iResearch
艾瑞咨询

2024年中国网络安全硬件设备发展洞察报告

引言

习近平总书记在2023年全国网络安全和信息化工作会议中做出重要指示指出，新时代新征程中，网信事业的重要地位作用日益凸显，要坚持筑牢国家网络安全屏障，大力推动网信事业高质量发展。近年来，国务院、网信办、工信部发布一系列网络安全相关政策，旨在加强网络安全体系保障与能力建设，推进传统安全产品升级，筑牢可信可控的数字安全屏障。在这一背景下，网络安全硬件设备成为行业关注焦点，它是定制化集成上游元器件后，针对客户特定网安需求场景，提供一系列专业化解决方案的安全设备。

艾瑞咨询测算，2024年中国网络安全硬件设备整体规模预计达到35.9亿元，其中专用网络安全硬件平台占比40.0%；随着国产化电子元器件的成熟，下游行业涌现对于信创设备的需求，在专用网络硬件安全平台中占比已达到30%，并有望进一步提升。

总览行业竞争格局，在专用网安硬件平台市场中，陆企乐研科技以22.3%的份额排名第一，台湾厂商仍然占据重要位置；在信创这一细分市场中，乐研科技具有明显领先优势，以49.7%的市场份额排名第一。

展望未来，行业呈现三大主要发展趋势。

- 头部供应商的技术更成熟且产品覆盖度更高，同时具有更强的供应链保障，需求方采购方式也由分散向集中转变，因此行业的市场集中度会继续增强，头部厂商的优势预计将更明显；
- 相关国产化软硬件成熟度提升，从“可用”进入到“好用”阶段，在政策的大力支持下国产化网络安全硬件设备将会成为未来行业增长的主要动力；
- 在复杂多变的网络环境下，需求方对于网络安全产品的要求将继续提升，专用网络安全硬件平台将逐步替代通用网络安全硬件设备。

CONTENTS

目录

01/ 中国网络安全硬件设备发展现状观察

政策引导网络安全行业积极发展

法律法规与行业指南持续丰富，引导企业发掘网络安全建设需求

2021-2023年中国网络安全领域相关政策及法规摘录

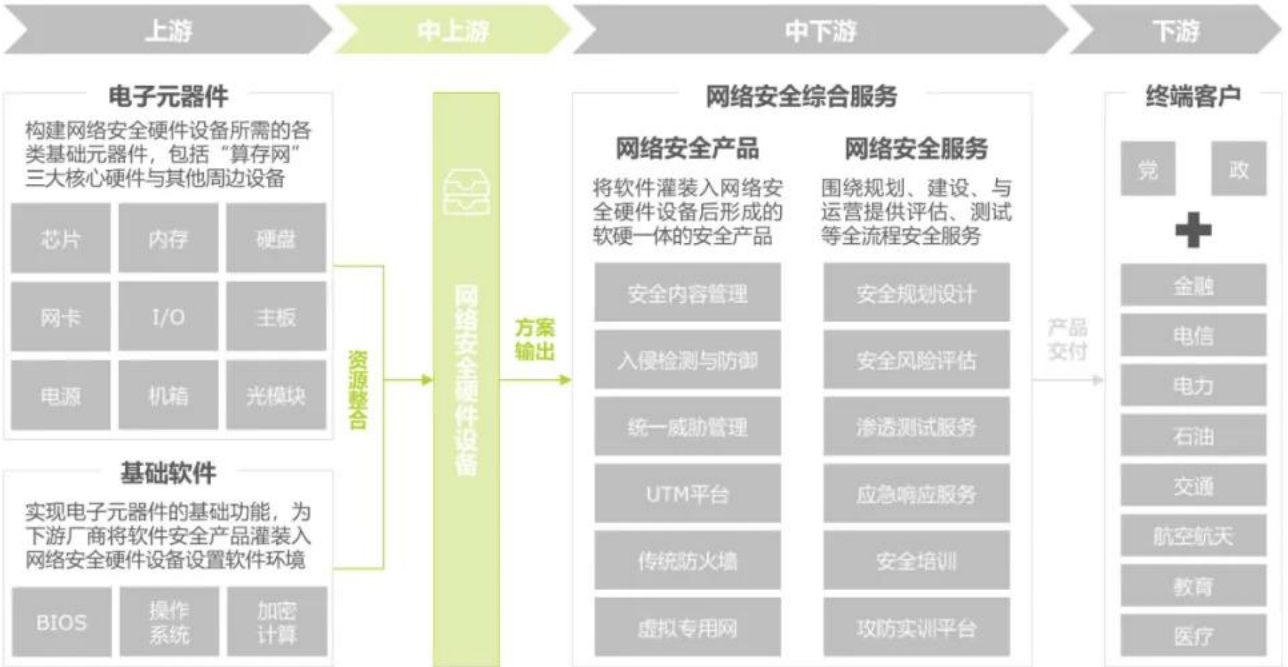
时间	发布机构	政策名称	内容摘要
2021.3	国务院	《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》	**全面加强网络安全保障体系和能力建设**，切实维护新型领域安全，从基础设施，国际合作等多方面培育壮大网络安全等新兴数字产业
2021.4	国务院	《关键信息基础设施安全保护条例》	对公共通信、能源、交通等重要行业和领域的**网络设施**、信息系统实施安全保护和监督管理
2021.7	工信部	《网络安全产业高质量发展三年行动计划（2021-2023年）》	引导国家制造业转型升级基金等政府引导基金向**网络安全新技术、新模式以及融合创新领域倾斜，加快传统安全产品升级**
2022.2	网信办等13部门	《网络安全审查办法》	关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当进行网络安全审查
2023.1	工信部等16部门	《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》	数据安全产业是为保障**数据持续处于有效保护、合法利用、有序流动状态**提供技术、产品和服务的新兴业态
2023.2	中共中央国务院	《数字中国建设整体布局规划》	需要“筑牢可信可控的数字安全屏障”，**强调网络安全是数字中国建设的重要基础，是新安全格局的关键组成部分**
2023.7	网信办等4部委	《网络关键设备和网络安全专用产品目录》	目录列出包括防火墙、入侵检测系统（IDS）、统一威胁管理产品（UTM）等**34项网络安全专用产品**
2023.12	网信办	《网络安全事件报告管理办法（征求意见稿）》	将网络安全事件划分为“一般”、“较大”、“重大”与“特别重大”四个等级，规范各等级网安事件的处置报告时间、对象与内容

来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。

网络安全硬件设备产业全景

网络安全硬件设备厂商位于产业链中上游，为网络安全综合服务厂商的产品、服务及综合解决方案提供基础底座

中国网络安全硬件设备产业链



来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

网安硬件设备分类一：通用与专用

网络安全的通用设备与专用平台在市场定位、定制化能力与迭代周期上存在显著差异，通用设备正在向专用平台全面转向

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

网安硬件设备分类二：传统与信创（1/3）

网络安全信创产品沿着“安全软件-安全硬件设备-元器件及基础软件”的方向，由产业链顶层向底层逐步替代传统网安方案

传统网络安全硬件设备即全部或部分使用非国产电子元器件或基础软件配置而成的网络安全产品；相对应的，信创网络安全硬件设备的全部基础软硬件模块均为国产。网络安全行业整体遵循由安全软件到硬件设备再到基础元器件与软件的国产化顺序。2000年起，国产网络安全综合服务类厂商逐步兴起，推出国产化网络安全软件；进入2010年，网络安全硬件陆商开始在与台企的竞争中逐渐崭露头角；2015年后，以CPU、存储、网卡为代表的基础电子元器件国产化加速，同时国产化操作系统、数据库等基础软件也陆续研发推出，由此形成了从底层到上层的端到端网络安全解决方案。

中国网络安全行业信创发展三阶段

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

网安硬件设备分类二：传统与信创（2/3）

供给侧布局端到端国产化安全产品，需求侧发力完成国产替代目标；信创产品正在成为行业发展的重要力量

- **信创供给侧：**信创安全厂商分布于产业链上游“基础硬件”中的“网络安全硬件设备”领域以及产业链下游的“网络安全综合服务”领域。其中，网络安全综合服务领域已出现多家上市企业，形成一批优秀的国产化安全类解决方案，是行业发展的主导力量，同时也将信创需求向上游传导；随着“网络安全基础硬件”领域中算存网产品能力的不断完善，网络安全硬件设备厂商能够承接更多下游信创需求，加紧国产替代。
- **信创需求侧：**信创“2+8+N”体系覆盖广泛，政策已对这些行业提出逐步提升国产化率的目标，未来国产化仍有广泛的想象空间，可能继续向汽车、物流、消费等更多领域渗透。

网络安全硬件设备在中国信创产业中的位置及主要厂商

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

网安硬件设备分类二：传统与信创（3/3）

信创软硬件产品较传统更加丰富，对网络安全设备厂商能力要求更强

国内信创产业发展以来，在基础软硬件领域形成了百花齐放的生态体系。如基础硬件领域，国外网安硬件主要配置X86型CPU，较少配置ARM类CPU，但国内方面同时配置X86、ARM、LoongArch、Alpha等多种架构的CPU产品。更丰富的生态体系给予网络安全硬件设备厂商更多选择，但同时也加大了产品适配的复杂性，对厂商技术能力要求更强。

传统与信创基础软硬件生态对比

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

02/ 中国网络安全硬件设备行业规模及竞争格局

中国整体网络安全硬件设备市场规模

网络安全行业即将突破瓶颈期，推动网络安全硬件设备市场进入转型期

- **当前态势：**2023年中国整体网络安全市场增速持续放缓，网络安全软件和安全服务成为支撑市场增长的主要因素，网络安全硬件产品营收表现不及预期，网络安全企业作为网络安全硬件设备厂商的主要客户，在网络安全硬件设备领域的采购规模缩减，导致网络安全硬件设备市场呈负增长态势。
- **影响因素：**头部网络安全企业2022年前大量采购网络安全硬件设备，以预防芯片供应链变动对生产经营活动的影响，但宏观经济环境的不确定性，使各行业对网络安全硬件产品预算缩减，项目建设周期延长，网络安全硬件设备市场出现供过于求的状况，导致网络安全企业2022-2023年间采购重点从“寻增量”转变为“清库存”，短期内限制了网络安全硬件市场的进一步增长。
- **长期发展：**传统行业数字化建设加速和国产化信息技术创新软硬件产品的普及，驱动各行业企业不断扩大网络安全领域投入。从2024年上半年开始，网络安全企业“清库存”陆续完成，网络安全硬件采购需求逐步恢复，新的采购需求相继释放，行业重新回到增长区间。预计在2025年，网络安全硬件设备市场将迎来拐点，并在数字化和国产化双重因素推动下，步入新的高速发展期。

2018-2028年中国整体网络安全硬件设备市场规模及增速

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

中国整体网络安全硬件设备市场规模

增量需求即将释放，供给侧厂商不断优化能力以匹配新采购要求

- **从需求侧看，**网络安全企业已逐步完成库存清理任务，即将开始新一轮网络安全硬件设备采购周期，网络安全硬件设备市场即将迎来拐点。在人工智能、大模型等新技术的刺激下，各行业数字化进程将进一步加速，对网络安全相关产品的需求也将进一步释放，进而带动网络安全硬件设备市场增长。
- **从供给侧看：**网络安全硬件设备行业逐步从通用化向专业化转型，在行业头部厂商的持续努力下，网络安全硬件平台供应链体系进一步成熟，产品迭代和生产周期不断缩减，可有效满足网络安全企业对网络安全硬件平台产品的采购需求，支撑网络安全硬件设备市场的进一步发展。

网络安全硬件设备市场增长驱动因素

网安企业需求拐点即将出现

网络安全企业已经完成库存清理，即将进入库存周期的新阶段，对网络安全硬件设备的采购规模将逐步扩大。同时，受行业发展趋势影响，专业化网络安全硬件平台及国产化网络安全硬件平台将成为采购重点。

网安行业新趋势刺激新需求

从技术领域看，以大模型为代表的人工智能等新兴技术的发展，将让网络安全威胁更为多元，网络安全防护场景更多样，网络安全软硬件产品需求更迫切，驱动网络安全硬件设备需求增长。从产业角度看，国产化趋势从党政领延伸到传统行业，将推动网络安全设备国产化进程

硬件设备产业链不断完善

网络安全硬件设备产业链不断完善，在头部厂商牵头下，产业链各环节分工协作效率显著提升，资源配置效率更高，行业生态更完善。网络安全硬件设备更新迭代周期缩短，产品生产成本有效缩减，专业设备内和国产化设备性价比优势更为凸显

硬件设备厂商能力不断提升

网络安全硬件厂商始终坚持在专业设备和国产化设备领域的技术创新，扩大研发投入，打造创新性的产品解决方案，提升硬件性能，使网络安全硬件平台满足应用场景多元化的要求

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

专用网络安全硬件平台市场规模

专用网络安全硬件平台逐步成为数字化时期网安企业采购重点

信息化时期，网络安全威胁种类较为有限，对网络安全硬件产品功能需求较为集中，对网络安全硬件平台性能要求更多参考计算平台/服务器的标准。因此，很多服务器和工控机厂商长期为网络安全企业提供综合网络安全硬件平台，以满足通用网络安全场景的防护需要，并占据行业主导。数字化时期，网络安全场景日益丰富，网络安全企业对网络安全硬件平台产品功能要求更为多元，性能要求愈加严格，驱动具备更强稳定性、可靠性、可拓展性的专用网络安全硬件平台逐步成为网络安全企业采购重点。

2018-2028年中国专用网络安全硬件平台规模及增速

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

专用网络安全硬件平台市场结构

市场需求逐步放大，供给能力显著增强，专用网络安全硬件平台市占率稳步提升

- **从需求侧看：**网络安全威胁日益繁杂，对网络安全硬件产品功能需求趋于多元，要求网络安全硬件平台具备更强定制化能力、更好的软件适配性，更丰富的产品供应模式，以满足不同安全场景的精细化和专业安全防护要求，驱动专业网络安全设备需求逐步提升。
- **从供给侧看：**专业网络安全硬件平台起步较晚，在发展初期厂商资源整合能力不足，导致产品优异但产能有限，较难进一步扩大市场空间。随着专业网络安全硬件平台生态逐步完善，头部厂商经过长期深耕，不断打通上下游产业链各环节，持续优化资源整合能力，产品生产和迭代可匹配网络安全企业业务发展节奏，平台功能和性能可满足日趋严格的行业标准，专业网络安全硬件平台市场份额有望进一步扩大。

2018-2028年中国专用网络安全硬件平台市场占比

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

国产化网络安全硬件平台市场规模

传统行业国产化进程加速，国产化网络安全硬件平台潜在需求即将释放

过去几年，国产化网络安全市场虽受整体经济环境及网络安全企业清理库存策略的影响增长出现放缓，但仍保持扩张态势，是网络安全硬件平台行业唯一保持正向增长的细分领域。各类国产化信息技术产品渗透率持续提升，逐步从传统党政领域加速向其他关键基础行业（如金融、教育、医疗等）拓展，是驱动国产化网络安全硬件平台增长的关键因素。在新的采购周期，国产化网络安全硬件平台将成为网络安全企业采购重点，并成为推动整体网络安全硬件平台行业增长的关键。

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

国产化网络安全硬件平台市场结构

厂商研发能力持续提升，资源配置持续优化，有效支撑国产化市场增长

- **从行业角度看：**网络安全是数字化建设的保障，始终是各行业在产业数字化时期的投入重点。目前，IT国产化广度不断扩大，已逐步从党政领域，加速延展至关系民生的传统行业，相关行业对国产化网络安全产品的需求将显著提升，网络安全产品国产化升级将进一步推动国产化网络安全硬件平台的需求增长。
- **从企业角度看：**网络安全平台厂商从技术和供应链着手：一方面，持续提升研发能力，不断提升国产化网络安全平台产品适配性、可靠性、稳定性、可拓展性；另一方面，不断强化与行业上下游伙伴合作，优化资源配置，构建高效稳健的供应链体系，产品性价比优势更为显著。随着国产化网络安全硬件平台的技术能力和商业模式日趋完善和成熟，国产化网络安全硬件平台市场占比将进一步提升

2018-2028年中国国产化网络安全硬件平台市场占比

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

中国专用网络安全硬件平台市场份额

头部厂商竞争优势明显，市场格局未来有望形成头部聚集效应

格局高度集中，CR5占比56.8%。随着专用网络安全硬件平台厂商进一步完善产业链资源整合，优化供应链管理能力，产品矩阵进一步丰富，可覆盖客户更多场景需求，提升网络安全硬件平台全品类的综合竞争力。此外，产业数字化加深，网络安全防护要求日益严格，专业化网络安全硬件平台将成为网安企业采购重点，具备提供全品类网络安全硬件平台的头部厂商，将因此获益，进一步巩固并扩大市场占有率。

2023年中国专用网络安全硬件平台市场份额

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

2024 上半年中国专用网络安全硬件平台市场份额

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制

中国国产化网络安全硬件平台市场份额

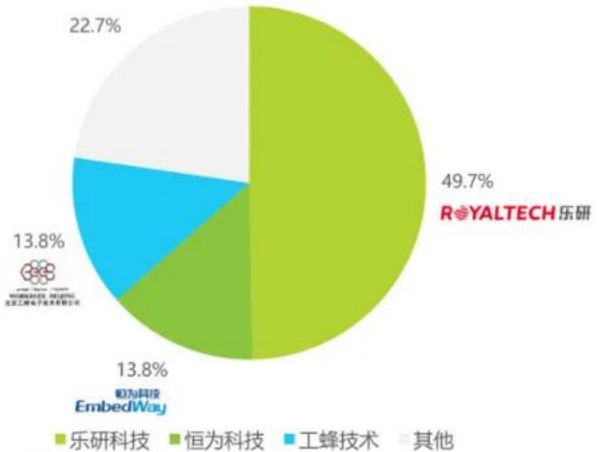
市场头部效应明显，乐研科技等国产厂商占据主导位置

格局较为稳定，CR3占比66.4%。在国产化领域，头部厂商通过不断提升科研创新能力，完善业内生态合作，其网络安全硬件平台适配性、可靠性、稳定性、可拓展性持续提升，网络安全企业客户对其产品的信任度和认知度不断增强。持续提升的产品技术能力、行业内生态影响力、行业客户的忠诚度有望帮助头部网络安全硬件平台厂商进一步扩大与中长尾厂商的竞争优势，巩固并扩大市场份额。

2023年中国国产化网络安全硬件平市场份额

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

2024 上半年年中国国产化网络安全硬件平台市场份额



来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制

03/ 中国网络安全硬件设备厂商案例

行业代表企业分析：乐研科技

整合供应链资源，强化生态合作，聚焦专业化和国产化网络安全设备

- 乐研公司致力于网络安全设备的研发、生产、销售和服务，专注为国内各网络安全软件厂商提供全面的软硬件系统整合解决方案及专业的设计制造服务，应用场景涵盖网络安全、智能交通、安防监控、物联网、工业自动化等细分行业领域。
- 经过长期发展，凭借优秀的人才、先进的技术、丰富的经验，以及持续迭代、应用数字化管理工具，构建覆盖中低端到高端的各类专业化网络安全平台产品体系，乐研科技成为国内网络安全设备的主流供应商之一。通过生态合作，不断完善供应链资源整合，有效缩短产品迭代周期，保证产品交付实效；依托科学的研发、生产、供应、销售体系，完善的售前售后服务能力，不断扩展在全国的业务布局。
- 在国产化趋势逐步深化的当下，乐研科技积极响应国家政策，在关键器件和设备自主可控方面持续发力，率先推出基于飞腾、龙芯、兆芯等国内厂商CPU芯片的网络安全设备，并已经实现批量生产和销售，为实现网络安全行业的供应链安全提供有力保障。

卓越的资源整合能力

- 乐研科技在苏州设有12000平米的大规模制造中心，一期设计产能15万台/年，覆盖大-中-小批量生产,高效专业的生产、质检体系，能够满足不同类型客户的交期需求
- 乐研科技不断探索创新型的产品架构及解决方案，形成差异化产品体系，为客户提供多种产品方案选择，快速的工程样品服务,保证产品供货稳定

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

行业代表企业分析：乐研科技

ROYALTECH乐研

iResearch 艾瑞咨询

国产化创新、服务化转型、数字化管理、生态化合作、资本化运作五大优势共同构筑乐研科技行业核心竞争力

国产化创新

产品国产化：乐研科技同时采购传统与信创基础电子元器件；在保障安全性的同时丰富了自身产品矩阵

产品应用创新：深挖国产基础硬件潜力，创新开拓出一系列国产化硬件在网络安全领域中的应用实践

裕泰PHY芯片 | 网迅网卡 | 电源、存储...

服务化转型

下游需求升级：网络安全综合服务厂商基于成本控制，需要网络设备供应商有能力将软件灌装入硬件产品后整体销售

商业模式转型：乐研科技敏锐捕捉这一行业趋势，利用自身技术优势，向“硬件+软件”的服务型厂商转型，提升自身产品附加价值

硬件 ➡ 硬件 + 软件 + 服务

数字化管理

数字化系统部署：乐研科技持续加码数字化升级，在内部管理、产品制造、客户服务等多领域落地数字化、智能化系统

企业精细化管理：通过对企业全域的数字化基础升级，提升企业内部管理效率，增加企业整体运转效率

ERP | CRM | SRM | MES | ...

生态化合作

构筑网络安全生态：乐研科技与包括芯片、BIOS、操作系统、网卡等产业链上下游各类厂商建立战略合作关系，共同构筑行业生态

形成产业生态合力：乐研科技积极参与生态内技术交流、产品合作开发、方案合作设计，夯实供应链，控制成本，同时开拓新市场

基础硬件 | 基础软件 | 安全软件

资本化运作

一级市场融资：乐研科技吸引了包括中电基金、建信股权等一众优秀投资人加入，在财务及战略方面获得了重要支持

二级市场上市：乐研科技正在积极推进上市计划，预计通过上市丰富资本支持并提升品牌知名度，巩固业内市场地位

战略融资 ➡ 筹备上市

ROYALTECH乐研

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

行业代表企业分析：立华科技

专注于网络安全、电信行业及边缘计算，高度定制化产品推动行业升级

立华科技是专业的网络安全、边缘计算和人工智能应用的产品的提供商，并提供硬件平台OEM/ODM解决方案及产业链服务。立华科技聚焦垂直行业，以高性价比的定制化的服务体系闻名，在电力能源行业有丰富的项目经验。立华科技将通过相关多元化策略进行渗透式发展，持续拓展业务范围，以智能化和定制化的的解决方案促进各行业领域数字化、网络化、智能化的升级和转型。

立华科技产品体系

国产化尝试	顺应国产化趋势，开展国产化产品开发，但开发时间较短，投入有限，成型产品规格不多，市场应用案例有待增加
定制客制	建立了在系统设计、产品工程、生产制造、技术支持及营销各方面的专业团队，具备从前期方案设计、小量试制、批量生产到售后维修、现场服务等完善的客制化服务体系。以极高的性价比、强大的性能以及高度客制化的服务体系，聚焦垂直行业，提供更适合企业的OEM/ODM解决方案。
智能化	加入了边缘计算产业联盟（ECC），推动边缘AI发展，深化数字化转型。开发了一系列智能化产品和解决方案，支持电力能源行业的数字化转型，实现更高效、更可靠的电力系统管理。

来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。

行业代表企业分析：兴汉网际

AI赋能个性化定制服务，为网络安全、云互联（SD-WAN）、物联网领域提供全面解决方案，推动企业网络升级和创新

兴汉网际的主营市场涵盖信息安全硬件及网络通信硬件的定制开发及平台集成服务，包括网安主机及模组、网络接入及边缘通讯白盒以及特种行业通讯加固整机等系列产品。这些产品广泛应用于防火墙、IDS/IPS、UTM、WAF、审计、VPN、网闸等网络安全领域，以及互联网接入、5G小基站、边缘计算场景和特种行业的高可靠计算需求领域。兴汉网际在在AI大力投入以达到更高的信息安全等级，完整成熟的客制化服务体系带来更高的客户黏性，为多家头部网络安全企业提供产品与技术服务。

兴汉网际产品体系

来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。

行业代表企业分析：恒为科技

深厚的网络可视化积累，国产化和智能化共同结合研发实现新价值

恒为科技是国内领先的网络可视化基础架构供应商，也是国产化智能系统平台的中坚力量，同时积极拥抱AI技术与产业的爆发趋势，结合自身的技术优势开展智算可视化研发。恒为科技在保持业务基本盘稳健发展的基础上，发展新兴智算产业，23年全年营收7.71亿元，净利润稳定增长达到0.79亿元，其中网络可视化业务收入3.76亿元，收入结构健康，智能系统平台3.92亿元且占比有所升高。恒为以其有机结合的国产化和智能化的软硬件平台解决方案，展现了其前瞻性和创造性，推动行业技术进步和数字化转型。

恒为科技产品体系

来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。

04/ 中国网络安全硬件设备发展趋势洞悉

趋势1：企业增加支出对抗安全风险

全球范围内网络安全风险持续存在，未来企业继续加码安全类支出

网络安全事件在全球范围内仍频繁发生，而缺乏网络安全管理制度安排、必要的风险保障技术以及配套设施的企业更容易被黑客侵入，导致巨大经济损失。

终端用户对于网络安全持续投入，Gartner预计2024年全球安全和风险管理终端用户总支出将达到2150亿美元，且增速较前两年仍有提高。企业用户在缩减成本的大趋势下，对于安全类支出不减反增，更突出了安全因素是企业发展过程中的核心考量。

2023年中国网络安全事件摘录

时间	事件
3月	永州市某物业明文存有6000余名业主姓名、电话、身份证号、银行账户等敏感数据信息；人脸识别系统、车辆管理系统均存在登录账号弱口令，账号未设置权限管理的安全隐患
3月	浙江某科技有限公司为政府部门开发运维信息管理系统的过程中，将采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露
5月	太湖县某房地产公司对存放业主用户数据的办公电脑未采取任何安全防护措施，未采取必要技术措施保障公司数据安全，导致大量数据信息面临泄露的重大风险
6月	中国人民大学一硕士毕业生利用自己的专业技能，盗取了学校内网数据，收集了全校本硕博学生的个人信息，然后公开发布在某网站上进行颜值打分
7月	大量疑似南亚印度地区APT组织活动频繁猖獗，针对我国境内教育航空工业、科研单位、军工、政府等行业发起多次攻击
8月	安全人员发现黑客组织“Patchwork”正在针对中国政府、能源等机构发动大规模钓鱼邮件攻击
11月	国内某家能源集团的相关数据在暗网上被黑客以 50 比特币的价格拍卖，泄露数据中涵盖了财务数据、设计图纸、职工信息等内容

来源：公开资料整理，艾瑞咨询研究院自主研究及绘制。

2022-2024年全球安全和风险管理终端用户支出

来源：Gartner，艾瑞咨询研究院自主研究及绘制。

趋势2：市场集中度趋向更高

三大原因促使头部厂商优势扩大：头部厂商技术更成熟、产品覆盖度更高，可获取更强的供应链保障，需求方采购方式逐渐转变

产品与技术

头部厂商技术较成熟 产品覆盖较全面

网络安全硬件设备的配置涉及包括CPU、内存、网卡、扩展槽、串口、电源等各类模块的选型及搭配，从而组成型号各异，覆盖高、中、基础的全线产品。

供应链

头部厂商可获得更强的供应链支持

目前以芯片为代表的国产化基础电子元器件出货量受限，头部厂商对这类稀缺资源更易获取，从而在信创安全产品的开发与生产中占据先机，扩大自身行业市场份额。

需求方采购

由“天女散花”式转变为集中采购

随着网络安全硬件设备行业的逐渐成熟，以及头部厂商的不断壮大，网络安全综合服务厂商已不需向各家供应商分散要货，而仅需向一家头部供应商采购即可满足所有需求。

网络安全设备配置过程中所涉及的基础电子元器件

CPU	芯片组	内存
网卡	硬盘位	冗余电源
机箱风扇	Bypass	USB
显示屏	扩展槽	网络接口
串口	SATA	RAID

供应商视角下的头部与非头部企业优劣势对比

非头部企业	头部企业
☒ 下游需求未知 渠道不稳定	☑ 具备较为稳定的下游需求
☒ 产品及方案未经市场验证	☑ 具备已验证的产品及方案
☒ 中小企业生存时间不确定	☑ 具备彼此长期合作互信

需求方视角下采购方式的转变

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。

趋势3：信创是未来行业发展的主要动力

信创产品矩阵逐渐丰富，性能水平逐步增强，相比国际厂商更具性价比

产品矩阵丰富：信创厂商持续推出多系列产品，可覆盖包括路由器、防火墙、密码机等多种网安设备及使用场景。
产品性能增强：信创CPU性能逐年提升，与国际厂商的差距也在逐步缩小，逐渐由“可用”转为“好用”。需求方态度也在发生变化，由过往出于政策强制要求的被动接受转变为主动需求。如，运营商方面，中国电信2024年集采计划中信创类服务器需求占比达到67.5%，而这一数字在2020年仅为19.9%；中国移动与联通对国产化芯片的重视也在逐年提升。
产品更具性价比：信创产品在性能提升的同时，价格相较于同类国际厂商有较大优势，具有较强性价比。

Phytium飞腾	FT-2000+/64		FTC662内核 16nm工艺 1.8-2.2GHz主频	腾云S2500		FTC663内核 16nm工艺 2.0-2.2GHz主频	腾云S5000C		FTC862内核 14nm工艺 最高2.8GHz主频
HYGON	海光3000系列		4-8内核 32路PCIe通道 2.0-3.3GHz主频	海光5000系列		8-16内核 64路PCIe通道 2.5-3.2GHz主频	海光7000系列		16-32内核 128路PCIe通道 2.0-3.3GHz主频
Kunpeng	鲲鹏916		24内核 16nm工艺 2.4GHz主频	鲲鹏920-3226		32-48内核 7nm工艺 2.6GHz主频	鲲鹏920-6426		64内核 7nm工艺 2.6GHz主频
龙芯中科	龙芯3C5000		16内核 560GFlops 峰值运算速度 2.0-2.2GHz主频	龙芯3D5000		32内核 1024GFlops 峰值运算速度 >2.0主频	龙芯3C6000		16内核 12nm工艺 2.5GHz主频

来源：公开资料整理，专家访谈，艾瑞咨询研究院自主研究及绘制。