网络安全系列报告之二：行业成长趋势不改，新兴安全及服务成为增长风口

东方证券 ORIENT SECURITIES

深度报告

【行业·证券研究报告】

核心观点

- **网络安全行业市场规模快速增长，整体竞争格局分散。**赛迪顾问《中国网络安全发展白皮书（2019）》报告显示，2018 年我国网络安全行业的市场规模为 495.2 亿元，同比增长 20.9%，而同期全球网络安全市场规模为 1269.8 亿美元，同比增速为 8.5%。相较于全球市场，我国网络安全行业的市场规模占比较小，但增速更快，未来具有巨大的发展空间，预计 2021 年我国网络安全的市场规模超过 900 亿元。由于网络安全行业细分程度高，不同的细分市场都有相应的专业厂商，但没有一家厂商能够实现网络安全领域的全覆盖，导致行业整体竞争格局较为分散，但虚拟专用网、防火墙等成熟细分领域集中度较高。
- **事件+政策+技术，刺激网络安全行业需求不断释放。**近年来，网络病毒、数据泄露等网络安全事件层出不穷。由于企业的核心业务越发依托信息系统，面对日益严峻的安全态势，企业主动加大对网络安全的投入力度。同时《网络安全法》、等保 2.0、《密码法》等一系列政策文件相继出台，为我国网络安全行业的有序发展提供了良好的政策保障和法律依托，进一步刺激网络安全市场需求。另外，新兴技术的应用带来新的安全风险，安全防护对象由传统的 PC、服务器拓展至云平台、大数据和泛终端，使得安全整体规模不断拓展。
- **新兴安全发展迅速，积极防御产品成为未来趋势。**云计算、物联网等新兴技术加速与各行业融合，云安全等新市场应运而生，并成为行业重要的增长风口。云安全市场 18 年规模达到 37.8 亿元，同比增长 44.8%，预计 18-21 年的复合增速将达到 45.2%，显著高于行业整体增速。面对日益复杂的网络安全环境以及新一代安全威胁，传统单点防御逐渐失效，而新兴技术带来了安全产品的迭代升级，推动安全体系由被动防御向主动防御演进。态势感知产品通过大数据分析、人工智能等新兴技术的赋能，以及持续的监测响应、深度分析以及预示预警，可有效检测和防御新型安全威胁，逐渐成为主动防御时代的安全大脑。
- **安全服务占比不断提升。**全球网络安全市场以安全服务为主， 2018 年占比达到 64.4%，而同期我国安全市场结构中安全硬件占比接近一半，安全服务占比仅为 14%，但占比逐年提升。当前严峻的安全态势以及新兴技术的普及使得企业安全架构和管理变得更加复杂，风险评估、安全管理咨询、安全托管服务等越发受重视，随着虚拟化及云服务理念的渗透，企业对于持续性的安全服务需求逐渐增加，安全服务占比将逐渐提升。

投资建议与投资标的

- 当前传统安全产品市场已接近成熟，格局较为稳定，各个头部厂商均拥有自己优势的细分市场。结合行业未来发展趋势，我们认为未来两类安全厂商具备快速成长机会：

  1）基本盘稳固，并在云安全等新兴安全领域或安全服务市场拓展顺利的网络安全公司，建议关注安恒信息(688023，未评级)、启明星辰(002439，未评级)、南洋股份(002212，未评级)、绿盟科技(300369，未评级)、山石网科(688030，未评级)；

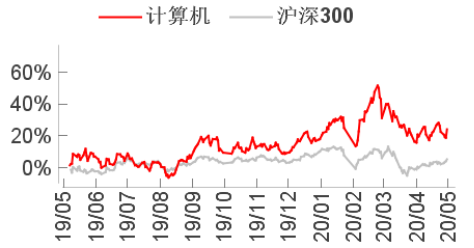
  2）立足良好细分赛道，并在其他行业拥有强劲增长点的网络安全公司，建议关注深信服(300454，增持)、美亚柏科(300188，未评级)。

风险提示

- 政策落地不及预期的风险；市场竞争加剧的风险

行业评级	看好 中性 看淡 (维持)
国家/地区	中国
行业	计算机行业
报告发布日期	2020 年 05 月 06 日

行业表现



资料来源：WIND、东方证券研究所

证券分析师	浦俊懿
	021-63325888*6106
	pujunyi@orientsec.com.cn
	执业证书编号：S0860514050004
联系人	陈超
	021-63325888-3144
	chenchao3@orientsec.com.cn
联系人	徐宝龙
	021-63325888-7900
	xubaolong@orientsec.com.cn

目 录

图表目录

一、行业概况：行业细分程度高，未来市场空间广阔

1.1 网络安全的概念和内涵不断演进

随着科技的进步和社会的发展，网络安全的概念和内涵不断演进。其发展历程可分为起源期、萌芽期、成长期和加速期四个时期，分别对应通信加密时代、计算机安全时代、信息安全时代以及网络空间安全时代。目前网络安全正处于网络空间安全时代的加速期：

- **起源期（通信加密时代，1940s 至 1980s）：**通信加密是网络安全的前身，尽管彼时计算机网络未大规模普及，也并未形成民间的商业市场，但通信信号的加密已经属于国家安全的重要范畴，密码技术作为最为重要和基础的支撑技术，一直延续至今；
- **萌芽期（计算机安全时代，1980s 至 2000 年）：**彼时安全的关注点在于计算机设备本身，包括硬件、操作系统以及存储的电子数据，趋势科技、卡巴斯基、瑞星等国内外安全厂商相继产生，防病毒产品、数据加密等是主要的产品形态。同时各国相继出台了网络安全相关的法律法规，如美国的《计算机安全法》、我国的《计算机信息系统安全保护条例》；
- **成长期（信息安全时代，2000-2013 年）：**随着 PC 和互联网的普及，企业信息化程度不断提高，自动化和远程办公的需求不断增加，安全的关注点逐渐从终端延伸到网络，此时的信息安全主要包括两方面，一是网络边界安全，产品包括防火墙、VPN 等，二是信息系统本身及其承载内容的安全，其中信息安全时代更侧重于边界安全；
- **加速期（网络空间安全时代，2014 年至今）：**随着“云大物移智”等新兴技术不断发展，万物互联的时代逐渐开启，网络空间成为继海、陆、空、天后的第五空间。2014 年中央网络安全和信息化领导小组成立，随后网络安全法、等保 2.0 等政策不断出台，网络安全上升为国家战略。与信息安全时代的区别在于网络边界逐渐模糊或消失，仅凭传统的边界安全已不能做到有效防护，防护理念和技术发生深刻改变，主动安全逐渐兴起。安全解决方案和安全服务也越来越被重视。

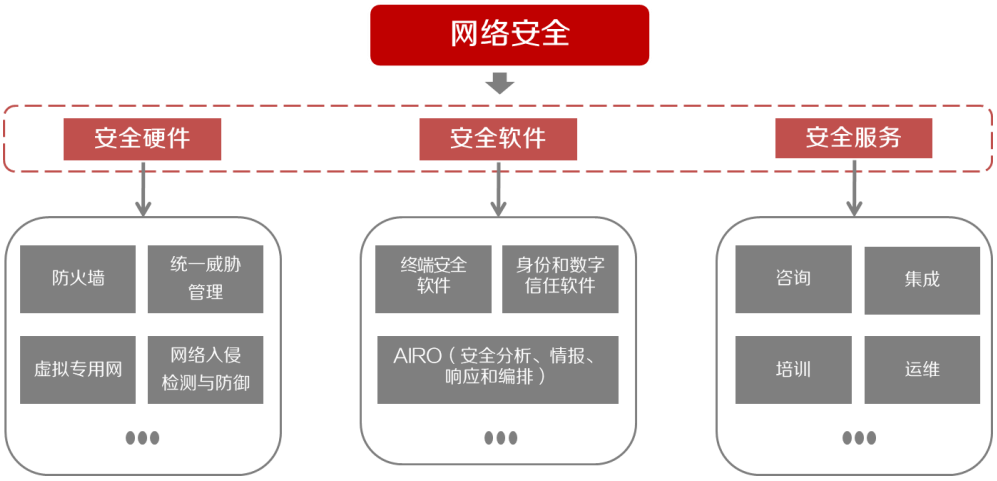
图 1：网络安全的发展历程

数据来源：安全牛，东方证券研究所

1.2 细分领域众多，行业竞争格局相对分散

网络安全细分市场众多，同时随着技术的发展细分程度进一步增加。按照产品结构划分，网络安全可以划分为安全硬件、安全软件及安全服务三大类，而每一大类产品包含众多的细分市场，如安全硬件包括防火墙、VPN、入侵检测与防御等，安全软件包括防病毒软件、终端安全软件、邮件安全软件等，安全服务包括咨询、集成、培训、运维等。技术的进步带来网络安全环境更加复杂，网络安全的防护范围、防护手段以及防护目标不断扩充，同时新型的攻击手段不断出现，这将不断催生出新的产品形态，使得网络安全的细分程度不断增加，如云计算带来的云抗 DdoS、云身份管理等细分市场。

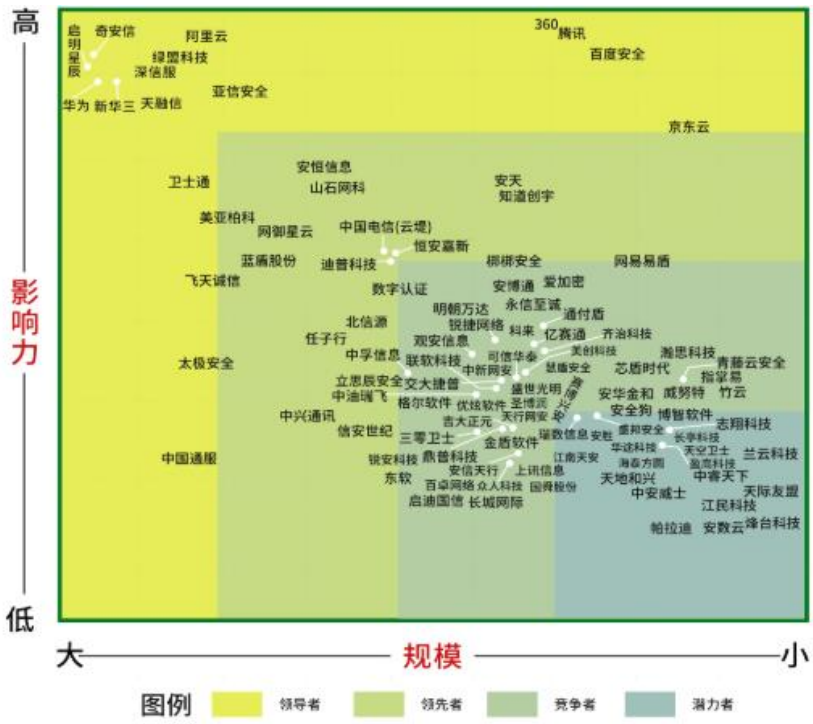
图 2：网络安全细分市场划分



数据来源：IDC，东方证券研究所

网络安全行业不断演进、细分程度高的特点，使得市场诞生出众多的网络安全厂商。《中国网络安全产业白皮书(2019)》的数据显示，2018 年我国共有 2898 家从事网络安全业务的企业，其中当年度新增企业 217 家，同比增长 8.1%。安全牛根据影响力及规模等指标构建了 2019 年国内网络安全百强企业矩阵，矩阵划分为领导者、领先者、竞争者和潜力者四个象限。具体来看，启明星辰、深信服、绿盟科技、奇安信等企业目前属于国内网络安全行业的第一梯队，处于领导者象限，安恒信息、美亚柏科、迪普科技、山石网科等企业属于第二梯队，处于领先者象限。竞争者和潜力者象限主要被众多的初创型企业占据。

图 3：国内网络安全 100 强企业（2019）



数据来源：安全牛，东方证券研究所

行业整体竞争格局相对分散，部分成熟细分领域集中度较高。由于网络安全行业细分程度高，不同的细分市场都有相应的专业厂商，但没有一家厂商能够实现网络安全领域的全覆盖，导致行业整体竞争格局较为分散。另外，多数优势厂商在数个细分市场中占据领先地位，如深信服在虚拟专用网、安全内容管理等领域市占率领先，启明星辰在入侵检测与防御等领域市占率领先，使得这些相对成熟的细分市场集中度较高。

表 1：2018 年国内部分细分市场份额分布

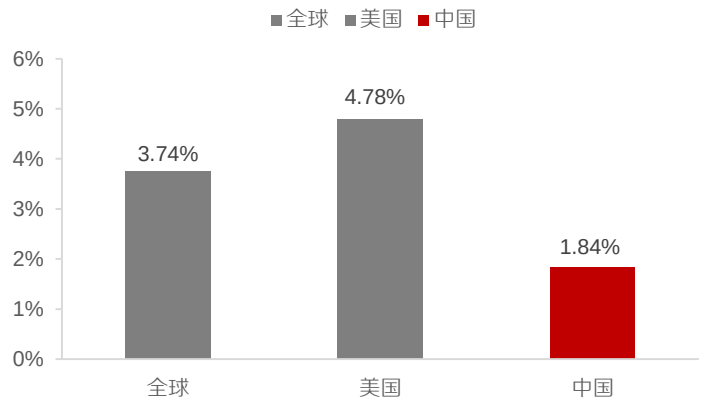
类型	细分市场	主要企业在细分市场市占率
安全硬件	虚拟专用网	深信服（30.6%）、启明星辰（10.6%）、天融信（7.2%）
	统一威胁管理	网御星云（16.2%）、深信服（14.1%）、奇安信（13.3%）
	安全内容管理	深信服（25.5%）、奇安信（13.34%）、绿盟（5.8%）
	入侵检测与防御	启明星辰（19.6%）、绿盟（19.3%）、新华三（11.3%）
	防火墙	天融信（22.4%）、华为（21.4%）、新华三（19.3%）
安全软件	终端安全软件	奇安信（22.9%）、Symantec（17.0%）、亚信安全（9.4%））
	身份和数字信任软件	吉大正元（16.3%）、亚信安全（15.0%）、格尔软件（11.3%）
	AIRO（安全分析、情报、响应和编排）	绿盟科技（21.2%）、启明星辰（16.0%）、IBM（15.6%）

数据来源：IDC，东方证券研究所

1.3 市场规模快速增长，未来前景广阔

相对于美国和全球平均水平，我国 IT 安全投入占 IT 整体投入的比例较低，未来我国 IT 安全投入有望加大。从 IT 安全投入占 IT 整体投入的比例看，全球平均水平在 3.74%，美国为 4.78%，而我国仅为 1.84%。再加上我国 IT 整体投入规模不及美国，我国实际的 IT 安全投入规模与美国相距甚远。近年来，我国逐渐重视网络安全的建设，相继出台了《网络安全法》、等保 2.0 标准等多项政策法规和标准推动网络安全产业的发展，网络安全的投入有望不断加大。

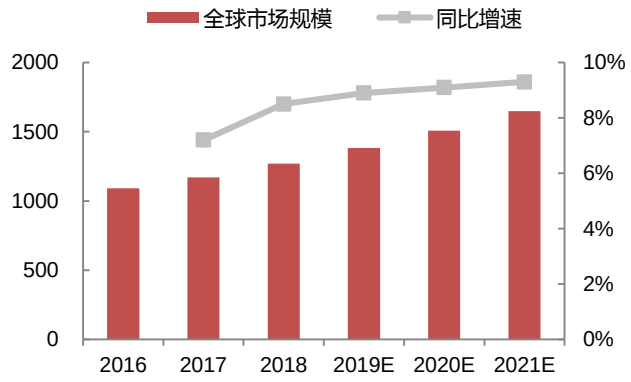
图 4：IT 安全投入占 IT 整体投入的比值



数据来源：IDC，东方证券研究所

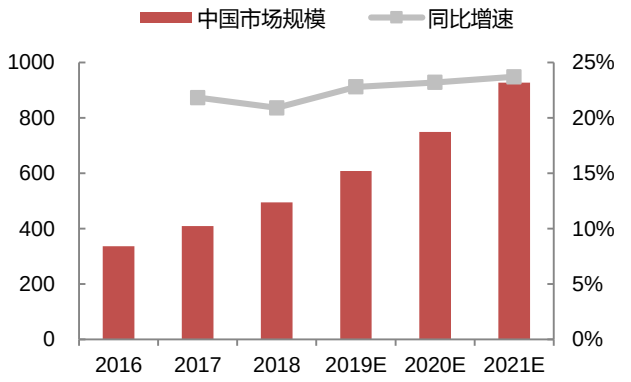
新兴技术使得网络安全内涵不断丰富，同时随着安全防护意识不断提高以及政策的不断驱动，我国网络安全行业的市场规模快速增长。赛迪顾问《中国网络安全发展白皮书（2019）》报告显示，2018 年我国网络安全行业的市场规模为 495.2 亿元，同比增长 20.9%，而同期全球网络安全市场规模为 1269.8 亿美元，同比增速为 8.5%。相较于全球市场，我国网络安全行业的市场规模占比较小，但增速更快，未来具有巨大的发展空间，预计 2021 年我国网络安全的市场规模超过 900 亿元。

图 5：全球网络安全市场规模及同比增速（亿美元，%）



数据来源：赛迪顾问，东方证券研究所

图 6：我国网络安全市场规模及同比增速（亿元，%）



数据来源：赛迪顾问，东方证券研究所

二、驱动因素：事件+政策+技术，刺激网络安全需求不断释放

2.1 安全态势严峻，企业主动安全意识逐渐增强

近年来，网络病毒、数据泄露等网络安全事件层出不穷。网络安全事件的规模越来越大，影响越来越广，波及了政府、金融、教育、制造业等各个领域。恶意程序及安全漏洞数量持续走高，安全态势日益复杂。根据 RiskIQ 发布的年度报告，2018 年全球因网络犯罪造成的损失达 15000 亿美元，较 2014 年的 4450 亿美元增长了 237%。

表 2：全球网络安全事件频发

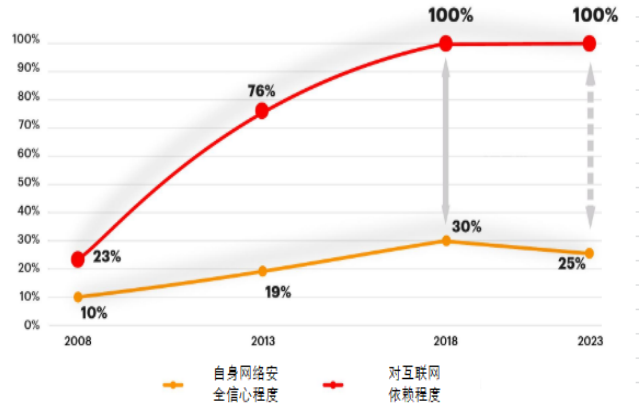
时间	事件名称	事件影响
2018.1	Intel CPU存在严重漏洞	自1995年起发布的x86处理器几乎全受该底层漏洞影响，攻击者可利用该漏洞直接访问核心内存中的敏感内容，包括用户账号密码及文件等
2018.3	美英澳等国多所大学遭遇网络攻击	通过钓鱼邮件，黑客盗取了美国144所大学及其他国家176所大学的31TB资料，价值高达34亿美元
2018.7	顺丰速运用户信息泄露	约3亿用户的个人信息（包含寄收件人姓名、地址和电话等）在暗网被兜售
2018.8	华住旗下酒店用户信息泄露	泄露的数据共计140G约5亿条信息，内容包括华住官网注册资料、酒店入住登记身份信息和酒店开房记录等
2018.8	台积电遭遇勒索病毒入侵	由于操作系统未及时安装补丁，导致感染勒索病毒后迅速扩散，预计损失超过17亿人民币
2018.11	万豪集团用户数据外泄	客房预订数据库自2014年起就已遭遇入侵，或导致5亿用户信息外泄，这些外泄数据包括用户姓名、电话号码、电子邮件、护照号码、SPG俱乐部帐号、支付卡号和支付卡有效期等敏感信息
2019.3	俄罗斯50多家大型企业遭到未知攻击者勒索	攻击使用物联网设备，尤其是路由器，伪装成欧尚、马格尼特、斯拉夫尼奥夫等50多家知名公司发送钓鱼电子邮件，对公司人员进行勒索攻击。
2019.10	社交媒体资料数据泄漏– 40亿条记录	在ElasticSearch服务器上泄露的数据共计约40亿条记录，包含姓名，电子邮件地址，电话号码，LinkedIN和Facebook个人资料信息。

数据来源：互联网，东方证券研究所

随着信息化建设的逐步推进，企业的核心业务越发依托信息系统，数据已成为企业的核心资产。根据埃森哲发布的报告显示，新兴技术的不断涌现使得企业自身业务越发依赖于互联网，网络安全风险也随之上升，但企业采用新技术的速度远远超过了解决相关安全问题的速度。在受访的 1700 多家企业中，仅有 30%的企业对自身的网络安全抱有信心，预计五年后这一数据将降到 25%，网络安全的发展和实施仍旧任重道远。另外，报告还预计未来五年网络攻击在全球范围内将给企业带来高达 5.2 万亿美元的额外成本或营收损失。

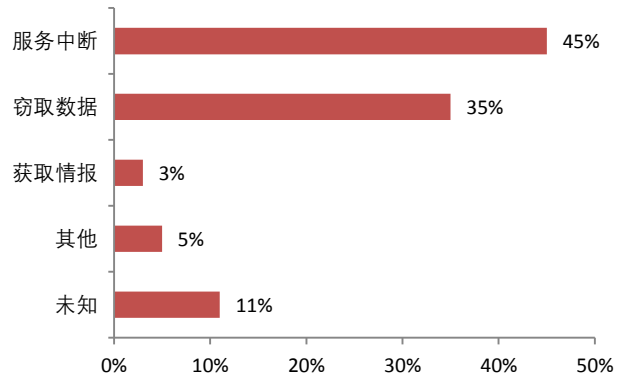
网络攻击的主要目标是服务中断和数据窃取。网络安全公司 Radware 发布的 2018-2019 年全球应用及网络安全报告显示，受访企业表示遭遇网络攻击的主要目标是服务中断和数据窃取，分别占到 45%和 35%。而网络攻击不仅使得服务中断或生产力损失，还会导致数据泄露、信息丢失，并带来不良的客户体验。

图 7：企业对互联网依赖程度及对自身安全的信心程度



数据来源：埃森哲，东方证券研究所

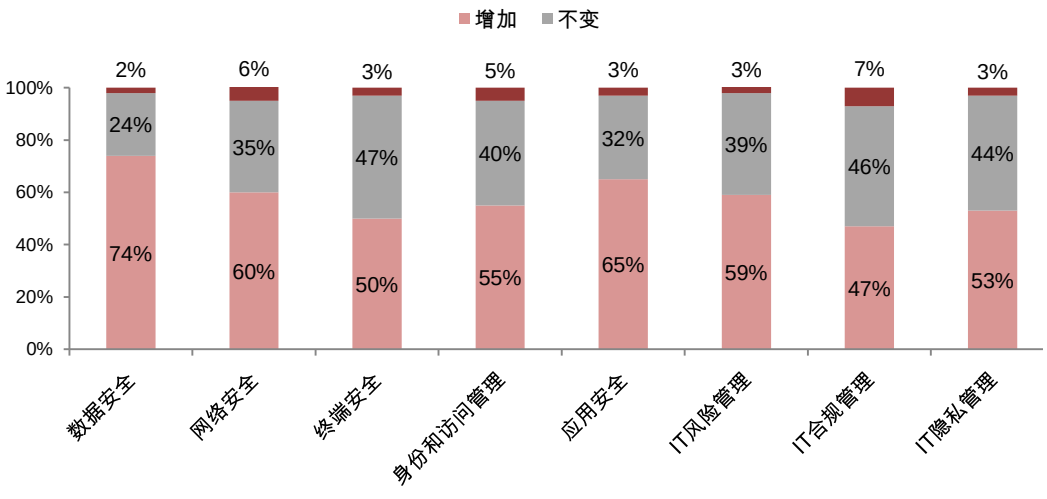
图 8：网络攻击的首要目标



数据来源：Radware，东方证券研究所

面对日益严峻的安全态势，越来越多的企业主动加大对网络安全的投入力度。根据 Gartner 调查统计，2017 年有超过一半的企业都增加了信息安全主要细分领域的支出，其中有 74%的企业增加了对数据安全的投入，65%的企业增加了应用安全的支出。由于安全形势日趋复杂，我们预计企业将继续增加对安全的投入。

图 9：全球企业/组织 IT 安全投入变化（2017）



数据来源：Gartner，东方证券研究所

2.2 国家战略先行，合规性与强制性驱动并重

面对严峻的网络安全形势，我国政府推出一系列网络安全政策，刺激下游市场需求不断释放。近年来，《网络安全法》、《国家网络空间安全战略》、《密码法》等一系列政策文件相继出台，尤其是 2019 年 12 月等保 2.0 标准的正式实施，对现有安全防护体系进行补充和完善，并对新兴网络领域实现全面覆盖，有力推动了国内网络安全市场的全面发展。这些都为我国网络安全市场产业的有序发展提供了良好的政策保障和法律依托，进一步刺激网络安全市场需求。

表 3：网络安全相关政策法规

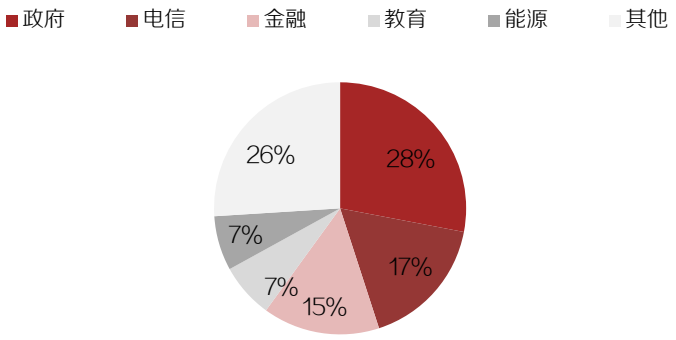
政策名称	发布时间	发布部门	相关内容
《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》	2012.6	国务院	提出健全安全防护和管理，保障重点领域信息安全举措：1）确保重要信息系统和基础信息网络安全；2）加强政府和涉密信息系统安全管理；3）保障工业控制系统安全；4）强化信息资源和个人信息保护
《国务院关于积极推进"互联网＋"行动的指导意见》	2015.7	国务院	提出"完善互联网融合法律规范和标准规范，增强安全意识，强化安全管理防护，保障网络安全"
《关于加强国家网络安全标准化工作的若干意见》	2016.8	国家质监总局、国标委	1）建立网络安全统筹协调、分工协作的工作机制；2）加强网络安全标准体系建设，提升标准质量和基础能力；3）强化网络安全标准宣传实施；4）加强国际网络安全标准化工作；5）抓好标准化人才队伍建设，并做好资金保障
《"十三五"国家信息化规划》	2016.12	国务院	提出"组织实施信息安全专项，建立关键信息基础设施安全防护平台，支持关键基础设施和重要信息系统，整体提升安全防御能力"
《国家网络空间安全战略》	2016.12	国家互联网信息办公室	提出：1)加强网络安全工作，推广使用安全可控产品；2)把有关个人信息保护的法律责任、法律要求落实到企业、机构；3)采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏
《软件和信息技术服务业发展规划（2016－2020年）》	2017.2	工信部	提出：1）发展信息安全产业，支持面向"云管端"环境下的基础类、网络与边界安全类、终端与数字内容安全类、安全管理类等信息安全产品研发和产业化；2）到"十三五"末信息安全产业规模达到 2000 亿元，年均增长 20%以上
《中华人民共和国网络安全法》	**2017.6**	**全国人大常务委员会**	**提出：1）国家直属部门及政府推动网络安全工作的职责；2）网络运营者及关键信息基础设施的运行安全规定；3）个人信息的保护规定；4）国家网络安全监测预警及汇报机制；5）相关处罚规定**
《网络安全等级保护测评机构管理办法》	2018.3	公安部	旨在加强网络安全等级保护测评机构管理，提高等级测评能力和服务水平
《关于推动资本市场服务网络强国建设的指导意见》	2018.4	网信办、证监会	提出充分发挥资本市场在资源配置中的重要作用，规范和促进网信企业创新发展，推进网络强国、数字中国建设
《网络安全等级保护条例（征求意见稿）》	**2018.6**	**公安部**	**对网络安全等级保护的适用范围、各监管部门的职责、网络运营者的安全保护义务以及网络安全等级保护建设提出了更加具体、操作性的要求，为开展等级保护工作提供了重要的法律支撑**
《公安机关互联网安全监督检查规定》	2018.9	公安部	定义检查主体单位、检查对象、检查内容，检查方式及处罚办法，旨在加强和规范公安机关互联网安全监督检查工作，防范网络违法犯罪，维护网络安全
《互联网个人信息安全保护指引》（征求意见稿）	2018.11	公安部	规定了个人信息安全保护的安全管理机制、安全技术措施和业务流程的安全
网络安全等级保护制度 2.0	**2019.5**	**国家标委**	**包括了定级指南、基本要求、安全设计要求及测评要求等内容，横向**

标准		会	扩展了对云计算、移动互联网、物联网、工业控制系统、大数据的安全要求，纵向扩展了对等保测评机构的规范管理
《国家网络安全产业发展规划》	2019.6	工信部	2020 年，依托产业园带动北京市网络安全产业规模超过 1000 亿元，拉动 GDP 增长超过 3300 亿元，打造不少于 3 家年收入超过 100 亿元的骨干企业，其次到到 2025 年，依托产业园建成我国网络安全产业“五个基地”
《密码法》	2019.10	全国人大常委	旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法制化水平，是我国密码领域的综合性、基础性法律

数据来源：政府网站，东方证券研究所

等保 2.0 的正式出台将进一步带动下游需求的快速扩张。网络安全是典型的需求驱动行业，当前从下游行业应用情况来看，政府、电信及金融领域的安全投入规模最大，2017 年分别占到全国安全总投资额的 28%、17%、15%，同时，教育、工业等其他领域的信息安全市场也日渐兴起。网络安全市场的下游客户结构决定了其具备强政策周期属性，因此我们认为等保 2.0 正式实施后，拥有第三级及以上信息系统较多的政府、金融、电信等领域势必会加大网络安全投入，以符合等保 2.0 的规范和要求。另外，等保 2.0 将云计算、移动互联网、物联网、工业控制等新兴技术领域纳入监管范围，相应领域网络安全产品及服务的需求也将随之提升，将促进整体安全市场进一步提速增长。

图 10：网络安全下游客户分布

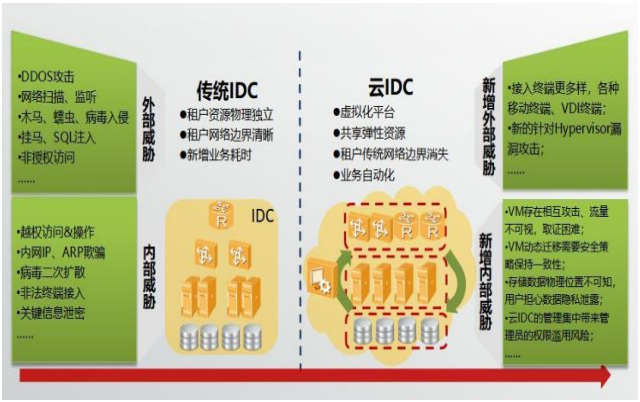


数据来源：中国信通院，东方证券研究所

2.3 新技术带来新风险，安全内涵不断延伸

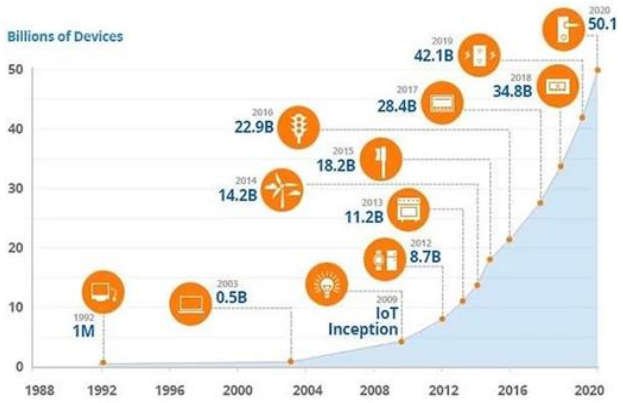
新兴技术的应用带来新的安全风险，安全防护对象由传统的 PC、服务器拓展至云平台、大数据和泛终端。以云计算和物联网为例，云计算使得 IT 基础架构发生根本性变化，云计算环境下服务器、存储、网络等虚拟化技术为云服务提供了基础技术支持，并解决了资源利用率及资源提供的自动扩展等问题，但也使得传统安全边界概念消失，使得云计算相较于传统 IT 架构面临更多的安全风险，如针对虚拟化平台的漏洞等。而物联网市场的快速发展、设备连接数量的迅速增加，也使得物联网面对的安全风险加剧。

图 11：云计算面临更多安全风险



数据来源：CSDN，东方证券研究所

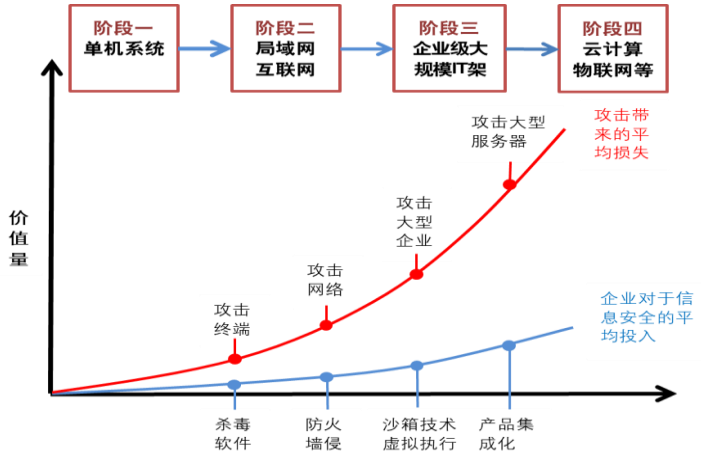
图 12：全球物联网设备数量高速增长（单位：十亿）



数据来源：CISCO，东方证券研究所

“云大物移智”等新技术的应用使得网络安全的价值量不断上升。网络安全并不能直接创造价值，其价值量由信息系统本身的价值决定。随着政企数字化转型的推进，云计算、大数据、物联网、移动互联网、人工智能等新兴技术与业务深度融合，信息系统及其承载的业务及数据的价值大大提升，网络安全风险等同于业务运营风险，这使得每次遭遇网络攻击造成的平均损失不断提高，对于信息系统及其承载的业务及数据的防护也变得越发必要。

图 13：网络安全价值不断提升



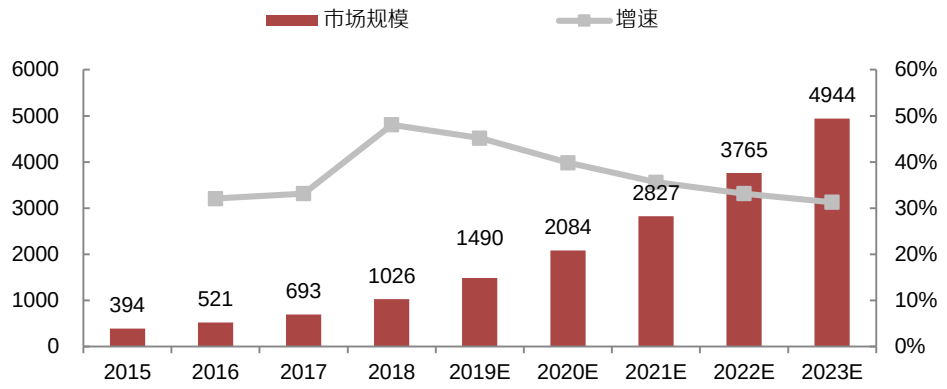
数据来源：智研咨询，东方证券研究所

三、行业趋势：新兴安全发展迅速，安全服务占比不断提升

3.1 云安全等新兴安全领域发展迅速

云计算、物联网等新兴技术加速与各行业融合。云计算采用分布式和虚拟化等技术带给上云用户低廉的运营成本和便捷的资源使用。随着“互联网+”等政策的积极推进，云计算作为信息技术创新服务模式的集中体现，已从互联网行业向政务、金融、工业等各个行业加速渗透。整体云服务市场继续保持快速增长，预计 2023 年将达到 4944 亿，未来三年 CAGR 依然保持在 30%以上。

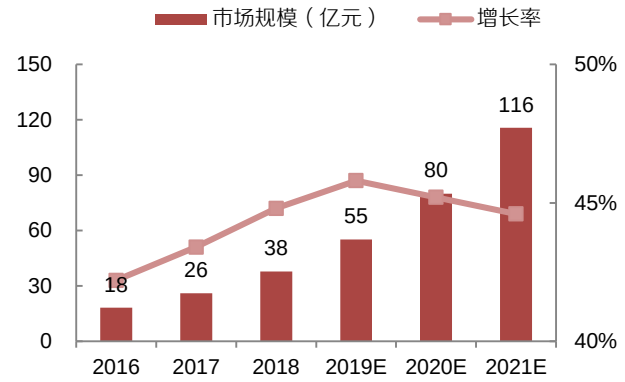
图 14：中国云服务市场整体规模及增速（亿元，%）



数据来源：艾瑞咨询，东方证券研究所

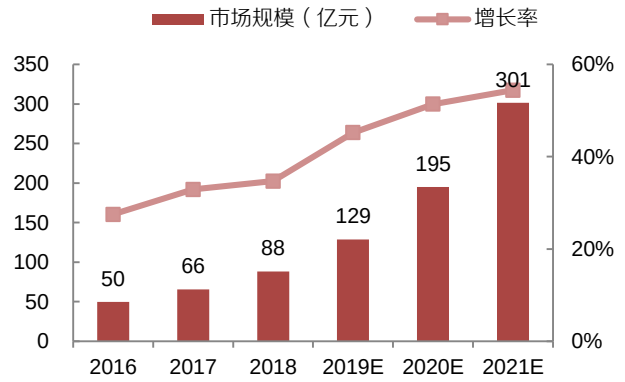
云安全、物联网安全等新兴安全市场增长迅速，成为行业重要的增长风口。2018 年云安全市场规模达到 37.8 亿元，同比增长 44.8%，预计 18-21 年的复合增速将达到 45.2%。随着我国云计算市场继续高速增长，云安全的需求将持续增加。同时，随着 5G、AI、边缘计算等技术的逐步落地，物联网产业迎来快速发展，联网终端呈现爆发增长，物联网安全将成为刚性需求。赛迪顾问的数据显示，2018 年国内物联网安全规模达到 88.2 亿元，同比增长 34.7%，随着万物互联的时代到来，未来有望实现加速发展。

图 15：我国云安全市场规模及同比增速（亿元，%）



数据来源：CCID，东方证券研究所

图 16：我国物联网安全市场规模及同比增速（亿元，%）



数据来源：CCID，东方证券研究所

3.2 积极防御产品成为未来趋势

新兴技术也带来了安全产品的迭代升级，推动安全体系由被动防御向主动防御演进。面对日益复杂的网络安全环境以及新一代安全威胁，传统单点防御逐渐失效。一方面云技术的普及使得基于边界的安全防御方法无法满足现有的安全防御要求。另一方面，由于传统被动的防御措施通常是将每个攻击方式作为单独的路径，每个阶段作为独立的时间来检查，而不是将这些阶段和方式作为一系列的网络事件来查看和分析，产生了众多的信息孤岛，因此零日攻击、高级持续性威胁（APT）等

新一代安全威胁能够绕过传统的安全检测和防御体系。随着大数据分析、人工智能、安全情报收集等技术的逐渐成熟和发展，安全检测技术对安全态势的分析、预警和预测越来越准确，具备数据分析、安全运营和情报收集等能力的中高位安全产品不断涌现，网络安全防御体系逐渐向自动响应、追查、威胁诱捕等方向的主动防御体系转变。

图 17：网络安全滑动标尺模型

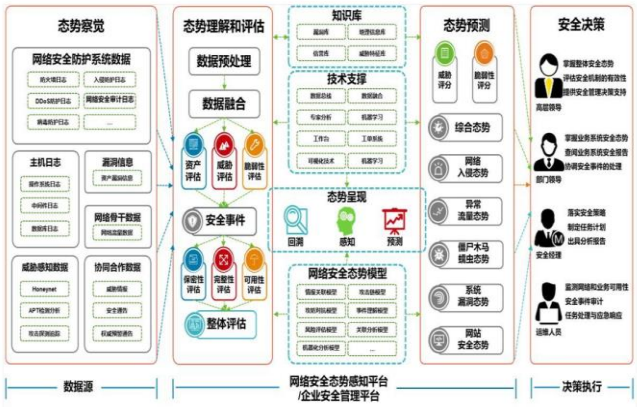
数据来源：奇安信，东方证券研究所

被动防御时代以边界防护为主，防火墙是最重要的产品，主动防御时代安全大脑是防御体系中最核心的组成部分，而态势感知充当的就是安全大脑的角色。态势感知的工作原理是对网络环境中引起网络态势发生变化的安全要素信息进行获取、理解，评估网络安全的状况，预测其发展趋势，并以可视化的方式展现给用户，帮助用户实现相应的安全决策与行动，从而实现积极主动的动态安全防御。通过大数据分析、人工智能等新兴技术的赋能，以及持续的监测响应、深度分析以及预示预警，可有效检测和防御新型安全威胁。

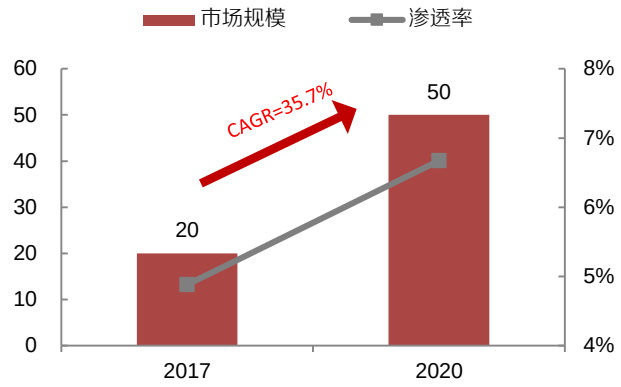
态势感知市场规模增长迅速，快于同期网络安全整体市场增速。根据安全牛的数据统计，2017 年国内态势感知的市场规模约为 20 亿元，预计 2020 年达到 50 亿元，CAGR 约为 35.7%，显著高于网络安全整体市场增速。态势感知作为主动防御体系的安全大脑，对于监管单位和关键信息基础设施相关的行业而言已成为必建设施，由于目前态势感知的市场渗透率较低，同时存量的态势感知需要不断扩容和更新以适应外部网络环境及内部客户需求的变化，我们认为态势感知市场规模有望继续保持高速增长趋势。

图 18：态势感知体系架构

图 19：我国态势感知市场规模及渗透率（亿元，%）



数据来源：绿盟科技，东方证券研究所

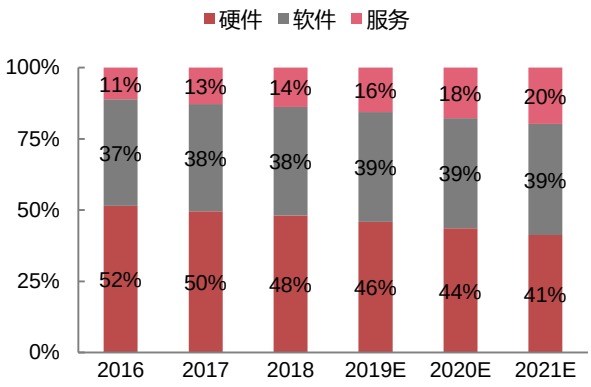


数据来源：安全牛，东方证券研究所

3.3 安全服务占比不断提升

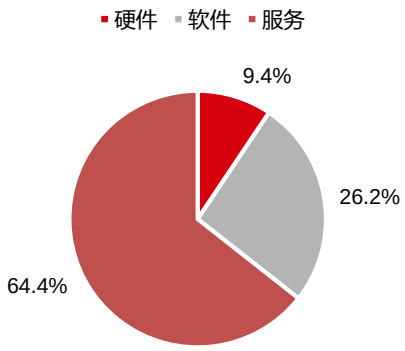
全球网络安全市场以安全服务为主，我国网络安全市场暂以安全硬件为主。2018 年全球网络安全市场结构中，安全服务占比达到 64.4%，头部安全厂商提供的安全服务以订阅化服务为主。而同期我国网络安全市场结构中安全硬件占比接近一半，安全服务占比仅为 14%，但占比逐年提升。当前严峻的安全态势以及新兴技术的普及使得企业安全架构和管理变得更加复杂，风险评估、安全管理咨询、安全托管服务等越发受重视，随着虚拟化及云服务理念的渗透，企业对于持续性的安全服务需求逐渐增加，安全服务占比将逐渐提升。

图 20：国内网络安全市场结构



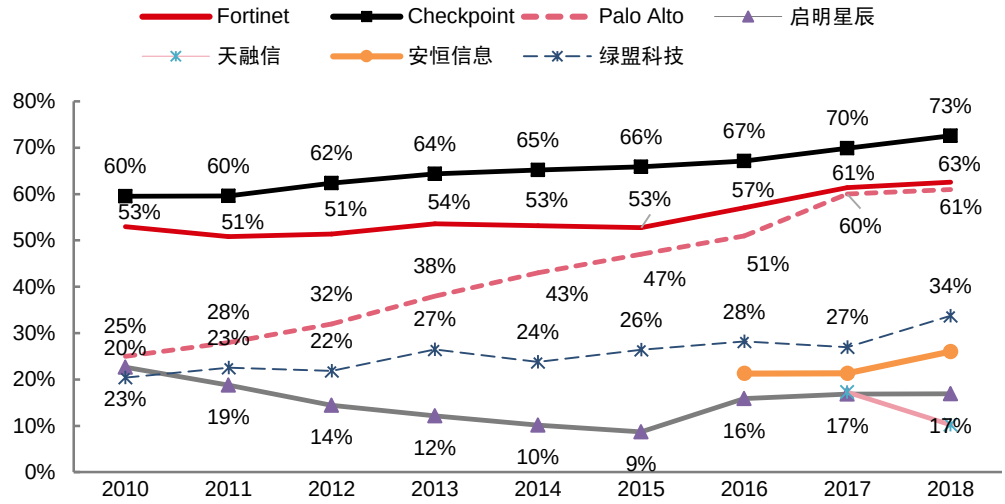
数据来源：CCID，东方证券研究所

图 21：全球网络安全市场结构（2018）



数据来源：CCID，东方证券研究所

图 22：国内外安全公司安全服务收入占比对比



数据来源：Wind，东方证券研究所

四、投资建议

尽管网络安全需求受到了短期疫情影响，但从长期来看行业仍处于景气度提升阶段。当前传统安全产品市场已接近成熟，格局较为稳定，各个头部厂商均拥有自己优势的细分市场。结合行业未来发展趋势，我们认为未来两类安全厂商具备快速成长机会：一是基本盘稳固，并在云安全等新兴安全领域或安全服务市场拓展顺利的网络安全公司，建议关注安恒信息(688023，未评级)、启明星辰(002439，未评级)、南洋股份(002212，未评级)、绿盟科技(300369，未评级)、山石网科(688030，未评级)；二是立足良好细分赛道，并在其他行业拥有强劲增长点的网络安全公司，建议关注深信服(300454，增持)、美亚柏科(300188，未评级)。

4.1 安恒信息：国内态势感知市场龙头，新兴安全业务增长迅速

营收保持高增长，安全服务占比不断提升。公司的主营业务包括网络信息安全基础产品、网络信息安全平台及网络信息安全服务，并构建了以基础产品为依托、以“新场景、新服务”为方向的专业安全产品和服务体系，公司的产品及服务涉及应用安全、大数据安全、云安全、物联网安全、工业控制安全及工业互联网安全等领域。2019 年公司实现营收 9.44 亿，同比增长 50.7%，其中安全服务实现收入 2.64 亿，同比增长 62.0%，营收占比为 28%。

图 23：安恒信息产品体系全线概念图

数据来源：安恒信息招股书，东方证券研究所

公司拥有多款产品市占率领先。公司的 Web 应用防火墙自发布后多次入围 Gartner 魔力象限推荐品牌， 2018 年度亚太市场份额 9.6%，排名第二；日志审计系统 2017 年国内市占率排名第一，数据库审计与风险控制系统、运维设计与风险控制系统、堡垒机等产品市场份额也均位于国内市场前列。

表 4：安恒信息基础安全产品市占率情况

产品名称	市场份额及排名
Web 应用防火墙	2017 年度市场份额为 16.7%，排名第二 2018 年度亚太市场份额 9.6%，排名第二
数据库审计与风险控制系统	2017 年度市场份额为 7.2%，排名第二
运维审计与风险控制系统	2016 年度市场份额为 14.5%，排名第三
Web 应用弱点扫描器、远程安全评估系统	2017 年度市场份额为 14.7%，排名第三
日志审计系统	2017 年度市场份额为 10.9%，排名第一
堡垒机	2018 年度亚太市场份额 8.8%。排名第一

数据来源：安恒信息，东方证券研究所

公司新兴安全平台业务发展迅速。公司依托态势感知技术推出了多款平台类产品，包括网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等，布局大数据安全等新兴安全领域。凭借领先的

技术实力和丰富的实施经验，公司新兴安全平台业务增长迅速，平台产品实现收入 2.72 亿，同比增长 91.2%，其中云安全平台产品同比增长 176%，大数据安全平台产品同比增长 63%，物联网安全产品同比增长 136%，在当前云安全等新兴安全高速发展的背景下有望继续保持良好发展态势。

表 5：安恒信息新兴安全平台业务发展情况（百万）

业务	2016年度	2017年度		2018年度		2019年度	
		营收	增长率	营收	增长率	营收	增长率
云安全平台产品	1.3	7.8	491%	31.4	318%	86.7	176%
大数据安全产品	16.4	42.2	157%	104.0	154%	169.1	63%
物联网平台产品	0.2	0.9	379%	6.7	632%	15.9	136%
合 计	17.9	50.9	184%	142.1	188%	271.7	91%

数据来源：Wind，东方证券研究所

4.2 深信服：领先的信息安全企业，超融合市占率不断提升

深信服的主营业务主要包括安全业务、云计算业务、企业级无线业务（19 年改为基础网络和物联网业务）。安全业务品类丰富，上网行为管理、VPN、防火墙、广域网优化、应用交付等多款产品依靠显著的技术优势，市占率常年保持行业领先。云计算业务主要以超融合为核心，提供企业云、桌面云等产品。基础网络和物联网业务（即企业级无线业务）主要由子公司信锐网科经营，产品包括无线控制器、无线接入点等。

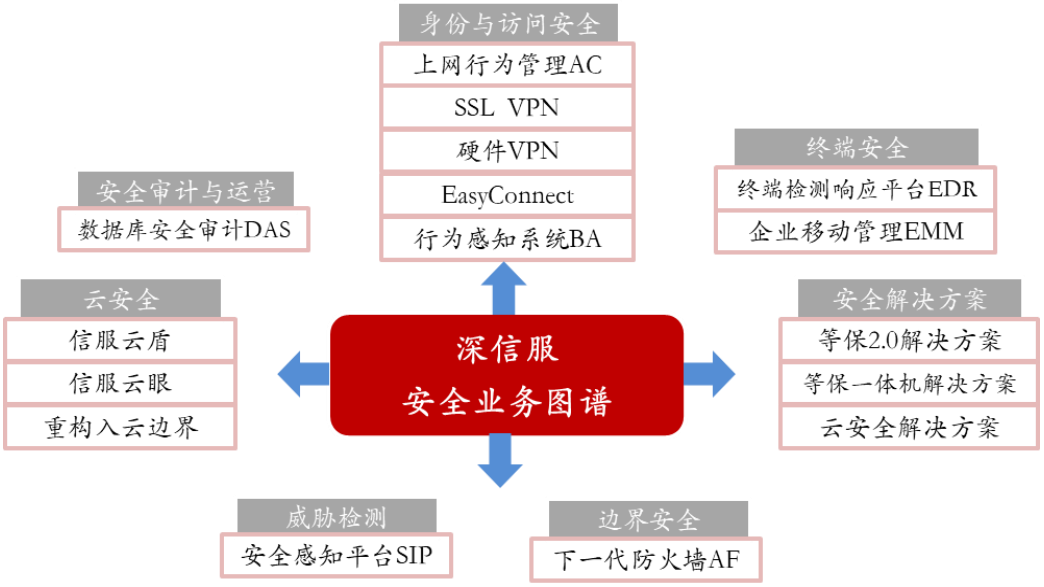
图 24：深信服主营业务

数据来源：深信服招股书，东方证券研究所

深信服在云安全、态势感知等新兴安全领域均有所布局。其中公司态势感知产品 SIP 进入了 IDC 中国态势感知解决方案领导者象限，在 IDC 创新技术能力指标获得满分。对比传统 SOC 日志处理性能提升 100 倍，可实现百亿级别的数据处理能力，威胁检测能力突出，具备更简单、更易决策的

安全可视以及自动化编排响应处置。目前公司已积累覆盖各级政府单位、教育、医疗等行业超过2000 个客户，2018 年销售额增长率高达 253%。

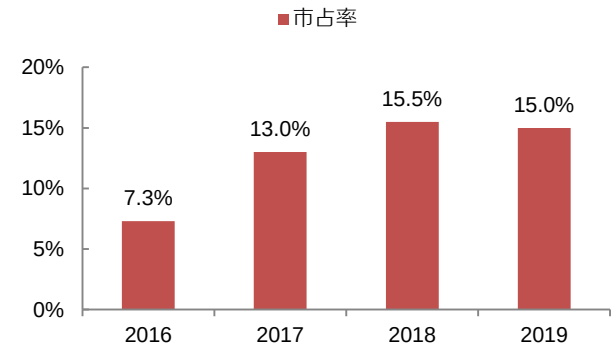
图 25：深信服安全业务图谱



数据来源：深信服，东方证券研究所

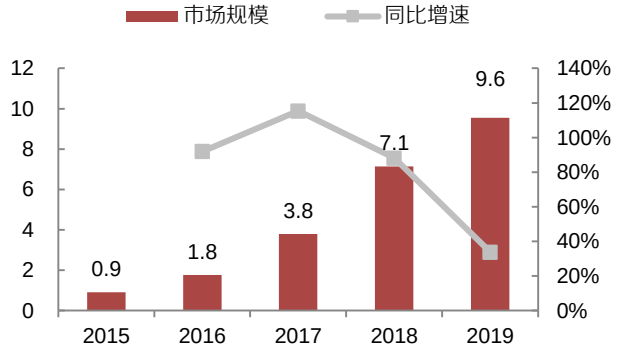
公司超融合市场份额稳居前三，云计算战略持续升级。近年来，在国内超融合软硬件整体市场快速增长的背景下，公司凭借其超融合产品在虚拟化及安全方面的优势稳居国内超融合厂商的第一梯队，市占率提升明显，从 2016 年的 7.3%上升到 2019 年的 15.0%。此外，20 年 3 月公司云计算业务战略再次升级，从过去的超融合承载业务向数据中心全面云化完成转变，以满足客户数据中心建设各个阶段的不同需求。同时还发布了 ARM 架构超融合、云计算平台以及云原生平台三大新品，形成独立产品+集成平台的开放式平台体系。我们认为公司云战略升级以及新产品的发布，将全面提升公司云计算整体解决方案能力以及覆盖领域，为公司后续的业务发展奠定良好的发展基础。

图 26：深信服超融合市占率



数据来源：CCID，东方证券研究所

图 27：国内超融合市场规模（亿美元，%）



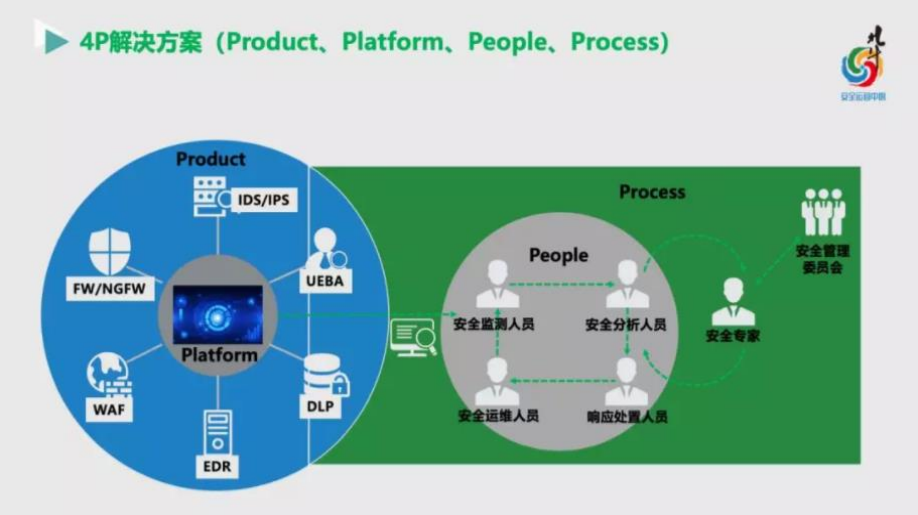
数据来源：CCID，东方证券研究所

4.3 启明星辰：信息安全行业龙头，态势感知为安全运营赋能

启明星辰是目前信息安全行业的龙头企业，拥有完善的专业安全产品线，横跨网关、检测、数据安全与平台、安全服务与工具等技术领域，共有百余个产品型号。其中，入侵检测与防御（IDS/IPS）、统一威胁管理（UTM）、安全管理平台（SOC）、数据安全、数据库安全审计与防护、堡垒机、网闸等产品的市场占有率第一。

公司安全运营、云安全及工业互联网安全三大战略新业务收入保持快速增长。2019 年公司新安全业务收入约占总收入 2 成（约 6 亿元），同比增长 200%。其中安全运营方面，公司已基本形成北京、成都、广州、杭州（东西南北）四大业务支撑中心及 30 余个城市运营中心，并已形成成熟的标准化运营体系，未来在持续扩大已有运营中心业务的基础上，将继续向其他二三级城市拓展， 20 年目标力争累计达到 80 个城市的覆盖。

图 28：启明星辰泰合网络安全态势感知平台



数据来源：启明星辰，东方证券研究所

4.4 南洋股份：电科入股领成长，老牌厂商焕新生

公司全资子公司天融信是网络安全领域的领先厂商之一，主要提供安全及大数据产品（包括安全网关、安全检测、数据安全、云安全等）以及安全服务（包括安全云服务、安全咨询与评估服务、安全运维服务等）两类产品。天融信具有多款市占率领先的细分产品，IDC 报告显示，2019 年天融信在防火墙以 23.97%的市场占有率排名第一，已连续 20 年位居国内防火墙市场第一品牌；此外，天融信在入侵防御硬件市场、VPN 硬件等市场的占有率领先。公司即将剥离线缆业务聚焦网络安全，同时电科网信入股成为公司第三大股东，公司也与腾讯云在云服务及网络安全等领域达成战略合作，这都对公司安全业务未来的拓展产生积极变化，

图 29：天融信以下一代防火墙（NGFW）为基础的安全防御体系

数据来源：天融信，东方证券研究所

公司在态势感知、安全服务等市场持续发力并取得成效。19 年公司网络安全业务实现收入 24.17 亿，同比增长 39.6%，在较高基数的基础上实现了快速增长。其中安全服务收入达到 3.37 亿同比增长 90.4%。另外天融信态势感知方案推广顺利，针对不同的客户群体先后推出了标准版、企业版、监管版等，以满足市场的差异化需求，目前已覆盖 20 多个行业。

图 30：天融信网络安全态势感知系统

数据来源：天融信，东方证券研究所

4.5 美亚柏科：电子取证市场领先，政务大数据业务成为新引擎

美亚柏科主要从事电子数据取证、大数据信息化以及网络空间安全等产品的研发、销售与服务，是相关领域的行业龙头，主要客户为国内各级司法机关及行政执法部门。公司业务包含 “四大产品+四大服务”：“四大产品”包括电子数据取证、大数据信息化平台、网络空间安全产品及专项执法装备，“四大服务”在四大产品的基础上衍生发展而来，包括存证云、培训及技术支持增值服务、网络空间安全服务及数据服务，这些产品与业务均致力于打击犯罪，实现社会治理。

图 31：美亚柏科主营业务结构图

数据来源：美亚柏科，东方证券研究所

电子取证业务收入增速逐渐恢复，大数据智能化平台成为增长核心。随着国家机构改革落地，公司相关采购和建设逐渐恢复。电子取证方面，19 年公司加快了取证 3.0 系列产品的落地，下游从网安逐步向刑侦、监察委、税务及军工等领域延伸，19 年实现收入 8.36 亿，同比增长 13.3%，增速较 18 年逐渐恢复。大数据智能化方面，公司参与部级大数据标准制定，积极把握各省市相关大数据平台建设需求，19 年实现收入 7.67 亿，同比增长 54.5%，已成为公司收入增长的核心动力。

图 32：美亚柏科大数据信息化发展方向

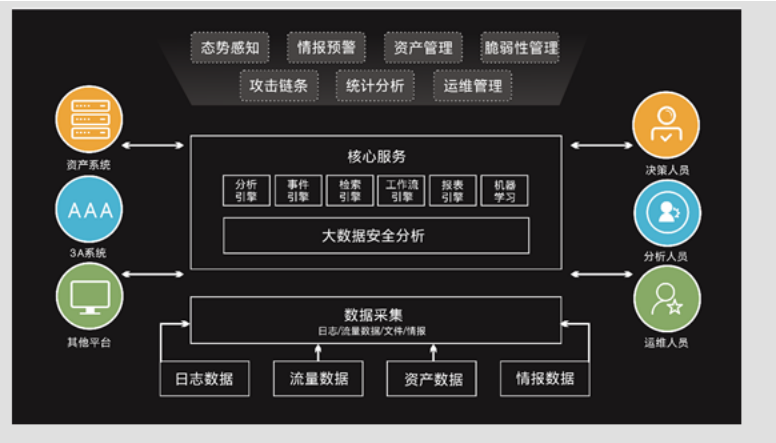
数据来源：美亚柏科，东方证券研究所

4.6 绿盟科技：P2SO 战略逐见成效，态势感知助力等保 2.0

绿盟科技是国内领先的、具有核心竞争力的企业级网络安全解决方案供应商。公司的竞争优势主要体现在行业领先的技术优势，不断创新的差异化产品和服务，优质的客户群体和丰富的行业经验，知名的品牌和行业领先的市场占有率等方面。公司的抗拒绝服务攻击系统（ADS）、网络入侵防护系统（NIPS）、远程安全评估系统（RSAS）、Web 应用防火墙（WAF）、数据泄露防护系统（DLP）等产品在 Gartner 报告、Frost & Sullivan 报告、IDC 报告及其他报告中，长年保持中国区市场占有率第一或竞争力领先。

公司持续推进 P2SO 战略，即向安全解决方案+安全运营模式转化。目前公司在工控安全、云安全等领域都取得不错的进展，并在智慧城市安全运营、行业联合安全运营及企业安全运营商发力，在中国电科产业基金入股后，公司积极拓展政府市场业务，2019 年公司实现收入 16.71 亿，同比增长 24.2%，归母净利润为 2.27 亿，同比增长 34.8%，收入及业绩均明显改善。

图 33：绿盟科技安全运营架构

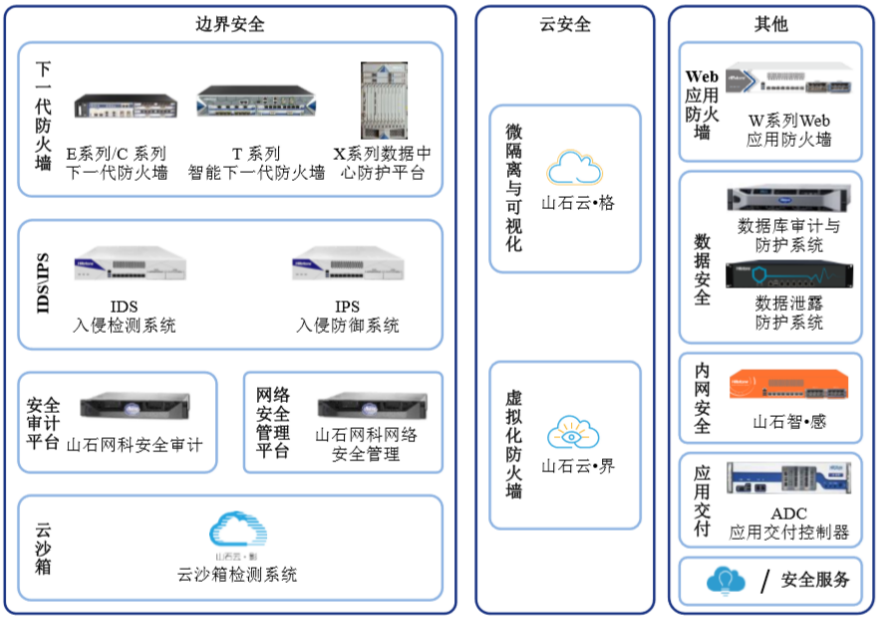


数据来源：绿盟科技官网，东方证券研究所

4.7 山石网科：边界安全领域领导厂商

山石网科是国内网络安全行业的技术创新领导厂商。自成立以来公司一直专注于网络安全领域前沿技术的创新，主要覆盖下一代防火墙、入侵检测和防御系统、安全审计、安全管理、Web 应用防火墙、内网安全在内的网络安全产品及服务。基于云计算场景，公司开发了完备的微隔离与可视化、虚拟化防火墙产品，为云端用户提供一站式、多平台安全解决方案，此外，公司还提供了数据安全、内网安全类的其他安全产品。公司下游客户主要为政府、金融、运营商、互联网、教育、医疗卫生等行业，已累计为超过 17,000 家用户提供高效、稳定的安全防护。

图 34：山石网科主要产品及服务



数据来源：山石网科招股书，东方证券研究所

公司多款核心产品受国内外权威机构认可。公司连续五年入选国际权威分析机构 Gartner 的“企业级防火墙魔力象限”、“UTM 魔力象限”，连续两年入选 Gartner 的 IDPS 魔力象限。2018 年公司被 Gartner 评为亚太地区企业级防火墙－全球性厂，2019 年成为中国唯一入选 Gartner《网络流量分析市场指南》的网络安全厂商；在新兴安全领域，公司的数据中心安全防护平台获得 Silicon Valley Communications 出版的《信息安全产品指南》“2019 年全球卓越奖”，云安全产品－山石云•格获得 VMware 公司的－VMware Ready‖认证，成为全球十余家获得该认证的网络安全产品之一。

表 6：山石网科核心产品获得国内外权威机构认可

边界安全领域	连续五年入选国际权威分析机构 Gartner 的“企业级防火墙魔力象限”、“UTM 魔力象限”
	连续两年入选 Gartner 的 IDPS 魔力象限
	2018 年被 Gartner 评为亚太地区企业级防火墙—全球性厂
	2019 年成为中国唯一入选 Gartner《网络流量分析市场指南》的网络安全厂商
云安全等新兴安全领域	公司数据中心防火墙、山石云•格、T 系列智能下一代防火墙分别获得《Cyber Defense Magazine》颁发的—最具创新数据中心安全产品奖、—下一代云安全方案奖、—突破性安全分析解决方案奖
	公司基于 NFV 的虚机微隔离安全解决方案分别获得中国网络安全联盟的“2018 年网络安全解决方案优秀奖”和中国关键信息基础设施联盟的“2018 关键信息基础设施优秀解决方案之技术创新奖”
	公司云安全产品—山石云•格‖获得 VMware 公司的 VMware Ready‖认证，成为全球十余家获得该认证的网络安全产品之一

数据来源：山石网科招股书，东方证券研究所

风险提示

政策落地不及预期的风险：政策是网络安全行业增长的重要驱动力，若等保 2.0 等标准以及其他相关政策落地或实施强度不及预期，整体行业需求也将降低。

市场竞争加剧的风险：若行业竞争加剧，具体表现为产品技术、价格和服务等各方面的竞争，如果建议关注的标的不能采取有效措施确保自身竞争优势，自身经营业绩将会受到不利影响。

分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明：

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断；分析师薪酬的任何组成部分无论是在过去、现在及将来，均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

投资评级和相关定义

报告发布日后的 12 个月内的公司的涨跌幅相对同期的上证指数/深证成指的涨跌幅为基准；

公司投资评级的量化标准

买入：相对强于市场基准指数收益率 15%以上；

增持：相对强于市场基准指数收益率 5%～15%；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

减持：相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内，分析师基于当时对该股票的研究状况，未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定，研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形；亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确投资评级；分析师在上述情况下暂停对该股票给予投资评级等信息，投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

行业投资评级的量化标准：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

看淡：相对于市场基准指数收益率在-5%以下。

未评级：由于在报告发出之时该行业不在本公司研究覆盖范围内，分析师基于当时对该行业的研究状况，未给予投资评级等相关信息。

暂停评级：由于研究报告发布当时该行业的投资价值分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确行业投资评级；分析师在上述情况下暂停对该行业给予投资评级信息，投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

东方证券 ORIENT SECURITIES

免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

在任何情况下，本公司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，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

东方证券研究所

地址： 上海市中山南路 318 号东方国际金融广场 26 楼

联系人： 王骏飞

电话： 021-63325888*1131

传真： 021-63326786

网址： www.dfzq.com.cn

Email： wangjunfei@orientsec.com.cn