2022年
中国网络安全行业白皮书

2022.08

目录

目录

目录

名词解释

- **APT：**高级长期威胁（Advanced Persistent Threat）的英文简称，是由攻击者针对特定目标，使用复杂恶意软件和恶意技术隐匿于业务计算系统中的漏洞，该类漏洞普遍具备高级、长期、威胁三个核心要素。
- **FTP服务器：**文件传输协议服务器（File Transfer Protocol Server）的英文简称，是基于FTP协议为互联网用户提供文件存储和访问服务的计算系统，支持用户通过计算机与各地区FTP协议服务器连接，实现对程序与信息进行访问或上传的目标。
- **DNS：**域名服务器（Domain Name Server）的英文简称，是支持域名与相应IP地址转换的服务器，本质为承载域名系统的主机，支持分层结构下的域名解析。
- **DDoS：**分布式拒绝服务攻击（Distributed Denial of Service Attack）的英文简称，实现原理为处于不同位置的攻击者主动或被动（受控制）同时向特定目标发动攻击，消耗被攻击系统网络带宽或系统资源，导致被攻击者业务系统中断或瘫痪的攻击类型。
- **DevOps：**过程、方法与系统（Development & Operations）的英文简称，是应用程序和软件开发过程中一组过程、方法与系统的统称，有助于促进系统构建、测试、发布流程的效率和可靠性。
- **SMB：**服务器信息块（Server Message Block）的英文简称，是用于Web连接和客户端与服务器之间进行信息沟通的一种局域网文件共享传输协议，是构建共享文件安全传输平台的基础。
- **WAF：**Web应用防护系统（Web Application Firewall）的英文简称，亦称为网站应用级入侵防御系统，是通过执行一系列针对HTTP、HTTPS的安全策略，专门为Web应用提供保护的安全产品。

中国网络安全行业概况

- 未来5年，中国网络安全产业将依托云计算技术，在端点安全、移动安全、云原生安全领域实现强势增长。
- 预计2022年，中国网络安全产业软件市场规模约达145.2亿元，硬件市场规模约达295.2亿元，安全服务市场规模约达258.43亿元，云安全市场规模约达155亿元。
- 相对硬件部署模式时期，未来，中国网络安全产品将以软件和云端为主流部署模式，逐渐呈现出竞争集中、收并购加码的发展态势。
- 相关法规升级和实施催生大量网安服务采购需求，为网络安全行业营造规范的发展环境。

定义与特点

网络安全定义与特点

网络安全的定义

网络安全在范畴上覆盖计算机网络运行环境安全和通信网络运行环境安全。网络安全服务商通过硬件模式、软件模式及云部署模式的安全防护手段，协助用户避免或减少因外部恶意行为、内部违规操作行为造成的信息资产泄露、损毁、丢失、篡改、窃取、勒索等安全事件。在企业资产数字化进程加速的背景下，网络安全防护工具全面上云。

传统安全

- 硬件模式
- 软件模式

云上安全

- 云端部署模式
- 部分软件模式

云上计算和存储资源为用户在网络环境下执行动态防御策略提供基础设施

云计算 + 云存储

全面监测安全态势
采集恶意活动路径
云安全中心分析
解决方案统一发送

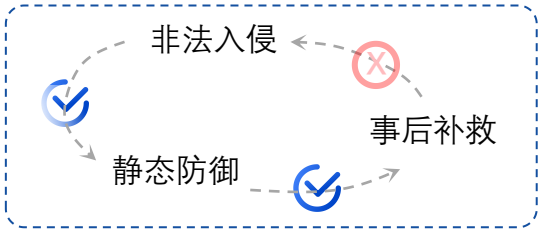
- 形成系统化检测方案、防御方案
- 应对Web3.0时代数据安全及隐私保护需求

网络安全防护特点

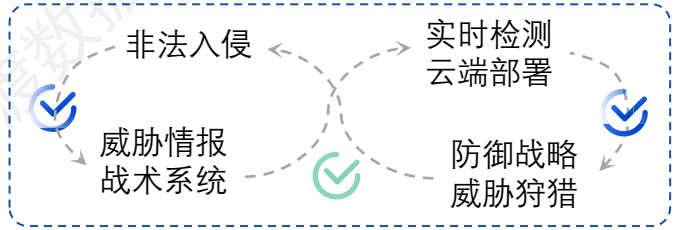
随国家网络安全等级保护标准的升级（目前为等保2.0）以及《网络安全法》、《数据安全法》、《个人隐私保护法》等相关法律法规的正式施行，网络安全防护理念从损失补救和静态防御逐步发展为“事前防御、动态防御”。

防护特点：从静态防御向动态防御进阶

静态：非闭环防护，信息孤立



动态：构建系统化防御机制，知己知彼



防护要点：攻防态势可视化、防护系统精细化、功能模块高度集成

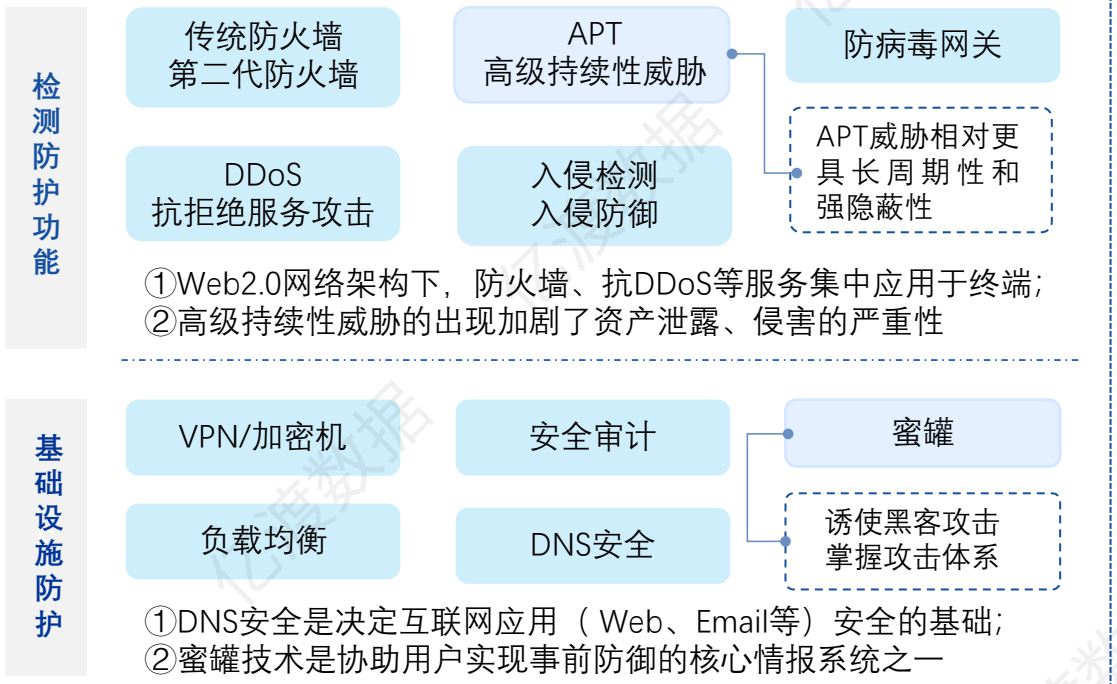
	要点解析	要点呈现
可视化	①流程可视：攻防过程全景态势； ②数据可视：实时监测攻防表现	呈现攻击源头、攻击周期、攻击战术等信息，降低攻防模型抽象性
精细化	主要体现在情报系统、数据标签、功能模块定义及定价模式等方面	情报系统、事件信息颗粒度细化；根据配置规则、数量、版本等细化定价
集成化	融合DevOps等技术理念，强化功能模块之间的联动和集成	攻击行为与防御对策之间联结深化，构建安全模块之间的防护闭环

网络安全产业核心产品及服务全景架构

网络安全产业核心产品及服务架构（1/6）

网络安全产品及服务通过采用检测、监测、扫描、溯源、查杀、审计等手段，协助用户抵御来自外部的恶意行为或来自内部的违规行为，避免业务资产和系统资产遭到入侵、损毁、泄露、篡改、窃取、丢失、勒索等威胁。从防护层面进行分类，当前网络安全产品主要覆盖基础架构安全、端点及应用安全、身份安全、移动安全、云安全、物联网安全及安全运维等。奇安信在基础架构安全层面的业务覆盖面相对较广。

▪ 基础架构安全



产品类别	头部服务商	其他服务商
传统防火墙 第二代防火墙	深信服、奇安信、启明星辰、华为、安恒信息、新华三等	迪普科技、天融信、山石网科、东软、安博通、交大捷普、亚信安全等
入侵检测防御	绿盟科技、启明星辰、奇安信、天融信、深信服、安恒信息等	交大捷普、东软、山石网科、迪普科技、蓝盾、紫光恒越、中科网威等
防病毒网关	奇安信、亚信安全、360安全、天融信等	江民科技、猎鹰安全、冠群金辰、瑞星等
VPN/加密机	奇安信、天融信、深信服、启明星辰、迪普科技等	东软、江南信安、渔翁、信大捷安、立思辰、国泰网信等
安全审计	奇安信、启明星辰、绿盟科技、深信服、天融信、任子行等	蓝盾、紫光恒越、安博通、锐捷、安信天行、安博通、观安等
抗DDoS	绿盟科技、奇安信、天融信、华为、新华三等	盛邦安全、迪普科技、中新网安等
抗APT威胁	奇安信、深信服、启明星辰、腾讯安全、亚信安全等	神州网云、一知安全、兰云科技、金睛云华、中睿天下、东巽科技等
应用交付/ 负载均衡	深信服、奇安信、天融信、新华三、山石网科等	迪普科技、太一星晨、信安世纪等
网络准入控制	联软科技、新华三、中孚信息、宁盾等	画方、盈高科技、金盾、广州世安、艾科网信、阳途、远望信息
蜜罐	安恒信息、长亭科技、知道创宇、青藤云安全、天翼安全等	默安科技、峰台科技、经纬信安、永信至诚、非凡安全等

注：表格中厂商名称不分排序先后，仅因涉及相关安全业务而被列入

网络安全产业核心产品及服务架构（2/6）

端点安全：在移动办公普及的背景下，平板电脑、笔记本电脑、智能手机等多元移动设备接入，让结构化网络暴露在更多恶意攻击之下。当前，中小型企业对端点安全重要性认知不足，远期，端点安全解决方案需要覆盖所有连接到企业网络的端侧设备。

应用安全：针对应用程序在运行过程中可能出现的数据窃取、泄露等问题，提供软件、硬件工具，常见防护模式包括**应用虚拟化**和**远程接入**等。

▪ 端点安全及应用安全

端点安全

- 端点保护平台（EPP）将朝着精简和集成的方向发展，应对端点的安全独特性，最终实现终端安全一体化；
- 约70%的系统漏洞起始于端点设备

终端检测响应

- 头部安全服务商均布局终端检测响应平台EDR，具备终端行为学习能力
- 实时监测终端运行状态，实现防护、管理、分析、整合四方面的组合运用

防恶意软件

- 依托云端备份、安全规范建立、访问权限限制、集中式补丁管理、威胁提取、威胁模拟等手段，确保端点安全

主机加固

云主机安全是主机加固的迭代；产品形态逐渐融入云架构；威胁溯源、微隔离等功能加成

linux主机　Windows

- 用户通常拥有大规模服务器集群，服务成本达到千万级别，且周期较长

终端安全管理

- 主要包括域控统一管理、系统漏洞补丁更新、安装软件合规、操作系统账号安全等
- 确保接入网络的移动终端符合使用规范和安全防范规范

应用安全

- 应用程序内置安全防护措施，常见的软件对策以防火墙、访问控制、防病毒、密码策略等；
- 企业在部署网络层安全防护策略之余，不可忽视应用层安全，宜部署完整的应用安全管理系统

Web应用层防护对策

Web应用防火墙

- 网络前端部署，突破传统架构
- 代表企业如绿盟科技、安恒信息、奇安信、启明星辰等

Web应用扫描

- Web应用程序扫描工具和监控工具，覆盖指纹识别、代码审计、防暴力破解、数据收集等功能

网页防篡改

网页防篡改技术经历了3轮迭代，针对增删改查行为进行实时拦截和阻断

页面轮询检测对比 → 内核驱动底层过滤

邮件安全

邮件传输基于SMTP协议进行，通过邮件的APT攻击、勒索加剧

以防钓鱼、防病毒、安全审计、邮件过滤等措施为核心

API安全

API接口漏洞将导致数据、图片等用户隐私泄露，API防护重点在于通信加密

包括可信身份令牌、加密签名、漏洞主动识别、API网关等措施

网络安全产业核心产品及服务架构（3/6）

身份系统是信息安全系统的核心，身份安全防护服务的核心在于用户身份认证、设备指纹认证、授权机制构建和维护等。系统化的身份治理平台已成为企业的基础安全平台。身份安全系统面临的核心威胁在于隐私侵犯、解决方案完整性不足和可用性不足等方面。当前，中小企业普遍缺乏搭建身份安全系统的能力，云基础设施的渗透和云原生技术的应用助力新型身份安全服务（如IDaaS）在B端和C端的普及。

- **身份安全** 身份安全领域呈现出较为明显的买方市场特征，头部云厂商加速入局，传统服务商面临来自用户侧、竞争侧双重压力

身份认证与权限管理	认证授权系统通过秘钥、生物特征等验证手段等确认用户身份，根据授权机制赋予权限	• 代表服务商：绿盟科技、奇安信、芯盾时代、阿里云、竹云等 • 其他服务商：景安云信、安讯奔、信安世纪等
运维审计堡垒机	堡垒机的前身为前置机，主要包括商业堡垒机和开源堡垒机，监控并审核运维人员对网络的操作行为	• 代表服务商：安恒信息、深信服、绿盟科技、齐治科技等 • 其他服务商：中信网安、建恒信安、帕拉迪、思福迪等
特权账号管理	针对高级权限系统账户保管和操作不善导致的信息泄露、恶意破坏而进行动态和自动化管理	• 代表服务商：安达亚、海颐安全、尚思卓越、江南科友等 安讯奔、齐治科技、帕拉迪、格尔软件等
数字证书	依托加密、解密、数字签名、签名认证等基础程序，数字证书保障数字传输进程的权威性和安全性 中国仅有约50家企业具备发放数字证书的资格	• 代表服务商：数字认知、吉大正元、安信天行等 • 其他服务商：格尔软件、牙周诚信、国富安、信大捷安等
硬件认证	硬件认证是电子认证领域的细分市场，服务机构普遍规模较小	• 代表服务商：天飞诚信、海泰方圆、龙脉科技、林果科技、宁盾、华大智宝、芯盾集团、神州融安

网络安全产业核心产品及服务架构（4/6）

移动安全防护对象为移动设备，具体防护方向包括APP漏洞挖掘、移动应用加固、移动应用逆向、移动平台漏洞挖掘、移动平台加固、移动环境病毒木马查杀拦截等。**物联网安全系统**可解决存在于物联网系统中的终端安全问题，与智慧城市建设同步前进。依托可视化管控、身份认证和授权、强制性安全策略等手段，物联网安全信任链逐渐成型。未来5年，物联网领域安全服务渗透率将成指数级增长。

▪ 移动安全及物联网安全

市场机遇：传统移动安全领域产品多采取非付费模式，但随消费者对安全产品认知提升和对付费模式接受度提升，未来移动安全市场或迎来新机遇

	产品形态	定义	代表服务商
	移动终端安全	应对终端漏洞和病毒提供加固、查杀等服务，保护移动端用户信息和隐私安全	梆梆安全、奇安信、天融信、芯盾集团、爱加密、几维安全等
	移动应用安全	针对间谍应用程序、银行恶意应用程序等终端恶意程序，为用户提供威胁防护方案	梆梆安全、爱加密、腾讯安全、海云安等
	移动安全管理	移动安全管理平台通过合规管理、业务感知、数据分析、威胁可视化展示等手段，对移动端应用进行安全加固	深信服、亚信安全、天融信、奇安信、联软科技、东软、信大捷安、爱加密等

物联网安全：针对物联网感知层、传输层、应用层、网络层可能面临的数据安全、隐私侵犯等威胁提供从端到面的安全防护解决方案

智慧联网驾驶系统安全对社会治安、生命安全产生直接影响，车联网系统或存在跨境数据安全问题

车联网安全

- 代表厂商：启明星辰、百度安全、360安全、东软、观安、天融信、信长城、银基等

覆盖前端接入安全、横纵业务安全、边界隔离安全等维度，确保精细化的访问控制、物联网应用识别及安全策略的优化

其他专网、物联网安全

- 代表厂商：天融信、天防安全、金盾、万物安全、云盾科技、信大捷安、北信源、安点科技等

网络安全产业核心产品及服务架构（5/6）

依托云计算架构、云基础设施在并行处理、网格计算等方面的优势，云安全服务为用户提供实时、自动化、多维联动的威胁抵御策略和安全事件处置策略。用户无需花费高额成本自行组建安全团队，可依托云服务共享模式，以较低成本和较高灵活性获取7*24的云端安全系统。当前，头部云厂商基于自身在云计算领域的技术积累，可真正实现安全防护服务的云化，其他服务商提供的云安全产品多停留在功能的镜像复制阶段。

- **云安全**

公有云安全：以中小企业用户为服务对象，助力用户实现业务负载从终端向云端的顺利迁移，进而推动IT架构的优化及用户核心业务创新；
私有云安全：面向私有云环境和混合云环境的大型政企用户，结合独特的业务环境，统一监控和管理云环境内安全情况

01 **云安全资源池**

安全能力池化的实现核心在于虚拟化环境的利用，可覆盖防火墙、身份认证、入侵检测、日志审计等多元化功能

- **代表厂商：**
深信服、奇安信、安恒信息、浪潮云、绿盟科技、新华三等

02 **微隔离**

微隔离技术区别于防火墙隔离技术，依托分布式、自适应架构，通过更细粒度实现非单点的流量监测和管理

- **代表厂商：**
蔷薇灵动、阿里云、腾讯云、观安、安全狗、青藤云安全、上元信安、云溪等

03 **IDaaS**

IDaaS部署模式在本质上与传统IAM服务逻辑一致，但在服务效率、服务灵活性、部署成本等方面具备显著优势

- **代表厂商：**
上海申石、阿里云、竹云、听云、玉符科技、宁盾、芯盾时代、派拉软件、安讯奔等

04 **云抗DDoS&云WAF**

云端防火墙和云抗D服务通过分布式架构实现集群防御、主动防御的目标，能够抗击更大规模流量攻击，依托更加轻量化的部署完成流量隔离

- **代表厂商：**
知道创宇、腾讯云安全、白山云科技、浪潮云、网宿科技、云盾智慧等

05 **云主机安全**

云主机安全是云端的第二道防火墙，通过资产清点、入侵检测、基线合规、风险发现等功能模块实现对云主机的全方位防护

- **代表厂商：**
青藤云安全、山石网科、安全狗、椒图科技、阿里云、杰思安全、腾讯云安全等

06 **容器安全**

容器环境安全建设主要涉及容器云内部基础设施安全、数据安全以及容器与外部环境的通信网络安全

- **代表厂商：**
青藤云安全、小佑科技、安全狗、默安科技、山石网科、观安、腾讯云安全等

网络安全产业核心产品及服务全景架构

网络安全产业核心产品及服务架构（6/6）

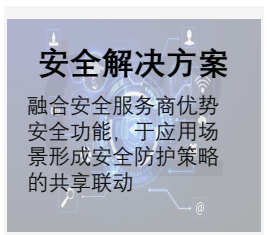
安全服务体系应用于从开发到应用的软件全生命周期，包括安全运维（向云上运维演进）、渗透测试、应急响应、安全众测、红蓝对抗等能力，而随安全合规等级升级和用户对安全防护效力落地重视度提升，通用安全服务应用场景和行业级安全解决方案应用场景均体现出理念升级和模式演变的特征，并与下游场景业务特征相结合，形成贯穿于纵向业务流程和横向组织架构的安全服务体系。

- **安全运维及其他安全服务**　**运维管理及安全系统要点：**构建适合应用场景核心业务需求的安全事件处理系统和流程

安全服务集成&上云

安全集成管理系统的建设以信息系统安全工程建设方法为依据，从安全需求分析、安全配置、防护流程设置、防护策略部署、安全效力评估等角度出发，对网络侧、端侧、移动侧的所有安全模块、安全单元、安全工具进行集成和管理。

- 传统安全运维以环境管理和设备维护管理等线下运维服务为核心
- 云环境下，安全运维服务集中在漏洞、风险、备份恢复、应急预案等策略管理和检测等方面



- 企业资产安全体系的构建需基于单点安全产品并通过功能联动构筑主动防御系统
- 基于安全上云的背景，用户可采集不同服务商提供的安全模块，实现责任共担和策略共享

服务模式	服务特征	代表服务商
安全运维及云上运维服务	结合业务场景特征构建信息安全保障体系，维护业务系统顺利运行	奇安信、360政企安全、绿盟科技、观安、蓝盾、远禾科技、天融信、安信天行等
渗透测试	通过模拟黑客攻击战术和技术，测试并寻找系统漏洞，进行补丁加固	千寻、安恒信息、绿盟科技、长亭科技、腾讯安全、四叶草安全、知道创宇等
应急响应	通过对大型安全事件和突发事件进行定位、溯源、处置保障业务运行	阿里云、绿盟科技、安恒信息、启明星辰、深信服、东软、奇安信、天融信等
安全众测	汇聚安全专家，探测因逻辑漏洞、权限问题等导致的漏洞和安全问题	阿里云、漏洞盒子、腾讯安全、360安全、漏洞银行、补天漏洞响应平台等
红蓝对抗	模拟鱼叉攻击、水坑攻击等黑客行为，提高应急处置和安全管理能力	腾讯安全、启明星辰、四叶草安全、安恒信息、长亭科技、安恒信息等
零信任	通过多源信任评估、动态访问控制等功能模块构建新型认证授权体系	腾讯安全、竹云、绿盟科技、天融信、奇安信、蔷薇灵动、云深互联、虎符科技等
数据安全&隐私保护	以数据库和日志审计、数据库加密等为核心，通过加密算法实现隐私计算	观安、全知科技、腾讯安全、帮帮安全、百度安全、爱加密、天融信等
开发安全	结合软件开发生命周期不同阶段，融入安全设计、安全测试编码等	360安全、默安科技、奇安信、开源网安、奇安信、悬镜、海云安等
威胁管理	融合多元化的威胁管理策略，构建统一和自动化的威胁管理平台	启明星辰、安恒信息、天融信、亚信安全、绿盟科技、深信服、六方云、东翼科技等

发展历程 中国网络信息安全行业发展阶段：由单点防御向纵深防御演进

1986年以来，中国网络信息安全行业的发展经历了包括起始期、萌芽期、快速发展期和全面升级期在内的四个阶段，云计算技术、物联网场景的发展从基础设施端和应用端助力中国网络信息安全产业进入发展成熟期。1940年至19世纪80年代，中国信息系统安全建设聚焦于通信层信号加密层面；19世纪80年代至2000年，以启明星辰、深信服等为代表的领导企业在以防病毒系统为代表的单点防护领域快速拓展市场、推进技术演变；2000年至2014年，中国网络安全防护向纵深防御阶段趋近，2014年后，自动化技术的应用推进主动防御体系的构建和应用。

19世纪80年代-90年代

中国网络安全市场尚未完全形成，网安防护技术快速迭代，但缺乏成熟的技术标准，行业竞争格局和用户特征尚不明确。

2000年-2013年

主要网络安全服务商确定自身技术路线，行业整体进入快速增长期，白名单查杀、人工智能引擎等新技术应用初见端倪。

2014年-2019年

中国网络安全市场在细分技术领域涌现出一批新服务商，此外，整体安全解决方案交付的形式受到用户青睐。

2020年至今

中国网络信息安全产业发展进入成熟阶段，以数据为核心驱动力，在技术、产品架构、服务理念等维度持续进阶，依托大数据、云计算、AI等核心技术打造动态防御系统。

引入期

1987年
- 1987年，中国成立信息中心信息安全处
- 1994年，《中华人民共和国计算机信息系统安全保护条例》颁布

1994年

在“九五”攻关等国家宏观产业政策扶持下，中国出现第一批专业从事网络安全产品研发的企业

90年代
- 1995年，天融信成立
- 1996年，启明星辰、北信源成立

萌芽期

2000-2007年
- 2000年，深信服成立
- 2003年，启明星辰推出分布式漏洞扫描与安全评估系统
- 2007年，北信源推出终端安全登录与监控审计系统

伴随利好政策出台，政企组织加强网络安全建设，完善IT和网络基础设施，新技术、新产品带动行业规模增长

2008-2013年
- 2010年，启明星辰上市
- 2012年，绿盟科技推出“Web应用漏洞扫描系统”
- 2012年，启明星辰推出万兆WAF、万兆ADM

发展期

2014-2015年
- 2014年，中国网络安全和信息化领导小组成立
- 2015年，腾讯和启明星辰达成合作，中国网络安全产业联盟成立

2016-2019年
- 2016年，中国网络空间安全协会成立，南洋股份并购天融信
- 2016年，《中华人民共和国网络安全法出台》
- 2018年，深信服在A股创业板挂牌上市
- 2019年，安恒信息登录科创板

成熟期

2020年
- 2020年，奇安信、安天等安全服务商披露多个境外组织对中国进行的APT攻击技术细节

持续升级
- 攻击模式趋于复杂，核心资产泄露及威胁勒索事件频发，云上资产暴露面增加，个人隐私保护需求凸显；《数据安全法》和《个人隐私保护法》正式施行

2021年-未来

中国网络安全等级保护制度、顶层策略逐步完善，产品和服务架构趋于精细，平台化、可视化等特征日渐凸显，在新技术及应用场景融合的大背景下，能够感知全盘态势并实现体系化防御的安全系统将引领全行业发展

产业链 中国网络安全行业产业链

中国网络安全行业产业链以各类安全硬件、安全软件、云安全服务、安全解决方案为核心。依托上游IT设备、操作系统、数据库等基础设施集成，各类安全硬件厂商、安全软件厂商、云安全服务商和安全解决方案服务商为下游B端、C端、G端需求方提供持续升级的网络安全和云安全服务。

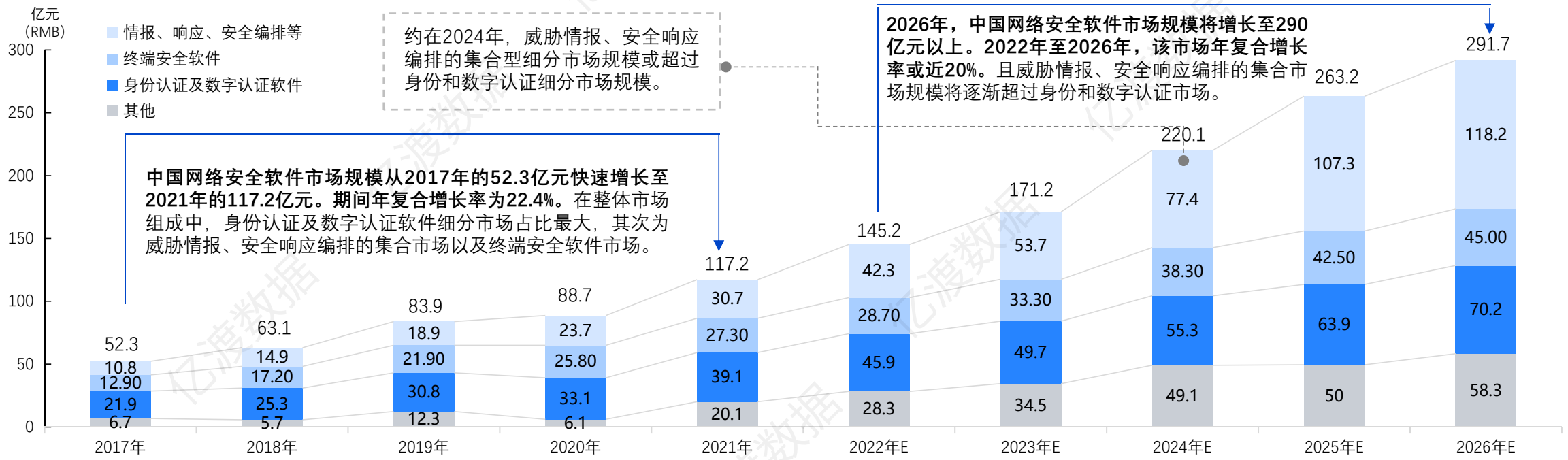
中国网络安全产业链供给端及消费端图谱

- **传统应用场景存量需求：**金融、泛互、电信及政务等领域数据资产迅速扩容，用户数据及系统安全升级，持续创造网络安全需求。
- **新型应用领域增量诉求：**能源、教育、医疗、教育、物联网、政务、泛互等领域安全合规需求凸显，安全架构迭代推进安全应用场景扩容。

市场规模 中国网络安全软件市场规模：威胁情报及安全响应编排业务增速或反超认证市场

本报告将中国网络安全软件市场细分为终端安全软件市场、身份认证和数字认证软件、SAIRO（安全情报、安全响应、安全编排、安全分析）等单点市场。随下游用户对软件形态安全产品接受度提升，且AI、云计算基础设施、物联网、5g通信等技术为各行各业赋能，安全软件的应用场景快速拓展，促进市场快速成长。随企业数字化转型进程推进，政企组织机构中网络安全系统的建设已不局限于满足合规要求，更多需要结合业务发展特点优化安全管理策略。相对硬件市场而言，下游用户对安全服务的需求和预算在逐步向软件和服务市场迁移。预计2026年，中国网络安全软件市场规模将超过290亿元。

中国网络安全行业软件市场规模，2017年-2026年预测

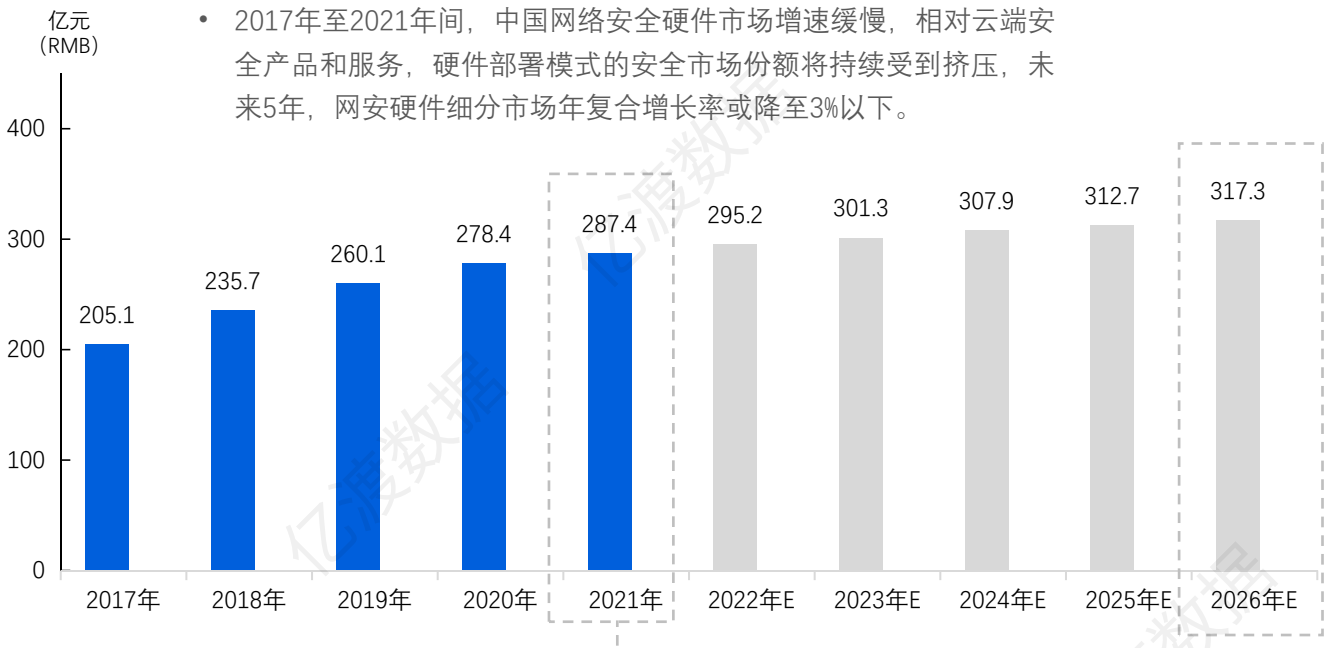


数据来源：亿渡数据

市场规模 中国网络安全硬件市场规模：硬件市场增长红利行至尾声

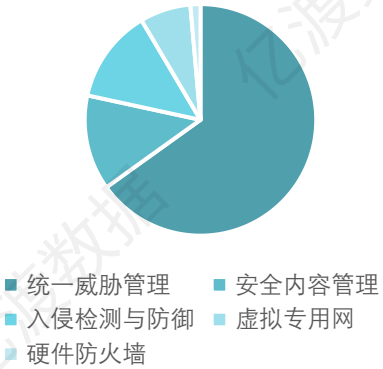
硬件市场是构成网络安全产业整体最大份额的市场，整体比重超过50%。2017年至2021年间，中国网络安全硬件市场规模从205.1亿元增长至287.4亿元，期间年复合增长率为8.8%。在网络安全硬件领域，主要细分市场覆盖统一威胁管理、安全内容管理、入侵检测与防御、硬件防火墙、虚拟专用网等。在众多细分市场中，占据较大份额的为统一威胁管理和安全内容管理领域。新冠疫情爆发以来，远程连接场景呈爆发式增长，政企组织对网络安全服务采购项目逐步启动，网安领域硬件厂商的经营状况相对疫情初期发生较大改善。

中国网络安全行业硬件市场规模，2017年-2026年预测

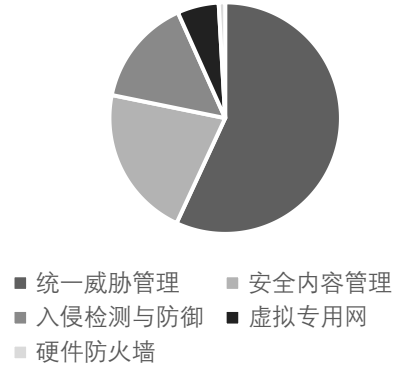


- 2017年至2021年间，中国网络安全硬件市场增速缓慢，相对云端安全产品和服务，硬件部署模式的安全市场份额将持续受到挤压，未来5年，网安硬件细分市场年复合增长率或降至3%以下。

中国网络安全行业硬件市场细分构成，2021年



中国网络安全行业硬件市场细分构成，2026E



- 预计到2026年，中国网络安全行业硬件市场构成中，安全内容管理市场份额比重将持续上升，而硬件防火墙市场份额或所剩无几。

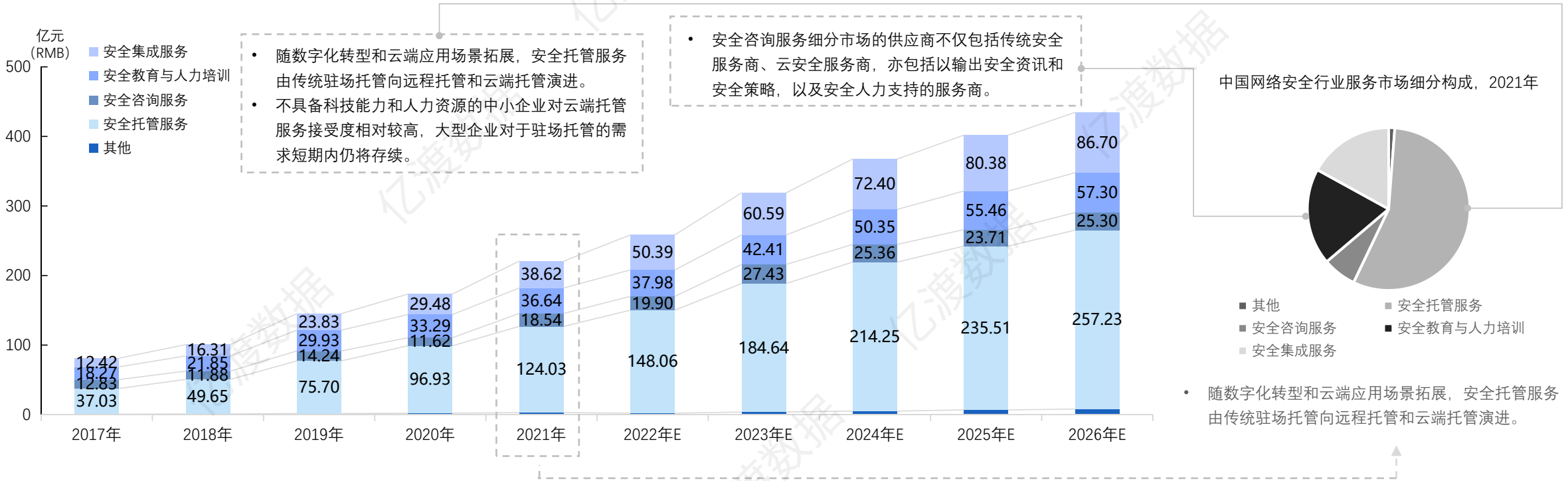
数据来源：亿渡数据

市场规模

中国网络安全服务市场规模：安全服务模式持续创新，云端托管或成趋势

区别于软件市场和硬件市场，网络安全服务市场由安全托管服务、安全咨询服务、安全教育与人力培训服务、安全集成服务等构成。其中，安全托管服务是由第三方安全服务厂商提供的人力支持解决方案，具体形式包括驻场托管安全服务、远程托管安全服务以及云端托管安全服务。安全集成服务是以安全策略设计、防护流程规划、安全项目管理和实施为核心的安全服务模式，为用户安全系统和应用的定制化开发提供支持。安全咨询服务以安全策略规划、安全合规、安全审计、安全测试、应急响应等。安全培训服务以IT教育培训服务、企业培训服务、教育认证等为核心。

中国网络安全服务行业市场规模，2017年-2026年预测

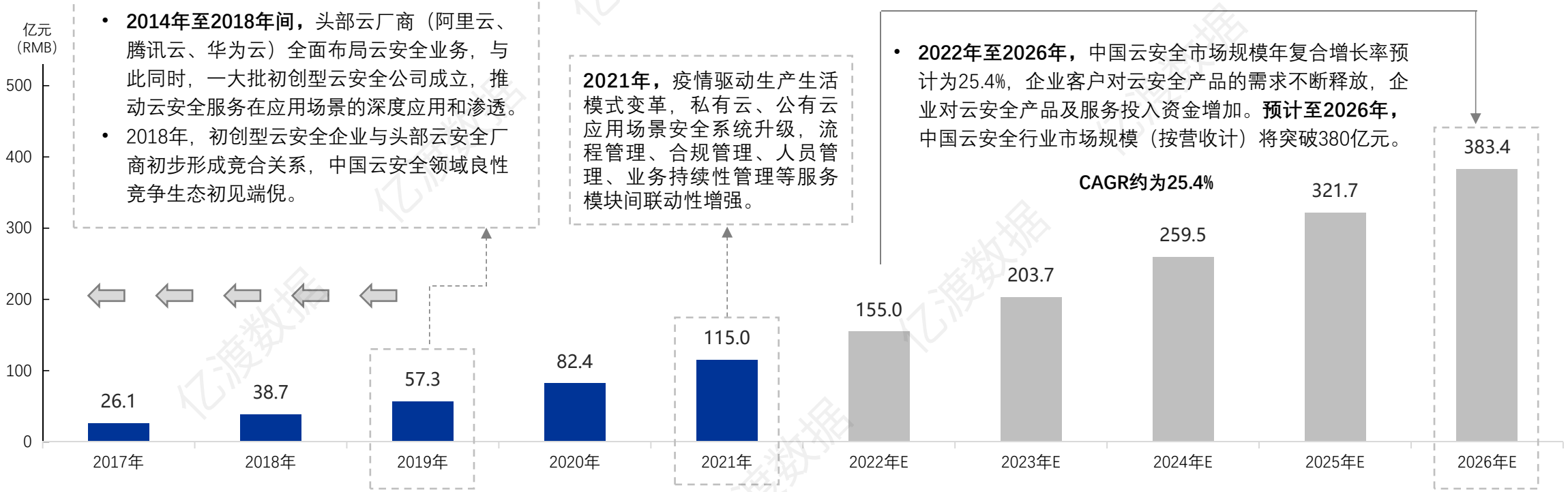


数据来源：亿渡数据

市场规模 中国云安全市场规模：公有云及私有云应用场景拓展，云技术推动安全架构升级

在自适应安全理念、智能化技术的推动下，2017-2021年，中国云安全市场规模从26.1亿元增长至115亿元，呈现快速增长态势。2021年，受疫情影响，远程办公场景增加，移动设备接入、远程系统接入现象更加普及，设备漏洞和弱口令导致企业和个人面临的安全事件威胁增加，云上安全防护需求呈现更加快速的增长态势。预计2022-2026年，在IoT设备进一步渗透和普及以及安全架构升级的趋势下，中国云安全市场规模年复合增长率将达到25.4%。云上安全防护手段将更趋主动、前置，技术划分更趋精细，应用场景持续拓展。

中国云安全行业市场规模（按营收计），2017年-2026年预测



数据来源：亿渡数据

相关政策 政策层级：中国网络安全市场政策及监管法规（1/2)

《“十四五”国家信息化规划》等利好政策颁布与实施，促进企业用户对网络安全需求释放，激励各细分市场快速发展

规模拓展
战略部署
支持类政策
创新激励
机制构建
统一管理
规范类政策
高效权威

颁布日期	颁布机构	政策	核心内容
2021年7月	工信部	《新型数据中心发展三年行动计划（2021-2023年）》	强调要提升网络安全保障能力，要依托安全态势监测、流量防护、威胁处置等安全技术手段，对数据中心底层设施和关键设备加强安全检测，防范多层次的安全风险隐患，进一步强化大型数据中心之间的安全协同
2019年9月	工信部	《关于促进网络安全产业发展的指导意见（征求意见稿）》	落实《中华人民共和国网络安全法》，到2025年，培育形成一批年营收超过20亿的网络安全企业，网络安全产业规模超过2,000亿元
2019年5月	教育部办公厅	《2019年教育信息化和网络安全工作要点》	核心目标中包含全面落实教育领域网络安全和信息化战略部署，出台落实网络安全责任制评价考核办法，建立网络安全培训机制等内容
2018年3月	中央网信办 工信部	《关于推动资本市场服务网络强国建设的指导意见》	推动网信事业和资本市场的协同发展，保障国家网络安全和金融安全
2017年11月	工信部	《关于开展2017年电信和互联网行业网络安全试点示范工作的通知》	在网络安全威胁监管预警、态势感知等八个方面引导企业和加强技术手段建设，增强企业防范和应对网络安全威胁的能力，拉动网络安全产业发展
2021年8月	全国人大常务委员会	《中华人民共和国个人信息保护法》	强调通过数据库安全的技术手段，核心数据加密存储技术，通过数据库防火墙实现批量数据防泄漏，支持通过数据脱敏实现批量个人数据的匿名化
2021年6月	全国人大常务委员会	《中华人民共和国数据安全法》	要求开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，立即采取补救措施；发生数据安全事件时，按照规定及时告知用户并向有关主管部门报告。国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制
2020年4月	网信办等12部门	《网络安全审查办法》	明确规定关键信息基础设施的运营者采购网络产品和服务，影响或者可能影响网络国家安全的，要进行网络安全审查；对于责权方提出更加明确的规定，运营商、银行等关键信息基础设施运营者都有义务做好网络安全工作

相关政策 政策层级：中国网络安全市场政策及监管法规（2/2）

- 在行业发展层面，鼓励企业按需使用云安全服务，提高信息安全保障能力，促进企业客户对网络安全产品与服务的需求持续释放；
- 在行业规范层面，明确网络空间的主权原则，网络产品和服务的提供者以及网络运营者的安全义务，为网络安全行业营造规范的发展环境。

规范类政策：密码管理、投入管理、考核管理、格式规范、监管规范、权益规范

颁布日期	颁布机构	政策	核心内容
2019年10月	全国人大常务委员会	《中华人民共和国密码法》	将规范密码应用和管理，促进密码事业发展，保证网络与信息安全，国家对密码分类管理
2019年3月	国务院	《中央企业负责人经营业绩考核办法》	新版较旧版增加了网络安全事件的考核要求，有助于极大增强相关企业负责人的网络安全意识并增加网络安全相关的投入，为《网络安全法》的贯彻落实提供支持
2019年3月	市场监管总局 中央网信办	《关于开展APP安全认证工作的公告》	APP安全认证工作开展，目的在于规范移动互联网应用程序手机，使用用户信息，特别是个人信息的行为，加强个人信息安全保护
2019年3月	国务院	《中央企业负责人经营业绩考核办法》	新版较旧版增加了网络安全事件的考核要求，有助于极大增强相关企业负责人的网络安全意识并增加网络安全相关的投入，为《网络安全法》的贯彻落实提供支持
2018年12月	中央网信办	《金融信息服务管理规定》	要求金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员，建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范
2018年10月	市场监管总局 国标委	《信息安全技术网络安全威胁信息格式规范》	对网络安全威胁信息进行结构化、标准化描述，以便实现各组织间网络安全威胁信息的共享和利用，并支持网络安全威胁管理和应用的自动化
2018年9月	公安部	《公安机关互联网安全监管检查规定》	《规定》明确，公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对互联网服务提供者和联网使用单位开展监管检查，以保障互联网服务提供者和个人合法权益
2016年11月	全国人大常务委员会	《中华人民共和国网络安全法》	进一步界定关键信息基础设施的范围，对攻击、破坏中国关键信息基础设施的境外组织和个人规定相应的惩治措施等；该法旨在维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展

相关政策 政策层级：中国网络安全地方政策及监管条例要点概述

颁布地区	政策	核心内容
北京	北京市加快新型基础设施建设行动方案（2020-2022年）	支持新型基础设施安全类、网络安全公共服务类、网络安全“高精尖”技术创新平台类安全组织建设
浙江	浙江省新型基础设施建设三年行动计划（2020-2022年）	提出软件产业、云计算产业、大数据产业发展目标，形成网络安全态势感知动态系统、网络安全监测预警、攻击溯源系统、工业控制系统安全监管等能力，定期开展网络攻防演练、网络安全攻防竞赛等活动
重庆	重庆市新型基础设施重大项目建设行动方案（2020-2022年）	完善数据安全保护制度，建立公共数据利用风险评估和反馈机制，加强网络安全基础设施建设，落实网络安全等级保护、核心信息系统分级保护制度
云南	云南省推进新型基础设施建设实施方案（2020-2022年）	加速人工智能、大数据、区块链等技术在网络安全领域的应用，寻求可信计算、动态防御、零信任安全等网络安全理念、架构应用，推动网络安全技术创新和融合，由提供安全产品向提供安全服务和解决方案转变，推进网安产品在金融、能源、通信等领域的应用

不同省市地区“新基建”三年规划凸显网络安全重要性

北京、重庆、浙江等地区出台“新基建”三年规划，将网络安全作为重要建设内容，将关键信息基础设施保障作为重点。

等保2.0实施并升级，进一步扩大等级保护制度规范的范围和所覆盖的安全防护技术维度

2019年，国家相关部门颁布多个规范网络安全产业秩序的要求，包括《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等标准在内的文件正式发布和实施。为确保业务开展符合等保2.0时代国家网络安全等级保护政策的新要求，各地市级以上各级政府机关、金融和能源等国家重点行业进一步加大对网络安全系统建设的投入。

等级保护政策、信息保护政策驱动通信、能源、交通、金融等行业关键信息基础设施运营团体加大安全投入

《关键信息基础设施安全保护条例》于2021年9月1日起正式施行，该条例从培训方式、制度机制、标准规范、技术创新等维度出发，提升通信、交通、能源、金融等行业主责部门构建和提升网络安全运维系统的能力，该条例的落地，将显著强化不同领域业务主体进行网络安全系统性建设、全面监管、定期检测、适时加固等方面的能力，维护关键信息基础设施的安全运营。

发展趋势 网络安全服务架构由单一趋于融合，被动防御转向主动防御，服务路线趋于精细化

新兴技术应用推进网络安全防护架构演变

在5G通信技术推动“云、物、智”发展的背景下，网络安全的防护对象也随之拓展，从传统PC、服务器、网络边缘延伸至混合云、智算中心、泛终端、新边界安全等领域。信息系统架构变化对信息安全防护带来新的挑战，安全运营中心的建设成为政企运营要务。

“被动防御”向“主动防御”转变

传统安全防护止于边界，在web3.0计算环境下，政企用户对网络安全的需求更趋迫切和多元化，关键信息基础设施安全防护理念从事后转为事前，由被动转为主动，更多用户在数字化转型和信息化改造初期将网安规划提升至战略层面，构建动态综合防御体系。

商业模式由单一产品转向“产品+服务”的复合模式

网络安全服务市场由安全托管服务、安全咨询服务、安全集成服务、IT教育与培训四个细分市场组成。随安全托管服务上云，全球范围更多的终端用户将安全托管服务供应商视作网安防御系统中的重要合作伙伴。具备实时、动态检测和响应能力的服务商愈受青睐。

集成服务路线和精细化产品路线并行

随云厂商加入各类安全产品市场竞争，网络安全市场竞争格局呈现出集中的趋势，头部厂商积极通过并购完善技术栈。但随着安全理念革新、安全技术精进，未来5年至10年，网络安全市场或出现一批专精于新兴安全技术渗透的中小型安全服务商。

未来5年，网络安全市场发展面临的机遇和挑战

■ 机遇

全球范围，政府及管理机构不断出台有利于网络安全市场发展的法规和引导政策，刺激技术创新，向网络安全产业释放红利。政策支持将网络安全上升至国家战略高度，中国计划到2025年，逐步实现“培育形成一批年营收超过20亿元的网络安全企业”、“网络安全产业规模超过2,000亿元”的目标。

■ 挑战

受疫情影响，现场技术服务和招投标项目进度受阻，供给端产业链流通速度降低，需求端遭遇不同程度经营困难，但与此同时，远程化办公、云化业务衍生更多远程安全运维需求。

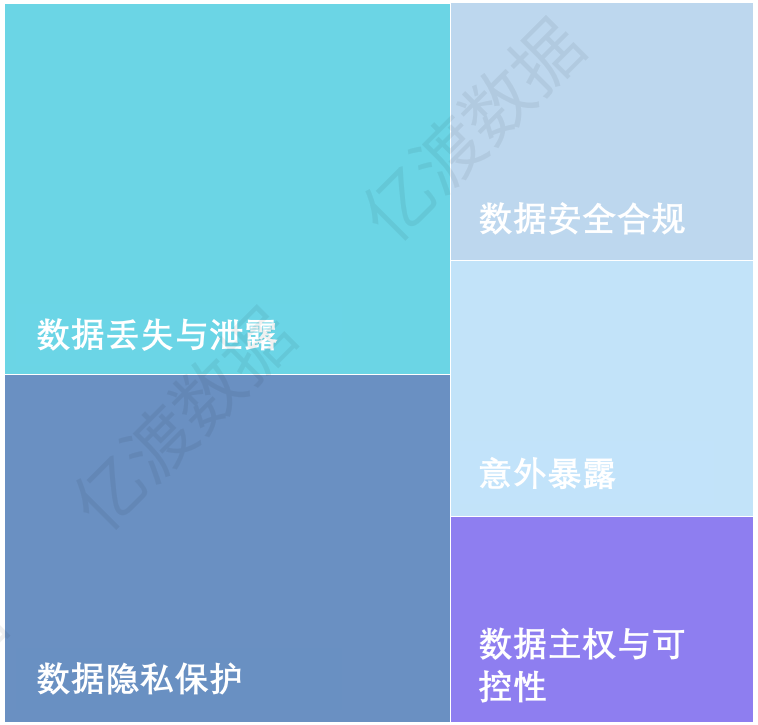
发展趋势 数据安全或成为网络安全服务的重点聚焦领域

企业用户对数据安全防护技术的要求日渐升级，安全服务商通过数据脱敏、电子文档加密、数据存储备份与恢复、数据库安全、数据泄露防护等能力，助力政企用户建立具备完整性、可用性、机密性的数据处理系统

当前，安全服务商提供的安全产品已全面覆盖终端、云端和移动端，产品架构和服务模式随用户关注重点演变而呈现倾斜。2021年，在数据安全应用领域，政企用户关注点占据前五位的问题分别为**数据丢失与泄露（65%）**、**数据隐私保护（60%）**、**数据安全合规（35%）**、意外暴露（37%）、数据主权与可控性（25%）。

随纵深防御安全策略升级，全套数据安全解决方案将覆盖从**终端**到**网络、存储、应用、移动端**和**云端**的各类应用场景。传统数据安全服务主要针对已知威胁，存在较强的边界意识，而在云计算、大数据等新兴技术渗透的背景下，以APT为代表的持续性威胁对用户造成数据窃取、数据篡改、勒索等多种形式的损害。新型数据安全解决方案多以自适应动态安全体系为基础，在实现安全防护的同时，兼顾用户业务稳定性和需求，通过策略实践评估、事件分组归类等手段实现对数据系统的全生命周期管理。

数据安全问题关注度热力占比（前五位），2021年



数据来源：亿渡数据整理

《数据安全管理办法（征求意见稿）》

随企业数据上云加速和网络安全等级保护制度落地，业务主体对数据库加密的要求成为“关键信息基础设施”的刚性需求，以易部署、稳定性高、透明性好为特征的数据库加密产品受到用户青睐。

《个人信息出境安全评估办法（征求意见稿）》

政策的出台进一步明确了对于敏感数据全生命周期的管理规范要求。随政府数据共享与开放力度加强，大数据规模化应用拓展，用户对隐私和敏感数据匿名化需求凸显，数据库脱敏产品将成为数据安全的重要组成部分，云上数据脱敏或成主流。

中国网络安全行业热点细分领域概述

- 在基础安全领域，硬件WAF、蜜罐等领域市场处于平稳增长阶段，其中，蜜罐产品快速迭代，存在较大增量市场空间。
- 在端点安全领域，EDR系统、主机和服务器加固以及其他终端安全防护工具之间联动性持续增强。
- 在云安全领域，云主机安全及容器安全产品成为市场关注重点。
- 在安全方案领域，基于新理念的身份管理、API安全及渗透测试将持续快速演进。

网络基础层安全市场简析

防火墙 防火墙为内部网络系统提供抵御外部入侵的抗攻击屏障

防火墙系统简述及特征

防火墙是网络安全防护系统的第一道防线，可基于**已定义的安全规则**控制网络流量流通，目的在于为安全、可信、可控的内部网络系统建立一道抵御外部不可信网络系统攻击的屏障，应用至今已形成较为成熟的技术模式。

中国防火墙形态演进五阶段

包过滤防火墙

与路由器同时期出现，依托包过滤技术支持基基础流量的访问控制

代理防火墙

通过应用层代理连接内部和外部网络间的通信，安全度较高，但处理成本较高

里程碑

状态检测防火墙

基于传统过滤包技术，通过检查引擎截取数据包，以应用层状态判断是否接受连接

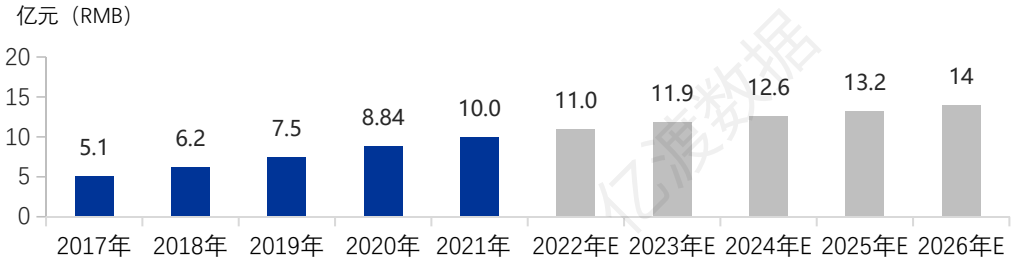
自适应代理防火墙

结合代理类型防火墙和包过滤防火墙的优点，大幅提升防火墙性能

下一代防火墙

- 在数据包过滤、状态检测功能之余，具备诸如VPN功能，能够抵御高级恶意软件攻击和应用层攻击

中国硬件WAF市场规模，2017年-2026年预测



数据来源：亿渡数据

2021年，在新冠疫情爆发的影响下，利用Web脆弱性而进行的网络攻击事件加剧，网络安全建设项目、采购项目延期，硬件安全产品部署难度提升，硬件形态的WAF市场扩容速度明显放缓，软件形态WAF需求量保持平稳，云WAF市场增速超过硬件WAF细分市场。

- 主流防火墙品牌及优劣势

主流品牌（不完全，不分先后）	服务要点	用户关注点
Fortinet	集成SD-WAN功能，**强化API扩展性**，有效防御加密流量中的攻击	可视化与自动化流程融合，支持**基于用户业务特征**的网络分段部署
Check Point	以威胁防护技术创新升级为重点，支持**跨所有网络分段**的防护能力	对应用程序具有广泛覆盖，支持混合云基础架构，助力企业对抗**多向量攻击**
华为	SD-WAN功能覆盖**分布式办公实例**，具备可视化策略编排管理器	集成蜜罐功能，但尚未支持与第三方安全信息和安全事件管理的集成
深信服	云端威胁情报服务与云WAF联动，自主搭建全面的**威胁分析系统**	可在服务层面给予用户即时支持，采用**集中管理模式**，提升防火墙管理效率
山石网科	扩展安全架构，集成并强化VPN功能	防火墙内威胁检测功能持续扩展

蜜罐 蜜罐通过诱饵技术获取黑客工具及黑客通信网络，提升用户对抗攻击效率

蜜罐技术原理及特征

蜜罐是通过欺骗性技术，于主机、网络服务等层面设置诱饵，捕获并分析非法攻击工具及模式，推演攻击形式，协助用户了解安全威胁态势，并依托安全技术及管理策略增强防护系统效率。此外，蜜罐技术支持用户了解黑客网络及工具。

蜜罐部署模式

无代理模式

独立部署：

通过物理旁路、串联等方式连接交换机，实现模拟资产与网络IP的连接部署；该模式下，蜜罐与网络联通，或存在蜜罐逃逸、穿透等威胁

代理模式

非独立部署：

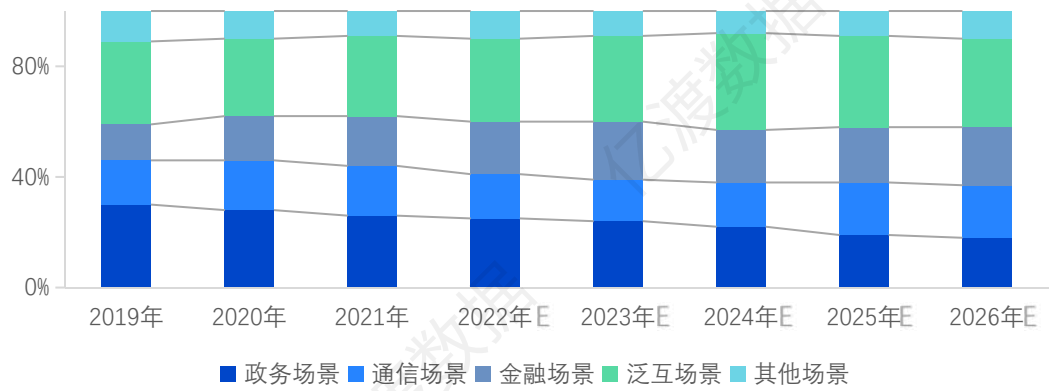
仿真资产IP地址通过主机agent模式映射至真实网络，通过多节点扩大仿真资产暴露面，牵引流量至蜜罐，提升诱使策略有效性和安全常态化

诱饵

仿真资产部署：

通过网联诱饵、文件诱饵、邮件诱饵等形式部署蜜罐系统，助力用户捕捉攻击；但多数产品尚未支持诱饵自动分发、自动更新、自动消除等技术

中国蜜罐应用情况，2019年-2026年预测



数据来源：亿渡数据

蜜罐战术简析：

- 根据攻击者特征布局战术

非法入侵者寻找不同层面资产突破口，利用漏洞绕过防护边界，入侵用户内网，防守侧依托关键节点蜜罐收集攻击策略，诱使攻击。

- 网络异常行为监测

防守侧凭借探测工具（Ping探测、ARP探测等）监测异常行为，识别攻击方法及负载，统一分析并判断攻击意图，布局防御节点。

- 模拟资产并布局欺骗系统

通过节点探针，监测网络扫描探测行为，映射蜜罐服务。

入侵检测与防御 入侵检测与入侵防御系统实时监测网络设备，夯实安全监控引擎

IDP系统简述及特征

入侵检测防御系统包含入侵检测体系（IDS）及入侵防御体系（IPS）。IDS系统具备灵活部署、轻量化、即时反应等优点，并随新技术应用和新应用场景拓展而快速变化，成为用户端安全防护架构采用最为广泛的产品之一。

IDS产品能力评价指标

- **安全功能**
  - 数据探测
  - 检测结果处理
  - 入侵分析
  - 产品灵活性
  - 入侵响应
  - 还原能力
  - 管理控制
- **自主安全功能**
  - 身份鉴别
  - 通信安全
  - 管理员身份
  - 运行安全
  - 安全审计
  - 安全升级
  - 安全事件记录
- **安全性能**
  - 误报率
  - 漏报率
  - 监控力
    - 吞吐率
    - 并发率
  - 还原力

IDS系统普遍存在漏洞，需与其他安全管理软件形成入侵检测、网络监控、网络管理多元结合的工具，检测软件在提升管理便捷性的同时增加了保障。

IPS产品能力评价指标

- **功能要求**
  - 入侵事件分析
  - 入侵响应速度
  - 入侵事件审计
  - 管理控制
- **自主安全**
  - 标识与鉴别
  - 用户管理有效性
  - 安全功能丰富度
  - 安全审计
- **安全保障要求** 一级/二级/三级保障
- **性能评价**
  - 吞吐量
  - 误报率
  - 漏报率

功能要求+自身安全要求

IDS系统以提供安全事件监测和报警为主要工作模式，IPS系统核心在于阻断攻击行为。相对而言，IDS系统具备即插即用、轻量化部署的特点，IPS系统则采用串联部署模式，通过纵深防御模式为用户强化抗攻击能力。

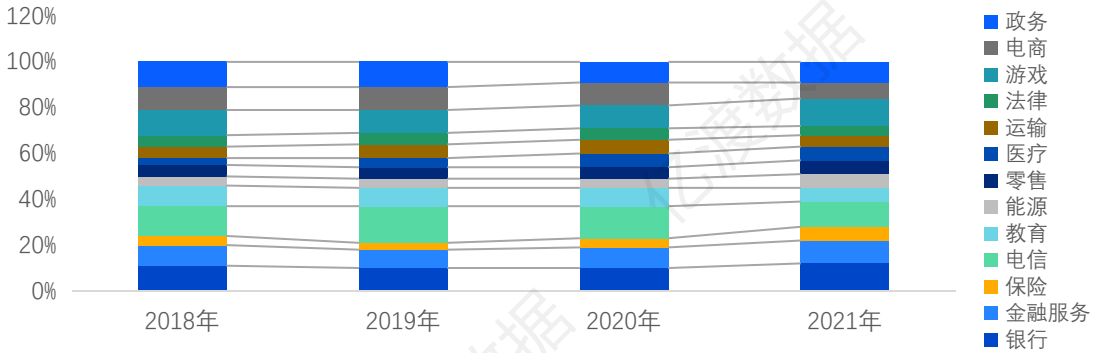
随新一代防火墙功能的升级和演变，IDS和IPS系统呈现出更强的融合趋势，各类防火墙、安全网关等产品更多融合IPS方案，产品功能的交互和融合或进一步促进IDP整体市场的发展。

抗拒绝服务攻击 全球范围DDoS攻击频率激增，各领域关键基础设施受威胁范围扩大

DDoS攻击特征及影响

DDoS为分布式拒绝攻击，黑客将攻击者分布于不同位置，同时向相同目标开展分布并协同的统一性攻击。DDoS攻击将使目标服务器、网络系统无法维持正常操作和运转。常见DDoS攻击多包括攻击者、主控端、代理端、攻击目标四部分。

DDoS攻击场景占比



数据来源：亿渡数据

DDoS攻击类型简析

攻击类型	攻击对象	攻击模式
ICMP Flood攻击	底层操作系统	针对IP主机和路由器之间通信渠道，发送大量ping数据包，消耗主机资源导致系统瘫痪
DNS Flood攻击	底层操作系统	以瘫痪DNS服务可用性为目标，利用DNS查询请求放大攻击流量，造成网络拥堵和瘫痪
ACK Flood 攻击	主机服务器	利用服务器与客户端之间SYN连接时要求ACK应答的请求进行ACK反射攻击
UDP Flood攻击	网络主机	利用UDP协议的无连接性质，针对服务器发送大量UDP数据包，攻击核心设备防火墙
SYN Flood攻击	进程和连接	利用TCP协议三次握手特征，攻击导致大量TCP处于半链接状态，耗费进程资源和内存
CC攻击	服务器和系统	依托代理服务器生成大量伪装性合法请求，增加页面访问压力，占用系统资源

DDoS攻击分层归类

- 网络层
  - ICMP Flood攻击
  - IGMP Flood攻击
- 传输层
  - UDP Flood攻击
  - SYN Flood攻击
  - TCP Flood攻击
  - ACK攻击
  - SSL攻击
- 应用层
  - 各类DNS攻击
  - HTTP攻击
  - SNMP攻击
  - NTP攻击

随网络安全事件影响范围扩展，受DDoS攻击的领域从传统通信、金融、政务等领域拓展至包括电商、零售、医疗、游戏等更加广泛的领域。2021年，受DDoS攻击领域最多的仍教育领域受攻击程度有所下降，能源、零售、医疗、法律等领域DDoS攻击维持平稳态势。此外，医疗和政务领域面临的攻击态势或趋严峻。

APT APT攻击具备不确定性、隐蔽性和强针对性，当前较难实现全防护效果

APT威胁特征及趋向

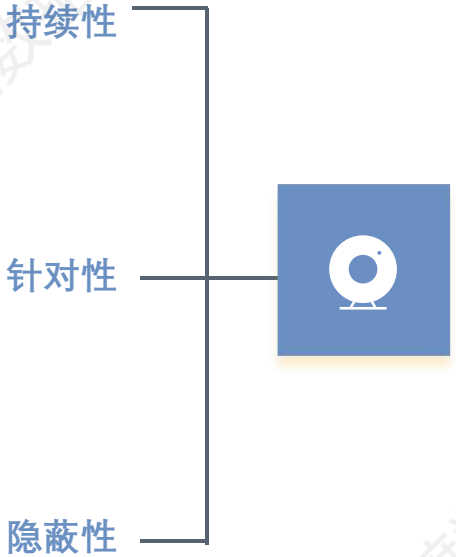
高级持续性威胁攻击对象通常针对政府机构、企业核心资产而展开，攻击渠道覆盖移动设备、服务器、邮件系统等。远期，APT检测与防御将加速融合IDS技术、大数据技术和AI技术，构建基于深度学习的APT自主防御平台。

APT攻击模式主流特征

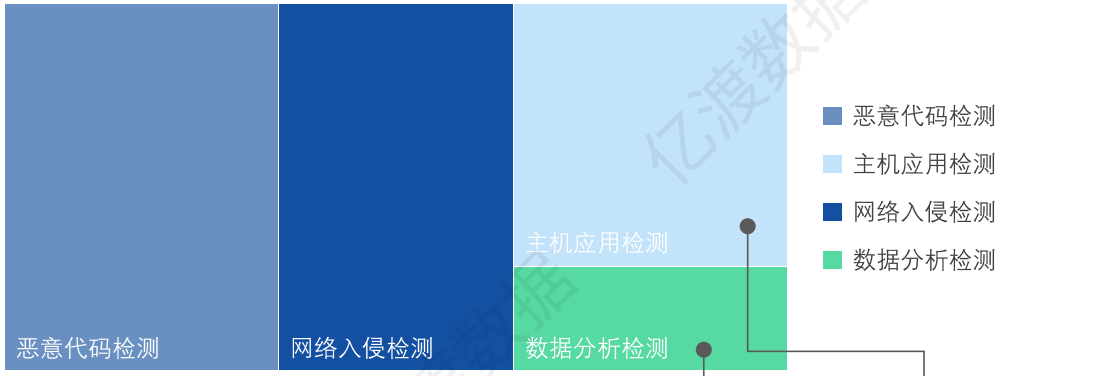
结合前期准备、过程中入侵、持续性内网深度渗透实现对攻击技术环节的全覆盖，延长攻击覆盖时间线及渗透范围。

以具备高密度数据和知识产权的资产主体为攻击对象， 相对传统广撒网的攻击模式，APT攻击更加专注于特定组织和系统。

依托各类绕过手段，通过搜索引擎、数据泄露、爬虫等手段对攻击对象进行持续渗透，利用针对性恶意软件对目标网络系统进行隐蔽性绕过攻击。



APT攻击检测手段及其特征



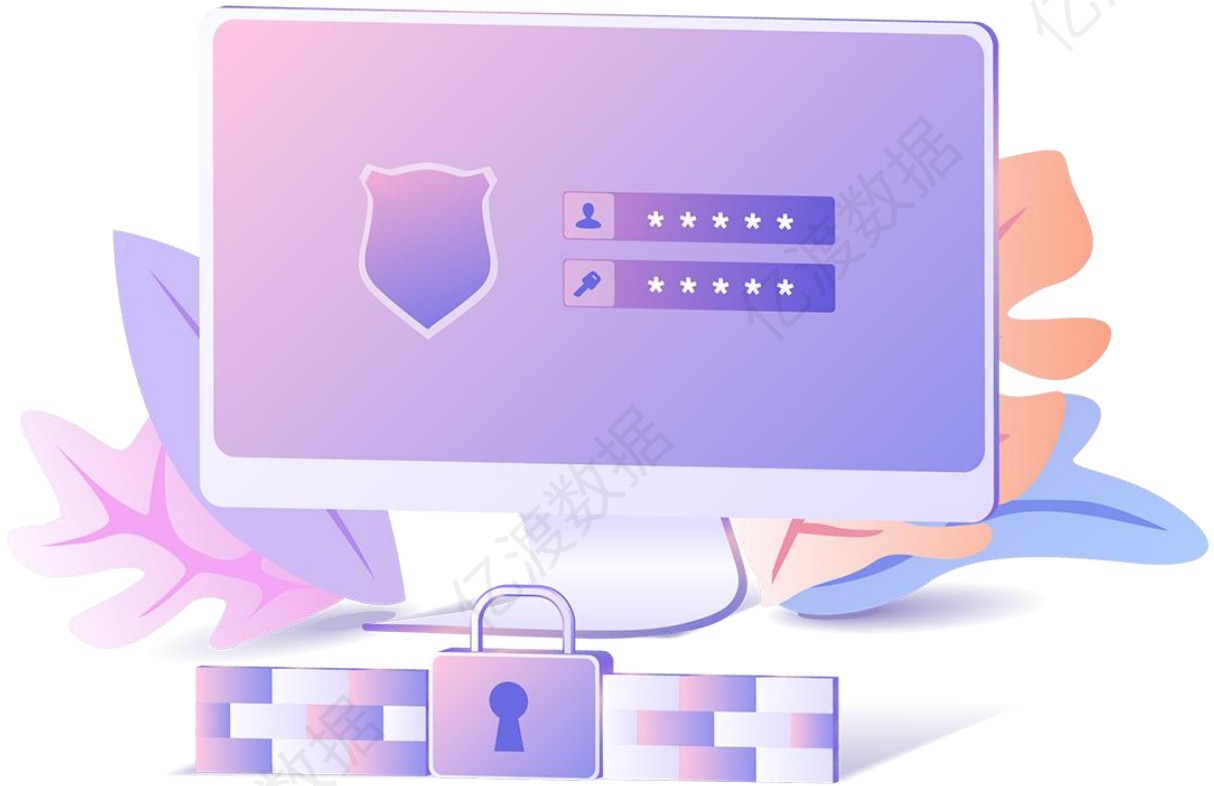
恶意代码静态分析：对恶意样本进行特征分析，总结特征码并构建特征数据库，基于特征数据匹配结果呈现恶意代码及相关信息

基于数据分析还原攻击路径：依托大数据存储和分析技术，全面分析日志数据，并通过机器学习分析数据，检出攻击

基于网络端传统模式进行检测：APT攻击形式多样且变换频繁，可基于恶意代码通信渠道，采用传统入侵检测方式，获取APT通信模式

主机节点检测：于组织内主机系统、服务器系统不同节点布置并强化安全措施，避免系统遭受外部恶意代码攻击

数据来源：亿渡数据



端点安全市场简析

终端检测响应

终端检测与响应系统融合多源技术，并与SoC、SIEM等平台联动

终端检测与响应（EDR）简述

EDR系统融合大数据分析、沙箱分析、机器学习、行为分析等技术，支持终端层面深度监控、威胁分析、安全取证、事件响应追溯等功能，并支持SIEM、SOC、态势感知平台的融合与联动。

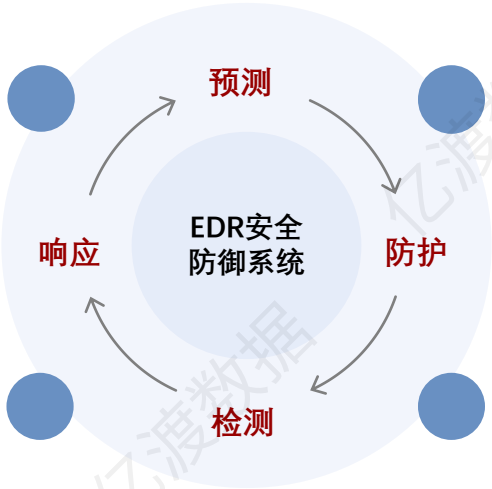
EDR安全系统关键技术及特征

关键技术	基础特征	发展方向
终端安全防护技术	覆盖基线核查、补丁加固、行为监测、终端管理、策略分发等	更加兼容各类操作系统、应用系统和平台
安全数据采集技术	静态数据采集：资产、端口等信息 动态数据采集：各类操作行为等	提升数据种类、属性等标准的统一性
大数据分析技术	融合深度学习、强度学习、聚类分析、关联分析等识别安全威胁	对数据分析持续性提升，提升事前预测准确性
威胁情报分析技术	整合多维度关键数据，多源情报，对攻击进行追踪和溯源	强化威胁捕获能力，威胁情报多场景共用
安全取证技术	追查并回溯攻击行为，实时监测终端设备运行状态	持续强化数据取证真实性、完整性和关联性

注：中国市场EDR产品供应商以深信服、奇安信、天融信为代表，境外头部供应商包括卡巴斯基、CrowdStrike、Comodo等。随产品形态发展，EDR防护系统在物联网场景中实现更加广泛的应用渗透。

EDR安全防护系统关键节点

终端威胁检测与响应系统基于预测、防护、检测、响应四环节构成全方位防护技术体系，构成防护代理、管理平台、分析中心和安全态势四部分，支持终端防护技术、数据采集技术、大数据技术、威胁情报技术、安全取证技术等技术手段的组合应用。



基本情报和数据手段的分析：系统实时获取终端运行数据，依托后端分析手段，主动探测和识别终端设备可能存在的安全风险，预测恶意行为动向。

事前、事中及事后防护手段：基于机器学习技术构建主动学习的终端行为模式，并支持安全事件和防护规则之间的匹配，实现对威胁的探测和实时阻断。

即时响应和检测：实时探测终端可能的风险点，针对高威端口、高危系统、异常进程和文件提供安全防护策略，依托持续性检测和修复提升终端安全防护效力；针对既有安全事件清洗代码，修补漏洞，并依托后端数据分析技术，对攻击相关特征进行关联分析、提取特征，实现对二次攻击的事前抵御。

主机加固 主机加固服务以优化网络和应用系统安全环境为目标，构建立体防护措施

主机加固层面及形式简述

主机加固主要指网络加固与应用系统加固和优化，针对网络层、主机层、应用层等空间进行安全标记、建立访问控制等多维防护措施，具体形式包括优化安全配置、安全补丁安装、系统风险防范、系统功能测试、完整备份、重建机制等，主机加固与杀毒软件可实现较强互补。以青藤云安全、安恒信息、深信服、天融信等为代表的服务商可提供较为全面的主机加固服务。

主机加固及优化关键环节

状态探查

针对系统状态进行安全需求分析、安全策略制定及风险系数评估，在对被加固系统进行安全等级分析后确认加固和优化方案效果及性价比

方案制定

根据业务运行时系统状态，调查系统安全漏洞，并根据系统安全缺陷制定安全加固和优化内容、步骤及时间线

策略实施

优化策略主要包含系统加固和加固效果测试两方面，针对不同加固措施进行相关功能性和安全性测试，在加固效果不足的情况下，采取再加固或重建系统等措施

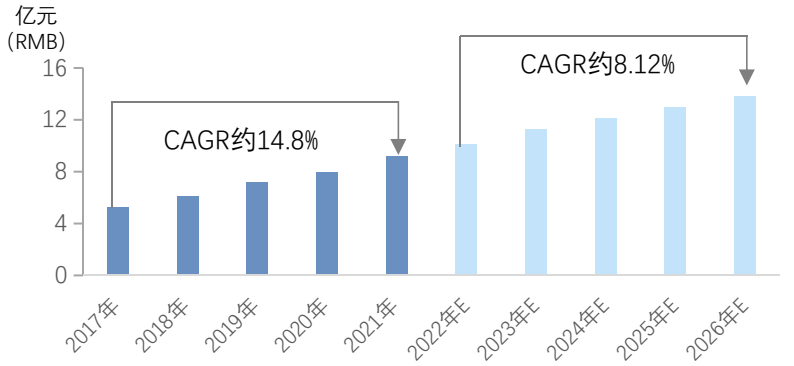
记录分析

针对加固和优化后系统与网络运行情况，进行定期检测和汇总，记录需覆盖加固过程、系统安全管理情况、系统加固后安全审计等结果

主机加固技术简述

- **网络设备加固技术：**针对边界路由器安全漏洞和操作系统隐患，调整用户权限和进程权限，进行全面安全配置；
- **网络结构调整：**针对网络层不断扩张的攻击，调整安全结构，应对各类病毒、分布式拒绝服务攻击等；
- **数据库加固：**以补丁安装、安全配置调整等方式强化数据库安全机制；
- **安全防护系统优化：**加速防火墙和入侵检测系统迭代升级，强化防护系统

中国操作系统安全加固市场规模，2017-2026年预测



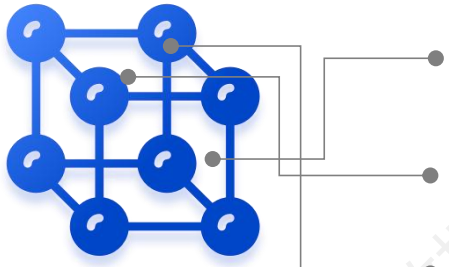
数据来源：亿渡数据

服务器加固 针对WEB服务器、FTP服务器、E-mail服务器存在的漏洞和配置问题进行优化

服务器加固机制及基础特征

服务器系统安全加固旨在提高服务器安全性和抗攻击能力，通过操作系统安全加固减少漏洞，维稳业务系统。较为常见的加固模式为系统内核加固，并结合身份认证、访问控制等模式为业务安全运行提供保障。

服务器核心防护原理——三层内核加固



操作系统	应对内核脚本攻击及内部攻击，针对系统管理账户进行权限分散操作
应用层	应对应用级代码攻击，根据应用中主体和客体安全标志判断威胁力
网络层	应对嗅探攻击，由操作系统执行授权规则，对各类端口及进程进行强管理

根据服务器各层特征对操作系统注册表、文件、服务等采取身份及授权控制的保护，应对客体、病毒等对系统的入侵，打通网络层与应用层主动防护机制，保证业务连续稳定。

服务器加固服务阶段性演进

- **安全配置加固：**从静态层面提升安全策略有效性，基于定期检查及动态监控系统提升服务器安全等级。

对抗密码暴力破解 | 分散管理权限集中度

及时清除多余账户 | 限制远程登录权限

- **安全合规加固：**合规性加固以账户、数据文件为管理对象，强化对进程、内存、网络连接的安全管理。

系统管理：对账户、数据、应用等进行日常维护

系统审计：针对内部管理角色、安全角色行为进行审计

\+

系统安全：进行权限分配、日志管理等安全操作

- 安全反控制加固：加强对隐藏性攻击的识别，即时阻断入侵通道，确保对关键进程和操作系统的掌控。

从管理员账户、远程进程、上传工具等层面进行控制

注重进程中、服务器再启动、系统替换等过程中的隐藏攻击

阻断入侵者对控制通道的渗透

对关键进程及关键操作进行监控

数据来源：亿渡数据

恶意软件防护

恶意软件持续演变，防护系统覆盖范围由传统网络级拓展至云端和边缘网络

恶意软件防护

恶意软件涉及病毒、蠕虫、木马等多种形式，通过破坏或获取用户敏感信息对终端、移动终端等设备正常运行造成威胁，侵害用户合法权益。通过结合威胁情报、沙盒等工具，恶意软件防范系统助力用户保护终端、网络及电子邮件系统。

恶意软件基础分类及特征

类型	感染方式	代表性工具/案例
勒索软件	依托定向循环技术加密核心资产	WannaCry、Petya等恐吓软件
广告软件	网络广告重定向及下载	免费游戏、浏览器扩展等
间谍软件	窃取及监听用户网络行为，向第三方出售用户隐私数据	键盘行为记录程序
加密劫持	加密挖掘软件与操作系统后台运行	非法占用资源挖掘加密货币
Rootkit	隐藏非法访问手段及踪迹	程式进程隐藏软件组合

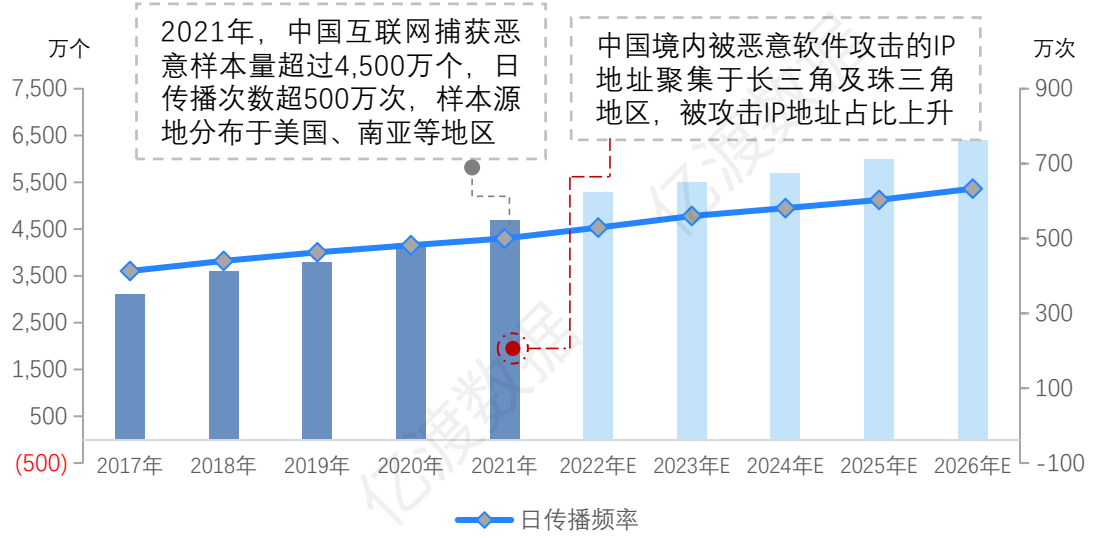
恶意软件防护三环节

恶意软件检测：监控网络流量、日志等资源受恶意软件感染的信号（供应商如IBM、HP、Splunk等）

恶意软件防护：覆盖反间谍软件、高级防火墙、应用程序控制等软件（供应商如Cylance、Carbon Black等）

恶意软件清理：针对恶意软件特征及渗透度采取针对性清除措施

中国恶意程序样本数量及日传播频率，2017-2026年预测



数据来源：亿渡数据

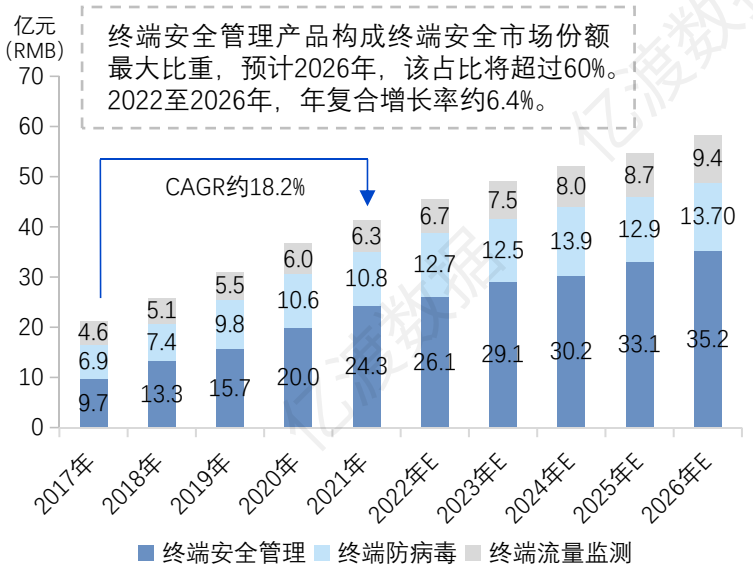
恶意软件防护系统可视性及即时性提升

传统模式下，恶意软件防护系统多通过硬件设备实现功能，随云基础设施普及，恶意软件防护系统向云端部署模式转化，并结合沙盒、威胁情报、恶意软件拦截等功能以及机器学习技术，持续监测网络行为、资产状态，助力用户快速发现、防范并清除恶意软件，防护范围从基础网络扩展至各类边缘网络，结合静态与动态分析，主动防范已知威胁和未知威胁。

终端安全 终端安全管理系统助力端到端威胁检测和抵抗力升级，从静态合规趋向动态防护

终端安全管理以安全策略设置、终端网络接入查验、网络进程访问控制、防病毒软件管理、终端接入查验、系统补丁管理等功能为核心，构建多源终端安全管理功能体系。终端安全管理与安全运维、用户行为管理、数据安全管理、存储介质管理、服务器访问控制安全管理、日志审计分析等平台联动，解决终端安全问题，降低信息泄露可能性，支持用户数据全生命周期防护。如绿盟科技、中软国际、360安全等服务商为代表的安全厂商推动终端安全管理从基础合规向能力升级演进，显著增强终端设备针对各类威胁的检测和防护能力。

中国终端安全产品市场规模，2017-2026年预测



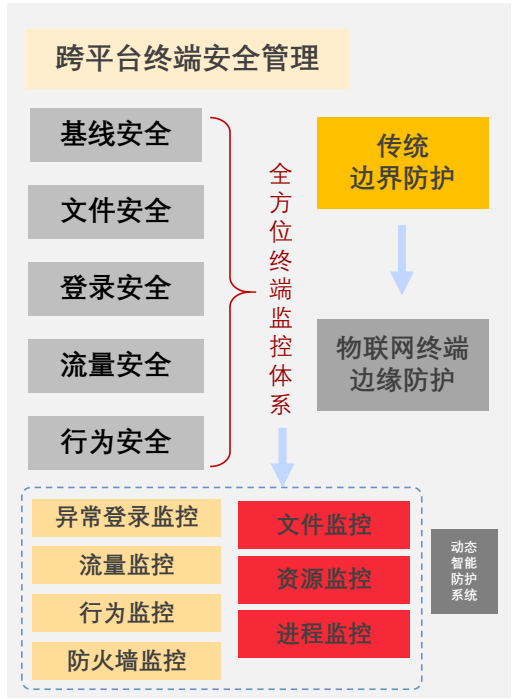
数据来源：亿渡数据

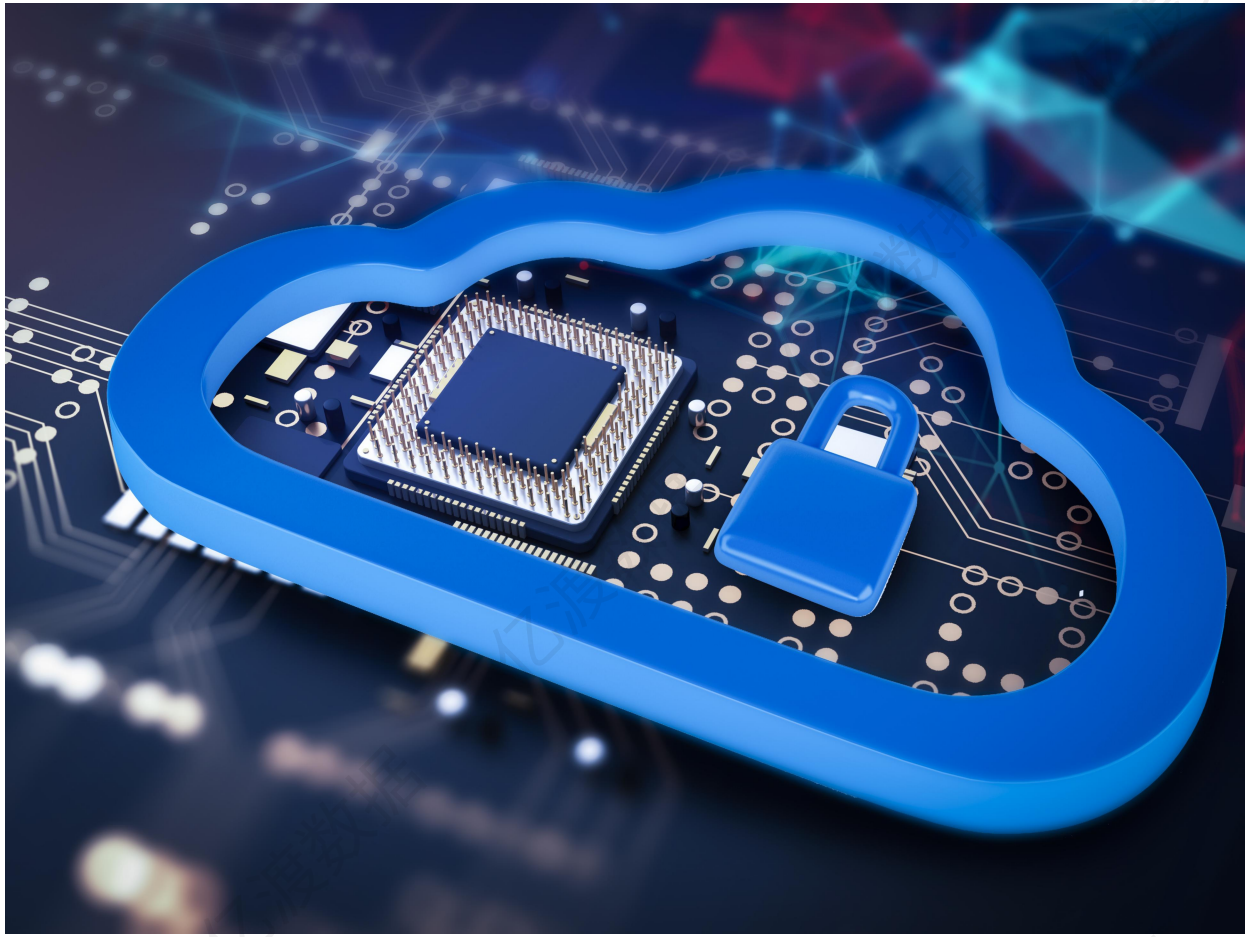
终端安全管理于主流操作系统部署维度

Windows	Linux	IOS	Android
主机监控审计	权限管理	网络接入认证控制	移动审批管理
终端安全登录			
电子文件安全传输	安全管理	电子资料安全网关	
可信移动存储介质管理	外发管理		电子文档移动终端安全
光盘刻录监控与审计		运维审计管理系统	
打印安全监控与审计	审批管理		
移动存储安全管理	集中管控	统一身份认证	移动终端安全管理
可信计算管理			

注：统一终端安全管理系统基于探针部署技术，结合多源检测工具及感知手段，构建立体化终端安全风险探知体系，支持入侵识别、病毒检测、访问行为捕获、蜜罐检测等威胁场景的应用。

物联网终端安全管理结构





云安全市场简析

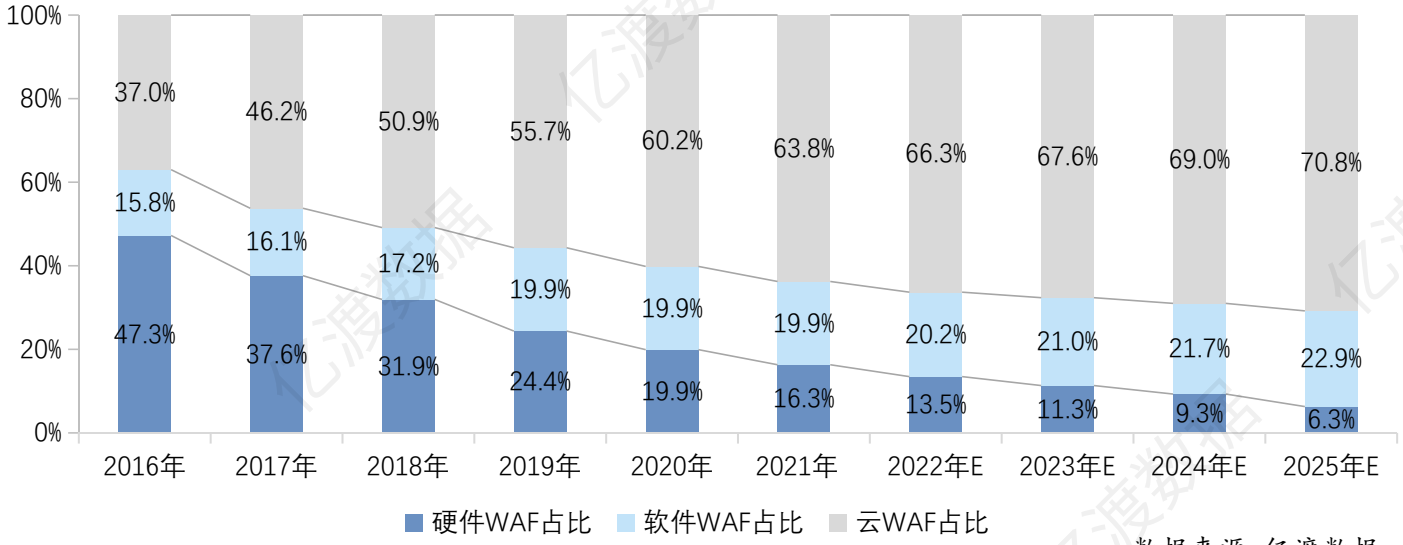
云WAF与云安全领域其他产品共同构成“关键信息基础设施”体系

云WAF基于云基础设施，实现更大范围功能集成

云WAF为WAF防护方案在云端的表现形态，核心能力在于执行针对HTTP、HTTPS的安全防护策略。云WAF依托DNS调度技术实现对原始网络流量的牵引，并对流量进行净化、过滤，最终将安全流量回传至后端真实网络环境，达到保护终端场景Web应用安全的作用。当前，云WAF产品在公有云和私有云场景的应用全面铺开。对云WAF市场各梯队竞争厂商而言，公有云场景对云WAF业务整体营收的贡献较为显著。

中国WAF行业细分市场规模占比（按细分市场营收计），2017-2026年预测

2017年以来，中国云WAF、软件WAF市场份额对硬件WAF市场份额的挤占趋势愈发明晰。未来随政企用户业务全面上云，云WAF市场份额仍将居于首位。预计2022年起，中国云WAF、软件WAF市场份额进入平缓增长周期，硬件WAF、软件WAF、云WAF市场份额占比保持相对平稳态势。



数据来源：亿渡数据

不同云WAF部署模式及特点

当前，部分云厂商已推出采用“反向代理+透明代理”双工作模式或“反向代理+透明代理+镜像代理”多重工作模式的云WAF服务。相对传统单一的反向代理模式，多重工作模式并用的结构能够满足下游用户对简洁部署、初始部署等差异化服务的述求。

反向代理

- 反向代理模式下，真实服务器地址被映射至反向代理服务器，WAF无需劫持客户端与服务器端之间的会话内容

透明代理

- 透明代理模式下，客户端无需知晓代理服务器存在与否，代理云WAF通过改编报文的方式将客户端请求传送至真实地址

镜像代理

- 端口镜像工作模式下，云WAF只对HTTP流量进行监控以及异常流量告警，不采取拦截阻断措施

路由代理

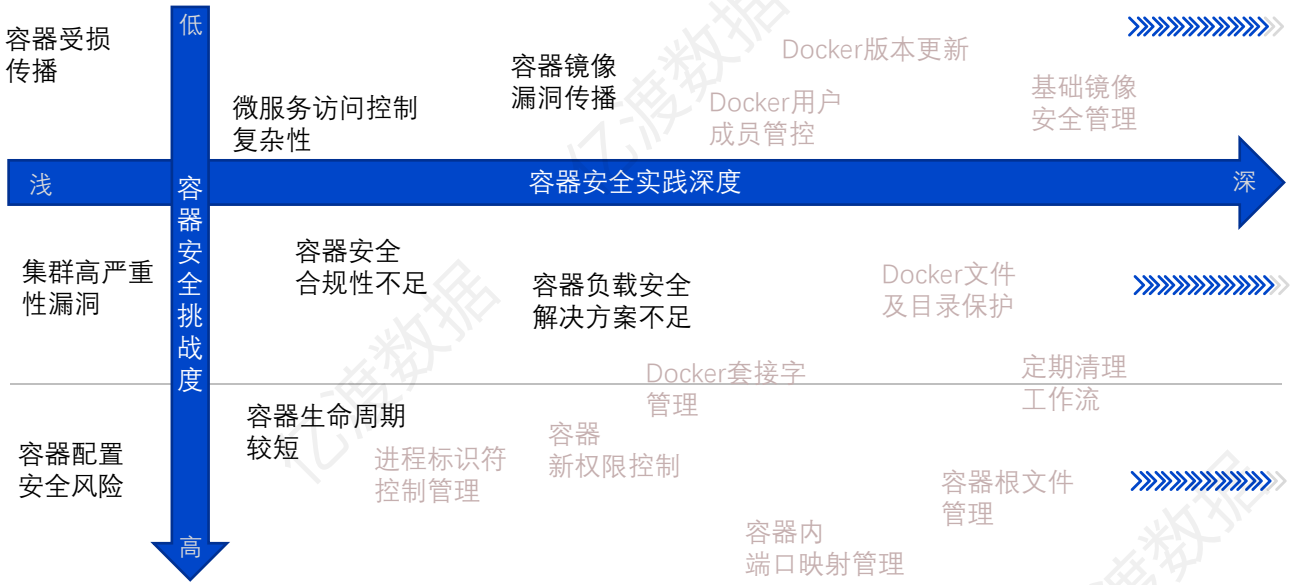
- 路由代理工作与透明代理工作的区别在于转发模式不同；透明代理通过网桥转发，路由代理通过路由实现转发

容器安全 容器安全重点关注容器构建、部署、运行等关键节点安全运维及用户管理

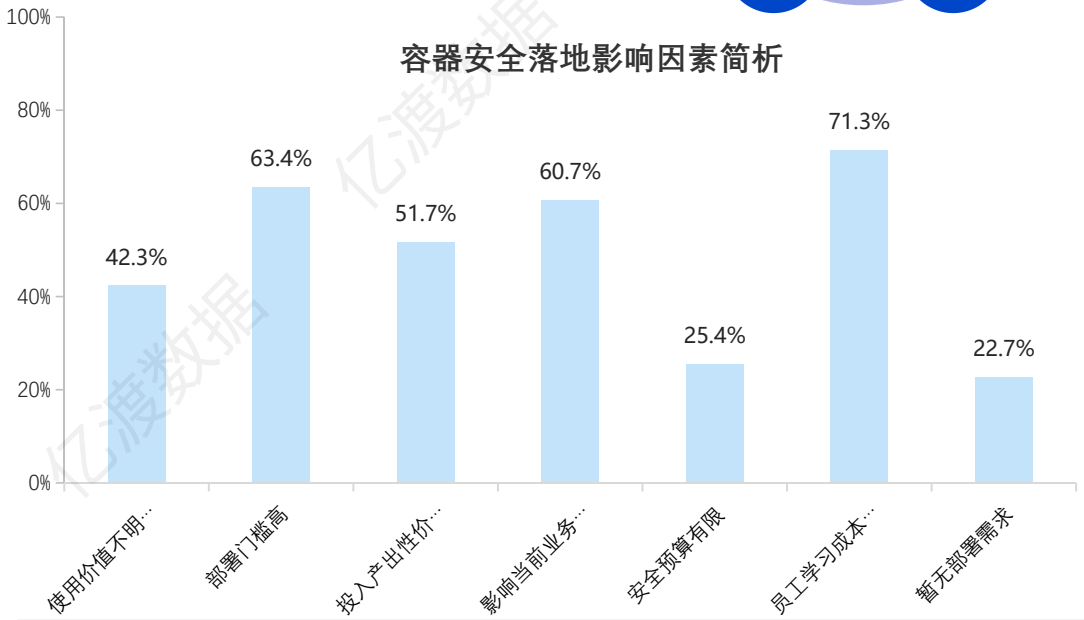
容器安全强化权限控制、运维管理、数据审计，推进全生命周期安全体系构建

容器安全产品是针对容器宿主机、容器软件、容器集群、容器运行时态势、容器镜像及相关基线合规提供的安全解决方案。当前，容器安全防护核心在于主机防护和加固，重点关注Docker 容器安全风险和挑战以及Kubernetes环境下的安全防护实践。相对传统安全模型对于安全边界明晰的划分，云环境下的零信任理念打破传统物理边界，亟需构建体系化的容器安全结构，提高应用侧全生命周期安全防护水平。当前，提供容器安全服务的代表性供应商包括青藤云安全、腾讯云安全、山石网科、阿里云、默安科技、小佑科技等。

容器安全实践与挑战性评价（以Docker为例）



容器安全落地影响因素简析



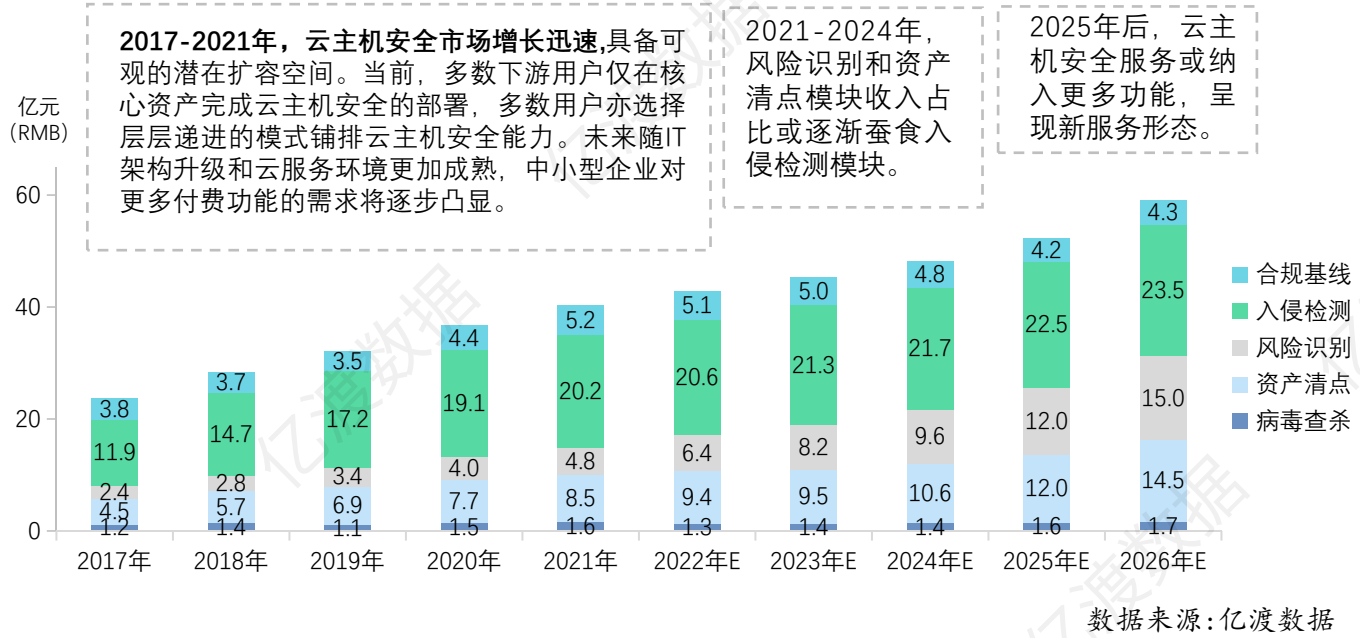
安全管理及安全运营复杂度较高，故而容器安全服务落地受限，影响程度相对较高的因素包括部署成本和学习成本。

云主机安全 资产清点、入侵检测2大功能是决定云主机安全竞争力的核心模块

中国云主机安全市场具备增量扩容空间，下游市场刚性需求显著

随IT产业和云服务市场快速升级扩容，云端主机、设备端主机面临的攻击面扩大，AI算法的应用显著提高安全产品风险对抗能力，但变种攻击和未知威胁的预测仍为难点。网络安全市场整体呈现较强的碎片化特征，云主机安全细分市场或成为网络安全领域第二个防火墙赛道，未来5年，云主机安全细分市场规模年复合增长率将保持在约30%的水平。

中国云主机安全市场规模构成，2017-2026年预测



数据来源:亿渡数据

云主机安全能力拓展，呈现出以安全管控、稳健部署、用户灵活自定义为导向的特点

- **追查攻击外联路径的溯源能力：**

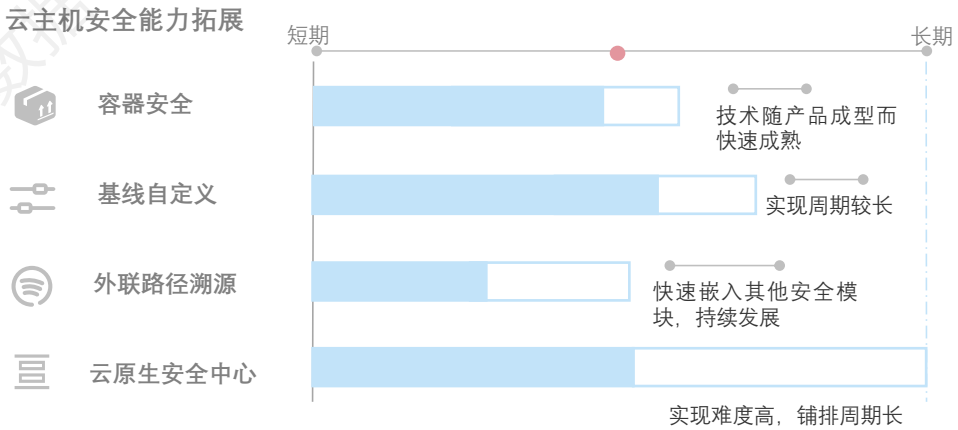
云主机安全基于ATT&CK检测模型形成勒索追踪能力，溯源链路延伸至勒索行为外联路径；

- **防容器逃逸检测能力**

容器逃逸防范工具依赖规模化检测能力和底层I/O数据检测能力；

- **自定义基线检查能力**

更强的差异化基线检查能力或体现在云主机内置安全规则与安全等级规范匹配的细化程度。



云身份管理

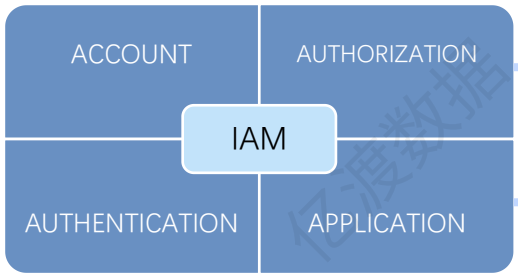
云身份管理模式呈现出由单一认证向整合认证演进的趋势

部署模式持续演进，推动身份管控效率的提升

早期云端IAM服务多面向企业内部员工管理，为内部身份访问管理提供解决方案；信息化进程加速公众版身份认证需求扩容，CIAM提供了面向公众的认证解决方案，相对而言，CIAM在本质功能方面较IAM有了更多拓展，但也面临更艰巨的技术挑战。

作为第三方云服务商构建的专项（IDaaS）身份认证管理云服务，IDaaS从本质上改变了身份管控服务的部署方式，助力企业简化管理方式，大幅减轻身份管控带来的时间及人力成本。

云身份管理（IDaaS）四要素



EIAM

- ✓ 针对员工身份管理
- ✓ 离散式身份认证授权
- ✓ 即时系统维护和更新

CIAM

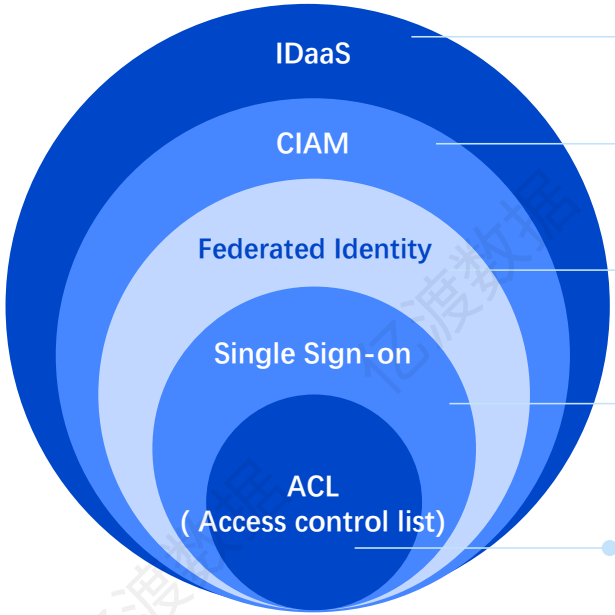
- ✓ 针对消费者身份管理
- ✓ 云上算力所需即所用
- ✓ 安全系数待提升

身份即服务(Identity as a service, iaas)：IAM基于云架构、云算力的灵活订阅模型

云身份管理（IDaaS）从本质上改变了身份管控服务的部署方式，助力企业简化管理方式，大幅减轻身份管控带来的时间及人力成本

数字化转型背景下，身份认证服务模式呈现出由单一认证向整合认证演进的趋势，传统ACL提供单一认证服务，单点登录功能则助力用户一次登陆满足接续验证需求。随身份认证服务流程上云，IDaaS模式依托云算力、云部署，进一步减少繁琐的认证流程，助力企业更加安全高效地实现身份认证管理。

云端数字身份验证模式演进



IDaaS

- ✓ 提供完整的IAM云上解决方案

CIAM

- ✓ 可用于管理客户身份认证
- ✓ 除了传统的认证方式，可对用户画像分析

Federated Identity

- ✓ 在互信的系统中仅需要一次验证

单点登录

ACL

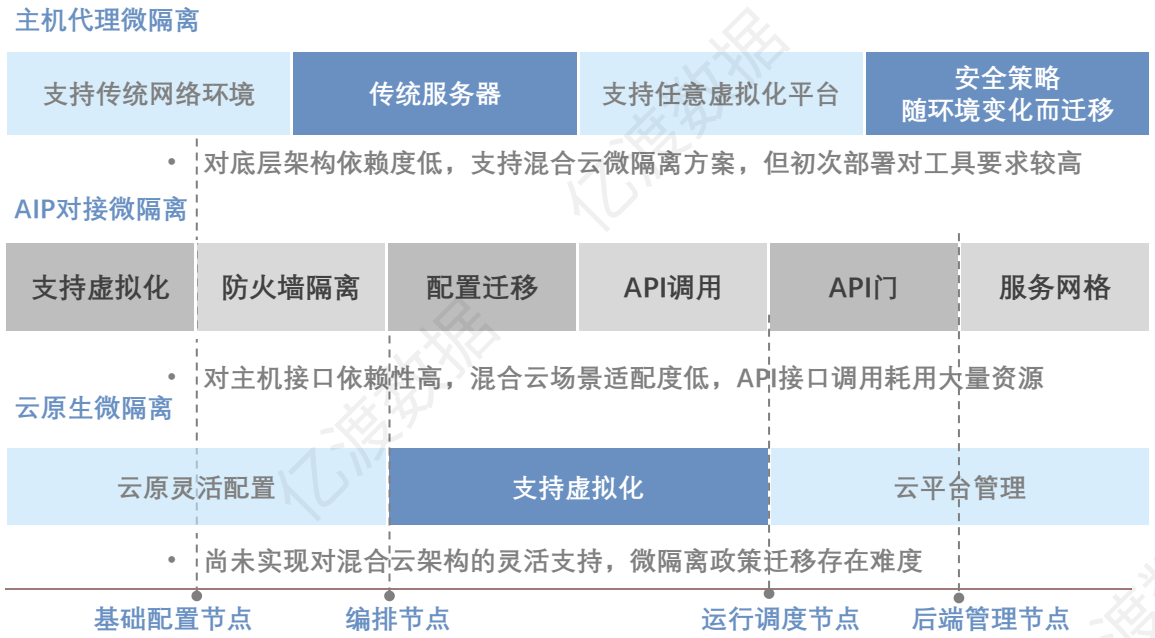
- ✓ 验证方式单一，如用户密码等单一特征信息
- ✓ 用户可通过单个验证码进行身份核验
- ✓ ACL通常支持认证模式在单体系统中的应用
- ✓ 随着运行系统和应用增加，用户需要注册多个账号

低 → 系统适配复杂程度 → 高

微隔离 用户业务架构频繁升级，微隔离技术有效提升安全策略对业务环境的适应性

微隔离主流模式及技术路径简述

微隔离亦可称为软件定义隔离和微分段，通过安全中心将安全策略分配至独立系统，结合传统网络安全技术，控制资源访问和授权，实现安全策略的精细化执行，助力资产间信任体系的构建。主流微隔离模式分为基于主机代理微隔离、基于虚拟机微隔离以及网络隔离。技术路径包括主机代理、API对接、云原生三种，相对而言，当前IT环境下，主机代理模式能够更加灵活应对架构升级和业务环境变化。



微隔离系统助力安全措施的细粒度部署和运维管理

微隔离技术支持下，传统区域层面网络隔离可进一步细化至主机端口隔离、应用隔离、访问隔离、容器隔离等层面，安全中心可依托微隔离架构集中部署防护策略，提升安全策略和系统调度的灵活性，依托可视化技术提升身份验证和策略验证的有效性，抵御外部非法操作及内部违规操作在内网的破坏渗透。

微隔离解决传统网络架构安全问题

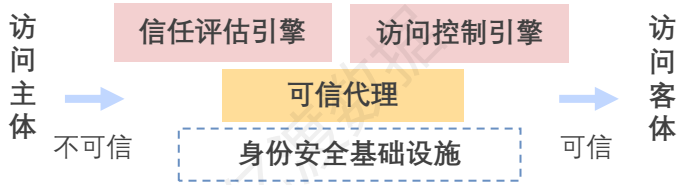
1	**隔离措施缺乏精细化处理：**传统模式下，网络隔离颗粒度下沉至域层面，主要支持南北向流量之间的内外隔离，对域内东西向流量隔离缺乏有效措施，较难防控安全事件在域内的横向扩散，单点突破或导致全域感染；	针对网络隔离缺陷，虚拟化环境隔离技术的出现提供了细粒度策略控制方案，支持业务内外部网络环境隔离，增强东西向、南北向流量可视化程度。
2	**维护策略灵活性不足：**当前网络环境急剧变化，虚拟机部署于离散性业务环境，传统网络隔离策略尚无法支持安全策略对环境的自适应，更新速度不足，安全策略过于复杂对用户正常业务运转造成影响；	
3	**账户访问权限可视化不足：**传统模式下，用户对于内部账户访问不同业务系统缺乏有效隔离管理措施，管理可视化程度较低，易造成系统核心资产泄露，对外部账户渗透内部系统行为缺乏可视化管理。	

其他安全解决方案市场简析

零信任 以“持续验证、用不信任”为基本理念，零信任体系推动访问与授权机制演进

零信任是基于信任动态清零和信任动态赋予的基本理念，助力政企用户实现对身份认证和授权的全域全周期管理。当前，主流零信任架构以身份核验、业务安全访问、持续授权、动态访问控制四部分为核心业务能力构成，助力用户实现全平台身份统一管理、动态授权、风险评估和安全管理自动化。零信任架构关键在于全面消除未授权访问，实现细粒度访问控制。

零信任逻辑架构组件



核心场景零信任应用挑战及方案

应用场景	业务安全核心挑战	零信任解决方案
金融产业场景	✓ 分支机构激增，接入压力大 ✓ 跨界经营，对外接口激增 ✓ 远程接口迅速增加	账号信任最小化；平台与业务信任系统联通；增强弱密码管理有效性
互联网产业场景	✓ 远程办公及运维激增，终端权限控制难度提升 ✓ 物联网海量接入暴露资产	提升终端安全合规性；强化单点登录及运维效率；推动零信任与安全运营中心联动
通信产业场景	✓ 业务暴露面及运维复杂度增加，VPN安全性欠佳	减少资产暴露面，严格进行细粒度访问控制
物流产业场景	✓ 瘦终端配置低，防护难度高 ✓ 安全产品及理念共享度低	提升终端设备安全性、用户身份和权限管理统一性
能源产业场景	✓ 能源网联终端拓扑差异较大 ✓ 认证及授权管理难度大 ✓ 缺乏原生安全技术及措施	通过接入安全代理方式统一终端结构，对人员、资产、应用等采用统一认证和管理方法，降低安全方案对业务影响
地产产业场景	✓ 数据泄露隐患增加 ✓ 内部人员安全意识不足	通过零信任引擎提升新人评估有效性，即时阻断数据泄露

零信任服务体系功能架构

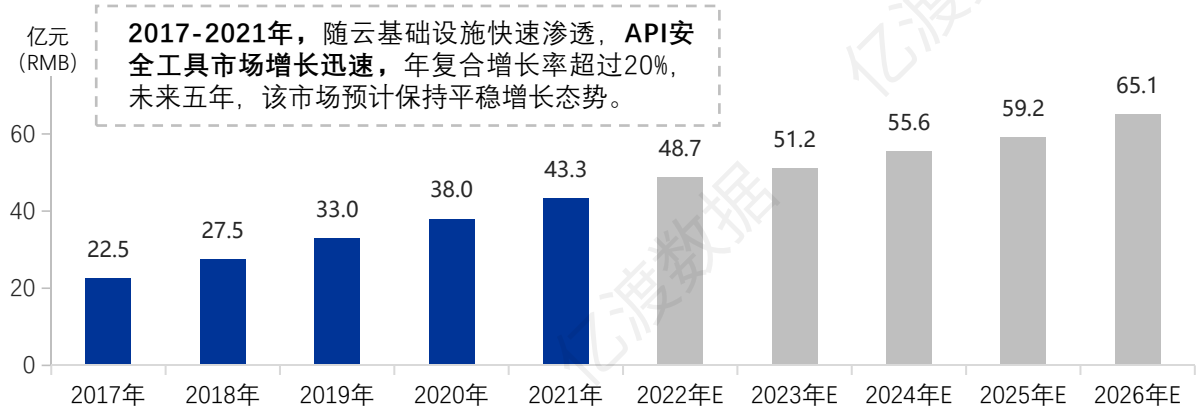
服务商	零信任体系	功能架构覆盖				
		网络安全	终端安全	应用安全	数据安全	身份安全
绿盟科技	ISOP、UIP、SAG	●	●	●	●	●
奇安信	零信任基础架构			●		●
启明星辰	零信任安全解决方案	●	●	●	●	●
蔷薇灵动	蜂巢自适应微隔离安全平台	●		●	●	●
深信服	零信任访问控制体系aTrust	●	●	●	●	●
天融信	零信任安全解决方案				●	●
腾讯云安全	T-Sec零信任无边界访问控制系统	●	●	●	●	●
任子行	智行零信任访问控制系统	●	●	●	●	●

注：服务商名称按照首字母排序，不分先后

API安全 业务侧开放式API应用激增，API安全复杂性提升，为业务安全整体运维带来挑战

随互联网应用普及和数字孪生进展加速，政企业务线上迁移、线上交互频率大幅提升，API调用量随之激增。API作为业务运行关键组件，其安全性、稳定性、可靠性成为保证用户体验的首要需求。当前，API应用所面临核心安全威胁包括端点暴露下的DDoS攻击、应用程序漏洞利用、站点API凭证盗用等，或造成敏感数据泄露、核心数据滥用、数据合规失效的风险。

中国API安全工具市场规模，2017-2026年预测



当前，常见的API防护措施包括API网关控制、API漏洞利用、TLS等加密技术使用、API接口可信身份令牌使用、API接口访问频率限制等。完整的API安全体系由API资产分组归类和资产生命周期管理、API运行及异常行为监控、API层攻击防护及API敏感数据识别和防护四部分构成。未来，随API安全技术演进，防护重点将从绕过攻击、DDoS攻击等向XSS注入、SQL注入、缓冲区溢出攻击等方向转移，防护手段自动化、可视化水平亦将升级。

射频网络安全应达到的效果

API安全策略的实施以云计算服务、API网关、其他平台集成为基础而实现。API应用程序中可能面临的安全事件多存在于程序合并过程中，安全结构呈现多层次特征，安全策略实施效果较大程度受到API构建过程中所选技术栈类型影响。

渗透测试 渗透测试通过模拟恶意行为及其路径，主动发现业务系统安全漏洞

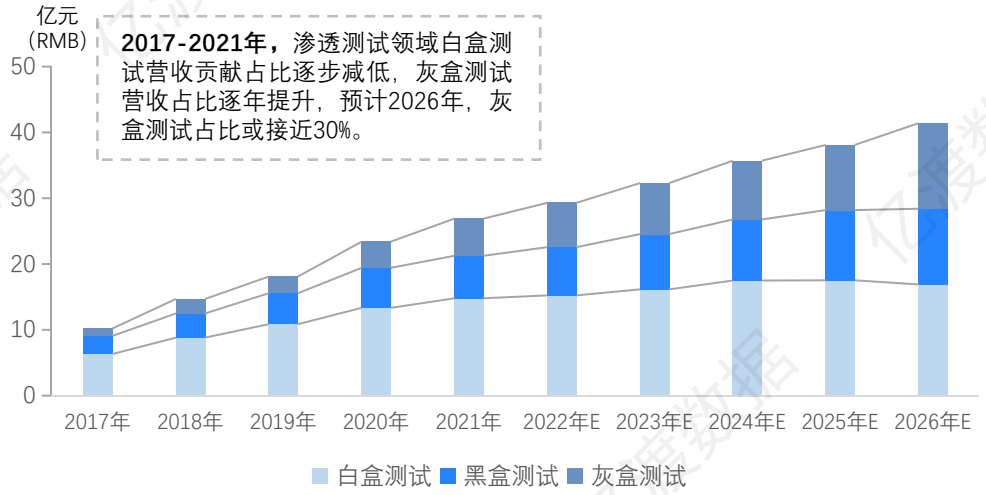
渗透测试本质为授权行为，通过模拟攻击者入侵行为和流程判断系统安全水平。渗透测试人员通过不同攻击手段对指定网络或系统环境进行内部和外部测试，主要针对系统防护弱点、漏洞、技术缺陷进行主动分析，并输出测试结果，根据测试结果反馈可能存在的安全隐患和安全问题，部署相应的安全措施。渗透测试相对漏洞扫描更具深度和精细化程度，从技术层面对系统安全进行定性分析，验证既有安全工具有效性。在安全培训层面，渗透测试结果为内部人员提供安全教学案例；在架构强化层面，渗透测试结果可为安全原则制定提供参考。

渗透测试服务内容及服务环境

云端及终端渗透测试节点及环境

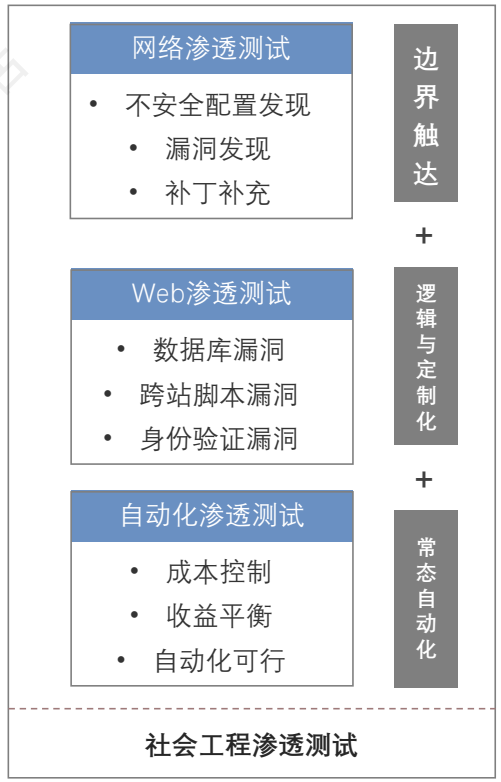
		验证点
安全弱点 路径式串联	Android层面	技术安全性验证
专业化 漏洞发现与修复	iOS层面	安全隐患点验证
漏洞修复 结果验证	网页层面	安全意识验证
漏洞修复 方案评估	移动程序层面	安全原理验证
	制造业/ 工控领域	

中国云渗透测试市场规模，2017-2026年预测



从应用样本角度分类，渗透测试可分为白盒测试、黑盒测试和灰盒测试三类。从执行角度而言，渗透测试是逐步深入的业务过程，以攻击者视角出发，全方位检验业务系统安全架构适宜性和防护措施落实程度及有效性。

渗透测试核心应用场景及特征



身份认证管理

认证因素相关底层技术快速演进，认证因素应用形态趋于饱和

现阶段，密码认证、生物特征认证、短信认证等方式已经成为企业端及公众端主流认证手段。随人脸识别、指纹识别、声纹识别、虹膜识别等生物特征识别技术演进及应用范围扩展，即时交互认证手段在下游市场迅速渗透，IAM领域认证因素市场亦逐步趋于饱和，相对单点技术开发商而言，安全服务商未能在认证因素市场占据纵深技术优势。当前，认证因素相关底层技术的集成助力用户侧形成更为完善的安全系统，而对于安全服务商而言，其身份认证产品并未得到本质优化。远期，安全服务商在认证因素领域或面临逐步收缩的市场空间以及来自智能产业的替代威胁。

认证因素手段及特征简析

基于信息

基于知识的验证方式，基于所掌握的信息进行持续验证

拥有特征

基于用户拥有的某种特征，验证选项如OTP、电子邮件验证

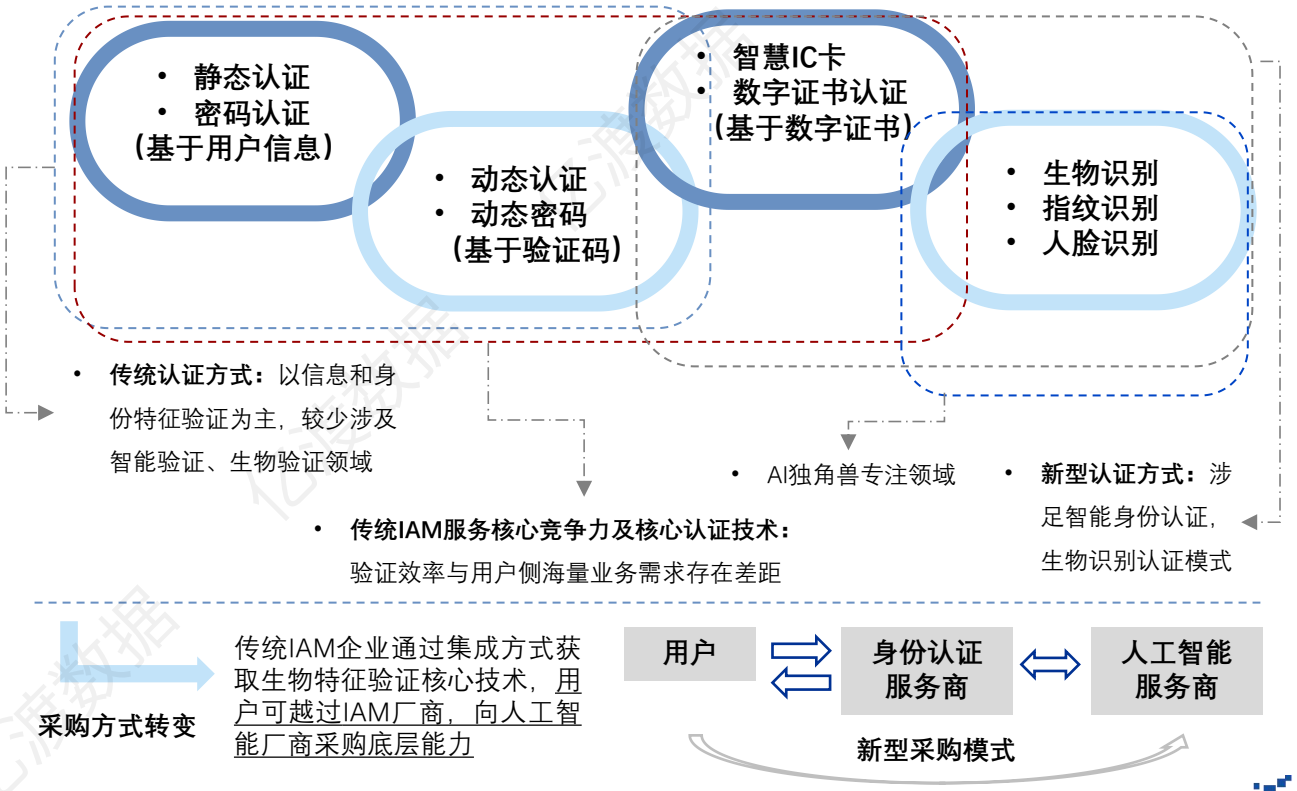
身份特征

基于用户独特的内饰生物特征进行验证

- **底层识别技术直采：**

以金融、政务为代表的下游应用领域认证手段已广泛从指纹识别扩展到人脸识别、声纹识别，为降低中间成本，保持技术模块松耦合度，企业用户多通过识别技术直采或向安全厂商指定技术集成方的方式获取新型认证手段。具备生物特征识别底层技术研发能力的企业多为头部AI企业或AI独角兽，安全体系建设较为成熟的下游用户多向AI企业直接采购识别技术。

身份认证因素市场发展进程



日志分析审计

日志审计系统助力业务人员实现对业务态势和系统安全性的综合性分析管理

安全供应商通过搭建日志审计平台，助力用户全面整合业务系统中包括用户行为、用户访问路径、系统运行情况、安全事件统计、系统漏洞等综合安全信息，平台提供信息分组归类、标准化、脆弱性分析、告警处置等功能，支持对业务系统信息的全方位审计。当前，日志审计核心目标包括多源数据规范、集中化日志存储、多点关联分析、安全立体结构搭建等。依托日志审计平台服务，政企用户管理员可实时掌控业务环境IT系统安全性和运行态势，掌握安全事件位置及路径。此外，通过日志汇总和系统性分析，业务人员可实现对系统信息的针对性安全审计分析，并结合历史汇总分析结果，针对潜在安全事件和系统问题建立快速定位方法，快速跟踪问题并助力业务系统恢复正常。

日志审计系统基础架构及利用效率简析

以业务层特征可视化平台及云端大数据计算平台为基础，为日志统一存储、管理、统计、相关性分析提供基础。

业务层

+

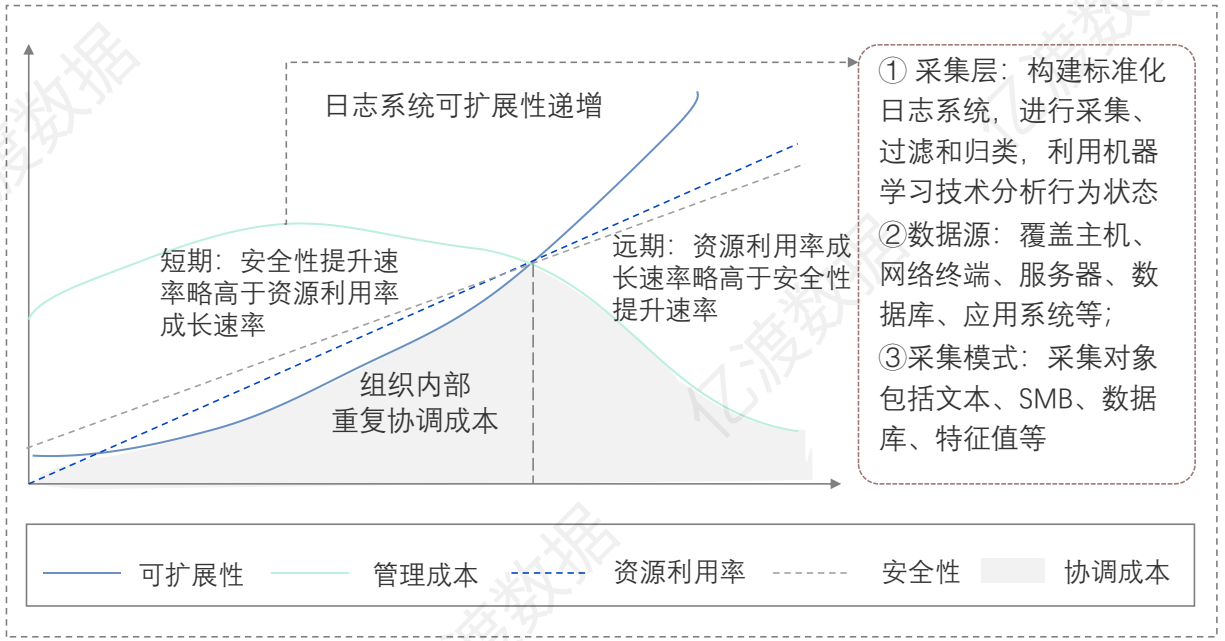
计算层

可视化：综合性查询、告警、钻取、图表统计、趋势分析等

关联分析、告警、审计分析

账户映射关系、规则库、专家经验

大数据分析平台：
标准化、提取、实时分析、统计



有效的日志审计系统需具备以下特征：①日志采集引擎支持至少6个月以上的日志存储；②日志分类清晰，类别可定制、可扩展；③日志管理及访问权限规划清晰，提升日志审计可操作性；④依托自动化分析工具提升日志分析专业性和效率；⑤支持低时延的数据查询需求。

行业典型企业介绍

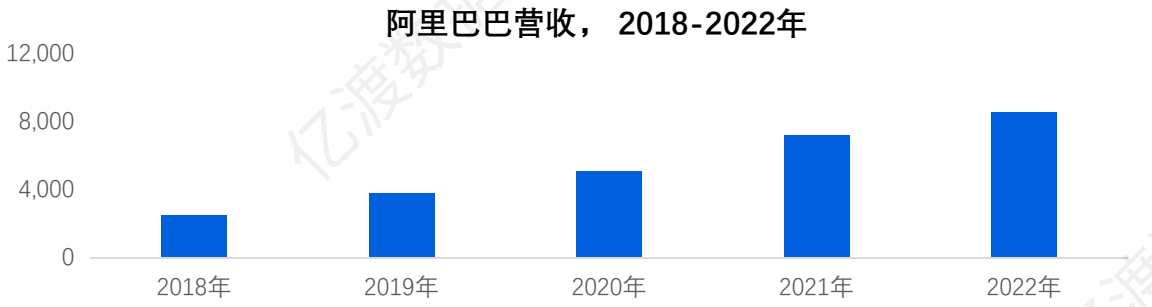
- 阿里云
- 腾讯云
- 绿盟科技
- 奇安信
- 深信服
- 椒图科技
- 芯盾时代
- 青藤云安全
- 蔷薇灵动
- 任子行

大型典型企业 阿里云安全

企业介绍 阿里云

阿里云是阿里巴巴集团旗下云服务供应商，在中国及全球范围属于头部云计算和人工智能科技创新企业，所提供云端服务覆盖云服务器、云数据库、云安全、云应用及部分免费云服务。此外，阿里云提供基于大数据技术、人工智能技术为各行业企业用户及政务用户提供标准化及定制化的前沿解决方案。阿里云服务对象涉及金融、制造、政务、交通、医疗、能源、电信等众多领域。

阿里云安全业务线为市场提供基于云基础设施架构的安全软件和即时安全服务，同时为用户提供安全功能的镜像及相关服务，通过阿里云基础云原生能力实现即开即用的独立安全组件。阿里云安全旗下安全组件覆盖云安全中心、云防火墙、Web应用防火墙、DDoS防护等安全产品。从基础侧、数据侧、应用侧、业务侧、账户侧、运营侧等方面为用户提供全面覆盖的安全服务。



数据来源:公司财报

产品介绍

阿里云安全架构在互联网用户侧提供包括DDoS防御、WAF和云防火墙在内的安全机制，在云企业网侧通过负载均衡、VPC、云防火墙构建公有云云安全中心，在私有云侧则通过高速通道阿里云专线提供专用IDC部署。此外，在数据防护侧，阿里云通过OSS、Redis、ODPS、RDS等板块为用户提供敏感数据防护能力，并于数据库侧提供统一身份授权、堡垒机、RAM、秘钥管理、加密服务、证书等在内的审计服务，其中，RAM服务应用覆盖面包括运维人员、开发人员、办公用户等阿里云用户。

核心产品	产品概要
DDoS防护	针对企业在网络端受DDoS攻击后服务停顿的情况，提供全球部署的DDoS网络清洗服务，依托秒级检测能力和自动化引擎，即时缓解DDoS攻击，保障业务稳定运营。
云安全中心	集成实时识别、实时分析和预警功能为一体，基于防勒索、防病毒、防篡改、合规检查等功能为一体，助力用户构建包括检测、响应、溯源的自动安全运营闭环。
云防火墙	本质为公有云环境下SaaS模式部署的防火墙，针对互联网资产暴露情况提供一键接入的IP管理和访问策略，支持等保2.0对虚拟边界、IPS入侵检测、网络日志管理的合规要求。
数据安全中心	基于业务需求对数据进行分组归类，提供精准化数据权限监控、数据监控、异常检测等安全服务，支持对数据泄露等异常事件进行风险预警和用户信息保护。
内容安全	支持用户对图片、视频、文本、语音等多对象进行场景检测，通过站点检测功能、OSS违规检测功能助力用户降低内容违规风险，支持用户通过调用API的方式识别场景任务。
应用身份服务	阿里云身份服务集身份验证、权限、应用管理服务等为一体，助力用户与本地、云端部署覆盖办公系统、业务系统、第三方SaaS系统身份的一体化通用身份应用服务。

大型典型企业 腾讯云安全

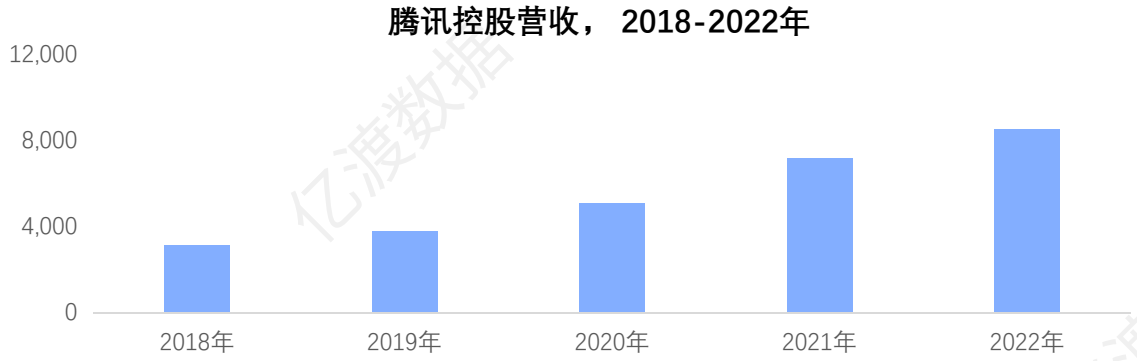
企业介绍

腾讯云

腾讯云安全在安全技术开发和应用研究、安全运营及安全平台保障方面持续演进，随机器学习技术、大数据技术应用的渗透和成熟，腾讯云安全实现对各层级风险信息的实时监控，以及对各类安全事件的挖掘和预警，助力政企用户抵御快速演变的APT攻击。

腾讯云安全旗下七大安全实验室联合开展对安全漏洞的研究，并将漏洞信息实时下发至各安全平台和应用场景，以提升云计算平台整体的安全性。

通过平台保障、事件响应和预警、漏洞挖掘与修复、恶意行为打击、安全解决方案等板块的联动，腾讯云安全为各类政企用户提供全方位覆盖的安全防护网。基于自身在云计算基础设施方面的技术先导优势，腾讯云安全为客户云端业务和数据资源提供日趋完善的保障网。



数据来源:公司财报

产品介绍

依托腾讯安全大脑，构建自适应闭环安全防护安全体系，覆盖安全运营中心、业务安全服务体系等，产品矩阵包括终端安全、网络安全、云安全、业务安全、数据安全、安全管理、安全服务等。

网络安全

- 威胁追溯及情报查询
- 高级威胁检测系统
- 主机安全及堡垒机
- 安全运营中心零信任网关
- 移动安全小程序安全
- 企业移动管理网络入侵防护

终端安全

- 主机安全
- 零信任安全管理
- 企业移动管理

数据安全

- 堡垒机
- 数据安全审计
- 敏感数据处理

应用安全

- 移动安全小程序安全
- 移动安全开发安全
- 移动安全数据安全
- 移动安全数据库安全

业务安全

- 风控平台
- 保险反欺诈
- 营销风控
- 内容安全
- 保险反欺诈

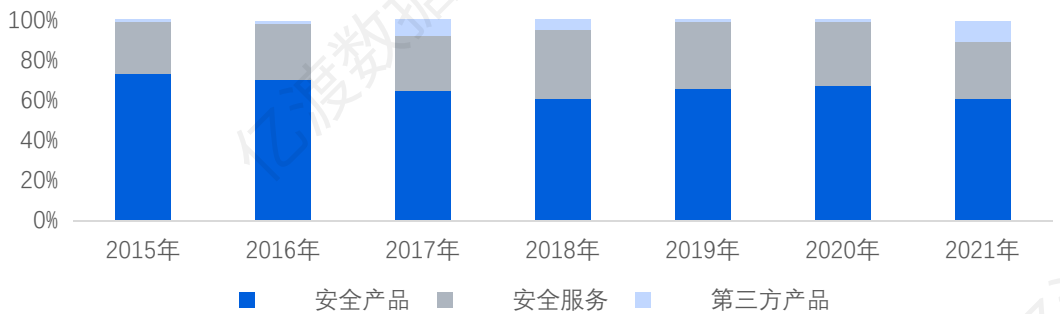
大型典型企业 绿盟科技

企业介绍

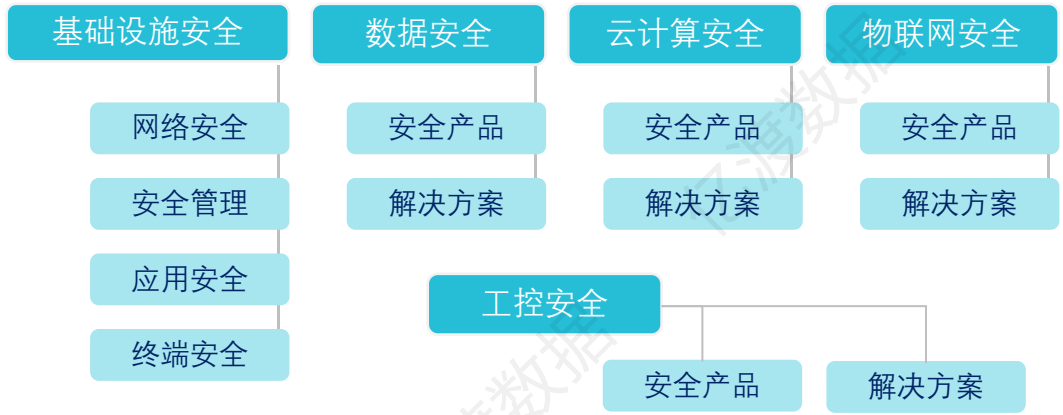
绿盟科技所提供的安全管理服务是基于“安全运营+”的安全运维和安全技术保障一体化智慧安全运营方案。绿盟科技在北京、武汉、成都、美国硅谷建立研发中心，其中，接近60%的员工为公司研发及技术人员，为公司发展积累充足的人才储备。

绿盟科技创立于2000年，为政务用户、运营商、金融、能源、互联网、教育、医疗等领域用户提供全栈网络安全产品，以及全方位的安全解决方案和系统化的安全运营服务。绿盟科技的安全业务产品线覆盖基础设施安全（网络安全、安全管理、应用安全、终端安全、身份与访问管理等）、数据安全（产品及解决方案）、云计算安全（产品及解决方案）、物联网安全（产品及解决方案）、工控安全（产品及解决方案）等，并持续推动技术应用创新。

绿盟科技业务营收占比， 2015-2021年



数据来源:公司财报



企业优势

- 技术研发实力持续强化：绿盟科技参与公安部、国家信息中心、证券业协会、中国电信等国家、行业、企业级别各类安全运营规范和安全防护标准的制定工作，绿盟科技建立的中文漏洞库应用范围持续扩大，在抗拒绝服务、漏洞扫描等方面具备先发优势。
- 建设智慧安全体系：绿盟科技依托对企业安全体系的理解和架构搭建，将智能、敏捷、持续运营作为“智慧安全”战略转型的要点，通过运用所积累的安全能力，为众多用户提供小时级响应。
- 售后支持灵活即时：绿盟科技在北京、上海、广州、武汉等地建立分公司及分支机构，为各地区用户提供即时技术支持。

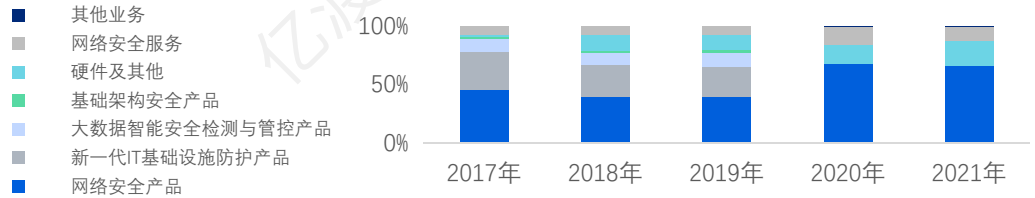
大型典型企业 奇安信

企业介绍

奇安信成立于2014年，为政府、企业用户提供网络安全领域新一代产品和服务，在安全理念方面提出网络安全建设三部曲，助力政企用户高效应对数字时代网络安全领域的挑战。依托持续创新和实战攻防演练，奇安信建立起基于大数据技术和人工智能技术的安全运营全栈产品体系和解决方案，在全球范围布局广域安全服务运营体系（分支机构遍布印度尼西亚、新加坡、加拿大等国家）。2020年，奇安信在科创板挂牌上市。

奇安信集团在基础产品架构方面围绕软件和硬件同步进行开发，在硬件侧构建根本性防御，在软件侧通过安全应用开发保护用户资产安全。在新一代IT基础设施防护方面，奇安信聚焦泛终端业务、新边界业务、大数据业务等，依托大数据智能安全检测与管控产品对数据进行自适应检测和快速响应服务，结合SaaS、软硬件集成、纯软件等模式为用户提供威胁灵敏检测、态势感知、安全管理等服务。

奇安信业务营收占比，2017-2021年



数据来源：公司财报

主要产品

基于政企用户在数字化转型时代对内生安全、动态安全、安全机制联动等方面的需求，依托大数据技术、人工智能技术以及在实时网络攻防、平台化建设等方面积累的技术优势和实战能力，结合政企用户切实业务特征，搭建新一代网络安全产品架构。奇安信提供的全栈安全防护方案覆盖态势感知、数据安全、云安全、工业安全、终端安全、边界安全、应用安全、开发安全、电子取证、信创等板块。

- 态势感知：监管、运营、攻防态势感知
- 数据安全：数据安全防护、零信任、身份认证
- 云安全：计算安全、容器安全、网站云安全
- 工业安全：安全防护、检测审计、运营管理
- 终端安全：办公终端、移动终端防护
- 边界安全：网关、网络隔离、网络入侵检测防御
- 开发安全：代码安全、漏洞扫描和应用交付系统
- 电子取证：终端取证、网络空间取证

大型典型企业 深信服

企业介绍

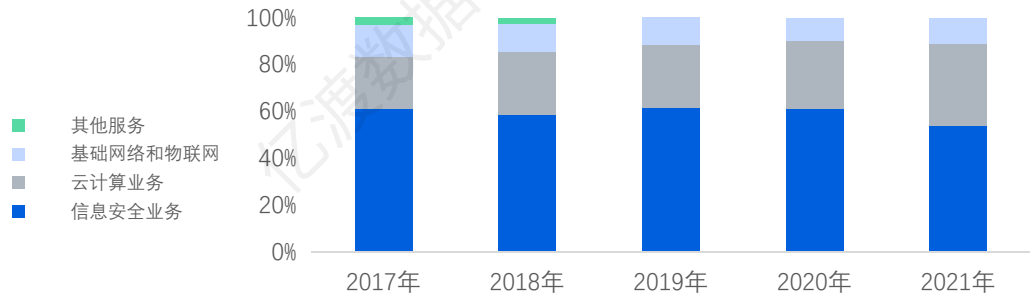
深信服科技股份有限公司（以下简称“深信服”）成立于2000年12月，是一家以企业级安全、云计算服务、IT基础设施产品和服务为核心业务的技术方案供应商，旗下包括深信服智安全、信服云、深信服新IT三个主要业务品牌。深信服在全球范围广泛布局，设立国际分支机构超过50个。

在云业务板块，深信服推动传统数据中心的云化演进，提供包括超融合、分布式存储、私有云、桌面云、托管云等在内的产品。

在安全业务板块，深信服提供的产品和服务聚焦于防火墙、安全感知、等保合规、EDR、广域网安全、边界安全、行业安全解决方案等领域。

当前，深信服在全球范围拥有超过10万的企业用户数量。截至2022年4月，深信服申请专利综述超过2,350个。

深信服业务营收占比， 2017-2021年



数据来源:公司财报

产品介绍

深信服以用户为中心进行研发，依托云端算力和人工智能技术支撑，提供有效的安全保护产品和服务策略，建立人机共同智慧的主动安全监测和自动闭环处置系统，助力用户实现网络安全检查的常态化。

边界安全

核心为融合边界对抗威胁的下一代防火墙，具备多重智能模型和手段

终端安全

包括终端检测响应平台EDR和企业移动管理平台EMM

云安全

云眼：持续风险评估和实时监测；云盾：自动处置、在线值守集成

态势感知

面向全行业的大数据安全分析平台，及检测、可视、响应于一体

安全审计与运营

推进数据安全防护和大数据分析技术融合，提供完整数据库审计服务

身份访问与安全

支持最小化访问权限，以多元加密技术和认证方式，确保身份安全

大型典型企业 任子行

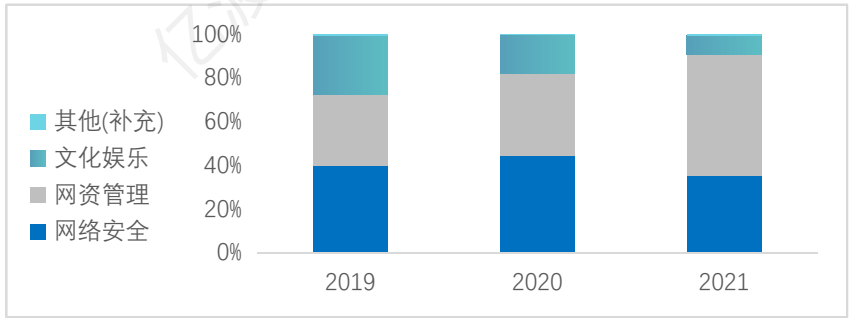
企业介绍

任子行网络技术股份有限公司成立于2000年5月，并于2012年4月，在深圳证券交易所创业板正式挂牌上市（**证券代码 300311**）。业务涵盖5G、网络安全、信息安全、公共安全、网络资源安全、工业互联网安全等众多领域，已成为国内技术最为全面的大规模网络空间安全防护解决方案提供商。

任子行在全国拥有30余处分支机构，服务客户10余万家。是国家多部委重大网络安全工程建设骨干团队，也是国家网络安全服务支撑单位。

任子行立志于围绕国家在网络空间治理和网络安全保障方面的战略需求，从网络犯罪治理、信息安全治理、网络安全治理三大领域入手，突破网络空间安全治理支撑性关键技术，致力成为国家网络空间安全治理工作的核心技术支撑力量，**国内领先的“网络空间数据治理专家”**。

任子行业务营收占比，2019-2021年



数据来源:公司财报

主要产品

任子行专注于为用户网络提供零信任安全、数据安全、边界安全、安全感知、安全接入、安全审计、安全服务等全方位、立体化的网络空间安全防护解决方案。主要面向企事业单位、医疗、教育、金融、军工、通信运营商、能源、连锁酒店商超等客户，是传统及新兴网络安全市场生态的重要建设者、信息技术应用创新的实践者。

零信任安全

浏览器
客户端
SDK
安全大脑
安全网关
API网关

数据安全

数据库防火墙
数据库运维
数据库加密
数据防泄漏
动态脱敏
静态脱敏
视频防泄密

边界安全

下一代墙
入侵检测
入侵防御
防病毒网关
网闸
光闸
WAF

安全感知

态势感知
安管平台
漏洞扫描

安全接入

SD-WAN
视频防火墙
安全审计网关
安全审计AP

安全审计

网络审计
日志审计
运维审计
数据库审计
行为管理

安全服务

安全加固
安全评估
安全咨询
安全培训
渗透测试
攻防演练
应急响应
重保服务

新型典型企业 椒图科技

企业介绍

安盾椒图科技有限公司（以下简称“椒图科技”）是中国网络信息安全领域主机安全产品和服务供应商、等保合规解决方案供应商。
椒图科技持续打造国产自主可控的信息安全保障系统，长久专攻安全操作系统的研发，基于国家安全等级保护制度，为用户提供安全产品。
椒图科技自主研发多模态的JHSE主机安全环境系统，适用于Linux Server、 Windows Server等商用服务器操作系统。
椒图科技安全产品广泛应用于政务、国防、金融、能源、税务、海关等核心领域。其团队在服务器操作系统安全领域积累超过10年的研究，并于2005年参与《信息安全技术信息系统安全等级保护基本要求》的起草工作。此外，椒图科技与政府、研究机构等各类组织开展多重合作，通过技术先导、优势互补等方式持续扩大影响力。

椒图科技融资情况，截至2022年6月

时间	2018-09
轮次	A轮
融资金额	8,000万人民币
投资方	奇安投资

数据来源：IT桔子

竞争优势

椒图科技推出“云锁”，在外部资产感知、应用识别、资产导入/导出方面构建具备技术和架构先导性的资产管理架构，依托多维度的可定制化界面为用户提供全视角服务器信息资产管理服务。

产品介绍

资产管理

主机搭载Agent，自动识别相关外部访问环境，依托自动化识别、资产信息自动化导入导出强化对资产的精细化管理

安全运维

覆盖恶意代码扫描、漏洞和补丁管理、合规性检查、弱口令检查、批量运维等领域，强化安全与运维的全域结合

流量控制

通过流可视化、微隔离技术、异常流量、外联控制四个板块实现对业务流量的清晰管理，快速处置主机异常情况

动态防御

包括入侵检测、RASP应用运行时自我保护、操作系统内核加固、文件防篡改和完整性保护、防爬虫/扫描器等多维度防御策略

攻击溯源

以命令审计、攻击溯源、安全日志等手段为支撑，基于大数据分析，对安全日记进行关联分析，全面追踪系统安全问题

系统及审计管理

支持双重身份认证，将系统管理员、安全管理员和审计管理员三个角色分立；打造具备抗抵赖性、高可用性的安全日志

新型典型企业 芯盾时代

企业介绍

北京芯盾时代科技有限公司（以下简称“芯盾时代”）于2015年07月23日在北京成立。芯盾时代是业务安全产品和服务的供应商，提出“以人为核心的业务安全”理念，依托人工智能技术，为用户提供全面契合业务场景的全生命周期安全防护方案。2020年9月，芯盾时代获得数亿元C+轮融资。

产品介绍

芯盾时代具备代表性优势的技术领域包括统一终端安全、智能决策大脑、零信任网络访问等多重维度。核心业务线为智能业务安全产品线、零信任企业安全产品线。芯盾时代依托人工智能技术和零信任架构为企业用户提供可维持业务系统安全稳定运行的安全服务系统，应用覆盖移动办公安全、全场景统一身份管理、边界安全防护等方面。

芯盾时代融资情况，截至2022年6月

时间	2015-10	2017-03	2017-12	2020-09
轮次	A轮	B1轮	B2轮	C+轮
融资金额	未知	227.7万人民币	1.2亿人民币	数亿人民币
投资方	未知	SIG海纳亚洲 红点中国等	云锋基金 昊翔资本等	国泰财富 SIG海纳亚洲等

数据来源：IT桔子

竞争优势

芯盾时代基于自身在企业身份管理平台积累的大量实战经验，领先构建零信任业务安全平台，支持对用户操作行为的持续分析和动态分析，为企业用户提供跨组织架构、跨业务系统的安全保障。
芯盾时代所提供的安全解决方案渗透政务、金融、运营商和大型企业，动态分析用户行为，所提出的全场景安全治理方案普遍受到市场认可。

智能业务安全产品

覆盖用户身份与访问管理、操作系统用户身份与访问管理、特权用户躬与访问管理、双因素认证和企业移动管理

零信任企业安全产品

覆盖安全客户端、安全应用网关、安全API网关、动态访问控制引擎、智能安全大脑、安全运营中心等板块

跨场景跨组织解决方案

- 覆盖金融、互联网、政务、运营商、大型企业等领域的用户
- 多重领域应用移动APP安全解决方案，金融领域更多依靠零信任和全场景身份治理解决方案
- 大型企业侧解决方案热点可以车联网安全解决方案、移动办公安全解决方案、互联网营销反欺诈解决方案为代表

新型典型企业 青藤云安全

企业介绍

青藤云安全于2014年成立于北京，在主机端构建集预测、防御、响应、监测为一体的服务器安全防护体系。青藤云安全打造的主机端态势感知平台助力用户实现对安全事件的持续监控、分析和快速响应。在应用环境层面，青藤云安全支持公有云、私有云、混合云等多维度的业务环境，支持安全策略统一下发和统一管理，在风险预测、威胁感知等方面实现精准管理，提升安全事件的响应效率。在场景侧，青藤云安全服务渗透金融、运营商、大型企业、互联网、医疗、教育等领域。青藤云安全具备较强的技术自主研发、技术自主突破能力，在主机安全和容器安全、威胁狩猎平台构建等方面持续应用领先研究成果。在漏洞发现领域，青藤云安全依托自有实验室和各类自动化分析工具，在多项安全攻防活动中表现突出，持续为用户提供快速响应服务。

青藤云安全融资情况，截至2022年6月

时间	2014-08	2015-12	2018-02	2021-06
轮次	天使轮	A轮	B轮	C轮
融资金额	650万	6,000万	2亿人民币	6亿人民币
投资方	真格基金 云天使基金 丰厚资本	红点中国 宽带资本等	红杉资本 红点中国 真格基金等	GGV纪源资本（领头） 博华资本 红杉资本等

数据来源：IT桔子

产品介绍

在产品侧，青藤云安全推出青藤万相、青藤蜂巢、青藤猎鹰、青藤雷火四个产品线，核心覆盖主机、云原生、威胁情报、检测引擎等系统。

青藤万相主机自适应安全平台

01 基于自适应安全架构，将传统防御手段转为主动防御策略，集成资产清点、风险发现、入侵检测、合规基线和病毒查杀五个模块

青藤蜂巢云原生安全平台

02 通过对容器安全情况的监控和分析，为用户展现容器应用的全生命周期安全

青藤猎鹰威胁狩猎平台

03 助力用户深度应用ATT&CK模型下的攻防经验，挖掘安全数据，实现事件溯源、安全能力整合等多个目的

青藤雷火AI-Webshell检测系统

04 自研Webshell检测引擎，基于AI推理技术，融合各类威胁变形和混淆，持续提升在公开测试和强对抗环境下的检测能力

新型典型企业 蔷薇灵动

企业介绍

北京蔷薇灵动科技有限公司（以下简称“蔷薇灵动”）基于微隔离技术针对云端智能计算中心东西向流量管理提供端到端的解决方案。应用场景覆盖政企网络内部安全规范和管理、混合云架构下统一安全管理策略实施、容器隔离方案部署实施以及DevSecOps的全生命周期开发和部署方案等。2022年，蔷薇灵动入选北京市“专精特新”中小企业名单。

当前，蔷薇灵动所服务的客户群体主要涉及金融、政务、运营商、互联网、能源等领域，通过强化安全管理可视化、模型精简化、安全策略自适应调整、流量联动分析、漏洞精细化管理等方式，助力用户降低安全策略部署与优化所需时间成本，提升安全管理效率，并快速适应和应用环境隔离、网络域隔离、端到端隔离等模式下的安全策略，实现对内外部流量更细颗粒度的安全策略管理。

蔷薇灵动融资情况，截至2022年6月

时间	2021-09
轮次	A轮
融资金额	近亿元
投资方	腾讯投资、琥珀资本 东方富海等

数据来源：IT桔子

产品介绍

蔷薇灵动以微隔离细分领域为核心业务，构建覆盖可视化管理、混合云统一安全管理、安全智算中心、勒索病毒管理等板块的业务架构。

1、可视化业务拓扑
于混合云环境统一绘制流量拓扑图，以交互式呈现方式助力用户控制和调整流量、策略

2、策略型安全管理模型
依托可视化、精简化模型构建安全策略，通过自然语言提供应用及虚拟机定义法

3、基于自适应算法的策略
结合微隔离技术，实现端到端身份及访问控制

4、异常流量分析
针对全域流量进行监控，为端到端流量提供攻击溯源、合规性检查等查验能力

5、漏洞分析与屏蔽
基于微隔离技术，分析工作负载漏洞，并未用户提供漏洞攻击分析及屏蔽方案

6、混合云统一安全管理
针对操作系统提供多云、跨云、跨平台统一安全管理服务

蜂后：安全计算中心
依托即时计算构建拓扑结构，持续通过计算优化安全策略，推送至应用终端

蜂群：安全管理终端安装
安全控制引擎实时汇集工作流信息至安全计算中心，计算中心发布策略对工作流安全态势进行精准调试

法律声明

版权声明

免责声明

本报告中行业数据及相关市场预测主要为行业研究员采用桌面研究、行业访谈、市场调查及其他研究方法，建立统计预测模型估算获得，只提供给用户作为市场参考资料。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。在不同时期，亿渡数据可能撰写并发布与本报告所载资料、看法及推测不一致得报告。本公司不保证本报告所含信息及资料保持在最新状态，本公司将随时补充、更新和修订有关信息及资料，但不保证及时通知或发布。在任何情况下，本公司亦不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。