 AC-1000 V13.0

产品概述

公司的 IT 管理员肩负着一项重要的职责，那就是全面了解公司内网的方方面面。这包括全局网络分布、终端设备部署、IP 分配以及网络设备分布使用情况。为了更好地履行这一职责，管理员需要掌握先进的技术和工具，以便实时监控和分析网络资源的使用情况。

在这个背景下，AC（认证计费）系统应运而生，它是一款功能强大的网络管理工具，可以帮助 IT 管理员全面了解公司内网的资源分配和使用情况。通过 AC 系统，管理员可以实时查看各个终端设备的活动状态，了解 IP 地址的分配和使用情况，以及监控网络设备的分布和使用效果。

AC 系统提供了丰富的历史数据和报表功能，使管理员能够轻松地分析网络资源的使用趋势，为优化网络提供全面、第一手的数据支持。这些数据可以帮助管理员发现潜在的网络问题，例如网络拥堵、IP 地址浪费等，从而采取针对性的措施进行调整和优化。

功能特点

AC 支持扫描到内网中的指定网段中网络终端设备，并对扫描到的设备进行设备类型识别。

可以分析出镜像流量到 AC 的终端设备的终端指纹信息（设备类型、IP、MAC、操作系统、在线状态、开放的端口、厂家等基本详情），AC 支持通过 tcp、dhcp、arp、http（https）、dicom 等协议识别终端特征，真实环境测试下发现率和识别率远高于国内厂家设备，支持 PC、移动设备、哑终端、专用设备的发现和型号识别：支持 Windows、Linux、MAC、瘦客户机等 PC；支持手机、平板等移动设备；少支持服务器、交换机、无线控制器等 7 类以上网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等 10 类以上哑终端；

考虑到设备扫描时间真空，通过定期扫描（比如每天全网扫描一次、每两小时重新扫描到的但没有解析的设备）使扫描过后才接入网络的设备无法隐藏。

◎主动识别

主动识别采用了开源嗅探工具来主动探测指定网段内的设备信息，根据不同设备的 TCP/IP 协议栈的差异，与已知的内置设备指纹库匹配得出具体的操作系统信息，通过本机的 ARP 信息获取设备的 mac，再根据 IEEE 标准规范，用 MAC 匹配对应的厂商。通过内置脚本，完成探测并识别其他哑终端设备类型。

◎被动识别

被动式就是不主动发送数据包，通过抓取流量信息，进行分析获取相应的设备信息，被动识别主要采用的技术手段：

http：通过 http 流量的字段信息，能够获取设备的终端型号等信息

Dhcp：分析 dhcp 的 request 包，分析其中指定字段信息，提取厂商、主机名特征标识，将这些信息作为终端类型识别的指纹，与一个事先维护的已知终端厂商标识库匹配，确定终端厂商、主机名信息。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安三所

★证书编号：23SS00051-A

★有效期：2023 年 9 月 1 日至 2025 年 9 月 1 日

所属品牌：深信服科技股份有限公司

发布时间：2011 年 9 月 23 日

产品适用领域：政府、教育、医疗、

企业、金融等行业

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn

深圳市联软科技股份有限公司

深圳市联软科技股份有限公司创立于 2003 年，专注于企业级网络安全市场，为政企客户提供网络安全产品和服务。深耕金融行业，产品已在银行、保险、证券等金融各细分领域得到广泛应用，在端点安全产品在金融领域市场份额居行业前列，并在制造业、运营商、党政军、医疗、能源和交通等行业构建了较强的市场影响力，已服务超过 3000 家高端行业客户。17 年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、并成为国内率先落地基于“零信任安全”产品的厂商之一。2019 年，联软科技并购魔方安全，获得了以攻击者视角对全网暴露面进行主动持续监控与管理的能力。近 5 年来，联软科技营收以超过 50% 的平均增速在网络安全行业高速增长，并在 2020 年引入中网投、高新投战略投资，正式成为网络安全“国家队”。

网址: <https://www.leagsoft.com/>

电话: 0755-86219298

地址: 深圳市南山区粤海街道科技园社区科苑路 15 号科兴科学园 A 栋 A2-901

产品名称：联软网络接入控制系统

产品概述

联软网络接入控制系统（以下简称 UniNAC），是解决安全管理问题的基础设施，可以对接入网络的客户机设备进行控制，杜绝非法外来电脑接入内部网络，同时将有问题的客户机隔离或限制其访问，直到这些有问题的客户机修复为止。一方面可以防止这些客户机成为蠕虫和病毒攻击的目标，还可以防止这些主机成为传播病毒的源头。为大型机构的网络安全、终端管理、信息安全管理提供直接支撑。

UniNAC 是中国最早支持 802.1x 协议、业内最早直接支持 Cisco NAC 架构的网络准入控制系统。UniNAC 提倡直接与网络设备联动实现网络准入控制，以实现最佳的网络安全性、可靠性和组网灵活性，目前能直接联动的网络设备型号达数百种。通过与网络设备联动及联软 NACC 准入控制器配合，UniNAC 能解决各种复杂环境下的网络准入控制问题，包括：LAN（Switch/HUB）、WiFi、WAN、VPN，甚至 NAT 环境。

功能特点

◎ 802.1x

IEEE 802.1x 是 IEEE 制定关于用户接入网络的认证标准，全称是“基于端口的网络接入控制”，属于 IEEE 802.1x 网络协议的一部分。它为想要连接到 LAN 或 WLAN 的设备提供了一种

认证机制。IEEE802.1x 一般部署在 LAN 网络的接入层交换机上或者 WLAN 网络的无线控制器上。其准入控制流程如下：

- ★ 每一个 802.1x 交换机端口，交换机都为其创建两个虚拟接口；
- ★ Controlled Port：只有通过 802.1x 认证后才被导通；
- ★ Uncontrolled port：仅仅用于传输 802.1x 认证流程，即 EAP 包（EAPOL）。

初始状态下，交换机上的所有端口处于关闭状态，仅允许 802.1x 协议数据流通过，当用户通过 802.1x 协议登录交换机时，交换机将用户名 / 口令传送到 Radius 服务器进行认证。如用户名及口令通过验证，则相应的交换机端口打开以允许用户访问相应的网络资源。

UniNAC 准入控制器结合 802.1x 来解决终端电脑身份认证的问题，通过动态切换 VLAN 或者下载 ACL 列表的方式来控制网络资源访问，具有以下优点：

- ★ 支持多厂商网络设备：包括 Cisco、华为、H3C、Juniper 等；
- ★ 控制点是网络的接入层交换机，最接近终端电脑，对不符合策略的电脑可以完全禁止其访问任何网络，使其对网络的危害最小。

◎ Cisco EoU

EoU（EAP over UDP）是 Cisco 的专有协议。EoU 是 Cisco NAC 技术的第一个实现版本，2003 年最早在 Cisco 的路由器上实现，后来在 Cisco 的 3 层交换机上也实现了 EoU。和 802.1x 相比，最大的区别是 802.1x 在网络接入层进行准入控制，而 EoU 则是在网络的汇聚层或核心层进行准入控制。

EoU 的工作原理是当支持 EoU 的汇聚层设备接收到终端设备发来的数据包时，汇聚层 EoU 设备将要求终端设备进行 EAP 认证。EAP 认证包封装在 UDP 包内，在 EAP 认证的内容中，如果安全状态不符合企业安全策略，汇聚层 EoU 设备将从策略服务器上下载 ACL，限制不安全的客户端的网络访问，并对其进行修复。

EoU 技术的优点是它对网络接入设备要求不高，因而覆盖面较高，且由于网络环境中汇聚层设备数量一般会大大少于接入层设备数量，因此部署相对较为容易。

◎ 硬件网关型准入

联软 NACC 准入控制器是一种基于 Cisco EoU 协议的硬件网关型网络准入控制设备，专为解决非 802.1x 网络环境下（接入层交换机或者 AP 不支持 802.1x 协议且汇聚层 / 核心层不支持 Cisco EoU 协议）的网络准入控制问题而设计。联软 NACC 准入控制器通常部署在网络核心交换机或指定服务器前，来判断接入设备是否符合接入安全要求。与 802.1x/EoU 相比，采用 NACC 硬件网关实现准入控制，业务实现流程清晰可靠、环节少，用户只需要购买少量网关设备，并通过网关方式或者旁路方式部署至网络关键节点处，即可实现全面的准入控制。

联软 NACC 准入控制器支持 3 种部署模式：网关部署模式（即串联模式）、策略路由模式（上行控制、下行不控制）和端口镜像模式。

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS029-812

★有效期：2024年6月6日至2029年6月5日

所属品牌：联软科技

发布时间：2014年9月30日

产品适用领域：金融业、医疗业、制造业

产品咨询邮箱：Lrkjzjzc@leagsoft.com



深圳万物安全科技有限公司

深圳万物安全科技有限公司（简称“万物安全”）围绕战略新一代信息技术产业，聚焦网络安全新质生产力“AI+ 物联网安全”，“颠覆式创新和硬科技”实力获得工信部“网安中心”和“火炬中心”高度认可并获奖，连续三年被“全球权威咨询机构 IDC- 金融视频物联安全”分析报告评为第一、国家保密局百家信创单位之一、中国网络安全产业联盟理事单位、关键信息基础设施安全保障联盟副理事长单位。

万物安全产品和解决方案，基于云原生和零信任架构，融合 AI、信创、数据安全等最新技术，为金融、能源、医疗、交通等提供全生命周期的物联网安全运营和管控能力，满足《网络安全法》、《关基保护条例》、《网络数据安全条例》等国家政策法规要求，已成为物联网安全领导者。。

网址: <https://www.iottepa.com>

电话: 0755-26658957

地址: 中国·深圳·福田·国际金融科技城 6 楼

产品名称：安防准入管理

产品概述

安防准入管理系统通过提供物联网资产的发现识别、非法接入控制等产品能力，助力企业单位全面掌握网络中的物联网设备，及时发现未知或未授权的资产，有效降低安全盲区。同时，阻止未经授权设备接入网络，避免潜在的网络攻击。增强对物联网资产的可见性，还能对网络风险进行实时监控和预警，提升整体安全管理水平，确保业务系统稳定、合规地运行。

功能特点

◎智能化资产管理

系统方式取代人工，自动发现和识别资产，实时更新资产信息，提供动态台账，提升管理效率，提高资产信息准确度；

◎智能化运维管理

自动化描绘安防网络拓扑，识别设备分布，持续监控设备变化，设备异常实时告警并附设备详细信息，辅助故障处理；

◎自动化设备状态监控

持续监控技防设备的状态变化，设备离线实时声光告警，提供设备定位信息，辅助快速故障处置，提升效率；

◎自动化视频漏录监测

自动化监控各类摄像头的录像状态，视频漏录或者视频文件丢失及时预警，解决人工方式难以及时发现风险问题；

◎网络安全防护

建立统一设备入网规范，识别并阻断非行内技防设备接入安防网络，如私接、仿冒等，防范网络入侵；

◎数据安全保障

针对性对视频文件进行加密保护，预防文件下载泄密；提供水印追溯能力，防范视频调阅通过拍照或者截图泄密；

◎基础合规检查

提供对视频文件保存天数检查，保存天数不达标及时预警；提供对网络隔离状态检测，因误操作、人为等因素导致的隔离时效及时预警；

◎安全合规检查

周期性对物联网资产漏洞、弱口令等风险进行自动识别，提供详细漏洞信息及修复建议，保障技防设备安全合规；

技术指标

支持配置准入策略，设备接入后判定其是否为合法资产并对合法资产自动准入。同时，支持通过预准入策略从 IP 地址、MAC 地址或终端类型维度为计划新增的资产预留直接准入的权限，当资产信息匹配到有效的预准入策略后，系统将直接判定其为合法设备并自动准入；

支持将不符合准入策略的资产定义为私接设备，支持自动阻断私接设备并产生告警；

支持通过私有协议、公有协议、流量分析及联动交换机等多种技术组合，发现识别的资产信息，包括 IP 地址、MAC 地址、资产类型、端口、服务、品牌、型号、资产位置、资产名字、组织架构、状态、安全状态、交换机联动状态、上线 / 离线时间、引擎信息、主资产 IP、主资产 MAC、交换机 IP 等；

支持对同一个资产产生的不同数据进行判定并合并，将合并后的资产展示在列表中，列表信息包括 IP 地址（主资产的 IP 地址）、资产类型、品牌、型号、资产名字、组织架构、状态以及安全状态信息。合并后确定多个资产的主从关系，单击资产 IP 展示主资产和从资产信息，支持手动解除资产合并；

支持自动化监测资产在线状态，将离线资产展示在列表中，列表信息包括 IP 地址、资产类型、品牌、型号、资产名字、资产位置、组织架构、状态、安全状态、频繁离线以及离线时间，单击“频繁下线”列的图标可展示对应资产的历史离线记录；

支持根据主动探测的资产信息、网络信息，实时绘制网络拓扑结构；

通过 AC 联动，系统可以获取网段内所有无线 AP 的信息以及各无线 AP 下的无线设备资产，将对应的资产展示在列表中，列表信息包括 MAC 地址、IP 地址、资产类型、品牌、型号、

AP-IP 地址以及 AP-MAC 地址；

支持通过扫描指定端口，通过分析 banner 信息辅助发现识别使用对应端口的资产，并将所获取的信息展示在列表中，列表信息包括 IP 地址、端口、协议、软件、版本号、Web 地址、Web 标题以及分析引擎；

支持通过分析引擎的镜像流量，被动发现识别资产信息，并将信息展示在列表中，列表信息包括 IP 地址、资产类型（展示为整合多元识别后的数据）、系统、端口、协议、软件以及是否安全传输。单击“查看详情”可展示网络流量资产测绘的详细信息；

支持以引擎为维度统计各个引擎下所有资产使用的总流量，将流量信息展示在列表中，列表信息包括引擎名称、上行流量、上行带宽占比、下行流量和下行带宽占比；

支持非法 DHCP 监测，对监测到的非法 DHCP 服务器系统进行告警及阻断；

支持实时监测是否存在网络隔离失效的隔离网，并产生告警记录通知管理员；

支持实时检测违规接入的 NAT 设备，对监测到的非法设备进行告警及阻断；

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS029-870

★有效期：2024 年 08 月 02 日至 2029 年 08 月 01 日

所属品牌：万物安全产品体系 -LA 标品

发布时间：2024 年 9 月 13 日

产品适用领域：金融业、银行业、交通行业、智慧城市、交易行业

产品照片：



产品咨询二维码

产品咨询邮箱：huangjt@iottepa.com

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：腾讯 iOA 零信任安全管理系统

产品概述

腾讯 iOA 终端准入是腾讯面向政府、金融、医疗、教育等大型事业单位推出的企业终端管理的解决方案。它基于用户核心服务保护模式，对非法访问用户核心服务的终端进行管控和限制，对接入内部网络的终端进行严格、高细粒度的管控，身份不合法和安全基线不合规者拒绝接入网络，保证合法以及安全的终端入网，全过程进行严格管控、全方位的操作审计。同时，它可以对入网请求用户的终端做健康评估并对不满足条件的终端进行修复，实现内网标准化管理，降低内网安全风险。

功能特点

◎终端自动识别：自动发现网络拓扑及接入设备，支持多类型设备认证，包括如打印机、IP camera、IP 电话、ATM 等 IoT 设备的识别与管控；

◎接入认证方式灵活：支持有 802.1x 客户端、无客户端、WebPortal 多种方式认证，同时支持 MAC 地址、交换机端口、Agent ID、终端硬件 ID 等进行灵活绑定等方式。

◎接入场景支持丰富：支持有线、无线、VPN、HUB、NAT、漫游、远程分支机构等多种网络接入场景接入认证。

◎终端合规检查：自动监测终端安全，合规检查断网，对通过身份认证但不满足安全检查的终端不予以网络接入，并强制引导移至隔离修复区，提示用户安装有关补丁、杀毒软件、配置操作系统有关安全设置等。

◎非法终端网络阻断：及时发现并阻止未授权终端对内网资源的访问，从而确保内部网络的安全。

◎接入故障自动收集：后台系统提供用户接入故障的原因、接入位置等信息，便于管理员维护。

◎安全报表：可根据规则自动生成网络控制安全报表，全面了解在网设备接入。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00149-A

★有效期：2024 年 02 月 02 日至 2026 年 02 月 02 日

所属品牌：腾讯安全

发布时间：2020 年 9 月

产品适用领域：泛互、金融、政府等

产品照片：



产品咨询二维码



产品 logo:



产品咨询邮箱：amerlinwang@tencent.com

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，国有资本占股近 50%。

基于“安全协同·AI 赋能”的战略理念，公司在工业互联网安全领域持续深耕，团队核心成员是中国工业互联网安全事业的第一批践行者。

长扬科技在业界开创了“智能工业安全大脑”的产品理念，以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了 60 余款产品，面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉 AI 安全分析、工业零信任安全、工业数据安全和工业数据通信等多维度产品，构建覆盖工业互联网安全产业完整生命周期的安全保障体系。

公司总部位于北京，并在西安、武汉、郑州、成都、上海、广州等全国近 30 个城市建有研发中心及服务分支机构，形成了覆盖全国的“网状战略布局”，可为客户提供强有力的本地化服务。长扬科技积累了超过 32 个行业细分领域、4000 余家工业企业的安全服务经验，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，提供 4 大类、27 项标准化服务，致力于为工业企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：<https://www.cy-tech.net/>

电话：010-82194186

地址：北京市海淀区闵庄路 3 号四季慧谷·国家网络安全产业园 2 期 15 号楼

产品名称：物联网安全运营平台 IOTP/V1.0

产品概述

物联网安全运营平台是集资产管理、风险监测、威胁预警、防护一体的物联网安全解决方案。通过对物联网设备的全面资产测绘，精准识别每一个接入设备及其特征。利用先进的物联网设备指纹技术，为设备建立唯一标识。平台能够实时监测网络中设备的运行状态和通信行为，全景式感知安全风险。一旦发现异常行为或潜在威胁，立即触发预警并采取阻断措施。同时，该平台提供设备漏洞检测与修复建议，能够确保物联网系统的稳定、安全运行，为企业和组织的物联网系统保驾护航。

功能特点

物联网安全运营平台：从资产、安全、运维、行为多个方面提供数据分析支持，全面管控物联网系统中的各类安全态势。

◎资产管控

物联网资产识别

物联网终端访问控制

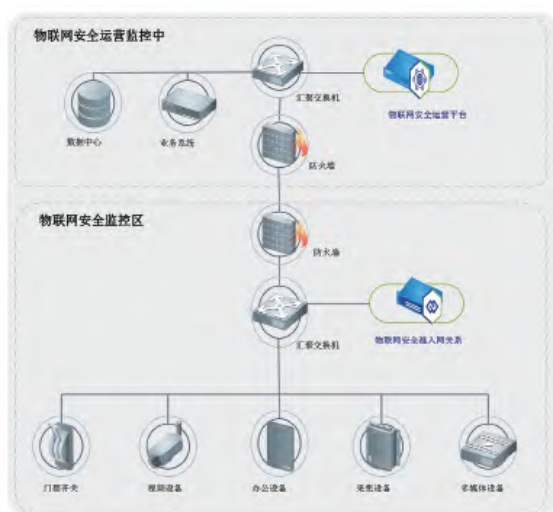
物联网终端安全自检

◎安全运营

违规外联检测

异常行为实时告警

威胁感知风险管控



典型部署架构

◎监控中心

部署【物联网安全运营平台】，负责资产统计、安全分析、综合展示、探针统一管控、策略下发等；实现实体资产分析，发现来自内部的威胁和风险，提高内部信息安全、数据安全、行为合规等。

◎监控区域

部署【物联网安全准入网关系统】，对物联网全网的前端资产探测、接入风险监控、数据上报等。

技术指标

资产识别能力	能够识别 IOT（资产大类包括：智能摄像头、录像机、ip 对讲、门禁系统、报警系统、交换机、服务器、PC、其他哑终端。）、传统 IT 设备、IT 软件
	资产识别率 95% 以上
资产探测速度	单 C 段资产探测 10 分钟左右

阻断速度	单资产阻断时间 8s 内；
漏洞库	集成不少于 3000 个物联网设备漏洞，覆盖 CVE、CNVD、CNNVD；
物联网设备指纹	支持海康威视、大华、宇视、天地伟业、雄迈、汉邦高科、安科数字、威视达康、索尼、海思、中维世纪、升泰科技、奇偶科技、科达、英飞拓、智美达、晶睿通讯、MayGion、安讯士、IQeye 等不少于 200 个物联网设备厂商，设备指纹不少于 500 种。
物联网协议指纹	支持 Dahua-DVR、RTSP、ONVIF、SIP、VSTARCAM 等不少于 5 种物联网协议指纹。
资产查询速度	百亿秒级查询
传输速度	支持扫描限速：高速，中速，低速
	低速不超过 100Kb/s
	高速不超过 1Mb/s

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
- ★证书编号：24SS01395-A
- ★有效期：2024 年 9 月 20 日至 2026 年 9 月 20 日

所属品牌：长扬科技

发布时间：2024 年 9 月

产品适用领域：金融、粮库、电力、水利等行业领域

产品照片：



产品咨询二维码

产品咨询邮箱：jianwen.jin@cy-tech.net

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望网络接入控制系统

产品概述

远望网络接入控制系统是一套以旁路控制技术为主的网络准入控制系统，秉承不改变现有网络结构的特性，为用户解决终端入网的合规性要求。产品依据最新的 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》，满足等保中“安全区域边界”非授权设备私自联入内网的管控要求。

功能特点

◎入网申请和审核。通过对设备进行入网申请和审核流程管理，可确保当入网设备发生安全风险和安全事件时能责任到人。

◎资产管理。可按照组织机构和网络 IP 资源划分，实现全网资产信息直观展现和快速定位。

◎接入控制。对未注册设备通过 TCP 协议管控，实现网络阻断并跳转到隔离区强制注册。同时记录其跳转和访问日志信息，提供该信息查询功能。

◎双向认证。基于装终端代理程序防火墙实现，在安装终端代理程序的主机上鉴别访问者的合法性，阻断未授权的网络访问。

◎ 802.1x。提供已安装代理程序的终端完成交换机 802.1x 协议认证，同时支持多种认证方式帐号密码、数字证书等。

◎ Mac 认证。提供通过以 MAC 地址验证的方式来完成交换机 Mac 认证。

◎入网安检。对接入内部网络的终端在入网前进行安全检查，确保接入内网的终端符合安全要求，防止造成内网隐患。对于不符合安全要求的终端进行隔离修复，修复完成后才能入网。

◎身份认证。在使用终端前对用户身份进行鉴别，保证终端用户身份的合法性，同时对身份认证操作日志进行审计。

◎设备替换阻断。能自动识别网络摄像机的接入，在开启接入控制时，能对网络摄像机自动放行，当网络摄像机的 IP 地址被替换为其他设备时能自动对替换设备进行接入控制。

◎成效报告。成效报告按月生成，内容包含：当月的注册率变化趋势、非法设备访问拦截情况、安检通过率变化趋势和安检通过设备情况统计。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402231855

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：远望

发布时间：2015 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询邮箱：mail@chinayuanwang.com



产品咨询二维码



USB 移动存储介质管理系统

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家级专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区昆明湖南路 47 号国防教育基地二层

产品名称：USB 安全管理系统

产品概述

USB 安全管理系统是一款防止 USB 移动存储设备滥用导致病毒传播的产品，它通过控制 USB 移动存储设备的使用、病毒检查，实现对 USB 移动存储设备的“认证、授权、杀毒、审计”等功能。既满足用户通过 USB 移动存储设备进行文件资料高速、便捷传输，又保证了文件资料的安全性、可靠性，有效阻止未知病毒文件在用户业务系统内的传播，保障用户业务系统安全。

产品采用工业级的硬件设计，可以通过网线和主机直接连接，也可以通过交换机连接到主机所在的局域网。USB 移动存储设备插入 USB 安全管理系统后，可以通过 Web 浏览器、FTP、SFTP、UNC（网络共享）等方式访问 USB 移动存储设备上的资源，实现“一处接入，全网使用”。

功能特点

◎设备接入控制

基于设备唯一性标识对 USB 移动存储设备进行入网授权，实现 USB 存储设备安全接入管控，未经过授权的外部移动存储介质一律禁止使用。

◎设备病毒查杀

使用专业病毒库，自动对插入系统的 USB 移动存储设备进行病毒扫描，对扫描出的病毒

文件进行告警、隔离或删除。

◎文件黑白名单管控

支持根据文件后缀、特征值设置文件白名单，自动屏蔽高风险文件；支持对文件后缀设置黑名单，防止重要敏感文件的外泄。

◎支持多种访问方式

可以通过 WEB、FTP、SFTP、UNC 以及专用 C/S 客户端等访问方式，多样化访问 USB 移动存储设备上的资源，满足各类新老系统使用环境的要求。

◎支持多种权限管理

支持系统管理员、安全操作员、安全审计员三权管理；支持设备级的使用权限控制；支持自主设备共享实现文件在不同用户之间的便捷分享。

◎全面的日志审计

支持用户操作日志、USB 移动存储设备使用日志及操作系统运行日志的审计和导出操作，有效追踪和定位用户行为。

◎网安信息采集上报

支持对接电力监控系统网络安全监测装置，自动上报 USB 相关各类安全事件信息，满足安全监管的需要。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106230246

★有效期：2023 年 2 月 10 日至 2025 年 2 月 10 日

所属品牌：珞安科技

发布时间：2021 年 3 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业。

产品照片：



产品咨询邮箱：liss@icssla.com



产品咨询二维码

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISASecure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 6000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.winicssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特移动介质安检站

产品概述

威努特移动介质安检站是各类移动存储介质病毒查杀的专用设备，该设备采用软硬件一体化设计，对勒索病毒等恶意代码程序进行查杀，设备采用高敏电容触摸屏实现病毒查杀的极简操控，搭配 4G 物联网实现病毒库的自动更新，以多类型的业务接口满足各类介质的接入，存储介质经安检站查杀后自动生成病毒查杀标记，结合工控主机卫士对病毒查杀标记进行验证，无杀毒标记的介质将被阻止读取，以此保证工业生产网络免受病毒及恶意代码程序的侵扰。

功能特点

◎高效双病毒引擎

移动介质安检站采用双病毒引擎交叉进行病毒检测，能有效提高病毒检出率。

◎自动更新病毒库

基于 4G 物联网自动更新病毒库，有效保障恶意代码防范能力的有效性。

◎灵活部署应用

不受限于网络结构，直接部署于厂区、场站、车间等入口处，灵活部署方便现场应用。

◎全金属加固机身

机身通体采用金属板材，仅暴露自动病毒查杀的 USB 接口，配备锁具可防止暴力拆解。

◎多类型介质杀毒

普通 U 盘、移动硬盘、存储卡等介质均可查毒，外来人员随身介质亦可有效管控，有效防止勒索病毒的泛滥。

◎强制杀毒验证闭环

杀毒后自动生成特殊格式的杀毒标记，可供工控主机卫士开展查毒验证，形成完整的技术管控闭环。

◎完善的介质管控方案

移动介质安检站结合安全 U 盘、专用写入软件、工控主机卫士，可针对移动存储介质进行注册、授权、分组管理、读写控制、病毒查杀、杀毒验证、日志审计、注销等一系列综合管控方案。

◎完美衔接企业管理制度

以技术手段补全工业企业移动存储介质的管理流程，辅助工业企业构建安全的工作业务流程。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106232082

★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：威努特

发布时间：2021 年 7 月 15 日

产品适用领域：电力、石油石化、
轨道交通、钢铁、市政、烟草、
智能制造等

产品照片：



产品咨询二维码

产品咨询邮箱：support@winicssec.com

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，国有资本占股近 50%。

基于“安全协同·AI 赋能”的战略理念，公司在工业互联网安全领域持续深耕，团队核心成员是中国工业互联网安全事业的第一批践行者。

长扬科技在业界开创了“智能工业安全大脑”的产品理念，以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了 60 余款产品，面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉 AI 安全分析、工业零信任安全、工业数据安全和工业数据通信等多维度产品，构建覆盖工业互联网安全产业完整生命周期的安全保障体系。

公司总部位于北京，并在西安、武汉、郑州、成都、上海、广州等全国近 30 个城市建有研发中心及服务分支机构，形成了覆盖全国的“网状战略布局”，可为客户提供强有力的本地化服务。长扬科技积累了超过 32 个行业细分领域、4000 余家工业企业的安全服务经验，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，提供 4 大类、27 项标准化服务，致力于为工业企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：<https://www.cy-tech.net/>

电话：010-82194186

地址：北京市海淀区闵庄路 3 号四季慧谷·国家网络安全产业园 2 期 15 号楼

产品名称：长扬 USB 存储介质安全检测平台 USD/V2.0

产品概述

长扬 USB 存储介质安全检测平台产品是基于 USB 存储设备的全生命周期理念推出的应对工业控制系统环境 USB 存储介质安全的专门解决方案。该产品通过 USB 存储设备的注册、分发、权限分配、操作审计和事件溯源功能，确保 USB 存储介质在整个使用过程中始终符合安全管理标准，即使 USB 存储介质丢失或被盗，也能通过权限控制、远程锁定功能，防止敏感信息泄露。

另外，平台可以对存储介质中的文件进行病毒和恶意代码的查杀，针对安全的 USB 存储介质嵌入安全标记，无安全标记的 USB 存储介质禁止在内部网络中使用，防止病毒和恶意代码通过 USB 存储介质摆渡到内部网络中，通过多种技术手段的使用确保制定的 USB 介质管理制度和规范能被正确执行，实现了 USB 存储介质安全防护与安全管理一体化。

功能特点

◎存储介质全生命周期管理

长扬 USB 存储介质安全检测平台具有全面的 USB 存储介质管理功能，能够对 USB 存储介质的注册、接入、使用、退出等全过程进行实时监控和记录。平台能够详细记录 USB 存储介质的访问权限、访问时间、访问主机等信息，便于管理员实时了解系统内 USB 存储介质的使用情况。

此外，平台还具备异常行为预警功能，当发生异常的 USB 存储介质接入、权限变更、病毒感染等情况时，平台会立即向管理员发出警报，确保及时发现并处理安全问题。

◎可信接入与访问

长扬 USB 存储介质安全检测平台支持对 USB 存储介质进行统一注册、统一赋权、统一认证，够通过对 USB 存储介质采取身份鉴别、访问控制、行为审计等手段，实现 USB 移动存储介质与内部主机之间的可信访问。

◎安全标记和识别

长扬 USB 存储介质安全检测平台内置下一代智能病毒检测引擎，将人工智能、算法和机器学习应用于恶意代码的预测、鉴定和阻止，可对蠕虫病毒、恶意软件、勒索软件、引导区病毒、木马等恶意文件进行有效查杀，抵御已知恶意软件的有效性高达 99%。USB 存储介质经病毒查杀后将被打上安全标记，具有安全标记的介质才能在主机上使用，未经过病毒查杀的移动介质将被拒绝读写。

◎集中管理，多级安全

长扬 USB 存储介质安全检测平台支持通过管理平台实现查看 USB 存储介质的状态，执行批量操作，如更新安全策略、锁定丢失设备、擦除敏感数据等。通过为不同区域的安全检测平台配置不同的安全策略，可以实现不同场景和安全防护级别下的差异化安全防护需求，防止外部恶意攻击、内部数据泄露以及病毒传播，确保业务系统的安全稳定运行。

◎兼容性与扩展性

长扬 USB 存储介质安全检测平台具有良好的兼容性与扩展性，轻量化客户端对系统资源的需求极低，不影响主机性能，兼容各种操作系统和终端硬件平台，同时可以与长扬工控主机卫士、长扬防勒索软件等产品协同工作，提供更全面的终端安全防护能力。平台还支持平滑升级，随着安全技术的不断发展，平台可以不断引入新的防护功能和策略，确保产品始终处于安全防护的前沿。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01063-A

★有效期：2024 年 7 月 26 日至 2026 年 7 月 26 日

所属品牌：长扬科技

发布时间：2024 年 10 月

产品适用领域：电力、电网、石油石化、智能制造行业

产品照片：



产品咨询二维码

产品咨询邮箱：guodong.zhang@cy-tech.net

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望移动存储注册管理系统及安全 U 盘

产品概述

远望移动存储注册管理系统及安全 U 盘是一款 USB 移动存储介质管理系统安全产品，其产品样式为软硬件结合，提供了对接入信息系统的 USB 移动存储介质进行统一管理，统一认证、监控和审计的功能。可对违规使用移动存储介质，违规泄密行为进行预警，协助管理人员加强移动存储介质和信息保密安全的管理。

功能特点

移动存储注册管理系统是利用信息保密、访问控制、审计等技术手段，对内网中移动存储设备进行科学管理，杜绝外来存储介质非法进入内网；使内部涉密信息无法通过移动存储介质的不规范使用而泄密。

◎有效的注册管理

- A、移动存储介质接入注册和认证管理；
- B、移动存储介质数据读写控制管理；

◎用户身份验证

所有移动存储介质在使用前均要经过授权中心统一授权，并根据授权信息产生移动存储介质管理台账。经过系统授权后的移动存储介质才能在内网中使用，未经授权的移动存储介质将被严格控制使用，杜绝外来存储介质非法进入内网使用。

◎日志实时记录

移动存储介质使用过程中，系统会实时记录用户接入移动存储介质的行为并写入设备日志区；系统通过记录操作设备的相关信息、访问开始时间、访问结束时间等信息确认使用者及主机的唯一性，为事件查处提供依据。日志的记录方式采用先写日志后执行动作的串行操作，日志写入成功后操作才能继续，该策略保证了日志信息的可靠和完整性。

◎安全审计

对移动存储介质数据交换行为进行安全审计。

A、提供详细的文件操作审计记录：包括文件创建、删除、修改和重命名等操作，（包括文件名、审计描述、时间、用户名、计算机 IP 地址和其他必要信息）；

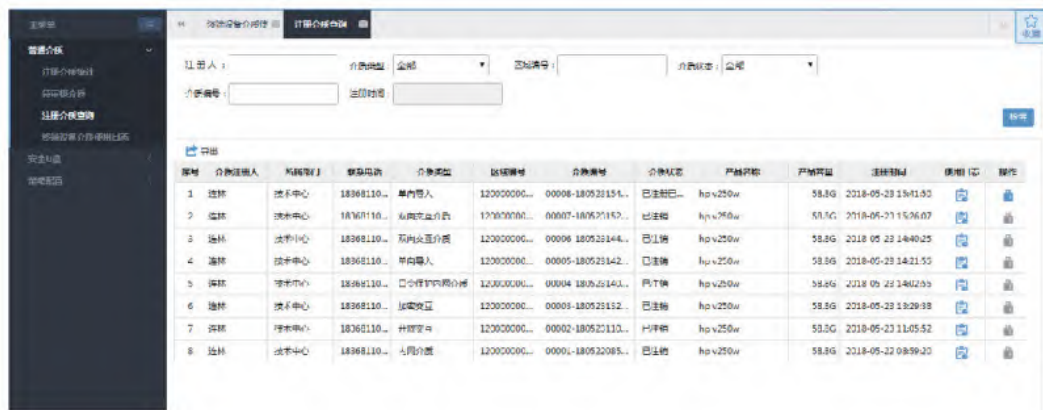
B、提供详细的移动存储设备的插入和拔出动作记录，具体包括事件类型、移动存储介质的名称、用户、计算机 IP 地址和事件时间。

◎区分涉密与非涉密的数据交换过程

对于涉密信息，通过技术手段坚决杜绝与外网设备的信息传递。普通的非涉密信息则在保证安全的前提下允许交互。

◎违规行为自动预警和通报

对于违规使用移动存储介质及 USB 端口，违规对涉密信息传递出内网的行为，在安全管理平台上自动产生预警或通报。



远望移动存储注册管理系统界面图

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0403231906

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：远望

发布时间：2010 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询二维码

产品咨询邮箱：mail@chinayuanwang.com



文件加密产品

北京信安世纪科技股份有限公司

北京信安世纪科技股份有限公司（股票代码：688201）成立于 2001 年 8 月，是科技创新型的信息安全产品和解决方案提供商。公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全、通信安全等基础性安全问题，为金融、政府、企业、军队等重要领域的核心业务系统提供先进的网络安全产品与安全解决方案。

网址：www.infosec.com.cn

电话：010-68025518/400-670-5518

地址：北京市海淀区建枫路（南延）6 号院金隅西三旗科技园 2 号楼信安大厦

产品名称：NetEDS 数据加解密服务系统

产品概述

NetEDS 数据加解密服务系统是信安世纪自主研发的一款基于商用密码算法与技术实现的高性能数据安全产品，拥有“强安全”、“多场景”、“高性能”三重优势，可提供密钥管理、数据加解密、数据脱敏、数据防篡改、凭据管理等安全服务，能够对敏感数据、重要信息等进行加密保护，有效降低因数据泄露带来的安全风险，帮助用户切实履行《数据安全法》、《个人信息保护法》等法律法规要求的数据保护义务。

功能特点

◎双系统鉴别

数据库管理系统账户除需要经过数据库管理系统的鉴别之外，还需信安 NetEDS 数据加解密服务系统的身份鉴别。

◎数据存储加密

对指定数据进行加密；

数据加密粒度支持表 / 字段级；

支持随机数加密技术，保证相同的明文数据加密后密文数据不同；

支持国家密码管理局规定的加密算法。

◎应用权限控制

产品能对应用系统、IP 地址和数据库管理系统账户进行绑定，保障只有受信的数据库管理系统账户和应用系统通过特定的 IP 地址才有密文数据的访问权限。

◎密文访问控制

提供独立于数据库管理系统自身的权限控制体系，所有账户（包括数据库管理系统特权账

户)访问密文数据前均通过信安 NetEDS 数据加解密服务系统管理员的授权;

支持对所有账户(包括数据库管理系统特权账户)可以访问的密文数据范围、访问权限(如新增、修改和删除权限)进行限制;

具备对密文数据访问的时间范围进行限制的功能;

具备对密文数据访问的源 IP 地址范围进行限制的功能。

◎密文索引

产品支持密文索引功能,并能对密文索引进行管理。

◎完整性校验

能对数据库数据或日志文件进行完整性校验;

检测到完整性受到破坏的重要数据产品应具有自动恢复的措施。

◎权限分离

产品将与数据库加固产品管理的权限进行分离,实现特权用户的权限分离,并至少具备系统管理员、安全管理员和安全审计员。系统管理员负责系统配置、系统运行状态监控等工作;安全管理员负责密文数据配置、密文权限控制等安全维护工作。安全审计员负责审计开关的控制、审计数据的查看、审计数据的管理等工作。信安 NetEDS 数据加解密服务系统禁止存在具有所有权限的超级管理员。

◎数据库状态监控

产品支持对数据库的状态监测,监测内容包括数据库的启动时间、用户连接时间、表空间状态平均执行频率等。

技术指标

- (1) 支持多种加密方式
- (2) 支持三级密钥体系
- (3) 支持多种认证与访问控制机制
- (4) 支持国密 SSL
- (5) 达到密码模块安全二级水平
- (6) 支持千万级密钥容量
- (7) 支持万级并发处理能力
- (8) 支持万兆级加解密性能

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称:公安部计算机信息系统安全产品质量监督检验中心

★证书编号:24SS010487-A

★有效期:2024年10月12日至2026年10月12日

所属品牌：信安世纪

发布时间：2022.10.25

产品适用领域：政企、医疗、金融、交通、教育、电力等需要进行数据加解密场景

产品照片：



产品咨询邮箱：market@infosec.com.cn



产品咨询二维码

江苏敏捷科技股份有限公司

江苏敏捷科技股份有限公司（以下简称“敏捷科技”）由全球主动信息防护技术原创团队创办，是数据安全国际化领先企业和中国数据安全领域的开拓者和领跑者，致力于帮助各类企业、科研院所及政府解决数据安全与管理难题。

基于卓越的产品、强大的研发实力和前瞻的创新理念，敏捷科技获得行业内的高度认可。目前已拥有百余项软件著作权及多项国家级专利，先后荣获工信部中国信息安全最具影响力企业奖、中国网络安全和信息产业领军企业、首批工控安全服务能力咨询机构、江苏省规划布局重点软件企业、江苏省重点网安企业、江苏省专精特新企业等国家级、省部级奖项和荣誉。

敏捷科技的营销和服务网络覆盖全国，总部位于苏州，在南京、苏州两地设有研发中心，同时在全国各大城市建立稳定而完善的销售及售后服务体系。敏捷科技旗下的系列产品及解决方案已成功应用于数千万终端，产品在制造、能源、设计、交通、政府、军工、医疗、金融、教育、地产等领域得到广泛应用，累计客户量过万。先后服务了中国中车、一汽集团、东风汽车、长安汽车、南钢、沙钢、中信泰富特钢、苏交科、成勘院、云南网安、紫金山实验室、泸州老窖、天合光能等国资央企或行业标杆企业，护航企业数字化转型发展。

网址：www.agile-china.com

电话：025-84521143

地址：江苏省南京市栖霞区紫东国际创意园 A7-603

产品名称：敏捷数据安全卫士系统 Agile DGS

产品概述

敏捷科技按照国家网络安全法、数据安全法、网络安全等级保护、商业秘密保护等要求，并结合实际业务场景下文件安全管理的业务需求，在原有的数据安全产品基础上，提出数据安全卫士系统 DGS 这一整体数据安全与数据管理管控平台，为用户的各类电子文件提供全生命周期的安全保护和有效管理。

功能特点

◎主动加密：文件在创建、浏览、编辑、归档、分发、销毁的所有环节下均为透明加密状态。受控文件在管控内部使用不受限制，跨部门文件传输、编辑等都可进行。不影响使用习惯。有效防止数据信息通过微信、邮箱、移动硬盘等方式外泄，敏感信息看不懂拿不走

◎智能加密：按照企业情况，所有数据分类分级定密。核心数据全加密，个人文件不加密，明文密文安全交互。

◎落地加密：电子文件从管控平台下载到本地客户端上时，实施落地自动加密，保障数据的落地安全。

◎外发管控：加密文件通过严格审批后才能解密，与外部交互。企业根据用户层级自定义外发策略，实现分级审批、多级审批。

◎行为审计：实时审计终端文件的拷贝、打印、外传等行为，并对识别文件中包含的敏感内容，进行告警或阻断。

◎数据溯源：利用数字水印和电子标签技术，对设备屏幕、涉密文档和纸质文件上打标记，预防拍照、截图和打印外泄敏感内容，以及对外泄文件进行分析，定位出泄密源头。

技术指标

加解密速度 100M/s；占用内存不超过 50M；支持 100G 大文件加解密；兼容系统 windows、Linux、Mac、iOS、Android、鸿蒙和国产化信创系统。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231371

★有效期：2023 年 6 月 2 日至 2025 年 6 月 2 日

所属品牌：敏捷科技

发布时间：2016 年 4 月 1 日

产品适用领域：电力、水利、智能制造、新能源、医疗、运营商、金融、地产、军工、政府部门等

产品照片：



产品咨询二维码

产品咨询邮箱：nihaiyan@agile-china.com



数据泄露防护产品

北京梆梆安全科技有限公司

北京梆梆安全科技有限公司成立于 2010 年。公司以移动安全为核心，逐渐将安全防护能力向传统互联网及物联网延伸，创新性提出“共享安全”理念，围绕业务安全、移动安全、物联网安全、安全服务“四位一体”的产研体系帮助用户制定网络安全建设规划，构筑覆盖全网络环境的新型信息安全立体纵深防御系统。

梆梆安全的产品与服务范围涵盖网络安全体系建设规划、安全咨询、安全检测、安全防护、威胁感知、应急响应、安全服务、安全培训等。同时，梆梆安全还致力于研究和掌握物联网安全、人工智能安全等前瞻性技术，不断创新，并在智能设备安全、车联网安全等层面取得了丰硕成果。

到目前为止，梆梆安全已经为 10 万家注册企业及开发者的超过 100 万个移动应用提供安全服务，这些应用已经累计安装在 10 亿个移动终端上。覆盖金融、运营商、互联网、物联网、政府、能源、教育、医疗、企业等各大行业。

目前，梆梆安全已取得 190 项软件著作权、85 项授权专利，并有 170 余项专利正在申请，108 项注册商标证书。此外，梆梆安全还拥有信息安全服务资质风险评估一级资质、信息安全等级保护安全建设服务机构能力评估证书、计算机信息系统安全专用产品销售许可证，入选 CNCERT 网络安全应急服务支撑单位，获得国家网络与信息安全信息通报机制技术支持单位资格，建立经交通运输部认定的交通运输网络安全技术交通运输行业研发中心。

网址：www.bangcle.com

电话：010-62660308

地址：北京市海淀区学院路 30 号科大天工大厦 A 座 20 层

产品名称：API 安全平台

产品概述

梆梆 API 安全平台通过对 API 上线运行后的数据流量进行实时检测，解决 API 上线运行后所面临的各种安全风险，为企业建立一套完整的 API 安全防护管控机制，产品从 API 资产管理、API 风险检测、API 敏感数据识别、API 防护管控四大核心模块，帮助企业解决资产数据难治理、风险行为难发现、数据泄露难感知、威胁攻击难防护四大安全问题；

产品综合利用前端检测技术与后端流量分析技术，将 API 访问端和 API 服务端之间建立端到端的安全访问机制，降低企业在设计 API 之初所遗留的安全风险，并引入零信任理念，建立可信机制，确保前后端访问行为均经安全认证，且采用 AI/ML 技术，针对大量的业务往来和频繁的业务更新以及不断变化的攻击方式，进行动态持续化的检测及自动化防御机制，解决企业

在数字化转型下建立的新业务所带来的新型安全风险等问题。

功能特点

◎资产发现与管理

★ API 资产台账建立

产品通过在流量当中使用自研资产识别引擎，自动化发现所有内部使用、外部共享和第三方组件的 API 资产，有效识别出 API 后可自动化进行归类，亦可快速进行分组和打标签，为企业形成清晰的资产台账，帮助企业掌握全局 API 资产。

★ “僵尸 / 影子” API 发现

由业务下线、版本升级、API 弃用等各种原因导致的一些 API 未能及时下线、API 未被及时管理等，这类 API 处于长期无人访问并无人维护且在还在线上运行，产品采用行为分析技术可有效发现僵尸 / 影子 API，帮助企业进行统一管理。

◎敏感数据监测

★敏感数据识别

产品通过内置的个人 / 敏感信息识别标签，有效识别身份证号、手机号、用户地址、银行卡号等涉敏数据，且支持自定义录入企业商业数据规则。

★敏感数据流向分析

产品针对 API 接口上所承载的敏感数据，可记录敏感接口的流动状况、敏感数据的流动状况，以此来清晰展示 API 接口承载的敏感数据的流向情况。

★数据泄露检测

针对敏感数据接口的脱库、撞库、越权查询、批量查询等各种数据泄露风险，可进行实时检测，同步生成告警日志。

◎风险检测能力

★异常行为检测

利用自主研发的异常行为检测引擎，可检测网络中发现的异常行为，如高频 / 低频访问、异常大量访问、非工作时间访问、非可信终端访问、非可信地域访问等。

★脆弱性检测

支持检测 API 本身存在的脆弱性，如鉴权认证失效、权限未经检验、参数未经效验、请求访问异常、访问路径异常等。

★漏洞攻击检测

支持检测通用型漏洞：依靠持续收录的内部漏洞库，可支持检测常见的如：sql 注入、xss、文件上传等通用型漏洞；

支持检测未授权漏洞：支持检测因授权管理不当导致的攻击行为，如：横向越权、越权绕过等；

支持检测业务逻辑漏洞：支持检测因业务逻辑漏洞导致的攻击行为，如：薅羊毛、刷单、

占库存、抢票等；

◎安全管控能力

★直接阻断

通过串接部署，平台可直接阻断不法请求、恶意请求、访问越界等行为。

★限流限速

支持对 API 请求执行一定的限流策略，考虑到系统的处理能力，需要对 API 请求做一定的限流防护。此类场景可以用于缓解基于 API 的 DDoS 攻击，有效防止资源消耗在恶意的 API 请求上。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部安全与警用电子产品质量检测中心

★证书编号：23YS00525-A

★有效期：2023 年 12 月 29 日至 2025 年 12 月 29 日

所属品牌：梆梆安全

发布时间：2023 年 3 月

产品适用领域：政府、运营商、金融、互联网、游戏、医疗、商城等

产品照片：



产品咨询二维码

产品咨询邮箱：market@bangcle.com

北京明朝万达科技股份有限公司

北京明朝万达科技股份有限公司成立于 2005 年，是中国新一代信息安全技术企业的代表厂商，专注于数据安全、公共安全、云安全、大数据安全及加密应用技术解决方案等服务。公司现有员工 700 余人，总部设于北京，在上海、广州、成都、西安等地设有分支机构。凭借在数据安全领域取得的优异成就，明朝万达于 2019 年获得中央网信办背景中网投、国家发改委背景国投创合联合投资，并于 2020 年获得中国电科集团（CETC）战略投资。

基于“动态数据安全，数据全生命周期管控”的产品理念，明朝万达始终以守护用户数据价值为己任，致力于让安全真正服务于业务发展。在大数据、云计算等新技术应用背景下，明朝万达以数据安全为核心、自主可控的国密算法应用技术为基础，研发的 Chinasec（安元）数据安全系列产品及解决方案，覆盖数据产生、存储、交换、使用等全生命周期重要环节，实现对服务器、数据库、PC 终端、移动终端以及网络通信的全 IT 架构下数据安全的协同联动管理，打造企业级的数据安全防护体系。

网址：www.wondersoft.cn

电话：400-650-8968

地址：北京市海淀区阜外亮甲店 1 号恩济西园产业园 16 号楼 B 座一层 106

产品名称：Chinasec（安元）数据防泄漏系统

产品概述

Chinasec（安元）数据防泄漏系统是针对企业面临的数据泄漏风险，采用内容分析引擎，利用关键字、正则表达式、文件指纹、自然语言处理等规则，对企业外发数据进行解析与扫描，实时识别、监控、保护企业敏感数据。对即将发生、正在发生的泄漏敏感数据行为按照预置策略及时阻断并告警，防止企业敏感数据传输到企业外部，有效避免数据泄漏带来的安全风险，实现对企业外发敏感数据的可知、可见、可控的一体化解决方案。

功能特点

- （1）全面覆盖端、边、网、云各个数据泄漏点
- （2）提供统一的数据识别技术和规则管理
- （3）支持基于数据严重性的实时分级管控能力
- （4）支持 NLP、机器学习和分类分级技术
- （5）提供黑白名单特权处置
- （6）支持丰富的个性化审批能力

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00128-A

★有效期：2023 年 9 月 28 日至 2025 年 9 月 28 日

所属品牌：明朝万达

发布时间：2016 年

产品适用领域：金融、政企、能源、运营商、互联网等

产品照片：



明朝万达
Wondersoft



产品咨询二维码

产品咨询邮箱：marketing@wondersoft.cn

北京数安行科技有限公司

北京数安行科技有限公司（简称数安行）是专注于数据运营安全的创新型的数据安全厂商。公司主营产品涵盖数据分类分级、数据安全风险监测与风险评估，数据安全风险态势感知，个人信息合规与隐私保护，数据安全计算与安全计量，零信任数据安全，下一代数据泄露防护、数据运营安全等，主要为数字化背景的企业提供数据安全产品和服务。数安行以 DataSecOps 为理念，以 AI 人工智能技术为核心驱动，将数据安全左移，在数据处理的第一现场对数据采取安全措施，平衡业务与安全，打造以数据运营为核心的数据安全生态体系，助力数字化转型，致力于让用户的数据安全地创造价值。数安行以承载和保护每一个用户的数据运营安全为愿景，持续创新，合作共赢，成就用户。公司核心团队拥有近 20 年数据安全领域产研和市场服务经验，技术积累雄厚，服务于金融、运营商、互联网、教育、高端制造、软件与信息技术服务、工业互联网、能源、政府等各行业客户。

网址：www.datasecops.com.cn

电话：400-118-9698

地址：北京市海淀区上地信息路 12 号中关村发展大厦 A403

产品名称：数安行数据泄露防护系统

产品概述

数安行数据泄露防护系统是一款以 AI 技术为驱动的智能数据安全解决方案。通过深度内容识别技术，对组织内的数据资产进行细致的分类分级管理，监控审计敏感数据的流转，在数据处理的过程中提供审计、追溯以及基于风险评估的自适应安全防护能力，确保数据安全。该系统执行基于内容 - 源 - 目的 - 响应的策略流程，既确保了数据资产的安全，防止了数据的违规滥用和泄露，同时也支持合法商业用途的数据处理，保障了业务流程的安全与流畅。本系统以流动数据价值保护为核心，对各种类型的数据使用及变化过程进行标注跟踪，支持数据使用链路的智能聚合及快速溯源，实时感知数据违规使用及流转风险，具备基于数据角色及用户风险的自适应精准防护能力，动态感知数据在各业务流程环节以及各类数据角色使用过程中的风险，并提供精准、适宜的防护手段，不影响数据正常流转效率及业务的正常运行。本系统全流程的数据流动治理与安全防护，无需对业务及网络进行改造，即可映射用户数据业务全流程，实现数据跟踪及风险防护体系与业务流程的独立运行，互不干扰。数安行数据泄露防护系统具备高度的弹性和可控性，使得系统能够为组织的数据安全提供强有力的保障，确保数据在流转和使用过程中的安全，同时支持业务的高效运行。

功能特点

◎统一安全管理平台：一体化弹性可扩展的管理平台，集中管理安全代理，实现统一的敏感数据智能识别、数据流转监控策略管理，对于数据流转进行集中审计及跟踪溯源。

◎轻量化：部署方式边界，资源占用低的轻量化安全代理，对性能以及用户使用习惯无任何影响。

◎AI 驱动的敏感数据深度识别：系统内置 1000+ 敏感数据分类模型，对海量数据中的敏感数据进行快速识别。基于小数据机器学习技术，自动学习新的数据分类模型，全面覆盖用户特有及新增业务数据。

◎实时监控与响应：采用人工智能技术，实时监控数据流动，快速响应潜在的数据泄露风险，实现事前预防、事中控制和事后审计。

◎自适应安全防护：基于数据安全风险智能评估模型进行自适应保护，用户体验更顺畅、业务零影响。

◎国产化支持：支持国产软硬件平台，实现国产化替代，确保数据处理全程在国内完成，增强数据安全性。

技术指标

◎数据识别：支持主流文档的识别，具备多种数据识别方法。

◎提升检测能力：AI 增强的数据泄露防护能够更准确地识别和检测敏感信息，减少误报和漏报，提高数据泄露防护的有效性。

◎数据全链路监控：具备对数据流动的监控能力，能够实时监测数据处理活动，并及时发现和处理异常事件。

◎数据追溯：具备数据追溯功能，能够对数据的访问和使用进行记录和分析，对违规行为进行追溯和取证。

◎自适应保护：具备对数据的保护能力，根据数据安全风险采取适宜的安全措施等。

◎数据可见性提升：提供数据分布的可视化呈现，帮助企业更好地了解和控制敏感数据全链路安全风险。

◎大规模部署：大规模的用户和设备管理，适应大型企业的需求，实现全面的数据安全处理。

◎高度兼容性：支持多种文件格式和系统，确保在不同业务环境中的兼容性和有效性。

◎法规遵从：帮助企业满足数据保护相关的合规要求，减少因数据泄露带来的合规风险和经济损失。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：24SS00308-A

★有效期：2024 年 3 月 15 日至 2026 年 3 月 15 日

所属品牌：数安行 DataSecOps

发布时间：2021 年 1 月

产品适用领域：金融、运营商、电力、能源、教育、高端制造、医疗、软

件与信息技术服务、工业互联网、互联网、政府等各行业客户

产品照片：



产品咨询二维码

产品咨询邮箱：sales@datasecops.com.cn

北京天空卫士网络安全技术有限公司

北京天空卫士网络安全技术有限公司(以下简称天空卫士)成立于2015年,是一家总部设立在北京经济技术开发区的数据安全技术企业。天空卫士作为国内数据安全治理的倡导者和引领者,致力于发展以人和数据为核心的新一代数据安全技术,将统一内容安全技术(UCS)和内部威胁管理技术(ITM)相融合,创立了内部威胁防护技术体系(ITP)。天空卫士是目前为止,亚太地区唯一入选 Gartner E-DLP 全球企业级数据防泄露指南、ESG 邮件安全网关市场指南和 CASB 观察者名单的中国网络安全企业。

公司自成立以来,一直保持高速发展的势头,不断强化新技术和新产品研发,完善数据安全体系。现如今,拥有七大品类,近二十种数据安全产品,并在全球率先推出数据安全治理自动化体系(DSAG)。产品已在政府、金融、高科技、制造业、大型企业以及互联网等部门和行业广泛部署并使用。

网址: www.skyguard.com.cn

电话: 010-50927295

地址: 北京市亦庄经济技术开发区宏达工业园永昌8号科技广场8660

产品名称: 数据防泄露

产品概述

天空卫士数据防泄漏系统(DLP)全面保护企业整个IT架构的数据资产,覆盖网络、终端、移动端、应用端、云端,移动端六大通道,结合行为分析和态势感知技术对入向、出向的违规行为执行监控、阻断,实现多维度、全覆盖。无论在 Web、云端、电子邮件、网络还是端点,全方位保护用户的数据安全。

功能特点

◎先进的数据收集技术,360度覆盖数据存在位置

DLP 主要功能是对数据进行处理,因此,在部署上,DLP 产品需要各种数据的收集技术将数据收集到平台上进行分析。在分析完成后,根据部署的方式和策略对数据采取动作进行处理。天空卫士 DLP 可以最大范围的完成在数据位置和应用系统的数据收集,包括网络、邮件、存储、终端等多种类型。

◎内容识别与人的行为分析相结合,提高产品易用性,减少误报。

天空卫士的内部威胁管理(ITM)技术能基于海量数据对内部用户的异常行为和内部威胁进行预测,直接以“人”为视角给出判定,抓住“坏人”,主动出击,在数据泄露之前进行阻止,并为安全分析人员提供可靠的依据

◎国际领先的机器学习技术，形成敏感数据样本模型，极大的提高数据识别的效率和准确率

可以对大量的无特定格式文件样本进行快速学习和分类，分类产生的模型（Model）可用来对数据进行分析并计算该数据是否属于某一个分类，另外可以对新的、并未出现在样本中的数据进行较为准确的预测。

◎精准的内容识别技术，可识别多种格式的数据，从源头阻止数据泄露事件的发生。

DLP 支持对图片、打印文件、红头文件扫描件、传真页、票据，表单等进行识别，并执行安全策略检查，无论是网络、邮件、还是存储通道。通过扫描笔记本、台式机、数据库等端点存储的机密数据，并可将其复制、移动至安全区域，对违规外发的数据及时拦截，不留泄密隐患。

◎记录数据的全生命周期，为合规审计提供依据

所有用户的泄露行为，系统自动监控、跟踪、记录，违规用户详细信息会精确到人、邮箱、IP，通过控制台，甚至邮件，轻松处理泄露事件，流程记录一目了然。

◎内置丰富的策略模板，简化流程，降低成本。

系统自带覆盖大量行业的策略模板库，企业可根据行业特性简单快捷的配置安全策略；同时企业可根据实际需求，灵活的设置自定义策略，且策略动态可调整，更贴近用户的实际需求，减少人力成本的投入。

◎支持多种操作系统，充分适配国内不同企业的合规需求

支持主流操作系统，如 Windows XP/7/8/10、Windows server、MacOS、Linux 等主流操作系统，同时也支持国产化 X86 统信 UOS Linux 系统、ARM 麒麟 Linux 系统。

适用群体更加广泛，可以全面了解敏感数据在员工终端的分布，以及对终端外发数据进行实时审计与保护，为数据生命周期管理流程的提供技术支撑。

◎一体化水印技术防止外部拍摄、截屏与打印泄密

天空卫士 DLP 无需部署多个 Endpoint 程序或插件，可以依据终端配置对全局或特定用户与策略启用水印技术，支持应用程序水印、屏幕水印、打印水印。

◎终端分类标签技术支持

利用数据标签技术能够监控到敏感文件全生命周期的流动，无论数据是在传输、存储、使用、共享中都可以被记录。

技术指标

作为 DLP 的核心功能，数据分析技术是最为核心的处理技术，数据分析技术的支持方式和效率直接决定了 DLP 产品在进行数据处理时的准确率和分析速度。具体包含如下：

◎文件识别技术

文件识别的最大难度在于支持文件类型的广泛性和正确性，而天空卫士 DLP 以其高性能的处理引擎都能最大化的正确识别并进行分析和处理。

◎静态对比分析技术

天空卫士 DLP 包含多达 1700 种预定义的不同行业、不同类型的组合模板。

◎数字指纹技术

◎人工智能学习技术

◎数据态势感知技术

◎数据防泄露由 UCSS 硬件平台 + UCSC 硬件平台组成，需要用户自备用户自备 WIN/MAC/Linux 的 UCSC 硬件平台。

其中 UCSS 管理平台有三个型号，分别是 UCSS-1100、UCSS-5100 硬、UCSS-11000。配置如下：

UCSS-1100 硬件平台配置：1*Xeon E3，4*SATA RAID1 硬盘，2* 千兆网口，单电源，1U 机箱；

UCSS-5100 硬件平台配置：2*Xeon E5，2*SAS+2*SATA RAID1 硬盘，4* 千兆网口，双电源，1U 机箱；

UCSS-11000 硬件平台配置：2*Xeon E5，2*SAS +2*SATA RAID1 硬盘，4* 千兆网口，双电源，2U 机箱；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230503

★有效期：2023 年 3 月 17 日至 2025 年 3 月 17 日

所属品牌：SecGator

发布时间：2015 年 11 月 12 日

产品适用领域：金融、央企、信托、互联网、保险、能源、运营商、汽车行业、钢铁、航空、医疗、军队、政府、教育、交通运输、制造、军工、央企、快递、证券、基金、房地产、银行、

产品照片：



产品咨询二维码



UCSS-5100



UCSS-11000

产品咨询邮箱：marketing@skyguard.com.cn

北京亿赛通科技发展有限公司

北京亿赛通科技发展有限公司（以下简称：亿赛通）成立于 2003 年，是绿盟科技（证券代码：300369）全资子公司。近二十年的风雨兼程，已成功打造为数据安全领域专业的综合数据安全厂商，是国家双高新企业，并获得工信部“专精特新”小巨人企业认证。签约用户过万家、800 余万终端用户，连续多年获得 CCID、IDC、中国信通院等专业机构的高度认可。

亿赛通以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行业客户核心数据资产安全。全线产品覆盖云、网、端三大类应用场景，60 款+精细化产品模块，支持结构化、非结构化和半结构化数据安全治理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。

作为拥有完全自主知识产权并取得多项国家资质认定的双高新技术企业，亿赛通现拥有产品资质 200 余项、企业资质 150 余项、荣誉奖项 300 多个、成为 50 多家联盟协会专业会员，为多个数据安全项目输送专家，参与国标、行标、政府报告及行业研究报告等 30 多项。

网址：www.esafenet.com

电话：010-57933766

地址：北京市海淀区西二旗大街 39 号 4 层 401

产品名称：数据泄露防护系统

产品概述

亿赛通数据泄露防护系统（DLP）是一款融合机器学习、关联分析、密码技术、访问控制、数据标识等多种技术的综合性数据安全防护产品，该产品以数据为中心，分类分级为基础，为用户数据资产提供事前主动防御、事中实时监测、事后追踪溯源、全程态势感知，基于数据的全生命周期提供全方位、立体化防护。

亿赛通数据泄露防护系统（DLP），由亿赛通数据泄露防护系统、客户端（Windows 端、手机端、Linux 端、国产化客户端）组成。

亿赛通数据泄露防护系统：软件，提供统一管理平台对系统进行管理，包括用户管理、策略管理、系统维护、日志报表等；

客户端：安全软件，用于对终端上的数据提供分类分级、安全防护、安全监测等防护功能；

亿赛通网络数据泄露防护系统，简称网络 DLP（NetDLP），是一款基于网络协议分析与控制技术的安全防护系统。NetDLP 集被动审计和主动防御于一体，实现网络数据传输过程中各应

用协议分析、敏感数据识别审计、阻断策略响应访问控制。网络 DLP 产品不仅能识别网络行为的合法性，还能深入到 7 层网络协议，识别网络数据内容的合法性，能有效满足客户对敏感数据防丢失泄漏的痛点需求。

功能特点

◎**数据态势分析**：对策略数据和海量数据进行多维度统计分析，按照应用协议类型维度、访问时间维度、数据分类维度、数据风险等级维度、附件类型维度、处置响应方式（全量审计 / 策略中标审计 / 阻断）等多维度可视化方式展示网络数据态势。

◎**界面可视化部署配置**：网络 DLP 产品采用 WEB 界面可视化配置部署，系统上架上电后，系统自动启动。客户只需要在 WEB 界面进行 IP 地址配置，用户添加授权即可正常使用系统，让系统配置部署不再成为头疼的事。

◎**用户分级管理**：网络 DLP 支持用户分部门 / 组管理，每个部门 / 组可以建立独立的策略组，策略组仅本部门 / 组可见。策略数据仅本部门 / 组可查看。

◎**系统运行态势一览展示**：为了让客户第一时间掌握系统当前运行的态势，产品提供了系统运行态势一览展板。在这里您可以看到当前设备 CPU，内存，磁盘，网络等硬件资源的使用情况，您还可以看到当前网络流量，系统对数据包处理情况，策略部署量，策略数据抓取量，海量审计信息量等。整个系统运行情况一目了然。

◎**组合策略设置，敏感识别更准确**：网络 DLP 产品支持多策略组合，组合策略中的各个策略之间采用“与”的关系，帮助客户进一步缩小敏感数据范围，达到更精准的识别效果。

◎**策略数据查询浏览，多角度查看数据**：产品对策略数据提供了一键式数据浏览和精细化数据查询，即方便了客户对数据粗看的省时省力也提供了客户详细查看数据的刚性需要。

◎**全流量数据解析**：网络 DLP 产品不仅支持策略审计的中标数据分析获取，同时支持了全量数据的数据分析获取。这样的产品特色功能有效的解决了系统上线初期无有效策略中标、策略设置覆盖性差、策略制定不合理等问题，保证了在策略不合适的环境下也能对数据进行审计，保证敏感数据获取的不疏漏。

◎**支持海量数据分类 / 聚类**：通过机器学习研判，对海量数据进行数据分类和聚类，机器学习样本支持离线学习后导入。

◎**文档安全防护**：文档安全可实现在不影响用户工作效率的同时保障用户数据资产安全。能够对用户数据资产进行智能分级保护，将数据防护焦点聚集在重要数据资产上，对不同重要程度数据资产施行不同强度的防护手段，帮助用户精准防护企业数据资产。同时支持用户对外发数据进行权限控制，保护脱离企业内网环境的数据文档安全可控，实现安全与效率共存，轻松保障数据资产安全。

◎**端口管控**：端口管控可对 PC 端口进行实时管控，严防企业核心数据外泄，端口管控范围包含蓝牙、光驱、串口 / 并口、USB 接口、WIFI 接口、调制解调器、红外设备等，帮助用户实时防护终端数据安全，降低数据安全风险。

技术指标

◎ NetDLP-1000 系统产品采用软硬件一体机模式，集业务平台和审计引擎于一体，支持旁路部署和串路部署，最大处理能力为 1000M（机型：2U；CPU：16 核；内存：32GB；硬盘：2*8TB；SSD：960G；网卡：集成四口千兆口；3 个扩展插槽；电源：550W 双电源）。

◎ NetDLP-2000 系统产品采用软硬件一体机模式，集业务平台和审计引擎于一体，支持旁路部署和串路部署，最大处理能力为 2G（机型：2U；CPU：20 核；内存：64GB；硬盘：2*16TB；SSD：960G；网卡：集成四口千兆口；3 个扩展插槽；电源：550W 双电源）。

◎ NetDLP-5000 系统产品采用软硬件一体机模式，集业务平台和审计引擎于一体，支持旁路部署和串路部署，最大处理能力为 5G（机型：2U；CPU：24 核；内存：128GB；硬盘：4*16TB；SSD：2T；网卡：集成 2 口千兆口，2 个万兆光网口（多模）；3 个扩展插槽；电源：550W 双电源）。

◎终端 DLP：

识别技术：支持识别技术包括关键字、正则表达式、文件属性、文档指纹、数据库指纹、文档分类、文档标签；

响应动作：支持对违规外发敏感数据行为进行阻断、警告、警告并允许用户选择是否阻断、审计、邮件告警；

传输通道：

IM 软件：微信、企业微信、钉钉、飞书、QQ、RTX

邮件客户端：Outlook、Foxmail

网盘：百度网盘（拖拽、选择上传、拷贝粘贴）

浏览器：IE、Edge、火狐、谷歌、360 安全浏览器、360 极速浏览器

文件共享、远程桌面、USB 拷贝、打印、刻录

支持自定义配置要检测的进程触发敏感内容停止使用

支持 Windows 自带共享目录文件外发检测

识别数据：支持对常用办公类文档识别，文件类型包括：Office 2007、2010、2013、2016、2019；WPS2016、2019（WPS 文件、WPS Excel 文件、WPS PowerPoint 文件）；pdf 文件、txt 文本文件、csv 文件、rtf 文件；

支持对常用压缩包文件进行识别，文件类型包括：winzip、7-zip、rar（支持 20 层嵌套非加密压缩）；

支持对图片识别，文件类型包括：jpeg、tif、tiff、bmp、png（OCR 模块单购）。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230817

★有效期：2023 年 4 月 14 日至 2025 年 4 月 14 日

所属品牌：北京亿赛通科技发展有限公司

发布时间：最新版本发布时间：2023 年 3 月 1 日。

产品适用领域：政府、金融、能源、运营商

产品照片：



产品咨询邮箱：liucunwei@esafenet.com

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

作为行业领导者，安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

2020 年 11 月 23 日，安恒信息正式成为 2022 年杭州第 19 届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

网址：<https://www.dbappsecurity.com.cn/>

电话：0571-28860999

地址：杭州市滨江区联慧街 188 号安恒大厦

产品名称：AiDLP 数据防泄漏系统

产品概述

安恒 AiDLP 数据防泄漏系统以防止用户数据资产违规或非授权输出为目标，以价值数据泄漏风险为驱动，依据数据资产特征，灵活采用深层内容分析、智能识别、实时敏感数据监测、实时告警、全方位审计等手段，实施安全域边界场景下敏感数据资产外发管控，防止安全域内部敏感信息被非授权泄漏、扩散。当数据泄漏事件发生后，系统支持快速对数据泄漏事件进行溯源分析，帮助企事业快速定位泄漏源，评估事件影响面及影响程度。

安恒 AiDLP 数据防泄漏系统的核心价值主要在：

★资产盘点及溯源分析

通过全流量监测与分析，实现企业数据资产的自动盘点与呈现，提供泄漏事件的溯源分析能力。

★高效构建行业敏感词库

快速适应行业特征，通过自动化方式快速构建敏感词库，实现对行业特定词汇的准确识别和标记，提高数据泄露监测的广度和深度。

★敏感资产流转可视化

通过文件流转链路的可视化展示，帮助用户全面了解敏感资产的传输路径和使用情况，实现对敏感资产的全方位监控和管理。

★强化员工数据保护意识

通过系统的监测分析，有效发现员工的数据泄露违规行为进行预警和通知，从而提升和强化员工的数据保护意识。

系统支持旁路部署、串接部署方式，支持加密流量解密，灵活适应客户现场部署需求。

功能特点

◎协议解析还原

产品支持对 HTTP/S、SMTP、POP3、IMAP、FTP、SMB、NFS 等协议解析，对协议所承载的数据内容进行还原，实现实时双向流量的内容审计。

◎文件内容识别

系统支持包括 Office 系列文件、图片文件、压缩文件、版式文件、网页文件、文本文件等常见办公文件类型解析和内容提取；支持多种语言识别包括中文简体、中文繁体、英文、韩文、日文等内容提取，中文简体和英文大小写自动转换；支持多种汉字编码格式识别包括 Unicode、UTF-8、GB18030 等。

◎策略规则匹配

主要包括关键词（含例外关键词）策略、正则表达式策略、文件属性（文件类型，大小，名称，作者）策略、非结构化文件指纹策略、图章策略、红头文件策略等，策略匹配功能支持“与”“或”“非”三种判断的各自组合关系，可灵活配置各类细粒度检测规则。

◎事件告警处置

针对被策略命中的数据出域行为，进行事件告警，用户可选择发送邮件、短信、钉钉等提醒措施，实现高效处置。

◎数据资产梳理

通过网络流量解析及内容识别技术，对安全域输出的数据进行梳理，形成动态数据资产目录，识别热点资产、热点输出源、资产流向、流转方式数据流动态势。

◎异常行为识别

通过采集和分析流量日志数据，可发现非工作时间操作、高频访问、超量外发、点滴式泄露等异常行为。有效追踪待离职、内鬼、粗心员工等内部风险人员的异常数据操作行为。

◎接口集成联动

系统提供开放的开发接口，供第三方系统开发及整合。可向数据分析平台导出日志和事件信息，支持 Syslog、Kafka 等。

集成 AD 域组织信息，实现的员工真实身份的关联，形成公司内部应用访问审计，对出域文件资产进行综合溯源分析，查找源头。

◎复合型指纹识别

通过提取非结构化文件的精确指纹和内容指纹，快速高效对文件内容进行精确和模糊匹配，识别变形文件输出行为，高效支撑特定文件的溯源追踪和关联文件的变形分析等业务场景，有

效保护商业秘密、知识产权、核心数据、重要数据等敏感数据。

◎预置行业策略

预置行业分类分级模模版：内置金融、电信、工业、等行业数据分类分级模版以及个人信息分类分级模版，对敏感数据进行数据分类分级标记，针对不同行业根据数据的价值、重要程度分门别类，根据数据使用过程中的敏感程度对数据进行分级，便于企业为不同级别的数据提供不同程度的安全防护。

预置行业特征策略：内置行业特征信息的策略库，包括不限于电信、金融、科技、通用敏感词汇、社会安全（涉黄涉暴）等行业特征信息及个人信息。

技术指标

◎功能指标：

具备全流量审计、1300+ 文件类型识别、正则表达式识别、数据标识符、红头文件匹配、图章识别、异常行为识别、Email 邮件识别、变形文件识别、非结构化指纹识别、结构化指纹识别、智能分类、语义模型、资产管理、查询分析、报表输出等功能模块。

◎性能指标：

系统吞吐 10Gbps；

最大并发连接数 150 万；

系统延时 $\leq 0.5\text{ms}$ ；

应用层最大吞吐率 3600 Mbps；

HTTP 协议吞吐率 3600 Mbps；

SMTP 协议吞吐率 600Mbps；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：404230808

★有效期：2023 年 4 月 14 日至 2025 年 4 月 14 日

所属品牌：安恒数盾

发布时间：2023 年 04 月 14 日

产品适用领域：政府、医疗、公安、运营商、企业、军工、教育、能源、金融

产品照片：



产品咨询邮箱：beric.liu@dbappsecurity.com.cn

杭州亿格云科技有限公司

杭州亿格云科技有限公司（以下简称“亿格云”），成立于 2021 年 7 月，总部位于杭州，在杭州和深圳设有研发中心，在北京、上海、深圳等地设有分公司。

亿格云是 SASE 安全服务商，通过自主研发的 SASE 服务平台——亿格云枢，产品提供包括零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）和统一端点管理（UEM）等功能，帮助企业以更低成本、更高效率建设更加安全、更好体验的下一代办公场景的安全体系，从而解决企业数字化转型过程中遇到的混合和分支办公安全、数据安全、终端安全等问题。

亿格云核心团队人员来自阿里云安全的产品和研发骨干，打造过多个服务超过 10 万家企业、营收破亿级的安全产品，拥有丰富的安全从业经验和极强的技术研发实力。

亿格云已服务近 200 家上市公司和独角兽企业等在内的行业客户，包括吉利控股、金地集团、零跑汽车、小红书、奈雪控股、美图、广联达等多领域头部企业，并在智能制造、金融、零售、游戏、泛互联网等行业得到客户广泛认可。

网址：<https://www.eaglecloud.com/>

电话：0571-86113822

地址：浙江省杭州市余杭区仓前街道海智中心 4 幢 8 层

产品名称：亿格云枢

产品概述

「亿格云枢」是亿格云基于云原生安全技术构建在阿里云、腾讯云、AWS、GCP 上的全球多云多活的 SASE 平台，通过 SASE 理念实现全新网络和安全架构，全平台以身份为边界，形成云网端融合云原生安全体系，以 SaaS 化服务提供零信任网络访问（ZTNA）、数据防泄漏（XDLP）、威胁检测响应（XDR）、防病毒（EPP）、上网行为管理（SWG）、统一端点管理（UEM）等安全能力，打破了企业建设办公网安全需要部署 10 多个办公安全产品且安全产品间烟囱化现状，崭新架构和安全服务为企业带来多项收益：

- ★ 对网络架构零调整和现有应用零改造，可快速收敛互联网暴露面，落地零信任安全体系
- ★ 让企业能简单实现统一管控办公网网络和安全策略
- ★ 实现总部、分支、居家办公、移动办公等不同场景下一致的高安全能力
- ★ SaaS 化部署带来的 15 分钟完成安全交付的高效运维
- ★ 全平台全功能的客户端 SDK，无缝集成到企业自有办公应用，减少推广阻力和落地工作量

★基于云原生网络构建和强化私有网络协议实现一张全球就近接入的加速网络，大幅提高跨运营商和跨境链路的访问质量，网络使用体验远优于普通互联网，同等条件下网速远高于VPN

★轻端重云、稳定高、安全功能融合，少量资源占用对终端用户的无打扰网络访问和安全防护体验

功能特点

◎ IT 管理：

包含终端管理、合规检测、外设管控、软件管理、网络准入等功能，统一管理企业办公终端，并能够基于终端的设备状态、软件、地理位置、时间等因素对终端进行动态可信分析，提供对风险人员、风险终端告警通知或拒绝入网等的管理能力。

◎内网访问：

从应用管理、应用管控、访问控制、门户应用等方面更安全、高效、可靠的解决企业内网应用连接的难题。

◎动态决策：

动态决策即根据情况的不断变化而作出决策。云枢基于终端的设备状态、软件、地理位置、时间等因素对终端进行动态可信分析，提供对风险人员、风险终端告警通知或拒绝入网等的管理能力。

◎安全防护：

安全能力一体化，融合终端威胁检测响应、病毒查杀、漏洞修复、DNS 安全、威胁情报、上网管控等安全能力，一站式解决终端遇到的安全威胁，极大地降低 IT 团队管理成本和维护多款安全产品导致的繁重工作量。

◎数据安全（XDLP）：

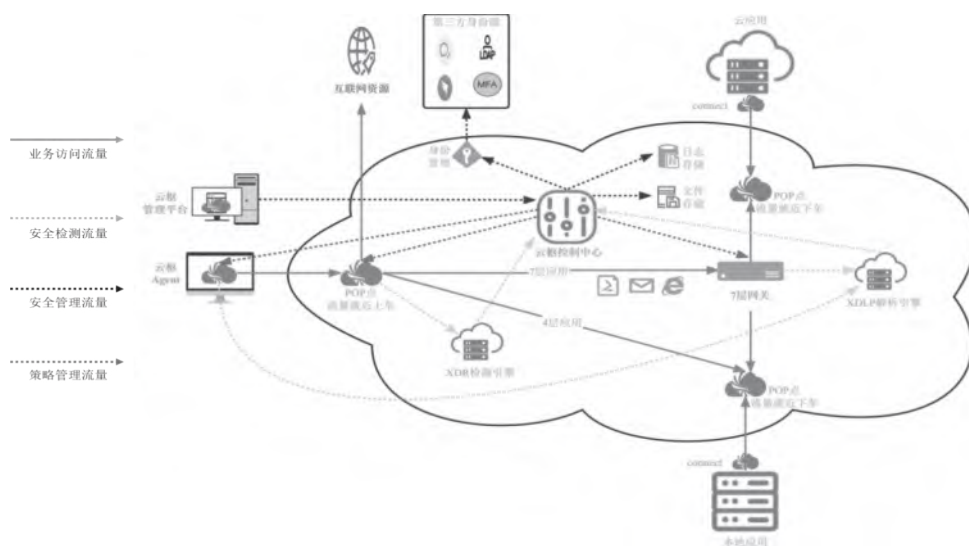
XDLP 将终端数据防泄漏（EDLP），网关数据防泄漏（NDLP）和用户行为分析（UEBA）安全能力，通过云原生的架构，进行安全融合，从而从源头解决传统单点数据防泄漏产品中遇到的难运维、高误报、高漏报、无上下文和终端用户体验差的难题。从风险人员、敏感数据、通道，三位一体一站式解决企业办公、数据安全需求。

◎日志审计：

提供全面的审计日志，系统性记录所有日志，包括内网审计日志、动态决策日志、合规检测日志、安全审计日志、数据扫描日志、操作日志、安全分析日志、应用健康检测、网络准入日志等进行集中管理和储存，轻松满足公司合规要求和审计需求。

技术指标

如上图所示，亿格云平台组件分为 Agent、POP 节点、7 层网关、Connector、XDLP 引擎、XDR 引擎、控制中心等，其中控制中心又包含管控平台、身份管理组件、对象存储组件、数据



库存储组件等。

◎ **Agent**：终端层面所有能力的集中管理客户端，与控制中心及 POP 节点通讯，具有多重作用，包括身份认证及设备基础信息上报、接收控制中心下发的终端层面管理策略及流量引流策略、通讯流量加密、证书替换、内网应用访问流量引流至 POP 节点（PA_L1_POP）、互联网需深度解析流量引流至 POP 节点（IA_POP）、上报终端侧策略执行结果及审计信息、投递审计文件及需要深度解析的文件。

◎ **POP 节点**：全球部署超 50+POP 节点，跨境访问场景下提升 80% 访问速度，私有化部署网络层通讯核心组件，POP 节点之间构建加速网络链路，按功能又区分为 IA_POP、PA_L1_POP、PA_L2_POP 等，其中 IA_POP 负责处理 Agent 引流过来的需深度解析的互联网访问流量，并代理访问互联网资源、SaaS 应用资源等；PA_L1_POP 负责处理终端引流过来的企业内部资源访问流量，对于 http、https 流量将投递至 7 层网关进一步处置，4 层访问流量直接转发至与目标应用通讯质量最高的 PA_L2_POP；PA_L2_POP 负责与就近的 Connector 建立连接，并处理 PA_L1_POP 及 7 层网关引流过来的内网访问流量，与 Connector 进行通讯。

◎ **7 层网关**：私有化部署，负责处理 PA_L1_POP 引流过来的 7 层流量及 PA_L2_POP 返回的 7 层流量，可卸载企业应用的证书进行流量处置，融合多重网关层安全组件，包括 API 访问权限控制、流量内容解析、水印网关、下载控制等。可私有化部署。

◎ **Connector**：私有化部署在客户数据中心、云内网，负责与就近 PA_L2_POP 建立链接，接收并卸载 Agent 流量加密证书、转发至对应内网应用。

◎ **XDLP 检测引擎**：处理 Agent、7 层网关无法直接处理的部分流量及文件的 DLP 解析，例如 Mail 流量、图片文件 OCR 识别。可私有化部署。

◎ **XDR 检测引擎**：处理 Agent 无法进行安全分析的文件样本，例如未知病毒文件的云查杀。

江苏敏捷科技股份有限公司

江苏敏捷科技股份有限公司（以下简称“敏捷科技”）由全球主动信息防护技术原创团队创办，是数据安全国际化领先企业和中国数据安全领域的开拓者和领跑者，致力于帮助各类企业、科研院所及政府解决数据安全与管理难题。

基于卓越的产品、强大的研发实力和前瞻的创新理念，敏捷科技获得行业内的高度认可。目前已拥有百余项软件著作权及多项国家级专利，先后荣获工信部中国信息安全最具影响力企业奖、中国网络安全和信息产业领军企业、首批工控安全服务能力咨询机构、江苏省规划布局重点软件企业、江苏省重点网安企业、江苏省专精特新企业等国家级、省部级奖项和荣誉。

敏捷科技的营销和服务网络覆盖全国，总部位于苏州，在南京、苏州两地设有研发中心，同时在全国各大城市建立稳定而完善的销售及售后服务体系。敏捷科技旗下的系列产品及解决方案已成功应用于数千万终端，产品在制造、能源、设计、交通、政府、军工、医疗、金融、教育、地产等领域得到广泛应用，累计客户量过万。先后服务了中国中车、一汽集团、东风汽车、长安汽车、南钢、沙钢、苏交科、成勘院、云南网安、泸州老窖、天合光能等国资央企或行业标杆企业，护航企业数字化转型发展。

网址：www.agile-china.com

电话：025-84521143

地址：江苏省南京市秦淮区龙蟠中路 233 号锦创中心 21 楼

产品名称：敏捷数据泄露防护系统软件

产品概述

敏捷科技数据防泄密 DLP 是一款以内容识别为核心，通过识别扩展到对数据的防控，具备智能发现、智能加密、智能管控、智能审计功能于一体的综合性数据安全产品，可帮助用户从事前预防、事中控制和事后审计对数据进行全生命周期的安全防护。作为 DGS 的数据泄漏防护模块是以监控为主，审计为辅的方式，防止员工泄露企业信息，给企业带来损失。

功能特点

- ◎敏感内容识别：系统支持关键词、正则表达式等多种方式定义敏感内容模板；
- ◎邮件管控：对邮件正文及附件内容进行过滤，涉及到敏感内容时，客户端采取相应策略控制；
- ◎即时通讯管控：使用即时通讯工具发送敏感文件时，进行警告或阻止，并有发送文件记录；

- ◎文件操作管控：管控终端上的文件操作，可以进行禁止、审计、备份等管控操作；
- ◎网络传输管控：记录终端上传到 FTP 或指定私有云盘服务器的文件日志；
- ◎异常报警：监控用户外发文件数据、大小等，超过设定的阈值即向管理员发送预警。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231910

★有效期：2023 年 06 月 05 日至 2025 年 06 月 25 日

所属品牌：敏捷科技

发布时间：2018 年

产品适用领域：电力、水利、智能制造、新能源、医疗、运营商、金融、
地产、军工、政府部门等

产品照片：



产品咨询二维码

产品咨询邮箱：nihaiyan@agile-china.com

绿盟科技集团股份有限公司

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于2000年4月，总部位于北京。公司于2014年1月29日在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有50余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和代表处，深入开展全球业务。绿盟科技高度重视安全研究和技术创新，致力于跟踪国内外最新网络安全攻防技术，星云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，分别专注于云安全、物联网安全、威胁感知与监测、漏洞挖掘与利用、数据智能、新型攻防对抗、网络空间安全战略、威胁情报八个领域，在基础安全研究和前沿安全领域进行积极的探索。基于多年的安全研究，绿盟科技为政企用户提供安全检查与评估类、安全检测与防护类、认证与访问控制类、安全审计类、安全运营及管理类等70余款高品质安全产品。其中，抗拒绝服务攻击系统（ADS）、安全和漏洞管理（AIRO）、网络入侵防护系统（IDPS）、Web应用防火墙（WAF）等多款产品获国际权威咨询机构推崇。

网址：<https://www.nsfocus.com.cn/>

电话：010-68438880

地址：北京市海淀区北洼路4号益泰大厦3层

产品名称：绿盟数据泄露防护系统

产品概述

绿盟数据泄露防护系统（NSFOCUS DLP），基于机器学习、关联分析、密码技术、访问控制、数据标识等多种技术的综合性数据安全防护产品。对数据生命周期中的各种泄密途径进行全方位检测防护，起到对敏感数据泄露行为的事前发现，事中拦截以及事后溯源。

功能特点

◎数据态势分析

对策略数据和海量数据进行多维度统计分析，按照应用协议类型维度、访问时间维度、数据分类维度、数据风险等级维度、附件类型维度、处置响应方式（全量审计 / 策略中标审计 / 阻断）等多维度可视化方式展示网络数据态势。

◎界面可视化部署配置

网络DLP产品采用WEB界面可视化配置部署，系统上架上电后，系统自动启动。客户只

需要在 WEB 界面进行 IP 地址配置，用户添加授权即可正常使用系统，让系统配置部署不再成为头疼的事。

◎用户分级管理

网络 DLP 支持用户分部门 / 组管理，每个部门 / 组可以建立独立的策略组，策略组仅本部门 / 组可见。策略数据仅本部门 / 组可查看。

◎系统运行态势一览展示

为了让客户第一时间掌握系统当前运行的态势，产品提供了系统运行态势一览展板。在这里您可以看到当前设备 CPU，内存，磁盘，网络等硬件资源的使用情况，您还可以看到当前网络流量，系统对数据包处理情况，策略部署量，策略数据抓取量，海量审计信息量等。整个系统运行情况一目了然。

◎组合策略设置，敏感识别更准确

网络 DLP 产品支持多策略组合，组合策略中的各个策略之间采用“与”的关系，帮助客户进一步缩小敏感数据范围，达到更精准的识别效果。

◎策略数据查询浏览，多角度查看数据

产品对策略数据提供了一键式数据浏览和精细化数据查询，即方便了客户对数据粗看的省时省力也提供了客户详细查看数据的刚性需要。

◎全流量数据解析

网络 DLP 产品不仅支持策略审计的中标数据分析获取，同时支持了全量数据的数据分析获取。这样的产品特色功能有效的解决了系统上线初期无有效策略中标、策略设置覆盖性差、策略制定不合理等问题，保证了在策略不合适的情况下也能对数据进行审计，保证敏感数据获取的不疏漏。

◎支持海量数据分类 / 聚类

通过机器学习研判，对海量数据进行数据分类和聚类，机器学习样本支持离线学习后导入。

技术指标

◎全网络流量信息审计获取

产品提供了全流量网络协议数据分析能力，有效的解决了策略下发不及时、不准确情况下的网络数据审计不完整的问题。

产品支持了 IPv4 和 IPv6 双栈协议，保证互联网应用协议的全面支持。

产品支持了日常用到的大部分数据访问和传输协议，并且支持对互联网应用协议的扩容定制化，保证协议数据获取的全面性和及时性。

◎准确的内容分析、识别能力

产品采用多种数据处理和运算技术，保证了数据获取、分析、识别、统计的准确性，为客户提供最佳的数据识别服务：

- ★采用多通道处理，流量智能平衡技术，实时处理网络信息，实现准确的协议信息还原；
- ★多线程、多模式并发策略识别，准确识别出网络流量中的敏感信息；
- ★多维度的信息统计方案，将信息的多个角度呈现在客户面前，实现总体信息准确掌控；
- ★采用大数据的预处理运算机制，从多个角度对信息进行分析、比对、匹配，实现了一张报表看清所有信息的能力；

◎快速的数据处理分析能力

为了保证服务响应的时效性，系统在多个角度进行成品性能提升：

- ★协议分析：采用多通道处理，流量智能平衡技术，快速实时处理数据库访问流量；
- ★策略匹配：协议分析与策略匹配在内存中进行，采用多模匹配算法，并行匹配输出；
- ★数据入库：多线程、多链接并发入库，大数据处理能力，实现数据秒级数万条写入；
- ★检索分析：采用大数据架构及分片快速索引技术，在亿级数据量下可实现秒级响应；

◎支持多种部署形式

产品在单机部署方面支持旁路部署和串路部署两种方式

- ★单机旁路部署：型号丰富，满足旁路模式下不同流量和网络接口数据处理性能需求；
- ★单机串路部署：满足 HTTPS 加密协议应用数据识别分析的客户需要，同时支持了在不同流量和网络接口下的型号细分选择；

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
- ★证书编号：24SS00961-A
- ★有效期：2024 年 7 月 5 日至 2026 年 7 月 5 日

所属品牌：绿盟科技

产品适用领域：运营商、科教文卫（高校、医疗）、政府（政法、政务）、能源、金融、企业、交通

产品照片：



奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟（CCIA）发布的 2021 年、2022 年、2023 年“中国网络安全产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神流转数据监测系统

产品概述

奇安信网神流转数据监测系统提供了一套基于流量检测的数据流转风险评估的技术手段和方法，解决企业数据暴露面梳理不清、数据网络流转途径不明、数据流转风险、数据窃取风险、可疑访问风险等无感知的问题；并且在企业正常开展数据业务的同时，能清晰掌握业务数据、个人信息、重要数据等敏感数据的流转情况，在看清数据流向的同时，能直观地看到带有个人信息、重要数据的敏感数据是通过什么人、在什么时间、在什么地点、通过什么方式、访问了什么数据、涉及到什么业务系统、发送到了哪里的整个数据流转过程。

功能特点

- (1) 丰富的应用识别特征库；
- (2) 全面的威胁检测能力；
- (3) 健全的漏洞特征库。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS024-903

★有效期：2024 年 09 月 06 日至 2029 年 09 月 05 日

所属品牌：奇安信网神

发布时间：2022 年 11 月

产品适用领域：党政、央企、电力、水利、智能制、交通、金融

产品照片：



产品咨询二维码

产品咨询邮箱：kefu@qianxin.com

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于1996年，由留美博士严望佳女士创建，2010年在深圳A股中小板上市（股票代码：002439），是网络安全产业中主力经典产业板块的龙头企业，是新兴前沿产业板块的引领企业，是可持续健康业务模式和健康产业生态的支柱企业。

2024年1月，启明星辰正式由中国移动实控，标志着公司迈入全新的发展阶段。中国移动致力于推动信息通信技术服务经济社会民生，以创世界一流企业、做网络强国、数字中国、智慧社会主力军为目标，已成为全球网络规模最大、客户数量最多、盈利能力和品牌价值领先、市值排名前列的电信运营企业。

启明星辰作为中国移动专责网信安全专业子公司，将全面贯彻“总体国家安全观”，发挥国资央企“科技创新、产业控制、安全支撑”三大作用，肩负起中国移动“安全核心技术攻坚者、安全产品服务引领者、安全运营体系支撑者”三大角色，围绕构建大网信安全板块进行战略布局，引领网络安全产业的升级与发展。

多年来，启明星辰持续深耕于信息安全行业，始终以用户的需求为根本动力，将场景化安全思维融入到客户的实际业务环境中，不断地进行创新实践，帮助客户建立起完善的安全保障体系，逐渐成为政府、金融、能源、运营商、税务、交通、制造等国内高端企业级客户的首选品牌。启明星辰入侵检测/入侵防御、统一威胁管理、安全管理平台、数据安全、运维安全审计、数据库安全审计与防护、漏洞扫描、工业防火墙、硬件WAF、托管安全服务等十余款产品持续多年保持第一品牌。

网址：<https://www.venustech.com.cn/>

电话：010-82779088

地址：北京市海淀区东北旺西路8号中关村软件园21号启明星辰大厦

产品名称：天榕数据脱敏系统

产品概述

天榕数据脱敏系统（DBMasking），是一款针对敏感数据进行抽取、转换、脱敏的数据安全产品。系统可以对多种类型数据库的敏感数据进行自动识别发现，针对用户不同的应用场景提供灵活的策略和脱敏方案配置。在帮助企业实施高效脱敏的处理的同时，提供脱敏后数据的高保真性、数据之间的关联性，充分满足用户针对不同应用场景下的各种脱敏需求，使脱敏后的数据可以安全的应用于测试、开发、分析和第三方大数据分析等环境。

产品具备高可靠性、高安全性、跨平台的特性，可从不同类型的生产数据库创建、操纵和管理所需的各类数据库脱敏任务，实现对在各种应用场景下对数据高仿真程度需求和高效

管理。

功能特点

◎**敏感数据自动识别**：通过敏感数据自动发现与内置脱敏算法联动，可自动为用户推荐合适的脱敏算法，进一步减轻用户在脱敏策略设置过程中的大量繁复的配置工作，将用户从海量的字段定义敏感数据元的工作中解脱出来，大大提高了系统的可用性。

◎**脱敏任务管理**：提供包括任务新增、任务停止、任务启动、任务暂停、任务继续等丰富的任务管理功能，并可以显示脱敏任务失败的具体时间、字段等信息。用户可在任务中定义脱敏数据来源、脱敏数据去向以及选取最适合的数据脱敏方案。

◎**脱敏数据子集定义**：针对用户实际需求场景，对源数据库抽取部分数据进行脱敏，可以按照指定列、指定行数、指定的数据内容和配置 SQL 语句等方式定义和管理数据子集。以满足用户对于生产库进行抽样、增量分发脱敏的需求，有效解决用户对于安全性或高效性兼顾的要求。

◎**数据水印**：系统支持对数据库和结构化文件添加数据水印，支持从一种数据到另外一种数据的异构方式对数据进行添加数据水印信息。数据打水印的整个过程实现自动化，水印密钥不可见，保证数据水印的密钥的安全性。

◎**数据溯源**：系统支持数据库溯源和文件溯源，满足用户不同场景的溯源需求。针对数据泄露事件，可通过泄露数据样本进行溯源追责，降低数据使用的安全隐患，提高对数据安全管理意识。

技术指标

◎**数据库兼容**：系统兼容多种关系型数据库脱敏和异构数据库间的脱敏，包括 PostgreSQL、MariaDB、DaMeng、SqlServer、Sybase、Gbase、TeleDB、Hive、DB2、MySQL、MongoDB、Informix、Oracle、Hbase、Kingbase 等多种数据库类型，同时支持对 TXT、EXCEL、DMP、CSV、DEL 等文本文件脱敏。

◎**敏感数据识别**：系统内置识、正则表达式、关键词、关键字、字段名、字段类型、备注等等方式发现敏感数据，能对姓名、手机号码、身份证号码、地址、银行卡、公司名称、工作单位、固定电话、存折账号、邮编、电子邮箱、护照号码、营业执照号码等敏感信息实现自动识别。

◎**脱敏算法配置**：脱敏算法包含数据遮蔽、固定值映射、随机脱敏、加密算法、乱序脱敏、差分隐私等。根据实际脱敏场景和需要组合成脱敏规则，也可自定义规则进行算法扩展，从而保障脱敏数据唯一性、关联性、合法性。

◎**数据水印鲁棒性**：泄露数据即使破坏，数据水印信息也可实现泄露溯源，上传泄露数据即启动溯源水印信息，数据无规律，不可见，具有非常好的隐蔽性，保证水印密钥的安全，泄露数据即使被破坏，水印信息同样可溯源。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231232

★有效期：2023 年 05 月 26 日至 2025 年 5 月 26 日

所属品牌：启明星辰

发布时间：2018 年

产品适用领域：金融、医疗、政府、运营商、电力能源等

产品照片：



产品咨询邮箱：support@venustech.com.cn



产品咨询二维码

深圳市联软科技股份有限公司

深圳市联软科技股份有限公司创立于 2004 年，专注于企业级网络安全市场，为政企客户提供网络安全产品和服务。深耕金融行业，产品已在银行、保险、证券等金融各细分领域得到广泛应用，在端点安全产品在金融领域市场份额居行业前列，并在制造业、运营商、党政军、医疗、能源和交通等行业构建了较强的市场影响力，已服务超过 3000 家高端行业客户。17 年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、并成为国内率先落地基于“零信任安全”产品的厂商之一。2019 年，联软科技并购魔方安全，获得了以攻击者视角对全网暴露面进行主动持续监控与管理的能力。近 5 年来，联软科技营收以超过 50% 的平均增速在网络安全行业高速增长，并在 2020 年引入中网投、高新投战略投资，正式成为网络安全“国家队”。

网址：<https://www.leagsoft.com/>

电话：0755-86219298

地址：深圳市南山区粤海街道科技园社区科苑路 15 号科兴科学园 A 栋 A2-901

产品名称：联软 UniDLP 数据防泄露系统

产品概述

UniDLP 数据防泄露系统以终端数据发现和数据分类分级为基础，采取用户权限控制、文件内容识别、文档透明加解密、数据安全隔离、数据安全流转、网络应用和外设管理、业务数据访问控制、水印和隐写等多种技术手段组合，通过数据活动监测、数据访问控制、数据风险评估、数据审计溯源，以业务场景为驱动保护企业所有员工终端的数据资产和数据活动，实现客户终端数据防泄露或泄露后追踪溯源。

功能特点

◎定义与发现

支持通过数据来源、文档内容来定义数据是否敏感，通过对文档格式的识别和文档内容的感知，实现对终端数据的智能分类、分级及可视化展现。

◎控制与保护

通过外发通道管控、访问权限控制、文件加解密、安全计算环境隔离、数据安全流转、行为审计与追溯等功能与技术，打造完善的数据安全防护与信息防扩散系统。

◎协同与联动

与安全数据摆渡系统协同，实现跨网或网内不同用户间的数据安全流转，通过与准入控制

系统协同，实现资源访问控制。

◎功能完整、方案成熟、大规模应用

功能完整：从准入控制到终端管控，从内容识别到数据保护，从行为分析到泄密预警，从网络到终端，从应用到内容，从已知风险管控到未知威胁发现；

稳定、易部署：不对文件染色，不改造业务系统，不影响应用访问速度，不指定文件系统类型、应用程序版本；

大规模应用：数据防护方案目前已在银行、证券、制造业、物流交通、政府、能源及电力等行业得到了广泛推广。

◎以场景驱动，最大限度保障业务效率

针对不同类型用户、数据类型、使用环境，提供多种技术手段和方案供选择，实现安全保护的“度”与业务效率的最佳平衡。

◎内置大数据引擎，保障审计追溯效果

大数据引擎支持并行计算与横向线性扩展，实现海量审计数据的高速存储、计算和分析。

◎数据防扩散

以联软科技水印技术为基础的《信息防扩散解决方案》，能很好解决企业文档在流转过程中的扩散问题。该方案包括：

- ★明文、二维码、图片、矢量（隐形水印）等在内的多种水印生成方案；
- ★可以根据设备和用户信息自动生成上述不同类型的水印效果；
- ★可以将上述不同类型的水印，根据业务系统、文件敏感级别触发式的加载到设备的屏幕上以及打印件中；
- ★员工可以通过 Web 页面上传、发布、分享、外发企业文档，管理员可对员工上述的行为进行权限管控和水印方案制定；
- ★通过将企业业务系统与联软科技的水印服务器进行对接，将上述不同类型水印嵌入到业务系统页面和从业务系统下载的文档中；
- ★除了明文水印外，还有用户无感知的矢量水印，该技术为联软的专利技术；此外，还有用户不可见的数字盲水印，仅需将截图上传，进行隐水印码解析，即可实现信息泄露追溯；
- ★触发式加载：只有在访问关键的业务系统、编辑重要的文档、打开指定的应用时才加载水印，且最大限度将水印的影响降到最低。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231411

★有效期：2023 年 6 月 9 日至 2025 年 6 月 9 日

所属品牌：联软科技

发布时间：2017 年 5 月 9 日

产品适用领域：金融、医疗、制造业、党政军、央国企。

产品咨询邮箱：Lrkjzjc@leagsoft.com



产品咨询二维码

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信数据防泄漏系统

产品概述

天融信数据防泄漏系统（简称：终端DLP）是一款专业的敏感数据发现与保护产品，产品采用模块化设计，同时引入的Docker技术、大数据分析技术等前沿技术，为终端防泄漏系统打造强悍的系统底层支撑。系统通过对PC上多种操作进行监控，对于所操作数据进行数据检测，从精确匹配的关键字到内容模糊查找，从基于文件内容到基于文件属性的检测，从被动的事件上报到主动拦截，全方位的数据安全防护措施能够真正的帮助企业实现数据安全。

功能特点

◎敏感数据发现

敏感数据梳理是数据泄露防护的关键步骤之一，通过关键字识别、正则表达式识别、文件类型识别、OCR文件识别等关键技术进行核心数据识别，能够帮助用户快速进行核心数据资产发现与梳理，并为敏感数据防护提供强有力依据。

◎敏感数据保护

敏感信息泄露防护能够有效对通过 IM 工具、网络、邮件、网盘等进行敏感数据外发或上传行为进行实时防护，防护措施包括审计、阻断、告警等，能够很好的对企业数据资产进行实时防护，帮助用户解决无法控制数据资产外泄的困扰。

◎文件分发管理

系统可以将需要下发的文件上传至管理平台进行统一管理，下发时通过终端任务统一下发，可根据实际需求设置错峰下发或者定时下发。对于可执行文件的下发，还可设置下发后是否立即运行，方便用户对企业内终端及资产进行统一管理和维护。

◎加密文件识别

文件被加上阅读密码或压缩密码后，文件内容无法被检测与识别，导致安全策略被绕过，出现敏感数据外泄风险。加密文件识别功能可精准发现该类文件，并进行有效的安全拦截。

◎屏幕水印

屏幕水印是在整个桌面上显现水印信息，水印信息包括：责任人、主机名、IP 地址、MAC 地址、登录用户、日期时间等信息，同时也支持用户自定义文字显示。一旦发生敏感数据泄露事件，屏幕水印可为企业提供有效溯源依据，管理员可直接通过屏幕水印信息快速定位泄漏源。

◎策略模板

敏感数据防泄漏策略配置较为复杂，为方便用户使用，系统提供策略模板功能，用户可通过策略模板针对不同应用场景定制专属策略模板，并在正式策略中快速复制，减少策略配置难度。

◎动态安全策略

系统提供动态安全策略，终端接入后无需手动添加策略，将自动添加动态策略，实时生效，实现真正的动态防御效果。

技术指标

支持 CentOS 和欧拉环境，采用 Docker 部署方式，能够快速恢复，横向扩展，可移植性强。

支持 win7 及以上操作系统

支持麒麟、UOS 操作系统

UOS/麒麟操作系统支持通过管控中心进行统一安装包推送和安装

系统内置数据分类库，包括：PDF、Word、Excel、PPT、Visio、AutoCAD、文本、XML、网页、EPub 电子书、微软 XPS、源代码、设计图纸、zip、rar、7zip、CAB、BZ2、ARJ、GZ、TAR、wim 等文件类型

系统内置程序分类库，包括即时通讯工具、浏览器、邮件客户端、远程协助、网盘、刻录、剪切板、打印、文件共享、移动存储等 10 大类超 30 款应用程序

系统内置关键字字典，包括：求职、合同、工资奖金、财务信息、价格信息、采购机会、产品设计文档、市场营销等超 100 大类关键字

系统内置正则表达式分类库，包括：身份证号、电话号、银行卡号、QQ 号、微信号、快递单号、生产日期等超 75 大类正则表达式

系统支持加密文件识别，能够准确识添加阅读密码、压缩密码的文件，并将文件识别为敏感文件

支持对即时通讯、邮件客户端、网盘客户端、浏览器上传、剪切板、打印、刻录、网络共享、移动存储、远程协助等外泄通道进行监控，并能够针对每个通道进行阻断、提示、审计等处理行为配置

支持屏幕水印功能，支持在屏幕水印上显示：责任人、主机名、IP 地址、MAC 地址、登录用户、时间等信息，同时还支持用户自定义显示内容

系统提供动态策略，根据终端标签定制专属安全策略

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00086-A

★有效期：2024 年 01 月 19 日至 2026 年 01 月 19 日

所属品牌：天融信

发布时间：2014 年 7 月

产品适用领域：政府、企业、能源等

产品照片：



产品咨询二维码

产品咨询 feng_chong@topsec.com.cn

远江盛邦（北京）网络安全科技股份有限公司

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全，股票代码：688651）成立于 2010 年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为用户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。公司秉持精准识别、精确防御、深入场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防护、溯源管理及网络空间地图等领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能各行业用户的数字化安全转型，护航国家网络空间安全战略实施落地。

网址：www.webray.com.cn

电话：4006-911-199

地址：北京市海淀区上地九街 9 号 2 层 209 号

产品名称：API 与 Web 安全防护系统

产品概述

API 与 Web 安全防护系统通过对访问流量进行分析，自动发现流量中的 API 接口，帮助用户快速梳理环境中未知 API 资产，并基于未知和已知 API 资产构建 API 资产画像；通过 API 资产画像，快速了解到 API 资产的访问行为以及存在的异常情况，针对性地进行安全防护和一键下线等操作，构建完整的 API 全生命周期安全防护方案。

功能特点

◎ API 资产识别

API 与 Web 安全防护系统通过对流量进行智能分析，配合机器学习引擎识别并过滤静态资源以及 html 响应中的资源，自动发现流量中的 API 接口及对应登录账号，实现 API 接口自动识别、分组管理及登录账号关联展示。

◎ API 资产画像

API 与 Web 安全防护系统采用全量分析技术精准构建 API 资产画像，帮助用户快速统计各个 API 的使用情况、安全状况和风险情况，从资产的访问次数、活跃时间、异常调用次数、漏洞个数、标签、请求方法、访问日历、资产健康状态、API 弱点详情、敏感数据泄露风险、安全风险事件等多维度进行资产画像。

◎ API 数据分析

API 与 Web 安全防护系统通过 API 数据信息态势感知大屏、可视化敏感数据流转分析、出境敏感数据合规自查多种可视化分析技术，帮助用户掌握资产风险概况及潜在隐患。

◎ API 风险识别

API 与 Web 安全防护系统通过识别资产自身安全隐患，主动对 API 接口进行漏洞扫描和评估，便于后续采取措施进行修复和加固；防护外部网络威胁，根据 API 接口的访问行为以及客户业务情况，灵活制定防护手段，如阻断、封禁、限速、黑白名单等方式，提升整体的安全防护能力。

◎ API 安全应急响应

API 与 Web 安全防护系统简化策略可在突发紧急情况下，以最快速和最直接的方式，来实现 API 资产一键下线，保证客户数据安全。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231802

★有效期：2023 年 6 月 21 日至 2025 年 6 月 21 日

所属品牌：远江盛邦（北京）网络安全科技股份有限公司

发布时间：2023 年 06 月 21 日

产品适用领域：电力能源、通信、政府、金融、教育、交通、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：support@webray.com.cn



安全配置检查产品

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 10000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.winicssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特安全配置核查系统

产品概述

威努特安全配置核查系统是一款针对资产配置进行核查的检查工具，系统采用机-机（计算机与计算机）交互方式代替传统的人-机交互方式，自动访问工业控制网络中软硬件资产，采用机器语言模拟人工访问工业控制网络资产的全过程，自动采集工业控制网络资产的安全配置并进行解析，与安全知识库中的配置要求和基线进行比对，检查安全配置符合情况，出具详细的核查报告；为工业企业用户提供常态化的安全配置脆弱性核查。

功能特点

◎丰富的配置核查项

系统内置了丰富的配置核查库，支持超过 30 个厂商 10 大类产品 65 款设备和系统，涉及 2400 多条检查项；支持 IT 信息网络和工控系统网络的配置核查，支持大数据、云计算基础设施的配置核查，核查对象和检查项支持升级扩展和自定义。

◎规范专业的配置核查库

系统内置丰富的符合各行业要求的配置安全规范，可根据需要在设备类型中选取核查项目组成规范，自定义核查规范模板，支持等保检查、工信部检查、电力检查等规范。

◎灵活的核查任务配置

系统支持对核查对象进行多维度分组核查，可以灵活设置核查对象范围、检查项粒度、核查强度、核查频度，系统提供了可视化的编辑界面，可对核查项的标准值进行修改，极大的增加了核查灵活度。

◎良好的核查环境适应性

支持在线核查和离线核查，支持跳板机，支持 RDP、WinRM、SMB、SSH 等普适性协议，具备编排调度 API，可以与第三方系统集成、调用。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00515-A

★有效期：2023 年 12 月 29 日至 2025 年 12 月 29 日

所属品牌：威努特

发布时间：2018 年 10 月 15 日

产品适用领域：电力、石油石化、轨道交通、钢铁、市政、烟草、智能制造等

产品照片：



产品咨询邮箱：support@winicssec.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

多年来，启明星辰集团持续深耕于信息安全行业，始终以用户的需求为根本动力，将场景化安全思维融入到客户的实际业务环境中，不断地进行创新实践，帮助客户建立起完善的安全保障体系，逐渐成为政府、金融、能源、运营商、税务、交通、制造等国内高端企业级客户的首选品牌。集团入侵检测/入侵防御、统一威胁管理、安全管理平台、数据安全、运维安全审计、数据库安全审计与防护、漏洞扫描、工业防火墙、托管安全服务等十余款产品持续多年保持第一品牌。

启明星辰集团积极防御实验室（ADLab）成立于1999年，是中国网络安全行业最早成立的攻防技术研究实验室之一，微软MAPP计划核心成员，“黑雀攻击”概念首推者。截至目前，ADLab通过CVE发布Windows、Linux、Unix等操作系统安全或软件漏洞1100余个，通过CNVD/CNNVD/NVDB累计发布安全原创漏洞3000余个，持续保持国际网络安全领域一流水准。实验室研究方向涵盖操作系统与应用系统安全研究、移动智能终端安全研究、物联网智能设备安全研究、Web安全研究、工控系统安全研究、云安全研究，研究成果应用于产品核心技术研究、国家重点科技项目攻关、专业安全服务等。

网址：<https://www.venustech.com.cn/>

电话：010-82779088

地址：北京市海淀区东北旺西路8号中关村软件园21号启明星辰大厦

产品名称：安全配置核查管理系统

产品概述

启明星辰针对各行业特点和安全基线规范基准，推出了专业检查平台——安全配置核查管理系统，使安全检查过程达到自动化、标准化、持续化、可视化。它可以大大提高检查结果的准确性和合规性，用以在大型企业的上线安全检查、第三方入网安全检查、合规安全检查（上级检查）、日常安全检查和安全管理任务中，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力和达到整体合规要求。

安全配置核查管理系统，主要应用于设备入网、工程验收、日常维护、合规检查等方面。通过对目标系统展开合规安全检查，找出不符合的项并选择和实施安全措施来控制安全风险。

功能特点

◎复杂网络的多渠道检查支持

支持多协议的登录检查机制：因网络环境和承载的业务不同，目标设备所开放的登录协

议也不同，检查必须支持多种协议的登录方式，支持 SSH、Telnet、WINRM、SMB、RDP、串口。

◎覆盖全面的行业规范

结合安全基线管理功能，推进系统规范流程化管理；

结合安全基线管理功能，促进原有 IT 系统的检查、整改和约束；实现安全管理工作的同步实施、发展的规范化和流程化。

产品支持等保、工信部、移动、金融、电力、中石化、烟草等各个方向的行业规范。

◎任务的多方式执行

考虑用户对于设备的管理细粒度和网络复杂度，从这两个维度出发，实现多种方式的核查任务管理：

立即扫描：从资产入手，立即检查，并对检查结果及时呈现，并完成历次检查情况的展现、结果对比分析。

定时扫描：针对组合的检查任务指定在某个时间开始核查，需要指定被检查的设备群，并对检查结果进行呈现，提供对比分析及趋势分析。

周期扫描：针对组合的检查任务提供周期性核查，需要指定被检查的设备群以及周期形态（每小时、每天、每周、每月），并对检查结果进行呈现，提供对比分析及趋势分析。

离线脚本：在目标主机上运行脚本并把结果导入到任务中即可，实现 vbs 和 session log 方式。

◎不断丰富完善的 CheckList 知识库

启明星辰多年安全服务经验积累，形成了国内最完善的专业安全服务体系和专业安全服务方法论，制定了完善详细的安全配置检查点。不断丰富基线配置检查系统 Checklist 知识库，同时可根据不同行业相关基线规范，对知识库实现定制管理，匹配各行业安全配置需求。

◎不可或缺的配置变更监测

开启系统中的配置变更功能，实现对重要配置项的变更监测。通过周期进行重要配置项的变更检查，监控系统中重要文件、端口、目录、注册表、启动项、进程等配置是否发生了异常变更，以便发现系统异常，及时采取有效的防护措施保护系统安全。

技术指标

基于抽象语法树的异构网络设备配置采集与解析技术：

◎网络设备配置采集技术

基于 ssh 命令行接口的异构设备配置采集只是执行的命令不一样，执行配置采集的操作具有相同的模式“ssh 登录 -> 执行脚本验证设备类型、版本 -> 执行配置采集脚本 -> 获取脚本回显（原始配置）”，因此，可以通过维护设备类型识别知识和配置采集知识，使得系统通过配置而不是软件更新就可以适应不同版本设备的原始配置采集，用户通过自定义设备类型识别知识和配置采集知识就可以不断扩充支持的设备类型的配置采集。

◎网络设备配置解析技术

配置自动化核查系统的一个主要技术难点是不同厂商、不同型号的设备配置语法语义经常不统一，如果直接针对原始配置的文本进行核查算法设计，算法实现需要花费大量精力进行各种文本信息的处理，导致开发效率低下、容易出错、兼容性差。由于网络设备提供给用户访问的配置都是按照厂商定义的语法进行描述的文本，因此可以利用成熟的词法、语法分析技术，将配置的文本分析交给基于语法分析的配置解析与翻译模块，将配置翻译成统一描述的结构信息，基于结构化的配置信息简化配置核查算法的实现，提高算法的设备兼容性和开发效率。

◎配置解析与翻译技术方案

采用 ANTLR 生成网络设备配置的词法、语法分析器，自动生成设备配置的抽象语法树和树的遍历器，通过语法树分析的监听器机制实现异构网络设备配置翻译成统一描述结构的配置信息，基于统一结构的设备配置信息可以为配置核查算法屏蔽异构设备的差异性。

◎多协议登录认证技术：

为了保证目标网络环境的基线配置安全性，又因为大部分的主机及应用组件的安全配置文件权限较高，在非登录情况下无法进行基线的安全配置检查，所以配置核查分系统需要使用远程登录的方式，精准核查基线配置的安全性。

★配置核查分系统的采集层综合了多种常用协议，如 SSH、Telnet、RDP、串口等协议，当任务被调度时，可实现以管理员权限通过，远程密钥加密连接或串口直连方式登录目标操作系统，并通过运行 shell、bat 命令进行交互，保证交互过程的安全性。

★通过 XML ExpectItem，配置系统登录，采集过程中交互参数及交互动作，实现登录采集结果获取自动化，错误信息展示灵活丰富。

网络安全专用产品安全认证或安全检测结果证明

(1) 网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS002056-A

★有效期：2024 年 2 月 8 日至 2025 年 2 月 10 日

(2) 网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00206-A

★有效期：2024 年 2 月 8 日至 2025 年 2 月 10 日

所属品牌：启明星辰和网御星云

发布时间：2009 年

产品适用领域：运营商、政府、金融、军队、企业、电力、公安等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

深圳万物安全科技有限公司

深圳万物安全科技有限公司（简称“万物安全”）围绕战略新一代信息技术产业，聚焦网络安全新质生产力“AI+ 物联网安全”，“颠覆式创新和硬科技”实力获得工信部“网安中心”和“火炬中心”高度认可并获奖，连续三年被“全球权威咨询机构 IDC- 金融视频物联安全”分析报告评为第一、国家保密局百家信创单位之一、中国网络安全产业联盟理事单位、关键信息基础设施安全保障联盟副理事长单位。

万物安全产品和解决方案，基于云原生和零信任架构，融合 AI、信创、数据安全等最新技术，为金融、能源、医疗、交通等提供全生命周期的物联网安全运营和管控能力，满足《网络安全法》、《关基保护条例》、《网络数据安全条例》等国家政策法规要求，已成为物联网安全领导者。

网址：<https://www.iottepa.com>

电话：0755-26658957

地址：中国·深圳·福田·国际金融科技城 6 楼

产品名称：安防网安全检测

产品概述

产品针对安防网应用场景下的资产管理与安全运营痛点问题响应相关政策法规要求，重点帮助企业客户对安防网资产进行运维管理与安全检查，实现对网络资产的发现识别、资产台账核查、风险评估、合规评分、检查报告生成，让企业单位及时发现问题、整改问题，提高安全防护水平，确保安防网应用业务建设的持续安全可靠。

功能特点

◎资产发现识别

通过主动探测方式，实现全网安防设备的资产发现和识别，建立全网动态资产台账，及时发现未纳管资产；

◎安防网漏洞检测

具备专业安防网漏洞库，并定期更新，可按照自身需求自定义风险扫描时间，识别全网安防设备漏洞风险

◎弱口令风险检查

集成丰富的弱口令字典库，支持自动检测资产的弱口令风险并在弱口令列表中展示

◎视频存储完整性检测

定期检查网络内 NVR、DVR 的录像状况，查看是否有漏录情况的发生，同时系统可根据不

同行业对于视频存储天数的要求，设定不同的存储天数阈值，若不满足设定的存储天数，即产生告警

◎非法 DHCP 检测

支持检测网络中是否存在非法 DHCP 服务器，检测的风险问题及时展现在风险列表中

◎自动化生成报表

自动生成包含资产信息、各项风险安全检测信息等分析报告，支持依据《银行业金融机构安全评估》网络安全检测标准并输出专项检测报告

技术指标

◎支持根据不同的检测目标选择安防资产扫描、安防漏洞检测、弱口令风险检测、视频漏录检测、录像保存天数不达标检测、非法 DHCP 检测等检测类型；

◎支持配置视频存储达标天数和漏录秒数，检查录像存储合规情况，支持目标 NVR 网络连通性测试，支持一键导入录像机联动配置；

◎支持联动网络交换机发现网络资产，支持一键导入交换机联动配置；

◎支持非法 DHCP 发现检测；

◎自动生成分析报告，包含资产信息、各项风险安全检测信息、汇总统计信息等，支持按名称搜索检测报告，提供评估报告的在线预览和文件下载功能；

◎支持根据《银行业金融机构安全评估办法》4095 号文新增的网络和数据安全相关的内容，进行评估检测，评估出相应的扣分情况及报告；

◎支持记录用户所有操作行为；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231311

★有效期：2023 年 06 月 02 日至 2025 年 06 月 02 日

所属品牌：万物安全产品体系 -LA 标品

发布时间：2024 年 9 月 13 日

产品适用领域：金融业、交通行业、医疗行业、教育行业

产品照片：



产品咨询二维码



产品咨询邮箱：huangjt@iottpa.com

远江盛邦（北京）网络安全科技股份有限公司

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全，股票代码：688651）成立于 2010 年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为用户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。公司秉持精准识别、精确防御、深入场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图等领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能各行业用户的数字化安全转型，护航国家网络空间安全战略实施落地。

网址：www.webray.com.cn

电话：4006-911-199

地址：北京市海淀区上地九街 9 号 2 层 209 号

产品名称：一体化漏洞评估系统（RayScan）

产品概述

一体化漏洞评估系统（RayScan）是一款针对设备入网、网站上线、日常运维、安全事件脆弱点分析、等保合规等场景提供的一体化脆弱性分析与评估产品。能够为监管、能源、金融、教育等行业用户提供涵盖系统漏洞检测、Web 漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测在内的五合一脆弱性检测能力。

系统基于盛邦安全多年漏洞发现和安全服务经验，结合高效的主机存活探测技术及精细化的爬虫等技术，通过对主流操作系统、Web 站点 / 应用、数据库、网络设备、各种常见应用等的深入扫描，帮助用户在安全事件之前发现潜在风险，在漏洞窗口期跟踪修补情况，以及在安全事件之后定位脆弱点从而进行整改。系统持续致力于提升检测准确性及全面性，为用户提供准确的分析结果和专业的整改建议。据国际知名调研公司 IDC 统计，盛邦安全一体化漏洞评估系统（RayScan）近年来市场份额稳步增长，市场占有率位居国内前三甲。

功能特点

一体化漏洞评估系统（RayScan）提供五合一的安全扫描能力，对网络环境中各个网元进行脆弱性检测。

◎系统漏洞扫描

支持针对网络环境中的各种主机、交换机路由器、防火墙、中间件等存在的常见漏洞、典型漏洞（如心脏出血）、0day 漏洞等进行扫描和检查。具体功能如下：

★支持扫描通用操作系统，涵盖 Windows 系列、苹果操作系统、Linux、AIX、HPUX、

IRIX、BSD、Solaris 等。

★支持扫描交换路由设备，涵盖 Cisco、Juniper、华为、F5、Checkpoint、锐捷在内的主流厂商的设备。

★支持扫描安全设备，涵盖 Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto、华为在内的主流厂商的防火墙等安全设备。

★支持扫描物联网设备，如主流厂商海康威视、宇视、华为、大华、Brickcom、索尼、TP-LINK、AXIS、佳能等的摄像头，三星、惠普、爱普生、佳能等厂商的打印机。

★支持针对工控专用设备包括 PLC、SCADA、DCS、工控专用网络设备的漏洞扫描。

★支持国产操作系统、数据库的扫描，国产操作系统包含中标麒麟、凝思、华为欧拉、深度、红旗、中兴新支点，国产数据库包括神通、人大金仓、南大通用、达梦。

★支持大数据组件框架漏洞检测，如 zookeeper、ElasticSearch、ActiveMQ、Kibana、Hadoop 等。

◎ Web 漏洞扫描

系统支持检测网站存在的 OWASP Top10 定义的 Web 漏洞如注入（SQL 注入、Cookie 注入、XPath 注入、代码注入、框架注入、Base64 注入、命令注入、操作系统命令注入）、XSS 跨站脚本、伪造跨站点请求（CSRF）、网页挂马、暗链、敏感信息泄露、安全配置错误等漏洞风险。并直观展示出来，便于快速定位。

◎数据库漏洞扫描

采用先进的数据库发现技术和实例发现技术等，可针对当下主流的数据库，如 Oracle、MySQL、Postgres、IBMDB2、MongoDB、SQLServer、Informix、Sybase 等进行漏洞检测，包括对数据库系统的各项设置、数据库系统软件本身已知漏洞、数据库系统完整性进行检查和对数据库系统的整体安全性做出评估，并给出提高数据库安全性的修复建议。通过登录扫描可对数据库的系统表甚至字段进行安全检测。

◎安全基线检测

参考国内外标准、行业技术规范和安全运维最佳实践构建了以业务系统为核心，覆盖业务层、系统支撑层的安全配置基线模型。从业务系统安全要求出发，将要求分解到对应的支撑系统的具体安全要求。可以支持在线和离线两种形式下发任务，支撑系统包括操作系统、数据库、中间件和应用系统，还包括网络设备和安全设备等。针对这些支撑系统的具体产品类型如 Windows、Oracle、WebLogic、交换机、防火墙等，根据具体的安全要求可细化到可执行和实现的具体要求，并可以对同类设备，不同品牌型号，形成具体的安全要求及配置检查方法。

◎弱口令

对系统存在的弱口令做检测，支持知名的协议、数据库、中间件、HTTP 服务、HTTPS 服务和摄像头检测如 TELNET、FTP、SSH、POP3、RDP、SMTP、Oracle、MySQL、PostgreSQL、MsSQL、Sybase、Informix、HTTP、大华摄像头、华为摄像头等。系统内置默认的字典库，并

支持上传自定义的字典库，丰富平台弱密码检测能力。

技术指标

系统能提供五大扫描模块，包含系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查，可灵活修改每个模块的配置参数以满足不同场景下的扫描需求。

支持部署在 IPV4、IPV6 环境下，且系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查等各类型任务均支持添加 IPv6 扫描目标。

支持多路扫描，除管理口外，设备所有网口均可用于扫描，支持同时对多个隔离子网进行扫描。

提供快速上线向导，首次登录时能在快速向导指引下一步一步完成上线部署配置。

支持自定义访问控制策略，能够限制访问系统的源 IP，能够限制访问系统的方式，如仅支持 Web 访问或仅支持 SSH 访问。

支持针对指定 IP 段，同时一键下发系统扫描、Web 扫描、弱口令扫描任务，Web 扫描能够自动发现该网段内的在线网站并开展扫描。

支持筛选任务列表中已完成的任务，批量导出离线报表。

系统应支持实时显示扫描进度及结果，能够在扫描过程中实时查看主机信息及漏洞信息。

支持一键复制指定任务的配置，针对新的扫描目标创建相同配置的任务。

支持自定义任务执行方式，支持立即扫描、定时扫描、周期性扫描等多种扫描方式，周期扫描时间可精确到每天、每周或每月的某天、某时、某分。

支持检测的系统漏洞数不少于 35 万，覆盖 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 多种漏洞标准。

支持通过 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP、WMI、RSH、REXEC、WINRM、SNMP 等协议对目标主机进行深度登录扫描。

支持自动探测指定 IP 段的已知、未知 Web 站点，并可一键转为 Web 资产或一键下发 Web 扫描任务。

支持 Web 应用系统登录验证功能，验证 Web 登录认证信息的正确性，以确保登录扫描正常执行。

支持中间件弱口令检测，包括但不限于：Tomcat、WebLogic、JBoss、WebSphere、GlassFish。

支持摄像头弱口令检测，包含主流厂商摄像头如大华、华为、宇视、海康。

支持离线导出报表，报表支持 Excel、Word、HTML、PDF、XML 格式，用户可以直接下载报表或系统自动发送报表到对应管理员邮箱和 FTP 服务器。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS013-163

★有效期：2021 年 6 月 18 日至 2026 年 6 月 17 日

所属品牌：远江盛邦（北京）网络安全科技股份有限公司

发布时间：2010 年

产品适用领域：电力能源、通信、政府、金融、教育、交通、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：support@webray.com.cn



运维安全管理产品

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区上地东路 1 号院华控大厦 7 层

产品名称：电力监控系统便携式运维网关

产品概述

电力监控系统便携式运维网关是珞安科技为解决电力监控系统运维过程中的种种漏洞和安全隐患而研发的一种运维安全隔离设备，通过串接在运维终端与被运维对象之间，配合 USBKEY 使用，运维成员、运维工具等外部要素与被运维对象等内部要素进行隔离，并对工作班成员的敏感操作、违规行为和运维工具的运行风险进行实时监督管控，防止外部网络攻击、恶意代码、违规操作等行为破坏内部系统。同时，对运维工作全过程进行日志、屏幕录像、通信报文等多维度记录，实现内部系统运维工作事前有防范、事中有监督、事后有审计的目标。系统由内置客户端安全专用密盾（用于运维终端）和平板式便携专用硬件装置构成，对整个运维检修过程进行安全管控。

功能特点

◎运维权限管控

系统支持静态口令、生物特征信息、USBKEY 等多种方式实现人员身份认证，遵循三权分立和最小权限原则。

◎恶意代码检测

对接入工控系统实施运维的厂家电脑以及需要进行下装的工程文件进行恶意代码检查，

防范病毒感染。同时，对具有恶意代码的文件进行隔离处理，并将该文件进行取证、归档和管理。

◎高危指令管控

限制运维人员可使用的运维操作命令，规避误操作引起的潜在生产事故；支持风险指令和控制类指令的告警和二次授权。

◎违规外联管控

密盾实时监测运维终端的外设状态，包括 USB 端口以及冗余网卡等；防止在运维过程中，运维终端的文件拷贝行为以及连接互联网的行为，有效遏制病毒网络入侵的潜在风险。

◎多场景运维

涵盖网口运维、串口运维、USB 运维和 KVM 运维等工业现场常见场景的运维需要；既支持传统的命令行运维、界面运维，也支持各种工控协议运维；同时，还提供旁路运维、渗透运维、快速运维等一些特殊场景下的运维诉求，满足安全监管的同时兼顾运维便利性。

◎网络通信代理

系统默认阻断内外网的所有通信通道，根据授权动态开启运维通道，采用通信代理的方式对运维中的多种协议实现透明转发和数据阻断告警，避免了直接通信带来的各种安全隐患，从而有效地提高现场运维的安全性。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01621-A

★有效期：2024 年 11 月 1 日至 2026 年 11 月 1 日

所属品牌：珞安科技

发布时间：2020 年 9 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业

产品照片：



产品咨询邮箱：support@icssla.com



产品咨询二维码

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISA Secure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 6000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.wincssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特安全运维管理系统

产品概述

威努特安全运维管理系统是集用户（Account）管理、授权（Authorization）管理、认证（Authentication）管理和审计（Audit）管理于一体的集中安全运维管理系统。该系统能够为企业提供集中的管理平台，减少系统维护工作量；能够为企业全面的用户和资源管理，减少企业的维护成本；能够帮助企业制定严格的资源访问策略，并且采用强身份认证手段，全面保障系统资源的安全；能够详细记录用户对资源的访问及操作，满足对用户行为审计的需求。

功能特点

◎清晰化的运维大屏展示

支持管理员首页拓扑图，包括运维用户、资产、资产组，并实时监测运维用户与被运维资产之间的运维关系，展示运维用户名称、运维方式、上次登录时间，展示资产名称、资产 IP、资产类型等信息。

◎全面的工业现场业务支持

全面支持工业现场上位机、服务器、工业网络设备、应用系统、数据库、安全设备等资产

的安全运维管理。

◎全面的运维协议支持

全面支持字符运维（SSH、Telnet）、图形运维（VNC、RDP）、文件传输（FTP、SFTP）、数据库运维（Mysql、SqlServer、Oracle 等）、WEB 运维（Https、Http）等。

◎多元化的认证授权体系

支持本地认证、LDAP 认证、RADIUS 认证、USB key 认证等多种认证方式，并可根据用户实际需求，设置混合认证方式，不同主账号采取不同的认证方式，实现按需认证。

◎灵活多样的登录方式

支持运维人员通过浏览器或第三方客户端工具（xshell、SecureCRT、putty 等）登录到运维设备或系统，最大程度上保证运维人员的操作习惯不被改变。

◎全过程的运维行为审计

产品可以完整审计运维人员从登陆到退出的全过程，最大程度上保障用户的运维管理工作。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230867

★有效期：2023 年 04 月 21 日至 2025 年 04 月 21 日

所属品牌：威努特

发布时间：2019 年 4 月 1 日

产品适用领域：电力、石油石化、轨道交通、市政、烟草、智能制造等

产品照片：



产品咨询邮箱：support@winicssec.com



产品咨询二维码

北京亿赛通科技发展有限公司

北京亿赛通科技发展有限公司（以下简称：亿赛通）成立于 2003 年，是绿盟科技（证券代码：300369）全资子公司。近二十年的风雨兼程，已成功打造为数据安全领域专业的综合数据安全厂商，是国家双高新企业，并获得工信部“专精特新”小巨人企业认证。签约用户过万家、800 余万终端用户，连续多年获得 CCID、IDC、中国信通院等专业机构的高度认可。

亿赛通以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行业客户核心数据资产安全。全线产品覆盖云、网、端三大类应用场景，60 款 + 精细化产品模块，支持结构化、非结构化和半结构化数据安全治理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。

作为拥有完全自主知识产权并取得多项国家资质认定的双高新技术企业，亿赛通现拥有产品资质 200 余项、企业资质 150 余项、荣誉奖项 300 多个、成为 50 多家联盟协会专业会员，为多个数据安全项目输送专家，参与国标、行标、政府报告及行业研究报告等 30 多项。

网址：www.esafenet.com

电话：010-57933766

地址：北京市海淀区西二旗大街 39 号 4 层 401

产品名称：数据库运维安全管理系统

产品概述

亿赛通数据库运维安全管理系统（ESAFENET DOSM）是一款具备全面运维管理、数据资产监控、安全合规审计等多能力、综合性数据安全产品。

产品可规范数据运维操作流程，监控分析运维活动，主动防御风险行为。亦可进行独立部署与配置，最大限度不改变现网环境的前提下达到运维管理、安全防护和分析溯源的目的。提供运维工单管理、账号管理以及基于 SQL 协议分析技术下的主动防御与检测系统，起到有序、合规、安全的数据运维操作与管理。支持国际通用、国内主流以及非关系性大数据、数据仓库等资产环境下的数据运维管理，且不会损耗和影响数据库性能。针对运维期间涉及敏感数据的使用，提供了完全透明、实时的对敏感数据掩码能力。还提供了诸如：屏蔽、重置、仿真、映射等多种脱敏算法。运维行为发生后，会从语句、会话、IP、数据库用户、业务用户、响应时间、影响行数等多种维度进行运维操作记录和事后分析，为运维管理与追责提供溯源依据和证据来源。在运维审计报表方面，提供各种合规性报表以外，还提供报表自定义能力。用户可以根据自身需求选择报表内容和形式，创建自己所需报表；除了在线报表以外，系统还提供周期

性报表，包括：日报、月报、周报、自定义周期报表等形式。

功能特点

◎**资产自动发现**：系统通过对数据库流量采集和数据解析，利用各数据库类型的协议特征，实现对不同类型数据库的自动识别。同时，可从协议内容中获取到更为精确的数据库参数，数据库自动发现信息，经用户手工确认并完善后，即可将被发现的数据库加入到防护对象中。

◎**资产发现与分类分级**：支持静\动态扫描、手动添加等多种资产发现方式，自动发现数据资产的基本信息；支持数据库资产的分类分级，功能以已授权数据资产为基础，依据行业标准预制的规则，对资产的内部数据进行自动随机抽样，识别解析，发现敏感数据，并对敏感数据进行分类分级打标。

◎**漏洞风险监测与评估**：支持国内外主流数据库的安全检查与漏洞发现；通过风险评估量化资产风险等级，并给出问题修复建议。

◎**运维工单管理**：产品提供运维工单管理能力，统一运维登录入口，约束运维访问行为，防止非法访问行为对核心资产、数据造成负面影响。运维申请支持：访问源（IP、数据库用户、客户端工具）、访问对象（数据库、表等）、运维行为（支持 SQL 操作类型、运维 SQL 语句、运维脚本）、执行时间范围等维度细颗粒化行为申请，并且支持最大支持不少于 10M 的脚本运维脚本上传。

◎**身份认证管理**：产品提供多因子运维身份认证机制，包括：Ukey、Web 口令认证、动态令牌认证、审批口令认证以及终端零信任。用于解决多人一账号、一人多账号以及运维环境共享场景下的运维身份鉴别及权限控制问题。

◎**访问检测与防御**：针对不同的运维人员提供敏感表的操作权限、访问行数和影响行数的控制，以及限制 NOWHERE 查询和更新，同时配合 SQL 白名单和 SQL 黑名单，对访问行为进行快速判断。符合运维工单申请动作得进行快速放行，不符合工单特征的运维操作进行实时阻断，阻止非法运维操作，避免 7 亿赛通数据库运维安全管理系统白皮书免大规模数据泄露和数据篡改事件的发生。同时，产品提供精细化的权限控制系统，包括：用户、终端、对象、时间等元素。在控制操作中增加了 Update Nowhere、delete Nowhere 等高危操作；控制规则中增加返回行数和影响行数控制。

◎**敏感数据脱敏**：通过灵活应用脱敏规则，脱敏规则包含了敏感数据特征以及对于这类数据的脱敏算法。

运维操作记录：经过通信协议解析和 SQL 语法分析，获取运维会话和操作行为相关信息，形成记录并保存。

技术指标

◎ DAS-DOSM 2000 平台系统（1U，包含单电源模块、2*USB 接口、1*RJ45 串口，2*GE 管理口，4 个接口扩展槽位，16G 内存，4T SATA 硬盘，提供数据安全运维管理能力，默认支持

32 个数据库实例。) 数据库网络吞吐量为: 200Mbps, SQL 处理性能 10000 条 / 秒。

◎ DAS-DOSM 5000 平台系统 (2U, 包含冗余电源模块、2*USB 接口、1*RJ45 串口, 2*GE 管理口, 8 个接口扩展槽位, 32G 内存, 4T SATA 硬盘, 提供数据安全运维管理能力, 默认支持 64 个数据库实例。) 数据库网络吞吐量为: 500Mbps, SQL 处理性能 20000 条 / 秒。

◎ DAS-DOSM 10000 平台系统 (2U, 包含冗余电源模块、2*USB 接口、1*RJ45 串口, 2*GE 管理口, 4 个接口扩展槽位, 128G 内存, 4T*3 SATA 硬盘, 提供数据安全运维管理能力, 默认支持 64 个数据库实例。) 数据库网络吞吐量为: 800Mbps, SQL 处理性能 40000 条 / 秒。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号: 0404230637

★有效期: 2023 年 3 月 31 日至 2025 年 3 月 31 日

所属品牌: 北京亿赛通科技发展有限公司

发布时间: 最新版本发布时间: 2023 年 3 月 14 日。

产品适用领域: 金融、能源、医疗、运营商

产品照片:



产品咨询邮箱: liucunwei@esafenet.com



产品咨询二维码

北京云弈科技有限公司

北京云弈科技有限公司是一家专注于自主研发的国家高新技术企业和“专精特新”企业，致力于国家网络空间安全监测、防护和治理，聚焦于攻防能力与产品能力一体化输出的安全服务商。

基于实战对抗优势，构建了六位一体的纵深安全防御体系，研发出云戟主机自适应安全、弈盾网站云防御、天视资产风险监控、云弈国密堡垒机、海御异常流量清洗、幻鲸网络诱捕等系列产品，完成了产品与各类国产化操作系统、国产化芯片的适配，实现了自主可靠、安全可控。同时也提供渗透测试、红蓝对抗、重保服务、应急响应、等保咨询、密评咨询等安全运营服务，为各行业提供攻防一体化解决方案。

凭借攻防一体化安全能力解决方案，已获得了政府、运营商、金融、能源、教育、互联网等行业的数千家客户应用与认可。云弈科技致力于国家网络空间安全的技术创新和服务输出，积极履行社会责任，为构建安全可靠的数字化强国贡献力量。

网址：www.yunyisec.com

电话：010-60555155

地址：北京市通州区光华路甲 1 号院 27 号楼 302

产品名称：统一安全运维管理系统

产品概述

统一安全运维管理系统是内置生物识别认证的堡垒机，用于对第三方或内部运维管理员操作行为进行集中管控审计的平台。可帮助客户规范运维操作行为、控制并降低安全风险、满足等级保护及其他法规对 IT 内控合规性的要求。

功能特点

◎国产化适配、国密算法

适配主流的国产化操作系统和主流的国产化 CPU；采用国密算法加密客户端传输通道和目标服务器传输通道。

◎集中账号管理

对所有服务器、网络设备账号进行集中管理，完成对账号整个生命周期的监控和管理，降低管理大量用户账号的难度和工作量。

◎统一身份认证

提供静态密码、动态口令、短信认证、证书认证、指纹识别认证以及第三方认证等多种认

证方式，提高对用户认证的安全性和可靠性。

◎细粒度资源授权

提供统一的界面对用户、角色及行为和资源进行授权，达到对权限的细粒度控制，可以对各自的管理对象进行授权。

◎细粒度访问控制

采用细粒度的命令策略，管理员会根据其角色为其指定相应的控制策略来限定用户，最大限度保护用户资源的安全。

◎加强操作审计

加强审计操作人员的账号使用（登录、资源访问）情况、资源使用情况等，更好地对账号的完整使用过程进行追踪。

◎完善的多维审计

支持日志、会话、录像回放及同步监控等多种审计方式。

◎无控件式安装

支持 Web (H5) 免客户端模式，无需安装控件，操作便捷。

◎全自动化运维

针对重复性的运维工作，支持预置脚本和任务，定期的自动化执行。

技术指标

◎基础版：起始 50 管理设备数，最多可管理 150 设备数。

支持生物指纹认证及二代证身份认证，支持旁路、VPN 部署模式，支持 SSH/RDP/Telnet/Rlogin 动态智能命令识别、监控、屏幕录相及回放，支持 oracle/ftp/web 的审计、命令识别及回放，支持 Linux/Unix/ 网络设备的配置文件审计功能。

专业版：起始 200 管理设备数，最多可扩展到 300 设备数。

支持生物指纹认证及二代证身份认证，支持旁路、VPN 部署模式，支持 SSH/RDP/Telnet/Rlogin 动态智能命令识别、监控、屏幕录相及回放，支持 oracle/ftp/web 的审计、命令识别及回放，支持 Linux/Unix/ 网络设备的配置文件审计功能。

◎增强版：无设备数限制。

支持生物指纹认证及二代证身份认证，支持旁路、VPN 部署模式，支持 SSH/RDP/Telnet/Rlogin 动态智能命令识别、监控、屏幕录相及回放，支持 oracle/ftp/web 的审计、命令识别及回放，支持 Linux/Unix/ 网络设备的配置文件审计功能。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查认证和市场监管大数据中心

★证书编号：CCRC-2024-CS035-719

★有效期：2024 年 4 月 08 日至 2029 年 4 月 07 日

所属品牌：云弈科技

发布时间：2017 年

产品适用领域：政府、运营商、金融、能源、教育、互联网等

产品照片：



产品咨询二维码



产品咨询邮箱：feiyang.kong@yunyisec.com

北京长亭科技有限公司

长亭科技是国际顶尖的技术驱动型安全公司，全球首发基于智能语义分析的下一代 Web 应用防火墙产品，成为中国 WAF 市场份额占有率增速最快的下一代网络安全公司。目前，公司已发布 10 余款自研技术驱动产品，形成以攻（安全评估系统）、防（下一代 Web 应用防火墙、高级威胁分析预警系统）、知（安全分析与管理平台、攻击面管理运营平台）、查（主机安全管理平台）、抓（伪装欺骗系统）为核心的新一代安全防护体系，并提供优质的安全测试及咨询服务，为企业级客户带来智能的全新安全防护思路。

网址：www.chaitin.cn

电话：4000-327-707

地址：北京市朝阳区天辰东路 7 号楼 -2 至 8 层 101 内北区 6 层 602 室

产品名称：长亭运维审计与管理系统 V2.0

产品概述

长亭运维审计与管理系统是集用户（Account）管理、授权（Authorization）管理、认证（Authentication）管理和综合审计（Audit）于一体的集中运维管理系统。能够为用户提供全面的用户和资源管理，制定严格的资源访问策略，通过身份认证手段，全面保障系统资源的安全；可详细记录用户对资源的访问及操作，达到对用户行为审计的需要，减少系统维护工作，提高工作效率。

功能特点

◎多元化的认证方式

自身提供了证书认证、手机动态令牌、M A C 地址认证、A D 域认证等服务，也可与第三方 C A、动态令牌等进行结合。支持任意组合认证，提高访问的安全性。

◎强大的资源管理能力

支持柱形图方式查看系统中不同资源所占比例，包括 Unix 资源、网络资源、windows 资源、数据库资源、C/S 资源、B/S 资源等。支持按资源类型上传资源管理驱动程序，可使资源的管理更具有针对性。支持应用发布代填驱动自定义上传，针对不同应用资源，采用相对应的代填脚本。

◎账号的全生命周期管理

主账号支持分组管理，分组可以采用树形方式展现，不限制分组层级数量，具备完整的用户账号、从账号、同步等管理功能。支持手动登录账号、口令自动添加功能，操作员单点登录

时，手动输入的账号、口令，系统会自动添加到该资源账号列表中，避免重复添加。

◎灵活的授权管理功能

支持角色管理、岗位授权、资源自动授权，资源账号批量授权等灵活配置管理功能。

◎全面的审计管理

图形资源访问时，支持鼠标、键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放。支持 Windows 图形审计的监控，管理员可以随时查看运维人员的操作，并且可以发送告警信息进行会话锁定和解锁。图形审计支持画质如灰度、灰度低级的设置，帧间隔，压缩比等设置；采用 ES 搜索引擎，审计数据查询速度更快，结果更准确；所有审计回放及监控操作，均基于 web 实现，无需再安装客户端插件；支持在审计录像回放中加入水印等安全功能，有效保障企业数据安全。

◎直观的可视化页面展现

支持对在线用户、在线主机、计划任务、运维数据、实时监控等统计数据进行页面展示；支持对策略分布、威胁分布、系统运行状态等数据进行图形展示；支持对主机运维、计划任务、用户运维等数据 Top 展示。

技术指标

指标	指标项	规格要求
组织结构	分组管理	支持树形结构的无限级数分级管理；直接展示岗位的所属组织和层级管理
	用户管理	支持用户批量操作，包括导入导出、注销、初始化口令等操作；用户类型可自定义，支持创建临时用户
	资源管理	支持资源的登录及改密驱动的自定义扩展，基于资源组的扩展属性自定义
从账号管理（设备账号）	资源账号上收	运维人员输入账号密码成功单点登录后，系统将自动上收账号到对应资源的账号列表
	自动改密	支持对资源进行密码变更；密码变更可以根据密码策略的要求进行变更。支持周期性执行改密任务
	密码拨测计划	定期检查平台存储的设备账号密码与设备实际密码是否匹配，以便校验密码一致性
授权管理	角色管理	支持自定义角色。系统功能模块按需分配给角色，角色可按组节点进行定义，从而实现分层分级分权的管理模式
	授权管理	支持在树形组织结构下直接建立岗位，基于岗位添加人员与资源进行授权关系的快速建立
		通过在岗位上绑定资源筛选规则。支持用户与资源账号一对一、一对多授权方式，并单独为每一个授权指定策略

指标	指标项	规格要求
单点登录 SS0	WEB 方式单点登录	支持无需安装任何控件，即可基于浏览器进行 RDP 等协议的单点登录，支持通过安装控件，调用 mstsc, crt 等运维工具进行单点登录
		支持设置 web 登录时，运维界面添加水印功能，防止敏感信息通过截图拍照泄漏
	会话共管	多个运维人员通过会话共管方式同时运维一台目标资源，同时审计记录
	身份切换代填	支持网络设备 enable 和 unix 主机 su 等身份切换的单点登录功能
	Winscp 工具登录	支持采用 winscp 工具连接 FTP、SFTP、windows 文件共享目标，并且支持大文件的断点续传
	RDP 属性修改	支持 RDP-Tcp 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别，修改属性后能够保证正常连接 RDP 且不影响审计。
认证管理	身份认证	自身提供证书认证服务，也可与第三方 CA、动态令牌等方式进行结合，支持组合认证
审计管理	图形审计	图形资源访问时，支持键盘、剪切板、文件传输记录，对图形资源的审计回放时，可从某个键盘、剪切板、文件传输记录的指定位置开始回放。
		RDP 审计策略支持关键帧，帧间隔，录像文件压缩比等设置，以缩小录像文件大小。支持画质选择。
	字符审计	可审计字符命令方式的访问所有交互内容，可还原操作过程的命令输入和结果输出，可高亮显示高危命令。
	OCR 识别	支持对审计中的文字进行识别。
	录像回放	支持审计录像回放时自带实时动态水印，防止录像回放时敏感信息被截图和拍照。
		倍速 / 低速播放、拖动、暂停、停止、重新播放等播放控制操作。

网络安全专用产品安全认证或安全检测结果证明

- 网络安全专用产品安全检测证书
- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
 - ★证书编号：24SS00897-A
 - ★有效期：2024 年 6 月 28 日至 2026 年 6 月 28 日

所属品牌：长亭科技

发布时间：2023 年 12 月

产品适用领域：金融、电力、能源、政府、交通、教育、医疗、运营商等

产品照片：



产品咨询二维码



产品咨询邮箱：info@chaitin.com

福建省海峡信息技术有限公司

福建省海峡信息技术有限公司是国内最早专业从事网络安全自主研发、产品销售及安全服务的公司之一。2022 年 4 月，海峡信息正式成为福建广电网络集团直属单位。海峡信息是国有控股高新技术企业、国家“专精特新”小巨人企业、福建省创新型研发机构、行业领先的网络安全整体解决方案提供商，是福建省唯一通过国家信息安全服务资质安全运营认证、信息安全服务资质二级认证（安全工程 / 风险评估）的企业，2022 年入选福建省重点上市后备企业，在江西、四川、湖北、湖南等地设有办事处及技术支撑机构。

在技术探索领域，海峡信息成立了“两大实验室”和“一中心”，在过去的二十多年里，一直专注于网络安全产品与服务领域。以创新研发和实战攻防为核心，致力于探索网络安全的最新前沿方向。

在科研成果方面，累计获得了福建省、市科学技术进步奖 8 项；发明专利授权 10 项；拥有软件著作权 100 多项。海峡信息独立承担的福建省高新技术重点项目、火炬计划项目及福建省重大招标项目。所有产品均以创新研发和实战攻防为核心，构建了一个基于主动防御、动态防御、精准防护、整体防护的综合防控体系，广泛应用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域。

网址: <https://www.si.net.cn>

电话: 0591-87303711

地址: 福建省福州市鼓楼区北二环中路 61 号 2 号楼

产品名称：黑盾运维安全管理系统

产品概述

由于在工 T 系统建设中存在事前身份不确定、授权不清晰，事中操作不透明、过程不可控，事后结果无法审计、责任不明确导致客户业务及运维服务面临安全风险。

黑盾运维安全管理系统可对服务器、网络设备、安全设备的操作监控，实现账号集中管理、高强度认证加固、细粒度访问授权控制、加密和图形操作协议的审计等功能，让内部人员、第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免了误操作和非授权操作带来的隐患。

功能特点

◎ SS0 单点登录：运维安全管理系统提供了基于 B/S 和 C/S 的应用系统。单点登录为具有

多账号的用户提供了方便快捷的访问途径，使用户无需记忆多种登录用户 ID 和口令，同时由于系统自身是采用强认证的系统，从而提高了用户认证环节的安全性。

SSO 单点登录支持 web 见面在线登录和离线单点登录操作，无需登录 Web 页面，可联动本地 CT 等客户端实现直连模式的登录，不改变使用习惯，方便快捷。

◎**集中账号管理**：运维安全管理系统对所有服务器、网络设备账号的集中管理。可以完成对账号整个生命周期的监控和管理，且降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。单位可以实现将账号与具体的自然人相关联。

◎**集中身份认证**：运维安全管理系统为用户提供统一的认证接口，支持多种认证方式。采用统一的认证接口不但便于对用户认证的管理，且系统具有灵活的定制接口，可以方便的与第三方 LDAP 认证服务器对接。能够采用更加安全的认证模式，提高认证的安全性和可靠性。

◎**统一资源授权**：运维安全管理系统提供统一的界面，对相应用户、角色及行为和资源进行授权，系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权，最大限度保护用户资源的安全。

◎**集中访问控制**：运维安全管理系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，用来分配给具体的用户限制其系统行为，管理员根据其自身的角色为其指定相应的控制策略来限定用户，真正做到 who、where、when、what。然而更好的提高系统的安全性。对做到运维用户多次登录失败自动锁定账号功能，支持限制运维用户访问源 IP、访问时间段的的功能。

◎**集中操作审计**：操作审计管理分为内部审计和行为审计，内部审计针对堡垒机自身的操作情况的审计。行为审计主要针对操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。生成的日志支持丰富的查询和操作方式。

◎**工单审批**：工单审批模式，第三方运维人员或普通运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行运维操作，更好的提高运维流程简单并记录相应操作。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00712-A

★有效期：2024 年 5 月 24 日至 2026 年 5 月 24 日

所属品牌：黑盾

发布时间：2020 年 3 月 30 日

产品适用领域：适用于智慧政务、医疗、教育、金融、部队、交通、水利
等关键领域

产品照片：



产品咨询二维码

产品咨询邮箱：chenxf@heidun.net

福建中信网安信息科技有限公司

福建中信网安信息科技有限公司以数据安全守护者为使命，致力于网络与数据安全领域，是一家集研发、生产、销售和服务于一体的高新技术企业。中信网安在国内首家提出基于时空网格技术的“云、网、端、数”多维度动态安全监管技术体系，公司依托领先的技术研发与创新能力，先后荣获国家级专精特新“小巨人”企业、国家高新技术企业、工业和信息化部 5G 应用安全创新推广中心、工业和信息化部重点实验室“商用密码应用工作组”及“大数据安全工作组”成员单位、国家知识产权优势企业、福建省级新型研发机构、福建省产业领军团队等多项荣誉，服务用户数量超过 2000 家，并在北京冬奥会、第四十四届世界遗产大会、世界航海装备大会、中国侨智发展大会、历届数字中国建设峰会等大型活动的安保实践中勇担重任，以专业的技术、可靠的服务成为客户心中最信赖的网络与数据安全领军企业。

网址：<https://www.cicisp.com/>

电话：0591-87895020

地址：福建省福州市晋安区鼓山镇福光路 318 号 2 号楼 8 层

产品名称：华安星运维安全管理系统

产品概述

华安星运维安全管理系统具备强大的输入输出审计功能，不仅能够详细记录用户操作的每一条指令，而且能够将所有的输出信息全部记录下来；具备审计回放功能，能够模拟用户的在线操作过程，丰富和完善了网络的内控审计功能。运维安全管理系统能够在自身记录审计信息的同时在外部某台计算机上做存储备份，可以极大增强审计信息的安全性，保证审计人员有据可查。

功能特点

◎ SSO 单点登录

提供了基于 B/S 和 C/S 的应用系统。单点登录为具有多账号的用户提供了方便快捷的访问途径，使用户无需记忆多种登录用户 ID 和口令，同时由于系统自身是采用强认证的系统，从而提高了用户认证环节的安全性。SSO 单点登录支持 web 见面在线登录和离线单点登录操作，无需登录 Web 页面，可联动本地 CRT 等客户端实现直连模式的登录，不改变使用习惯，方便快捷。

◎ 集中账号管理

系统对所有服务器、网络设备账号的集中管理。可以完成对账号整个生命周期的监控和管

理，且降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患，并且制定统一的、标准的用户账号安全策略。单位可以实现将账号与具体的自然人相关联。

◎集中身份认证

系统为用户提供统一的认证接口，支持多种认证方式。采用统一的认证接口不但便于对用户认证的管理，且系统具有灵活的定制接口，可以方便的与第三方 LDAP 认证服务器对接。

◎统一资源授权

系统提供统一的界面，对相应用户、角色及行为和资源进行授权，系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权，最大限度保护用户资源的安全。

◎集中访问控制

系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，用来分配给具体的用户限制其系统行为，管理员根据其自身的角色为其指定相应的控制策略来限定用户。

◎集中操作审计

操作审计管理分为内部审计和行为审计，内部审计针对堡垒机自身的操作情况的审计。行为审计主要针对操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。生成的日志支持丰富的查询和操作方式。

◎工单审批

工单审批模式，第三方运维人员或普通运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行运维操作，更好的提高运维流程简单并记录相应操作。

技术指标

◎单点登录

系统支持对各类设备（ssh、telnet 等协议）的凭证（如账号、口令）进行统一管理，系统支持单点登录进行集中访问。

◎访问和权限控制

系统支持对运维用户、运维资源（ssh、telnet 等协议）进行权限管理和控制。

◎行为审计

审计记录：对运维用户所有的操作进行审计，审计内容包括：源 IP、目标 IP、协议类型、用户名、资源类型、操作时间、操作时长等审计信息，并支持生成回放录像、指令、内容等形式进行界面展示。

审计查阅：系统支持审计员进行查阅审计信息，并支持查询、高级查询、指令查询、内容查询等快速便捷的查询所有审计信息。

◎管理员身份鉴别

身份识别：系统支持唯一用户名进行创建和登录，不允许创建同名账号进行使用。

基本鉴别：系统支持采用用户名和静态口令鉴别机制进行登录，并可进行设置密码口令的复杂难度和有效期进行定期提示变更密码。

鉴别失败处理：系统支持设置账号密码锁定策略，当账号密码口令失败次数符合锁定策略时，进行强制锁定该用户。

◎安全管理

安全管理功能：系统支持授权管理有进行修改系统用户口令，并可指定密码复杂难度、用户锁定等策略进行使用。可通过该权限用户进行添加资源信息录入。

远程管理安全：系统通过 https 加密协议进行页面管理访问。

鉴别数据保护：系统通过 mysql 数据库进行后台加密存储所有用户口令、资源口令。

超时锁定或注销：系统具有超时注销功能，终止会话后需要再次进行身份鉴别才能重新操作。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS035-858

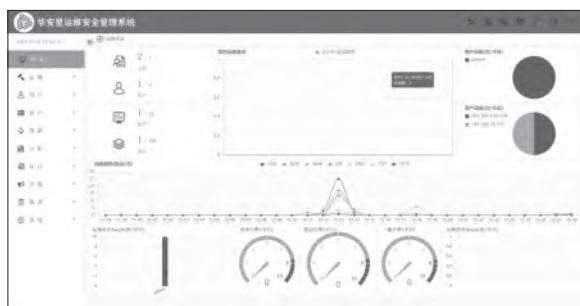
★有效期：2024 年 7 月 23 日至 2029 年 7 月 22 日

所属品牌：华安星

发布时间：2018 年 1 月

产品适用领域：电力、能源、医疗

产品照片：



产品咨询邮箱：zxwa@cicisp.com



产品咨询二维码

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

作为行业领导者，安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

2020 年 11 月 23 日，安恒信息正式成为 2022 年杭州第 19 届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

网址：<https://www.dbappsecurity.com.cn/>

电话：0571-28860999

地址：杭州市滨江区联慧街 188 号安恒大厦

产品名称：明御运维审计与风险控制系统

产品概述

明御[®]运维审计与风险控制系统（简称“DAS-USM”）是安恒信息在多年运维安全管理的理论和实践经验积累的基础上，结合各类法律法规（如等级保护、赛班斯法案 SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001 等）对运维审计的要求，采用 B/S 架构，集“身份认证（Authentication）、账户管理（Account）、控制权限（Authorization）、日志审计（Audit）”于一体，支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，具备全方位运维风险控制能力的统一安全管理与审计产品。

DAS-USM 提供了丰富、全面的管理功能，如客户分权、集中授权、单点登录、统一审计、自动运维、命令控制、工单流程、系统自审等，帮助客户解决责任认定难、管理不规范、权限混乱、控制力度不足、审计不全面等难题。

在部署方面，DAS-USM 采用物理旁路、逻辑网关的网络部署模式，不影响网络拓扑和业务系统的运行，可通过网络访问控制系统（如：防火墙、带有 ACL 功能的交换机）的配合下，让 DAS-USM 成为唯一的入口，确保“终端至 DAS-USM 的管理端口可达、DAS-USM 与目标主机的运维协议可达”。

功能特点

明御运维审计与风险控制系统（以下简称“DAS-USM”），提供了丰富、全面的管理功能，

帮助客户解决责任认定难、管理不规范、权限混乱、控制力度不足、审计不全面等难题。

◎**客户分权**：支持多种客户角色：超级管理员、部门管理员、配置管理员、审计管理员、运维员、审计员、系统管理员、密码管理员，每种用户角色的权限都不同，为用户设立不同的角色提供了选择，并且满足合规对三权分立的要求，并提供灵活的角色自定义能力。

◎**集中授权**：通过集中授权，帮助客户梳理客户与主机直接的关系，并且提供一对一、一对多、多对一、多对多的灵活授权模式。

◎**单点登录**：DAS-USM 支持托管主机的账户和密码，运维人员直接点击 <登录> 即可成功自动登录到目标主机中进行运维操作，无需输入主机的账户和密码。

◎**统一审计**：DAS-USM 对所有的操作进行详细记录，并提供综合查询功能；审计日志可以在线播放也可以离线播放，所有的审计日志支持自动备份和自动归档。

◎**自动运维**：对运维人员来说，需要定期手工执行命令；对网管人员来说，需要定期手工备份网络设备的配置信息。通过 DAS-USM 的自动化运维功能，实现自动化的运维任务并将执行结果通知相关人员。

◎**命令控制**：DAS-USM 提供了集中的命令控制策略功能，支持字符协议及数据库协议的命令级策略控制，支持通配符和正则表达式两种方式，实现阻断会话、阻断命令、审批、直接放行 4 种动作。

◎**工单流程**：操作人员向管理员申请需要访问的设备，申请时可以选择：设备 IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。

管理员对运维工单进行审核之后以邮件方式通知给运维人员。如果允许，则运维人员才可访问，否则就无法访问。

◎**系统自审**：DAS-USM 作为审计类产品，不光要实现对操作行为进行审计，还要做到对系统自身变化信息进行审计，并且形成系统报表分析。

技术指标

◎功能指标：

具备客户分权、集中授权、单点登录、统一审计、自动运维、命令控制、工单流程、系统自审等功能模块。

具备国密认证、通信、存储三合一方案、可支持信创场景运维，兼容 UOS 和银河麒麟操作系统、支持混合云管理功能、支持多种运维方式等。

运维方式多样：兼容多种客户端工具（如 Xshell、SecureCRT、mstsc、VNC Viewer、Putty、winscp、flashFXP、SecureFX、OpenSSH 等）和更加灵活的运维方式：

★ **Web 登录运维**：适用于习惯从 Web 页面登录目标主机的运维人员

★ **客户端登录运维**：适用于习惯使用本地客户端工具登录 DAS-USM 再登录目标主机的运维人员

★ **批量自动登录运维**：适用于习惯一次性登录多台目标主机的运维人员

★网关透明登录运维：适用于习惯使用本地客户端工具直接登录目标主机的运维人员

★ Openssh 代理登录运维：适用于习惯用苹果系统、安卓系统、Ubuntu、Linux/Unix 的 PC 终端登录目标主机的运维人员，以及自动化运维等复杂场景。

(2) 安恒信息自主研发了一套自动学习技术：自动收集主机的 IP、协议、端口号、账户、密码等信息，并且可以学习到运维人员的权限关系，进一步实现自动授权。特别适用与前期对授权关系不清晰、资产信息不完整的场景。

◎硬件性能指标：

外部接口参数

以太网口：千兆电管理口 *2，千兆业务电口 *4，千兆业务光口 *4（含 2 个千兆 SFP 多模光模块）

USB 口：2 个 USB 口

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00228-A

★有效期：2024 年 2 月 23 日至 2026 年 2 月 23 日

所属品牌：明御

发布时间：2011 年 11 月 15 日

产品适用领域：政府、医疗、公安、运营商、企业、军工、教育、能源、金融

产品照片：



产品咨询邮箱：beric.liu@dbappsecurity.com.cn

江苏保旺达软件技术有限公司

江苏保旺达软件技术有限公司，成立于 2011 年 5 月，公司聚焦数据安全、身份识别和访问管理、堡垒机、云安全、应用安全、网络安全等专业安全领域，为政府、运营商、军工、金融、能源等行业用户和各类型企业用户提供安全、合规、全生命周期、全业务场景的信息安全整体解决方案和服务，为企业数字化转型提供数字安全保障。公司积极推动 AI、区块链、数据标记、联邦学习、安全多方计算等前沿技术和现有安全场景融合，加快打造安全数据中台、数据要素安全共享交换平台等创新产品。公司主要产品在细分领域均占据领先地位。

网址：<https://www.bwda.net/>

电话：025-86592222

地址：南京市江北新区星火路 9 号软件大厦 B 座 9-10 楼

产品名称：保旺达身份认证和访问管理平台

产品概述

保旺达身份认证和访问管理平台，从合规性、安全性、保密性角度出发，解决网络运维过程中通常存在的账号管理混乱、操作指令控制手段缺失、审计功能缺乏等问题和风险隐患，强调管理理念上统一、集中，实现业务的灵活、相容，提升内网运维安全能力，赋能企业数字化转型。

功能特点

管理平台、门户平台、认证服务支持容器化部署，所有功能组件可弹性扩展，可基于业务和应用所需动态调整、实时优化；

提供多租户能力，按照“分权分域”的理念隔离用户和资源信息，支持管理不同子公司、部门间的资源和用户信息；

支持核心数据加密存储，有效保护数据安全，支持页面自定义水印，防止截屏泄密敏感数据；

系统提供丰富的 API 接口，通过统一 API 实现层次化、服务化的能力封装，能够提供原子服务能力。

技术指标

采用“零信任”架构不断分析终端、网络、行为等风险，评价用户身份是否合规，并持续认证和动态授权，从而保护访问的安全性；

基于零信任的访问控制，用户准入访问时，对用户身份、终端等安全属性进行综合评估并完成认证；访问应用系统时，持续、动态评估用户可信度及被访资产的安全风险，实时监测用户的访问行为；

提供统一密钥管理及加解密安全服务，实现各个应用系统内部涉及数据加密的密钥管理，为确保密钥的定期生成、发放、更新，提供集中管理能力，保障业务数据的传输安全；

反向代理服务将应用进行伪装与隐藏，访问请求不再知道真实的访问地址，以隐藏的方式接管终端到服务器间的通讯。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部网络安全保卫局

★证书编号：23SS00417-A

★有效期：2023 年 12 月 15 日至 2025 年 12 月 15 日

所属品牌：保旺达

发布时间：2011 年 10 月

产品适用领域：政府、运营商、军工、金融、企业

产品咨询邮箱：shaodeyun@bwda.net



产品咨询二维码

南京聚铭网络科技有限公司

聚铭网络是由腾讯、国家中小企业发展子基金、江苏高投毅达宁海创业投资基金等投资的国内领先的安全运营商。

公司先后荣获了“高新技术企业”、“江苏省专精特新企业”、“江苏省规划布局内重点软件企业”、“江苏省软件企业技术中心认定企业”、“南京市工程技术研究中心认定企业”、“双软企业”、“创新型企业企业家培育企业”、“创业南京高层次创业人才引进企业”、“国家信息安全漏洞库 CNNVD 技术支撑单位”、“数据安全 10 强企业”等荣誉，公司专注于网络安全智能分析和检测，提供全面的信息安全防护，为达成“让安全更简单”的使命而不懈努力。

公司每年投入大量的科研经费用于产品研发和人才培养引进，先成立了“聚铭安全攻防实验室”，后又与南京大学联合成立了“数据科学联合实验室”，两大实验室用于网络安全前沿技术的预研。目前公司产品荣获了江苏省软件产品金慧奖、江苏省重点推广应用新技术新产品、南京市新兴产业重点推广应用新产品等荣誉。

凭借先进的技术和优质的服务，目前公司产品已服务教育、医疗、政府、电信、能源、金融等行业超 10000 家政企客户，云端托管客户超 6500 家。公司在北京、南京成立了双总部中心，同时在各地设有分支机构，业务覆盖全国 31 个省市及香港地区。

网址：<https://www.juminfo.com/>

电话：400-1158-400；025-52205520

南京总部：南京市雨花台区软件大道 180 号大数据产业基地 7 栋 4 层

产品名称：聚铭安全运维审计系统

产品概述

随着企事业单位信息化建设加快，日趋复杂的 IT 系统和不同背景的运维人员行为给信息系统安全带来较大风险，为满足用户内部运维安全的迫切需求，聚铭网络研发了新一代安全运维审计系统——聚铭安全运维审计系统。产品支持对运维人员在运维过程中进行统一身份认证、统一授权、统一监控、统一审计，消除了传统运维过程中的盲区，实现了运维简单化、操作可控化、过程可视化，是企事业单位 IT 内控有效的运维审计系统。

功能特点

◎单点登录：单点登录为具有多账号的用户提供了方便快捷的访问途径，使用户无需记忆多种登录用户 ID 和口令。单点登录可以实现与用户授权管理的无缝连接，可以通过对用户、角

色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。

◎集中账号管理：通过建立集中账号管理，企业可以实现将账号与具体的自然人相关联。通过这种关联，可以实现多级的用户管理和细粒度的用户授权。

◎身份认证：集中身份认证提供静态密码、动态口令和生物识别指纹认证方式等多种认证方式，极大地增强了安全运维审计系统用户认证的安全性和可靠性。

◎资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。

◎访问控制：提供细粒度的访问控制，最大限度保护用户资源的安全。

◎操作审计：操作审计管理主要审计操作人员的账号使用（登录、资源访问）情况、资源使用情况等，能更好地对运维人员账号的完整使用过程进行追踪。通过系统自身的用户认证系统、用户授权系统，以及访问控制等详细记录整个会话过程中用户的全部行为日志。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS035-1011

★有效期：2024 年 12 月 5 日至 2029 年 12 月 4 日

所属品牌：聚铭网络

发布时间：2018 年 3 月 27 日

产品适用领域：政府、教育、医疗、金融、电信、能源

产品照片：



产品咨询二维码

产品咨询邮箱：yangping@juminfo.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟（CCIA）发布的 2021 年、2022 年、2023 年“中国网络安全产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神特权账号管理系统

产品概述

奇安信网神特权账号管理系统（以下统称为 PAM）是奇安信集团在多年运维安全管理的理论和实践经验积累的基础上，结合各类法律法规对运维审计的要求，采用 B/S 架构，基于特权访问闭环管理流程，提供特权账号的发现和纳管、自动改密、验证和巡检、访问权限控制、锁定和释放等功能，帮助用户系统化、流程化和规范化特权账号管理的工作，降低特权账号管理不善带来的安全风险，防范攻击者利用特权账号对敏感数据进行窃取，满足合规性要求，推动企业核心业务发展。满足政府、金融、电力、高新技术企业、医疗卫生、电子政务等行业客户的特权访问管理需求。

功能特点

◎身份认证：根据用户场景的实际需要，为不同用户提供不同类型的认证方式，既支持基本的静态口令方式，又能够提供双因子认证方式，例如 OTP 口令、USBKey、短信验证码。同时，PAM 还能够集成现有认证方式，例如 AD 域、Radius，实现用户认证的统一管理。

◎**授权管理**：PAM 基于最小权限原则设置访问控制策略和细粒度的命令级授权策略，既可以实现对资源的访问权限的控制，也可以实现对操作命令、文件传输权限、剪切板操作权限控制。

◎**操作审计**：PAM 能够基于唯一身份标识，通过对用户从登录到退出 PAM 的全程操作行为进行审计，监控用户对目标设备的所有操作，聚焦关键事件，实现对安全事件的实时发现与预警。

◎**账号发现功能**：PAM 的特权账号发现引擎旨在持续发现 IT 环境的变化，通过手动或自动的方式触发账号发现策略，采用预设的特权账号批量连接目标设备，对目标设备进行扫描、以及对历史扫描情况的对比，及时发现未纳管账号、后门账号、僵尸账号和权限变更账号，让安全人员快速掌握企业特权账号的分布、使用和变更的情况。

◎**账号弱密码检测功能**：PAM 提供目标设备托管至 PAM、未托管至 PAM 两个维度全面的账号弱密码检测功能，支持平台包括 Linux/Unix、Windows Server、Oracle、MySQL、SQLServer 等，可自定义弱密码集、弱密码规则，全面的检测资源的弱密码分布情况。

◎**账号改密、验证功能**：账号密码的定期改密、验证是账号管理最重要的任务。PAM 支持对主机、网络设备、数据库、中间件等各类资源作为运维管理用途系统账号密码的变更操作。用户可预设密码变更周期、密码复杂度及密码变更范围等信息，采用手动或自动化方式触发改密计划对指定资源账号进行改密操作。针对改密附件，可以设置两个接收人，并且发送的附件是加密，两个接收人分别收到账号的前半段和后半段密码，两段密码合并之后才能够得到完整的密码。并且支持手动或自动化的方式验证特权账号密码的正确性。

◎**账号安全存储功能**：PAM 的密码保险箱提供了账号密码安全存储功能，帮助企业转变原有的管理模式，让企业能够更容易地管理和保护各种类型的特权账号凭证。PAM 根据部门做到数据隔离，不同部门的管理员不能跨部门访问数据，做到审计、资源、账号等数据的隔离。

技术指标

◎**账号信息收集**：通过自动或人工的方式下发账号发现任务给策略执行器，该任务包含若干资产信息，策略执行器会重新请求一次账号信息然后通过执行相应资产插件完成对资产账号信息的收集工作。

◎**账号风险分析**：通过多台机器账号信息的扫描，可以在监控大盘对所有资产的僵尸账号、幽灵账号、长期未改密账号等风险。除报表外，还可以直接将账号纳管进系统内，完成定期巡检与改密。

◎**账号改密**：通过策略执行器，加载不同插件可以支持常见账号改密功能；除常见账号，还可以通过自定义改密脚本，实现对 Web 类型账号、特殊版本的网络设备账号进行改密；同时，在防止恶意脚本破坏客户环境方面，脚本上传时会采用签名技术，校验脚本合法性，来避免恶意脚本。脚本会通过策略执行器完成改密，同时管理中心会保存多次改密前后的密码，避免密码意外丢失。

◎**弱密码扫描**：支持上传弱密码集配置常见的弱密码，或者由系统按用户指定规则生成弱密码集。在扫描阶段，首先由策略执行器将资产上的账号特征文件加密传输拉取至本地，然后

使用相应密码加密算法与弱密码集中密码匹配，并将匹配结果返回给管理中心，由管理中心进行进一步分析。

◎应用内嵌账号：PAM 旨在实现全面的特权账号管理，包括各类应用程序和工具对账号密码的使用需求。第三方工具（例如漏洞扫描、安全扫描、自动化工具、IT 管理等）能够通过 PAM 提供的 API 和 SDK、JDBC 驱动动态获取密码，配置文件和脚本中保存的静态密码则是通过文件推送的方式定期更新。为了确保应用身份的可靠性，PAM 会给应用生成唯一的身份标识，应用使用这个身份标识到 PAM 去请求并获取账号密码。

◎双账号：为了避免改密对业务系统造成影响，PAM 提出了“双账号”模式。双帐号是具有同样权限的两个帐号，应用程序通过其中任意一个帐号访问资产（例如数据库），都能正常执行操作（例如查询数据库）。

◎账号密码变更留痕：针对系统中各类密码变更操作，无论是人为修改还是改密计划自动执行的操作，均支持留痕审计功能。针对历史密码，可设置保存的版本数量或周期。

◎账号威胁分析功能：PAM 提供了独立的大屏，用于展示账号的威胁，包括：未纳管账号、长期未登录账号、长期未改密账号、权限变更账号、弱密码等，同时能够实时展示账号动态。

◎监控大盘：通过 PAM 监控大盘，全面的监控账号风险，通过长期未登录、长期未改密、权限变动、弱密码等维度，结合相关的账号管理策略，实施监控账号的风险，通过图表的方式全面展示账号的风险，及时提醒相关的管理人员。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：24SS00128-A

★有效期：2024 年 1 月 26 日至 2026 年 1 月 26 日

所属品牌：奇安信网神

发布时间：2020 年 4 月 2 日

产品适用领域：银行、金融、电力、大企业、公安、卫生、电子政务等

产品照片：



产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年在深圳 A 股中小板上市（股票代码：002439），是网络安全产业中主力经典产业板块的龙头企业，是新兴前沿产业板块的引领企业，是可持续健康业务模式和健康产业生态的支柱企业。

2024 年 1 月，启明星辰正式由中国移动实控，标志着公司迈入全新的发展阶段。中国移动致力于推动信息通信技术服务经济社会民生，以创世界一流企业、做网络强国、数字中国、智慧社会主力军为目标，已成为全球网络规模最大、客户数量最多、盈利能力和品牌价值领先、市值排名前列的电信运营企业。

启明星辰作为中国移动专责网信安全专业子公司，将全面贯彻“总体国家安全观”，发挥国资央企“科技创新、产业控制、安全支撑”三大作用，肩负起中国移动“安全核心技术攻坚者、安全产品服务引领者、安全运营体系支撑者”三大角色，围绕构建大网信安全板块进行战略布局，引领网络安全产业的升级与发展。

多年来，启明星辰持续深耕于信息安全行业，始终以用户的需求为根本动力，将场景化安全思维融入到客户的实际业务环境中，不断地进行创新实践，帮助客户建立起完善的安全保障体系，逐渐成为政府、金融、能源、运营商、税务、交通、制造等国内高端企业级客户的首选品牌。启明星辰入侵检测 / 入侵防御、统一威胁管理、安全管理平台、数据安全、运维安全审计、数据库安全审计与防护、漏洞扫描、工业防火墙、硬件 WAF、托管安全服务等十余款产品持续多年保持第一品牌。

网址：<https://www.venustech.com.cn/>

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：天玑运维安全网关 V6.0

产品概述

天玑运维安全网关 V6.0(以下简称运维安全网关系统)是一种管控和审计运维人员操作的网络安全设备。

管理员可以使用运维安全网关系统控制运维人员能运维哪些设备，执行哪些操作命令，避免运维人员非法或无意执行高危操作，并对运维人员的操作进行实时监控和事后审计。

运维人员通过运维安全网关系统做运维，不必记录设备的 ip 地址、用户名、口令等信息，也避免这些敏感信息的泄露，极大地方便了运维工作，提升运维效率。

运维安全网关系统对整个运维过程从事前预防、事中控制和事后审计进行全程参与。

事前预防：建立”自然人-资源-资源帐号”关系,实现统一认证和授权。

事中控制：建立”自然人-操作-资源”关系,实现操作审计和控制。

事后审计：建立”自然人-资源-审计日志”关系,实现事后溯源和责任界定。

功能特点

◎单点登录

运维用户只需经过天玥运维安全网关 V6.0 一次认证,通过返回的授权列表,直接访问目标资源,无须二次输入帐号和密码。运维用户只需要记住自己的天玥运维安全网关 V6.0 登录帐号、密码即可,无需记忆繁多的目标资源 IP、帐号和密码信息。

◎身份认证

天玥运维安全网关 V6.0 为每一个运维人员创建唯一的运维帐号(主帐号),运维帐号是获取目标设备访问权利的唯一帐号,进行运维操作时,所有设备账号(从帐号)均与主帐号进行关联,确保所有运维行为审计记录的一致性,从而准确定位事故责任人,弥补传统网络安全审计产品无法准确定位用户身份的缺陷,有效解决帐号共用问题。

◎访问授权

天玥运维安全网关 V6.0 通过基于角色的权限访问控制,实现细粒度授权与策略控制。管理员可根据目标资源设置不同角色;支持时间、命令、审批规则制定,实现不同运维用户访问资源遵从不同的控制策略。

◎会话审计

天玥运维安全网关 V6.0 能够对运维人员登录目标设备上进行的操作进行全程记录,包括字符协议(SSH、TELNET)、文件传输协议(FTP、SFTP)、数据库协议的所有操作命令的完整详细记录,图形协议(RDP、VNC)的完整操作图形记录。能够以回放的形式重现运维人员对目标设备的整个操作过程,从而真正实现对操作内容的完全审计。

◎告警与阻断

天玥运维安全网关 V6.0 支持根据已设定的访问控制策略,自动检测日常运维过程中发生的越权访问、违规操作等安全事件,系统能够根据预设规则进行自动的告警或阻断违规的操作行为。

◎审计报表

支持按日、周、月为周期自动生成周期性报表。

技术指标

支持双因认证,包括 USB-KEY 认证、动态口令认证、国密动态口令认证、手机令牌认证、Windows AD、RADIUS、LDAP、短信、北京 CA、吉大正元等。

支持运维协议运维管控和审计,包括 SSH、TELNET、FTP、SFTP、SCP、RDP、VNC、Oracle、PostgreSQL、MySQL、DB2、Informix、SYBASE、Mssql(2005,2008,2012)等。

支持数据库协议命令级审计，包括 Oracle(支持 ORACLERAC)、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata 等。

支持帐号稽核，导出异常帐号稽核情况报告，包括僵尸帐号、幽灵帐号、孤儿帐号。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00245-A

★有效期：2023 年 11 月 3 日至 2025 年 11 月 3 日

所属品牌：启明星辰

发布时间：2018 年

产品适用领域：运营商、政府、企业、能源、公安等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

山东中网云安智能科技有限公司

山东中网云安智能科技有限公司成立于 2016 年，是一家专业以信息安全等级保护、工业控制安全及信息技术应用创新为主营业务的企业。公司主要产品有：安全隔离网闸、安全隔离单向光闸、数据安全交换平台、集中控制与安全管理、防火墙、堡垒机、日志审计、数据库审计、网络安全审计、漏洞扫描、入侵防御、WEB 应用防护、网页防篡改、网络准入控制、网络服务管理（智能 DNS）、上网行为管理、主动防御及智能预警系统（PDS）、流量控制、应用交付等全系列等保产品，其中 19 款产品共计 121 个型号入围了中央政府采购网络安全产品协议供货中标目录，三款核心产品于 2022 年 07 月通过公安三所检测并正式入围最新一期的国家 XC 安全产品推荐名录。主营业务范围：信息安全可信计算、信息安全等级保护 2.0 建设及整改、涉密信息安全、工控安全、大数据安全等方面的产品研发、生产、销售及服务。在智慧城市、大数据中心、云服务、工业、党政、金融、通信、能源、交通、航空航天、医疗、教育等行业提供网络安全防护解决方案，尤其在智慧政务、智慧政法、智慧社区等城市数字化转型中对核心数据共享的安全需求上，中网云安实现了在海量数据集中的同时保障共享和交换的安全性。

网址：www.cnnecs.net

电话：0531-86985080

地址：济南市历下区龙奥北路 8 号玉兰广场 2 号楼 20 层

产品名称：中网云安运维审计与访问控制系统

产品概述

中网云安运维审计与访问控制系统（简称 NCS-OAC），俗称堡垒机，基于统一身份管理（Account）、访问控制管理（Authentication）、权限管理（Authonzation）、操作行为审计（Audit）的 4A 安全思想模型技术框架实现。能够为用户提供统一的集中管理平台，解决账号混乱、定位不明、权限粗放、审计不严、取证困难等问题。

功能特点

◎全面的资源支持：安全运维支持 SSH、TELNET、RLOGIN 等字符协议，RDP、X11、VNC 等图形协议，FTP、SFTP 等文件协议，及通过应发布扩展 HTTP、HTTPS、数据库、PCanywhere 等。

◎强大的认证方式支持：支持用户名密码、CA、RSA 动态口令、Radius、LDAP、AD 域、短信等认证方式。

◎全面的账号管理：批量导入用户列表、适应分级管理模式、限制管理员的管理范围、临时帐号、资源改密、集成动态口令。

◎内置 SSL VPN 模块：系统内置 SSL VPN 服务器，保障运维人员安全管控接入堡垒机。

◎内置 OPT 模块：内置了动态密码模块，无需用户购买第三方服务器。

◎丰富的部署方式：支持单机、双机热备、集中管理分级部署等多种部署方式，实现在面对各种规模和复杂的运维场景都能够灵活、可靠运行。

◎集中运维授权：通过堡垒机的集中授权，帮助客户梳理用户与主机之间的关系，并且提供一对一、一对多、多对一，多对多的灵活授权模式。

◎精细命令控制：提供集中的命令控制策略功能，支持字符协议及数据库协议的命令级策略控制，支持通配符和正则表达式两种方式，实现阻断会话、阻断命令、审批、直接放行 4 种动作。

◎统一操作审计：对所有的操作进行详细记录，并提供综合查询功能；审计日志可以在线播放也可以离线播放，所有的审计日志支持自动备份和自动归档。

技术指标

具备如下运维安全管理产品安全技术功能

单点登录：单点登录；

安全功能要求：访问控制、审计记录、审计查阅、会话监视、会话回放、告警、违规操作阻断、高可用性；

标识与鉴别：身份标识、基本鉴别、鉴别失败处理、超时锁定或注销；

安全管理：安全功能管理、管理员角色、远程管理加密、远程管理主机、鉴别数据保护；

审计日志：审计日志生成、审计日志存储、审计日志管理。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01025-A

★有效期：2024 年 07 月 19 日至 2026 年 07 月 19 日

所属品牌：非攻墨道

发布时间：2019 年 10 月 15 日

产品适用领域：党务、政务、税务、医疗、金融、电信、教育、能源、电力、证券、企业

产品照片：



产品咨询邮箱：lipeng@cnnecs.net



产品咨询二维码

上海派拉软件股份有限公司

上海派拉软件股份有限公司（简称：派拉软件）成立于 2008 年，是国内最早从事身份安全研发的原厂商，致力于为企业和机构提供以“数字身份”为核心的数字化能力底座与安全基石，覆盖身份安全、应用安全、数据安全，在上海、北京、广州、武汉、成都、长春、深圳、济南、厦门、合肥、杭州、西安等地设有研发中心和服务机构，拥有 600+ 行业专家和资深团队，服务能力遍布全国。

作为国内数字身份安全的领导者，派拉软件基于“身份优先”的零信任架构（Zero Trust），从全域身份治理和安全访问控制，逐步延伸到特权访问管理、API 管理、数据访问控制管理等产品和解决方案，不断扩展数字身份安全能力；重点围绕企业数字化转型三大核心要素，即人、应用服务、数据，提供相应的身份安全、应用服务安全、数据安全产品与解决方案，有效解决企业和机构数字化转型建设过程中暴露面大、过度信任、权限管理难、数据泄露等问题，高效应对更加复杂、多变的内外部安全威胁，为企业和机构强化数字化转型安全防护能力，建立体系化、端到端的数字化安全基石。

网址：<https://www.paraview.cn>

电话：400-6655-581

地址：上海市浦东新区高科东路 777 弄 8 号楼阳光商业中心写字楼 10 层

产品名称：派拉特权访问管理软件 V6.0

产品概述

账号特权访问管理平台（Privileged Access Management, PAM）是一款专业设计的安全解决方案，旨在有效管理和监控组织内关键系统和数据的访问权限。该平台专注于保护拥有特权访问权力的账户，以防范内部和外部威胁，提高整体网络安全性。

功能特点

◎全面的特权访问控制：PAM 平台提供了精细的权限管理机制，确保只有授权用户能够访问关键系统和敏感数据。通过严格的审计和监控功能，可实现对每一次访问的实时记录和可追溯性。

◎多层次身份验证：强化身份验证是 PAM 的核心，支持多因素身份验证（MFA），生物识别技术等高级认证方式，以确保特权账户的真实身份，防范身份盗窃和滥用。

◎会话管理与录像：PAM 平台能够监控和记录特权访问的所有会话活动，包括命令执行、文件访问等。这有助于及时发现异常行为并进行快速响应，同时提供审计日志用于合规性要求。

◎**密码管理与轮换**：针对特权账户的密码安全是 PAM 的关键职责，平台支持定期的密码轮换、密码策略的强化，并提供安全的密码存储和分发机制。

◎**实时告警和响应**：PAM 平台配备实时告警系统，能够检测到异常访问行为并立即通知相关人员。同时，提供灵活的响应机制，帮助迅速应对潜在的威胁。

◎**合规性与审计支持**：PAM 平台内置了各种合规性标准的支持，可帮助组织满足法规要求，如 GDPR、HIPAA 等，并提供详尽的审计报告，方便审计和监管。

技术指标

◎身份验证与访问控制

多因素身份验证（MFA）支持，包括硬件令牌、手机验证等。

精细的访问控制机制，支持基于角色、组织单元和资源的访问权限定义。

◎会话管理与监控

实时会话监控，记录和审计特权账户的活动。

录像和回放功能，用于详细审计和调查异常活动。

◎密码管理与安全存储

定期密码轮换机制，避免长期使用相同的特权密码。

安全的密码存储，使用强加密算法，以防止密码泄露风险。

◎实时告警和响应

实时异常行为检测，支持配置可疑活动的告警阈值。

高效的响应机制，包括通知、自动化响应和隔离特权账户的能力。

◎合规性与审计支持

内置各种合规性标准的支持，如 GDPR、HIPAA 等。

生成详尽的审计报告，记录访问、权限变更和安全事件。

◎密码策略强化

灵活的密码策略配置，包括密码长度、复杂性要求等。

集成密码策略的自动强制执行机制。

◎集成与互操作性

易于集成到现有身份验证和目录服务，如 LDAP、Active Directory 等。

API 和插件支持，以便与其他安全工具和系统集成。

◎性能与可扩展性

高性能的特权访问请求处理，确保对关键系统的访问不受显著的延迟。

可扩展的架构，支持大规模部署和适应增长的需求。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231040

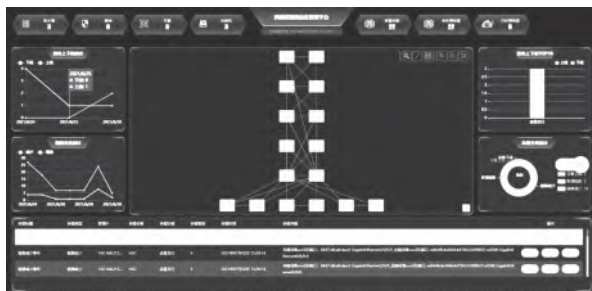
★有效期：2023 年 5 月 5 日至 2025 年 5 月 5 日

所属品牌：派拉

发布时间：2023 年 2 月 14 日

产品适用领域：金融，政府，能源，高端制造

产品照片：



产品咨询邮箱：marketing@paraview.cn



产品咨询二维码

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：深信服运维安全管理系统

产品概述

运维安全管理系统集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计为一体，能够对 IT 资产（如服务器、网络设备、安全设备、数据库等）的操作过程进行有效的运维操作审计，使运维审计由事件审计提升为操作内容审计，通过事前预防、事中控制和事后审计的能力全面解决运维安全问题，进而提高 IT 运维管理水平。

功能特点

◎**账号的集中管理能力**：通过建立集中的账号管理，一方面对有运维需求的用户分配针对自然人的系统账号，另一方面将服务器、网络设备等设备资源的账号收集到统一位置管理。从而达到对身份认证和系统授权的完整账号管理模式。通过统一的账号管理能够制定统一的、标准的账号安全策略，有效解决账号中存在的安全隐患等问题，同时降低了管理员管理大量账号的难度和工作量。

◎**细粒度的管控策略**：提供基于访问时间、访问地址、组、资源、资源账号、系统账号、

操作行为、操作命令等的强访问控制。通过制定细粒度的访问策略、限制高危命令的执行，达到全方位细粒度的访问控制。

◎**自由选择运维模式**：根据运维人员的实际使用习惯，能够支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、MSTSC 等常用的本地客户端工具进行运维操作。同时，考虑到运维人员类型的不同、使用场景的不同以及客户端环境的不同等，在支持调用本地客户端工具运维的同时，用户还可以根据需要直接通过 WEB 方式实现单点登录。无需安装任何插件，方便快捷的满足不同运维人员使用的场景，简化对客户端运维环境的要求。

◎**资源账号改密**：依照等级保护基本要求，对于内网设备的口令需要定时按照一定的复杂程度进行变更，堡垒主机提供自动定时批量修改从账号口令的功能。用户可自定义口令变更时间、周期、复杂程度等内容。极大的减轻了运维人员的工作压力。

◎**会话实时监控与阻断**：运维人员在线运维操作的实时监控。管理员可以以图像的方式实时的监视运维人员的运维操作，如果发现运维人员存在不合规的操作，管理员有权限实现对当前会话的实时阻断。

◎**详实的运维审计**：对不同类型的设备、不同的访问方式都能提供非常详尽的运维审计日志。针对运维人员的基本信息、被运维资源的地址、账号、协议等信息进行完整记录。与此同时，还能提供运维过程的完整录像视频，真实、直观的重现操作人员的操作过程。为了提高审计效率，对于操作过程过长的录像，能够通过关键字定位到关键位置后，通过定点播放查看关键部分的操作录像。

技术指标

◎**自定义系统角色**：内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。

◎**运维资源多样化**：支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源。支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。

◎**定期改密**：支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式。

◎**事中控制**：支持命令黑名单，对字符型设备（如 linux/unix/ 网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等。

◎**事后审计**：对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放；图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安三所

★证书编号：24SS00001-A

★有效期：2024 年 1 月 5 日至 2026 年 1 月 5 日

所属品牌：深信服科技股份有限公司

发布时间：2020 年

产品适用领域：医疗、政府、铁路、能源、高校、政企

产品照片：



产品咨询邮箱：market@sangfor.com.cn



产品咨询二维码

深圳万物安全科技有限公司

深圳万物安全科技有限公司（简称“万物安全”）围绕战略新一代信息技术产业，聚焦网络安全新质生产力“AI+ 物联网安全”，“颠覆式创新和硬科技”实力获得工信部“网安中心”和“火炬中心”高度认可并获奖，连续三年被“全球权威咨询机构 IDC- 金融视频物联安全”分析报告评为第一、国家保密局百家信创单位之一、中国网络安全产业联盟理事单位、关键信息基础设施安全保障联盟副理事长单位。

万物安全产品和解决方案，基于云原生和零信任架构，融合 AI、信创、数据安全等最新技术，为金融、能源、医疗、交通等提供全生命周期的物联网安全运营和管控能力，满足《网络安全法》、《关基保护条例》、《网络数据安全条例》等国家政策法规要求，已成为物联网安全领导者。

网址：<https://www.iottepa.com>

电话：0755-26658957

地址：中国·深圳·福田·国际金融科技城 6 楼

产品名称：大屏内容安全

产品概述

深圳万物安全科技有限公司是国内物联网安全的领导者。针对公共显示屏安全管理存在的孤岛化、被动管控、技术手段落后等问题，我们运用自主研发的 AI 图像与文本识别技术，推出了创新的大屏内容安全产品。我们的产品结构融合了图像隐形水印、AI 超算、边缘计算硬件和软件管控平台，为银行、高校、医院、高速公路等提供全面的公共显示屏内容安全管理方案。通过这一方案，不仅能有效预防涉政、涉黄等敏感内容的出现，更能实现高效、主动的安全管理，确保公共信息显示的合规性。我们的产品旨在打破传统安全管理的局限，通过先进的技术手段，为客户打造一个安全、可靠的公共显示屏环境，从而避免潜在的安全风险，保障信息的健康传播。

功能特点

◎接入设备管理基础信息

大屏内容安全统一管理平台采用 GIS 地图，直观展示所接入的所有设备的位置、工作状态、报警，当设备节点出现任何问题时，通过地图上的设备示意，及时向用户发出报警。

◎接入设备状态监测控

大屏内容安全统一管理平台提供“设备运行状态”展示页面，在该页面下，用户可选中具

体的大屏内容安全设备，查看设备的详细信息，包括但不限于设备运行状态、视频检测状态、文字检测状态、设备防护状态、屏幕连接状态、视频流参数等。

◎告警管理

当接入的大屏内容安全设备监测到内容安全问题，或者监测到设备或者接口的故障时，将及时上报相关信息给大屏内容安全统一管理平台，由大屏内容安全统一管理平台向用户发出报警，提供报警事件详情的展示页面。

◎大屏内容安全设备管理控制

大屏内容安全统一管理平台提供管理控制途径，用于设置盒谐系列产品的工作模式，包括过滤和透传模式等。

◎历史数据检索功能

大屏内容安全统一管理平台存储所有盒谐系列设备的历史设备状态、历史事件信息，日志存储至少 12 个月，并提供对应的筛选检索机制。

◎用户角色与系统设备管理

大屏内容安全统一管理平台初始提供超级用户，客户可登陆超级用户，进行设备初始化配置、创建下级用户、分配角色、创建组织架构。

技术指标

◎支持通过抽取视频帧的方式，对视频帧画面进行图像检测，检测项目包括：

- ★不良画面特征：包括色情、涉政、暴恐、违禁等不良画面特征；
- ★敏感人物头像：包括落马官员、劣迹艺人等人脸头像；
- ★不良文字内容：包括色情、涉政、暴恐、违禁、低俗辱骂等；
- ★支持常规视频文件格式，包括 mp4、avi、mov 等；

◎支持对图片画面进行图像检测，检测项目包括：

- ★不良画面特征：包括色情、涉政、暴恐、违禁等不良画面特征；
- ★敏感人物头像：包括落马官员、劣迹艺人等人脸头像；
- ★不良文字内容：包括色情、涉政、暴恐、违禁、低俗辱骂等；
- ★支持常规图片文件格式，包括 jpg、png、bmp、gif 等；

◎支持对文档的文本内容进行文本审核，审核内容包括：

- ★不良文字内容：包括色情、涉政、暴恐、违禁、低俗辱骂等；
- ★敏感人物人名：包括落马官员、劣迹艺人等人名检测；
- ★支持常规文档文件格式，包括 doc、docx、ppt、pptx、xls、xlsx、pdf、txt 等；

◎系统支持检测数据展示功能，包括文件类型、文件名、文件大小、上传时间、报警类型、报警时间点、报警内容截图等；

◎大屏内容安全统一管理平台采用 GIS 地图，直观展示所接入的所有设备的位置、工作状态、报警，当设备节点出现任何问题时，通过地图上的设备示意，及时向用户发出报警；

◎支持上传文件、下载及报警事件存储；

◎支持用户自定义敏感词库；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231827

★有效期：2023 年 06 月 21 日至 2025 年 06 月 21 日

所属品牌：万物安全产品体系 -LA 标品

发布时间：2024 年 9 月 13 日

产品适用领域：金融业、银行业、交通行业、智慧城市、交易行业

产品照片：



产品咨询二维码



产品咨询邮箱：huangjt@iottpa.com

沈阳东软系统集成工程有限公司

沈阳东软系统集成工程有限公司 1997 年 3 月 6 日成立，注册资金 7500 万元。公司秉承“超越技术的应用智慧”的经营理念，为客户提供优秀的计算机系统集成解决方案为核心业务方向，以客户为中心，面向政府、公检法和企业的信息基础设施建设，围绕客户的核心业务，提供软件和安全解决方案。业务范围包括：计算机信息系统软件开发、硬件系统安装调试、面向客户的 IT 信息系统规划和建设方案、IT 设施运营维护、技术培训、建筑智能化设计与施工、信息安全服务、商用密码产品的生产及销售等。近年来，在政府、通信、医疗卫生、交通、税务、教育、电力、安全等领域，保持领先地位，市场遍布全国十几个省市地区。

网址：<http://www.neusoft.com>

电话：010-57080489

地址：辽宁省沈阳市浑南区创新路 175-3 号 501、502、503、504、510 室

产品名称：东软 NetEye 运维安全网关系统

产品概述

“运维安全网关（NABH）”目标是为组织 IT 系统核心服务器的运维操作提供强有力的监控、审计手段，使其切实满足内控管理中的合规性要求。

NABH 可对主机、服务器、网络设备、安全设备等的管理维护进行安全、有效、直观的操作审计，对策略配置、系统维护、内部访问等进行详细的记录，提供细粒度的审计，并支持操作过程的全程回放。NABH 弥补了传统审计系统的不足，将运维审计由事件审计提升为内容审计，并将身份认证、授权、管理、审计有机地结合，保证只有合法用户才能使用其拥有运维权限的关键资源。NABH 为组织在 IT 操作风险控制、内控安全和合规性等方面提供一套完善、有效的审计手段。

功能特点

◎采用了先进的设计理念和体系架构

东软 NetEye 运维安全网关系统采用先进的面向服务的设计理念和消息机制，确保应用和系统的灵活性和稳定性。

◎全面的协议支持

东软 NetEye 运维安全网关系统支持全面的资产协议运维，支持的协议包括：

文本协议：Telnet、SSH、(S)FTP；

图像协议：RDP、VNC、X11；

Web 协议：HTTP、HTTPS；

数据库协议：Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix、MySQL；

应用协议：Weblogic、EMC、F5、Radware、VMware vSphere Client、ADS、NetApp、Symantec pcAnywhere。

◎业界最完备和安全的运维端到堡垒机的访问机制

东软 NetEye 运维安全网关系统具有业界最完备和安全的运维端到堡垒机的访问机制，采用强加密的 SSL 传输控制命令，完全避免可能存在的嗅探行为，确保数据传输安全。同时，产品还支持一次一密动态口令的认证方式。

◎精确的操作命令识别技术

东软 NetEye 运维安全网关系统能支持超长 SQL 查询语句（大于 4K）识别，以及 Telnet、SSH 超长命令识别。

◎智能的设备凭证托管和单点登录能力

东软 NetEye 运维安全网关系统提供智能的设备凭证托管服务，可以在登录时自动填入已授权的设备账户凭证，并在受委托的情况下定期去修改账户凭证。通过大量地研究和分析各类系统登录和改密机制，使得东软产品可以自适应绝大部分系统，不需要定制相关脚本。

管理员事先将设备账号及其密码保存在堡垒机，运维人员登录堡垒机并经过认证授权后就可以直接访问目标设备，无须再次手工输入设备账号和密码信息，无须记忆多个设备账号和密码，实现真正意义上的单点登录（SSO），提高运维人员工作效率、改善用户体验。

◎全面对象实例化和人性化的人员与设备管理

东软 NetEye 运维安全网关系统采用符合用户线性化操作习惯的界面交互设计，以及符合用户层次化思维的设备管理界面设计，用户使用上手快、操作方便。

在人员与设备管理上，提供了各种人性化的措施，例如，支持全列表视图的模糊查询、支持设备批量扫描以及自动识别新增设备等功能。

◎智能的虚拟化操作回放

提供图像形式的回放，真实、直观、可视地重现当时的操作过程；回放提供快放、慢放、拖拽方式，方便快速定位和查看；针对命令交互方式的协议，提供按命令进行定位回放；针对图像协议，提供按时间进行定位回放。

◎图形并发业界最优

东软 NetEye 运维安全网关系统采用高效 RDP 代理机制，图形 RDP 会话最大并发数为 500 个。

◎双机热备中零延时配置与操作日志同步

东软 NetEye 运维安全网关系统支持双机热备中设备间零延时配置同步，支持双机热备中设备间操作日志零延时同步。

技术指标

◎支持协议：telnet、ssh、rdp、vnc、xwin、http、https、ftp、sftp、AS400、SQLServer、

SYBase、MySQL、oracle、db2、informix;

◎**端口安全技术**：采用端口安全机制，不开放或变相开放 3389、22、21、23、5900 等高危端口实现高效协议代理；

◎**操作体验**：支持 WindowsUI 设计，采用 windows 操作系统风格，所有对象（用户、设备、账户、会话等）采用图标化展现，操作简便，无需专门培训即可完成相关操作。

◎**RDP 协议代理技术**：采用真正意义上的 RDP 协议级代理机制，而非经过多次应用级转换的“RDP 代理”，使得 RDP 运维代理最高效，单台设备即可实现 500 以上的 RDP 并发访问；

◎**自动发现**：支持网络环境中新增目标设备的自动发现功能，减轻堡垒机维护人员的工作负担；

◎**数据库 sql 语句黑白名单**：不仅支持命令行操作界面的 SQL 语句阻断功能，还支持图形客户端连接工具的 SQL 语句阻断（如 plsql、SQLplus、toad 等），以防止数据库管理员的误操作；

◎**文件传输黑白名单**：支持文件传输的黑白名单，针对不同用户可设置不同的文件传输权限，比如不允许上传、下载、删除、修改等权限；

◎**双机部署**：支持高可用的 HA 双机部署，采用心跳线和数据线两条线路，确保数据无延时同步，支持对方存活检察和服务自动修复功能；

◎**集群部署**：支持自建集群部署，不依赖任何第三方设备，如 F5、单独的存储设备等，支持无缝横向扩展；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230271

★有效期：2023 年 02 月 10 日至 2025 年 02 月 10 日

所属品牌：东软 NetEye

发布时间：2011 年 9 月 9 日

产品适用领域：政府、医疗、电力

产品照片：



产品咨询邮箱：servicedesk@neusoft.com



产品咨询二维码

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：运维安全中心（堡垒机）

产品概述

腾讯云运维安全中心（堡垒机）（Operation and Maintenance Security Center (Bastion Host)）可为您的 IT 资产提供代理访问以及智能操作审计服务，为客户构建一套完善的事前预防、事中监控、事后审计安全管理体系。

功能特点

◎全面的资产管理：支持多云、线下资产的统一管理，支持主流的操作系统和数据库版本，有效辅助管理员进行安全运维。

◎细粒度权限控制：支持基于用户、资产、账号、操作权限等维度进行细粒度授权，确保用户所拥有的权限是其访问资产、完成工作任务的最小化权限。

◎良好的运维体验：支持多种主流运维操作客户端工具，并且适配 Windows 和 MacOS 终端，运维过程当中，不改变运维人员原有的操作习惯。

◎智能账号管理：支持账号推送和改密计划，协助管理人员对资产账号进行管理

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01809-A

★有效期：2024 年 12 月 06 日至 2026 年 12 月 06 日

所属品牌：腾讯安全

发布时间：2019 年 10 月 18 日

产品适用领域：金融、出行、传媒、零售、医疗

产品照片：



产品咨询二维码



产品咨询邮箱：jessecchen@tencent.com

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<http://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼天融信科技集团

产品名称：天融信工业运维安全审计系统

产品概述

天融信工业运维安全审计系统是一款针对工业主机、工业网络设备、工业安全设备、应用系统、数据库等设备进行集中运维管理和审计的安全产品。通过集中化账号管理、高强度认证加固、细粒度授权控制和多形式审计记录，使内部人员、第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免误操作和非授权操作带来的隐患，有效保障工业企业资产安全运行和数据安全使用。

功能特点

◎自动化运维管理

系统支持手动或自动执行运维脚本，可使用各种内置模板、自定义脚本进行功能扩展来完成特定任务，执行资产信息获取、自动探测、命令执行、文件分发、脚本任务等，提高运维工作效率、改善用户体验。

◎集中化账号管理

系统建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，无缝对接工业

上位机、工业安全设备、工业网络设备、工业服务器、中间件等，完成对账号整个生命周期的管理。

◎多元化认证机制

系统提供统一的认证鉴权接口，支持本地认证、LDAP 认证、RADIUS 认证、USBkey 认证、动态口令等多种方式，实现统一、灵活、高强度的认证管理，保证资产运维管理的安全性和可靠性。

◎细粒度权限控制

系统可基于访问用户、时间、IP 地址等维度进行权限控制，细化控制规则，规范运维人员日常管理方式，保证系统入口的安全性，简化授权管理，杜绝非法用户、非法 IP 接入。

◎全方位运维审计

系统可对经过工业堡垒机的全部操作进行日志记录，完整审计运维人员从登陆到退出的全过程，帮助管理人员及时发现违规操作，准确定位身份，以便追查取证。

◎高可靠性运维保障

系统采用双重冗余设计框架，同时支持 HA 双机热备功能，规避单点故障隐患，最大程度上保障用户运维管理工作的连续性和高可靠性。

◎运维数据安全加密

系统对配置数据和用户数据都进行了加密处理，避免了信息泄露的风险。在管理页面的前台、后台通信中，除了通信链路本身的加密，还对用户密码等关键信息进行了二次加密，防止恶意用户监听、截获和篡改数据，充分保障用户在操作全过程中的安全性。

◎强大的自动化运维技术

系统通过自动化运维框架支持多节点发布、远程任务执行，无需在被管理节点上安装附加软件，可使用各种内置模块、共享脚本库、自定义脚本进行功能扩展来完成特定任务，如资产信息获取、自动探测、命令执行、脚本任务、文件分发等，灵活方便的运用于 DevOps 的开发、测试、实施、监控、分析工作中。

◎高效图像识别技术

系统采用了图像模式识别技术，通过加载训练过的运维图片集合，可以识别图形操作中的程序标题、快捷方式标题、窗口内容中的文本信息，识别的方式具有更广泛的通用性，将识别出来的操作记录以文字指令方式存储，通过指令审计可以直接定位到相应的审计视频，进行视频定点回放，让审计内容更完整并具有层次化，另外，文本检索也提高了图形操作的审计效率。

技术指标

◎功能指标

支持 SSH、RDP、VNC、SFTP、Telnet、FTP、HTTP、HTTPS、X11 等运维协议
持密码认证、证书认证、OTP 认证、短信认证、UKey 认证等双因素认证方式

支持通过远程协助操作邀请其他运维用户登录资产，共同运维资产

可管理工控设备包括工控防火墙、工控监测审计、工控入侵检测、工控主机卫士、工控集中管理、工控漏扫、工业态势，支持单点登陆

支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权

支持实时监控运维终端与资产正在进行的会话和操作，可中断运维人员与资产的连接

◎性能指标

天融信工业运维安全审计系统管理主机数量覆盖 100 个至 300 个，字符并发数覆盖 100 个至 300 个，图形并发数覆盖 50 至 150 个。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：中国网络安全审查技术与认证中心

★证书编号：24SS00019-A

★有效期：2024 年 01 月 05 日至 2026 年 01 月 05 日

所属品牌：北京天融信网络安全技术有限公司

发布时间：2021 年 1 月 10 日

产品适用领域：天融信工业运维安全审计系统可广泛应用在轨道交通、电力、冶金、煤炭、石油化工、市政、烟草、智能制造、核电等行业。

产品照片：



产品咨询二维码

产品咨询邮箱：feng_chong@topsec.com.cn

产品名称：天融信运维安全管理系统

产品概述

天融信运维安全管理系统是面向政府、企事业单位等组织机构推出的兼具运维管理和合规审计的产品。通过集中化账号管理、高强度认证加固、细粒度授权控制和多形式审计记录，使内部人员和第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免误操作和非授权操作带来的隐患，有效保障组织机构的服务器、虚拟机、网络设备、安全设备、数据库、业务系统等资产的安全运行和数据的安全使用。堡垒机以单点登录为核心，运维代理技术为支撑，通过高可用的部署方式，为用户提供跨平台资产管理、自动化运维和运维分析报表等运维管理工具。

功能特点

◎单点登录：天融信运维安全管理系统提供了基于 B/S 和 C/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证的访问被授权的多种基于 B/S 和 C/S 的应用系统。单点登录（Single Sign On）包含用户单点和代填登录两个工作流程。单点是用户通过一次登录，即具有多资产多账号的访问权限，为多系统多账号管理的运维人员提供了统一、方便、快捷的访问途经。代填登录使用户无需记忆大量资产登录账号和口令。配合认证加固功能和密码策略，在保证便捷性的同时加强认证环节，实现统一安全登录。运维用户通过浏览器登录堡垒机 WebUI，使用浏览器作为 Web 客户端登录目标设备；运维用户通过 RDP、SSH、VNC、Telnet、FTP、SFTP、HTTP/HTTPS 等协议连接运维代理，访问目标资产。还可以实现调用 SecureCRT、XShell、Putty、Mstsc、Xftp、WinScp 等客户端工具登录目标设备。

◎HTML5 代理：天融信运维安全管理系统的单点登录采用了 HTML5 运维代理，无需安装 Agent 和插件，即可实现跨平台、多协议（SSH、RDP、FTP、SFTP、Telnet、VNC、DB 等）的运维代理和安全审计功能。

系统采用 HTML5 技术实现了模拟的运维客户端，用户无需调用本地客户端，在浏览器里即可以 SSH、RDP 等方式对资产进行运维。在运维过程中，前台 HTML5 模拟客户端会连接后台的运维代理引擎，包括 SSH Web 代理、RDP Web 代理、Telnet Web 代理、VNC Web 代理、FTP Web 代理、SFTP Web 代理、DB Web 代理、HTTP/HTTPS Web 代理和应用 Web 代理等子模块，代理引擎将 Web 流量进行解析、审计，并转化为运维协议，通过 SSH、RDP、Telnet、VNC、FTP、SFTP、DB 等特定协议连接资产。

技术指标

单点登录；
访问控制；
操作审计；

会话监视；
会话回放；
告警；
违规操作阻断；
高可用性；
标识与鉴别；
安全管理；
审计日志；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230755

★有效期：2023 年 4 月 7 日至 2025 年 4 月 7 日

所属品牌：天融信

发布时间：2019 年

产品适用领域：天融信运维安全管理系统适用于各个行业，如政府、能源、
交通、金融、教育、企业集团、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：feng_chong@topsec.com.cn

产品名称：天融信运维安全审计系统

产品概述

天融信运维安全审计系统是面向政府、企事业单位等组织机构推出的兼具运维管理和合规审计的产品。通过集中化账号管理、高强度认证加固、细粒度授权控制和多形式审计记录，使内部人员和第三方人员的操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免误操作和非授权操作带来的隐患，有效保障组织机构的服务器、虚拟机、网络设备、安全设备、数据库、业务系统等资产的安全运行和数据的安全使用。堡垒机以单点登录为核心，运

维代理技术为支撑，通过高可用的部署方式，为用户提供跨平台资产管理、自动化运维和运维分析报表等运维管理工具。

功能特点

◎单点登录：天融信运维安全审计系统提供了基于 B/S 和 C/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证的访问被授权的多种基于 B/S 和 C/S 的应用系统。单点登录（Single Sign On）包含用户单点和代填登录两个工作流程。单点是用户通过一次登录，即具有多资产多账号的访问权限，为多系统多账号管理的运维人员提供了统一、方便、快捷的访问途经。代填登录使用户无需记忆大量资产登录账号和口令。配合认证加固功能和密码策略，在保证便捷性的同时加强认证环节，实现统一安全登录。运维用户通过浏览器登录堡垒机 WebUI，使用浏览器作为 Web 客户端登录目标设备；运维用户通过 RDP、SSH、VNC、Telnet、FTP、SFTP、HTTP/HTTPS 等协议连接运维代理，访问目标资产。还可以实现调用 SecureCRT、XShell、Putty、Mstsc、Xftp、WinScp 等客户端工具登录目标设备。

◎HTML5 代理：天融信运维安全审计系统的单点登录采用了 HTML5 运维代理，无需安装 Agent 和插件，即可实现跨平台、多协议（SSH、RDP、FTP、SFTP、Telnet、VNC、DB 等）的运维代理和安全审计功能。

系统采用 HTML5 技术实现了模拟的运维客户端，用户无需调用本地客户端，在浏览器里即可以 SSH、RDP 等方式对资产进行运维。在运维过程中，前台 HTML5 模拟客户端会连接后台的运维代理引擎，包括 SSH Web 代理、RDP Web 代理、Telnet Web 代理、VNC Web 代理、FTP Web 代理、SFTP Web 代理、DB Web 代理、HTTP/HTTPS Web 代理和应用 Web 代理等子模块，代理引擎将 Web 流量进行解析、审计，并转化为运维协议，通过 SSH、RDP、Telnet、VNC、FTP、SFTP、DB 等特定协议连接资产。

技术指标

- 单点登录；
- 访问控制；
- 操作审计；
- 会话监视；
- 会话回放；
- 告警；
- 违规操作阻断；
- 高可用性；
- 标识与鉴别；
- 安全管理；
- 审计日志；

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：中华人民共和国公安部

★证书编号：23SS00218-A

★有效期：2023 年 10 月 27 日至 2025 年 10 月 27 日

所属品牌：天融信

发布时间：2012 年

产品适用领域：天融信运维安全审计系统适用于各个行业，如政府、能源、
交通、金融、教育、企业集团、医疗等

产品照片：



产品咨询邮箱：feng_chong@topsec.com.cn



产品咨询二维码

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和“工业互联网+安全生产”的国家高新技术企业，国有资本占股近 50%。

基于“安全协同·AI 赋能”的战略理念，公司在工业互联网安全领域持续深耕，长扬科技在业界开创了“智能工业安全大脑”的产品理念，将产品及服务聚焦工业互联网安全及大数据应用领域，并通过人工智能技术赋予客户在网络和业务两个层面的安全防护能力。面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉 AI 安全分析、工业零信任安全、工业数据安全等多维度产品，构建覆盖工业互联网安全产业完整生命周期的工控网络安全保障体系。产品及解决方案已广泛应用于电力、石油石化、轨道交通、城市市政、智能制造、钢铁冶金等行业，满足等保 2.0 及关键信息基础设施安全保护条例要求。

长扬科技基于对国家工业互联网安全相关政策、法规与标准的持续研究和深度解读，积累超过 32 个行业细分领域、4000 余家工业企业的安全服务经验，可提供涵盖安全咨询规划、安全实施交付、大安全运营和安全培训 4 大类、27 项标准化服务产品，致力于为工业企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：www.cy-tech.net

电话：400-6655087

地址：北京市海淀区闵庄路 3 号玉泉慧谷 2 期 15 号

产品名称：长扬安全运维管理平台（SSA）

产品概述

为满足用户对工控系统安全运维日益迫切的需求，长扬科技依托强大的研发实力和丰富的行业经验，自主研发软硬件一体化的长扬安全运维管理平台（SSA）。在企业运维过程中，该产品通过对运维人员进行统一身份认证、统一授权、统一审计、统一监控，有效消除传统运维的盲区，实现了运维简单化、操作可控化、过程可视化，是企业内控最有效的管理平台。

功能特点

◎强大的应用发布系统

应用发布系统支持单应用和多应用两种模式，可以按需关闭某些应用中的图形界面功能。使用应用发布系统，可以严格限制运维用户的访问权限。

◎审计信息“零管理”

支持“日志零管理”技术，所有管理员需要的日常操作日志均可由系统定时自动在后台运

行，如日志自动维护、日志查询、多种类别的审计报表等。

◎支持多种管理方式

提供带外管理功能，解决远程应急管理的需求，减少用户运营成本、提高运营效率、减少宕机时间、提高服务质量，web 管理灵活方便。

◎方便灵活的可扩展性

支持多个硬件管理口，即插即用；具备对多个区域网段同时管理的能力，具备邮件、日志数据库记录、打印机输出、运行自定义命令等多种实时报警方式，真正实现第一时间发现故障。

技术指标

◎管理流程更加规范统一

为用户提供统一集中的账号管理，支持主流操作系统、网络设备、应用系统的账号安全策略配置；更支持指纹识别等多种身份认证方式，满足多种场景多种级别的安全要求，满足 IT 审计合规性需求。

◎提升运维效率

设备既可以实现对 B/S、C/S 应用系统资源的访问权限控制，也可以实现对数据库、主机（操作员站、工程师站、数据服务器等）及网络设备的操作的权限控制；用户只需要登录一次就可以访问相互信任的应用系统，简化管理提高用户效率，实现高度精细化管理。

◎减少操作风险

设备本身不影响网络拓扑和业务数据流，更支持双机热备和集中分级管理。

实时监控既能及时阻断危险又能防患于未然：对用户运维行为实时监控，可自定义访问策略，对重要指令进行二次审批，对危险运维指令实时阻断。

提供详尽完整的操作审计数据，有力支撑运维全过程的分析和管理的

可对安全设备、网络设备、数据库和服务器进行全方位的监控和管理，将用户所有的操作日志行为通过集中录屏、录像、文字多维度详尽记录和回放，所有操作均可审计和检索查询，便于分析挖掘问题根因和事后的安全事故责任认定。

产品安全认证或安全检测结果证明等

（1）计算机信息系统安全专用产品销售许可证

★证书编号：0404230617

★有效期：2023 年 3 月 24 日至 2025 年 3 月 24 日

（2）计算机信息系统安全专用产品销售许可证

★证书编号：0404231329

★有效期：2023 年 6 月 2 日至 2025 年 6 月 2 日

所属品牌：长扬科技

发布时间：2021 年

产品适用领域：城市市政、工业互联网、轨道交通、化工、能源、信息系
统集成、教育

产品照片：



产品咨询二维码

产品咨询邮箱：support@cy-tech.net

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望统一安全管理与运维审计系统

产品概述

远望统一安全管理与运维审计系统结合 ITIL、ITSM、IT 内控、SOX 法案\COBIT 法规、信息安全等级保护及 IT 运维管理要求，融合运维管理和运维安全的特性，切断终端对服务器、数据库系统及网络资源的直接访问，采用代理转发的方式接管终端对网络资源的直接访问，集中实现用户的身份认证、授权管理、访问控制和操作审计。

功能特点

◎全面单点登录

支持各类于运维协议和工具的账号密码代填，实现单点登录。只需通过堡垒机认证，可直接访问后端所有授权的设备和资产。系统除了支持常规的图形终端协议（RDP、VNC、X11）、字符终端协议（Telnet、SSH）、文件传输协议（FTP、SFTP）、WEB 应用协议（HTTP、HTTPS），支持各类数据库运维工具（Oracle、SQL Server、DB2、MySQL、Informix、Sybase、PostgreSQL、Mongo DB、达梦、人大金仓等），还支持各类其他应用工具（AS400、Real VNC、PCAnywhere、Radmin、DameWare、CiscoASDM、VMware vSphere Client 等），各类协议及应用程序单点登录的内置支持多达 80 余种；另外针对个性化应用程序的登录还支持自定义程序代填方式（CommonAPP），可满足绝大部分程序的单点登录支持。

◎多因素身份鉴别

系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、Radius 认证、LDAP、AD 域、数字证书认证、动态令牌认证、USBKEY 认证、指纹认证、手机动态令牌认证、CAS 认证、SAML 认证等 10 余种认证因子；

系统内置动态令牌认证系统，用户无需额外部署认证服务器，通过配置动态令牌实现双因素认证；并且自有 OTP 动态令牌 APP 和微信小程序，同时可兼容 Google、FreeOTP、ZB 身份验证器等常用手机动态令牌 APP 认证；

支持多因子认证自定义组合，可为不同用户组分配不同的认证策略，支持单因素，双因素和多因素的认证策略。

◎传输审计和控制技术

实现对图形终端 RDP、图形应用操作的细粒度访问控制，支持对磁盘通道、剪贴板、声音、打印机、智能卡进行控制，控制细粒度到具体的自然人以及磁盘通道、剪贴板的上下行操作控制，并对下载文件进行提取备份；

提供对 FTP/SFTP 传输的文件审计及备份提取功能，对传输的内容严格审计及上下行操作控制，杜绝小概率安全事件，记录审计结果。当事件发生时，可追查至恶意文件及脚本的源头。

◎OCR 标题栏识别技术

OCR 标题栏识别技术是一种图像信息数字化的过程，这个过程帮助运维人员快速、高质量地将图形运维审计录像（RDP 操作）进行数字化处理，"实时存储并提取标题栏文字信息，对海量图形操作审计信息进行快速检索、精确定位播放；解决了传统的图形运维审计通过拖拉、快进等方式回放审计记录寻找始发源头的不确定性和时效性问题。通过预设策略，借助 OCR 识别技术对敏感文件的访问进行告警输出，实现对敏感文件访问的实时监控。

◎全面的部署方式及可靠的数据同步技术

系统支持双机热备、集群、分级部署模式，同时通过专利技术确保在双机热备，集群部署，分布式部署模式下的数据同步的可靠性和及时性，实现配置信息和审计日志实时同步，有效解决大数据同步的问题。

◎无缝应用发布技术

全面支持 RemoteAPP 无缝应用发布功能，实现无缝应用发布卓越的用户体验，所有应用发布均可本地化展示，无缝应用发布技术使得用户可以通过远程桌面服务远程访问程序，就好像它们在最终用户的本地计算机上运行一样。

◎移动平台接入技术

自主开发移动 app 程序，且该 app 软件已在 AppStore 和安卓平台发布。只需在移动终端安装 app 软件，即可实现对 Linux 资产、windows 资产、数据库及其它应用资产的统一移动运维，并进行身份认证，权限控制，账号管理和行为审计的统一安全管理。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：23SS00310-A

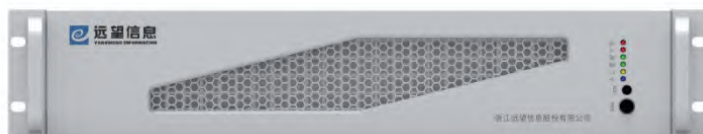
★有效期：2023 年 11 月 17 日至 2025 年 11 月 17 日

所属品牌：远望

发布时间：2023 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询二维码

产品咨询邮箱：mail@chinayuanwang.com



日志分析产品

北京安信天行科技有限公司

北京安信天行科技有限公司是国有控股企业，立足于自主知识产权网络安全产品、提供可管理信息安全服务的综合解决方案提供商。

以提供专业的网络安全服务为核心，安信天行建立了完备的安全运营服务体系、权威的安全服务资质体系和专业化安全服务团队，为政务、卫生、纪检、教育、广电、企业等各领域千余家单位信息化建设保驾护航。作为国家重大活动网络安全保卫技术支持单位，安信天行持续为 2008 年北京奥运会、国庆 70 周年、中国共产党成立 100 周年庆祝大会、2022 年冬奥会冬残奥会等重大活动提供网络安全保障工作，为活动的顺利举办做出重要贡献。

以人为本，开拓创新，安信天行先后承担工信部、国家保密局等国家科技攻关和课题研究项目，荣获“科技进步奖”、“高新技术企业”、“国家信息安全漏洞库技术支撑单位”、“国家信息安全漏洞平台成员单位”等荣誉。目前，安信天行已取得国家专利技术及自主知识产权近百项，打造了安全态势感知、安全防御、数据安全、保密安全等四条产品线，帮助用户构建全方位的网络安全保障体系，并已在各个行业取得了广泛应用。

安信天行将坚持“以服务求生存、用创新谋发展”理念，保障用户网络空间安全，致力于成为用户最信赖的网络安全企业。

网址：www.axtx.com.cn

电话：010-58045858

地址：北京市海淀区北四环西路 68 号左岸工社 10 层 1001

产品名称：日志分析管理系统

产品概述

日志分析管理系统是安信天行自主研发的一套日志分析与管理系统。它具备对整个信息系统中的各类资产数据进行集中采集、统一管理、智能审计的分析功能，是一套集中统一的日志综合管理平台。日志分析管理系统能够 7*24 小时不间断地对主机设备、网络设备、安全设备、数据库、中间件记录的各种不同日志进行集中采集，格式化处理，关联分析和可视化呈现，帮助运维人员实现海量日志数据的监控、管理、分析，提高业务的安全性和可靠性。

安信天行日志分析管理系统是在综合考虑客户需求和市场现状后而推出的统一日志管理分析以及日志审计系统，系统可以集中收集、长时间存放所有的原始日志，同时可以高效准确完成海量日志分析统计工作，实现统一监控，全面分析，及时告警、从而确保系统的安全稳定运行。

功能特点

◎产品功能

★资产监控

系统支持实时告警数、资产总数、日志事件总数、系统健康状况的显示。支持查看详情，支持告警弹框、声音提醒。

★资产管理

可查询资产详情画像；支持手动导出资产概要信息，开启 / 关闭资产采集数据；资产画像支持查看资产概要信息以及资产异常信息列表等综合信息；

★日志查询

系统支持多条件组合查询；支持原始日志全文检索。

★高级查询

支持丰富的过滤条件：设备 IP、来源 IP、目的 MAC、来源端口、目的端口、目的地址 IPV6、源 MAC、源地址 IPV6、操作用户、事件级别、应用名称、请求信息请求方式等。

★事件设置

系统支持复杂的组合特征事件自定义，可自由设置不同分类属性，支持动作与动作之间的关系，动作与特征的关系，复杂特征动作和复杂特征动作之间的关系，以此实现复杂的事件分析研判与追踪。

★告警管理

系统支持根据时间范围、级别、规则类型、告警全文关键字等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出。支持多种告警方式，支持在全局显示告警提醒。

★攻击分析

实现对不同安全域、不同时间的多来源安全相关事件进行多维度（多种时空属性和网络属性）的关联分析、异常行为检测和追踪溯源分析。

★报告管理

系统提供综合报表、资产报表、事件报表三大报表管理引擎，可以灵活管理报告开关。

◎产品特点

★全面采集

系统采用多种技术手段，充分适应用户实际网络环境的运行情况，采集用户网络中分散在各个位置的各种厂商、各种类型的海量日志，并对传输链的各个环节进行监控，消除无关数据，合并重复的资产日志，确保资产数据的全面收集。

★变频采集

平台自动监控采集日志通道拥堵状态，实现客户端采集和平台之间采用变频链接方式，根据算法，根据平台接收通道负载和当前 CPU、内存使用率综合判断负载，负载过大降低采集频率，等待负载过小再依次上传历史日志。

★协议采集

系统利用数据采集引擎、数据处理引擎采用被动与主动采集技术相结合，通过包括但不限于 Syslog、SNMP Trap、Winlogbeat、Telnet/SSH、Filebeat、FTP/SFTP/SCP、JDBC 文件等标准协议从审计对象获取海量日志数据。

★一键升级

Agent 采集客户端支持通过平台心跳链接方式接收升级指令，由平台主动创建批量升级任务下发，实现客户端成功接收指令后开始自动升级（单选升级和批量升级），极大减少运维人员重复工作带来的不便。

★数据挖掘

日志审计系统支持对存储的历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。

技术指标

设备管理	需支持以列表形式展现关联设备资产关键属性信息功能，包括但不限于主机名、IP、设备状态、日志总数、采集状态、添加时间等；需支持基于 excel 格式资产的批量导入功能；需支持基于 excel 格式的资产密码批量修改功能。
	需支持资产的分组管理功能，可将资产按照类型分组；需支持按照资产分组、子分组的查找功能，进行资产的分类检索；
日志采集	需支持对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面审计功能。
	需支持服务器系统日志、安全日志、中间件系统、访问日志、网络设备、安全设备发送的 Syslog 日志等多种类型日志收集功能。
	需支持通过 syslog 等多种采集方式完成各种日志的收集功能。
日志管理	需支持思科、华为、锐捷等主流厂商交换机、路由器的日志获取、分析与告警功能；需支持防火墙、IDS、IPS 等安全设备日志获取、分析与告警；需支持 Windows、Linux 操作系统、数据库、中间件的日志获取、分析与告警；
	需支持针对某项设备资产设置日志告警策略功能；需提供根据关键字段进行日志、告警的关键字查询；需支持告警日志多格式的导出功能。
	需支持自动生成日志周报表功能，支持日志报告的下载。
告警管理	需支持对发现的严重事件的自动告警功能，告警内容支持用户自定义字段。
	需支持日志、事件、报警查看和展示功能，包括日志可视化展示以及日志、事件、报警数据的精准定位。
	需支持查看某规则的告警信息功能，对告警日志可按各告警字段进行查询。
	需支持展示日志告警和日志统计分析的实时综合性监控界面。

备份归档	需支持按日志属性（原始日志、重要日志、告警日志）、日志类型、存储周期的方式选择备份功能，支持原始日志与分析后日志分离。支持数据库备份；支持历史日志恢复导入；
	需支持各种配置项的备份和导入功能。
	需支持各种配置项的一键备份和恢复功能；当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。
权限管理	需支持角色的权限管理机制允许多用户访问功能。角色能够从设备和功能两个维度进行定义，从而达到控制谁可以对什么设备进行什么操作的控制粒度；支持禁止与允许用户访问日志审计系统的 IP 地址限制。支持限定管理员只允许查看自己所负责设备的日志；

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
- ★证书编号：24SS00136-A
- ★有效期：2024 年 2 月 2 日至 2026 年 2 月 2 日

所属品牌：北京安信天行科技有限公司

发布时间：2017 年 10 月 11 日

产品适用领域：政务、卫生、金融、教育、电信、交通等。

产品照片：



产品咨询二维码

产品咨询邮箱：axtxmarketing@bjca.org.cn

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区上地东路 1 号院华控大厦 7 层

产品名称：日志审计与分析系统

产品概述

日志审计与分析系统是面向工控网络的日志数据采集、归并、留存的日志管理系统。产品兼容大多数主流厂商的日志格式和数据流格式，通过大数据分析 with 搜索技术，对海量日志进行关联分析，实现安全事件溯源，协助运维人员进行安全监视、审计追踪、调查取证等操作。

功能特点

◎多类型日志采集

系统提供 TCP、UDP、SYSLOG、SNMP、FTP、SFTP、WMI、代理插件上传、文本文件上传等多种方式进行日志采集，可智能识别各种路由器、交换机、防火墙、应用系统等设备产生的日志信息。

◎大数据搜索技术，快速溯源

采用大数据搜索技术，通过垂直搜索引擎对无序化的信息进行高效检索，使用倒排索引、事件关联评分机制实现单台低端设备即可实时检索亿级规模日志。

◎可扩展分布式部署

采用可扩展的系统结构，支持分布式部署，通过将设备进行多级划分、横向扩展，可轻松

实现云端架构部署。

◎先进的关联分析算法

利用大数据分析算法，使用非关系型数据库，通过全内存运算的方式，对事件信息进行复杂的关联分析与时间序列关联分析处理，对安全威胁事件进行及时告警。

◎丰富的自定义报表

系统根据不同的业务场景，预置丰富多样的报表和各事件板块进行主题数据分析，提供高效、智能的报表生成工具，轻松整合多源数据，形成全局数据视野，掌控网络全局。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01482-A

★有效期：2024 年 10 月 12 日至 2026 年 10 月 12 日

所属品牌：珞安科技

发布时间：2019 年 1 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业

产品照片：



产品咨询二维码

产品咨询邮箱：support@icssla.com

北京威努特技术有限公司

北京威努特技术有限公司（简称：威努特）是国内工控安全行业领军企业，凭借卓越的技术创新能力成为全球六家荣获国际自动化协会 ISASecure 认证企业之一和首批国家级专精特新“小巨人”企业。

威努特秉承“专注工控，捍卫安全”的使命，依托率先独创的工业网络“白环境”核心技术理念，以自主研发的全系列工控网络安全产品为基础，为电力、轨道交通、石油石化、市政、烟草、智能制造、军工等国家重要行业用户提供全生命周期纵深防御解决方案和专业化的安全服务，迄今已为国内及“一带一路”沿线国家的 10000 多家行业客户实现了业务安全合规运行。有关国家权威机构市场分析表明，威努特多款产品如工业防火墙、工控主机卫士、工控漏扫、工控漏挖等，均位列中国工控安全市场发展能力及市场地位第一。

作为中国工控安全国家队，威努特积极推动产业集群建设，构建生态圈发展，参与工控安全领域国家、行业标准制定和重大活动网络安全技术保障工作，始终以保护我国关键信息基础设施网络空间安全为己任，成为中国网络安全建设的中坚力量！

网址：www.wincssec.com

电话：4000-680-620

地址：北京市海淀区上地三街 9 号 F 座 9 层 907

产品名称：威努特日志审计与分析系统

产品概述

威努特日志审计与分析系统能够实时接收并解析网络设备、安全设备、主机设备、数据库、中间系统的日志，将各种形式的日志整理重塑成统一的日志格式，支持海量日志的留存和检索，满足网络安全法对日志保存 6 个月以上的要求，能够帮助一线人员从海量日志中快速定位查找找到相关日志，业务系统运行异常或遭受攻击等场景下能够自动实时告警并通知给相关责任人。

功能特点

◎ AB 网场景日志采集

工业网络 AB 网部署情况较多，日志源无论在 A 网还是 B 网，都可以无缝采集并上报日志，系统自动识别、统一处理，不影响后续的数据分析。

◎ 电力监控装置对接

采集代理 agent 支持南方电网的《电力监控系统网络安全态势感知采集装置技术规范》，可以采集工业主机操作系统和业务日志，agent 软件经过上千个工业现场项目验证，轻量级、运行

稳定、系统资源消耗少。

◎智能关联分析引擎

支持事件关联、时序关联、统计关联分析功能，提供网络异常、流量异常、登录异常、行为异常等百余种关联分析策略。

◎工业流量日志分析

百种工业主机安全事件日志接收和解析，包括 Windows/Linux/Solaris/AIX 系统日志、未经批准非法使用外部设备日志（U 盘、CDROM、网卡、串口、并口）、禁用软件和服务日志、未经授权非法访问敏感文件日志、非法连接外网日志、违规开发高危端口日志等。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00980-A

★有效期：2024 年 7 月 12 日至 2026 年 7 月 12 日

所属品牌：威努特

发布时间：2018 年 8 月 15 日

产品适用领域：电力、石油石化、轨道交通、市政、烟草、智能制造等产

品照片：



产品咨询邮箱：support@winicsssec.com



产品咨询二维码

北京长亭科技有限公司

长亭科技是国际顶尖的技术驱动型安全公司，全球首发基于智能语义分析的下一代 Web 应用防火墙产品，成为中国 WAF 市场份额占有率增速最快的下一代网络安全公司。目前，公司已发布 10 余款自研技术驱动产品，形成以攻（安全评估系统）、防（下一代 Web 应用防火墙、高级威胁分析预警系统）、知（安全分析与管理平台、攻击面管理运营平台）、查（主机安全管理平台）、抓（伪装欺骗系统）为核心的新一代安全防护体系，并提供优质的安全测试及咨询服务，为企业级客户带来智能的全新安全防护思路。

网址：www.chaitin.cn

电话：4000-327-707

地址：北京市朝阳区天辰东路 7 号楼 -2 至 8 层 101 内北区 6 层 602 室

产品名称：长亭日志审计分析系统 V2.0

产品概述

长亭日志审计分析系统具备对整个信息系统中的各类日志进行集中采集、集中管理、集中审计的能力。能够实时采集各种不同厂商的安全设备、网络设备、主机、操作系统以及各种应用系统产生的日志、事件、报警等信息，并将数据信息汇集到展示平台，进行集中存储、展现、查询和审计。支持对网络安全事件的收集与分析，发现疑似攻击或违规访问时可告警并响应；根据历史数据进行安全审计，生成审计报表，满足合规要求；对收集和分析的网络安全事件进行备份归档。

通过部署长亭日志审计分析系统，一方面可以集中收集、长时间存放所有的记录日志，避免日志遭到恶意篡改或删除而在安全事件发生时无据可查的状况发生。另一方面，强大的日志审计能力可以为组织审计人员提供日志实时监控、高效检索、审计报表等日志审计手段，从而使原本不可能完成的海量日志审计工作可以在短时间内轻松完成，大大减少信息部门的工作量。

功能特点

◎集中化的日志综合审计

长亭日志审计分析系统提供强大的日志综合审计功能，为不同层级的用户提供了多视角、多层次的审计视图。

系统首先提供了全局监视仪表板和统计视图，可在一个屏幕中看到不同设备类型、不同安全区域的实时日志流曲线、统计图，以及网络整体运行态势、待处理告警信息等。同时具备日

志查询功能和规则、统计关联等分析方法，可制定查询策略，针对归一化后的日志或者原始日志进行综合条件查询和模糊查询。

◎全面的智能收集功能

不断的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控；可配置过滤和聚合功能可以消除无关数据，并且合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

◎创新的日志解析能力

解析规则激活，仅当接收到对应的日志后，规则才会被激活，同时支持未识别日志水印处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）；日志解析性能与接入的日志设备数量无关。

◎先进关联算法

长亭日志审计分析系统的关联分析引擎采用实时流分析+全量数据关联分析的设计，同时保证了关联分析的实时性和超长的时间范围覆盖度，采用实时流分析+全量数据关联分析的设计在多方面都有巨大的优势。关联算法也有独到之处：标准化之上的关联规则，适应性强；可定制性强，几乎可根据通用事件的任何字段进行关联；基于逻辑表达式，可以进行复杂关联；时序宽容，无惧乱序。

◎可维护性及可拓展性

系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。硬件系统采用模块结构，保证系统内存、CPU 及储存容量的扩展；硬件配置的升级不会引起软件的修改和开发；每个组件都可以横向扩展，通过增加设备满足业务需求。

◎采用通用的安全事件标准

根据多年的网络安全经验，总结出了通用标准的安全事件归一化格式和分类体系结构。长亭日志审计分析系统可以以标准方式处理各种安全事件日志（攻击、入侵、异常）、行为事件日志（内控、违规）、弱点扫描日志（弱点、漏洞）、状态监控日志（可用性、性能、状态）、安全视角的事件描述等。

技术指标

模块	功能	具体要求
日志采集	采集类型及方式	支持市面主流安全设备、网络设备、中间件、服务器、数据库、操作系统、应用系统、云平台等设备对象的日志采集；
		支持主动、被动相结合的数据采集方式；支持日志转发；支持 Syslog、SNMP、JDBC、WMI、FTP、文件等进行数据采集；支持通过 Agent 采集日志数据；
		采集内容支持日志采集、文件采集（文件监控无需开启 ftp、sftp 协议）、流量采集；
	采集展示及处理	对元数据进行重加工或扩展加工，通过正则匹配、OID 映射等配置文件编写，上传至现有日志审计平台，直接实现数据的扩展兼容；

模块	功能	具体要求
日志审计	关联分析	支持所有事件字段参与关联规则进行关联分析，触发关联分析规则可产生告警；支持跨设备日志关联分析；
		提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则，关联内容支持不少于资产等 8 种信息；
	关系图谱	支持自动生成主机访问关系图谱。关系图谱支持无限级延伸，支持点击业务主机节点自动绘制访问关系；
		支持根据内置事件类型，按照用户环境需求，定义无限级深度事件模型，绘制全网事件关联关系模型，提供基于模型而非特征的问题发现能力，辅助发现未知威胁；
	可视化分析	自动分析网络流量，绘制流量流向图并自动更新流量流向图，支持按权重显示 IP 地址、端口；支持鼠标滑过加粗显示节点和关系；
		满足单位根据萨班斯法案 SOX 中对认证管理、账号管理、权限管理、操作管理、攻击管理、风险管理等相关事件要求统计；
统计报表	报表管理	满足单位信息安全要 ISO27001 中对资产管理、人力资源安全管理等相关事件要求统计；
		内置综合、用户访问、安全监测、信息审计、系统状态等报表组；支持 PDF、Word、HTML 等多种格式导出报表；
日志告警	告警管理	支持根据时间范围、级别、规则类型、告警全文关键字等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出。
		支持弹框、警示音、邮件、发送 SNMP Trap、Syslog 等告警动作；可以针对不同类型、不同种类以及不同安全级别指定不同的告警方式；
资产管理		支持在资产列表页面，以环形图、饼状图形式对资产分组和类型进行统计；
		支持按照角色对资产的日志查看权限进行授权；
		支持为一个 IP 分配多种业务类型，同时收取收集不同类型日志，并进行正确解析；
系统管理		支持存储空间使用率图表、动态监控，超过阈值进行告警，并自动清理存储；
		预留日志转发接口，至少支持将设备类型、设备 ip、事件类型等至少 16 类信息；

网络安全专用产品安全认证或安全检测结果证明

- 网络安全专用产品安全检测证书
- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
 - ★证书编号：24SS00989-A
 - ★有效期：2024 年 7 月 12 日至 2026 年 7 月 12 日

所属品牌：长亭科技

发布时间：2023 年 12 月

产品适用领域：金融、电力、能源、政府、交通、教育、医疗、运营商等

产品照片：



产品咨询邮箱：info@chaitin.com



产品咨询二维码

福建省海峡信息技术有限公司

福建省海峡信息技术有限公司是国内最早专业从事网络安全自主研发、产品销售及安全服务的公司之一。2022年4月，海峡信息正式成为福建广电网络集团直属单位。海峡信息是国有控股高新技术企业、国家“专精特新”小巨人企业、福建省创新型研发机构、行业领先的网络安全整体解决方案提供商，是福建省唯一通过国家信息安全服务资质安全运营认证、信息安全服务资质二级认证（安全工程/风险评估）的企业，2022年入选福建省重点上市后备企业，在江西、四川、湖北、湖南等地设有办事处及技术支撑机构。

在技术探索领域，海峡信息成立了“两大实验室”和“一中心”，在过去的二十多年里，一直专注于网络安全产品与服务领域。以创新研发和实战攻防为核心，致力于探索网络安全的最新前沿方向。

在科研成果方面，累计获得了福建省、市科学技术进步奖8项；发明专利授权10项；拥有软件著作权100多项。海峡信息独立承担的福建省高新技术重点项目、火炬计划项目及福建省重大招标项目。所有产品均以创新研发和实战攻防为核心，构建了一个基于主动防御、动态防御、精准防护、整体防护的综合防控体系，广泛应用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域。

网址：<https://www.si.net.cn>

电话：0591-87303711

地址：福建省福州市鼓楼区北二环中路61号2号楼

产品名称：黑盾综合日志审计分析系统

产品概述

黑盾综合日志审计分析系统实时不间断地采集汇聚企业中所有设备和业务系统的日志信息，协助用户进行安全分析及合规审计，及时有效的发现异常安全事件及审计违规事件。

产品采用B/S架构操作方式，分为安全管理对象层、采集层、分析处理层、业务功能层以及综合展现层。1、安全管理对象：面向各种安全风险进行采集和汇总，安全对象涵盖了人员、网络、安全设施、系统、终端、应用等。2、采集层：采集各种设备的事件日志，标准化为统一的格式，然后进行过滤、归并、预处理，作为大数据分析的前提和基础。3、分析处理层：系统通过审计分析引擎、关联分析引擎、统计分析引擎对海量日志进行挖掘分析，找到潜在的安全风险，并且形成事件结果传递给业务功能层。4、业务功能层：业务功能层实现对企业信息安全业务的支撑。在此基础上，通过分析事件与资产的相互关系，产生告警及报表。与此同时，业务功能层提供日志管理、资产管理、报表管理、采集管理、事件分析和审计管理，分别支撑用户的相

关业务功能。5、综合展现层：综合展现层是综合日志审计分析系统的展示层。该层通过个人工作台和安全概览，将整个系统收集、分析、管理的安全事件、告警概况等信息多维度的展现。

功能特点

系统包含日志采集、日志管理、事件告警、资产管理、审计管理、报表管理、系统管理等7个核心功能。基于强大的采集引擎实时采集不同厂商不同种类的日志，并且标准化为统一格式，再结合关联分析技术、审计分析模型、资产管理模块等形成对应的安全审计事件，用户可以进行查询、分析和判断。同时系统配备了全球IP归属及地理位置信息数据，为安全事件的分析、溯源提供了有力支撑。1. 全面的日志处理能力：支持异构海量的日志源接入，通过日志标准化技术智能的进行数据整合，支持上百种主流设备日志接入以及特殊设备定制接入。结合大数据技术、并发内存处理机制、高性能硬件设备能够提供海量日志处理能力、检索能力和存储能力，支持《中华人民共和国网络安全法》留存6个月日志的规定。2. 强大的安全防护能力：内置了准确有效的安全分析模型，并且通过大数据关联分析技术实时分析海量日志，精准挖掘潜在威胁风险，轻松溯源根本原因。3. 高效的业务运营能力：相比于在运维人员不同设备之间来回跳转查看日志，统一控制平台为运维人员不仅解决了设备分散、信息分析的问题，同时还提供系统分析能力辅助运维人员做出决策判断。结合资产管理模块、报表管理模块、告警监控模块、系统管理模块，为日常运维工作提供可视化、便捷的工具，提高运维人员的工作效率。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01136-A

★有效期：2024年8月9日至2026年8月9日

所属品牌：黑盾

发布时间：2020年5月28日

产品适用领域：适用于智慧政务、医疗、教育、金融、部队、交通、水利等关键领域

产品照片：



产品咨询邮箱：chenxf@heidun.net



产品咨询二维码

福建中信网安信息科技有限公司

福建中信网安信息科技有限公司以数据安全守护者为使命，致力于网络与数据安全领域，是一家集研发、生产、销售和服务于一体的高新技术企业。

中信网安在国内首家提出基于时空网格技术的“云、网、端、数”多维度动态安全监管技术体系，公司依托领先的技术研发与创新能力，先后荣获国家级“专精特新”小巨人企业、福建省新型研发机构、福建省产业领军团队、福建省科技小巨人领军企业、福建省企业技术中心等多项荣誉，服务用户数量超过 3000 家，并在第 44 届世界遗产大会、世界航海装备大会、历届数字中国建设峰会等大型活动的安保实践中勇担重任，以专业的技术、可靠的服务成为客户心中最信赖的网络与数据安全领军企业。

网址: <https://www.cicisp.com/>

电话: 0591-87895020

地址: 福建省福州市晋安区鼓山镇福光路 318 号 2 号楼 8 层

产品名称：华安星安全事件统一管理系统

产品概述

华安星安全事件统一管理系统为安全事件的分析、溯源提供了有力支撑，进行全生命周期日志管理，还能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台，可 7X24 小时监测安全设备、路由器、交换机、服务器等设备的核心参数，可以帮助网络管理人员实时了解网络的连接情况、配置情况和运行情况。

功能特点

◎集中化的日志综合审计

系统提供强大的日志综合审计功能，为不同层级的用户提供了多视角、多层次的审计视图。系统首先为用户提供了全局监视仪表盘，可以在一个屏幕中看到不同设备类型、不同安全区域的实时日志流曲线、统计图，以及网络整体运行态势、待处理告警信息等。用户可以自定义仪表盘，按需设计仪表盘显示的内容和布局，可以为不同角色的用户建立不同维度的仪表盘。系统提供了统计视图，审计员可以根据内置或者自定义的统计策略，从日志的多个维度实时进行安全事件统计分析，并以柱图、饼图、堆积图等形式进行可视化的展示。审计员可以查看一段时间内的主机流量排行、主机登录失败次数排行、活跃病毒排行、网络设备故障排行、最多访问用户排行等。

◎全面的智能收集功能

不断的连接检查和完整性检查以及可自定义的缓存功能，可确保平台接收到所有数据，并对传输链的各个环节进行监控；可配置过滤和聚合功能可以消除无关数据，并且合并重复的设备日志，强大的数据压缩功能可节省昂贵的带宽。

◎标准化日志

各种安全事件日志（攻击、入侵、异常）、各种行为事件日志（内控、违规）、各种弱点扫描日志（弱点、漏洞）、各种状态监控日志（可用性、性能、状态）、安全视角的事件描述：事件目标对象归类、事件行为归类、事件特征归类、事件结果归类、攻击分类、检测设备归类。

◎创新的日志解析能力

解析规则激活，仅当接收到对应的日志后，规则才会被激活，同时支持未识别日志水印处理，采用多级解析功能和动态规划算法，实现灵活的未解析日志事件处理，同时支持多种解析方法（如正则表达式、分隔符、MIB 信息映射配置等）；日志解析性能与接入的日志设备数量无关。

◎先进关联算法

系统的关联分析引擎采用实时流分析 + 全量数据关联分析的设计，同时保证了关联分析的实时性和超长的时间范围覆盖度，采用实时流分析 + 全量数据关联分析的设计无论在分析速度、分析维度、时间跨度、灵活性、IO 抗压能力方面都有巨大的优势。

◎可维护性及可拓展性

系统具有对自身的维护配置功能，如：系统参数设置、系统日志管理等。硬件系统采用模块结构，保证系统内存、CPU 及储存容量的扩展；硬件配置的升级不会引起软件的修改和开发；每个组件都可以横向扩展，通过增加设备满足业务需求。

◎灵活的部署方式

系统采用旁路方式部署，在不改变网络结构的情况下，实现对信息系统产生的事件进行统一的管理和存储。

技术指标

◎日志采集

用户通过指定需要采集的目标、相关采集参数（Syslog 等被动方式无需指定）相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。

◎日志解析

支持多种解析方法，如正则表达式等，将代码级别的日志解析为通俗易懂，且按照一定字段规则展示的日志，更方便于用户通过解析后的日志进行事件排查和追溯。

◎日志集中存储

各种安全事件日志（攻击、入侵、异常）、各种行为事件日志（内控、违规）安全视角的事件描述：归类后进行统一的存储。

◎日志分析展示

通过关联策略的建立，系统不仅支持以预定义规则的方式进行关联，还支持基于模式发现方式的关联；系统支持短时间内的序列关联等。从日志的多个维度实时进行安全事件统计分析，并以柱图、饼图、堆积图等形式进行可视化的展示。审计员可以查看一段时间内的主机流量排行、主机登录失败次数排行、最多访问用户排行等等。

◎安全事件收集和识别

支持通过标准协议（syslog）收集防火墙、IDS、IPS 等安全产品的日志，并基于解析规则、分析规则对日志进行分析处理，形成格式统一的安全事件记录。

◎安全事件告警

支持设置告警规则，对发现的安全事件进行告警，主动通知管理员。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS012-609

★有效期：2023 年 12 月 26 日至 2028 年 12 月 25 日

所属品牌：华安星

发布时间：2018 年 8 月

产品适用领域：能源、政务、医疗

产品照片：



产品咨询邮箱：zxwa@cicisp.com



产品咨询二维码

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

作为行业领导者，安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

2020 年 11 月 23 日，安恒信息正式成为 2022 年杭州第 19 届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

网址：<https://www.dbappsecurity.com.cn/>

电话：0571-28860999

地址：杭州市滨江区联慧街 188 号安恒大厦

产品名称：明御综合日志审计分析平台

产品概述

明御®综合日志审计分析平台（简称 DAS-Logger）作为信息系统的综合性管理平台，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营安全；明御®综合日志审计平台通过基于国际标准化的关联分析引擎，为客户提供全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，为客户提供真正可信赖的事件追责依据和业务运行的深度安全。同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，协助用户全面审计信息系统整体安全状况。

明御®综合日志审计分析平台旨在实现网络资产安全状况的统一管理，使企业的利益受损风险降低，广泛适用于政府、金融、运营商、公安、电力能源、税务、工商、社保、交通、卫生、教育、电子商务及各企事业单位等。

功能特点

◎日志收集能力

支持 syslog、agent、ftp、tcp、snmp trap、kafka、HTTP 等方式对市面上几乎所有的网络安全设备、交换设备、路由设备、操作系统、应用系统、数据库等资产所产生的日志信息进行

收集。

◎日志解析能力

内置的 5000+ 解析规则，对不同设备不同格式的日志进行细粒度解析，解析维度多达 200+，确保所接收的所有日志统一标准化处理。

◎关联分析能力

内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为 6 大类 50+ 子类的安全分析场景，基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等维度建立安全评估模型，提供全维度、跨设备、细粒度的关联分析，深度发现潜在安全事件。

◎事件检索能力

拥有极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果，查询条件多达 200+ 且可灵活组合查询，可帮助客户快速查找问题根源。

◎审计规则扩展能力

内置基础审计、Windows 审计、Linux 审计、PCI、SOX、ISO27001、WEB 安全等解决方案包，包含攻击威胁报表、等保合规性报表、各种审计报告及报表等 1000+ 种，为客户提供全面的审计视角。

◎性能监控能力

支持对多种操作系统、数据库以及应用程序进行性能监控，通过设置性能参数阈值，超过阈值将会产生告警并可通过邮件、短信等方式进行发送，第一时间通知相关负责人，提高设备预警能力。

◎对接能力

具备丰富的扩展接口（查询接口、视图接口、统计接口、告警接口）、日志转发接口以及大数据平台、态势感知平台对接接口，支持自定义各种事件转发和事件告警，拥有强大而灵活的对接能力，可为上层多种应用提供丰富的数据。

技术指标

◎功能指标

内置的 5000+ 解析规则内置基础审计、Windows 审计、Linux 审计、PCI、SOX、ISO27001、WEB 安全等解决方案包，包含攻击威胁报表、等保合规性报表、各种审计报告及报表等 1000+ 种，为客户提供全面的审计视角支持 syslog、agent、ftp、tcp、snmp trap、kafka、HTTP 等方式对市面上几乎所有的网络安全设备可支持 sm3，sm4 等国密算法对于日志的加解密

◎性能指标

每秒处理日志 30000 条 / 秒；

秒级查询亿级数据；

资产纳管数量 4000 个。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS012-253

★有效期：2023 年 7 月 1 日至 2028 年 6 月 30 日

所属品牌：明御

发布时间：2023 年 7 月 1 日

产品适用领域：政府、医疗、公安、运营商、企业、军工、教育、能源、金融

产品照片：



产品咨询邮箱：beric.liu@dbappsecurity.com.cn

南京聚铭网络科技有限公司

聚铭网络是由腾讯、国家中小企业发展子基金、江苏高投毅达宁海创业投资基金等投资的国内领先的安全运营商。

公司先后荣获了“高新技术企业”、“江苏省专精特新企业”、“江苏省规划布局内重点软件企业”、“江苏省软件企业技术中心认定企业”、“南京市工程技术研究中心认定企业”、“双软企业”、“创新型企业家培育企业”、“创业南京高层次创业人才引进企业”、“国家信息安全漏洞库CNNVD技术支撑单位”、“数据安全10强企业”等荣誉，公司专注于网络安全智能分析和检测，提供全面的信息安全防护，为达成“让安全更简单”的使命而不懈努力。

公司每年投入大量的科研经费用于产品研发和人才培养引进，先成立了“聚铭安全攻防实验室”，后又与南京大学联合成立了“数据科学联合实验室”，两大实验室用于网络安全前沿技术的预研。目前公司产品荣获了江苏省软件产品金慧奖、江苏省重点推广应用新技术新产品、南京市新兴产业重点推广应用新产品等荣誉。

凭借先进的技术和优质的服务，目前公司产品已服务教育、医疗、政府、电信、能源、金融等行业超10000家政企客户，云端托管客户超6500家。公司在北京、南京成立了双总部中心，同时在各地设有分支机构，业务覆盖全国31个省市及香港地区。

网址：<https://www.juminfo.com/>

电话：400-1158-400；025-52205520

南京总部：南京市雨花台区软件大道180号大数据产业基地7栋4层

产品名称：聚铭综合日志分析系统

产品概述

聚铭综合日志分析系统能够实时、不间断地采集并整合各类设备的日志信息，借助先进的关联分析与机器学习技术，助力用户从庞杂的日志数据中快速识别异常安全事件，全面满足合规审计、分析调查及数据留存等日志多场景使用需求。

功能特点

◎海量存储，万无一失

1、专利数据存储和抗抵赖技术，真正0丢失防篡改。

双保险存储：采用业内独家的原始日志与索引日志双重存储技术，确保数据安全无忧，彻底杜绝数据丢失的风险。

智能负载均衡：采用前置负载均衡技术，当设备发生故障时，系统能够自动将请求转发至

无故障设备，确保数据的稳定存储。

数据国密签名：采用国密算法签名技术，确保日志数据的完整性和抗抵赖性，防止任何篡改行为。

2、专利压缩存储技术，成本大幅削减 67%

采用数据压缩专利技术的日志审计，实际存储空间仅为本公司未使用该技术产品的三分之一，大幅节省了约 67% 的成本。

◎包罗万象，性能之巅

1、专利日志识别技术 + 聚铭长期标准化能力积累，全面支持所有厂商类型设备。

主流设备全面覆盖：适配千余种厂商设备，快速识别并智能化解析资产日志。

标准化免费更新：针对市面上新品牌、新产品，每半个月提供标准化更新下载。

用户按需 DIY：提供用户自定义的 API 接口策略，满足个性化需求。

AI 自学习识别：依托 AI 大模型能力，实现自动化日志采集与识别。

2、单机每秒 10W+EPS，超高性能处理。

轻松应对每秒超 10 万条日志的处理需求，支持无限动态扩容，确保在大规模日志场景下依然能够稳定高效运行。

◎多维分析，精准狙击

1、专利安全检测分析技术，从海量数据中精准挖掘隐匿威胁。

多源异构下，威胁无处遁形：融合机器学习方法与关系代数算子，对各类设备日志建立关系模型，实现深度威胁检测。

用户行为，了如指掌：通过相似度算法，对行为日志聚类形成用户分组，高效全面识别用户异常行为。

安全告警归并，精准降噪：通过日志字段的布局特征提取，计算与安全告警特征的相似度，实现安全告警归并。

实名认证，审计与溯源保障：针对 DHCP、NAT 等场景与实名认证系统联动，一旦发生威胁事件，可快速追溯至具体责任人。

2、AI 大模型赋能，运维省心省力。

日志智能解读，小白变专家：融合安全垂直领域的先进大模型技术，实现日志的一键解读，让复杂的数据变得简单易懂。

智能客服，随叫随到：聚铭 AI 助手随时待命，即时解答您的所有疑问，让运维工作更加得心应手。

◎更多守护能力

秒级检索查询：亿级 (TB) 原始日志查询耗时低于 1 秒。

智能降噪告警：从每天 10 亿条原始数据中最终精准告警约为 10 条，大幅减少误报。

灵活审计报表：具备丰富的合规模板，全面满足合规审计要求。

高效快捷交付：快速部署，1 天内零定制标准高效交付。

日志国产化版本：聚铭综合日志分析系统国产化版本，在性能、功能及成本效益方面均可满足信创环境下的日志管理和等保建设需求，实现“鱼”与“熊掌”兼得。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0304230295

★有效期：2023 年 2 月 17 日至 2025 年 2 月 17 日

所属品牌：聚铭网络

发布时间：2016 年 10 月 21 日

产品适用领域：政府、教育、医疗、金融、电信、能源

产品照片：



产品咨询二维码

产品咨询邮箱：yangping@juminfo.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟（CCIA）发布的 2021 年、2022 年、2023 年“中国网络安全产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神威胁检测平台

产品概述

奇安信网神威胁检测平台 QAXTIP 是奇安信集团面向企事业单位推出的一款以奇安信云端大数据为基础，通过奇安信威胁情报中心安全运营后，面向企业提供各类海量高价值热点威胁情报的安全产品，通过为大数据平台、各类网元设备提供机读消费及提供安全运营人读情报，提高威胁发现能力。本系统依托奇安信集团多年来积累的海量网络安全和互联网基础数据资源，提供经过安全运营后的威胁情报数据服务。本地存储数亿的海量热点库，通过本地 API 接口与多源情报汇聚能力，为安全大数据平台提供数据支撑，实现威胁发现、协助用户开展 APT 攻击、恶意软件、钓鱼网站等网络安全事件检测，评估网络安全事件整体危害，并提升追踪溯源攻击者的效率和成功率，通过安全运营提升企业整体安全能力。

功能特点

◎独家海量安全大数据资源

奇安信依靠强大的样本收集能力、国内领先的网络数据及 APT 发现能力，囊括数百家情报

源以及多个安全研究团队的 APT 情报，覆盖全球当前流行的勒索软件、ExploitKit 以及 APT 攻击事件、攻击团伙等各类独家海量安全大数据资源。

◎安全分析团队专业化体系化运营

奇安信威胁情报中心配备专业分析团队，具有丰富的情报分析经验、技能和完整的数据处理流程体系，通过数据收集、数据清洗、数据关联、验证、上下文和格式化的高精准数据处理与有效的分析整合，保证威胁情报数据的高质量、高时效性与高精度度。

◎类型丰富的情报能力输出

原始数据经过奇安信威胁情报中心商业情报加工处理流程体系形成多种情报数据。在情报消费阶段，可将威胁情报赋能到边界类设备、终端设备、安全服务和安全运营，并为服务和运维提供安全保障。同时可共享给客户、政府机构、安全服务商和安全厂家。

◎情报联动发现企业内潜在威胁

通过将已有安全设备与威胁情报进行联动，用情报数据激活用户已有数据，让海量历史数据重新活跃起来，形成有效数据。通过联动监测类和态势感知类设备，做到发现威胁、感知威胁、分析威胁和处理威胁，真正为用户发现潜在未知威胁。

◎海量高质量数据支撑研判决策与响应

基于先进的机器学习技术、自动化多层次关联，深度挖掘信息，为用户提供高效精准的情报响应能力输出，对指定实体进行充分的关联与富化。准确、丰富的上下文数据能够支撑用户进行攻击定性分析、恶意家族 / 攻击团伙溯源、误报排查等各类分析工作，从而为处置响应的决策制定提供关键证据与指导。

◎实战化场景助力攻防检测

将威胁情报应用于日志威胁发现、恶意样本鉴定、恶意邮件检测等综合实战化场景，实现用户业务的深度结合，挖掘出企业实际面临的安全风险与遭受的网络攻击，从而制定针对性的防御手段，有效排除风险，遏制网络攻击的蔓延。

◎内生情报体系构建企业私有威胁情报中心

将奇安信云端情报数据在用户本地下沉，并实现情报源的整合管理；基于多途径的情报共享，赋能用户侧第三方设备；通过与用户自有身份认证系统对接，为安全分析师提供更便捷的事件响应、威胁研判、追踪溯源方式；提供全面的数据运营分析能力，让用户了解企业的安全运营状况。从而构建一体化内生情报管理体系，帮助企业建立自己的威胁情报中心。

技术指标

◎威胁研判：情报关联分析与定性分析，支撑精准响应；

◎多源聚合：多源情报汇聚管理与综合评分，打造企业私有威胁情报中心；

◎情报共享：通过高性能查询 API 接口与标准 STIX 情报格式，为第三方设备提供情报赋能；

◎漏洞情报：经专家分析师人工研判与运营，提供漏洞优先级排序与切实可行的解决

方案；

◎ APT 档案库：以可视化大屏呈现全球攻击组织，提供 APT 组织情报与综合画像；

◎安全通告：全面多维度安全热点资讯，通过威胁分析与风险通告及时了解漏洞与攻击事件风险态势；

◎日志检测：各类安全设备日志接入与威胁模型检测，挖掘攻击事件线索；

◎样本深度鉴定：动静态检测结合的高对抗情报沙箱，精确识别恶意软件；

◎邮件检测：为企业提供本地邮件批量自动化检测服务，精准快速鉴别钓鱼邮件、伪造邮件及附件威胁；

◎数据运营分析：可视化多维度运营报表，为企业安全决策制定提供数据支撑。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息质量监督检验中心

★证书编号：24SS01032-A

★有效期：2024 年 7 月 19 日至 2026 年 7 月 19 日

所属品牌：奇安信网神

发布时间：2018 年

产品适用领域：全行业

产品照片：



产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年启明星辰集团在深圳 A 股中小板上市（股票代码：002439）。经过二十余年的积累与沉淀，启明星辰集团已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，是网络安全产业中主力经典产业板块的龙头企业、新兴前沿产业板块的引领企业以及可持续健康业务模式和健康产业生态的支柱企业。

启明星辰集团自成立起，经历了不断跨越的自我升华，迈入“I”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence）。依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领产业未来最具吸引力的数据安全、工业数字化安全、新算力安全等板块高增长，致力于打造自主可控的安全生态体系，为用户提供专业的安全服务。

集团总部位于北京市中关村软件园启明星辰大厦，DT（数据时代）总部位于杭州高新区（滨江），全国云安全总部位于苏州高新区，在全国各省、市、自治区设立了分支机构，拥有覆盖全国的渠道和服务体系，为用户提供网络安全产品、服务和解决方案。

网址：<https://www.venustech.com.cn>

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：泰合信息安全运营中心系统 - 日志审计

产品概述

泰合信息安全运营中心系统 - 日志审计是基于十多年信息安全积累的基础之上，推出的海量日志全生命周期管理日志审计产品。

能够通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

采用新一代的基于超微内核的技术架构，融合多种信息安全技术和管理理念，充分实现组织、管理、技术三个体系的合理调配，帮助用户进行基于日志的综合审计和日志全生命周期管理，从而最大化的保障网络、主机和应用系统安全机制的有效性。

具有广泛的应用范围和客户群，在政府、电信、金融、电力、公安、军工、企业等行业均有成功的应用。

功能特点

◎日志多维度高适应采集

泰合信息安全运营中心系统 - 日志审计综合采用多种技术手段,充分适应用户实际网络环境的运行情况,采集用户网络中分散在各个位置的各种厂商、各种类型的海量日志。为了最大程度地采集各种厂商、各种类型的日志信息,泰合信息安全运营中心系统 - 日志审计没有强求审计数据源必须具备什么日志协议,而是支持通过多种协议方式采集日志。采集不仅包括主动还包括被动方式,这些协议包括并不仅限于: Syslog、SNMP Trap、FTP、OPSEC LEA、NETBIOS、ODBC、WMI、Shell 脚本、HTTP / HTTPS 等等,同时还支持大数据组件 ES、HDFS、Kafka、Mango 等日志任务采集。

◎智能范式化解析

支持日志智能范式化功能,将新设备原始日志输入对话框,系统能自动识别原始日志,并匹配映射系统通用标准字段实现原始日志解析,且通过备用字段进行扩展字段的调整;同时还可以进行解析字段的编辑和调整,确保日志解析达到想要的细粒度和效果。

◎基于字段资源碰撞的关联分析技术

内置了多类型的审计场景,能通过可视化的规则编辑器进行对应字段资源的引用,无需限定关联维度,同时加入统计分析计数进行综合判定,实现规则的科学合理的设定和优化改善等,同时可以实现规则的扩展。以此实现审计的最终目的,实现威胁场景的监测。

◎自动化告警处置

支持对告警事件进行实时管理,对告警事件进行多维度分类管理,包括事件的通用分类和按攻击视角进行步骤分类等,同时可以自定义分组类别实现告警事件监控管理。

支持对告警事件进行状态管理,包括未处理、未确认和已确认等状态,可以对告警事件状态进行跟踪和编辑,同时支持告警事件定位和追溯,实现告警事件溯源分析。

技术指标

◎日志采集

支持 Lotus Domino、Check Point、VMWare 的日志采集任务;

支持定制任务进行日志数据采集扩展,包括文本格式、目录下文本和数据库格式日志采集,支持编辑正则表达式和 SQL 语句进行日志采集,支持设置自定义任务时间;

◎日志范式化

支持为未解析日志提供一种简洁在线编辑解析文件视图,做到精准解析;

支持对范式化字段进行枚举,范式化字段至少包括事件接收时间、用户名称、源地址、源端口、操作、目的地址、目的端口、对象、结果、持续时间、响应、归并条目、事件名称、事件内容摘要、事件分类、等级、原始等级、原始类型、产生时间、网络协议、网络应用协议、设备地址、设备名称、设备类型、程序名称、原始消息、厂商、产品、解析关联等 65 个字段,字段名称支持自定义;

◎日志查询

支持交互式事件分析模式,支持历史查询记录浏览和快捷查询;

◎日志存储转发

支持日志加密压缩传输,支持加密压缩方式转发,加密方式支持 SM4 国密算法,支持定时转发;

◎日志统计分析

支持日志源统计功能,可以综合展示采集日志总数、日志范式化成功率、24 小时日志量、接入设备数量、日志接收速率等;

◎安全场景分析

支持基于规则的关联分析引擎,能够提供逻辑关联、统计关联的关联分析能力;关联规则支持规则嵌套和引用,通过多规则联合,可精确识别复杂安全事件和场景;

支持安全监测场景,至少包含恶意代码、可疑控制、入侵利用、违规行为、嗅探行为、关联审计等;

◎资产管理

支持手动编辑、导入方式录入资产数据,支持资产标签设置,能够根据收到事件的设备地址自动识别新的资产并自动添加到资产库中;

◎告警管理

支持关联分析的结果进行告警重定义功能,能够对规则触发的告警时间和关联后事件的任意字段进行重定义,包括修订告警级别和告警类型等;

◎报表管理

系统内置等保报表、PCI 合规报表、SOX 合规报表、ISO27001 报表等合规性报表;

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称:公安部计算机信息系统安全产品质量监督检验中心

★证书编号:24SS00827-A

★有效期:2024 年 06 月 14 日至 2026 年 06 月 14 日

所属品牌:启明星辰/网御星云

发布时间:2014 年

产品适用领域:政府、企业、能源、运营商、教育、医疗、公安等

产品照片:



产品咨询二维码

产品咨询邮箱: support@venustech.com.cn

深信服科技股份有限公司

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT 基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超 9000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

从 2013 年开始，深信服就全情投入信创产业发展，坚持“双模拉齐，先进升级”，获得了包括“信创工委卓越贡献成员单位”在内的多项权威认可。

一直以来，深信服十分重视研发和创新。持续将 20% 年收入投入研发，并在深圳、北京、长沙、南京和成都设立 5 大研发中心，研发人员比例约为 40%，坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万用户正在使用深信服的产品。根据 IDC 数据，深信服 VPN、全网行为管理、下一代防火墙、应用交付和桌面云均为中国市占率第一，超融合、EDR 也均为中国市占率前三。

网址：www.sangfor.com.cn

电话：400-806-6868

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

产品名称：深信服日志分析管理系统

产品概述

深信服日志分析管理系统针对信息安全事件的“可发现”、“可处理”、“可审计”、“可度量”四大目标进行规划和设计，提供了众多基于日志分析功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控及安全告警等，能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

企业大多会部署各种安全厂商的设备，每种设备均会产生不同格式的日志；日志分散在系统内各处，缺乏统一的日志保存策略，也缺乏集中的、统一的审计平台；每日可达千万级的事件日志量，且同一设备重复信息过多，检索困难，更无法对多种来源的海量日志进行关联分析。《网络安全法》要求按照规定留存相关的网络日志不少于六个月；《网络安全等级保护 2.0 国家标准》规定业务流程的合规管理、等保 2 级以上系统必须有日志留存；这些都明确提出了对于日志审计的要求。深信服日志分析管理系统能够实时不间断地采集汇聚企业中不同厂商不同种类的安全设备、网络设备、主机、操作系统、用户业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及审计违规。

功能特点

◎**数据采集**：采集是深信服日志分析管理系统的重要功能模块，它承载了日志或事件采集标准化、过滤、归并功能。采集管理是系统进行分析的第一步，用户通过指定需要采集的目标、相关采集参数、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。

◎**数据范式化**：接入方式包括被动接收（syslog、winlogbeat、snmp trap）、主动拉取（wmi、JDBC、Webservice、FTP、SFTP）两大类不同的系统或设备所产生的日志格式是不尽相同的，这给分析和统计带了巨大的麻烦，所以在深信服日志分析管理系统中内置了众多的标准化脚本以处理这种情形；即便对于某些特殊的设备，如某个系统的新型号，您没有发现相关的解析脚本，深信服日志分析管理系统也提供了相应的定制方法以解决这些问题。

◎**数据转发**：支持将归一化后的数据通过 syslog 协议转发到第三方系统中，包括对接安全感知平台。当前产品的优势之一：是支持无缝对接安全感知平台，且感知平台可对接入的数据进行分析。

◎**审计策略**：审计策略是指在海量日志中提取出用户关心的那部分日志，将原始日志按照一定的内容解析成用户可理解事件。例如 windows 主机会产生大量日志，用户只关注登录日志，那么可以配置一条审计策略将其过滤解析出来。当前系统中内置了针对 windows 主机、linux 主机、数据库的 150+ 审计策略。

◎**事件分析**：深信服日志分析管理系统的事件分析功能是系统中的核心功能之一；其中关联分析策略主要侧重于各类日志之间可能存在的逻辑关联关系。匹配上规则后，会产生对应的事件，在事件页面展示。深信服日志分析管理系统不仅支持以预定义规则的方式进行事件关联，还支持基于状态、时序、归并等发现方式的关联。

对于事件关联分析所产生的结果将在关联事件中呈现，如果符合关联策略，将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。

◎**审计管理**：深信服日志分析管理系统的审计管理功能是系统的核心功能之一，其中审计策略主要侧重于发现日志中相关要素是否和预定的策略相符，如时间、地点、人员、方式等；日志分析管理系统支持以预定义规则的方式进行审计；支持基于模式发现方式的关联。对于根据审计策略所产生的审计违规结果，系统将在审计事件中呈现给用户，如果符合定制的审计策略，也会在实时监控模块以告警形式展现给用户。

◎**告警监控**：所谓告警是指用户特别需要关注的安全问题，这些问题来源于事件分析、审计分析的结果。告警监控中包括了如下功能：用户可以通过定义过滤器以监控需要特别关注的告警信息，用户也可以根据个人需求，设置告警的提示音、界面显示方式等；

技术指标

◎全面的采集能力

数据采集是日志审计的基础功能，当前主要实现的有：

支持 200+ 款设备日志归一化。

支持 30+ 款设备日志深度分析匹配规则产生安全事件。

采用 Logstash 数据采集框架采集数据，大大提升了接入性能。

通过主被动结合的手段，实时地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息进行集中化存储、备份、查询、审计、告警、响应，出具相关的合规报表报告，实现全生命周期的日志管理。SIP-Logger 主要通过 syslog、ftp、sftp、jdbc、webservice 等方式收集第三方日志，包括：网络设备（路由器、交换机等）；安全设备（防火墙、WAF、IDS、IPS 等）；操作系统（windows、linux 各系列）；中间件（apache、FTP 服务器、邮件服务器、IIS、DNS 等）；数据库（Mysql、Sql server、Oracle 等）共 800+ 款设备的日志。

◎强大的检索查询

亿级（TB）原始日志查询耗时低于 1 秒；支持统一日志检索，包括精确匹配和模糊匹配等；支持多条件组合查询，提供详细的帮助文档。

◎丰富的合规报表

支持导出 5 种类型的报表：主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表。

◎灵活的部署方式

支持单机、分布式、集群采集。

◎简便易用的界面风格

系统通过提供入门向导、个人工作台、任务通知、快捷菜单等方式，为用户提供了简单易用的界面，即使是初次使用深信服日志分析管理系统，也完全能在较短的时间内掌握。

◎灵活通用的系统设计

深信服日志分析管理系统具有极大的灵活性，主要体现在如下几个方面：

可配置的安全概览等系统功能菜单；支持用户自定义的事件关联策略、审计策略；灵活的日志标准化解析脚本；具有优秀扩展性的第三方接口，如告警外发 Syslog 与第三方平台对接。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS012-429

★有效期：2023 年 9 月 7 日至 2028 年 9 月 6 日

所属品牌：深信服科技股份有限公司

发布时间：2020 年

产品适用领域：政府、企业、医疗、教育等

产品照片：



产品咨询二维码

产品咨询邮箱：market@sangfor.com.cn

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<http://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼天融信科技集团

产品名称：天融信工控日志收集与分析系统

产品概述

天融信工控日志收集与分析系统是一款面向工业应用环境开发的日志审计类产品，系统采用主被动相结合的技术手段，通过Syslog、SNMP Trap、NetFlow、Telnet/SSH、WMI、FTP/SFTP/SCP、JDBC、文件等多种方式，对工业控制系统网络中不同厂家的安全设备、网络设备、工业主机、操作系统、上位组态软件、数据库系统等资产信息进行日志采集与分析，系统满足《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》与《工业控制系统信息安全防护指南》中对工业控制系统网络安全对日志收集、存储、分析的要求，为工业企业安全生产提供数据支撑。

功能特点

◎海量数据采集能力

系统支持至少26类350种安全设备、网络设备、服务器、工控应用系统日志等日志源进行采集，涵盖主流的安全厂商、工控厂商。采集具有多种方式，支持Syslog、Snmpttrap、Netflow、

WMI、FTP、SFTP、SCP、JDBC、文件等形式。通过日志进行采集、规范化管理、深度分析和可视化展示。

◎高效数据处理能力

系统采用大数据处理模式，对采集到的日志进行数据进行日志归一化处理、支持原始日志和归一化后的日志数据存储与查询，储存压缩比可达 10:1，查询速度可达到百亿级日志查询秒级查询。直观展现安全事件的发生、访问源、危险等级以及影响范围的分别情况。

◎综合统计分析能力

系统支持管理员用不同角度对安全信息进行可视化分析，系统支持结果分析、日志挖掘、时间线、关系图、折线图、时序表、柱状图等形式，对流量分布情况、访问关系、端口访问关系、关联关系等进行分析，能够快速帮助客户发现安全事件源和目的，为事后溯源提供充足证据。

◎丰富可视呈现能力

系统内置丰富数据展示模式，基于全球地图、全国地图、逻辑拓扑图、IP 地址全球定位、饼状图、柱状图、曲线图、时间轴等，支持对日志查询结果快速自动分析，充分提升安全日志审计效率。同时支持将数据以 PDF、WORD、EXCEL、HTML 等方式不同格式进行导出。

◎合规检查必备利器

系统通过对全面日志的高速采集、异构格式归一化、以及高效压缩存储（6 个月以上）、快速查询、综合分析、可视化等技术满足 GB/T 22239-2019《信息安全技术信息系统安全等级保护基本要求》要求二级及以上系统需要进行“安全审计”的合规性需求。

技术指标

◎功能指标

支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据

支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统、工业防火墙、工控审计、工控漏扫、工控入侵、工控网闸、工控主机卫士等；等不少于 26 类 300 种日志对象的日志数据采集

支持单级部署和代理分布式部署采集日志

支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于 10s

数据存储能力：压缩加密存储，压缩比不低 10:1；日志存储不低于 10000 条/M

支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数

◎性能指标

天融信工控日志收集于分析系统日志源数量覆盖 100 个至 300 个，日志采集处理峰值覆盖 8000EPS 至 20000EPS。

产品安全认证或安全检测结果证明等

网络关键设备和网络安全专用产品安全认证证书 / 网络安全专用产品安全检测证书

★检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00129-A

★有效期：2024 年 01 月 26 日至 2026 年 01 月 26 日

所属品牌：北京天融信网络安全技术有限公司

发布时间：2022 年 2 月 14 日

产品适用领域：天融信工控日志收集与分析系统可广泛应用在轨道交通、电力、冶金、煤炭、石油化工、市政、烟草、智能制造、核电等行业。

产品照片：



产品咨询邮箱：feng_chong@topsec.com.cn



产品咨询二维码

产品名称：天融信日志收集与分析系统**产品概述**

天融信日志收集与分析系统，是基于非关系型数据存储系统的新一代海量日志管理系统。系统基于消息总线的分布式架构，采用主被动结合的技术手段，7*24 小时不间断采集网络中安全设备、网络设备、服务器资源和应用系统的日志，通过对日志的采集、处理、存储、备份、查询统计、合规报表以及关联分析，实现海量日志的全生命周期管理；

天融信日志收集与分析系统基于消息总线的分布式架构，采用非关系型数据存储技术，突破海量数据采集、存储、索引和运算的性能瓶颈，在有限资源占用情况下支撑海量数据高效处理，实现日志“收得全”、“查得快”、“存得下”等能力；

全面日志采集：多种类、多厂商日志高速采集，复杂日志格式化处理，解决设备繁多、分散、格式异构问题；

极致存储压缩：基于高效存储压缩，极大减少硬盘空间占用，应对大数据量场景下日志留存需求，符合相关政策法律规定；

百亿级数据即查即显：任意字符串组合检索，百亿级数据多条件交互式检索结果返回时间小于 10 秒，协助完成事件定位、溯源。

多维日志可视：内置多维数据在线分析模型，实时在线分析、展示，直观体现系统运行状况。

功能特点

◎设备类型及日志类型支持广泛

系统目前支持已支持 26 类 300 多种设备的信息采集，涵盖国内外主流厂商，系统利用数据采集引擎、数据处理引擎采用被动与主动采集技术相结合，通过包含但不限于 Syslog、SNMP Trap、NetFlow、Telnet/SSH、WMI、FTP/SFTP/SCP、JDBC、文件等标准协议从审计对象获取海量日志数据。

◎海量日志高效采集与处理

系统会对数据采集引擎采集到海量日志数据进行归一化、过滤、分类等处理，归一化、过滤、分类过程可根据需要配置不同的环节与流程，采集处理性能可达 30000EPS。同时将原始数据以及处理后的数据交给数据存储子系统进行原始数据以及归一化数据的压缩加密存储。压缩比为 10:1，确保原始数据不被篡改的同时极大提高了磁盘空间的利用率。

系统利用专用日志格式化描述语言多原始日志进行归一化处理，归一化描述语言支持热部署，无需重启系统即可应用。提供的归一化字段包含但不限于网络协议、网络应用协议、设备地址、设备名称、设备类型、接收时间、产生时间、日志持续时间、用户名称、目的地址、目的 MAC 地址、目的端口、源地址、源 MAC 地址、源端口、日志的事件名称、摘要、等级、原始等级、原始类型等。

◎交互式全文检索

系统采用基于自主研发的快速搜索引擎——TopQuerying，运用类似于 Google 的搜索技术，可以针对任意字符串集合进行数据检索，实现百亿级数据多条件交互式检索结果返回时间小于 10 秒。丰富的查询字段和专业定制的查询模板，让查询更简单、易用；支持查询结果下钻上卷，支持原始日志与归一化日志同屏显示。支持查询结果显示界面快捷统计。

◎数据多维度统计分析

系统提供 500 多种的统计主题，内置基于等保、ISO 27001、SOX 等合规性要求的分析场景。用户可以通过丰富的合规分析策略对全网的安全事件进行全方位、多视角、大跨度、细粒度的实时监测、分析、查询、调查、追溯，动态了解系统的合规情况。支持管理员从不同角度进行安全信息的可视化分析。统计报表支持按照排行、趋势和概要等进行展示，对于统计结果系统提供了表格及多种图形表现形式（饼图、柱状图、曲线图等），使管理员一目了然。

技术指标

◎系统性能

日志采集峰值：35000EPS；日志采集均值：20000EPS；

支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于 10s；

数据存储能力：压缩加密存储，压缩比不低 10:1；日志存储不低于 10000 条 /M；

◎数据采集处理

支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据；

支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者；

支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出；

支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；

支持独立展示每个被采集源最近 24 小时的日志数量趋势，便于掌握设备的安全事件情况；

支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态；

支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；

支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志；

◎数据存储

支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储；

支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；

◎数据查询

支持首页以全国地图、全球地图展示最近 24 小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息；

支持等于、不等于、大于、小于、正则表达式等查询条件；支持多条件组合查询；

支持对常用查询条件进行保存，可重复使用；支持查询条件缓存，通过快速调用系统右侧隐藏栏中缓存的查询条件，提升常用条件的检索速度；

支持为不同类型日志设置不同的查询条件和显示条件；

支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息；

支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源 IP 和目的 IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果；

支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析；

◎统计分析

系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；

支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警；

系统内置多种维度的数据在线分析模型，在数据查询结果界面直接对查询结果数据进行多维度在线数据分析，分析结果实时展示，分析模型包括但不限于树图、散点图、关系图、折线图、时序图、柱状图等。

网络安全专用产品安全认证或安全检测结果证明

(1) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CSO36-512

★有效期：2023年10月23日至2028年10月22日

(2) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CSO36-510

★有效期：2023年10月23日至2028年10月22日

(3) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CSO12-254

★有效期：2023年1月9日至2028年1月8日

(4) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CSO36-513

★有效期：2023年10月23日至2028年10月22日

所属品牌：天融信

发布时间：2003 年 10 月 12 日

产品适用领域：天融信日志收集与分析系统适用于政府、金融、电信、电力、石油、交通、航空航天、教育、医疗、企业等各行业。

产品照片：



天融信日志收集与分析系统 V3



天融信日志收集与分析系统 TA-LOG V3

证书编号：CCRC-2023-CSO36-512

证书编号：CCRC-2023-CSO12-254

产品咨询邮箱：feng_chong@topsec.com.cn



产品咨询二维码

亚信安全科技股份有限公司

亚信安全是中国网络安全软件领域的领跑者，是业内“懂网、懂云”的网络安全公司。承继亚信 30 年互联网建设经验，肩负守护互联网之使命，亚信安全于 2015 年正式启航，目前已成为建设中国网络安全的重要力量。不负使命，成功执行建党 100 周年、历年两会等国家重要网络安全保障任务 30 余次。

依托互联网建设能力，让亚信安全具备强大的“懂网”业务能力与资源优势；深耕网络安全高精技术，让亚信安全拥有优异的“懂云”技术基因。亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理及 5G 安全等领域突破核心技术，用实力筑牢云、网、边、端之安全防线。

亚信安全在中国网络安全电信行业细分市场份额占比第一，连续五年蝉联身份安全中国市场份额第一，终端安全中国市场份额占比第二，在威胁情报、EDR、XDR 等细分技术领域均居于领导者象限，是中国网络安全企业 10 强。

网址：www.asiainfo-sec.com

电话：400-820-8876

地址：江苏省南京市雨花台区花神大道 98 号东久创新中心 1 号楼、2 号楼 3 楼

产品名称：亚信安全日志审计协同服务系统 AIRDS V2.0

产品概述

亚信安全日志审计协同服务系统是一款高性能的日志采集、处理、关联分析和并行审计监控的安全产品。它能够采集绝大多数的安全设备、网络设备、服务器以及应用系统的日志，支持代理和无代理的采集方式，能够自动识别常见的日志格式，同时内置上百种日志解析模型，支持自定义数据识别能力，具备毫秒级的数据检索能力。

系统通过内置的审计策略实现基础性审计与合规性审计。基础审计涵盖近期事件、登录事件、攻击威胁事件、配置变更事件、web 相关事件。合规性审计包括等级保护合规、SOX 合规、ISO27001 合规、PCI 合规。并根据审计结果生成对应的安全告警。

通过内置的高级检索查询语法对数据进行实时分析，实现基于标准字段的全文检索功能。

功能特点

◎多元设备日志接入

提供对安全设备、网络设备、服务器以及应用系统所生成的日志进行采集的能力，AIRDS 采集支持常用的采集协议与采集方式：TCP/UDP 协议、文件采集、目录采集、数据库采集、

FTP/SFTP 协议、SSH 指令采集、WebService 采集、SNMP 协议采集、API 接口采集等，同时还能提供定制化的采集满足个性的采集需求。

◎异构数据泛化解析

提供数据流式处理框架 DataProces，基于该框架可以对数据进行各种逻辑处理。系统内置了丰富的数据解析规则，所有数据都会进行规则的匹配，匹配到规则的数据会解析成通用的标准事件；

◎海量数据高速检索

采集解析之后的数据，以结构化的形式分布式存储在系统数据库中，对外提供数据查询与统计服务，从而实现海量数据检索与挖掘。

◎设备日志集中审计

提供独立的审计工作台，具备完整的设备日志审计能力。涵盖基础行为审计和合规性审计两大部分内容。实现对审计规则的定义，并根据规则生成对应的日志审计告警事件。审计规则的定义包含用户账户风险、服务器 / 系统风险、Web 服务器风险、数据库风险、文件完整性风险、潜在 windows 风险和潜在 Unix 风险。针对审计结果中的异常情况及时生成告警。

技术指标

◎大规模数据处理性能

采用的高性能采集、数据处理和搜索引擎，集成亚信安全多年积累成果，基于先进可自适应的技术架构，克服海量数据的存储、索引和运算的瓶颈。采用基于大数据的处理架构和存储框架，保障系统数据处理的性能与实效性。

◎智能的数据格式识别

采集覆盖了绝大多数的采集协议和采集方式，支持一键接入模式，也支持定制化采集模式；系统内置了上百种的日志类型的泛化解析模型，通过界面配置即可轻松完成特殊日志格式的识别。

◎多维的审计分析场景

内置了多种审计分析场景，涵盖基础行为审计和 SOX 合规、PCI 合规、ISO 合规等多项合规审计，满足不同用户的审计分析需求。

◎便捷的产品部署运维

采用高性能标准化硬件，支持一键部署方式，部署速度快，运行稳定可靠。

网络安全专用产品安全认证或安全检测结果证明

网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2024-CS036-768

★有效期：2024 年 5 月 10 日至 2029 年 5 月 9 日

所属品牌：亚信安全

发布时间：2022 年

产品适用领域：金融、企业、政府、电力、交通、医疗、运营商等

产品照片：



产品咨询二维码

产品咨询邮箱：sec-business@asiainfo-sec.com

浙江木链物联网科技有限公司

浙江木链物联网科技有限公司（简称：木链科技）受陈纯院士技术指导，成立于 2017 年，为工业互联网安全、工控网络安全代表企业。公司面向工业企业及关基单位提供安全合规整改、安全运营中心建设、网络安全实验室规划、安全业务创新及专业安全服务，并助力推动关键领域信息安全产品的高水平国产化替代。

目前公司已在军工、电力能源、石油石化、轨道交通、智能制造等重要领域部署产品、落地项目，包括某装备制造关基单位关基系统安全防护集成项目，中石油下属某储气库多维安全生产智慧化管控平台建设项目，核能行业某研究设计院网络安全靶场项目，核能行业燃料企业工控系统安全建设项目，大唐集团智慧电厂国产化替换升级采购项目等，多维度、多层次积极推动工业网络与信息安全发展和关键信息基础设施安全防护体系建设，为工业企业信息化数字化转型夯实安全基座。

“十四五”规划开局起步，数字化转型全面铺开推动网络安全加速发展。木链科技锚定网络强国、制造强国和数字中国建设目标，针对新技术下产生的工业新业态、新业务和新场景，为客户提供全面、有效、可持续的工业互联网安全建设方案。

网址：boolean.com.cn

电话：400-0571-950

地址：杭州市余杭区五常街道联创街 188 号贝达梦工场 C 座 10 楼

产品名称：BooleanGuard 日志审计与分析系统

产品概述

日志审计与分析系统支持日志全生命周期管理，支持配置不同种类日志的生命周期，支持全文检索，能够快速定位和发现事件发生的时间和原因，方便技术人员第一时间解决问题；满足等保和网络安全法对网络设备，安全设备日志进行集中收集和存储等合规性的要求；通过报表的形式直观自动输出日常安全日报、周报、月报，提高安全运维人员工作效率。通过设备、系统日志分析，有效实现安全日志和攻击的追本溯源，发现信息系统安全的薄弱环节，加强网络安全管理，提高网络安全等级和系统运行可靠性。

功能特点

◎海量日志集中管控：对全网网络环境中海量日志数据的集中收集和统一管理。消除了本地日志存储情况下可能被抹掉的危险，降低了日志分散存储的管理成本，提高了日志管理的可靠性。

◎**大数据技术高速检索**：基于大数据应用的高速检索引擎，通过匹配正则表达式、提取关键字等方式将非结构化的日志数据结构化，保证每次查询都是实时计算，并且在秒级以内实现响应。实现对海量日志的快速检索和精确匹配。

◎**可视化日志分析**：对日志数据进行统计分析的基础上生成丰富的报表，实现分析结果可视化，并且提供多种表格和图形表现形式（折线图、面积统计图），降低了管理人员对日志分析的难度。

◎**操作简洁易用**：用户交互体验度高，不需要用户掌握复杂的搜索语法，仅通过简单的搜索框和鼠标即可完成搜索查询。

◎**高度可扩展性**：日志审计与分析系统支持单点部署和集群部署，可以按照客户实际需求进行资源扩展，降低不必要的资源浪费。

技术指标

日志源授权 ≥ 100 （可扩）

日志处理能力 ≥ 4000 条/秒

动态缓存量 ≥ 1000 万

日志存储量 ≥ 10 亿

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230966

★有效期：2023 年 04 月 28 日至 2025 年 04 月 28 日

所属品牌：BoleanGuard®

发布时间：2021 年 03 月 13 日

产品适用领域：电力、钢铁、化工、水利、水务、交通运输、智能制造等。

产品照片：



产品咨询邮箱：info@bolean.com.cn



产品咨询二维码

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望日志审计分析系统

产品概述

远望日志安全分析系统是基于大数据技术的新一代日志收集和分析产品。是一个能够集中收集、管理、分析各类日志信息的日志处理平台，能够对全网海量的日志数据进行集中收集，实现日志的集中管理、实时监控、告警分析、快速检索等。既可以满足相关法律法规以及行业标准的合规性检查，又能切实的对产生的海量日志进行统一安全管理与深度分析。

功能特点

◎海量日志集中管理

可自动化地对海量数据进行采集和存储，实现对全网网络环境中海量日志数据的收集和统一管理，消除了本地日志存储可能被篡改和删除的风险，降低了日志分散存储的管理成本，提高了日志管理的可靠性。

◎大数据技术高速检索

采用基于大数据应用的高速检索引擎，通过匹配正则表达式、提取关键字等方式将非结构化的日志数据结构化，不仅保证每次查询都是实时计算，而且都能在秒级以内实现响应，实现对海量日志的快速检索和精确匹配。

◎满足企业合规性要求

国家主管部门为加强网络安全体系建设先后推出了等级保护、分级保护以及网络安全法等

法律法规，这些法律法规都直接或者间接地指出了要将日志审计作为信息系统审计的基本技术手段。系统可为用户开展合规性建设工作提供技术支撑，为企业法规遵从提供有力证据。

◎可视化日志分析

可以在对日志数据进行统计分析的基础上生成丰富的报表，实现分析结果可视化。iLOG 提供多种表格和图形表现形式（折线图、面积统计图），降低了管理人员对日志分析的难度。

◎高度可扩展性

支持单点部署和集群部署，可以按照客户实际需求进行资源扩展，降低不必要的资源浪费。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：23SS00337-A

★有效期：2023 年 11 月 24 日至 2025 年 11 月 24 日

所属品牌：远望

发布时间：2023 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询二维码

产品咨询邮箱：mail@chinayuanwang.com



身份鉴别产品

北京数字认证股份有限公司

北京数字认证股份有限公司（简称“数字认证”）成立于 2001 年，国有控股上市企业（股票代码：300579），是国内领先的网络安全解决方案提供商，也是拥有许可资质的电子认证服务提供商。数字认证以“共建可信任的数字世界”为愿景，以密码技术为核心驱动力，致力于保护网上业务安全可信开展、保障网络基础设施安全可靠运行、保护数据安全。数字认证充分发挥密码在建立网络信任和信息保护中的基础核心作用，坚持数字信任和数据安全两个战略主航道，提供可信数字身份、数据安全等解决方案，帮助用户构建身份可信、行为可信、电文可信、数据安全的网络空间。公司服务于政务、医疗、金融、教育、交通、电信、企业等数十个行业，为 30+ 国家部委客户、3 万+ 行业客户、2 亿+ 个人用户提供网络安全解决方案。一直以来，公司不断引领行业创新，产生了“第一张电子保单”、“第一张手写电子合同”、“第一张电子发票”、“第一张电子成绩单”等多项行业创新成果。公司积极服务于网络强国建设，积极承担重大网络安全保障任务，在北京 2022 年冬奥会和冬残奥会、建党 100 周年、国庆 70 周年、全国两会等国家重大活动信息安全保障工作中发挥了重要作用。数字认证努力实现关键核心技术安全可控，基于技术创新优势和行业领先地位，数字认证牵头和承担了“十四五”及“十三五”国家重点研发计划、工信部“工业互联网创新发展工程”、国家自然科学基金、国家信息化试点工程等 60 余项国家及省部级课题；牵头或参与编制密码、数字信任、网络安全等重要国家和行业标准 180 余项；创新成果形成 14 项专利、120 余项软著，先后荣获国家科技进步奖二等奖、省部级密码科技进步奖二等奖 2 次三等奖 7 次等多项荣誉。

网址：<https://www.bjca.cn/>

电话：400-9197-888

地址：北京市海淀区北四环西路 68 号双桥大厦 15 层（左岸工社）

产品名称：安全认证网关

产品概述

安全认证网关是一款集数据传输加密、身份鉴别等功能于一体的应用网关产品，遵循国家密码管理局相关规范，采用国家密码管理局公布的 SM2、SM3、SM4 等国产密码算法。

功能特点

安全认证网关提供内部网络的接入控制以及对接入用户进行强身份认证，解决用户使用应用系统时涉及的身份鉴别、权限控制、数据通信的机密性和完整性等安全问题，保证接入人员、应用和终端安全可信。可广泛应用于金融、公安、教育、卫生、政务以及交通等行业。

技术指标

每秒新建连接数（SM2）	36,000
最大用户并发数	20,000
最大并发连接数	1,100,000
最大加密吞吐量（Gbps）	9Gbps（千兆环境）

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

- ★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心
- ★证书编号：23SS00151-A
- ★有效期：2023 年 10 月 13 日至 2025 年 10 月 13 日

所属品牌：数字认证 发布时间：2019 年

产品适用领域：政务、卫生

产品照片：



产品咨询邮箱：service@bjca.org.cn



产品咨询二维码

北京芯盾时代科技有限公司

芯盾时代是领先的零信任业务安全产品方案提供商，是率先提出“以人为核心的业务安全”理念的公司。芯盾时代基于零信任安全理念，持续引领业务安全技术发展方向，帮助企业防范内外部的业务风险，提供场景化的全生命周期业务安全解决方案，助力客户打造安全、智能、可信的业务体系。

芯盾时代基于统一终端安全、智能决策大脑、零信任网络访问等多维技术，拥有完全自主知识产权的“智能业务安全产品线”和“零信任企业安全产品线”，保护企业业务系统安全和稳定运行，覆盖移动办公安全、全场景统一身份管理、网络边界安全防护、用户行为风险分析、金融账户及交易安全、交易 / 信贷 / 营销风控决策和反欺诈、移动 APP 安全等应用场景。

芯盾时代已连续三年被评为国家重点支持的专精特新“小巨人”企业，荣获 2023 年度北京市科学技术进步奖二等奖以及 2023 中国电子学会科技进步三等奖，在零信任安全、大数据风控、反欺诈 AI 模型、终端威胁感知、数据安全等领域拥有近百项发明专利，已牵头和参编 20+ 国家标准、行业标准和团体标准，已为金融、政府，央国企、运营商、互联网等 1000+ 头部客户落地零信任业务安全解决方案，为 3 亿 + 终端提供业务安全防护，累计保护 30,000 亿元金融交易，挽回超 100 亿元经济损失。

网址：www.trusfort.com

电话：400-818-0110

地址：北京市海淀区长春桥路 11 号万柳亿城中心 A 座 13 层

产品名称：零信任业务安全平台（SDP）

产品概述

零信任业务安全平台（SDP）致力于为用户解决在内外网连接、多数据中心远程访问、移动办公、全场景统一身份管理等场景下的安全需求，解决企业数字化办公场景下的安全风险。SDP 基于人（身份）、物（设备）、事（行为）的认证和授权重构访问控制的信任基础上，通过全面感知端点设备、身份、应用、服务、网络 and 人员行为等风险态势对业务和数据等资源的访问授予细粒度的最小权限，并进行动态访问控制和风险处置，实时保护服务资源、数据传输安全。

功能特点

◎高强度设备身份识别

融合主、被动式数据采掘技术，通过深度提取设备的底层硬件属性、操作系统内核特征、

协议栈参数及网络环境状态等多元信息元素，结合先进的机器学习算法模型，从而生成全球唯一且具有高度稳定性的设备指纹。具备终端基线检测能力，通过精细化且全面的态势感知，持续不断地对各类端点设备进行深度监测与评估。

◎资源网关双隐藏保障链路安全

零信任安全网关支持双重隐身的机制。可以实现网关自身的隐藏，提升网关自身的安全性，而后端应用通过网关反向代理，还可以实现应用资源的隐藏，以此实现双重隐身的效果，有效的缓解一些非法攻击的行为。在与网关建立连接的过程中，还会基于 SPA 单包授权机制，先认证后连接，从而保证通信过程整体的安全性，提升安全能力。

◎自适应信任评估实现动态访问控制

实时感知身份、设备、行为的风险信息，对每一次访问进行持续的信任评估，动态访问控制引擎根据评估结果实时生成访问控制策略，自动执行放行、阻断、二次认证、权限收敛等访问控制策略，避免风险访问造成的数据泄露，保障用户 / 终端和业务应用之间的安全访问。

◎安全沙箱保障终端数据安全

终端数据安全沙箱解决终端应用数据安全问题，包括提供安全访问控制、通信加密、数据文件加密、容器级隔离空间，用于隔离企业数据与个人数据、办公环境与互联网环境，实现对敏感数据的精确访问控制及有效隔离管控。

◎多维身份安全保障

从用户身份、设备身份及应用身份等多个维度实现身份的真实性判别，具备用户身份认证、终端身份标识、应用身份标识能力。

技术指标

◎服务隐身技术

基于 SPA 协议对可信客户端进行连接授权，执行默认“DenyAll”策略的高性能流量过滤。实现资源和 SDP 网关自身的全隐藏，缓解扫描、DDos 和其他非法攻击，成为恶意流量的黑洞。

◎国密安全认证

具有国密产品认证证书，支持 SM2/SM3/SM4/SM9 等国密算法，具有纯软件、低成本、易推广的特点，用户密钥抗窃取，认证机制易升级。

◎身份安全技术

统一身份管理、统一权限管理、统一认证管理、统一身份审计、动态访问控制等技术能力，规范人员身份安全管理。

◎高强度设备指纹技术

利用深度学习和数据统计模型对采集的设备属性进行逐层筛选，最终得到稳定性高且唯一性强的设备属性，进而生成高强度的设备指纹，作为设备全球的唯一 ID。

◎切面安全技术

在不干预业务正常流程的前提下，对系统实施更深层次、全方位的安全保护。

◎智能风险度量技术

利用大数据及人工智能技术，构建多维度的风险评估模型，从个体维度、团伙维度和流量通信维度进行全面风险度量。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00077-A

★有效期：2023 年 09 月 15 日至 2025 年 09 月 15 日

所属品牌：芯盾时代

发布时间：2018 年

产品适用领域：金融、政府、运营商、水利、能源、电力、制造、医疗等

产品照片：



产品咨询二维码

产品咨询邮箱：support@trusfort.com

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：零信任安全代理系统

产品概述

依托公司安全研究院十余年在网络安全领域的技术积累，迪普科技成功研发集合 SDP、IAM 及 MSG 技术的零信任系列产品，推出了适用于多行业、多业务场景的零信任架构解决方案，让用户网络真正实现“简单、智能、安全”，帮助企业安全快速完成数字化转型。

公司结合自身强大的研发实力，完善的产品线，将零信任与防火墙、态势感知等产品进行联动开发，不同产品组件能够对异常问题进行联动处置，保障了安全防护的全面性。

功能特点

我司零信任产品通过两次 SPA 单包敲门做到了网络真隐身，并将准入、桌管、杀毒等功能融入入客户端，同时提供软件开发工具包（SDK），可以嵌入第三方软件程序中，不需要进行二次登陆操作，认证登陆动作在后台进行，实现无感接入。不仅仅客户端可以对终端进行各种安

全检查与记录，管理平台、代理系统、客户端还能实现联动，确保系统健康运行。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402230809

★有效期：2023 年 4 月 14 日至 2025 年 4 月 14 日

所属品牌：迪普科技

发布时间：2021 年 6 月

产品适用领域：政府、运营商、金融

产品照片：



产品咨询二维码

产品咨询邮箱：linjiangge@dpotech.com

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址：www.qianxin.com

电话：95015

地址：北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神终端安全登录系统

产品概述

奇安信网神终端安全登录系统是一款专门为信创通用计算终端提供的增强身份鉴别产品，采用基于硬件 UKEY 的方式结合信创通用系统的认证校验要素，达到增强身份认证的目的，终端使用过程中结合拔 KEY 锁屏，登录失败锁定等功能大幅提高信创通用终端登录时身份识别的安全性，并通过登录日志信息对登录的行为做到有迹可循。

功能特点

◎注册功能

用户需在服务端进行信息注册。

◎绑定功能

将 UKEY 与用户以及终端账户做绑定，绑定后插入 UKEY 并输入 PIN 码才能登录操作系统。

◎解绑功能

当注销 UKEY 的登录功能时，需在系统上执行解绑操作。

◎解除锁定功能

输入 PIN 码多次失败后，系统会锁定此 UKEY，不再允许使用此 UKEY 登录，必须要解除锁定才能继续使用。

◎操作审计

记录各个用户的操作行为，便于进行行为审计。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230677

★有效期：2023 年 03 月 31 日至 2025 年 03 月 31 日

所属品牌：奇安信网神

发布时间：2018 年 3 月

产品适用领域：全行业

产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

启明星辰信息技术集团股份有限公司

启明星辰信息技术集团股份有限公司成立于 1996 年，由留美博士严望佳女士创建，2010 年在深圳 A 股中小板上市（股票代码：002439），是网络安全产业中主力经典产业板块的龙头企业，是新兴前沿产业板块的引领企业，是可持续健康业务模式和健康产业生态的支柱企业。

2024 年 1 月，启明星辰正式由中国移动实控，标志着公司迈入全新的发展阶段。中国移动致力于推动信息通信技术服务经济社会民生，以创世界一流企业、做网络强国、数字中国、智慧社会主力军为目标，已成为全球网络规模最大、客户数量最多、盈利能力和品牌价值领先、市值排名前列的电信运营企业。

启明星辰作为中国移动专责网信安全专业子公司，将全面贯彻“总体国家安全观”，发挥国资央企“科技创新、产业控制、安全支撑”三大作用，肩负起中国移动“安全核心技术攻坚者、安全产品服务引领者、安全运营体系支撑者”三大角色，围绕构建大网信安全板块进行战略布局，引领网络安全产业的升级与发展。

多年来，启明星辰持续深耕于信息安全行业，始终以用户的需求为根本动力，将场景化安全思维融入到客户的实际业务环境中，不断地进行创新实践，帮助客户建立起完善的安全保障体系，逐渐成为政府、金融、能源、运营商、税务、交通、制造等国内高端企业级客户的首选品牌。启明星辰入侵检测 / 入侵防御、统一威胁管理、安全管理平台、数据安全、运维安全审计、数据库安全审计与防护、漏洞扫描、工业防火墙、硬件 WAF、托管安全服务等十余款产品持续多年保持第一品牌。

网址：<https://www.venustech.com.cn/>

电话：010-82779088

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦

产品名称：天榕统一身份认证与访问控制平台

产品概述

天榕统一身份认证与访问控制平台（IAM），是一个对用户身份与用户访问进行综合管理的业务管理平台。平台涵盖了身份治理、用户全生命周期管理、可信身份认证、应用单点登录和用户行为审计等丰富功能。其中身份治理确保用户身份的准确性与合法性，为数字世界秩序奠定基础；可信身份认证严格把守数字世界大门，确保只有合法用户才能进入；应用单点登录为用户带来便捷、高效的体验，无需重复认证即可访问授权范围内的所有应用；通过用户行为审计监督用户举动，为数字空间的安全提供有力保障。

功能特点

◎**身份治理与身份服务**：IAM 从上游多身份源高效采集用户数据，汇聚后进行清理、整合与优化，确保全网用户身份数据唯一，实现“IP 到 ID”的安全防护，为企业安全管理和业务运营奠定基础。

◎**用户全生命周期管理**：用户身份创建、激活、变更到注销，实现全生命周期的精细管理，构建集中统一身份管理架构。统一维护用户认证凭据，管理组织机构和用户群组，便于分类管理。

◎**智能自适应多因素认证**：平台拥有丰富的认证方式，包括密码、邮箱、OTP、短信认证，对接钉钉、超级 SIM 认证等第三方平台，实现互联互通；集成指纹、人脸等多种认证方式，提供多样化认证，基于终端、网络、用户行为、业务多方面分析评估，提供自适应多因素认证，保障用户身份安全可靠。

◎**统一认证、单点登录**：全面实施 IAM 为用户带来便利与安全保障，用户只需在 IAM 一次认证即可访问授权业务，提高效率，减轻负担。平台集成多种标准单点登录协议，使基于这些协议的资源快速接入，实现单点登录。

◎**基于 AI 的持续信任评估**：风控中心采集多维度数据，结合 AI 智能分析模型预测感知风险，提供持续信任评估，动态管理用户访问业务行为，根据风险和评估结果调整权限策略，确保用户行为安全可控。

◎**集中、动态授权**：平台支持 RBAC、ABAC 和 PBAC 授权模型，整合风险评估实现动态访问管理，确保授权安全且符合业务需求。用户可将权限委托他人协助办公，系统严格监控管理权限的授予过程，防止滥用，确保业务顺利进行。

技术指标

◎**单点登录协议技术**：平台适配 CAS、OAuth、OIDC、SAML 等多种单点登录协议，对接多种类型资源，通过单点登录协议，资源可快速接入到平台，实现单点登录，统一授权。

◎**SaaS 技术**：平台采用云原生架构设计，微服务管理，产品支持 SaaS 化部署，可与各种云平台对接，一套系统提供多租户能力，租户之间数据安全隔离，保障租户数据安全。

◎**高性能、高可用**：平台通过分布式部署，保障认证业务的高可用；支持服务横向扩展，以保障高并发、高性能，为海量用户同时提供认证服务。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检查中心

★证书编号：24SS00676-A

★有效期：2024 年 05 月 17 日至 2026 年 05 月 17 日

所属品牌：启明星辰

发布时间：2021 年 6 月

产品适用领域：运营商、政府、企业、交通、电力等

产品照片：



产品咨询二维码

产品咨询邮箱：support@venustech.com.cn

上海派拉软件股份有限公司

上海派拉软件股份有限公司（简称：派拉软件）成立于 2008 年，是国内最早从事身份安全研发的原厂商，致力于为企业和机构提供以“数字身份”为核心的数字化能力底座与安全基石，覆盖身份安全、应用安全、数据安全，在上海、北京、广州、武汉、成都、长春、深圳、济南、厦门、合肥、杭州、西安等地设有研发中心和服务机构，拥有 600+ 行业专家和资深团队，服务能力遍布全国。

作为国内数字身份安全的领导者，派拉软件基于“身份优先”的零信任架构（Zero Trust），从全域身份治理和安全访问控制，逐步延伸到特权访问管理、API 管理、数据访问控制管理等产品和解决方案，不断扩展数字身份安全能力；重点围绕企业数字化转型三大核心要素，即人、应用服务、数据，提供相应的身份安全、应用服务安全、数据安全产品与解决方案，有效解决企业和机构数字化转型建设过程中暴露面大、过度信任、权限管理难、数据泄露等问题，高效应对更加复杂、多变的内外部安全威胁，为企业和机构强化数字化转型安全防护能力，建立体系化、端到端的数字化安全基石。

网址：<https://www.paraview.cn>

电话：400-6655-581

地址：上海市浦东新区高科东路 777 弄 8 号楼阳光商业中心写字楼 10 层

产品名称：派拉身份安全认证管理软件

产品概述

派拉身份安全认证管理软件，可以简单的理解为识别用户身份和访问控制的管理。

通过定义谁（身份）对哪些资源（应用）具有哪种访问权限（角色）来管理访问权限控制，是各类 IT 系统必不可少的基础安全管理机制和复杂云服务最核心的基础安全框架，是对资源提供可控安全的访问解决方案，是零信任安全架构的核心基础。

派拉身份安全认证管理软件的优点是，采用派拉身份安全认证管理软件后，用户只需要使用同一用户名、同一令牌就可以登录所有允许他登录的系统，用户使用更加方便。从安全角度出发，管理人员可以在认证系统集中地对各个应用系统上的用户进行管理。

功能特点

派拉软件身份管理平台核心功能包括用户管理、账号管理、权限管理、审计管理、应用管理及自助服务等，提供高效、便捷的管理功能和业务功能，支持微服务架构、弹性扩容和高并发部署。

◎ SSO 模块—单点登陆，认证方式

★单点登录

一套用户名密码即可访问所有应用，统一企业内部身份认证机制，提升企业应用的集成和管理能力。

支持主流认证协议，包括：CAS、OAuth2、OIDC、SAML、LTPA 等授权认证协议。

★认证

按角色、用户、用户类型不同认证方式登录；

支持账号密码登录、扫码认证、各类验证码、动态口令登录、生物识别认证、互联网认证等各种认证方式

Windows、MacOS 操作系统登录认证

◎ MFA 策略—登录策略配置

派拉软件身份管理平台提供丰富的 API 和 SDK，满足应用、系统和设备的快速接入，基于 OTP，内置支持数字 令牌、二维码认证，可与第三方认证数字证书、RSA、短信及生物识别认证集成，提供专属手机 APP，方便用户下载安装。

根据用户行为进行持续风险识别，结合不同的认证方式在不同场景或风险级别调用不同强度的认证能力。

◎ IDM—身份管理，应用管理，策略管理等后台管理功

★用户身份管理

支持用户全生命周期身份治理。

支持多用户类型，多组织架构，多岗管理

支持用户分级管理。

支持批量删除、启用、停用、锁定、解锁、重置密码操作。

★应用管理

支持应用分级管理。

表单代填可配置参数的字段映射，支持用户表、账号表、应用表的字段做映射

★账号管理

支持按组织、勾选的用户批量开通多个应用系统账号。

支持批量维护应用系统账号。

支持公共账号管理。

★权限管理

支持 RBAC、ABAC、PBAC 等授权模型。

支持细颗粒度权限控制。

支持数据权限控制。

支持多种方式授权，包括：管理员手动授权，自动化授权和用户自申请授权。

★上、下游数据同步

支持主推、被推两种模式。

支持 LDAP、AD、LDAP、API 等各类接口协议。

支持全量、增量数据同步。

同步日志可以查看详情，支持查看每次同步的成功记录数和失败记录数信息。

◎ Selfcare— 自助服务**★应用列表**

用户登录后，即可查看用户所绑定的应用列表，点击应用图标进入应用系统。

★查看登录日志

用户可查看本账号登录的详情信息，登录时间，登录 IP 地址，登录方式以及登录状态，便于用户了解自己账号登录信息及安全状况。

★密码自助，可自助修改密码、找回密码。

★个人自助，可自助绑定各类认证方式、个人信息自助修改。

◎ Audit— 日志审计

★身份管理审计管理。

★用户访问审计。

★用户自助审计。

技术指标**◎高性能**

★支持微服务、云原生架构，可提供互联网场景下的账号管理和统一身份认证。

★基础数据、配置可缓存，只是各类核心业务场景的高并发。

★利用内存式数据库缓存数据和保存票据，实现票据校验的高性能、高并发。

◎高可用性

★产品支持企业级高可用部署，避免单点故障。

★支持配置中心，实现动态加载更新。

★保证产品的 7*24 小时的稳定运行。

◎可扩展性

★各服务节点支持横向动态扩展。

★全面覆盖各类标准协议应用、非标应用的快速接入。

★支持自定义数据同步接口和推送接口。

★支持应用内组、角色、权限的字段任意扩展和表单任意扩展。

◎安全性

★支持多种认证协议，如：OAuth2.0，OIDC，CAS，LTPA，SAML 等，提高用户访问应用的安全性。

★支持数据同步过程中的签名和数据加密传输功能。

★支持敏感数据脱敏展现，敏感数据存储支持常见通用加密算法、国密加密算法加密存储。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230995

★有效期：2023 年 5 月 5 日至 2025 年 5 月 5 日

所属品牌：派拉

发布时间：2022 年 11 月 14 日

产品适用领域：金融，政府，能源，高端制造，教育等

产品照片：



产品咨询邮箱：marketing@paraview.cn



产品咨询二维码

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信终端安全登录系统

产品概述

天融信终端安全登录系统采用Ukey结合pin码进行双因素认证实现对人员身份认证、终端登录从而建立主动防御体系，支持热插拔，对内部用户进行有效管理，防止内部用户越权访问等违规行为发生，可对违规事件进行追踪、取证，充分保障内网的抗泄密风险能力。

功能特点

◎信息收集：系统支持对终端信息进行收集，从而帮助管理员全面了解终端信息。支持收集终端IP、MAC、操作系统、计算机账户等信息。

◎单点维护：系统提供了单点维护功能，管理员可对指定终端进行策略设置，完成对终端的安全登录管控。

◎安全登录：系统支持设置用户登录密码复杂、口令长度、鉴别次数等信息，同时支持拔key锁屏，可提高终端的桌面安全度。

◎双因素认证：系统采用Ukey+Pin码的方式完成对终端登录用户的身份鉴别，从而防止非

法人员登录涉密终端窃取信息。

◎**屏幕保护**：系统自动检测鼠标、键盘设备的信号，当鼠标、键盘停止操作达到指定时间上限时可自行锁定屏幕，防止他人窥屏。

技术指标

◎支持管理系统阈值配置，可查看系统的磁盘已使用百分比、内存已使用百分比、CPU 已使用百分比，支持骗、内存、CPU 超过阈值后报警。

◎支持通过网络接口进行远程管理，可根据管理主机 IP 地址，MAC 地址限制特定访问，非授权主机无法访问系统。

◎支持管理员创建组织结构，支持组织机构的导入导出，并可对人员进行分组管理

◎支持创建管理员用户，可管理管理员账户、key 等信息；并可对管理员进行身份鉴别可配置管理员登录口令长度、口令更换周期、账户锁定周期等信息

网络安全专用产品安全认证或安全检测结果证明

(1) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS037-483

★有效期：2023 年 10 月 11 日至 2028 年 10 月 10 日

(2) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS037-484

★有效期：2023 年 10 月 11 日至 2028 年 10 月 10 日

所属品牌：天融信

发布时间：2020 年 7 月

产品适用领域：政府、公检法等

产品照片：



产品咨询 feng_chong@topsec.com.cn



产品咨询二维码

长春吉大正元信息技术股份有限公司

长春吉大正元信息技术股份有限公司是中国领先的数字安全综合服务商，1999年成立，2020年在深交所挂牌上市，是国家网络空间安全及数字安全建设引领者，我国密码安全、电子认证、身份信任等领域领军企业，国内最大的公钥基础设施（PKI）产品供应商之一，国家数字安全科研项目、标准建设的主要参与者，国家重大活动的安全保障参与者。

吉大正元坚持技术创新，以密码技术为核心打造了密码安全、身份信任、数据安全、系统安全、网络安全、应用安全、业务安全等完整的数字安全产品体系、解决方案和服务能力，以及新一代数字安全体系“元安全”，涵盖数字安全防护设施与智能操作系统，提供数字经济安全运行环境，为数字经济发展和数字中国建设中的各行各业关键信息基础设施提供安全支撑与保障。

公司资质体系完善，服务覆盖政务、金融、能源等多行业客户，广泛参与建设国家金字工程，保障全国两会、载人航天、北京奥运会等重大社会、政治活动。据权威机构统计，公司在身份管理和访问控制软件市场的占有率连续多年稳居行业第一。

公司未来将持续探索数字安全与应用和数字经济产品技术，不断为用户提供领先的数字安全产品、服务和全方位数字安全解决方案，全面护航数字经济发展，夯实数字中国安全基石。

网址：www.jit.com.cn

电话：010-62618866

地址：北京市石景山区给古城街道中海时代广场B座16、17层

产品名称：吉大正元身份认证网关

产品概述

吉大正元身份认证网关是提供内部网络的接入控制以及对接入用户进行强身份认证和审计服务的产品，解决用户使用应用系统时涉及的身份验证、信息保密、权限控制等安全问题。

身份认证网关可以为用户提供统一、安全的身份认证服务，并根据用户提交的身份不同而分配不同的权限，以达到权限最小化分配。

◎应用保护：由于应用的复杂性和多样性，需要对使用不同协议的应用进行保护。

◎身份认证：提供高强度的身份认证方式，确保登录的用户确实为授权的个体，消除未授权用户非法访问的风险。

◎访问控制：允许用户定义合适的安全策略，可以有效保护对专用网络系统及应用的访问，可以根据用户的不同身份来确定其访问权限。

◎链路加密：使用密码技术和隧道协议来提供网络的保密性、认证性及信息完整性。

◎**责任认定**：可以通过提供的个人信息来综合认证用户的身份，并可以记录下其访问应用的情况，实现不可抵赖特性。

功能特点

◎支持的密码算法包括 SM1、SM2、SM3、SM4 等国密系列算法，符合国密局对密码算法的合规性要求。

◎以在通信双方之间建立加密连接的方法保证数据传输的机密性，防止数据在网络传输过程被非法用户窃取导致数据泄露，支持通信链路可以依据用户对安全和性能效率的需求选择是否加密，支持国密 SSL 加密传输。

◎提供双证书认证体系（签名证书、加密证书），通过双向认证对端证书来验证通信双方的身份，有效解决数据来源真实性问题，支持基于数字证书的单、双向认证，可以通过配置为单向、双向认证方式，设置用户是否需要提交证书。

◎日志审计功能：提供日志记录、查看、导出功能，日志审计模块全程记录加密服务器运行状态，包括程序运行日志、设备状态日志、配置管理日志。同时具备业务量统计功能；包括：历史业务量可以根据小时、天、月、年查看历史状态。

◎支持基于 SM3 的 MAC 算法来保证消息的完整性，防止数据在网络传输过程被非法用户篡改。

◎支持客户端安全检查功能，通过设定策略可验证客户端病毒库、防火墙、操作系统、补丁以及其他条件，客户端支持指定浏览器打开应用。

◎支持基于一些特定的资格进行基于角色的授权管理，支持证书 + 终端绑定访问控制

◎提供 Split DNS 功能，可以控制客户端 DNS 的请求顺序，以及请求 DNS server 的类型。

◎系统可视化管理：提供基于 Web 页面的完整图形化配置界面，根据具体网络环境和应用条件进行相关配置，并设置系统管理员、安全管理员和审计管理员角色进行分权管理，管理端支持 GMSSL 登录方式，确保管理端网络层安全通道满足测评要求

◎支持 OAuth、CAS、SAML 单点登录协议，具备自动判断用户是否登录成功的功能，网关能够为多应用环境下提供单点登录服务，形成统一简易门户，可定制登录页面。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01438-A

★有效期：2024 年 9 月 27 日至 2026 年 9 月 27 日

所属品牌：吉大正元

发布时间：2011 年 1 月 11 日

产品适用领域：公安、政府、能源、金融、教育、电力等

产品照片：



产品咨询：marketing@jit.com.cn

长扬科技（北京）股份有限公司

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，国有资本占股近 50%。

基于“安全协同·AI 赋能”的战略理念，公司在工业互联网安全领域持续深耕，团队核心成员是中国工业互联网安全事业的第一批践行者。

长扬科技在业界开创了“智能工业安全大脑”的产品理念，以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了 60 余款产品，面向集团级客户提供工业网络安全态势感知、工业网络安全纵深防御、工业视觉 AI 安全分析、工业零信任安全、工业数据安全和工业数据通信等多维度产品，构建覆盖工业互联网安全产业完整生命周期的安全保障体系。

公司总部位于北京，并在西安、武汉、郑州、成都、上海、广州等全国近 30 个城市建有研发中心及服务分支机构，形成了覆盖全国的“网状战略布局”，可为客户提供强有力的本地化服务。长扬科技积累了超过 32 个行业细分领域、4000 余家工业企业的安全服务经验，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，提供 4 大类、27 项标准化服务，致力于为企业数字化转型、智能化升级提供网络安全专业化保障服务。

网址：<https://www.cy-tech.net/>

电话：010-82194186

地址：北京市海淀区闵庄路 3 号四季慧谷·国家网络安全产业园 2 期 15 号楼

产品名称：长扬零信任访问控制系统 TAS/V1.0

产品概述

零信任访问控制系统是一个基于零信任安全理念和软件定义边界安全模型构建的安全访问控制系统。该系统以身份为基石，提供业务安全访问，具备动态访问控制和持续信任评估等功能，为企业网络构建无边界的数据安全防护体系；为企业远程办公、远程运维和远程研发测试提供数据安全保障。此外，依托零信任架构对应云-管-边-端的业务体系，构建工业互联网边缘侧安全智慧管理，强化对边缘侧的安全保护，有效防护潜在威胁。

零信任访问控制系统由终端接入安全层、数据传输安全层、核心应用安全层组成，各层能力基于相应产品实现，分别为零信任访问控制系统、统一身份认证平台、零信任应用安全网关、零信任边缘安全网关和零信任安全客户端。

功能特点

◎**统一身份认证**：长扬统一身份认证平台（IAM）是集身份帐号（Account）管理、认证（Authentication）管理、授权（Authorization）管理、安全审计（Audit）及应用管控（App Control）于一体的综合身份安全管理平台。IAM 可将用户身份信息集中存储，实现电子身份全生命周期管理，支持账号密码、短信、企业微信、AD 等多种认证方式。IAM 作为应用导航门户，支持 B/S、C/S 应用的单点登录，一站式访问，业务应用支持按需授权。IAM 以身份为基石，面向业务需求，安全链接各类应用、数据、流程，可为组织信息化业务融合及数字化安全管理提供重要支撑。

◎**业务按需授权**：管理员可以在零信任访问控制系统后台合理限制用户或设备可以访问哪些应用。例如，只允许财务部的员工访问财务系统，不允许访问 SVN、GitLab 等代码仓库系统。越权访问会被安全网关拦截。这样，就避免了用户过度授权，大大减少攻击面，也减少了员工泄密的可能。除了应用的维度之外，还可以对用户的访问位置、访问时间等维度进行限制。

◎**数据传输加密**：安全客户端支持国密 SSL 协议双向认证，采用国密算法对数据传输进行加密。

安全客户端在访问指定目标业务系统时自动切换至国密加密链接通道，调用国密加密秘钥 Key，使用国密算法来加密封包，同服务器协商密钥过程采用 SM2 算法加密，报头和荷载等采用 SM4 算法加密，从而保护整个业务访问过程。同时可以有效的阻止攻击者通过监听和中间人攻击等手段，获取业务应用的账号、密码和敏感信息。

安全客户端支持国密算法，包括 SM4 对称密码算法，SM2 椭圆曲线公钥密码算法，SM3 杂凑算法等，同时支持多家厂商国密硬件 UKey。

◎**全面实名审计**：安全客户端和安全网关对用户行为操作进行审计记录，如网页访问时间、网页内容复制、网页打印或者保存、文件下载等等。同时，客户端将审计信息上传至安全访问控制系统。

应用安全网关可以对用户的非法访问请求进行拦截并记录，同时对用户的访问次数以及应用的请求次数进行记录，并将所有信息传送至安全访问控制系统，通过平台态势感知模块对大量数据进行统计分析，形成可视化数据。

◎**边缘数据采集及防护**：基于边缘防火墙，学习工业协议指令，对内执行工业指令级的安全防护策略。南向接口支持 EthernetIP/ModbusTCP/ModbusRTU//S7Ethernet/DCS/CNC/ 仪表等多种工业设备协议解析；北向接口支持 OPC UA/Modbus TCP/Ethernet IP/MQTT/HTTP 等协议。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS00911-A

★有效期：2024 年 6 月 28 日至 2026 年 6 月 28 日

所属品牌：长扬科技

发布时间：2022 年 6 月 15 日

产品适用领域：政府、金融、工业等行业领域

产品照片：



产品咨询：jianwen.jin@cy-tech.net



产品咨询二维码

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望零信任访问控制系统

产品概述

远望零信任访问控制系统是一款基于零信任 SDP（软件定义边界）与 IAM（身份管理）技术实现的远程访问控制系统，可对业务实施安全隔离，访问者需要运行零信任终端，使用授权账号通过认证后才能连接和访问授权的业务系统，并且可以根据访问者的访问行为、运行环境等因素动态持续调整用户权限。

功能特点

VPN 网关认证。提供已安装代理程序的终端来完成 VPN 协议认证。

身份认证。在使用终端前可采用多因子认证方式对用户身份进行鉴别，保证终端用户身份的合法性，同时对身份认证操作日志进行审计。

◎动态验证授权：持续对用户的访问行为进行信任评估，通过检测异常行为、越权行为、威胁风险及终端配置情况，动态控制和调整用户访问权限，以保障应用业务的安全；

◎访问控制：统通过层层授权和防御机制，只授予人员所需的最小权限，进行细粒度的访问控制；

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0402231921

★有效期：2023 年 06 月 25 日至 2025 年 06 月 25 日

所属品牌：远望

发布时间：2023 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询二维码

产品咨询：mail@chinayuanwang.com



终端安全监测产品

北京杰思安全科技有限公司

北京杰思安全科技有限公司，成立于 2015 年，是一家专业研发、生产、销售主机安全响应系统软件的高科技民营企业；是国家高新技术企业，拥有自主知识产权专利、软著近百项；累计融资近亿元。

公司聚焦企业级端点安全，为用户提供基于操作系统的威胁检测和防护。凭借 EDR、CWPP、自适应微隔离等前沿安全技术，提升用户抵御未知威胁（包括勒索软件、0day 漏洞、APT 攻击、免杀木马等）的能力，增强对全网主机内部安全状况的掌控能力，弥补传统安全防护体系不足，重振企业网络安全信心。

公司自主研发的以杰思猎鹰为核心的一系列可控、可信产品，适用于云计算、大数据、工业控制、移动互联等新环境，满足服务器、PC 机、云主机、工控主机、移动智能终端、物联网终端、车联网终端等设备在新环境下的安全需求。

目前，已成功服务政府、运营商、金融、能源、交通、教育、互联网等数百名行业客户，为国家互联网应急中心、国务院扶贫开发领导小组办公室、国家卫生健康委员会、中国民用航空局、国家能源局、国家电网、中国铁路、中国石化、中国石油、中国烟草、中国电信、中国联通、中国移动、中国节能、鞍钢集团、鲁能集团等政企客户提供高效的主机威胁检测与响应。

网址：<https://www.majorsec.com>

电话：010-62946550

地址：北京市海淀区清河永泰园甲 1 号建金中心 4 层 402

产品名称：杰思猎鹰主机安全响应系统

产品概述

杰思猎鹰主机安全响应系统，是杰思安全基于多年端点安全领域防护经验，自主研发的一套基于操作系统的威胁检测与响应产品，能提供

能够帮助安全管理员快速精准地识别风险主机，实时追溯与响应，弥补传统安全防护不足，提升用户抵御网络威胁的能力。

可广泛部署于安装了 Windows、Linux、国产操作系统的服务器、云主机、PC 机、工控主机、移动智能终端、物联网终端、车联网终端等泛在行业主机。

功能特点

◎资产清点及管理

基于主机安全视角，帮助用户快速梳理和清点主机资产信息，从主机硬件资产、系统资产

到上层软件资产、账户资产，自动构建全面的资产安全视图。资产信息清晰可见，让用户对全网资产情况了如指掌；自动发现、自动分组、自动记录变更信息等功能，智能快速构建自适应主机安全防护边界，实时掌控变化。

◎端点脆弱性发现

提供覆盖 Windows、Linux 及多个国产操作系统的安全基线检查，包括防火墙、账号口令、日志、组策略配置等，内置多个行业和场景检查模版，提供基线修改指导，科学提高系统安全短板。同时，从行为合规检测、系统漏洞检测、注册表异常检测、关键配置检测、风险文件检测、账户风险检测等进行主机多锚点风险检测。结合自适应资产安全视图，呈现可视化的主机风险全貌，帮助用户在庞大网络内对风险主机进行秒级定位。

◎威胁入侵检测

通过自主研发的智能行为追踪检测技术，在不依赖病毒特征库的情况下，即能识别检测出各类活跃的恶意程序、针对主机系统的恶意攻击、对主机系统恶意破坏等。

通过守护操作系统关键入口点，并对攻击者常用和流行的攻击技术进行识别、归类、建模、训练、自学习。结合人工智能机器自学习技术，不断提升检测和识别精度，并自适应业务场景，不断优化防护机制，实现对已知为未知威胁的精准防护。

结合独创的主机环境变量横向对比技术，在全网同业务虚拟机服务器或主机中进行横向对比，感知主机异常变化，发现初期入侵点。并通过定点系统入口监控和行为合规监控，有效应对多种恶意程序的变形逃逸。

◎智能响应与处置

融入机器学习技术，贴合用户业务场景，不断进化用户侧行为检测与响应模型，响应精准度 > 99%。提供多种响应防护模式，结合近百种风险分类，可形成数十万个响应方案组合，提供不同业务场景下更理想的响应方式，为每个用户提供私人订制的响应方案。

◎溯源与调查分析

深度追踪安全事件发生全过程，在端点侧全面记录安全事件信息，图形化展示威胁事件的多维度信息关联，包括进程调用关系、网络关系、关键注册表、创建文件行为等，剖析每一个安全事件过程。可迅速定位失陷主机并还原事件发生过程，找到事件原点，同时与网络情报共享，形成完整事件证据链，锁定威胁源。

◎安全可视化管理

采用多视角风险呈现模式，构建出透明可视的安全管理平台，从网络、主机、文件、账户、行为、事件等多个角度深度分析，层层展现，暴露每一个风险点，帮助用户做到安全知己。结合事件深度溯源能力，透析安全事件，帮助用户做到安全知彼。

技术指标

◎看清主机内行为

清晰直观显示所有主机内部系统变化，看清用户业务在操作系统运行时面临的安全风险。

◎入侵威胁溯源

实时对黑客入侵客户业务主机过程进行“行为画像”，图形化展示威胁事件来源、传播途径、影响主机数量范围等，并统一防御和处置。

◎轻量设计，超强适配

软件占用主机资源极低，CPU 占用率 <1%，内存占用 <25MB, 磁盘空间占用 <30MB。安装简单快速，在操作系统界面上无弹窗打扰，全面支持 Windows、Linux 以及多个国产操作系统。

◎未知网络威胁检测防护

对于业务主机上传统杀毒软件库内没有的未知威胁，通过端点检测与响应核心技术，实时检测与分析入侵点和感染途径，并全网排查感染主机，及时处置和实时防护。

◎主机安全集中管理

提供所有业务主机内的系统操作，业务更新变化，人员使用情况，专用主机、业务服务器、云主机安全管理“一把抓”，扫清主机安全管理分治造成的监控真空，提升安全管理和应急响应效率。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0503230367

★有效期：2023 年 2 月 24 日至 2025 年 2 月 24 日

所属品牌：杰思安全

发布时间：2016 年

产品适用领域：政府、运营商、军队、金融、能源、交通、医疗、教育等

产品照片：



产品咨询二维码

产品咨询邮箱：marketing@majorsec.com

北京珞安科技有限责任公司

北京珞安科技有限责任公司（简称：珞安科技）成立于 2016 年，是专注工业网络空间安全的创新型高科技企业和国家级专精特新“小巨人”企业。

珞安科技拥有业内顶尖工控安全专家团队、工业网络空间安全研究实验室和北京、武汉、西安、天津大研发中心，坚持自主研发和技术创新深耕工控领域，以零信任理念和体系化思想为指导，打造“实战化、易部署、易维护”工控网络安全产品体系，全面覆盖工控安全、业务安全和工业互联网安全，为工业企业构建了全方位的工业网络空间安全防护体系。

珞安科技依托强大的技术原厂商实力，积极开展安全服务和安全运营，业务遍布发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业，覆盖 600 多家监管机构和大型工业企业。服务超 2000 家中小企业，创造多个业内大规模安全产品部署成功案例。在全国设有 20+ 分子公司及办事处，提供 7*24h 安全应急服务响应，保障国家关键信息基础设施安全稳定运行。

网址：<https://www.icssla.com/>

电话：010-8250-9710

地址：北京市海淀区昆明湖南路 47 号国防教育基地二层

产品名称：主机安全加固系统

产品概述

主机安全加固系统是一款综合运用安全标记、访问控制、完整性保护等多层次立体式防护手段，弥补通用操作系统安全性不高等固有缺陷的内核级跨平台安全加固产品。通过扩展操作系统的安全子系统，防范外部的渗透攻击，预防内部的主动泄密，解决工业终端面临的恶意代码执行、越权访问等各种异常问题，提升操作系统整体的安全保护能力，满足国家等级保护的三级要求。

功能特点

◎满足等保三级的安全技术要求

提供基于标记的强制访问控制，遵循 BLP、BiBA 原则，支持对操作系统的各类重要资源进行安全保护；提供非法外联探测，防止信息外泄；保障系统的完整与资源的安全使用。

◎全面的系统环境保护

采用白名单式管控技术，一键固化系统当前运行环境；支持程序白名单共享，实现安装即固化；采用独有的补丁跟踪技术和智能软件更新捕获技术，支持操作系统的补丁更新和应用软件升级。

◎贴合工业场景的安全身份认证

基于硬件 USBKEY，实现操作系统登录的增强身份认证，安全事件责任到人；门禁式生物指纹认证机制，让工业场景下的账户认证既安全又便捷。

◎细粒度的设备管控

白名单式的 U 盘管控，防范 U 盘滥用，阻断病毒传播；硬件级安全加密 U 盘，保障数据的存储安全；支持基于类别、供应商、产品编号等细化控制 USB 外设。支持 5G 网卡、无线热点、无线网卡、拨号等各种上网方式的细化管控。

◎优越的平台兼容性

支持 Win2000 至 Win11 操作系统，支持 RedHat、CentOS、Ubuntu、SUSE 等主流 Linux 系统，支持麒麟、统信、凝思、湖南麒麟、OpenEuler 等国产操作系统。

◎丰富的安全加固配置

提供 100+ 系统安全策略配置；提供帐户密码、共享、审核等关键系统安全配置项的统一配置；提供对关键文件、注册表项和业务进程的安全防护，预防恶意破坏；提供远程登录安全防护，限制登录用户、时间、位置、协议等，提高系统使用安全性。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231661

★有效期：2023 年 6 月 16 日至 2025 年 6 月 16 日

所属品牌：珞安科技

发布时间：2017 年 5 月

产品适用领域：发电、电网、石油石化、轨道交通、智能制造等 20 多个工业行业。

产品照片：



产品咨询二维码

产品咨询邮箱：liss@icssla.com

北京信安世纪科技股份有限公司

北京信安世纪科技股份有限公司（股票代码：688201）成立于2001年8月，是科技创新型的信息安全产品和解决方案提供商。公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全、通信安全等基础性安全问题，为金融、政府、企业、军队等重要领域的核心业务系统提供先进的网络安全产品与安全解决方案。

网址：www.infosec.com.cn

电话：010-68025518/400-670-5518

地址：北京市海淀区建枫路（南延）6号院金隅西三旗科技园2号楼信安大厦

产品名称：科云主机安全监控与审计系统

产品概述

科云主机安全监控与审计系统采用先进的内网安全技术，结合事前控制、事中监视、事后审计等技术手段，使内部的网络、系统和资源得到充分保护，建立起可靠的内部网络防范体系，并获得对内部网络终端完善的安全管理。

系统包含服务端与客户端，具备的主要功能包括终端准入控制、终端外设控制、网络行为控制、违规外联控制、补丁分发管理、移动磁盘管理等。

功能特点

◎符合安全标准

系统通过了中国人民解放军J信息安全测评认证中心、国家保密科技测评中心、公安部信息安全产品检测中心的安全检测，符合GJB5612、BMB17-2006、BMB23-2008以及GB/T22239-2019安全等级防护规范中的终端安全技术要求。

◎对接安全平台

系统支持与统一安全管理系统对接，能够接受统一安管系统的管理并上报安全事件、安全监测等数据，管理接口符合GCB010-2015《安全管理接口技术要求》、GCB007-2015《安全审计服务规范》的规范要求。

◎权威机构认证

产品在中国人民解放军J信息安全测评认证中心、国家保密科技测评中心、信息产业信息安全测评中心等权威测评机构通过测试，并获得J用信息安全产品认证（JC+）、涉密信息系统产品检测证书、软件著作权、国产麒麟系统兼容性认证证书。

◎国产自主可控

系统完全基于国产操作系统环境开发，服务端硬件平台支持主流国产自主可控硬件平台及

国产操作系统，客户端支持主流国产硬件平台及国产操作系统部署，支持不同类型终端通过一套主机管控系统服务端进行统一管理，具备较强的系统兼容能力和一体化管控能力。产品已在全 J 国产办公系统重点试点单位中应用，同时客户端支持跨平台（X86、国产化、道系统）混合部署。

◎高兼容性

系统与现用的 BM 综合管理系统完全兼容，包含基础平台、标签等系统。系统已在 J 方多个国产自主可控办公环境中试用，支持主管部门提出的典型安全部署模式，与可信环境进行联调测试，能够完全兼容，且能够稳定运行。

◎应用广泛

系统产品上市以来在多个行业得到广泛应用，目前已在多个省 / 市级党政机关、政府部门、人民银行、科研院所、检察院公安机关等行业应用部署，总部署点数超过 50 万点。

技术指标

◎级联部署

支持 2 套（或以上）服务端级联部署，下级节点能向上级节点上报机器及日志相关信息，上级节点能向下级节点下发管控策略，且能直接跳转至下级服务器进行相应管理操作。

◎终端、用户管理

支持对计算机终端、用户进行分组管理，支持分组嵌套。

◎身份认证

支持无缝接管操作系统登录，支持多种认证方式。

◎密码管理

支持对操作系统的用户密码进行密码复杂度检测。

◎准入控制

支持基于 SNMP、DHCP、802.1X、静态绑定的终端准入控制。

◎基线核查

支持对主机进程、服务的运行情况、主机各端口的监听状态、主机操作系统版本及补丁安装情况、主机防病毒等安全软件、应用软件的安装和运行情况、主机注册表（限 windows 系统）等进行合规性检查。

◎非法外联管理

支持对计算机终端违规外联的行为进行探测与控制。

支持对违规计算机终端进行断网、关机、重启等处置，并进行消息提醒和日志上报。

◎非法接入

支持对计算机终端非法接入其它内部网络的行为进行管理控制，通过对可访问的 IP 范围进行配置，当计算机终端出现范围以外的网络访问时触发非法接入违规。

支持对违规计算机终端进行断网、关机、重启等处置，并进行消息提醒。

◎ IP/MAC 绑定

支持 IP/Mac 绑定，可及时发现地址变更行为，对于违规修改地址的行为支持断网、自动恢复控制等处置方式。

◎终端网络防火墙

支持网络数据包过滤控制，可制定网络访问控制策略，支持 ICMP、TCP、UDP 协议。

◎进程控制

对计算机终端中运行的进程进行管控，支持通过黑白名单机制禁止 / 允许指定进程的运行，名单中的进程信息包括进程名称、进程路径、进程 MD5 值。

支持进程白名单导入。

◎服务控制

对计算机终端中的服务进行管控，支持通过黑白名单机制对指定服务进行启动 / 停止控制。

支持服务白名单导入。

◎文件访问控制

支持基于文件路径和文件类型的文件访问控制。

◎打印控制

支持对终端的打印功能进行允许 / 禁止控制。

◎刻录控制

支持对光驱的多种控制方式，支持光驱白名单。

◎ Windows 安全管理

针对 windows 平台终端提供注册表保护功能，可对 VMWare 虚拟机进行控制，支持禁止 / 允许开机进入 windows 安全模式。

◎移动磁盘管理

支持对移动磁盘进行控制和日志记录，控制方式包括禁用、只读、读写、审计只读、审计读写。

◎外设管理

支持对已知类型外设进行启用 / 禁用控制。

◎可信软件管理

支持对国产系统下 deb 软件包的导入与分析。

支持基于软件包分析数据进行软件运行控制。

◎软件分发与安装

支持通过 WEB 管理端界面上上传软件包。

◎补丁管理

支持 Windows 和 Linux 操作系统的补丁库管理，支持本地上传补丁，支持补丁检索。

◎终端资产管理

支持终端软硬件信息的自动采集上报和查询检索。

◎日志审计

具备日志记录、日志报表、日志自动清理等功能。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230486

★有效期：2023 年 03 月 10 日至 2025 年 03 月 10 日

所属品牌：信安世纪

发布时间：2012 年 7 月

产品适用领域：该产品适用于数据中心、云计算平台、金融与电信、工业自动化与智能制造、建筑与安防、企业 IT 运维与安全管理等领域

产品咨询邮箱：market@infosec.com.cn



产品咨询二维码

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

作为行业领导者，安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。

2020 年 11 月 23 日，安恒信息正式成为 2022 年杭州第 19 届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

网址：<https://www.dbappsecurity.com.cn/>

电话：0571-28860999

地址：杭州市滨江区联慧街 188 号安恒大厦

产品名称：安恒终端安全管理系统

产品概述：

安恒终端安全管理系统（UES），是安恒信息基于全新的“无极”架构开发，集成病毒查杀、主机监控审计、漏洞扫描及防护、入侵行为检测及告警、数据防泄露等核心技术的新一代终端安全一体化管控平台。是以终端安全管理为核心，提供包含检测预防、实时防护、安全保护、风险处置、事件追溯等能力的全生命周期管控与防护一体化终端安全解决方案。帮助客户准确识别、监控、修复风险终端，时刻保证终端资产在安全、合规、可信的前提下被使用。

功能特点：

安恒终端安全管理系统（UES）由管理控制中心和客户端组成：

管理控制中心部署在独立提供的服务器上，主要功能为把所有客户端信息集中于一体，便于集中监管和配置安全策略，聚合客户端情报信息进行后续的防护以及响应。管理控制中心采用 B/S 架构，安装完成后，用户可以在任意与管理控制中心网络可达的计算机上访问管理控制中心的 Web 管理平台，对终端进行管控；

客户端软件是一个独立的本地可执行程序，安装在需要被管控的终端上，完成管理员通过管理控制中心下发的任务和策略。

安恒终端安全管理系统主要功能如下：终端管理、防病毒、弱点检测、主机审计、数据防

泄漏、水印追溯、桌面管理、资产盘点、基线检查等核心功能。

技术指标：

◎功能指标：

具备终端管理、任务管理、漏洞管理、主机审计、防病毒、威胁情报、数据防泄漏、基线检查、水印追溯、桌面管理、统计分析、平台管理、用户中心等模块。

◎性能指标：

最大并发连接数 12 万；

系统延时 $\leq 5\text{ms}$ ；

小文件传输性能 ≥ 300 个 / 秒；

大文件传输性能 $\geq 20\text{MB/秒}$ ；

数据库传输性能 ≥ 1000 条 / 秒；

策略支持能力 ≥ 200 条（开启日志）

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0106230253

★有效期：2023 年 2 月 10 日至 2025 年 2 月 10 日

所属品牌：安恒

发布时间：2022 年 11 月 1 日

产品适用领域：政府、教育、企业、运营商

产品照片：



产品咨询邮箱：beric.liu@dbappsecurity.com.cn

杭州迪普科技股份有限公司

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业（股票代码：300768）。

迪普科技是国家信息安全漏洞库一级技术支撑单位、信息安全标准化技术委员会成员单位、中国网络安全产业联盟常务理事单位。公司获得了国家知识产权示范企业、国家重点软件企业、国家高新技术企业等多项荣誉。

自成立以来，公司坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2~7 融合式操作系统。依托于安全研究团队十多年以来的技术积累，开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

公司的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了 G20、APEC 峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域深耕，不断完善产品与解决方案，为客户创造更大价值。

网址：<https://www.dpotech.com/>

电话：0571-2828 1966

地址：浙江省杭州市滨江区月明路 595 号迪普科技 18 楼

产品名称：终端检测与响应系统

产品概述

DPtech XDR 终端检测与响应系统是集恶意代码防护、桌面管理、终端威胁检测与响应（EDR）于一体的全新一代

终端安全管理系统，系统建立统一管理的终端安全整体防护体系，有组织有计划地监测和分析终端安全状态，统一配

置终端安全策略，提供终端的安全保障能力，确保终端系统正常、高效的运行，提供彻底解决终端安全威胁的全生命

周期的管理，包括事前预警防范、事中应急处置、事后追责溯源，完成终端安全威胁闭环。

功能特点

◎防病毒系统的杀毒引擎采用了智能广谱技术、内存杀毒技术和比特动态滤毒技术等多项

全球顶尖的杀毒技术，可以安

全地清除引导区病毒、邮件病毒、恶意网页、木马程序、黑客程序、VBS 病毒生产机、宏病毒、蠕虫以及其他类型的病毒，查杀病毒数量超过 60000 种。

◎增强智能主动防御体系，对未知病毒实施多行为联动主动防御，更准确、更全面地防御未知病毒。系统级行为监控，

从注册表、系统进程、内存、网络等多方面对病毒行为进行主动防御，全方位保护系统安全。

◎大部分主流病毒技术都进入了驱动级，病毒已经不再一味逃避杀毒软件追杀，而是开始与杀毒软件争抢系统驱动的控

制权，使杀毒软件功能失效。防病毒系统拥有强大的自防御体系，阻止了病毒目前所有已知的破坏手段，从系统底层

保护自身安全，为保障系统安全打下了坚实的基础和前提。

◎越来越多的病毒开始利用 Rootkit 技术隐藏自身，利用 Hook 技术破坏系统文件，防止被安全软件所查杀。防病毒

系统反病毒 Rootkit、反病毒 Hook 技术能够检测出深藏的病毒文件、进程、注册表键值，并能够阻止病毒利用

Hook 技术破坏系统文件，接管病毒钩子，防御病毒于系统之外。

◎防病毒系统对终端使用的进程进行保护，防止病毒程序恶意关闭杀毒软件进程。对自身的安装程序和安装目录进行保护，防止中病毒计算机安装杀毒软件被病毒关闭，有效防止病毒镜像劫持，关闭杀毒软件的情况发生，即使中病毒后也可安装杀毒软件终端安全管理系统防病毒，高效的处理病毒问题。

◎可以对网络中各级控制中心的系统性能，CPU 使用率、磁盘使用率、服务状态等指标进行监控，让管理员一目了然的掌握整个系统的工作情况。

技术指标

◎高可用、可伸缩的系统架构；整体架构采用集群（Elasticsearch 集群、Kafka 集群、Redis 集群等）和服务组（事务服务器组、文件分发服务器组等）架构设计，并单独设计调度服务器对所有服务器根据资源使用情况进行全网自动化调度，单个服务器的软硬件故障不影响系统的整体运行，系统可根据计算、存储资源使用情况进行无限扩展，保证服务器和终端始终处于最佳工作状态，整体架构具有高可用、可伸缩、低耦合、低故障的优点，可灵活支持从几百台到上百万台的终端管理规模。

◎智能轻量高安全代理；借助于静态风险特征分析、动态行为序列分析、机器学习、终端行为的全面监控与数据采集等先进技术，降低传统防病毒软件对文件监控的依赖，减少文件监控对系统性能的影响，同时代理端能够根据宿主机硬件性能和资源占用情况进行自适应调度和优化，充分发挥机器学习算法在多核利用、并行计算、占用资源可控等方面的优势，保证代理

端以轻量级的资源占用实现高安全防护，有效识别和预防各类已知和未知威胁。

◎**下一代人工智能引擎 Protoss™**；人工智能引擎将人工智能、算法和机器学习应用于恶意代码的预测、鉴定和阻止，相比传统引擎具有更快、更强、更轻的特点，在线和离线情况均能够高效预测和预防对终端的已知和未知威胁。人工智能引擎的研发需要依赖于海量恶意样本的积累、高质量训练样本筛选、长期积累的恶意软件特征、机器学习算法的应用、跨平台工程实现，是高技术难度、高开发量、高维护量的工作，充分体现防病毒厂商的综合实力。

◎**强大的持续采集和检测能力**；基于终端强大的信息采集能力（内核态采集，覆盖 Windows 和 Linux 终端行为 20 大类 60 多个子项），依托终端安全大数据平台，以自定义进程唯一 ID 为主线，对攻击者完整攻击行为所采用的攻击步骤进行关联分析，根据攻击事件发生的时间序列，将该次完整的攻击步骤以图形的形式展现，实现攻击场景的重构。通过攻击场景重构的关联规则以及知识的形式化表述，将庞杂、无序的安全数据流转换为结构化、易于理解的攻击场景，将反映攻击过程和意图的场景图呈现出来，从而发现攻击者的攻击策略和目的，甚至推测下一步可能的攻击行为，以便于管理员做出及时有效的应急响应。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：国家计算机病毒应急处理中心计算机病毒防治产品检验实验室

★证书编号：23BD00068-A

★有效期：2023 年 09 月 15 日至 2025 年 09 月 15 日

所属品牌：迪普科技股份有限公司

发布时间：2021 年

产品适用领域：公安、电力、政府、交通、电力能源、科教文卫、大企业、
检法司、运营商

产品照片：



产品咨询邮箱：liandonghai@dpotech.com



产品咨询二维码

奇安信科技集团股份有限公司

奇安信科技集团股份有限公司（以下简称奇安信，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，2022 年营业总收入 62.23 亿元，在人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先；业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年“中国网安产业竞争力五十强”榜单中，奇安信连续三年排名第一。

奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，力争在“十四五”末期成为世界前三的网络安全企业。

网址: www.qianxin.com

电话: 95015

地址: 北京市西城区西直门外南路 26 号院 1 号楼

产品名称：奇安信网神主机监控与审计系统

产品概述

奇安信网神主机监控与审计系统是一款针对信创终端推出的一套主机行为监控与审计系统。能够对计算机进行全面的监控，包括文件的操作行为、外接设备挂载及卸载行为、打印刻录行为以及网络访问等行为进行实时监控，做到事中监控、事后审计，全方位帮助单位加强计算机的安全防护及管理，有效防止泄密事件的发生。系统可结合其它系统，如防病毒系统、终端安全登录系统、准入控制、运维管控、违规外联、多网切换等，共同打造自主可控一体化的解决方案。

功能特点

◎三员管理

默认为三员管理员，分别是系统管理员、安全管理员、审计管理员。系统管理员 (root) 负责系统配置及授权管理；安全管理员 (secadm) 负责安全策略设置及审计日志分析查看等；审计

管理员 (auditadm) 负责对系统管理员、安全管理员的操作日志进行审计。

◎行为监控

系统能够对主机的操作行为的进行实时监控，包括基础环境监控、系统监控、外设监控、进程监控、网络监控、文件监控、网络异常行为监控等。并上报审计日志信息，并对异常行为进行告警阻断，上报告警信息。

◎日志分析

系统能够对审计日志进行统计分析，包括风险占比分析、行为类别占比分析、协议统计分析等。可对统计结果进行排名分析，包括网址访问量排行，违规 IP 统计排行，违规用户统计排行分析，支持对违规部门进行统计排行分析。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405230622

★有效期：2023 年 03 月 24 日至 2025 年 03 月 24 日

所属品牌：奇安信网神

发布时间：2018 年 3 月

产品适用领域：全行业

产品咨询邮箱：kefu@qianxin.com



产品咨询二维码

厦门嘉佑安科信息技术有限公司

厦门嘉佑安科信息技术有限公司（下称：嘉佑安科）位于海上花园城市——厦门，注册资金人民币 1000 万元。在厦门、深圳、武汉三地设有研发中心，是一家致力于打造完善的隐私安全合规产品研发和技术运营管理体系，保护人民隐私安全合规的安全服务商。嘉佑安科母公司是国家高新技术企业、福建省重点上市后备企业、福建省数字经济核心产业领域未来独角兽企业、福建省科技小巨人领军企业、福建省互联网最具成长型企业、厦门十大科创板潜力企业、厦门市重点软件和信息服务企业，现拥有 150 项软著和专利。

公司坚守以“成为人民隐私安全的忠诚守护者”为企业愿景，勇担“保护国家安全、社会和谐稳定、保护人民合法权益”的企业使命，发展规划始终以人民根本利益为中心，通过发挥技术优势、专业的安全服务，为用户、政府、企业、开发者和消费者打造安全、稳固、可信的网络空间生态环境。

网址：<https://www.jusafety.com/home>

电话：18159885118

地址：厦门市思明区湖滨南路 57 号 21A 室 62

产品名称：观澜移动安全平台

产品概述

观澜移动安全平台是服务于企业内部对移动终端设备进行统一安全管理的服务平台。提供一键策略部署、配置、敏感词告警、管理员操作审计、安全策略审计、应用黑白名单等功能模块，辅助企业定时、定量主动获取移动智能终端上的设备信息、系统资源、应用安装、网络、文件、通话记录、短息记录、地理位置等信息，并采用安全加密协议将获取的信息上报监测平台，使得监测管理者能够在平台上规范化的管理企业移动智能终端设备，提高终端管理员对终端监测和管理的工作效率。

功能特点

- ◎策略配置：对于需要监测的设备能够提供集中定制和按组定制的方式下发监测策略。
- ◎敏感词库：支持灵活配置在短信聊天、网络传输过程中需监测和告警的敏感词。
- ◎应用黑名单：支持自主配置需要监测、告警的非授权应用程序。
- ◎设备管理：对受控设备的基本信息、软件安装情况、进程信息、网络使用情况、对文件执行的相关操作、设备的详细定位、通话记录、短信的收件箱及发件箱等进行监测、记录。具

体监测内容如下：

★设备信息监测：监测设备的用户信息、设备自身的相关信息（包括受控移动智能终端的硬件型号、设备序列号、系统软件版本等信息）以及监测的设备在线状态、系统资源（包括CPU、内存使用情况，用户存储空间使用情况，网络流量使用情况）。

★应用清单：监测设备安装的应用情况（包括应用的安装时间、名称、版本等）。

★进程信息：监测设备处于进程中的应用情况（包括运行的进程名称、内存占用大小等）。

★定时定位：支持实时查看该设备的详细定位。

★文件监测：支持对该设备设定的目录范围域或文件的创建、内容修改、移动、复制、删除等操作进行监测、记录。

★网络监测：对设备的网络使用情况进行监测、记录（包括数据传输时间，目标URL，接收、发送的数据内容等）

★通话记录监测：监测设备的通话记录情况、记录（包括来电、来电未接、去电的通信时间、通信号码等）。

★短信监测：监测设备短信的收件箱及发件箱、记录（包括通信时间、通信号码、短信内容等）。

★敏感词监测：监测设备在短信聊天、网络传输内容，若监测到预设的敏感词，则及时记录其次数、具体来源说明。

◎告警管理：提供应用黑名单告警、短信敏感词告警、网络敏感词告警、管理员操作告警。

◎审计管理：提供授权管理员的重要操作记录（包括增加、删除管理员，审计日志管理等）并提供按日期、时间、用户标识等条件对审计日志进行组合查询。审计日志存储在掉电非易失性存储介质中，保证留存时间不少于6个月；当存储空间达到阈值时，会通知授权管理。

技术指标

◎策略配置：对于需要监测的设备能够支持集中定制和按组定制的方式下发监测策略。

◎敏感词库：支持灵活配置在短信聊天、网络传输过程中需监测和告警的敏感词。

◎应用黑名单：支持自主配置需要监测、告警的非授权应用程序。

◎设备管理：支持对受控设备的基本信息、软件安装情况、进程信息、网络使用情况、对文件执行的相关操作、设备的详细定位、通话记录、短信的收件箱及发件箱等进行监测和记录。

◎告警管理：支持应用黑名单告警、短信敏感词告警、网络敏感词告警、管理员操作告警。

◎审计管理：支持授权管理员的重要操作记录（包括增加、删除管理员，审计日志管理等）并提供按日期、时间、用户标识等条件对审计日志进行组合查询。

◎日志通知：支持审计日志存储空间达到阈值时，提供通知授权管理功能。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01111-A

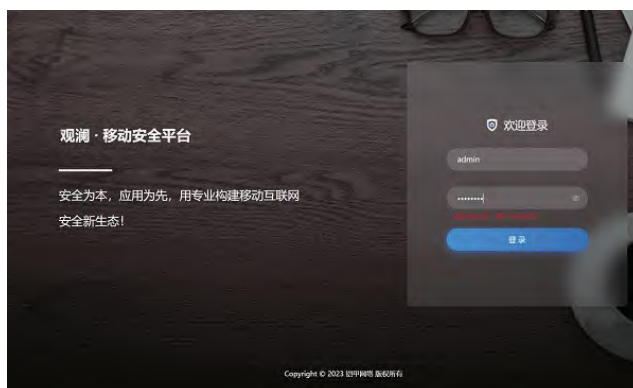
★有效期：2024 年 08 月 02 日至 2026 年 08 月 02 日

所属品牌：观澜移动安全平台 V1.0.0

发布时间：2024 年 7 月 31 日

产品适用领域：教育、通信、政府、能源、军工、制造、金融、软件、互联网等

产品照片：



产品咨询二维码

产品咨询邮箱：jy@kaijia.com

深圳市联软科技股份有限公司

深圳市联软科技股份有限公司创立于 2004 年，专注于企业级网络安全市场，为政企客户提供网络安全产品和服务。深耕金融行业，产品已在银行、保险、证券等金融各细分领域得到广泛应用，在端点安全产品在金融领域市场份额居行业前列，并在制造业、运营商、党政军、医疗、能源和交通等行业构建了较强的市场影响力，已服务超过 3000 家高端行业客户。17 年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、并成为国内率先落地基于“零信任安全”产品的厂商之一。2019 年，联软科技并购魔方安全，获得了以攻击者视角对全网暴露面进行主动持续监控与管理的能力。近 5 年来，联软科技营收以超过 50% 的平均增速在网络安全行业高速增长，并在 2020 年引入中网投、高新投战略投资，正式成为网络安全“国家队”。

网址：<https://www.leagsoft.com/>

电话：0755-86219298

地址：深圳市南山区粤海街道科技园社区科苑路 15 号科兴科学园 A 栋 A2-901

产品名称：联软 ESPP 企业安全监测保护平台软件 (内网主机监测)

产品概述

如今，为应对来自内外部的网络与数据安全威胁，数据防泄露、补丁管理、终端安全、接入认证、基线管理、资产管理等各种安全管理系统在大型机构内部网络中不断部署，这些分散的、不断增多的安全系统加重了管理负担，且因缺乏统一的架构，数据难以集中，系统间缺乏协同，使得安全效果有限。联软科技持续十多年研发，历经多次架构迭代的 ESPP 企业安全监测保护平台专为解决这一问题而设计，通过一个平台，统一框架，数据集中，实现更强更智能的安全保护，减轻安全管理负担，降低采购和维护成本。

功能特点

◎数据防泄露

将网络接入管控、终端与手机设备管控、DLP、沙盒、加密、水印、数据流转管控、文档追踪行为与内容审计等数据管控技术有机整合形成一个覆盖各种场景的数据防泄露体系，防范敏感数据被内部人员泄露或外来黑客窃取。

◎网络防入侵

将网络接入管控、终端与云主机设备管控、木马查杀、异常行为分析、入侵智能诱捕、威

胁情报等安全技术有机整合，形成一个智能化的防内网入侵与态势感知体系，防范外来黑客侵入内部网络。

◎合规与效率

通过网络准入控制、资产自动发现、安全策略强制执行等技术手段，让安全管理规定落地满足等保 2.0 要求，实现安全合规，同时平台下子系统提供多种资产管理、远程运维、Braise 自动化脚本、集中管控等手段，提升 IT 运维效率。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404231411

★有效期：2023 年 6 月 25 日至 2025 年 6 月 25 日

所属品牌：联软科技

发布时间：2015 年 9 月 30 日

产品适用领域：

金融、医疗、制造业、党政军、央国企

产品咨询邮箱：Lrkjzjzc@leagsoft.com



产品咨询二维码

神州灵云（北京）科技有限公司

神州灵云（北京）科技有限公司，成立于2016年，是基于大数据分析平台和人工智能技术，提供网络全流量实时分析和应用业务数据融合解决方案的高科技公司，是国内性能管理和全流量安全的开拓者。神州灵云独创地将全流量实时分析与应用代码级监控技术通过智能综合运维大数据平台进行融合，对网络、应用和业务数据进行建模分析，实现全链路一体化性能可观测。助力客户秒级定位故障位置，查找问题根因，并留存网络原始数据，加速向新一代智能运维 AIOps 转型，重塑 IT 服务价值。

网址：<http://www.dclingcloud.com>

电话：400-058-0958

地址：北京市朝阳区远安南二路2号院大望京中心A座1701室

产品名称：神州灵云内网主机安全检测系统

产品概述

神州灵云自主研发新一代基于大数据技术的内网主机安全检测系统，采用多种技术和机制来检测计算机网络环境中与安全有关的异常和威胁，核心构架设计由“大数据”来驱动，并使用机器学习来执行安全分析以达到传统安全产品无法检测出的未知威胁，且在很多重点行业均取得了阶段性突破。内网主机安全检测系统基于大数据架构使用行为分析算法来分析从端点采集的所有行为数据，能够成功检测出攻击行为，并提供主动防御能力以及溯源取证能力。

功能特点

神州灵云内网主机安全检测系统主要功能：

◎机器学习

机器学习是一门多学科交叉知识，是人工智能领域的核心，专门研究计算机如何模拟实现人类的学习行为，通过获取新的技能知识重组已有的知识体系，并不断完善自身性能。在大规模数据处理中，可以自动分析获得规律，然后利用这些规律预测未知的数据。

机器学习算法的步骤是先利用训练集文件的向量模型及其类别标记生成分类器，其次利用分类模型对待检测数据进行分类检测，通过将检测结果来与真实样本数据进行比对，评估分类器的效果，最后根据结果进一步完善分类器。

内网主机安全检测系统中，机器学习主要应用于端点所有正常行为和异常行为的提取，通过捕获大量的端点静态和动态的行为特征向量，采用机器学习的思想进行端点行为的训练建模和分类检测，得出该使用场景下正常和异常行为知识库，从而利用知识库可以更加高效地检测

出端点的异常行为。

◎日志采集引擎

在内网主机安全检测系统（简称内网主机安全检测系统）中，独有的强大的日志采集引擎采集的端点数据的维度是非常全的，包括进程、文件、网络、注册表等等。端点采集的所有行为数据为端点安全工作中防御、检测、响应以及溯源提供强有力的数据支撑能力。同时对于端点海量数据进行自动智能化的关联分析，追溯其攻击过程，寻找漏洞源和攻击源，是有效防御威胁攻击和确保端点安全的重要途径和方法。

内网主机安全检测系统独有的日志采集引擎的主要目标是不丢失终端安全相关的重要信息，并通过分析原始终端安全数据而形成全局、缜密、连贯的攻击视图。

尤其对于近些年流行的 APT 攻击，针对其极强持续性和阶段性，关联分析过程中应尽量收集各层面、各阶段的全方位信息，同时适量将时间窗口拉大，通过宽时间域数据分析提取具有内在关联的若干属性，识别出攻击发生的时间、地点、攻击类型和强度等信息。

◎主动威胁狩猎

内网主机安全检测系统的数据深度性提供了快速威胁狩猎能力，可以进行深度调查并实现大规模狩猎，可以快速、轻松地查询和流转端点数据。

内网主机安全检测系统可以手动或自动关联所有相关对象（进程、文件、线程、事件等等）。查询时，源进程、目标进程和父进程之间的所有交互都会在跨进程细节中清楚地显示出来。这让威胁分析者能够快速理解数据关系：威胁背后的根本原因及其所有上下文、关系和活动，并使他们能够理解端点上发生的事情的完整故事，并看到完整的事件链。

技术指标

◎基本要求

支持 Windows 全系列：windows xp/7/8/10 全系列，windows server 2003/ 2008/2012/2016 系列；支持 Linux Redhat、CentOS、SUSE、Debian、Ubuntu 等；支持国产化操作系统和国产化 CPU 全面兼容；客户端运行期间 CPU 占有率 <5%；

管理员管理支持系统管理员的角色自定义，支持对锁定账号可支持上级管理员手动解锁；

根据用户业务实际情况，当客户端负载过高时，客户端可自动休眠；

支持随机生成客户端卸载码，客户端卸载时需要输入正确的卸载码才能成功卸载客户端；

支持配置服务器 IP，能够解决在多级部署条件下跨地区移动办公场景、主备机来回切换及更换服务器 IP 等问题；

◎资产管理

支持对主机设为运维状态，避免在主机运维期间产生大量误报事件。运维期间不生成事件，只产生“运维日志”；可对主机设为隔离状态，隔离主机只能和服务器通信；收集主机的资产信息，包括：主机基本信息、硬件信息、软件信息、系统账户、进程列表、端口列表、服务列表、启动项列表、共享环境、环境变量、计划任务、web 站点、web 中间件、web 应用、web 应用框

架、内核模块、系统安装包、jar 包、数据库、容器等；能够对全网资产进行统一资产清点，统计基本资产（进程、端口、服务、启动项、共享、账号、系统安装包）、业务资产及主机资源消耗等信息，支持查看 18 种资产的分类，从主机和资产 2 个维度展示资产详细信息；

◎日志管理

支持采集 70+ 种主机行为日志，日志类型包括但不限于进程、文件、网络、域名、登录、账号、注册表、资源等；支持对日志进行上下文查询；支持对搜索的日志结果自定义创建统计图表，图表类型包括：折线图、面积图、柱状图、水平柱状图、饼状图、环状图、表格、数值图等，可对生成的图表添加至仪表盘操作。系统内置 3 个仪表盘，分别是：登录中心、进程访问和网络连接。每个仪表盘包含多个统计图表，用户无需看复杂的海量日志，只需关注日志仪表盘即可了解系统中主机的运行状况。可对仪表盘进行全屏、编辑等操作，也支持自定义仪表盘；

◎威胁狩猎

能够帮助用户在海量日志中快速检索威胁。支持关键字搜索，多个条件组合搜索，添加条件时可聚合展示对应值，即使用户不了解查询语法也可快速创建查询条件，可保存添加的查询条件，便于后期重复使用该条件，同时系统也内置了多个查询条件；展示日志所有字段，可自定义设置关注字段，设置后，日志列表中会显示关注字段信息。每个字段都可点击统计按钮，对该字段进行字段值、数量及百分比统计，并可对具体每个值进行正选、反选查询。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：24SS01305-A

★有效期：2024 年 9 月 06 日至 2026 年 9 月 06 日

所属品牌：神州灵云

发布时间：2020 年

产品适用领域：能源、政府、金融、医疗、军工等

产品照片：



神州灵云
DCLINGCLOUD



产品咨询二维码

产品咨询邮箱：support@dclingcloud.com

腾讯云计算（北京）有限责任公司

腾讯云计算（北京）有限责任公司（以下简称腾讯云）成立于 2010 年 10 月 21 日，注册资金 14250 万元，在北京、天津、上海、深圳和成都设立分支机构。

腾讯云是腾讯倾力打造的云计算品牌，面向全球的企业、组织、机构和个人开发者，提供全球领先的云计算、人工智能、大数据等产品与服务，是腾讯产业互联网的技术基座与连接器。拥有领先的科技创新能力，连接超过百万的开发者人群；充分开放公众号、小程序等内部生态能力，通过腾讯云启、腾讯千帆等平台计划，并联合包括渠道伙伴等外部生态伙伴，打造产业引擎，助力政务、文旅、教育等各行各业实现数字化升级。

网址：<https://cloud.tencent.com/>

电话：95716 或 4009100100 转 1

地址：北京市海淀区西北旺东路 10 号院西区 9 号楼 4 层 101

产品名称：腾讯 iOA—内网主机监测系统

产品概述

产品通过终端安全、身份安全、链路安全与零信任策略中心联动构建完整的零信任办公体系，对业务访问的整个过程进行持续的权限控制和安全检查，实现终端在任意网络环境中安全、稳定、高效的访问企业资源。

终端的管控是企业的核心需求之一，也是 iOA 产品的核心技术点之一。基础平台构建好之后，针对信创平台 iOA 基于零信任安全理念，高优先级需要支持设备安全。终端管理是设备安全中不可缺少的核心部分。企业通过终端管理实现企业安全基线的一致性，设备的统一性。

功能特点

◎可信身份验证

在对用户授予企业应用的访问权限之前，提供包括企业微信扫码、Token 双因子认证在内的多种身份验证方式，验证所有用户的身份，以防止网络钓鱼和其他访问威胁。

◎可信设备安全

在设备接入内网之前以及接入运行后，通过终端安全管理模块，持续检查设备安全状态，更好地透视与管控企业内网环境，限制任何不符合安全要求的设备对内网的访问。

◎可信应用访问

根据特定用户 / 用户组的职能以及需求授予访问权限，确保用户在接入内网后只能访问到权限内的应用和数据，实行最小权限原则，更好地保护敏感生产环境的访问安全。

◎高级威胁检测与告警

透视全网终端安全态势，秒级发现入侵隐患，云端联动最新威胁情报，对于高级威胁事件即时产生告警、快速响应并极速处置收敛风险。

◎多维度狙击信息泄露

从外设、文件、存储等多维度多层面保护企业敏感数据资产，对终端用户的泄密行为进行记录、告警、阻断，并对终端用户行为进行审计，提高员工保密意识。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0405231608

★有效期：2023 年 06 月 16 日至 2025 年 06 月 16 日

所属品牌：腾讯 iOA

发布时间：2020 年 5 月 15 日

产品适用领域：泛互、金融、政府等

产品照片：



产品咨询邮箱：amerlinwang@tencent.com



产品咨询二维码

天融信科技集团

天融信科技集团（证券代码：002212）创始于1995年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。多年来，天融信基于全产品系列、全业务方向、全行业营销、全区域覆盖的战略发展目标，面向基础网络、工业互联网、物联网、车联网等业务场景持续推出创新性的产品、方案和服务，成为国内自主研发产品品类最全的网络安全企业，形成“一专多强”核心能力，为政府、金融、运营商、能源、卫生、教育、交通、制造等各行业客户提供网络安全整体解决方案。截至目前，天融信已累计荣获2次国家级科技进步奖和7次省部级科技进步奖。同时，天融信防火墙已连续23年位居国内市场第一，VPN、安全服务、安全咨询、WAF、网闸、安全管理、终端安全等产品和服务连续多年位居市场前三，EDR、态势感知、工控安全系列产品和服务均处于领导者地位，IDPS、安全资源池、DLP等产品也位居市场前列。未来，天融信将始终以捍卫国家网络空间安全为己任，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

网址：<https://www.topsec.com.cn>

电话：010-82776666

地址：北京市海淀区西北旺东路10号院西区11号楼东侧天融信科技集团

产品名称：天融信主机监控与审计系统

产品概述

天融信主机监控与审计产品具有集中化、自动化、主动性管理的特征，能够有效的对终端进行主动安全防护和系统管理，系统严格按照等保、分保、国军标关于终端安全管理的技术要求进行设计的终端安全防护产品。在具备系统监控、非法外联检测、软件分发、资产管理、文件安全、移动存储介质管控、补丁管理等功能的基础上，增加了风险管理和主动防范机制，具备完善的终端安全风险监控和分析能力。

功能特点

◎终端行为监控

系统提供了对终端系统的行为进行统一监管，对主机的打印、文件操作、网络访问等行为进行了策略控制，满足了主机、区域安全性的安全需求。

◎终端系统监控

系统提供了对主机系统主要信息（包括进程/服务信息、账号信息、共享信息、注册表信息、软件信息、CPU使用率、系统盘使用率、系统盘可用空间、内存使用率、主网卡接收速率、

主网卡发送速率、系统累计运行时间、网络配置等）进行监视的功能，并通过定制策略对主机的资源、运行状态进行总体监控。

◎终端设备监控

对计算机外设如光驱、打印机、调制解调器、网络适配器、图形图像设备、通讯端口、红外设备、蓝牙设备、1394 控制器、PCMCIA 卡、便捷设备、USB 设备进行控制，通过策略定制限制主机是否允许使用外存设备。

◎移动存储管理

系统通过对移动存储介质写入不同控制权限及功能的标签，对移动存储设备进行标签化管理，区分内部介质和外部介质。并对制定范围内的终端授权，通过策略与标签的配合来实现对移动存储介质的控制。

◎非法外联监控

系统自动检测内网主机的非法外联行为，实时检测内部网络（包括物理隔离和逻辑隔离网络）用户通过调制解调器、ADSL、双网卡等设备非法外联互联网行为，并进行报警、断开网络、自动重启等管控措施。

◎文档检查与跟踪

系统提供了对主机进行文档安全检查及文件操作的跟踪功能。具体如下：

◎敏感信息检查

针对终端存储的 word、pdf、Excel、文本文件等进行全盘关键字检查，并根据策略对含有制定关键字的文档进行禁止发送、禁止打印、禁止拷贝等管控，同时将报警信息上报服务器。

◎文档跟踪

根据扩展名实现对文件操作的跟踪，跟踪文档的拷贝、压缩、解压缩、修改、删除、重命名、移动等行为。

◎双网切换策略

根据主机的网络访问控制能力对终端的内外网访问进行充分隔离，通过主动切换的方式实现终端的对不同网络的安全访问，访问同时对另外一个网络进行阻断，从而保证计算机终端的双网安全使用。

技术指标

支持对 Windows 系统管控及补丁分发

产品运行对 CPU 占用 <2%；内存占用 <20M

支持 B/S 模式管理，支持管理员三权分立。

支持指定主机的补丁检测时间（主机启动时检测或定时检测）、下载的补丁类型（安全更新程序、关键更新程序、工具、更新程序、更新程序集和更新包）、定时下载限速

支持打印监控，可对打印输出的文件设置水印标记，支持水印的自定义配置；支持对打印输出的文档进行二维码信息标记，扫描后可审计出责任人、IP 等信息，协助文档溯源工作。可监控打印服务、本地打印及网络打印行为，并审计打印文件名、时间、人员、页数等信息

支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档等流转方向，并可跟踪文档操作。

网络安全专用产品安全认证或安全检测结果证明

(1) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS038-485

★有效期：2023 年 10 月 11 日至 2028 年 10 月 10 日

(2) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS038-486

★有效期：2023 年 10 月 11 日至 2028 年 10 月 10 日

(3) 网络关键设备和网络安全专用产品安全认证证书

★安全认证机构名称：中国网络安全审查技术与认证中心

★证书编号：CCRC-2023-CS038-487

★有效期：2023 年 10 月 11 日至 2028 年 10 月 10 日

所属品牌：天融信

发布时间：2012 年 12 月

产品适用领域：公检法、政府等

产品照片：



产品咨询二维码

产品咨询：feng_chong@topsec.com.cn

亚信安全科技股份有限公司

亚信安全是中国网络安全软件领域的领跑者，是业内“懂网、懂云”的网络安全公司。承继亚信 30 年互联网建设经验，肩负守护互联网之使命，亚信安全于 2015 年正式启航，目前已成为建设中国网络安全的重要力量。不负使命，成功执行建党 100 周年、历年两会等国家重要网络安全保障任务 30 余次。

依托互联网建设能力，让亚信安全具备强大的“懂网”业务能力与资源优势；深耕网络安全高精技术，让亚信安全拥有优异的“懂云”技术基因。亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理及 5G 安全等领域突破核心技术，用实力筑牢云、网、边、端之安全防线。

亚信安全在中国网络安全电信行业细分市场份额占比第一，连续五年蝉联身份安全中国市场份额第一，终端安全中国市场份额占比第二，在威胁情报、EDR、XDR 等细分技术领域均居于领导者象限，是中国网络安全企业 10 强。

网址：www.asiainfo-sec.com

电话：400-820-8876

地址：江苏省南京市雨花台区花神大道 98 号东久创新中心 1 号楼、2 号楼 3 楼

产品名称：亚信安全终端安全管理系统 AOS-TSM V9.5

产品概述

2023 年 6 月，新一代终端安全 TrustOne 正式发布，极简新主义的创新理念为数字变革而来。以终端为支点，连通身份安全、业务安全以及数据安全的技术能力，亚信安全 TrustOne 完成了从防护功能的破局；围绕企业业务数智化的发展路径，从三大方面实现了终端安全立体化的革新。

功能特点

◎安全左移 强化暴露面收敛

TrustOne 采用持续威胁暴露面收敛（CTEM）技术，聚焦终端、身份、业务和数据的暴露面问题，持续发现企业的影子资产、高危漏洞、高危端口、弱密码等风险，进行智能评测风险等级，可视化 & 量化风险，从而最大化的减少入侵威胁，提升防护效率。

◎AI 加持 治理智能化威胁

面对智能化的高级威胁攻击，亚信安全 TrustOne 借助 AI 技术，完成了防御效率的全面提升。强化了未知威胁应对，能在分钟内处置最新攻击，并优化漏报与误报，确保 100% 告警分

析，持续提高检测精准度。

◎锚定业务 数据驱动高效运营

利用 SaaS 化订阅的服务模式，亚信安全 TrustOne 安全运营功能将完成质的提升。利用 AI 技术赋能安全运营，TrustOne 威胁告警响应时间从 4 小时提升至分钟级，将安全事件闭环时间 (MTTR) 从 2 天缩短至 10 分钟，海量终端安全告警缩减并精确至真实威胁，威胁研判准确率提升至 99%。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部第三研究所

★证书编号：23SS00073-A

★有效期：2023 年 9 月 15 日至 2025 年 9 月 15 日

所属品牌：亚信安全

发布时间：2023 年

产品适用领域：金融、企业、政府机构、制造业、医疗、运营商等等

产品照片：



产品咨询二维码

产品咨询：sec-business@asiainfo-sec.com

浙江远望信息股份有限公司

远望信息成立于 2004 年，公司主要从事政务网络安全防控体系及相关安全产品的研发、生产、销售和安全运营服务。公司专注于政府和企事业单位的网络安全管理领域，是数字政府安全防控体系构建的引领者，国内领先的网络安全整体解决方案供应商。公司产品覆盖政务网络安全、视频专网安全、保密安全、信创安全四大领域。

公司长期致力于“网络安全防控体系”思想、方法研究，前瞻性提出“以管理之道破解网络安全难题”的理念，历时十多年打造了数字政府安全防控体系；并立足“资产明晰化、风险可视化、管理信息化”三大方向的核心技术，自主研发了 40 余款安全产品，实现了对数字政府安全防控体系落地的全面支撑。

网址：www.cnywinfo.com

电话：400-826-1595

地址：杭州市滨江区启智街 89 号山科智能大厦 13 层

产品名称：远望主机监控与审计系统

产品概述

远望主机监控与审计系统是面向办公网推出的以安全管控为核心、以实时监测为支撑的全方位主机安全解决方案，构建能够有效监控非授权违规外联、违规软硬件安装、杀毒软件安装、外部设备使用的主机安全监测与管控体系。从终端基础安全、运行安全、应用行为安全、数据出口安全多维度保证内部数据安全，实现终端系统的全面安全防护和加固，保障内部网络安全。

功能特点

◎终端基础安全监测：监测终端的系统账户情况（包括弱口令、空口令、过期账户、无用账户）、开关机状态变化情况、软硬件变更情况、杀毒软件安装和运行情况、不合规软件安装和运行情况、无线网卡启用情况、风险进程运行情况等，发现异常进行告警。

◎终端运行安全监测：监测终端的 CPU 使用情况、内存占用情况、磁盘使用情况、网络流量情况的监测，及时发现运行异常情况进行异常告警。

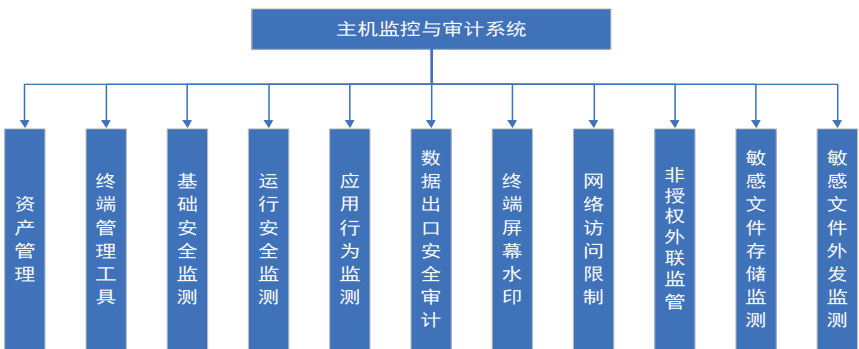
◎终端应用行为安全监测：监测终端用户游戏娱乐行为、下载行为、聊天行为、炒股行为、视频应用行为、挖矿行为、远程控制软件使用行为，记录行为审计日志。

◎终端数据出口安全审计：实现终端用户打印、刻录等行为的日志记录和禁用管控；FTP 访问、TELNET、远程协助、启用文件共享、移动存储介质使用等行为的日志记录；USB 设备、磁盘驱动器（USB 类型）、DVD/CD-ROM 等外设的接入审计和禁用管控。

◎终端屏幕水印：屏幕水印通过策略配置驱动，支持内容直接展示、二维码展示、点阵展示三种展示水印模式，支持水印内容项、水印样式的配置。支持根据水印内容进行溯源定位设备基本属性信息。

◎终端网络访问限制：支持制定防火墙策略、微隔离策略、分时上网管理策略限制终端的网络访问权限。

◎非授权外联监管：监测终端违规外联事件，控制外联持续发生和预防外联的发生。



产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

证书编号：0405231796

有效期：2023 年 06 月 21 日至 2025 年 06 月 21 日

所属品牌：远望

发布时间：2018 年

产品适用领域：政府、能源、金融、运营商、医疗、教育、企业等

产品照片：



产品咨询二维码

产品咨询：mail@chinayuanwang.com



电子文档安全管理产品

北京亿赛通科技发展有限公司

北京亿赛通科技发展有限公司（以下简称：亿赛通）成立于 2003 年，是绿盟科技（证券代码：300369）全资子公司。近二十年的风雨兼程，已成功打造为数据安全领域专业的综合数据安全厂商，是国家双高新企业，并获得工信部“专精特新”小巨人企业认证。签约用户过万家、800 余万终端用户，连续多年获得 CCID、IDC、中国信通院等专业机构的高度认可。

亿赛通以“分·放·管·服”数据安全建设理念为核心，以技术为支撑，对综合数据、商业数据、视频专网数据、工业数据、大数据、云数据等进行全方位多维度管理，保障各行业客户核心数据资产安全。全线产品覆盖云、网、端三大类应用场景，60 款 + 精细化产品模块，支持结构化、非结构化和半结构化数据安全治理，打造集数据安全合规、数据安全治理、数据安全防护、数据安全流转、数据库安全、安全服务为一体的数据安全领域综合解决方案。

作为拥有完全自主知识产权并取得多项国家资质认定的双高新技术企业，亿赛通现拥有产品资质 200 余项、企业资质 150 余项、荣誉奖项 300 多个、成为 50 多家联盟协会专业会员，为多个数据安全项目输送专家，参与国标、行标、政府报告及行业研究报告等 30 多项。

网址：www.esafenet.com

电话：010-57933766

地址：北京市海淀区西二旗大街 39 号 4 层 401

产品名称：新一代电子文档安全管理系统

产品概述

亿赛通新一代电子文档安全管理系统（简称：CDG）采用一体化平台架构设计，融合文档加密、分级管理、访问控制、关联分析、大数据分析、智能识别等核心技术，提供软硬一体全新产品形态，包含透明加密、智能加密、权限文档、数据分级管理、桌面安全管理、文件外发管理、集团管控、数据安全网关、加解密接口中间件、U 盘客户端十大核心组件，保护范围涵盖终端电脑（Windows、Mac、Linux、国产化（KOS、UOS）系统平台）、智能终端（Android、IOS、鸿蒙）以及各类应用系统（OA、知识管理、文档管理、项目管理、PDM 等）。产品从注重防护走向注重数据治理，从治理层面准确摸清企业敏感数据分布与流动态势；能够基于数据价值进行分级管理，将有限资源准确集中到重点敏感数据的使用和保护中；以用户为中心，对解密、外发、传播、违规操作等各类场景进行多维度、持续性安全监测、响应处置和溯源审计；从数据采集、处理、流转及存储四个阶段，全面剖析数据全生命周期过程中的问题和风险，打造动态防御体系。同时，产品满足超大规模应用，支持总分部数据互联互通以及安全策略统一集中管控，并全面兼容国产操作系统、CPU、数据库和基础应用软件，全方位保障用户终端数

据安全。

功能特点

◎文档加密：透明加密、半透明加密、智能加密、全盘扫描加密、落地加密、特权加密、浏览器上传下载加解密、流转工具批量制作加解密文件。

◎文档内容安全管理：内容安全控制、打印控制、打印水印、阅读水印。

◎数据分级管理：分类管理、分级管控。

◎文档外发安全管理：邮件外发审批、邮件白名单、邮件解密、外发管理。

◎权限管理：数据作者可以根据需要设定数据的传播范围（用户、部门、项目组等）和查看权限（只读、打印、修改、阅读次数、阅读时长），也可以根据企业需要建立权限模版，对文档批量授权。

◎流程管理：用户可以使用客户端工具或者直接右键点击文档发起申请流程，通过进入我的工作台链接到服务器页面查看申请流程情况，【我的申请】中可以查看已申请的流程表单；【我的待办】中可以查看需要我审批的流程表单信息；【我的已办】中可以查看已经审批过的流程表单。

◎桌面管理：终端环境管理、资产管理、软件管理、移动存储介质管理、终端行为管理、远程运维、安全监控审计、报表管理。

◎集团管控：基于 CDG 分布式系统架构方案，能够实现总部与分部之间的数据互联互通，可以将各个分部的组织架构、密钥、安全策略及用户信息定时同步至集团总部，方便总部统一集中监管。

◎防勒索：文件访问控制、文件安全防护、应用签名准入、恶意软件预警。

◎应用安全网关：应用安全网关可以为应用系统提供安全准入和数据加解密双重防护，安全准入通过终端身份识别、应用系统仿冒、传输隧道加密、终端访问日志等多方面进行应用数据安全访问控制，数据加密通过对应用系统核心数据进行上传解密、下载加密，解决企业核心数据离线安全使用。

◎安全中间件：安全中间件提供了统一、标准的 API 接口，可以为第三方应用系统提供加解密、EOD 外发文档制作、第三方流程审批集成的能力。

◎智能移动终端：为智能移动设备提供亿赛通专属 APP 安全服务，保证通过移动设备下载到客户端的加密数据可以正常查看，脱离受控范围无法使用。此模块一般与透明加密、应用安全网关或安全中间件等配合使用。

◎全文检索：全文检索系统，通过对流程审批（解密流程、外发流程）的文档进行内容解析，建立文档数据索引，日志管理员通过输入文档关键字内容，即可快速查询出包含相关内容的流程及文档，实现文档附件与流程的动态关联与查询。

技术指标

◎ CDG-N1：最大管理终端数 50；型号：1U；CPU：4 核 4 线程；存储：1*2T，可扩展到（1*8T）；内存：8G；网络：2 个千兆电口；电源：60W 单电源；亿赛通 Linux 操作系统、专业化数据库（MYSQL+ES）、CDG 服务端管理系统。

◎ CDG-N3：最大管理终端数 600。设备型号：2U；CPU：4 核 8 线程；存储：2*2T（Raid1）可扩展到（2*8T）；内存：16G；网络：2 个千兆电口（可扩展 2GE/2SFP）；电源：300W 双电源；亿赛通 Linux 操作系统、专业化数据库（MYSQL+ES）、CDG 服务端管理系统。

◎ CDG-N5：最大管理终端数 5000。设备型号：2U；CPU：20 核 40 线程；存储：3*4T（Raid5）可扩展到（8*8T）；内存：64G；网络：2 个千兆电口（可扩展 4GE/4SFP）；电源：550W 双电源；亿赛通 Linux 操作系统、专业化数据库（MYSQL+ES）、CDG 服务端管理系统。

◎ 文档加密：支持应用软件：office2007/2010/2013/2016（专业版、家庭和学生版）/2019（专业版、家庭和学生版）/2021（专业增强版）/office365（家庭版/商业标准版/企业版 E3）、AdobeReader8/9/10/11、Adobe Acrobat Reader、WPS2016 个人版/2019 个人版/WPSPro_11.8.2.8875wps2019 专业版、WPS11.8.2.8411_LSYH_1.2wps2019 专业版、WPS（11.1.0.11636、11.1.0.12763、11.8.2.11019）、AutoCAD2014/2016/2018/2019、Photoshop（cs6、cc2018、cc2020）、福昕 PDF 阅读器（V10.0.124.36236、V12.0.126.13146、V12.1.210.16090）、福昕高级 PDF 编辑器（V9.1、V10.1.0.37527、V11.0.0.49893）、福昕 PDF 编辑器个人版 V10.0.226.36120、中望 CAD 2020 企业版、万兴 PDF 企业版。

文档类型：doc、docx、xls、xlsx、ppt、pptx、pdf、dwg、psd、bmp、gif、jpg。

支持在 qq、微信、企微、钉钉、Foxmail、Outlook 等第三方软件内直接打开密文。

产品安全认证或安全检测结果证明等

计算机信息系统安全专用产品销售许可证

★证书编号：0404230700

★有效期：2023 年 3 月 31 日至 2025 年 3 月 31 日

所属品牌：北京亿赛通科技发展有限公司

最新版本发布日期：2023 年 8 月 1 日。

产品适用领域：政府、金融、新能源、医疗、芯片

产品照片：



产品咨询邮箱：liucunwei@esafenet.com



产品咨询二维码

深圳市联软科技股份有限公司

深圳市联软科技股份有限公司创立于 2004 年，专注于企业级网络安全市场，为政企客户提供网络安全产品和服务。深耕金融行业，产品已在银行、保险、证券等金融各细分领域得到广泛应用，在端点安全产品在金融领域市场份额居行业前列，并在制造业、运营商、党政军、医疗、能源和交通等行业构建了较强的市场影响力，已服务超过 3000 家高端行业客户。17 年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、并成为国内率先落地基于“零信任安全”产品的厂商之一。2019 年，联软科技并购魔方安全，获得了以攻击者视角对全网暴露面进行主动持续监控与管理的能力。近 5 年来，联软科技营收以超过 50% 的平均增速在网络安全行业高速增长，并在 2020 年引入中网投、高新投战略投资，正式成为网络安全“国家队”。

网址：<https://www.leagsoft.com/>

电话：0755-86219298

地址：深圳市南山区粤海街道科技园社区科苑路 15 号科兴科学园 A 栋 A2-901

产品名称：联软 UniDES 文档安全管理系统

产品概述

联软 UniDES 文档安全管理系统（以下简称 UniDES），是企业电子文件提供全生命周期安全保护和有效管理的解决方案，采用智能安全分析技术、操作系统内核技术、高强度的加密算法、灵活易用的安全策略，可以有效防止内部员工泄密和外部人员非法窃取企业核心重要数据资产。

UniDES 采用主动的智能安全加密策略，以透明加密技术为核心，利用高强度加密算法实现智能透明加密，系统综合集成了动态透明加密、文件内容识别等多种尖端技术，从文件创建到删除的整个生命周期内对其进行智能化的安全保护，有效控制终端用户对文件的读取、存储、复制、截屏、输出等使用权限，从而防止使用者之间的非法复制、非法截屏、非法流转、光盘拷贝，在不影响用户工作习惯及业务效率的同时，有效防止企事业单位核心信息资产外泄，在安全性和方便性之间找到了一个非常好的平衡点。

UniDES 可根据用户需求对电子文档进行自动加密、手动加密、智能加密和文档细粒度权限控制，对文档的全生命周期进行安全管控，做到事前防御、事中控制、事后审计，帮助企业搭建一套完善的文档防泄密体系，并且 UniDES 可与防火墙、防病毒、防水墙等安全产品完全兼容使用，可从“内部控制”层面对现有安全系统进行重要补充，因此 UniDES 可从信源上保证安全，在安全系统中起到不可替代的作用。

功能特点

◎文件加密

提供透明加密、强制加密、只读加密等多种加密方式，适应不同的办公场景；

基于文件内容识别技术，针对敏感文件进行加密，非敏感文件不加密；

对终端的文件提供下载加密、手动加密和批量加密功能；

结合上网审计功能，实现上传文件解密、下载文件加密效果；

通过邮件客户端、网页端发送邮件存在附件时，对邮件附件进行敏感检测，敏感数据则发送加密文件，非敏感数据则发送明文文件。

◎文档密级管理

对文档进行密级管理，最多可设置 9 个密级，用户只可以打开等于或低于自己密级权限的文档；

赋予高密级的人员修改文件密级的权限，低密级的人员赋予申请修改文件密级权限，以此进行更精细化灵活的权限控制。

◎访问权限控制

用户在获取授权文档后，根据文档的设置权限生效自身可操作范围，有效的杜绝了越权操作的行为；

加密文件打印权限控制，开放打印权限的用户需实现可追踪审计、限定打印机防止虚拟打印；

企业权限分配遵从“最小权限原则”，普通用户终端只有平时办公所用到的基本权限，一般没有解密、外发等权限；普通用户需要使用审批功能，由领导审核后，才能获得相应权限。

◎文件外发

用户获得加密文件外发权限，对文件权限进行设置后将文件外发，得到加密外发文件的用户在权限验证通过后方可打开文件；

用户可申请将加密文件进行明文外发；

◎设备离线办公

终端助手离线时，拥有脱机使用权限的终端才能使无障碍使用加密文件，没有脱机使用权限的终端需进行申请方可获得权限，否则将无法打开加密文件。

网络安全专用产品安全认证或安全检测结果证明

网络安全专用产品安全检测证书

★安全检测机构名称：公安部计算机信息系统安全产品质量监督检验中心

★证书编号：23SS00071-A

★有效期：2023 年 9 月 15 日至 2025 年 9 月 15 日