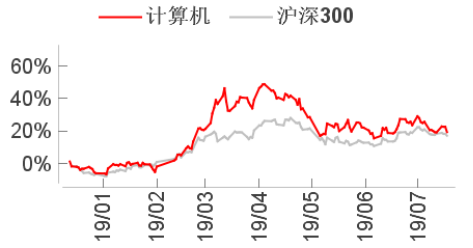
网络安全系列报告之一：态势感知——构建主动安全防御体系的智能大脑

东方证券 ORIENT SECURITIES

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	2019 年 12 月 12 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

证券分析师 游涓洋
010-66210783
youjuanyang@orientsec.com.cn
执业证书编号：S0860515080001

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

核心观点

- **当前安全体系正处于被动防御向主动防御过度阶段，态势感知是主动安全防御体系的智能大脑，类似于防火墙是被动防御体系中最重要的安全产品，态势感知将成为主动防御体系最核心的组成部分。**当前传统的被动防御已无法应对日益多样的新型威胁攻击，同时传统的安全管理也存在着安全数据缺乏分析、安全事件处置效率低下等诸多痛点，集检测、预警、响应处置功能为一体的态势感知成为了行业现实需要。态势感知的工作原理是对引起网络态势变化的安全要素信息进行获取、理解，评估整体网络安全的状况，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。
- **多项网络安全政策将态势感知建设列为重点任务，态势感知整体市场规模快速增长。**《网络安全法》以及等保 2.0 标准中都提及态势感知相关的建设内容，政策驱动叠加行业的现实需求使得态势感知保持快速增长。安全牛的数据统计，2017 年国内态势感知的市场规模为 20 亿元，预计 2020 年达到 50 亿元，CAGR 约为 35.7%，显著高于 2017-2019 年网络安全整体市场 22.3%的复合增速，预计整体安全市场的渗透率从 4.9%增长到 6.7%。
- **监管类行业态势感知已达到一定程度普及，能源、政府、教育等企业级市场呈现加速渗透趋势。**态势感知目标市场包括两种类型的客户：一是监管类行业客户，包括各级公安和各级网络安全和网信办等；二是关键信息基础设施保护类态势感知。由于监管类行业对于态势感知相关建设具有一定强制性且启动较早，因此渗透率较高，而企业级市场发展较监管类行业具有一定的滞后性，但由于市场基数大，实际需求高，建设热度正不断升高。截止目前，2019 年涉及态势感知的公开订单总数达到 526 个，其中标明态势感知建设具体金额的订单数量为 312 个，总金额达到 4.6 亿元。从订单数量分布情况看，能源行业涉及态势感知建设的订单数量最多，达到 142 个，占统计总订单数的 27%，其次为政府、教育、监管和医疗行业，订单数量分别达到 111 个、74 个、68 个和 54 个。
- **当前国内态势感知市场呈现“两超多强” 的竞争格局，行业特征利好优势企业拓展市场空间。**安恒信息和奇安信态势感知产品和市场的优势明显，处于国内态势感知市场的第一梯队，其他优势企业还包括深信服、启明星辰、绿盟科技、天融信等。技术和经验构成态势感知厂商的竞争壁垒，因此具有先发优势的态势感知厂商有望凭借不断积累的技术和经验提升自身的市场份额和品牌影响力

投资建议与投资标的

- 我们认为在态势感知市场快速发展的背景下，具有先发优势并能与其他产品线形成良好协同的安全厂商将最为受益，建议重点关注安恒信息(688023，未评级)、深信服(300454，增持)、启明星辰(002439，未评级)、绿盟科技(300369，未评级)、南洋股份(002212，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

深度报告

【行业·证券研究报告】

目 录

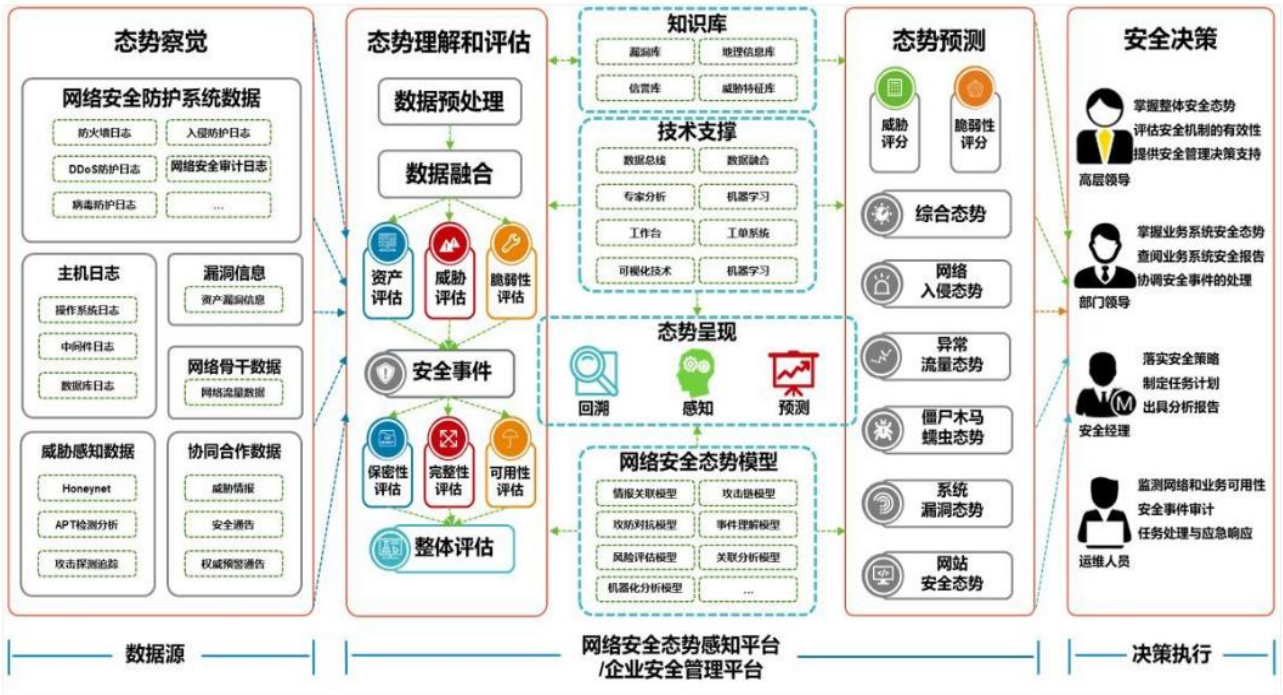
图表目录

一、态势感知是网络安全现实之所需、发展之所向

1.1 态势感知是主动防御时代最核心的网络安全平台

态势感知集检测、预警、响应处置功能为一体，是主动防御体系中的安全大脑。态势感知的概念最早由美国空军在 20 世纪 80 年代时提出，其最为广泛的定义是指“在一定的时空范围内认知和理解环境因素，并对未来的发展趋势进行预测”。随着互联网的迅猛发展，网络安全态势感知应运而生，其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。目前主流的态势感知产品支撑技术都是相近的，主要以全流量分析为核心，结合威胁情报、UEBA（用户实体行为分析）、机器学习、大数据关联分析等。**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。**

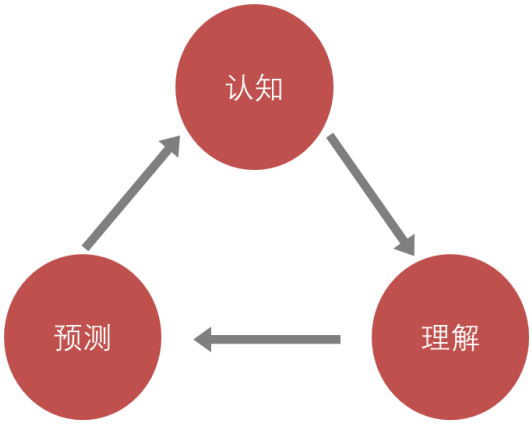
图 1：网络安全态势感知体系架构示例



数据来源：绿盟科技，东方证券研究所

态势要素的认知、理解和预测是网络安全态势感知的三个核心环节。网络安全态势感知的最终目标是对情境态势进行有效管理，不断针对网络攻击作出动态、积极的安全防御，以保障用户业务的正常运行。而实现态势感知，需要以安全大数据为基础，从全局视角来提升对各类安全威胁的发现识别、分析理解和响应处置，通常还以可视化的方式展现给用户。总体来说，态势感知主要包括态势认知、态势理解和态势预测三个环节。

图 2：网络安全态势感知的周期



数据来源：《网络安全态势感知提取、理解和预测》，东方证券研究所

1） 态势认知

态势认知是态势感知的前提，态势感知是通过各类检测工具，检测收集多层次多维度的影响系统安全性的数据。，从时间维度上看，不仅需要已有实时或准实时的数据，还需要通过更长时间的数据来分析一些异常行为，以发现一些多阶段的新型攻击方式，而从数据维度看，主要包含网络安全防护系统数据（如防火墙、WAF、IDS/IPS 等安全设备日志或告警等）、重要服务器及主机的数据（如服务器安全日志、进程调用和文件访问等）、网络骨干节点数据、协同合作数据（如第三方的威胁情报数据）、威胁感知数据以及资产脆弱性数据等。

图 3：态势感知采集的主要数据类型

数据来源：腾讯云+社区，东方证券研究所

2） 态势理解

态势理解是态势感知的核心，是在获取大量网络安全数据信息的基础上，通过解析信息之间的关联性，对其融合以获取当前的网络安全态势，通过评估定性或定量分析网络当前的安全状况和薄弱环节，并给出相应的应对措施。网络安全态势理解是从宏观的角度分析网络整体的安全状态，从而得到综合的安全评估，达到辅助决策的目的。

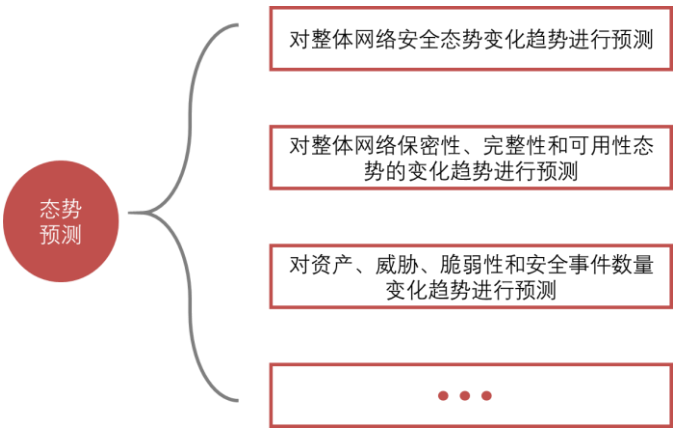
图 4：态势理解中态势评估框架举例

数据来源：腾讯云+社区，东方证券研究所

3） 态势预测

态势预测是根据网络安全态势的历史信息和当前状态，对网络未来安全状况的发展趋势进行预测，它是态势感知的基本目标。实现真正的主动防御需要安全预警技术，即通过已检测或分析到的报警信息来预测未来要发生的攻击行为，为组织的网络安全提供实时、动态、快速响应且主动的安全屏障。由于网络攻击的随机性和不确定性，使得网络安全态势变化是一个复杂的非线性过程，传统的预测模型方法已不适用，当前的研究主要朝智能预测方法发展。

图 5：黑客攻击逐渐向专业化和商业化转变



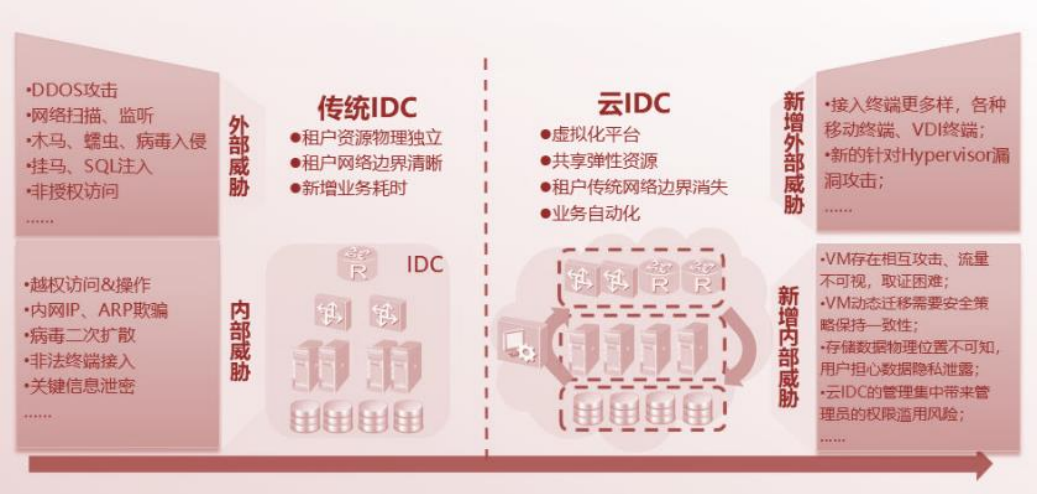
数据来源：腾讯云+社区，东方证券研究所

1.2 态势感知可有效应对新型的攻击威胁

新兴技术的落地应用使得传统网络安全边界消失，并带来新的安全风险。云计算、大数据、物联网等产业的快速发展催生出云安全、大数据安全等新兴安全领域，防护对象已由传统的 PC、服务器拓展至云平台、大数据和泛终端。以云计算为例，云计算使得 IT 基础架构发生根本性变化，企业

将其业务迁移到云端，租户传统网络边界消失，IT 基础资源集中在云端，因此遭受攻击后的影响和破坏性更大。相较于传统的 IT 架构，云计算还面临虚拟化安全、数据集中等新的安全问题。

图 6：云计算面临新的安全风险



数据来源：CSDN，东方证券研究所

黑客攻击逐渐向专业化和商业化转变。DT 时代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，引来黑客等恶意攻击者的觊觎，导致近年来数据泄露、敲诈勒索病毒等安全事件层出不穷。早期以极客为核心的黑客逐渐向组织化及专业化发展，攻击技术和手段更加高明，形成了以利益驱动的庞大黑客产业。黑客的“盈利方式”也变得多样，如售卖敏感信息直接变现、通过 DDos 攻击实现敲诈勒索或通过篡改信息改变资产所有权等，甚至提供 HaaS（攻击即服务）形式的服务，攻击者只需在线提交需求和付款，就能获得相应的云端攻击服务。这使得攻击者采取更加隐蔽的手段收集、窃取或者篡改信息，这要求企业或组织在发展新技术的同时需要快速辨别不利于自身安全的潜在威胁，保护自身免受网络攻击的危害。

图 7：黑客攻击逐渐向专业化和商业化转变

数据来源：安全牛，东方证券研究所

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，亟待构建新型防御体系。IDC 认为，未来 2 年 95%的大型企业计划增加使用云技术，这将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。这些威胁往往行动水平低而缓慢，通过若干个阶段和渠道躲避传统的被动防御手段，寻找到有漏洞的系统和敏感数据。

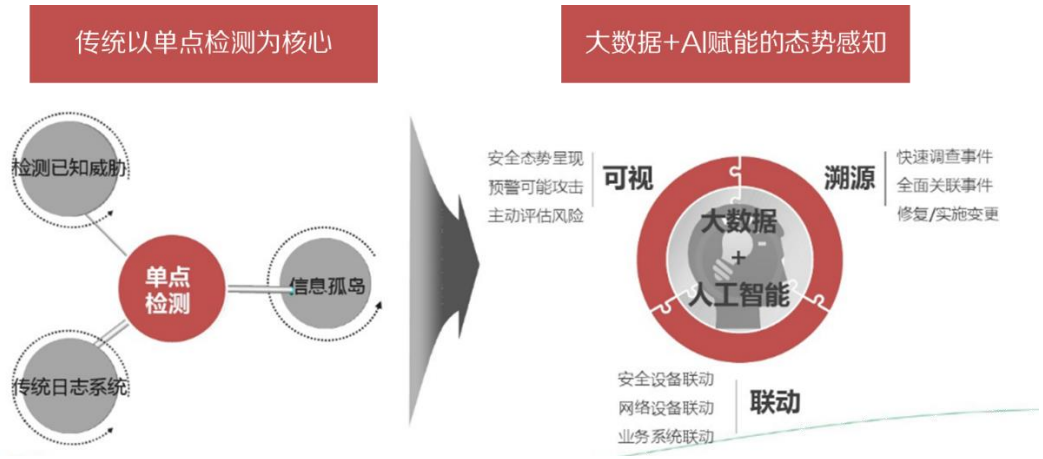
表 1：面对新一代安全威胁时传统单点防御的不足

传统防御产品	面对新一代安全威胁的不足
防火墙（FW）	防火墙通过过滤机制制定访问控制策略，允许通用的 httpWeb 流量，它可以拦截低层攻击行为，但对应用层的深层攻击行为无能为力
下一代防火墙（NGFW）	下一代防火墙（NGFW）增加了基于用户和应用的策略规则，但没有增加可以检测新一代安全威胁的内容或行为的动态保护
入侵检测/防御（IDS/IPS）	基于特征/签名检测机制无法检测出一个零日漏洞利用的任何异常，尤其是当恶意代码严重伪装或者分段投送时
防病毒（AV）	由于新一代威胁中的恶意软件及其利用的漏洞是未知的，若访问的网站声誉“清白”，传统的防病毒网关和 Web 过滤器会允许通过
反垃圾邮件	伪造的钓鱼网站使用不断变化的域名和网址，所以黑名单要滞后于攻击活动，而关闭一个钓鱼网站的平均时间超过 26 小时
Web 过滤	多数出站过滤器阻止含有不良信息的网站，仅不到四分之一的企业限制社交网站，另外，动态 URL、被黑的合法网站以及短期活跃的地址等会使静态 URL 黑名单失效
数据防泄漏（DLP）	DLP 工具主要针对身份证等个人信息，对于检测凭证或者知识产权的外泄来说过于粗略和繁琐。而回连通道的加密将使得数据泄露无法发现，其静态的方法与新一代威胁的动态属性不相匹配。

数据来源：知道创宇，东方证券研究所

主动防御体系成为发展趋势，态势感知可以有效防御新型攻击威胁。传统通过购买更多安全设备的被动防御策略已无法适应当前的网络安全形势，需要进一步提升安全运营水平的同时积极开展主动防御的建设。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、预警和预测将越来越准确，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。作为主动防御体系的安全大脑，大数据分析、人工智能等新兴技术赋予态势感知基于非特征检测技术的能力，通过各类安全设备的联动，以及持续监测、事件响应、深度分析以及预示预警，最终达到有效检测和防御新型安全威胁的目的。

图 8：大数据及 AI 赋能态势感知

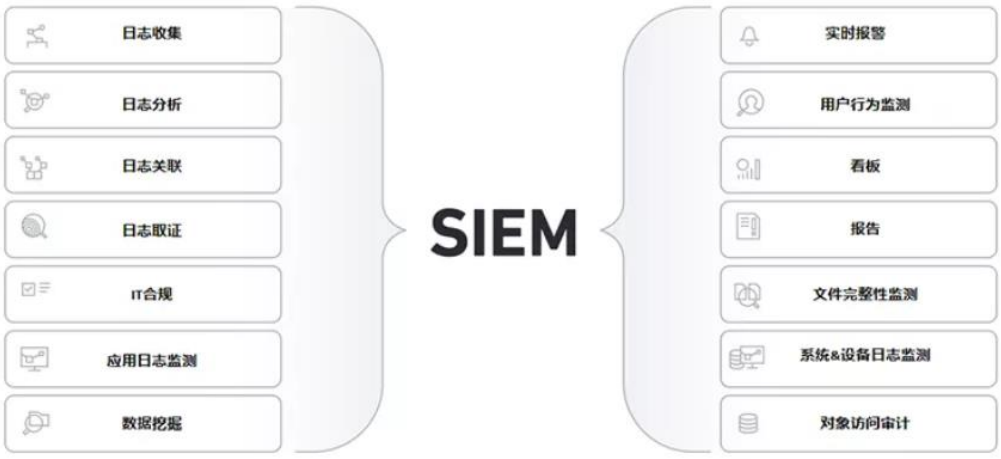


数据来源：华为，东方证券研究所

1.3 态势感知是 SOC/SIEM 能力的升级和进化

SOC/SIEM 等安全管理工具为态势感知提供基础支撑，涉及态势感知的认知和理解环节。SIEM（安全信息和事件管理）收集和聚合从主机系统到网络和安全设备生成的日志数据，识别、分类和分析产生的事件，提供安全事件的报告并并对潜在的安全问题作出警报，它解决了基于安全日志和系统运行日志的源头分散、难以统一分析的问题。SOC（安全运营中心）则是以 SIEM 为核心，是协助管理员进行事件及风险分析、预警管理及应急响应的集中式安全管理系统。通过 SIEM/SOC 对各安全环节的日志及系统相关的日志实现汇聚分析，并形成对安全环节的统一管理能力，这是态势感知必备的基础能力。

图 9：SIEM（安全信息和事件管理）的功能



数据来源：青藤云安全资讯，东方证券研究所

当前安全管理的过程存在诸多痛点。SOC/SIEM 作为一个复杂的实时响应系统，除了自身的技术能力，真正发挥作用还需要安全人员和运营流程的配合。然而当前安全人员严重匮乏，2018 年网络安全人力资源研究（ISC）的数据显示，全球网络安全人才缺口扩大至近 300 万，其中亚洲地区

的缺口达到了 214 万，63%的受访企业认为企业存在网络安全人员短缺的情况，这将严重制约 SOC/SIEM 能力的发挥和普及。此外，由于数据分析能力欠缺以及安全规划薄弱等因素，现实的安全管理存在诸多不足：

1）**海量安全数据缺少分析：**IDC 预测 2022 年各类开发的应用的数量将达到 5 亿款，相当于过去 40 年的总合，这一方面导致 IT 系统面临暴露的风险不断加剧，另一方将产生海量的安全数据。而 SOC/SIEM 对于得到的海量安全数据，缺乏内在的关联分析和数据挖掘，将影响安全事件的及时发现和处置；

2）**多种安全设备单独管理：**部分企业或组织在安全设备部署时缺乏统一规划和统一管控，导致一些安全事件发生时不能及时响应；

3）**安全事件处置效率低：**面对海量的安全日志和告警，通过人员来分析和处理的能力有限，导致事件处置的效率较低，可能会忽视真正的安全威胁。

图 10：当前安全管理存在诸多痛点

数据来源：华为，东方证券研究所

态势感知为用户提供预测、保护、检测和响应闭环能力的安全管理。态势感知的实现一方面要发挥 SIEM 的日志整合分析和检索能力以及 SOC 的统一管理能力，另一方面要进一步推动基础能力的改进和重构，在 SIEM/SOC 的基础上，依托于大数据分析、AI 等新兴技术，强化态势感知的自动化认知、理解和预测能力，减少对安全人员的依赖。在掌握整体安全情况的同时定向发现潜伏的安全威胁，并提供清晰明确的响应决策信息支撑、有效指挥对威胁行为体开展对抗，做到及时防御攻击、自我恢复甚至实施反制。

图 11：网络安全管理的发展方向

数据来源：IDC，东方证券研究所

二、政策扶持加码，态势感知市场前景广阔

2.1 政策密集出台，行业进入快速成长期

多项网络安全政策将态势感知建设列为重点任务。习近平主席在 2016 年网络安全和信息化工作座谈会上提出“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力”，态势感知迎来了一波建设热潮。同时态势感知建设也被列入了“十三五”国家信息化规划。随后，《网络安全法》以及等保 2.0 标准中都提及态势感知相关的建设内容。另外，由中国信通院牵头，腾讯、华为、安恒信息等企业参与编写的《面向云计算的安全解决方案 第一部分：态势感知平台》标准于 2019 年可信云大会上发布，成为国内首个面向云计算的安全态势感知平台标准，这有利于规范云计算环境下的态势感知系统建设，促进态势感知市场的良性发展。

表 2：态势感知相关的政策、会议及标准

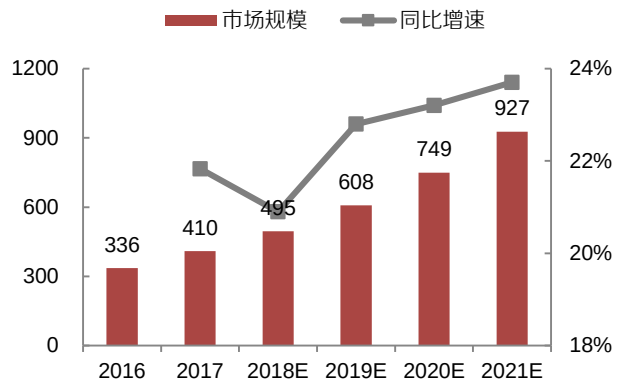
时间	部门	政策/会议名称	相关内容
2015.5	公安部	北京电视电话会议	提出各级公安机关要充分认识网络安全的严峻形势和加强网络安全工作的重要性、紧迫性，加强国家网络安全通报机制建设，进一步健全完善网络安全信息通报和监测预警机制建设，确保网络安全执法检查工作取得实效
2016.4	中央网络安全和信息化领导小组等	网络安全和信息化工作座谈会	**提出要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力**
2016.11	全国人民代表大会常务委员会	《中华人民共和国网络安全法》	国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监

			测预警信息。
2016.12	国务院	《“十三五”国家信息化规划的通知》（国发[2016]73号）	提出要全天候全方位感知网络安全态势，加强网络安全态势感知、监测预警和应急处置能力建设
2017.2	中央国家安全委员会	国家安全工作座谈会	提出要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护
2017.7	国家互联网信息办公室发布	《关键信息基础设施安全保护条例（征求意见稿）》	第六章“监测预警、应急处置和检测评估”中，对网络安全检测预警和信息通报提出了明确要求：国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度;国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度
2017.12	工信部	《工业控制系统 信息安全行动计 划（2018-2020年）》	到 2020 年，全系统工控安全管理工作体系基本建 立，全社会工控安全意识明显增强。建成全国在 线监测网络，应急资源库，仿真测试、信息共享、 信息通报平台（一网一库三平台），态势感知、安 全防护、应急处置能力显著提升。
2018.6	公安部	《网络安全等级保护条例(征求意见稿)》	相比信息系统安全等级保护 1.0，增加了安全检测、通报预警、应急处置、**态势感知**、能力建设的要求
2019.5	国家标委会	《网络安全等级保护制度 2.0 标准》	要求依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、**态势感知**、能力建设、监督检查、技术检测、安全可控、队伍建设、教育培训和经费保障等工作
2019.7	中国信通院等	《云计算安全解决方案第一部分，态势感知平台标准》	国内首个面向云计算的安全态势感知平台标准，旨在规范云计算环境下的态势感知系统建设，帮助企业掌握云计算环境态势，提高企业网络安全防护、安全运营等方面的能力。标准规定了面向云计算的安全态势感知平台的能力要求，包括三部分：一是平台总体功能框架;二是平台建设原则;三是平台各组成部分的能力要求

数据来源：政府网站，中国信通院，东方证券研究所

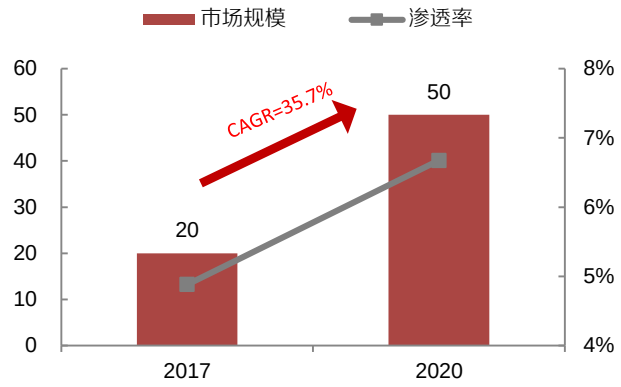
态势感知市场规模增长迅速，快于同期网络安全整体市场增速。根据赛迪顾问《中国网络安全发展白皮书（2019）》报告，2018 年，我国网络信息安全行业的市场规模达到了 495.2 亿元，同比增长 20.9%，预计 2021 年市场规模超过 900 亿元。而根据安全牛的数据统计，2017 年国内态势感知（定义为围绕安全运营中心(SOC)，并基于日志管理(SIEM)、大数据平台、威胁情报、关联分析、沙箱等等关键技术和多维度数据，为用户提供预测、保护、检测和响应闭环能力的安全系统）的市场规模约为 20 亿元，预计 2020 年达到 50 亿元，CAGR 约为 35.7%，显著高于 2017-2019 年网络安全整体市场 22.3%的复合增速，预计态势感知占整体安全市场的渗透率将从 4.9%增长到 6.7%。当前我们已经逐步迈进主动防御时代，随着等保 2.0 等政策的落地实施，整体网络安全市场将继续保持较高增速市场。**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，因此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 12：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

图 13：我国态势感知市场规模及渗透率（亿元，%）

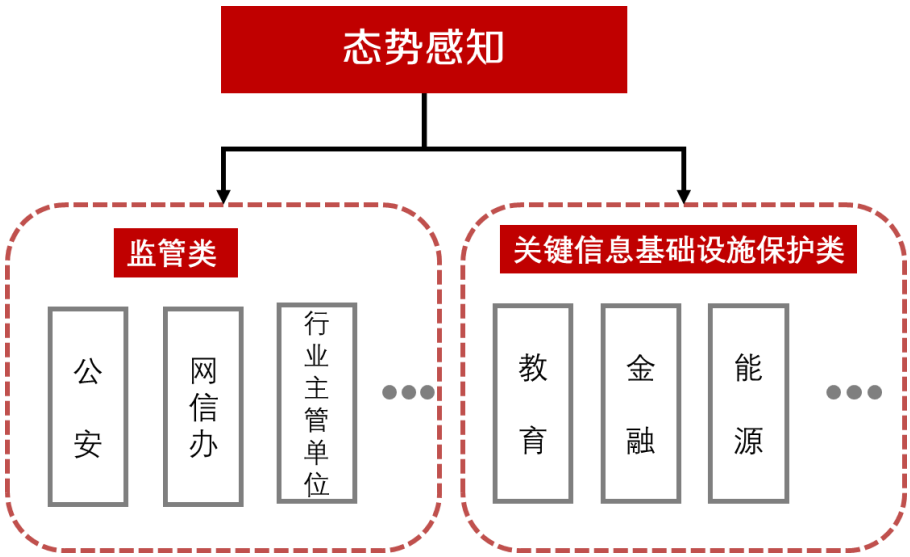


数据来源：安全牛，东方证券研究所

2.2 监管类行业已达到一定程度普及，能源、政府、教育等企业级市场加速渗透

当前态势感知平台的目标市场包括两种类型的客户：第一类是监管类行业态势感知平台，主要用于区域城市或者行业的监管，客户包括各级公安和各级网络安全和信息化委员会办公室（网信办）、各行业主管部门等；第二类是关键信息基础设施保护类态势感知，主要用于自身信息系统的安全防护，客户包括教育、金融、能源等行业的企业客户以及各级部委和政府用户等。

图 14：态势感知下游客户分类



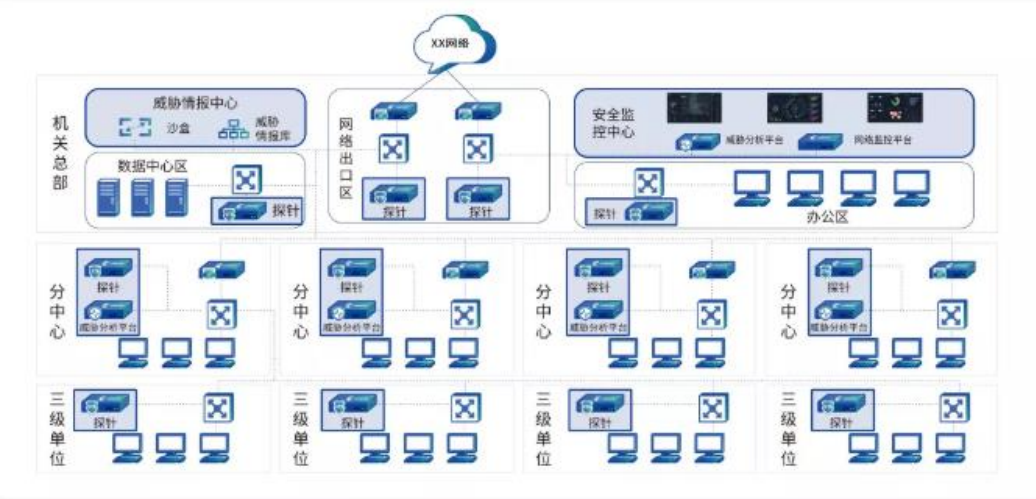
数据来源：安恒信息，东方证券研究所

监管类行业对于态势感知建设具有一定强制性。监管行业在构建态势感知平台时注重掌握全网或所监管行业的网络安全状态，涉及威胁告警、攻击态势以及定位安全事件。在 2017 年正式实施的《网络安全法》要求国家网信部门及负责关键信息基础设施安全保护工作的部门加强安全监测预

警等内容的建设。而网络安全信息收集、分析、网络安全监测预警等功能正是态势感知平台的长处之所在，所以《网络安全法》的出台增加了相关部门对于态势感知建设的强制性需求。

态势感知在公安行业起步较早且逐步普及。公安行业的需求主体包括部级部门 1 个，省级部门 34 个，地市级部门 293 个，目前行业态势感知主要提供商为安恒信息和奇安信两家公司，仅从安恒信息看，截止 2019 年 10 月公司态势感知产品在公安行业累积成交合同约 120 例，包含十多个省级平台以及近百个地市级平台，已达到一定的普及率。

图 15：态势感知平台部署拓扑模型



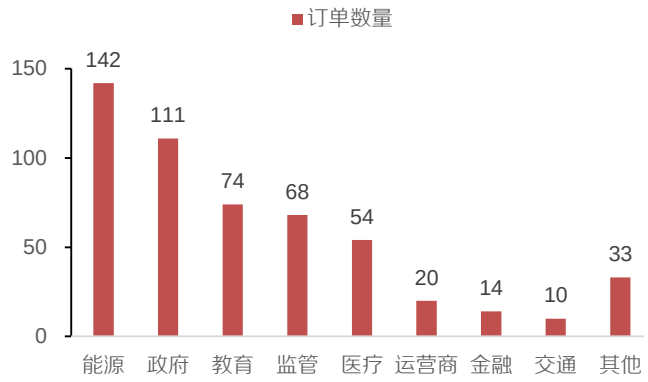
数据来源：深信服，东方证券研究所

对于关键信息基础设施保护类态势感知市场，产品定制化程度较高，这是由于不同行业客户对于态势感知产品的要求各有侧重：1）**政府机构**关注对外部攻击的防范，注重高级威胁检测和自身的威胁感知等能力；2）**能源行业**包含海量的智能终端，关系国家经济命脉及生产安全，更注重产品的兼容性以保障生产运营的可持续性；3）**金融行业**业务场景众多，需求重点在于产品的关联分析能力、威胁告警精确度以及用户行为分析能力等；4）**教育行业及医疗行业**核心业务系统繁多，涉及海量的敏感数据，因此更加关注产品的安全防护及威胁检测效果，防止敏感数据的泄露。

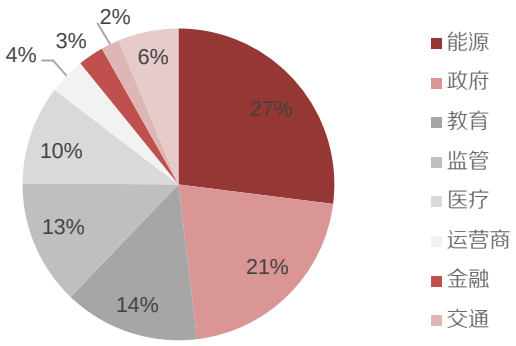
能源、政府以及教育行业态势感知建设景气度高。截止目前，2019 年涉及态势感知的公开订单总数达到 526 个，其中标明态势感知建设具体金额的订单数量为 312 个，总金额达到 4.6 亿元。从订单数量行业分布情况看，能源行业涉及态势感知建设的订单数量最多，达到 142 个，占统计总订单数的 27%，其次为政府及教育行业，订单数量分别达到 111 个和 74 个，数量占比分别为 21%和 14%。尽管态势感知在监管类行业已有一定的渗透率，但由于监管类市场巨大，涉及公安、网信以及各行业的主管部门，加上已建设平台的更新和扩容，仍呈现较高的需求景气度，订单数量达到 68 个，数量占比为 13%。

图 16：2019 年至今各行业态势感知订单数量分布情况

图 17：2019 年至今各行业态势感知订单数量占比情况



数据来源：招标采购导航网，东方证券研究所



数据来源：招标采购导航网，东方证券研究所

三、竞争格局呈现“两超多强”，行业特征利好优势企业

3.1 安恒信息和奇安信处于态势感知市场的第一梯队

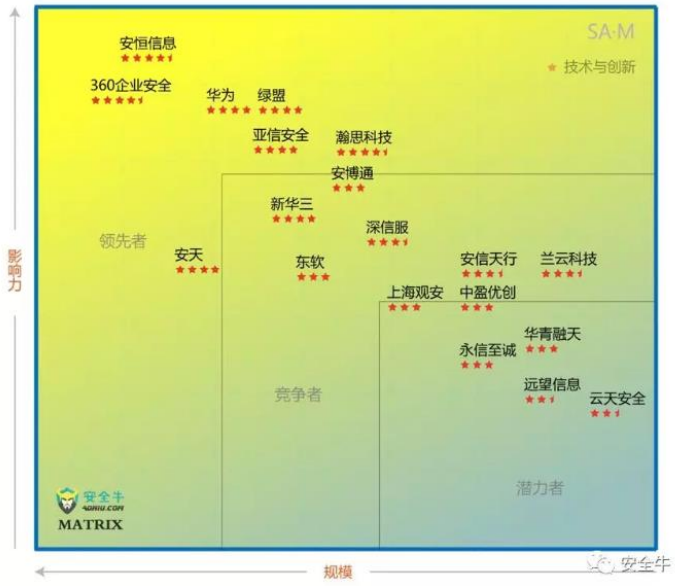
针对国内态势感知市场，安全牛和 IDC 分别给出了态势感知产品矩阵以及中国态势感知解决方案市场 2019 年厂商评估图：

1） 态势感知矩阵（安全牛，2018）

根据厂商的影响力、规模和技术创新力三个指标，态势感知矩阵可划分为领先者、竞争者和潜力者三个矩阵区。入选态势感知矩阵的厂商共 19 家，其中安恒信息、奇安信（原 360 企业安全）综合优势较为明显，它们与华为、绿盟科技等厂商处于领先者梯队，深信服、新华三、东软等厂商处于竞争者梯队，上海观安、华青融天等新兴安全厂商处于潜力者梯队。由于影响力、规模和技术创新力三个细分指标之间并非完全独立，三者是相辅相成的关系，所以处于领先者梯队的厂商通常在三个指标上均占优：

- **影响力**，主要考虑厂商品牌知名度、业界口碑以及市场地位等因素。单从该指标看，排名靠前的厂商均为知名的大型安全厂商，其中安恒信息处于第一梯队，奇安信、华为、绿盟科技处于第二梯队；
- **规模，**主要考虑厂商相关产品的营业收入、人员数量以及利润等因素。单从该指标看，奇安信和安恒信息领先于其他厂商，其中奇安信规模略大于安恒信息，上海观安等新兴安全厂商规模较小；
- **技术创新力，**主要考虑厂商的研发投入、产品化能力以及技术定位等因素。单从该指标看，安恒信息、奇安信以及瀚思科技处于领先位置，绿盟科技、华为等公司处于梯队。

图 18：2018 年安全牛发布的态势感知矩阵

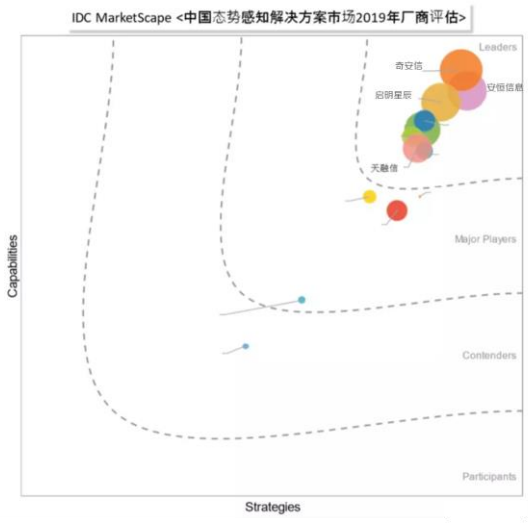


数据来源：安全牛，东方证券研究所

2） 中国态势感知解决方案市场厂商评估（IDC,2019）

IDC 发布的《中国态势感知解决方案市场 2019 年厂商评估》报告中，根据收入规模、产品技术能力、行业和客户拓展、生态系统建设以及未来发展战略等指标，将国内态势感知解决方案市场划分为领导者、主要厂商、竞争者和参与者四个象限。国内入选厂商共有 13 家，分别是安恒信息、奇安信、深信服、启明星辰、绿盟科技、天融信、新华三、华为、腾讯云、亚信安全、盛邦安全、兰云科技、盛华安。其中安恒信息与奇安信两家厂商竞争优势明显，在领导者象限排名靠前。

图 19：中国态势感知解决方案市场 MarketScape 象限图



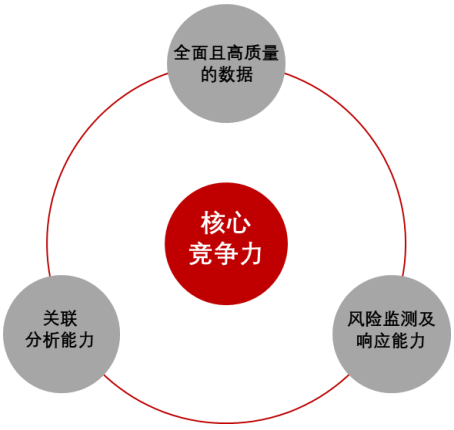
数据来源：IDC，东方证券研究所

综合来看，国内态势感知市场呈现“两超多强” 的竞争格局。安恒信息、奇安信处于国内态势感知市场的第一梯队，包揽两份榜单中的前二位置，绿盟科技、深信服、天融信、华为、新华三、亚信安全等安全厂商是目前态势感知市场的主要厂商。

3.2 态势感知市场特征利于优势企业拓展市场空间

态势感知产品的核心竞争力体现在全面且高质量的数据、关联分析能力以及风险监测及响应能力三个方面。全面高质量的数据是高质量数据分析的基础，主要涉及到态势感知认知环节中流量采集、日志采集等产品的能力。全面且高质量的数据获取一方面需要采集到各类的数据，如各类设备日志、重要节点流量、资产信息等，减少漏报和误报，另一方面需要对数据做好预处理，提高数据的质量。关联分析能力以及风险监测及响应能力涉及态势感知的理解环节，是态势感知发挥效用的关键。由于现阶段的网络攻击发生速度极快，高水平威胁行为体在长期潜伏后突然的攻击行为很难做到事前或事中预警及响应，因此需要结合厂商在长期的网络对抗中积累的经验知识，丰富和完善关联规则，实现对越来越多“已知”攻击行动的识别、预警和响应。

图 20：态势感知产品的核心竞争力



数据来源：安全牛，东方证券研究所

态势感知的建设与基础安全产品销售具有良好的协同作用。当前安全防御体系的建设已由“单一防护”及“补丁”模式发展到“系统规划、整体协防”模式，态势感知平台仅定位于“安全大脑”，完整的防护能力还需要布置众多的基础安全产品。当前态势感知市场的优势厂商一般都拥有各类基础的安全产品，如防火墙、安全网关等，但这些传统安全产品往往同质化严重，为公司贡献的营收增量有限。态势感知领域的优势厂商可以通过态势感知的建设带动传统基础安全产品的销售，收入增长中枢有望实现进一步上移。

技术和经验构成态势感知厂商的竞争壁垒，优势厂商有望继续扩大竞争优势。尽管态势感知产品的定制化程度较高，但不同行业的态势感知平台在技术架构以及核心技术存在共性，均需要数据的融合、大数据的分析，高效的感知发现、快速的响应处置等技术做基础支撑，因此从监管类行业向其他行业拓展的门槛不高。另一方面，态势感知真正实现还需要结合实时的数据采集、中长期的情报、经验和知识积累，以支撑短期相应和中长期防护策略的调整。因此，态势感知整体市场马太效应凸显，在态势感知向各行各业加速渗透的背景下，具备技术和经验优势的态势感知厂商有望提升自身的市场份额和品牌影响力。

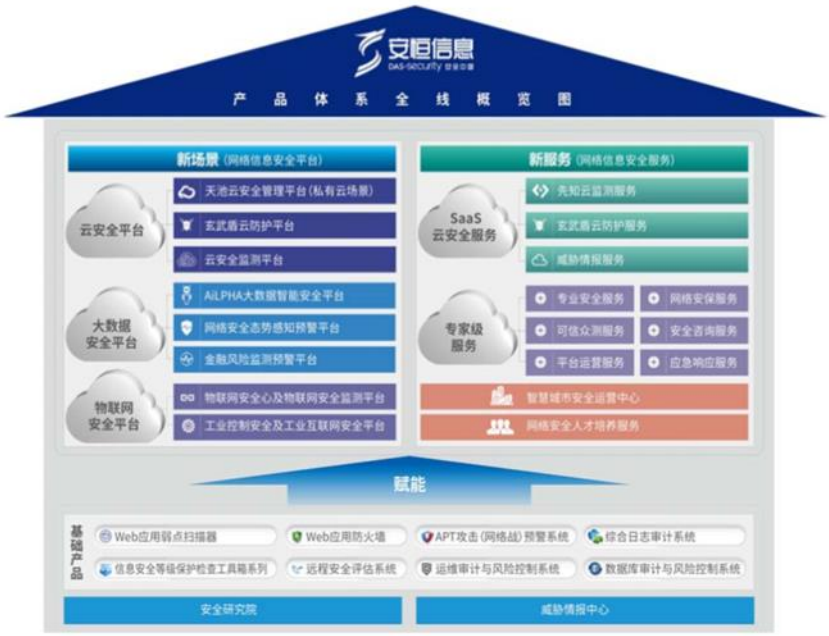
四、投资建议

当前安全体系正处于被动防御向主动防御过度阶段，态势感知是主动安全防御体系的智能大脑，类似于防火墙是被动防御体系中最重要的安全产品，态势感知将成为主动防御体系最核心的组成部分。监管类态势感知渗透率已达到一定水平，能源、教育、医疗等行业市场处于加速渗透状态。另外，随着客户 IT 架构或需求变化，以及外部网络攻击手段的进化，已部署的态势感知也有不断的扩容和更新需求，整体态势感知的市场规模将实现快速增长。我们认为在态势感知领域具有先发优势并能与其他产品线形成良好协同的安全厂商将最为受益，安恒信息(688023，未评级)、深信服(300454，增持)、启明星辰(002439，未评级)、绿盟科技(300369，未评级)、南洋股份(002212，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

安恒信息自设立以来一直专注于网络信息安全领域，是当前国内态势感知市场的龙头企业。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。

图 21：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，2017 年度国内市占率达到 16.7%，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等产品市场份额也均位于国内市场前列。

表 3：安恒信息基础安全产品市占率情况

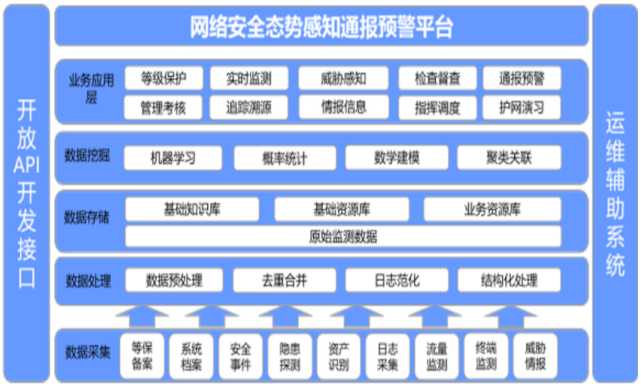
产品名称	市场份额及排名
Web 应用防火墙	2017 年度市场份额为 16.7%，排名第二
数据库审计与风险控制系统	2017 年度市场份额为 7.2%，排名第二
运维审计与风险控制系统	2016 年度市场份额为 14.5%，排名第三
Web 应用弱点扫描器、远程安全评估系统	2017 年度市场份额为 14.7%，排名第三
日志审计系统	2017 年度市场份额为 10.9%，排名第一

数据来源：安恒信息招股书，东方证券研究所

公司态势感知优势明显，实战能力突出。公司在日志审计、数据库审计、流量分析、大数据分析等方面积累的优势赋予了公司态势感知平台突出的数据汇聚以及威胁发现能力。公司深耕态势感知领域多年，具有丰富的行业实践，其态势感知产品落地案例累计超过 200 个，其中公安行业 120+、行业主管单位 20+，政企单位 60+。产品具备强大的实战能力，已协助全国各地公安发现安全事件 1000+起，成功追溯打击案件 50+起，累计抓捕黑客近百人。公司通过不断在不同行业拓展深入，逐渐形成面向不同用户，切合用户多样化安全管理需求的多样化态势感知产品，持续提升自身的竞争优势。

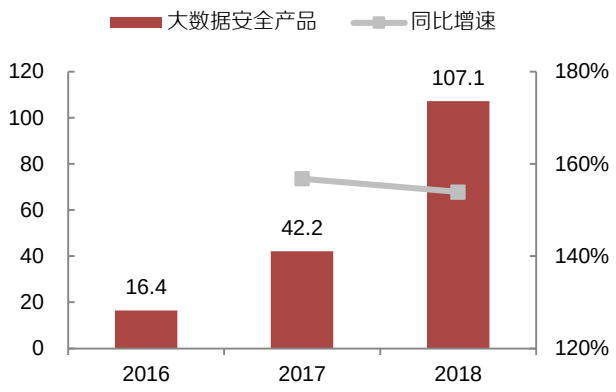
公司依托态势感知技术布局新兴安全领域。态势感知已成为公司的战略重点，依托态势感知技术公司推出了多款平台类产品，包括网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等，布局大数据安全等新兴安全领域，并赋能智慧城市安全运营中心业务。凭借领先的技术实力和丰富的实施经验，公司新兴安全业务增长迅速，其中 2018 年大数据安全产品营收规模达到 1.07 亿，同比增长 154%，有望继续保持高速增长。

图 22：安恒信息网络安全态势感知预警平台



数据来源：安恒信息招股书，东方证券研究所

图 23：安恒信息大数据安全产品营收及同比增速（百万，%）



数据来源：安恒信息招股书，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

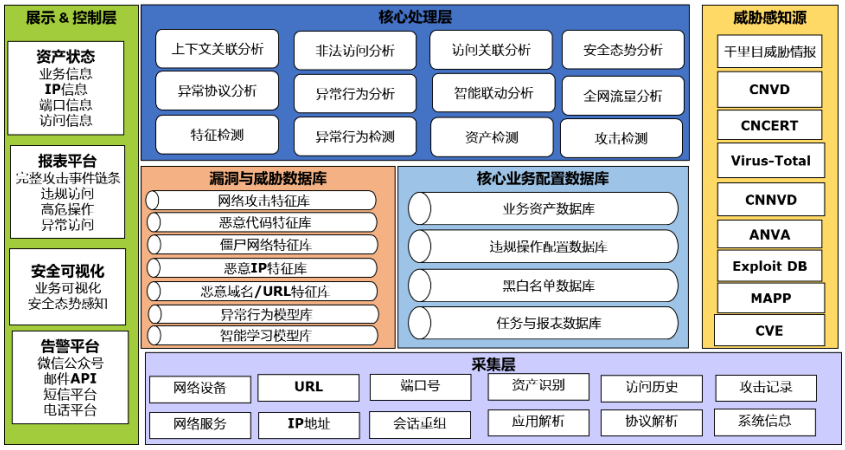
深信服的主营业务主要包括安全业务、云计算业务、企业级无线业务。安全业务品类丰富，上网行为管理、VPN、防火墙、广域网优化、应用交付等多款产品依靠显著的技术优势，市占率常年保持行业领先。云计算业务主要以超融合为核心，提供企业云、桌面云等产品。其中公司超融合市占率不断提升，从 2016 年的 7.3%上升到 2018 年的 15.5%。企业级无线业务主要由子公司信锐网科经营，产品包括无线控制器、无线接入点等。依托强大的研发和渠道能力，公司市场竞争力不断提升。

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

深信服态势感知技术创新及交付能力突出，产品营收增长迅速。公司同样进入了 IDC 中国态势感知解决方案领导者象限，其安全感知平台（SIP）在 IDC 创新技术能力指标获得满分。SIP 具有优异的产品架构，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。SIP 能够为用户提供超过 30 项标准化交付服务，依托公司自身强大的服务和渠道能力，项目最快可在 48 小时内交付。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：深信服态势感知平台架构



数据来源：深信服，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。

态势感知为公司安全运营赋能。公司智慧城市安全运营、工业互联网安全、云安全三大战略新业务进展顺利，2018 年公司三大新业务实现销售约 4 亿元，确认收入超过 2 亿元，其中智慧城市安全运营方面，公司已在成都、济南、青岛等 20 个城市开展相关业务，2019 年计划建设数量累计达到 35 个以上。公司提供的态势感知服务以运营中心的“安全智能+专家智慧”为依托，结合本地化有效情报数据，提供网络空间威胁感知、情境感知及关键信息基础设施安全防护，提升城市安全运营效能。

图 26：启明星辰泰合网络安全态势感知平台

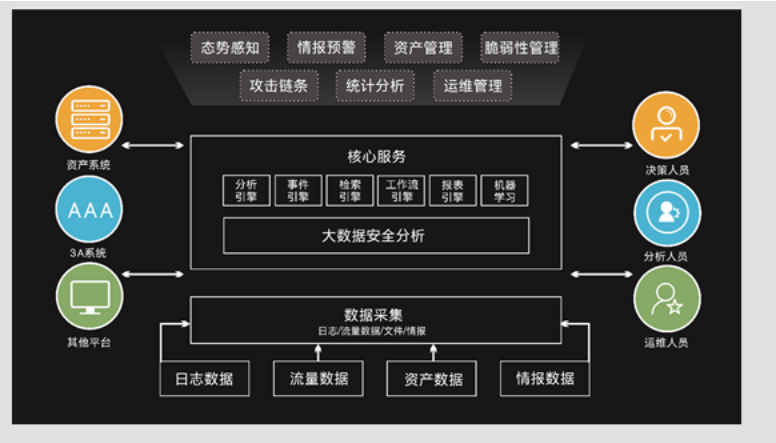
数据来源：启明星辰，东方证券研究所

4.4 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 年第三季度公司实现收入 3.44 亿，同比增长 38.3%，归母净利润为 0.32 亿，同比增长 88.2%，收入及业绩均明显改善。

图 27：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

绿盟科技依托态势感知助力等保 2.0 建设。等保 2.0 框架以“一个中心，三重防护”为指导思想，强调“主动防御、动态防御、整体防控和精准防护”。针对医疗、教育、政府、企业等中小客户，绿盟科技等级保护旗舰版解决方案以绿盟态势感知平台 ESP-H 和等保一体机为核心组件，协助客户建立一套“合规、安全、精简”的等级保护安全体系，满足等保合规需求。其中态势感知平台 ESP-H 集安全态势感知与预警、威胁检测与响应、漏洞发现与管理、日志收集与审计等全面的安全管理能力于一体，支持软硬一体化的形态，部署快捷，维护简单。

图 28：绿盟科技依托态势感知平台构建等保 2.0 防御体系

数据来源：绿盟科技，东方证券研究所

4.5 南洋股份：电信网科入股，持续拓展网络安全市场

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。其中天融信具有多款市占率领先的细分产品，IDC 报告显示，2018 年天融信在防火墙硬件以 22.4%的市场占有率排名第一；在入侵防御硬件市场、VPN 硬件市场中的市场占有率分别为 11.1%和 7.2%，分别位列第四和第三。2019 年 11 月，电科网信入股成为公司第三大股东，有望为公司的业务拓展产生更加积极的变化。

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

天融信以自身全面的网络安全产品体系为基础提供态势感知解决方案。天融信态势感知方案由平台、探针、威胁情报及安全服务综合组成，提供资产探测、脆弱性发现、威胁检测、行为审计等自有探针，同时能够开放性的融合用户已有多源异构探针形成全面的综合方案。公司态势感知的优势

在于多年来积累的大数据建模分析技术。面对复杂多变的网络形势，天融信的态势感知产品不断创新，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

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，若等级保护 2.0 等多项标准或政策落地或实施强度不及预期，态势感知需求也将降低。

市场竞争加剧的风险：若态势感知市场参与者增多，导致行业竞争激烈，不利于市场的良性发展。

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