头豹 LeadLeo

www.leadleo.com

2023年
中国工业信息安全行业概览

2023 China Industrial Information Security Industry Overview

2023 年中国産業情報セキュリティ産業の概要

概览标签：工业信息安全、网络安全、工控安全

报告主要作者：孙艺霞

2023/10

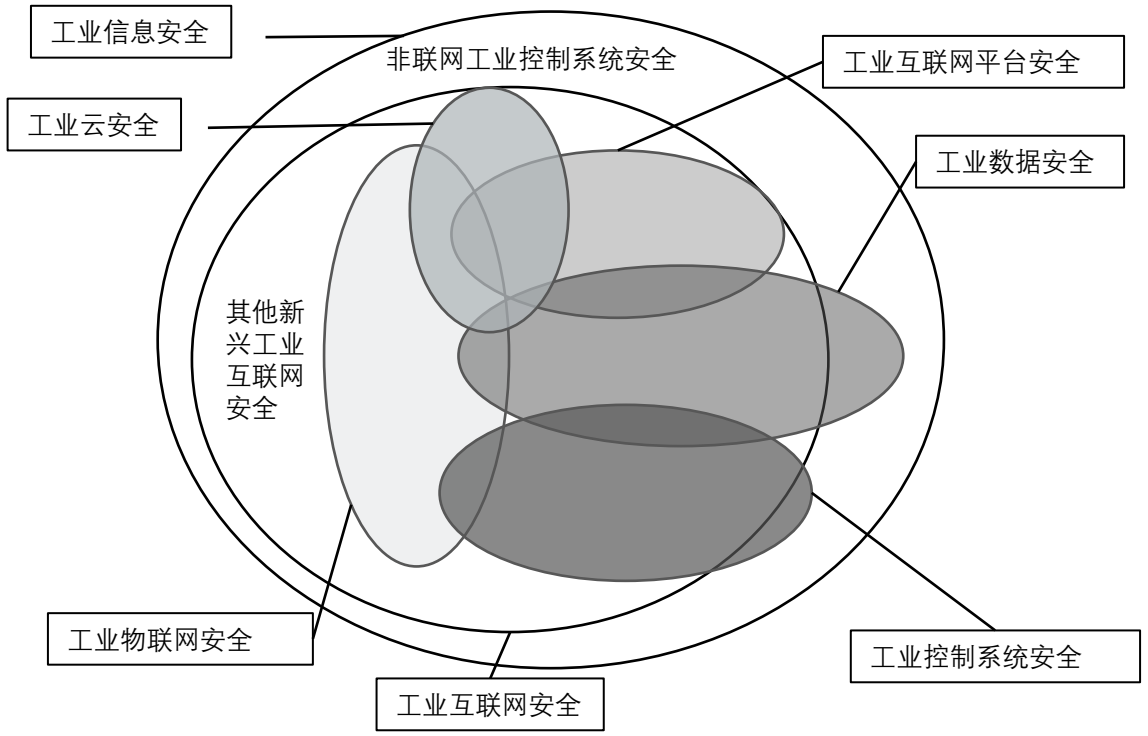
中国工业信息安全概念界定

工业信息安全是工业领域信息安全的总称，涉及工业领域各个环节，包括工业控制系统安全、工业数据安全、工业云安全等内容

工业信息安全相关概念

概念	定义
工业信息安全	是工业领域信息安全的总称，涉及工业领域各个环节。
工业互联网安全	工业互联网是满足工业智能化发展需求的关键网络基础设施。工业互联网安全即保障工业互联网现场设备、工业控制系统、网络基础设施、工业互联网应用、工业数据等各层防护对象的安全。
工业控制系统安全	工业控制系统是指用于操作、控制、辅助自动化工业生产过程的设备、系统、网络及控制器的集合，工业控制系统安全即保护工业控制系统或网络中的信息资源免受各种类型的威胁、干扰和破坏。
工业数据安全	工业数据是指在工业领域中，围绕典型智能制造模式，整个产品全生命周期各个环节所产生的各类数据及相关技术和应用的总称。工业数据安全即保障这类数据的安全。
工业云安全	工业云是一种面向工业的，通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的模式。工业云是工业互联网平台及工业物联网的基础技术，工业云安全是保障云中的系统、基础设施和数据的安全。
工业互联网平台安全	工业互联网平台是边缘数据采集系统、云计算基础设施及其上的开发、 应用、服务等软件的集合，是传统工业云平台的迭代升级。工业互联网平台安全涉及边缘层、平台 IaaS 层、平台 PaaS 层及平台 SaaS 层四个层面的安全防护。
工业物联网安全	工业物联网是物联网在工业领域中各类应用的总成，是实现广义工业领域范围的智慧应用及信息共享的基础平台。工业物联网安全即保障这类基础平台的安全。

工业信息安全概念关系图



- 工业信息安全泛指工业运行过程中的信息安全，涵盖范围广，既包括未连入工业互联网的工业系统和设备的安全，也包括了工业数字化、网络化及智能化运行过程中涉及工业领域的各个环节的安全。工业信息安全的本质是确保完成工业生产任务的流程不被篡改或破坏，实现正常的生产过程、完成既定的生产目标，且生产执行过程的要素流动不被监控或盗取。

来源：工业信息安全产业发展联盟、头豹研究院

中国工业信息安全技术体系及发展应用

中国工业信息安全技术体系主要包括外建安全和内嵌安全两类，其中外建安全中的防护类技术成熟度较高且市场应用水平较广，内嵌安全防护技术的市场应用水平整体偏低

工业信息安全技术发展成熟度与市场应用程度

- **中国工业信息安全技术体系包括外建安全和内嵌安全两类，其中外建安全中防护类技术如应用程序白名单、网络隔离等的成熟度及市场应用水平也较高，在基于指纹匹配的资产识别、基于漏洞库的风险关联、威胁溯源等检测类和响应类技术方面尚存在不足；内嵌安全防护方面，中国在通信访问控制、通信和数据加密、身份识别等技术方面已有突破但市场应用水平整体偏低。**

来源：专家访谈、中国工程院院刊、头豹研究院

02

市场分析

中国工业信息安全产业链布局

工业信息安全产业链完善，主要包括上游基础软硬件及网络设备与服务、中游工业信息安全产品与服务以及下游的各行业用户，中游参与者众多、市场竞争激烈，下游产品可在多领域应用

中国工业信息安全产业链

上游-基础软硬件/网络设备及服务

基础硬件

基础硬件包括服务器、存储器、芯片等，其中中国服务器行业自产率高，国产替代趋势明显

HUAWEI　SAMSUNG　inspur 浪潮　SK hynix　中科曙光 Sugon

基础软件

基础软件包括操作系统、数据库、中间件、虚拟化软件等，其中麒麟软件占据中国Linux操作系统市场第一

KYLINSOFT 麒麟软件　中科方德 NFS-CHINA 基础软件国家工程研究中心　IBM　红旗 Linux

网络设备及服务

网络设备包括交换机、路由器、WLAN等，其中新华三、华为位列企业级网络设备生产市场第一梯队

CISCO　H3C　HUAWEI　中国电信 CHINA TELECOM

中游-安全产品/服务

信息安全厂商

凭借传统IT信息安全技术发力工业安全领域

天融信 TOPSEC　NSFOCUS　360数字安全 数字安全的领导者

自动化背景厂商

主要通过成立子公司或工控安全部门进入工业信息安全领域

Schneider Electric　和利时 HollySys　中控·SUPCON

专注工业信息安全领域厂商

在应用领域上，各家企业拥有各自优势领域

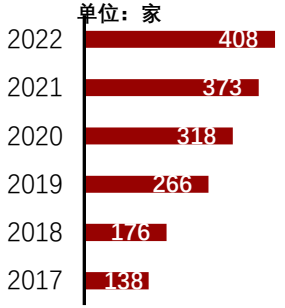
6cloud 六方云　长扬科技 CHANGYANG TECH　TDHX 天地和兴

系统集成商

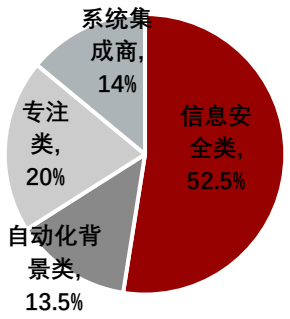
通过与安全厂商合作开发安全软硬件产品从而进入工业信息安全领域

H3C　HUAWEI　inspur 浪潮

中国工业信息安全企业数量，2017-2022年



中国工业信息安全厂商分布，2022年



下游-各类用户

- 能源电力类用户
- 石油石化类用户
- 烟草类用户
- 装备制造类用户
- 烟草类用户
- 轨道交通类用户
- 航空航天类用户
- ……

国家能源集团 CHN ENERGY　Sinopec　中国石油　广汽集团 GAC GROUP　中国铁建　中国中铁　中国航天　中国烟草 CHINA TOBACCO

下游行业应用占比情况，2022年

来源：企查查、头豹研究院

中国工业信息安全应用场景（1/4）：电力

电力行业是目前中国工业信息安全建设成熟度最高的行业，在行业应用中占比40%，2022年的安全投入达41.27亿元，受政策合规及电力行业信息化建设浪潮影响，未来5年市场规模将以15.4%的增速增长

工业互联网安全行业应用情况，2022年

电力行业工业信息安全市场规模，2018-2027年预测

中国工业信息安全产品在电力行业的应用，2022年

行业	应用环节	主要产品
电力	覆盖电力生产“发、输、变、配、用、调”各环节，重点应用于省级以上调度中心，地县级调度中心、发电厂，变电站、配电等	电网侧：电力专用隔离装置、电力防火墙、单向认证加密终端模块、拨号加密认证装置等。 发电侧：工业防火墙、入侵异常监测、主机加固、日志审计等。

电力行业受政策影响情况，2022年

时间	政策
2018年9月	《关于加强电力行业网络安全工作的指导意见》
2019年1月	国家电网 “三型两网”战略目标
2019年7月	《电力信息系统安全等级保护实施指南》
2022年11月	《电力行业网络安全等级保护管理办法》
2023年3月	《关于加快推进能源数字化智能化发展的若干意见》

- **电力行业信息化建设浪潮带动了安全防护相关建设工作，同时政府对已建项目及新建项目都提出了做好安全防护的要求，从而深化了工业信息安全产品在电力行业的应用。**

来源：中国信息安全评测中心、国家电网、中国工业互联网产业联盟、头豹研究院

中国工业信息安全应用场景（2/4）：智能制造

智能制造行业2022年在信息安全领域的投入达14亿元，在行业应用中占比13.6%，位居第二，智能制造覆盖多个领域，市场空间大，未来5年市场规模将以27.5%的增速增长

智能制造行业市场规模，2019-2026年预测

智能制造行业工业信息安全市场规模，2019-2027年预测

智能制造类企业的安全需求分析

类型	企业的安全需求分析
通信协议方面	智能制造行业大量工控系统中使用的协议存在安全性缺陷，同时随着TCP和OPC协议等通用协议应用逐渐普遍，通信协议漏洞问题凸显。
操作系统方面	通常在系统运行后基本不会安装任何补丁和升级，存在大量已知可利用漏洞和未知漏洞，易受到黑客攻击。
应用软件方面	常规的IT 防火墙等安全设备在应用软件开放其应用端口时，保障作用有限。
外部入侵威胁方面	APT攻击、蠕虫、混合攻击。黑客可以利用网络扫描和嗅探工具发现暴露在外的工控系统，发现漏洞进行攻击。

来源：专家访谈、工业信息安全产业联盟、珞安科技官网、头豹研究院

智能制造行业受政策影响情况，2022年

时间	颁布主体	政策
2015年5月	国务院	《中国制造2025》
2016年12月	工信部、财政部	《智能制造发展规划（2016—2020 年）》
2017年7月	国务院	《新一代人工智能发展规划》
2020年9月	工信部	《建材工业智能制造数字转型行动计划（2021-2023年）》
2021年12月	工信部、国家发改委、教育部、科技部、财政部、等八部门	《“十四五”智能制造发展规划》

来源：专家访谈、工业信息安全产业联盟、中国政府网、头豹研究院

中国工业信息安全应用场景（3/4）：石油石化

石油石化行业2022年工业信息安全市场规模达13.4亿元，市场占有率为13%，位居第三，当前石油石化行业的安全防护需求集中于边界隔离和安全加固，行业应用以防护类产品为主

石油石化行业企业的安全需求分析

类型	企业的安全需求分析
硬件方面	工业控制系统网络中存在大量广播信息易造成广播风暴。
软件方面	工控系统由于软件品牌多样而难以形成统一的防护规范策略；常规的IT防火墙和网闸无法适应OPC动态端口机制，无法发挥作用。
使用方面	网络使用者使用不当可能导致网络口令丢失、权限分配失策、系统被人入侵等情况，也会造成机密数据丢失、泄漏、系统瘫痪等故障。
非法授权使用	工控系统的权限管理的漏洞造成非授权使用，或受到来自外部的黑客攻击，有可能使工控系统误动作，甚至造成系统瘫痪。

石油石化行业工业信息安全市场规模，2018-2027年预测

中国工业信息安全产品在石油石化行业的应用，2022年

行业	应用环节	主要产品
石油石化	主要用于勘探生产、炼油化工、天然气与管道等领域，具体应用在场站及调度中心SCADA系统的边界、调度中心生产网交换机及场站工控交换机、场站生产监控终端、调度中心服务器、运维终端、监控工作站等环节。	**以防护类产品为主，**具体包括工业网闸、工业防火墙、工业安全审计系统、终端入侵检测设备、网络入侵检测设备、主机安全防护系统

石油石化行业受政策影响情况

时间	颁布单位	政策
2016年10月	工信部	《工业控制系统信息安全防护指南》
2017年6月	中国石油化工集团	《关于加强工业控制系统安全防护的指导意见》
2022年4月	工信部、发改委、科学技术部、生态环境部、应急管理部、国家能源局	《关于“十四五”推动石油石化行业高质量发展的指导意见》

- **中国政府明确提出要实施石化行业工业互联网企业网络安全分类分级管理**、推动商用密码应用，提升企业的安全防护水平，有助于工业信息安全产品在石油石化行业的深入应用。

来源：专家访谈、工业信息安全产业联盟、珞安科技官网、头豹研究院

中国工业信息安全应用场景（4/4）：轨道交通

轨道交通行业的工业信息安全市场需求增长较快，2022年工业信息安全市场规模达7.2亿元，市占率达7%，其安全防护需求多样，未来5年市场规模将以17.7%的增速增长

轨道交通行业企业的安全需求分析

类型	企业的安全需求分析
运行环境方面	雷击、温度、湿度等物理环境容易导致设备损坏，电压电流异常将引起交直流电源设备故障，进而影响设备正常运行。
网络结构方面	网络结构方面的安全威胁包括网络接口导致的漏洞、网络协议导致的漏洞、网络权限管理导致的漏洞、网络风险传播导致的安全威胁等。
平台系统方面	平台系统方面的安全威胁包括工业主机漏洞，数据库及云平台安全漏洞，主机、传感器、控制器故障导致的信息错误或缺失等。
应用软件方面	调度软件、控制软件等专业应用程序在开发之初就考虑到了安全问题，因此相对安全。然而，其他服务器软件、办公软件、打印机软件等常见商业软件存在大量的漏洞，对信息安全造成了潜在的风险。
通信方面	通信的安全威胁包括电磁干扰、拒绝服务、消息篡改、错误信息注入、未经授权访问、被动窃听、主动拒绝控制和承担控制权攻击等。
人员疏忽或误操作方面	工作人员在系统配置时如果未对一些系统中的默认值做安全性配置，访问口令往往极易被破解，如果工作人员疏忽或进行违规操作，就极有可能使系统遭受非法攻击。此外，工作人员的非法网络访问、非法硬件接入、非法权限管理等操作都能对信息安全造成巨大威胁。

- 轨道交通系统业务复杂、自动化程度高，各个子系统间相互协同，随着新一代信息技术推动轨道交通工业走向数字化、信息化、网络化，轨道交通行业也面临诸多方面的信息安全威胁。

来源：专家访谈、神州惠安官网、头豹研究院

轨道交通行业工业信息安全市场规模，2018-2027年预测

中国工业信息安全产品在轨道交通行业的应用，2022年

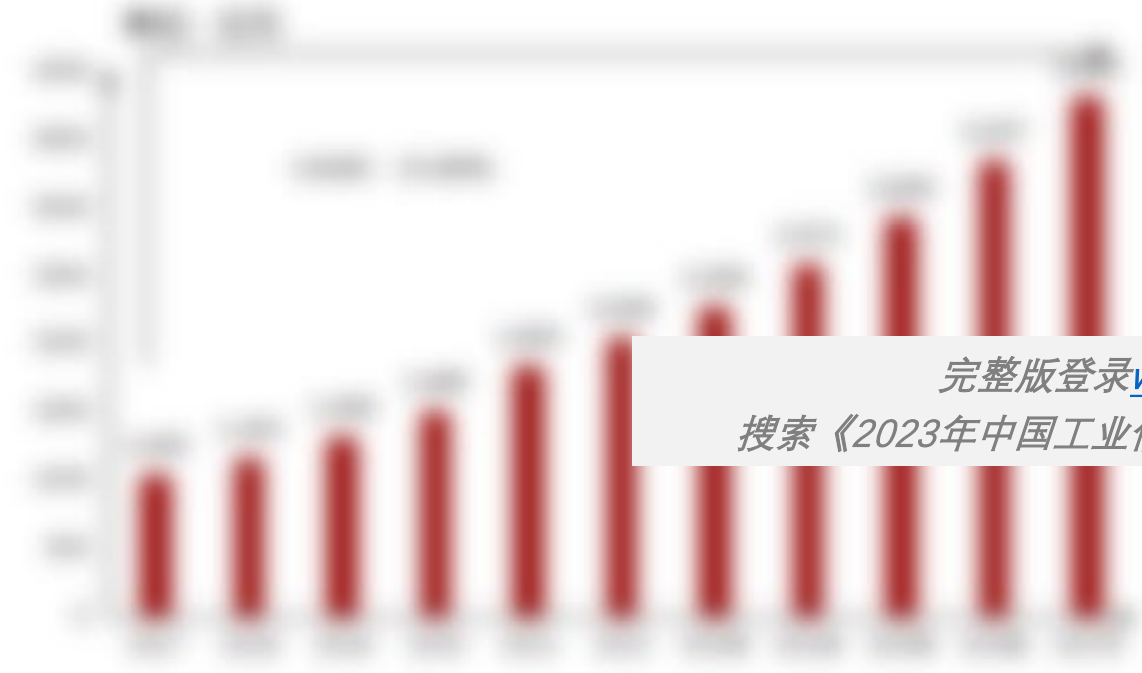
行业	应用环节	主要产品
轨道交通	以列车自动运行控制系统为核心，包括列车控制信号系统、综合监控系统和自动售检票系统等，还包括车站各类工作站服务器、交换机，车站、车辆段、停车场等站点各子系统边界处等。	工业防火墙、工控主机卫士、工控主机加固系统、工控数据库审计系统、工控监测分析预警平台、工控信息安全日志系统等

来源：工业信息安全产业联盟、珞安科技官网、头豹研究院

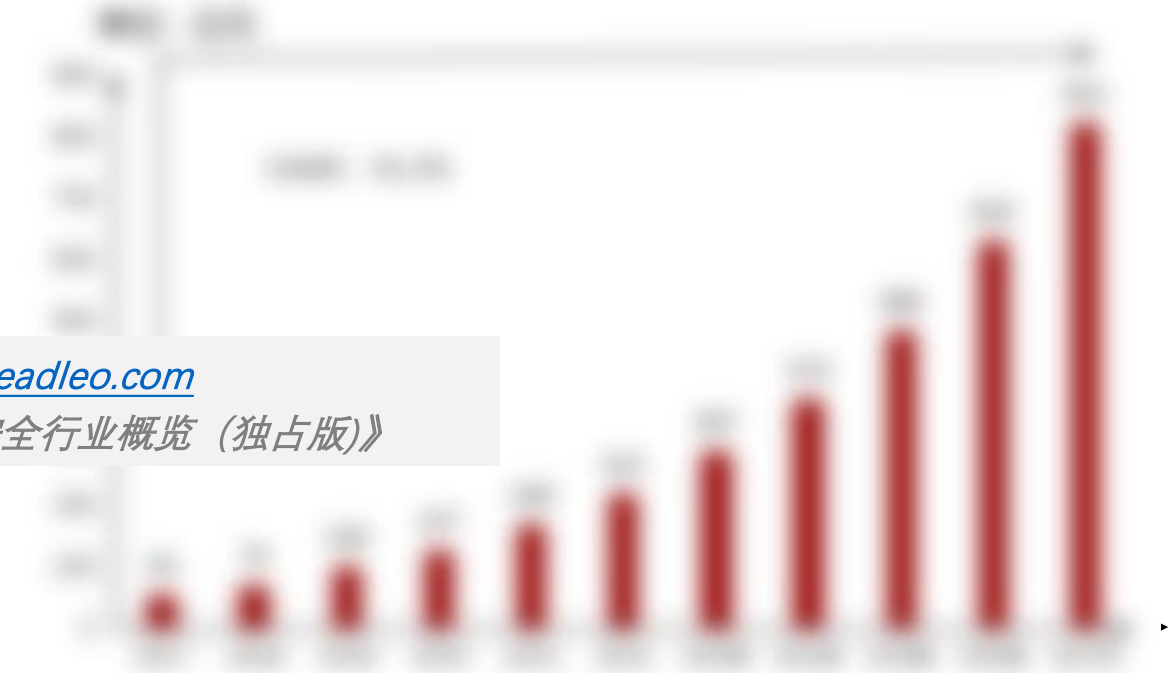
中国工业信息安全市场规模（1/2）：持续稳步增长

政策、互联网技术发展、企业安全需求增长等因素推动了行业的发展，中国工业信息安全行业市场规模从2017年的54.5亿元增长至2022年的221.15亿元，预计2027年市场规模至821亿元

中国信息安全市场规模，2017-2027年预测



中国工业信息安全行业市场规模，2017-2027年预测



来源：国家工业信息安全发展中心、工信部、工业信息安全产业联盟、头豹研究院

中国工业信息安全市场规模（2/2）：细分赛道高速增长

政策、互联网技术发展、企业安全需求增长等因素推动了行业的发展，中国工业信息安全行业市场规模从2017年的54.5亿元增长至2022年的221.15亿元，预计2027年市场规模至821亿元

中国工业信息安全市场规模-工业互联网安全

中国工业信息安全市场规模-工业控制系统信息安全

《网络安全等级保护2.0》标准体系
公安部，2019年12月

- 2017年《中华人民共和国网络安全法》的正式实施标志着等级保护2.0的正式启动。网络安全法明确“国家实行网络安全等级保护制度”。**网络安全等级保护2.0标准体系包括众多法规文件**，在等级保护1.0标准体系的基础上对**等级保护工作内容、保护对象、保护力度提升等方面进行扩展。**随着网络安全等级等保 2.0 标准的逐步落实，中国工业信息安全市场有望迎来更大的发展。

❑ **中国工业互联网安全行业高速增长，安全产品类占比75%，网络安全系列政策的密集出台推动工业互联网行业发展，2027年有望实现426亿元**

中国工业互联网安全作为工业信息安全的主要组成部分，在网络安全等级保护政策强调保护能力提升以及互联网技术不断发展的双重驱动下，中国工业互联网安全进入高速发展阶段，同时也推动中国工业信息安全行业快速发展。

《关键信息基础设施安全保护条例》
国务院 2021年9月

- 《关键信息基础设施安全保护条例》细化了《网络安全法》中对关键信息基础设施的要求，**从国家层面明确要求针对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的关键信息基础设施实行重点保护**，《条例》并要求工控企业应具备的基本安全防护能力，以及明确了未达到要求时相应的处罚，推动工控安全行业发展。

❑ **中国工业控制系统信息安全行业在2019年进入快速发展阶段，软件类产品占比40%，2022年市场规模达29亿元，2027年有望实现56亿元**

中国工业控制系统信息安全是工业信息安全领域的细分赛道，工业控制系统业信息安全行业主要受网络安全等级保护2.0标准影响在2019年进入快速发展阶段，同时受《关键信息基础设施安全保护条例》的政策影响，未来市场前景广阔。

来源：专家访谈、公安部、头豹研究院

中国工业信息安全行业市场主体：市场参与者多元化

中国工业信息安全市场参与者众多且多元化，传统信息安全厂商信息安全技术积累深厚；自动化背景厂商拥有丰富且现成的客户资源；专注于工业信息安全的企业具备深厚的行业知识，技术创新速度快

中国工业信息安全市场参与者分类

	信息安全厂商	自动化背景厂商	专注于工业信息安全的厂商	系统集成厂商
代表企业	360数字安全 数字安全的领导者、启明星辰、天融信 TOPSEC、安恒信息 DAS-Security、NSFOCUS、奇安信 新一代网络安全领军者	和利时 HollySys、Etrol安控、SIEMENS、Schneider Electric、中控·SUPCON	TDHX 天地和兴、威努特 WINICSSEC、6cloud 六方云、长扬科技 CHANGYANG TECH、LUOAN 珞安科技	inspur 浪潮、HUAWEI、美亚柏科 MEIYA PICO、H3C
竞争逻辑	❑ **业务逻辑：**从传统的IT信息安全业务发家，为各行业提供安全软硬件产品及服务，大多从2017年开始进入工业信息安全领域。 ❑ **竞争特点：**信息安全厂商深耕信息安全行业多年，信息安全技术积累较多，业务覆盖范围广，积累多个行业的安全应用实施案例，客户经验丰富，安全产品线丰富。	❑ **业务逻辑：**深耕工业领域多年，或通过成立工控安全部门或子公司进入工控安全领域，或通过与专注于工业信息安全的厂商合作，采取OEM方式开发具有信息安全功能的工控产品。 ❑ **竞争特点：**依靠深耕工业领域多年的优势，选择与专注于工业信息安全的厂商合作，具备现成的客户资源。	❑ **业务逻辑：**专注于工业领域，成立时间较短，凭借自身渠道和技术创新优势在工业信息安全市场中占得一定市场份额。 ❑ **竞争特点：**技术实力较强，对工业行业理解深厚，工控安全产品竞争力强，同时近些年受资本市场青睐，融资热度高，企业资金逐渐雄厚。	❑ **业务逻辑：**政策利好刺激这类企业布局工业信息安全领域，主要通过与安全厂商合作，共同开发安全软硬件产品。 ❑ **竞争特点：**系统集成商具备丰富的行业知识和本地化服务基础，与安全厂商合作可加快工业信息安全技术研发，提高技术能力。

来源：企业官网、头豹研究院

中国工业信息安全行业竞争格局：市场竞争激烈，未出现绝对的领导企业

工业信息安全市场竞争激烈，现阶段形成以天融信、奇安信等信息安全厂商领先的多强竞争态势，未来头部企业市场集中度将提升，专注工业信息安全领域的初创厂商有望获得更多市场份额

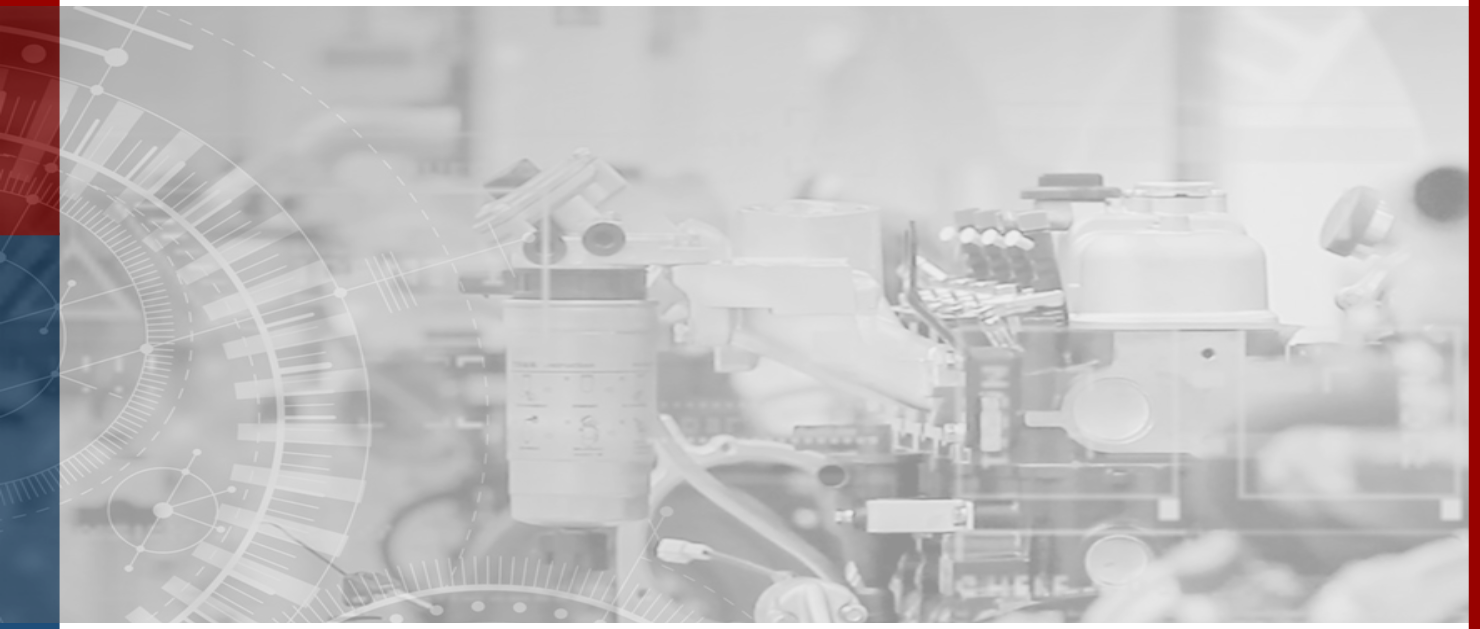
中国工业信息安全竞争格局

来源：专家访谈、企业年报、企业官网、头豹研究院

- **工业信息安全市场竞争激烈，现阶段传统信息安全厂商、专注于工业信息安全领域的厂商均有在工业信息安全领域中较为领先的企业，具体如传统信息安全厂商中的奇安信、天融信、启明星辰、绿盟科技以及专注工业信息安全领域的天地和兴、威努特、珞安科技、长扬科技等企业在市场竞争中占据优势地位。在工业数字化背景下，头部企业市场集中度将提升，专注工业信息安全领域的初创厂商有望得到更多市场份额**

头部厂商市场集中度有望提升：工业信息安全行业涉及的领域广，在行业内深耕时间长、具备丰富行业知识、安全解决方案应用案例多且覆盖行业广、技术能力强的企业更能占据市场竞争的优势。目前来看，头部企业中，不论是传统信息安全厂商还是专注于工业信息安全领域的厂商在技术能力上差距不明显。但在工业化和信息化不断融合过程中，工业信息安全头部厂商有望凭借其已形成的技术积累、品牌优势、客户资源、应用案例多样等进一步垒高行业壁垒，市场集中度进一步提升。

腰部企业竞争加剧，专注工业信息安全领域的初创厂商有望获得更多市场份额：专注工业信息安全领域的初创厂商虽然入行时间短，但近些年受到资本市场青睐，融资热度高涨，企业的资金实力更为雄厚，有望获得更多市场份额。



03

企业推荐

中国工业信息安全行业代表企业：启明星辰

启明星辰是传统信息安全产品和服务提供商，凭借前期的技术积累和实践耕耘，已有超千个的行业应用案例在电力、交通、石油石化等行业实施，在工业信息安全领域位居第一梯队

启明星辰基本情况

启明星辰　成立时间：1996年　上市时间：2010年

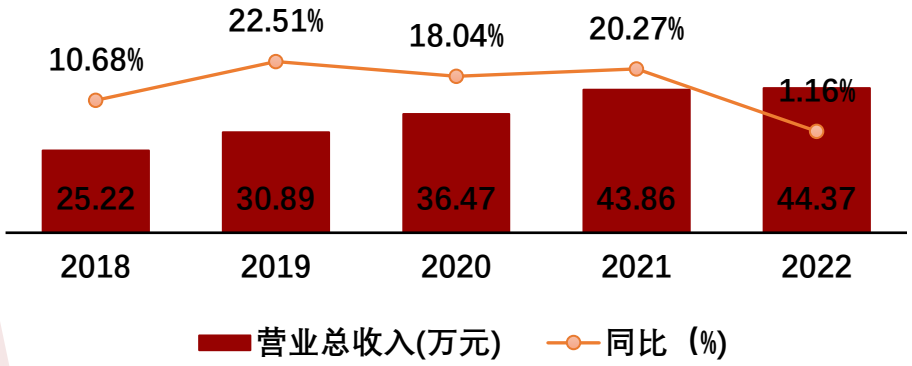
- 北京启明星辰信息技术股份有限公司（以下简称“启明星辰”）是一家拥有完全自主知识产权的信息安全企业，经过近四十年的发展，通过为客户提供网络安全产品、安全管理平台、安全服务与解决方案，已成为国内最具技术创新和产品开发实力的领导厂商之一。
- 启明星辰依托多年行业客户的基础优势，覆盖电力、金融、医疗、烟草、航空航天、制造、交通等多种行业应用场景的安全需求，行业应用案例超千个，在信息安全领域中处于领先地位。

工业信息安全领域主要产品情况

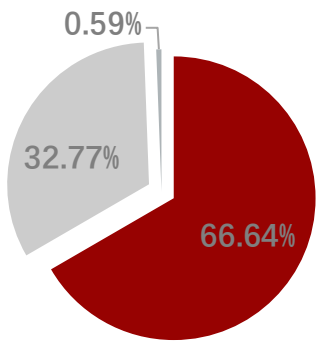
工业防火墙	工控IDS与审计	工控脆弱性扫描	工业SOC系统
工业网闸	工控检查工具箱	工业主机防护系统	工控态势感知

- ✓ 工业防火墙、工业网闸、工业IDS、工业态势感知系统、工控漏扫五个产品位列竞争格局领导者行列榜首
- ✓ 工控主机安全、工控安全审计产品继续占据行业领导者地位

启明星辰营业收入，2018-2022年



启明星辰营业收入构成，2022年



	毛利率
安全产品	62.53%
安全运营与服务	63.09%
其他业务	53.02%

信息安全业务
收入：44.11亿
毛利率：62.17%
收入占比：94.4%

来源：企业官网，企业年报、头豹研究院

中国工业信息安全行业代表企业：绿盟科技

绿盟科技是传统信息安全产品和服务提供商，拥有较深厚的技术积累和行业经验，网络安全产品线丰富，工业安全整体解决方案已在交通、电力等行业应用实施，在工业信息安全领域占据优势地位

绿盟科技基本情况

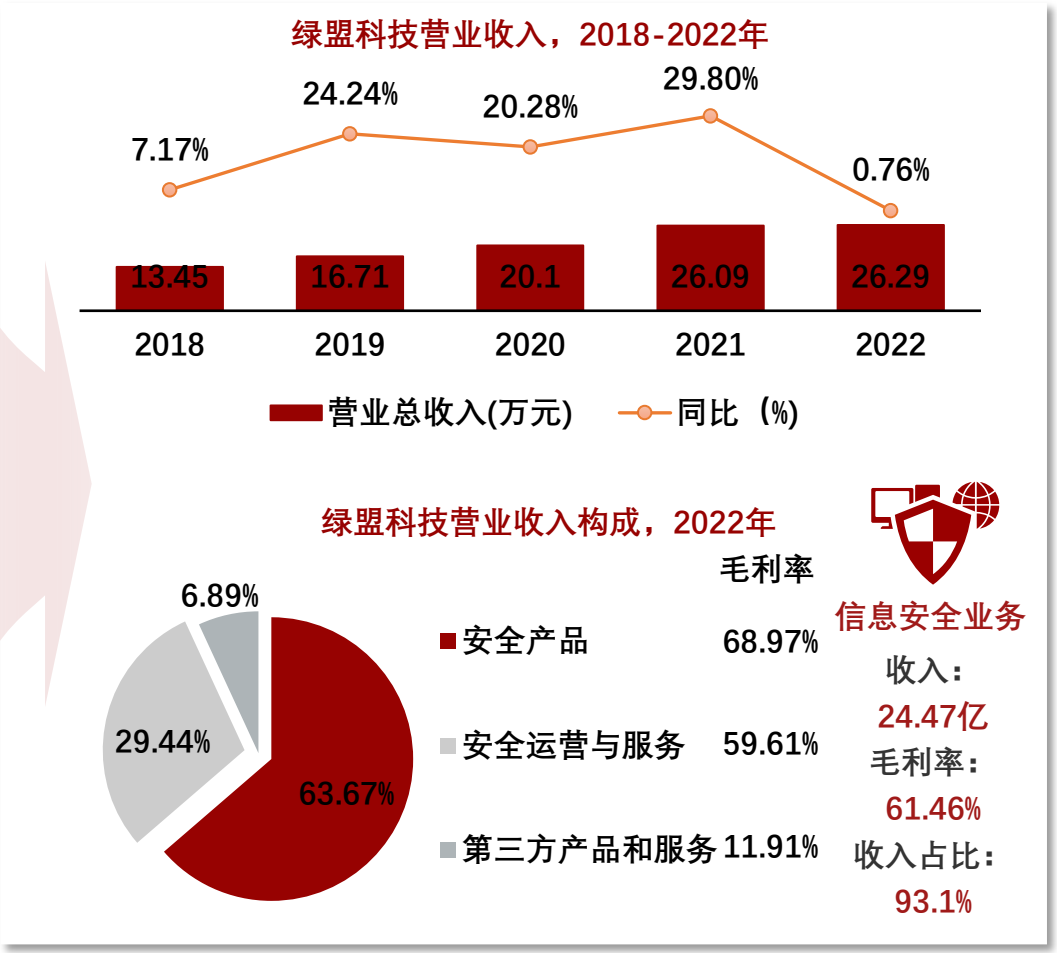
成立时间：2000年　　上市时间：2014年

- 绿盟科技集团股份有限公司（以下简称“绿盟科技”）深耕传统网络信息安全领域多年，在国内外设有50多个分支机构，为政府、金融、运营商、能源、交通、教育、医疗以及企业等行业用户，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。
- 绿盟科技凭借自身十多年的漏洞挖掘与分析检测经验，研发了国内首款工控漏洞扫描系统。其基于工控系统自身的特点，面向工控安全面临的威胁和风险，研发了一系列工控安全产品及解决方案。

工业信息安全领域主要产品情况

安全隔离与信息单向导入系统	工业安全隔离装置	工控安全审计系统	工控安全入侵检测系统	工控漏洞扫描系统	工业网络安全监测管理平台
	工业数据安全交换系统	工业安全网关	工业主机卫士系统	视频安全交换系统	工业网络安全合规评估工具

✓ 工控IDS、工业安全服务占据行业优势地位



来源：企业官网，企业年报、头豹研究院

方法论

- 头豹研究院布局中国市场，深入研究19大行业，持续跟踪532个垂直行业的市场变化，已沉淀超过100万行业研究价值数据元素，完成超过1万个独立的研究咨询项目。
- 头豹研究院依托中国活跃的经济环境，研究内容覆盖整个行业发展周期，伴随着行业内企业的创立，发展，扩张，到企业上市及上市后的成熟期，头豹各行业研究员积极探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业视野解读行业的沿革。
- 头豹研究院融合传统与新型的研究方法论，采用自主研发算法，结合行业交叉大数据，通过多元化调研方法，挖掘定量数据背后根因，剖析定性内容背后的逻辑，客观真实地阐述行业现状，前瞻性地预测行业未来发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 头豹研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 头豹研究院秉承匠心研究，砥砺前行的宗旨，以战略发展的视角分析行业，从执行落地的层面阐述观点，为每一位读者提供有深度有价值的研究报告。

法律声明

- 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- 本报告所涉及的观点或信息仅供参考，不构成任何证券或基金投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告或证券研究报告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。
- 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本报告所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本报告所载资料、意见及推测不一致的报告或文章。头豹均不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。