IDC MarketScape

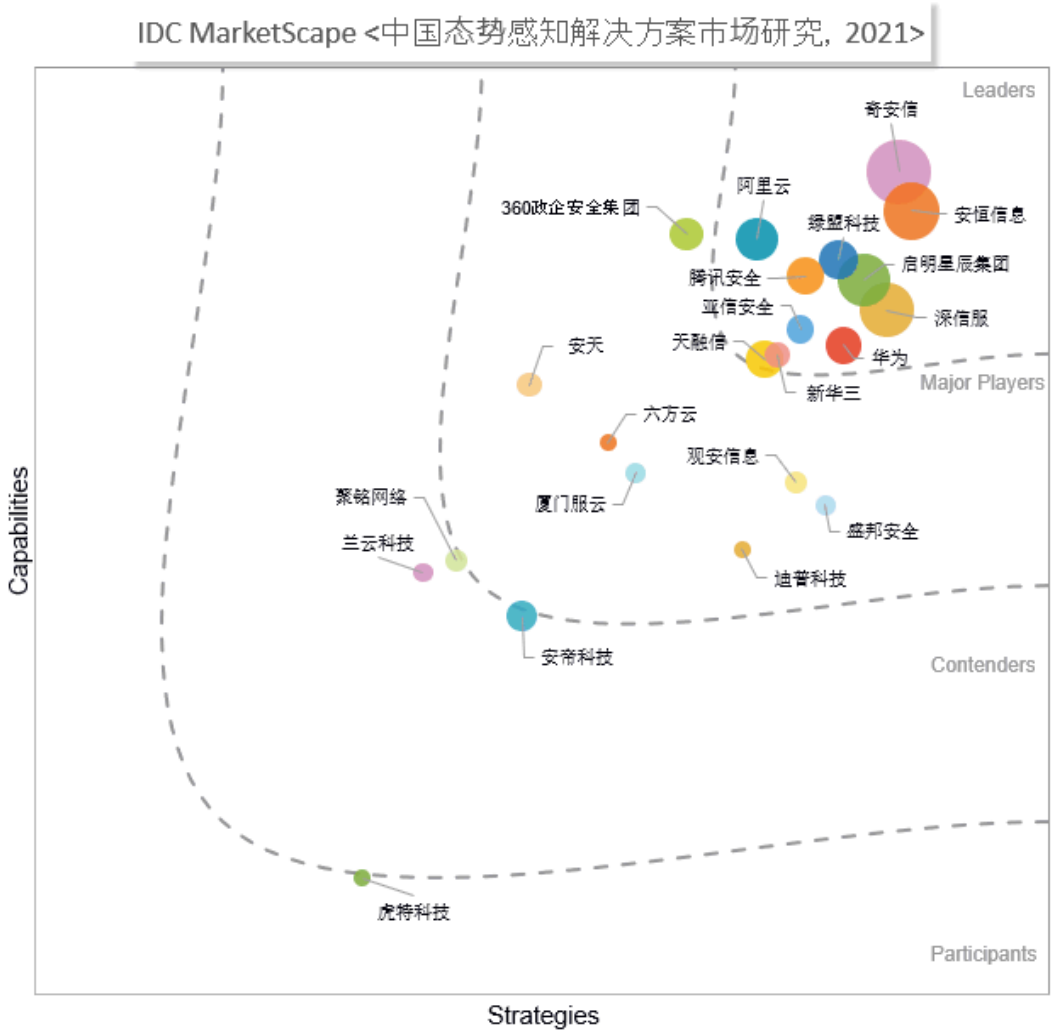
IDC MarketScape: 中国态势感知解决方案市场 2021，厂商评估

Austin Zhao

IDC MARKETSCAPE 图

图 1

IDC MarketScape：中国态势感知解决方案市场 2021，厂商评估



请参照附录的详细研究方法，市场定义和评分标准。

来源: IDC, 2021

November 2021, IDC #CHC47542121

IDC 观点

2021 年 9 月 1 日起，我国又一部网络安全重要法律条例《关键信息基础设施安全保护条例》正式实施，该条例中明确要求“保护工作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制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。”再次彰显了网络安全态势感知在整体网络安全防护体系中的重要作用。IDC 认为，全球范围频繁发生的网络攻击事件使得广大企业级客户清晰认识到网络安全对企业数字化转型的重要保障意义。同时，伴随着我国相关部门对网络安全日益严格和完善的监管制度的实施，已经有越来越多的企业正在改变原有相对孤立和被动的安全防护手段，通过统一的安全管理平台或态势感知解决方案将企业网络中各个安全组件和安全产品连通协作，力争打造协同作战、主动防御的安全架构，成为众多企业打造整体网络安全防御体系的首选。

2019 年，IDC 曾经发布《IDC MarketScape：中国态势感知解决方案市场 2019 年厂商评估》（IDC #CHC44880419）并得到市场的广泛关注。经过 2 年的市场发展，企业级客户对网络安全态势感知解决方案的建设目的和要求日趋成熟，安全产品和服务提供商的相关技术和产品也得到了持续打磨和快速迭代，同时，市场上也涌现出更多提供态势感知解决方案的专业安全厂商。为了进一步梳理和展现我国态势感知解决方案市场的现状和发展趋势，IDC 再次针对该市场进行了全面的调研，并输出本次报告。

IDC 认为，“网络安全分析、情报、响应、编排”（AIRO）是一套全面的解决方案，能够帮助企业衡量、解释和改善安全风险状况，在中国市场与之对应的便是态势感知解决方案，而网络安全态势感知平台则成为该方案的最终表现形态。在本次报告调研过程中，IDC 深入访谈了超过 20 家国内网络安全产品和服务提供商，并细致了解了其态势感知解决方案的技术特点和项目应用情况。

- 安全信息全面、实时的获取和分析是实现态势感知的关键。当前国内主要态势感知解决方案提供商已经通过自动化或半自动化的技术手段实现了网络设备信息、安全设备信息以及网络流量威胁分析数据的有效获取，并结合丰富的威胁情报信息进行威胁事件关联分析和溯源。同时，终端安全信息也正在越来越广泛地融入到态势感知的基础数据，显著提升了对恶意威胁的发现能力和分析颗粒度。
- 自动化编排与响应能力成为态势感知解决方案提供商能力差距的重要体现。为了满足企业级客户对态势感知平台的基本功能需求，国内主要态势感知解决方案提供商已经解决了“网络安全分析、情报、响应、编排”功能的有无问题，但通过功能所展现出来的技术实力和经验积累仍然存在差异。除了威胁检测这一核心能力，对威胁事件的编排与响应成为厂商重点发展的能力。同时，态势感知的编排与响应能力不应仅仅局限于设备一键阻断、添加黑白名单等简单操作，而是更多的与企业真实业务结合，制定规范化、流程化、协作化的高价值安全能力。
- 态势感知平台与其他安全产品的对接仍然缺乏统一接口。虽然目前已经有部分厂商正在努力通过“能力中台化”、开放式应用程序编程接口（API）等方式提升自身态势感知平台与第三方产品对接的标准化水平，但短期内安全厂商的产品和平台缺乏相对统一接口的问题仍将普遍存在。因此，中大型客户的态势感知平台建设项目的定制化开发依旧难以避免。
- 安全运营服务正在成为众多安全厂商重点投入的发展方向。IDC 认为，未来几年，我国企业级客户网络安全专业人才短缺的问题仍将存在，而态势感知平台往往功能丰富、技术性强、重要性高，需要安全运营人员快速发现、判断和处置安全事件，人才需求与供给的失衡将持续促进企业对专业的第三方安全运营服务需求的快速增长。因此，安全厂商越来越重视产品交付后在企业侧的实际应用情况，力争帮助企业实现实战化安全运营，同时提升客户粘性。
- 软件即服务（SaaS）化和远程托管的态势感知运营中心成为重要产品规划。企业上云是大势所趋，我国的公有云和私有云建设并驾齐驱，共同驱动云计算市场的快速发展。安全厂商也在顺应市场需求，积极打造安全产品和服务的 SaaS 化和远程托管能力。通过公有云或远程的统一态势感知运营中心实现云上租户网络安全状况的全面监测和管理，一方面解决企业级客户，特别是众多缺少专业安全人员的中小型企业安全能力不足的问题，助力企业安心上云；另一方面

帮助安全厂商实现大量云上租户的统一安全运营，降低安全服务成本的同时，还能实现与最终客户的直接联通，快速响应企业安全需求，提升客户满意度。

- 持续增强“网络安全分析、情报、响应、编排”能力依旧是态势感知解决方案的发展核心。安全厂商不断加大在先进技术领域的人员和资金投入，大数据分析、机器学习等技术已经广泛应用到态势感知解决方案的众多功能组件中，并有效提升了日志泛化、威胁检测、关联分析、溯源取证等能力。未来，安全厂商将继续增强包括人工智能（AI）在内的先进技术在实际业务场景中的应用，并提升这些先进技术在用户侧的效果感知。

IDC MARKETSCAPE 厂商入选标准

入选《IDC MarketScape: 中国态势感知解决方案市场 2021，厂商评估》报告的厂商需符合如下标准：

- 提供态势感知解决方案，并在态势感知领域有明确市场定位和长远规划的网络安全厂商。
- 该解决方案必须在中国有落地项目。
- 该解决方案必须至少提供以下功能：分析和情报、响应、编排（具体详见“市场定义”部分）。

给技术买家的建议

通过本次项目的调研，结合客户反馈和我们对市场的分析，向技术买家提出如下建议：

- 业务为先：作为企业主动网络安全防护体系的“智慧大脑”，态势感知平台不应成为业务发展的阻碍，该平台需要了解和适配不同行业客户的具体业务场景，尤其是针对中大型客户的安全需求和业务特点提供策略调整和定制化开发。例如政府和行业监管部门关注的监管态势感知平台、广大企业关注的运营态势感知平台、工业企业关注的工业互联网态势感知平台等，均具备自身独特的需求和关注功能点，从而使态势感知平台发挥更精准的安全防护作用。
- 威胁情报价值提升：威胁情报将在威胁判定和溯源方面发挥越来越重要的作用，甚至能够帮助企业提前感知同行业相关威胁，实现恶意威胁的主动防御。因此，技术买家应将优质的威胁情报融入到态势感知平台，提升平台威胁判定的准确性以及对新型威胁的及时感知能力。
- 技术和产品融合是趋势：虽然众多安全厂商都在努力拓展自有网络安全产品品类，力争凭一己之力为技术买家打造全面的态势感知解决方案，但优秀的安全产品需要技术的打磨和经验的积累。当前，广大安全厂商在平台建设、大数据分析、网络流量检测、终端安全防护、响应与编排自动化等方面各具优势。尤其是自身具备较强技术能力的大型技术买家，应全面评估各安全厂商的技术优势和产品特点，选择适合的产品组合打造高质量态势感知防护体系。
- 自动化能力是未来演进方向：随着企业规模的快速发展和 IT 资产的不断增加，态势感知平台获取和管理的数据量与日俱增，企业安全运营人员需要面对繁多的告警信息和安全事件。自动化/半自动化的分析和处置能力能够将安全运营人员从简单重复的工作流程中解放出来，腾出更多精力处置突发和复杂的安全事件，降低工作负载，提升工作价值。
- 托管安全服务助力平台价值最大化：IDC 定义下的托管安全服务分为三种类型。一是驻场安全服务（MSS-CPE），较多应用于大型本地化企业网络；二是本地托管安全服务（MSS-Hosted），较多应用于中小型本地化网络；三是云托管安全服务（CHESS），较多应用于公有云租户。对于缺少自有网络安全运营团队的技术买家来说，根据自身网络和业务属性选择适合的安全服务模式进行态势感知平台的托管运营是一个明智的选择。专业的安全服务人员能够更准确分析和更快速处置安全事件，充分发挥平台能力。
- 预算有限情况下需要分阶段建设：态势感知平台的建设是一个持续完善的过程，随着安全检测和防护技术的不断成熟，态势感知平台的相关功能或模块也将随之迭代更新。对于中大型企业

而言，态势感知平台将承载较多的功能需求，一次性实现整个平台的全面规划和建设是较难实现的目标。特别是在预算有限的情况下，企业更应做好项目的长远规划和分阶段建设。

- 需要关注产品易用性：虽然不是态势感知平台的核心价值，但对于广大中小型企业而言，简洁明确的功能和界面设计能够帮助网络安全管理人员快速掌握产品的使用方法，及时发现和处理威胁事件，并通过专业技术支持渠道解决复杂问题，最大程度实现态势感知平台的价值；而大型企业，尤其是重点行业头部企业的态势感知平台往往涵盖众多功能，以实现对安全事件的全生命周期管理，这就对产品的功能逻辑和界面设计提出了更高要求。如何帮助平台使用者一目了然地查看企业安全状态的关键信息，并能够快速找到所需信息和功能模块，无需在众多页面或窗口频繁跳转就显得更为重要。

厂商综合概况

本章节简要地解释了 IDC 通过厂商在 IDC MarketScape 中的位置得出的关键发现。在附录中概述了各个厂商基于各项标准的评估，该处展示了对各厂商的优势与机会的总结。

360 政企安全集团

360 政企安全集团在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

360 政企安全集团将自身定位于数字经济的守护者。过去 16 年专注为国家、政府、城市、企事业等提供网络安全技术、产品和服务。基于多年攻防实战经验及 230 亿安全研发投入，360 政企安全集团积累了海量安全大数据、强大的漏洞挖掘能力、高级持续性威胁（APT）狩猎能力、云端公共服务能力和全景攻防知识图谱，构建了以 360 安全大脑为核心，协同安全基础设施体系、安全专家运营应急体系、安全基础服务赋能体系的“四位一体”新一代安全能力框架。

优势

360 态势感知产品是基于安全大脑平台开发的，该平台整合安全数据、安全技术、安全能力等不同的安全要素，构建多维度、立体化、全空间的网络安全综合防护体系，实现技术手段创新、安全架构重塑、安全能力提升，在更大范围、更宽领域、更深层次推动智能安全运营。平台包括多项核心技术：

- **海量数据赋能**：360 安全大脑汇集了海量安全大数据，依靠顶尖安全专家的分析研究，产出的安全知识和威胁图谱从云端赋能态势感知产品，结合本地多种威胁分析引擎，及时精准发现很多传统手段无法发现的高级威胁攻击问题。。
- **强大技术能力**：态势感知平台采用先进的数据分析引擎，不但可以支持多数据源多维度关联分析，还可采用多层级分布式计算方式进行每秒 100 万笔超大数据量的分析计算，支持运营商级的数据处理。态势感知产品可根据客户的需求实现总部对分部的多级部署，总部可以监控查看各个分部的安全态势、安全告警，直接检索查询或溯源分析各个分部的原始日志信息，也可利用全局规则实现总部及各分部数据中心之间的跨数据中心统一关联分析，真正实现分级部署、数据同步、全局统一分析。
- **高位安全能力**：360 由覆盖全球的网络神经元实时监控全网攻击，安全专家持续跟踪分析攻击团队和新型攻击事件，产出威胁情报和检测规则，并下发到本地安全态势产品，一旦发现有新型恶意攻击，可瞬时部署到各个端点，实现全局联动整体防御 APT。
- **自动化评估能力**：360 实现抗攻击能力评估的落地实践。基于 16 年实战积累的高质量攻防技战术知识图谱，以及入侵者模拟攻击技术（Adversary Emulation System）自动化、体系化、实战化评估安全系统防御能力，度量安全产品的防护效果和业务系统的安全风险，提供分析报告和改进建议，帮助客户持续提升安全能力。

- **专业服务团队**：360 态势感知产品的背后是一支强大的专业技术支撑队伍，包括 17 支攻防专家团队、12 个安全研究中心，积累了大量攻防实战经验。依托于专业的安全专家，可帮助客户进行安全事件的分析、研判、处置等工作，提升安全运营的效率和效果。
- **广泛客户认可和支持**：态势感知平台是安全能力框架里最为核心的能力载体，向上获得 360 云端安全大脑赋能，中间连接 360 安全基础设施，向下对接生态产品及客户环境，帮助客户统一安全大数据，建立自己的智能“安全大脑”，目前已覆盖城市、电子政务、部委、金融、能源、运营商、网信等多个行业，同时已在重庆、天津、苏州、青岛、鹤壁、郑州等城市建立城市级分布式安全大脑节点，致力于把网络安全相关政府机构、运营商、国家科研单位、以及国企和民间的网络安全研究单位联合起来，统一安全大数据，形成网络安全的整体合力，构筑大安全时代的网络空间安全防线。

挑战

当前国内的态势感知领域的开发生态与国际领先水平相比仍有较大差距，产品的数据质量、数据互通和协同联动方面仍存在不足。360 政企安全集团致力于实现安全生态的共创、共享、共赢，未来持续完善数据模型接入标准、API 开放标准，建立应用程序（APP）开放框架，持续建立和完善多维威胁检测响应（XDR）体系生态伙伴，从接入数据质量、检测规则、联动处置进行深度整合和优化，探索客户安全生态的合作共赢模式。

阿里云

阿里云在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

阿里云计算有限公司是阿里巴巴集团旗下的云计算子公司，一直致力于提供稳定、可靠、安全、合规的云计算基础服务，通过提供创新的安全产品与服务，让用户轻松共享阿里云安全能力，为企业业务保驾护航。阿里云致力于确保云上每项业务的安全。利用阿里云平台上综合全面的安全服务套件，帮助客户快速建立一套强大的端到端保护机制，满足新应用或迁移应用的安全、数据安全和平台安全等需求，轻松审核和掌控持续的安全态势。

优势

阿里云态势感知系统结合阿里云威胁情报能力，同时依托于公有云强大的计算能力，将云上海量的攻击事件汇聚云端，并且从海量信息中通过数据汇聚、场景化模型设计、多形态的计算以及利用机器学习和分类统计等方法萃取得到情报知识库。

阿里公有云的计算能力深度挖掘原始信息里的情报知识，最大可能发现黑客背后团伙关系网络。情报的深度挖掘之后安全分析师验证判别情报质量和效果，做到所产生的情报在相应的应用场景里准确性接近 100%。同时态势感知结合离线计算（Max compute）、实时计算（Stream compute）、机器学习平台（PAI）支撑日志、漏洞、威胁情报、告警信息、蜜罐网络等安全特征和安全样本规模的加速训练，通过综合决策分析确保威胁分析的准确性，全面提升人工智能（AI）+安全的工程效率。

态势感知积累了大量阿里云内部安全运营的经验，在混合云场景中内置若干安全运营剧本，帮助运营管理者快速响应威胁事件。当发生威胁事件时及时止血和联动响应，有效帮助运营管理者提效三倍以上；同时内置多个安全编排组件，用户可以通过自定义剧本，针对自身的个性化运营场景进行定义，有效提升运营响应效率。

在产品方面，阿里云态势感知具备从威胁检测、安全防护、调查响应、安全运营、资产分析和关联响应的闭环能力：

- 威胁检测功能：具备云上超过 300 个威胁检测模型、云端蜜罐、威胁情报和云查分析，提供全面的安全告警类型检测，实时发现资产中的安全威胁、掌握资产的安全态势，检测资产中的安全告警事件，并提供修复处置能力。

- 安全防护功能：针对相关资产提供漏洞检测、云配置核查、安全基线检测、镜像检测等功能，提前发现脆弱风险，形成预警和修复机制，进行提前防护加固，保障基础安全能力。
- 调查响应功能：全面整合安全日志、网络日志、主机日志等信息，并结合多种云产品日志，通过大数据分析引擎对数据进行加工、聚合、可视化，同步威胁情报、机器学习引擎等形成攻击者入侵的链路图。
- 安全运营功能：安全运营中心实时展示资产的威胁概览信息和安全评分信息，提供资产全景、网络拓扑和安全态势的可视化界面，统一管控云上资产进行安全运营。
- 资产分析功能：自动化采集统计相关资产信息和资产指纹，从资产的类型、地域分布、防护状态、风险状态等维度分别展示资产的对应信息。
- 威胁情报关联分析：自动化集成威胁情报，在告警中进行关联分析，提供风险多维度的参考，便于进行威胁狩猎的响应处置。
- 自动化编排功能：通过安全编排和自动化响应（SOAR）的灵活拓展性实现各类自动化能力，提高安全运营效率，降低不必要人力成本。

挑战

态势感知产品领域的主要问题在于不同客户的业务架构、运营和分析的侧重点不同，以及用户复杂业务环境下态势感知的落地和应用问题。针对不同行业的威胁、业务特点、安全诉求、网络架构需要进行专项的梳理，并配套安全管家服务进行产品+人的模式进行有效应用和落地。

安帝科技

安帝科技在 2021 年中国态势感知解决方案市场评估中处于竞争者位置。

北京安帝科技有限公司是新兴的工业网络安全能力供应商，专注于网络化、数字化、智能化背景下的工业网络安全技术、产品、服务的研发应用和创新探索。该公司基于网络空间行为学理论及工业网络行为验证技术构建了工业大数据深度分析、威胁情报共享、威胁态势感知和事件协同响应等核心能力优势，为电力、水利、石油石化、轨道交通、烟草、钢铁冶金、智能制造、矿业等关键信息基础设施行业提供安全产品、服务和综合解决方案。

优势

安帝科技自主研发的工控网络安全态势感知产品采用模块化设计，可根据用户场景和需求进行定制化装配，更加贴近用户的网络情景，实用性更高，兼容性更强。该产品能够帮助客户实现网络安全监测预警、响应服务等全空间、全体系的纵深防御等，提升业务安全能力，保障了生产安全。实现了拍字节（PB）级数据处理和真实业务场景实时数据的采集、分析和处理，并结合大数据运算能力，实现安全建模和安全监测、预警、防护能力。

安帝科技的工控网络安全态势感知平台是一个产品体系，涵盖工业主机安全监测系统、工业安全流量日志分析系统、工业互联网安全运营平台、智慧运营应用程序（APP）系统等。该工控网络安全态势感知以工业网络安全大数据、工业关键基础设施数据为基础，以资产安全评估、物联网传感数据、威胁情报为信息支撑，通过智能分析技术全面感知、精准分析工控网络安全威胁，全面提升工控领域对网络安全威胁的发现识别、评估理解、态势感知和响应处置能力。

安帝科技态势感知平台具备以下特点：

- 工业网络设备兼容性强：工业环境设备小众、版本多、环境封闭，导致生产设备、网络设备、安全设备与态势感知平台兼容联动非常困难。安迪科技态势感知平台能够兼容主流工业环境中绝大部分生产设备、网络设备和安全设备。

- 大数据分析快速高效：面对海量的日志信息、威胁告警，人工分析难以保障时效性。安帝科技依托多年的行业积累和安全研究，结合大数据分析引擎，构建了多种工业网络安全分析模型，能够快速将海量安全数据进行建模分析，高效保障网络安全运营。
- 威胁情报智能关联分析：安帝科技态势感知平台可为用户精准提供威胁情报数据。通过威胁情报引擎实现网际互连协议（IP）、域名、统一资源定位器（URL）、文件信息摘要算法（MD5）等威胁情报关联分析，及时预警网络面临的安全风险。
- 未知威胁全方位感知：通过网络攻击行为、恶意代码传播、漏洞分布状态、重要系统风险等多种安全属性综合评估全网安全态势；通过对上述数据的深度挖掘、异常行为特征提取、原始日志分析等，实现未知安全威胁的全方位感知。
- 全局态势个性化呈现：支持自定义安全态势呈现方式，可根据关注度个性化配置各项数据展示形式及界面布局。支持数据钻取，可下钻数据进行可视化溯源分析；支持分级分区展示不同维度、不同视角的局部安全态势，满足多级个性化管理需求。
- 攻击行为还原追溯：通过实时感知当前网络攻击态势，关联记录攻击时间、攻击源 IP、目标 IP、攻击类型、攻击方式、攻击路线等信息，实时监测攻击者当前所处的攻击阶段、还原攻击路径，助力取证溯源。

挑战

工业生产领域各行业应用场景差异化非常大，需要解析繁多的工业协议，同时对于各类资产相关数据的处理、接入等方面也存在很多个性化需求。另外，工业企业部署的安全设备品牌多样，对安全集中监管带来挑战，特别是对于态势感知平台这类基于大数据进行可视化呈现的管理类产品，不同品牌设备的接入和监控是用户的重点关注点。

安恒信息

安恒信息在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

杭州安恒信息技术股份有限公司成立于 2007 年，于 2019 年登陆科创板。安恒信息秉承“助力安全中国、助推数字经济”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系。

优势

安恒信息态势感知依托在安全领域十几年的技术沉淀积累及多年来的行业实践，坚持自主创新，实现对安全威胁全生命周期管理，帮助企业实现安全运营闭环。主要特点包括：

- 安全数据汇聚：基于行业数据标准对数据进行标准化建模，能够对接各类安全设备日志，已支持超过 200 家厂商的 3000 余设备日志对接，实现安全数据统一管理、统一分析。同时基于大数据架构，实现超大规模存储查询能力。
- 完善的全息档案：以关键信息基础设施全生命周期数据治理为核心，引入安全知识图谱技术，将测绘、备案记录的域名、网际互连协议（IP）、指纹、身份作为线索信息，通过流式计算关联多个信息源中的高实时网络威胁数据和静态安全要素数据，建立关键信息基础设施单位、系统、人员的全息档案。
- 威胁检测能力突出：基于机器学习、大数据分析等前沿技术，通过流量分析、告警关联、威胁情报碰撞等手段实现安全威胁高检出率、低误报率。
- 将态势呈现于挂图作战的能力：深入研究网络空间地理学理论，围绕网络空间测绘与资产分析、地理资源和网络空间数据模型构建，研究绘制网络空间地理信息图谱，结合自研大屏可视化编辑系统，有机融入关键信息基础设施安全保卫平台，实现挂图作战，协助监管部门开展关键信息基础设施安全的保卫工作。

- 溯源分析灵活全面：基于终端资产指纹信息、设备日志、实时流量、云端威胁情报等数据，结合 ATT&CK 框架，利用知识图谱技术关联多源数据，提供资产风险分析、威胁场景分析、威胁情报分析、态势可视化分析等多维度安全分析，实现安全威胁的可视化推理溯源，满足用户日常安全运营分析工作及重大活动保障期间定向分析工作多元化需求。
- 响应闭环：通过安全能力 API 化实现安全能力集成，以安全能力管理安全设备，形成通用安全能力接口对外提供能力服务，保证高效快速的安全设备调用，已实现包括阻断 IP、放行 IP、消息通知、病毒扫描、漏洞扫描等超过 100 项能力覆盖。基于自动化编排响应策略实现检测、分析溯源、响应处置的安全闭环，根据响应策略自动联动终端检测与响应（EDR）进行终端溯源分析及病毒查杀、自动联动沙箱进行恶意文件检测、自动联动防火墙对阻断恶意 IP、自动联动消息通知及时告知安全风险。

安恒信息依托公司完整的人才和服务体系，通过专职的安全分析专家和安全服务团队提供“云+平台+服务”的运营模式，为用户提供及时有效的安全服务，为态势感知业务不间断稳定运行提供安全保障。

挑战

安恒信息在国内监管类态势感知市场具备广泛布局，并在多源安全数据采集、多维安全态势展示、多源威胁情报收集、网络安全监管业务等方面都有着丰富的创新实践经验。未来监管类态势感知技术的发展重点在数据的安全、情报的分析以及大数据分析，核心的突破点在于数据分级分权、情报采集能力以及针对多源异构数据持续的挖掘分析能力，这些都需要长期、持续的投入。同时，随着监管类态势感知在行业监管部门的拓展深入，需进一步加强对不同行业业务深耕，并加大帮助各行业客户网络安全专业人才培养。

安天

安天在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁，为客户数字化转型保驾护航。通过逾 20 年自主研发积累，依托端到端的安全能力和供应链关口前移的优势，帮助用户实现全场景的有效防御覆盖与可信场景构造。安天依托强大的威胁对抗体系实现深度客户赋能，驱动客户完成从威胁情报消费到自主安全能力生产的智能化安全运营变革。

优势

在逾 20 年的威胁检测与威胁对抗实战中，安天总结了具有自身特色的“识别”“塑造”“防护”“检测”和“响应”五个关键动作相关的安全防御矩阵，构建了一套动态综合防御体系。结合 ATT&CK 威胁框架，形成了面向实战对抗的态势感知解决方案，帮助用户实现智能化安全业务闭环。安天的态势感知解决方案以“资产清点”和“威胁对抗”为核心，一方面通过各类系统日志、网络流量、端点数据、事件信息的采集汇聚，实现对资产的清点识别、关键暴露面和脆弱性的检测、关键异常要素的提取和统一的策略调度；另一方面以“威胁对抗”为核心，从威胁的识别驱动分析、告警和处置的响应流程，构建以知识和规则策略为中心的体系，结合威胁情报驱动用户实现持续安全运营，实现纵向预测趋势和横向评估群体对象。此外，安天还采用了云化开发运维（DevOps）下的新型开发方式，覆盖开发、运维一体化过程的应用检测，保障产品自身的安全性。

基于上述技术特点，安天态势感知解决反感具备以下特性：

- 按照态势感知的要求构筑全要素采集能力，赋能数据采集。
- 以资产为中心，通过资产测绘还原网络空间地形，实现多层次叠加灵活、可交互的态势呈现。
- 良好的异常和威胁的智能化感知能力，支持按需监测和追踪溯源。
- 灵活的设备协同、线上线下多手段联动，提高面向处置的协同联动防御响应能力。
- 情报生产与利用形成能力闭环，有效构建威胁情报驱动的防御知识体系建设。

- 支持基于不完全的数据假设对态势进行智能化辅助分析和运营。

近年来，安天在哈尔滨、北京、武汉、上海、成都、深圳的研发团队规模持续增加，在终端探针、流量探针、后端数据处理、数据分析、用户行为分析等方向不断深化。公司在提供态势感知相关产品的同时，还注重打造符合用户实际场景和安全实效的服务与运营团队。团队包括安全专家、业务专家和经验丰富的服务人员，在北京、哈尔滨、武汉、成都、深圳、南京、上海多地都有售后和安全服务团队，可为用户提供 7x24 小时技术支撑服务，以及安全事件的应急响应与处置服务。

挑战

对产业升级和数字化转型有迫切需求的用户期望态势感知系统能高效识别、评估安全趋势，但面对异构的信息技术（IT）基础设施，如云上主机、容器等资产的动态可变识别挑战还很突出。其次，用户环境中有大量加密流量，如何通过解密、筛检来有效发现隐藏其中的恶意行为或攻击链极具挑战。同时，态势感知作为安全运营的能力支撑，需要厂商不仅向用户提供方案和系统，还应该进一步帮助用户建立起安全意识和实战能力，怎样才能更快、更有效地达成这个目标，还要持续尝试和优化。

迪普科技

迪普科技在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

杭州迪普科技股份有限公司以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技上市企业。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2-L7 融合式操作系统。在此基础上，依托于安全研究团队十多年以来在攻防研究、漏洞挖掘、威胁情报分析、安全事件响应等方面的技术积累，公司开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

优势

迪普科技态势感知解决方案的主要特点包括：

- 超大流量采集分析处理能力：迪普科技态势感知平台内置 18 类大数据组件，通过分布式部署探针的方式进行超大流量的采集，同时平台通过集群部署支撑超大流量的安全威胁实时告警、安全事件关联分析、安全威胁流量全包存储。前端采用优秀的大数据基础平台+业务微服务化+微前端框架的产品架构，在超大流量的场景下也不影响用户实际使用体验。
- 5G 场景的安全检测能力：针对于 5G 技术的广泛应用，迪普科技态势感知平台可以对 5G 场景进行安全监测，通过采集 5G 信令流及 5G 数据流，实现 5G 异常信令监测、5G 信令风暴监测、5G 网络攻击监测、多接入边缘计算（MEC）网站攻击检测等。
- 多源融合异构检测能力：迪普科技态势感知平台可以获取用户现场第三方平台的告警数据，与自身告警数据进行异构分析，全面扩展第三方检测能力，以提高安全威胁的检出率。
- AI 技术应用能力：迪普科技将 AI 检测技术应用在恶意加密流量识别、冰蝎检测、攻击者真实意图统一资源定位器（URL）识别、网站（Web）攻击检测、域名系统（DNS）异常流量检测等场景，使得检测能力得到大幅提升。
- 事件溯源能力：迪普科技将 ATT&CK 框架应用到态势感知的事件分析矩阵中，将 ATT&CK 战法中的 13 个攻击阶段与安全事件攻击链进行逐一映射。可帮助用户快速梳理攻击事件的原因、影响范围。同时对原始流量全包存储，在后续对攻击事件溯源取证时提供证据。
- 平台扩容能力：迪普科技态势感知平台对外服务采用微服务技术，各安全能力可单独在线热升级，其他安全能力不间断提供服务。各安全能力解耦运行，可灵活扩容漏洞管控平台、数据安全管控平台的功能。

- 安全服务全程参与：迪普科技安全服务团队配备有标准的《态势感知分析服务》、《态势感知策略调优》等服务的交付流程以及交付报告。可提供 7*24 小时的云安全服务，通过云端安全运营平台实时监测、分析、协助处置用户现网的安全事件。

挑战

当前态势感知领域所面临的困难和挑战在于各安全厂商态势感知的数据格式不一，没有统一的标准，想要做到对各家告警事件进行异构分析，提升安全检测的准确性，需要获取各家接口文档，并对平台进行相应的开发工作。

观安信息

观安信息在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

观安信息是一家提供大数据+泛安全产品与服务的高新技术企业，聚焦数据安全、网络空间安全、5G 安全、工业互联网安全、人工智能安全及公共安全等核心方向。经过多轮融资，观安信息已成为市场估值近 40 亿元的混合所有制企业。目前员工 1100 余人，已经是上海知名的综合网络与信息安全公司，具备信息安全领域的完整研发和服务资质。公司核心团队具有 20 年高端客户信息安全咨询服务经验和安全专业技术经验。

优势

观安信息的观鉴安全态势分析系统底层采用数据中台机制，支持海量多源异构数据的采集解析，分布式采集组件支持水平拓展，满足采集数据源不断增加的需求。产品支持大数据级的数据分析规模，支持历史数据分析，同时分析引擎具有扩展能力，可根据资源扩展或计算节点扩展自动提升引擎的分析能力。数据中台的数据仓库和数据服务体系将数据分层解耦、维度建模，深度挖掘大数据价值。产品通过数据服务接口的调用让业务功能灵活的运用数据，功能扩展和更新迭代更加敏捷便利。

观安信息的观鉴安全态势分析系统早期的目标客户为金融行业和运营商行业客户，分别解决了金融行业对安全分析细粒度高要求和运营商大网环境下海量资产难以统一监控的痛点。在产品不断迭代的过程中，观安信息将产品的重心逐步从安全事件挖掘分析转移到提升安全运营的效率和效果。如今的观鉴安全态势分析系统以安全运营为核心，将安全设备日志、主机日志、漏洞扫描结果，资产清单和威胁情报等多类多源异构数据进行交叉对比分析，以 ATT&CK 知识图谱作为可视化攻击阶段回放工具，为客户提供多角度纵深风险回放能力。辅以自研的 SOAR 工具，将安全分析专家的分析溯源和风险消弭经验落地到态势分析系统当中，进一步降低了企业对安全运维人员的能力和人力诉求。真正为各行业的客户提供一套“知其然，更知其未然”的安全态势分析产品。

观安信息态势感知产品团队已形成包括态势感知平台解决方案设计、产品设计、产品开发、态势产品运营和安全能力研究的团队格局，全面支撑态势感知的相关业务。除态势感知产品运营团队外，观安信息有专业交付团队，遍布全国各个区域，公司下辖的多个实验室也为态势感知平台提供坚实的技术支持。

挑战

不断出现的新型网络攻击和海量攻击数据的冲击，促使观安信息不但需要实现安全数据的统一管理、安全态势的直观展示及数据关联分析，还需要在 AI 分析模型、溯源定位等更高的技术领域不断探索、不断创新，努力超越网络攻击者的脚步，将网络攻击消灭在萌芽期，使企业客户的网络资产免受侵害。

虎特科技

虎特科技在 2021 年中国态势感知解决方案市场评估中处于参与者位置。

虎特信息科技（上海）有限公司成立于 2016 年。公司使命是致力于掌握国际信息安全趋势，自主研发先进的网络安全产品和服务。公司聚焦数据安全、网络空间安全、人工智能安全、及公共安全等核心方

向，为运营商、政府、金融、电力、公安、医疗等行业用户提供全面的信息安全解决方案。公司核心团队有着 10 多年信息安全专业技术经验、多年大数据分析经验。

优势

- 提升企业威胁检测与安全防护水平：利用平台的日志关联分析和威胁情报能力，大幅提高安全威胁的检出率以及对 APT 攻击的发现能力，无需管理人员再去面对海量的日志信息，无需企业投入更多专业的安全技术人员，大大提升企业积极防御的能力。

- 提升企业数据查找与事件追查能力：虎特科技态势感知平台（iView）采用搜索引擎技术作为本地数据存储和检索核心技术，采用 json 格式作为引擎的输入输出格式，这样可极大提高检索性能，可为企业本地的大规模数据保存、攻击证据留存和追查、实时关联分析提供坚实的技术保障。

- 帮助企业实现安全态势可视化：一方面可通过可视化技术将原本碎片化的威胁告警、异常行为告警、资产管理等数据结构化，形成高维度的可视化方案，便于用户理解；另一方面可以通过可视化技术将威胁事件与企业业务进行有机结合，通过态势感知大屏将内网全局的安全态势以图形化的方式直观呈现，将安全由不可见变为可见。

- 安全设备统一管理和联动，提升运维效率：通过平台的使用实现安全设备的统一运维、多种安全设备日志信息的整合和关联分析，大幅降低企业在安全运维方面投入的精力，降低安全威胁发现和处置的难度，有效提升企业安全管理效率。

- 降低企业安全运营与管理成本：用户可以直接通过态势感知模块直观查看企业内部不同资产组的风险分布，可以将风险以可视化的形式进行呈现。所有安全态势的展示都可实时刷新，及时将最新的安全态势呈现给管理者。同时，流程化的处置工单管理功能有利于工作的分配、记录以及处置经验的沉淀，降低企业安全运营与管理的资源投入。

挑战

当前单一安全设备的告警信息所展示的内容通常比较有限，而且经常缺少相关联的上下文信息，而不同的安全设备所提供的告警信息关注的问题角度不同，态势感知平台和安全管理人员需要识别这些告警，并将不同设备的告警信息进行整合智能泛化和关联分析，从而进一步发现潜在的问题。另外，如何识别和排除大量告警信息中的误报信息，也是虎特科技态势感知平台需要进一步克服的挑战。

华为

华为在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

华为创立于 1987 年，是全球知名的信息与通信（ICT）基础设施和智能终端提供商。目前华为约有 19.7 万员工，业务遍及 170 多个国家和地区，服务全球 30 多亿人口。华为承诺将构筑并全面实施端到端的全球网络安全保障体系作为公司的重要发展战略之一，同时承诺将公司对网络和业务安全性保障的责任置于公司的商业利益之上。华为云继承了华为以客户为中心、以“网络安全和隐私保护作为公司的最高纲领”的基因，始终坚持遵从最严格的行业规范，恪守业务边界，携手生态伙伴，打造最优质可信的云服务。

优势

华为 HiSec Insight 安全态势感知系统是华为安全的重点战略方向，作为华为 HiSec 安全解决方案的分析器，是整个解决方案的“安全大脑”，也是生态构建的基础。

- 从技术架构方面，华为 HiSec Insight 安全态势感知系统采用开放的大数据架构定义控制总线和数据总线，以实现针对第三方组件的标准化对接和联动，同时构建了以 HiSec Insight 为中心的 HiSec 安全态势感知解决方案。
- 在生态合作方面，华为主导成立了“华为安全商业联盟”，通过创新的联合安全解决方案，深度整合联盟伙伴的优秀产品，实现终端、网络、应用安全之间的协同联动，为广大客户提供整体安全产品、解决方案和服务。
- 在威胁分析检测方面，华为将智能检测能力贯穿至整个攻击链的威胁检测，从渗透、命令与控制、内部扩散以及数据窃取各个阶段进行关联分析，精准识别、主动发现未知通信威胁；同时运用智能算法+大数据技术结合用户和实体行为分析（UEBA）能力从海量数据中快速关联异常行为，快人一步检出高级威胁。
- 在威胁情报方面，华为具有独立的安全实验室未然实验室，专门进行攻防对抗实验、渗透测试、攻防技术研究，同时进行情报信息收集、威胁专项分析、漏洞分析、补丁制定、情报发布与共享。
- 在协同联动方面，华为 HiSec Insight 具有业界独有的云、网、安、端整体态势感知解决方案，华为 HiSec Insight 既可以与华为云平台进行对接，实现云上和云下形成统一安全态势检测，也可以和安全产品（防火墙、入侵防御系统、沙箱等）、网络产品（路由器、交换机等网络控制器）进行数据对接、策略联动。除此之外，还可以与合作伙伴产品进行联动，如蜜罐、身份安全管理、EDR、工单运维平台（IMOC）等，形成端到端的整体态势感知解决方案。
- 在平台自身可信方面，华为认为安全产品自身的安全可信是重中之重。华为 HiSec Insight 安全态势感知系统遵循华为安全可信的技术与实践，通过安全启动验证程序完整性；对开源及三方软件进行体系化管理；对产品进行全生命周期的可信安全管理；通过无漏洞、整洁、架构优雅和持续演进的 CleanCode 编码，多层面构筑产品的安全可信，从而最大程度上保障作为安全防护体系的核心大数据产品的自身安全性。

华为云提供可信的安全平台，持续将安全经验赋能到租户，提供丰富的 AI 检测模型、安全运营工具、极简的运维流程和专业的安全服务，起到引导安全运营的作用。结合华为 30 年安全经验积累，以云服务的形式，为客户建立由管理、技术与运维构成的安全风险管控体系，结合企业与机构业务的安全需求反馈和防控效果对用户安全防护进行持续改进，帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险并消除安全事件带来的损失。

挑战

华为态势感知解决方案未来增长面临的主要挑战是如何将该方案高性价比、快速交付给腰部以下客户。未来将以安全云服务形式提供，打破安全态势感知解决方案对运维服务人员的强依赖；完善生态合作，定义数据总线机制，让安全生态伙伴监测的数据更完整，补足缺少的安全组件；同时持续将 AI 能力用在态势感知解决方案上，辅助人工运营，降低持续运营成本。

随着企业数字化转型的深入，企业将大量的 IT 基础设施、业务迁移到云上，在享受云计算带来的便利的同时，也将引入安全合规、安全监管、数据治理、威胁攻击等新的安全挑战。

聚铭网络

聚铭网络在 2021 年中国态势感知解决方案市场评估中处于竞争者位置。

南京聚铭网络科技有限公司是腾讯战略投资的安全产品提供商和安全运营商，公司专注于网络安全智能分析和检测，提供全面的信息安全防护，为达成“让安全更简单”的使命而不懈努力。目前已服务医疗、教育、政府、金融、能源、电信等行业客户，业务覆盖全国 32 个省市地区。

优势

目前聚铭网络已经为医疗、教育、政府、金融、能源、电信等大量行业客户提供服务。另外该公司除了行业大客户直销外，在全国已经有超过 200 家签约渠道，在南京、北京、上海、西安等地设有子公司或办事处。该公司态势感知产品具备以下特点：

- 全息态势感知：集日志、流量、漏洞、违规配置、资产、威胁情报于一体的多维度、多源异构综合态势感知分析平台，充分体现“数据为王”的优势。
- 以资产为核心的精准失陷分析：告别海量安全事件困扰，围绕攻击者的攻击手法、渗透战术进行威胁识别分析，结合受害资产的异常行为、风险暴露情况，精准定性受害设备所处的威胁阶段及其危害影响。
- “溯源+取证”，知过往，明当下：全面的溯源分析不仅能够准确地回溯攻击者的渗透轨迹，从源头上消灭安全隐患，还能通过对内网的横向传播分析，精准全面地评估受害资产范围；而轻量级的终端取证更是能够让隐蔽的恶意软件，甚至无文件攻击无处遁形。
- “网络+安全”联动响应：为了提升安全运维效率，降低安全运维门槛，聚铭网络态势感知产品在联动防火墙、流量探针等设备进行内外网威胁行为封堵的基础上，还加强了与交换机的联动，实现内网受害资产的隔离限制，并且支持软件定义网络（SDN）、软件定义广域网（SD-WAN）网络场景，第一时间控制威胁蔓延。
- “云+端”的一体化安全运维保障：对于具备自主安全运维能力的客户来说，聚铭网络态势感知“端”的全面采集、定性分析、深度溯源、实时取证、便捷响应能力为运维提供了支撑保障；对于安全运维能力相对较弱的客户来说，聚铭网络提供了 7X24 小时的云端安全监控、云端安全分析、云端专家服务的管家式服务，帮助客户实现小投入大回报，告别安全运维门槛高的烦恼。

聚铭网络产品团队核心人员专注于安全运营中心、日志审计的研究，拥有近 20 年安全产品开发经验，为态势感知产品的研发打下了牢固的基础。

挑战

一方面，由于安全行业头部厂商在知名度、渠道覆盖深度等方面占据优势，聚铭网络便投入大量资源进行产品打造，在过去 5 年赢得大量用户的信赖。另一方面，聚铭网络需要紧跟国家政策、相关行业策略的变化，以更长远的眼光看待行业发展并做出前瞻规划。

兰云科技

兰云科技在 2021 年中国态势感知解决方案市场评估中处于竞争者位置。

兰云科技是一家网络安全监测与分析取证解决方案提供商。兰云科技认为，在网络安全防护体系中“检测只是开始，调查才能结案”，网络安全应构建以“破案”为中心的解决方案，以此降低安全事件调查分析的难度，提升安全事件调查分析的效率，从而提升破案率，让潜在犯罪分子不敢犯罪，降低犯罪率，让网络空间回归兰天白云。

优势

兰云科技的兰天智能安全平台以实战为目标，以大数据技术为基础，采集全量安全分析所需数据，采用安全运营和分析平台架构（SOAPA），包括沙箱、流量分析、威胁情报、机器学习等新技术，以及安全信息和事件管理（SIEM）、漏扫等传统成熟技术，再结合攻防实战、威胁狩猎、SOAR 等场景化能力，大幅提升用户安全运营效率，实现高级威胁的发现、调查分析、响应处置，以及安全集中管控的核心需求。

兰云科技态势感知平台的特点在于：

- 高级威胁发现能力：平台采用沙箱技术、关联分析技术、威胁情报、机器学习技术，能够准确检测高级威胁和异常行为。
- 高效的安全事件调查分析能力：能被检测到的威胁（或者线索）通常不再对目标网络产生危害，未被检测到的威胁才是真正对目标网络产生危害的。兰天智能安全平台通过将典型安全事件分析流程标准化，固化安全专家的经验，以及通过将调查过程转变成可视化的交互方式，使得安全事件的全面调查分析变得简单、高效。
- 创新的多维安全对象关联分析能力：平台定义了多维安全对象实体，包括：网元设备、安全设备、实体、虚拟终端、服务器、应用服务、流量特征、安全策略、漏洞、安全配置、分类分级的数据资产、数据流转路径等，并结合场景进行关联分析。
- 创新的基于攻防实战场景的精密编排能力：平台基于攻防实战场景设计了标准预案进行精密编排，包括：态势感知、场景分析、关联分析、威胁狩猎、自动化处置、溯源留证。实战场景包括业务系统分析、内网横向移动、管理协议异常、失陷主机、勒索软件、挖矿等多种典型场景。

挑战

兰天智能安全平台采用 SOAPA 架构，具有充分的开放性，支持接入各种安全产品或安全系统，但国内安全厂商众多，安全产品更是繁多，各有各的标准、接口。如何在平台和产品之间实现快速无缝对接，充分融合各类安全产品的优势，发挥整体解决方案的优势是一大挑战。

六方云

六方云在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

六方云是一家致力于提供工业互联网安全、关键信息基础设施保护的创新型公司。针对工业客户、政企客户的安全需求，六方云借助人工智能技术仿生人体免疫机制，创造性地提出了“AI 基因、威胁免疫”的安全理念，采用 “+AI”和“AI+” 战略将人工智能技术应用于全系列产品，通过提供“5+1”产品线、AI 安全技术的纵深防御解决方案及安全服务，帮助工业和政企客户构建安全威胁免疫系统，为国家关键信息基础设施安全保驾护航。

优势

六方云安全态势监测与管理平台依托海量工业互联网数据，运用大数据分析、数据融合、人工智能建模等技术，可实现全景/行业、集团/企业、厂站/边缘等不同层级的对网络安全状态的实时了解，对网络安全风险发展趋势的深刻洞察。其优势主要体现在：

1）采用无代码编程技术，可快速适配接收第三方数据，包括结构化、半结构化、非结构化、二进制等数据。

2）采用人工智能建模和大数据分析技术，基于身份、数据和资产的行为关联分析，结合工业机理模型和人工智能模型，实现诸如 APT 攻击、未知威胁、恶意加密流量、借助隐蔽隧道的数据泄露等威胁的实时与半实时检测能力。

3）采用告警、联动、攻击链展示、安全编排与自动化响应等技术方式，提供自动与半自动的处置响应能力，可快速联动网络控制器、安全控制器等系统及时阻断或隔离威胁、精确溯源、甚至是技术对抗等。

4）采用机器学习算法，基于设备的网络行为分析建立设备唯一的、难以仿冒的身份标识，使得企业构建基于零信任的网络安全体系，行业和监管部门实现准确的网络空间测绘成为可能。

5）借助对工控协议指令级解析技术和对工艺流程的深刻理解，围绕工业互联网的“四层、三网、两平台、一系统”，实现对工控操作指令从解析到解读，对工业数据从感知到认知，对工业信息安全状态从局部到整体，对工业信息安全风险从未知到掌控的真实转变。

挑战

工业领域每个行业都有自己独特的行业特性，工业态势感知产品需要贴合各行业现状来进行产品的落地。工业现场的运维人员对网络安全的意识相对较低，工业态势感知平台对企业网络运维及安全运营背负很大的压力。工业信息安全风险预测当前还存在技术瓶颈，随着工业数据处理从“囫囵吞枣”到“深度解读”的转变，大数据分析技术、人工智能建模技术的不断应用，工业态势感知的安全风险预测功能将会成为工业态势感知产品的 “杀手锏”。

绿盟科技

绿盟科技在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

绿盟科技集团股份有限公司成立于 2000 年 4 月，总部位于北京。绿盟科技基于多年的安全研究，秉持智慧安全 3.0 理念，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。公司一直致力于跟踪国内外最新网络安全攻防技术，设立了云、格物、伏影、天机、天枢、天元、平行、威胁情报八大实验室，专注于云计算安全、工业互联网安全、物联网安全、车联网业务场景安全、安全威胁监测与对抗技术、攻防对抗技术、数据智能安全研究等领域研究，在基础安全研究和前沿安全领域进行积极的探索，为公司的核心竞争力和持续创新能力提供有力保障。

优势

绿盟科技通过对典型客户的调研和分析，结合网络空间风险与威胁变化、国家要求、行业和企业客户发展与安全需求的变化，基于公司多年的产品研发经验和攻防实践技术积累，研制并发布了面向多个垂直行业和企业客户全方位的态势感知产品和解决方案，在覆盖 PC、服务器、网络等传统防护对象的基础上，满足云计算、大数据、移动互联网、工业互联网、物联网、车联网等新业务和新场景。

技术创新优势方面，绿盟科技在“智慧安全 3.0”理念的驱动下进行创新实践，在态势感知和安全管理领域持续以“实战化安全运营”为核心，形成了一系列实战化对抗相关技术能力的创新，如融合数据安全管理能力及零信任安全管理能力，除传统威胁检测、漏洞管理、资产管理、异常行为分析 UEBA、情报驱动威胁检测与分析、全流量深度检测与自动化安全编排与响应能力 SOAR 外，通过独创的分析推理引擎和独创的风险评分算法，将多种安全数据变量纳入安全指标考量范围，帮助客户建设从被动防御向主动安全转型的能力体系建设。智能决策能力层面，结合 ATT&CK 综合防御框架扩展了基于蜜罐、终端 EDR、本地情报平台等更多实体安全数据的关联分析，从威胁检测深度、精准度以及攻击结果判定等多维度威胁检测覆盖率、准确率和运营研判效率做了提升和突破，并积累了 5G 安全、车联网、工业互联网、物联网、多云安全管理等场景下的流量分析、建模和威胁检测场景算法。

在平台架构方面，绿盟科技已经形成绿盟中台架构 1.0，建立了水平、开放、集约的 IT 安全中台架构体系，通过融通安全数据、汇聚基础安全能力，实现安全能力开放共享、安全业务按需敏捷交付，基础安全能力原子化、服务化，聚合安全能力，对共性安全能力统一编排调用，统一纳管、高效协同，形成了云边端一体化防御体系，以标准 API 或软件开发工具包（SDK）方式开放给外部应用。在挂图作战能力维度，通过攻防沙盘、风险推演可视化能力，将人——地——网等新型可视化纽带关系展示出来，通过空间图、网络图清晰表达网络安全事件的全过程，对网络空间要素、模型运算和应急处置进行全生命周期的场景展示。

在产品与服务体系方面，绿盟科技立足国内“智慧运营”的未来发展，整合多方优势资源推出“城市安全运营中心”、“行业安全运营中心”及“企业一体化安全运营服务”，凭借完善的专业服务体系帮助

企业建立适合企业自身的安全运营和保障机制以及安全能力与安全经验库，刺激企业内部的战略性安全能力输出。

挑战

- 在市场营销方面，未来绿盟科技将积累的丰富的攻防实战经验应用于更多监管行业的新一代安全能力框架建设，协助政企客户完成关键信息基础设施信息安全防护方面的安全管理平台和安全大脑的建设，同时致力打造“公司+渠道”联合拓展的渠道销售模式，推出迎合中小市场的专项威胁分析和管理系统。
- 在产品技术方面，绿盟科技后续将围绕“绿盟中台架构”持续发力和拓展多态势能力整合，将工业互联网态势、数据安全态势、零信任安全态势、5G 安全态势等人、云、应用、网、边界和端的安全生态资源能力有效整合，构建以“作战、对抗、全场景攻防思维”的智能安全运营平台，将安全体系与数字体系融合，攻防能力与管控能力融合，为政企客户提供网络安全技术、产品和运营服务。
- 基于绿盟安全保障中台的安全运营重保新思路已经在政府、金融、运营商等各行业实践赋能，并取得了良好的客户反馈和使用效果，未来将常态化实践保障中台赋能思路，配合绿盟科技一体化安全运营服务，使政企客户的各类安全问题在日常运营中得到解决，持续提升企业安全水平，真正做到攻防保障工作常态化、体系化和实战化。

奇安信

奇安信在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

奇安信科技集团股份有限公司（以下简称奇安信）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内知名的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，奇安信是 2022 年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商；此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

优势

在产品体系方面，奇安信提供的产品体系能够覆盖网络安全态势感知相关应用领域，全面满足国内态势感知市场的主流需求。其中：奇安信网络空间安全态势感知平台，是平战结合、攻防兼备、智能开放的网络空间安全治理综合业务平台和指挥作战平台；奇安信态势感知与安全运营平台，面向企业安全运营应用领域，是基于大数据架构的新一代安全运营管理系统；奇安信攻防态势感知系统，针对网络安全分析领域，以攻防渗透和数据分析为核心竞争力，聚焦威胁检测和响应，提供安全服务和产品解决方案。奇安信威胁情报中心，基于奇安信自有的网络安全云端大数据以及先进的威胁情报运营体系，提供高价值的可机读战术情报、作战情报和战略情报等威胁情报能力，为态势感知产品进行赋能。

在服务体系方面，奇安信托管安全服务（MSS）服务提供从监测、分析到处置的闭环式托管运营服务，通过远程收集安全设备的日志和流量数据，利用大数据存储、分析技术，对各类安全数据进行关联分析和深入挖掘，通过 7*24 小时全面、持续的安全监测，及时发现各类网络攻击行为、系统脆弱性事件，并对安全事件进行通报预警及可视化呈现，一旦发生安全事件，安全专家对安全事件进行分析及研判，第一时间通知现场服务人员，协助客户对安全事件进行通知与处置等响应动作。

在技术创新优势方面，奇安信在“数据驱动安全”理念和“内生安全”的创新实践驱动下，形成了一系列国内优秀的网络安全态势感知相关技术创新。如：基于多维分析的安全风险计算模型、基于攻击溯源的自动化分析和同源关联、基于图关系模型的威胁情报分析、Sabre 分布式关联分析、天工安全大数据建模分析等创新技术。

在本地平台大数据体系方面，奇安信通过大量实战已经同时拥有可落地、见实效的大数据体系所必备的要素能力：多源异构数据采集、大数据存储计算、大数据深度治理、大数据分析建模、大数据应用以及持续运营等能力。

奇安信网络安全态势感知相关产品和解决方案均基于统一的大数据基础平台和体系结构，能够对海量、分散、隔离、不同来源和不同格式的数据进行集中采集、处理和存储，向应用平台提供开放的应用程序编程接口（API），以减少重复建设并简化产品整合，从而帮助快速建立安全大数据分析应用。

在态势感知市场，奇安信目前已积累了几千家成功案例，覆盖央企、电子政务、金融、运营商、高校等行业，区域覆盖全国各省市级区域，包括澳门和香港。奇安信态势感知产品为一系列国家重大活动提供了重要技术保障。

在产品研发团队方面，奇安信在态势感知领域的团队包括产品研发团队和后端安全研究团队，总人数近千人。在北京设立总部，在武汉、西安分别设立了研发中心。拥有一流的产品设计师、架构师、专业的数据引擎研发人员（负责关联分析引擎、机器学习与算法模型的研究和开发）、日志分析和安全建模工程师及熟练的仿真测试人员，为产品研发提供强有力保证。

挑战

奇安信还需要持续培育网络安全态势感知市场、培育客户和引导市场，认清态势感知的目标，根据客户不同行业的业务特点针对性深耕，更加重视安全运营，加大安全运营服务的占比。尊重安全人才培养的客观规律和要求，在安全数据和情报共享的基础上，允许并支持建立相对集中的安全运营模式，快速培养和形成更有战斗力的态势感知安全运营能力体系。

启明星辰集团

启明星辰集团在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

启明星辰信息技术集团股份有限公司成立于 1996 年，是国内知名的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。面临“数字中国”的新安全挑战，启明星辰集团基于场景化安全思维，打造自主可控的安全生态体系，赋能更加高效、智慧、安全的数字化应用场景，实现“护航数字中国，领航信息安全”的美好愿景。

优势

启明星辰集团态势感知是在 10 多年安全运营中心（SOC）产品的基础之上进行重构开发的产品，具备以下 6 大基础能力：

- 全量的数据接入能力：支持采集系统应用日志、威胁告警日志、设备安全运行日志、资产数据、脆弱性数据（系统漏洞、Web 漏洞、配置弱点等）、流数据、威胁情报数据等。
- 专业的大数据安全智能分析：支持基于分布式的关联分析引擎，AI 分析引擎，行为分析引擎，预置高价值攻击链分析场景，同时支持安全人员按需进行自定义。
- 全面的资产发现与风险评估能力：支持主动、被动发现未知资产，同时根据资产价值、脆弱性、威胁三个维度评估资产风险。
- 有效的预警与自动化处置能力：支持预警通告、调查、工单、SOAR 编排联动能力。
- 丰富的安全运行监控能力：支持 IT 系统的可用性、性能与服务水平监控、拓扑自动发现能力。
- 全天候态势感知呈现能力：包含内置通用态势大屏（综合态势、资产态势、攻击态势、脆弱性态势、风险态势等）以及自定义大屏组件。

启明星辰集团的态势感知版本分为监管类、企业运营类，监管侧态势感知基于全国一盘棋格局规划与国家平台实现数据上传下达，同时接收国家平台下达的指挥指令和共享信息。运营侧态势感知从风险可

见、威胁可见、及时预警、迅速闭环、成果可视维度来构建，持续收集防护目标对象的资产、运行、脆弱性、内外部安全情报、日志、流量及各类情境数据，从多维度多视角持续监测、评估和预测网络安全态势，及时进行风险预警、安全告警、联动处置和情报分享，构建一个全天候全方位的态势感知支撑平台，协助网络管理者从全局视角持续安全运营。

启明星辰集团态势感知的销售模式有三类：提供产品（按功能模块与管理授权许可售卖）、运营中心安全服务、云部署服务。

- 按管理节点收费：根据用户选购的功能模块与管理节点授权售卖；适用于用户已购买态势感知产品自己建设运维队伍的客户。
- 以态势感知产品为基础，为客户提供态势感知安全服务、第三方独立运营服务等，按期收费并提供安全服务报告；适用于没有自建安全运营队伍，需要厂商或第三方提供产品及服务的客户。目前启明星辰集团已在全国各地成立 85 个安全运营中心，为客户提供安全运营服务。
- 在云端部署态势感知，为租户提供态势感知服务；适用于云租户使用。

启明星辰集团态势感知研发团队近 300 人，分别在北京、上海、陕西、广东、成都、杭州设有研发资源。参与态势感知研发分析、后端技术支持团队还包括核心技术研究院、积极防御实验室（ADLab）、大数据实验室（BDLab）、金睛团队、安全运营团队。

挑战

态势感知处于蓬勃发展阶段，数字化转型带来的安全困境与挑战日益剧增，对网络安全运营、安全监管、指挥作战的需求在增加，对态势感知产品在数据源采集范围（物联网、车联网等）、大数据分析能力、智能运营联动处置能力、AI 分析算法方面都有了更高的要求，从而达到更好的宏观分析、预警响应、应急处置能力。

盛邦安全

盛邦安全在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

盛邦安全倡导“安全有道，治理先行”的安全理念，以“让网络空间更有序”为使命，在网络空间地图、业务安全、供应链安全、应用防御和脆弱性检测等领域已成为国内知名的网络安全产品及服务供应商之一。作为国家网络安全保障支撑单位，盛邦安全一直奋斗在网络安全一线，曾参与上海世博会、世界互联网大会、反法西斯战争胜利七十周年、新中国成立 70 周年庆典等多场重大活动的网络安全保障工作，是国家重大活动网络安全保障技术支撑的坚实力量之一。

优势

盛邦安全态势感知解决方案经过多年打磨，目前可以灵活应对不同行业场景的需求痛点，构建对应不同分析视角的多维度方案，如资产综合治理、风险监测预警、统一安全管理等，符合态势感知体系在通用分析模型的基础上具备个性化场景理解能力的技术要求。盛邦安全态势感知解决方案在产品理念、技术实现和市场应用方面具有如下特点：

- 丰富的数据源：方案包含了资产台账信息、资产脆弱性数据、入侵威胁事件、高级威胁事件和横向异常行为等多种类型的数据，可以提取资产 IP、端口、服务、系统、中间件、安全漏洞、弱口令、网站脚本（Webshell）后门、内容审计、恶意访问、非法扫描、僵尸主机、木马、蠕虫攻击、暴力破解、注入、跨站脚本、请求伪造等各种维度的元数据，原始信息丰富、研判依据全面，可以为态势感知提供可靠的数据支撑，并且在事件研判时提供详细的依据线索。
- 动态的资产视角：方案通过资产治理的安全视角建立了一套从网络资产管理出发，围绕资产属性、管理状态、自身安全性和被攻击风险进行关联分析的态势感知模型，在入侵监控、脆弱性监控的基础上进一步补全了事件分析的维度。通过在线感知、事件学习和手动梳理相结合的方

式，形成动态更新的资产台账，保障资产管理的准确性和时效性，协助用户从业务角度梳理安全态势，精准识别安全风险，合理执行应急响应措施。

- 精准的关联分析：方案包含了不同维度的原始安全事件，可以有效提升事件关联分析的准确性。通过态势感知方案的整合以及关联分析找出不同类型安全事件之间的联系，排除干扰因素，提取有效信息，并结合资产的健康状态、遭受威胁的可能性、威胁的破坏程度等信息准确判断事件影响程度并给出处置建议，进行下一步通报和处理动作。
- 闭环的处置流程：方案整体设计思路覆盖安全事件的态势监控、关联分析、事件研判、通报预警和应急处置等环节，可以针对某个安全事件提供从发现分析到处置跟踪的完整流程，并利用通报处置功能将安全技术与管理操作有效结合起来，协助用户跟进事件处置的整个过程，不论是高风险的入侵事件、高危漏洞或是非法行为等都能够真正意义上做到安全闭环处置。

挑战

盛邦安全态势感知解决方案在未来的探索当中，将继续发挥公司在网络资产画像方面的技术优势，在工业互联网、智慧园区等领域，针对特定业务场景进行专有资产学习、行为学习建模和分析算法研究，继续提升方案的适应性和可靠性。

深信服

深信服在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

深信服科技股份有限公司是一家专注于企业级安全、云计算、IT 基础设施与物联网的产品和服务供应商，拥有深信服智安全、信服云和深信服新 IT 三大业务品牌；目前，深信服员工规模超过 7500 名，在全球有 60 余个分支机构。公司持续将年收入的 20%投入到研发，并在深圳、北京、长沙、南京和硅谷设立 5 大研发中心，研发人员比例约为 40%。公司坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。

优势

态势感知内部分化为云化态势、安全运营（NGSOC）、高级威胁检测（NDR）、威胁检测一体机 4 大细分品类，主要面向公司商业市场、中端市场和头部行业客户三大客群进行分层分场景提供对应产品。

深信服态势感知产品采用“多流动态检测技术”，一种以 UEBA 和 AI 为核心，结合多方安全产品日志进行上下文关联分析的检测算法技术，面对各种不规则、隐秘性高的组合攻击手段，能够实现高检出低误报，基于全包存储和灵活检索分析。产品支持对全包流量进行深入研判分析，结合内置的 ATT&CK 举证检索能力，快速实现威胁定位和追踪，确定业务安全体系的关键脆弱性，锁定高级威胁入侵口。同时，产品采用 SOAR 技术联动多方安全产品进行闭环处置，为业务保驾护航。另外，产品结合全新开发的精细化工单模块，支持工单加签结论且抄送多方负责人，支持给运维者生成临时管理员账号闭环处置（限时回收）、支持基于工单进行通报、认领、限时处理提醒、加签评价形成完整闭环机制；让安全运营的流程更轻便，闭环更高效。

深信服态势感知团队有 750 名研发，包括检测能力团队、情报团队、算法团队、交互设计团队、服务团队、架构团队、测试团队、运营团队、规划团队、海外团队、云端服务团队、关键客户大项目支持团队、运营研发团队。

挑战

深信服需要面对国内多云化场景日益丰富和云内多维度威胁可视化需求的挑战，同时要做到云内检测方案的轻量化。一方面云内的云生态开放性、成熟度参差不齐，另一方面云场景涉及数据敏感性和多租户场景，在检测的同时要兼顾保障数据的隐秘性以及多租户多视角的自运营监控，需要投入更精细化的产品方案打磨和优化。同时，深信服也看到客户的带宽和流量越来越大，如何更具性价比地进行流量审计和检测会为旁路检测产品带来挑战。

腾讯安全

腾讯安全在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

腾讯安全作为腾讯立足互联网安全的行业品牌，致力于成为产业数字化升级进程中的安全战略官。依托 20 多年业务安全运营及黑灰产对抗经验，凭借行业知名安全专家、完备的安全大数据及 AI 技术积累，为企业构建“情报——攻防——管理——规划”四维安全战略，并提供紧贴业务需要的安全最佳实践，为政府及企业的数据、系统、业务安全，为产业数字化升级保驾护航。腾讯安全产品与服务涵盖云计算环境与传统网络环境，帮助企业级客户实现便捷、高效、稳定的安全能力接入。

优势

腾讯 T-Sec 安全运营中心（以下简称“SOC 平台”），是腾讯安全面向政府、金融、制造业、医疗、教育等大型企事业单位推出的一款以安全大数据分析和可视化为基础的智能化安全运营平台。通过对海量数据进行多维度分析、预警，并对威胁做出及时的智能处置，实现企业全网安全态势可知、可见、可控的闭环。

SOC 平台是以云原生为基础，对公有云、私有云、互联网数据中心（iDC）、办公网等多云混合云场景下的统一安全运营与管理平台，基于对设备、网络、业务环境的深层安全监控、持续安全分析，结合对开放互联网的安全探测、感知，构建了云时代场景下，融合威胁防御、检测、响应溯源和风险预防的持续迭代式安全自适应机制。SOC 平台围绕安全运营和风险管理，自下向上构建了以日志信息、流量信息、资产信息的大数据层，以关联分析、UEBA、情报分析三大引擎的分析层，以风险资产及脆弱性管理、威胁管理为核心的业务层，以及以 3D 大屏、手机端等可视化为特色的展示层，以调查响应、联动处置、SOAR 等自动化技术的响应层。帮助客户全面提升安全运营的智能化、自动化和可视化水平，实现安全运营效率的突破。

T-Sec 安全运营中心的核心技术特点表现在：

- 以云时代的大数据技术构建平台基础：腾讯将多年的云业务和大数据分析处理能力赋能到 SOC 平台中，体现了云原生优势，包括多租户安全运营、海量数据处理、事件分析与调查、可横向扩展的数据处理性能。与传统技术相比，更灵活地适应公有云、私有云、iDC、办公场景对数据平台的需求。
- 以关联、行为分析、威胁情报三大引擎和云端安全能力构建核心检测与分析能力：基于安全大数据和 AI 安全智能技术，对海量多源数据的实时关联分析，实现事前和事中的攻击检测；对用户和实体等关键对象的行为进行细粒度的持续分析、建模，发现偏离基线的异常行为，自动还原攻击时间线、用户和实体风险优先级和行为上下文。全面提升企业安全运营中对外部和内部的高级威胁发现能力。与此同时，腾讯威胁情报拥有庞大的威胁情报库、黑产知识图谱、安全云库等，覆盖云、管、端以及第三方数据。基于腾讯云端安全告警数据和腾讯安全知识图谱，集成多种威胁分析检测引擎与事件自动化调查引擎的能力，提供威胁检测与事件分析服务。SOC 平台内置威胁情报分析引擎，将腾讯云端安全能力下沉到产品侧，与多源数据进行关联分析，高效、精准识别外部威胁。
- 协同生态，构建自动化响应处置闭环：SOC 平台支持与腾讯内部以及生态厂商产品协同，形成安全响应处置闭环能力。对腾讯侧支持与腾讯天幕实现网络流量旁路阻断，与腾讯云防火墙、腾讯 iOA 终端安全产品协同联动。与外部 SOAR 产品构建安全运营与自动化编排解决方案，通过 SOAR 对接多家厂家防火墙、Web 应用防火墙（WAF）、终端安全管控软件、主机安全软件等，从网络、主机、终端侧实现 XDR 联动防护响应。
- 多种可视化技术满足“平时”、“战时”态势呈现：SOC 平台提供丰富的可视化呈现手段，借助游戏可视化引擎技术构建 3D 态势感知大屏，集成 BI 能力的灵活可配的仪表板控制台，以及利用小程序在手机端的安全风险可视呈现。满足日常、作战等场景下随时随地的业务呈现需求。

挑战

随着云计算、大数据、移动、物联和智能技术的发展，客户面临的暴露面不断扩大，需要纳入管理和监测的数据源、安全资产对象范围也在增加。因此，SOC 平台除了不断给客户提供先进的检测、分析、响应技术，同时也需要扩大对安全管理对象的覆盖面，例如，对工控环境、车联网、5G 网络、物联网等领域多维度设备的安全日志、告警的汇总接入。

天融信

天融信在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

天融信科技集团创始于 1995 年，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国知名的网络安全、大数据与云服务提供商。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

优势

天融信态势分析与安全运营解决方案（以下简称“态势感知方案”）围绕国家监管、行业监管、等保合规、实战演练、安全运营等多种场景需求设计，基于态势感知核心平台，融合探针设备、威胁情报及安全服务，实现多源异构安全数据采集、海量安全数据深度分析、实时监测告警、协同化安全处置、资产管理、安全设备集中配置、威胁情报管理、多个维度进行全面的态势分析展示。

天融信态势感知方案技术特点如下：

- 大数据架构设计：采用大数据架构，具备拍字节（PB）级数据分布式存储计算、全文检索、内存计算、流式计算能力，支持存储计算能力在线横向扩展，千亿级数据可达秒级检索响应。
- 多源异构数据接入：主被动采集组件丰富，可全面接入自研及第三方探针，涵盖基础资产探测、漏洞扫描、攻击检测、僵木蠕虫检测、分布式拒绝服务攻击（DDoS）检测、网站攻击检测、网络行为审计、高级持续性威胁（APT）检测、终端威胁防御、蜜罐等各类安全设备。
- 智能威胁分析：基于数据关联分析、用户行为分析、AI 深度分析等多种可视化分析引擎提供丰富的分析模型，对海量安全数据挖掘分析，实现威胁画像、资产画像、用户画像，发现潜藏威胁，丰富威胁检测能力。
- 自动化响应编排：具备安全响应编排能力，根据每个场景历史研判经验进行响应编排，当符合场景的告警发生时自动触发响应任务，将人工处置过程自动化，极大提升安全研判效率。
- 安全设备集中管控：采用集中管控思路实现安全设备集中管理，包括策略集中下发、配置集中备份、状态集中监测、联动接口集中管理。

天融信拥有多地研发中心，态势感知方案团队目前在北京、西安、成都、武汉、长沙、深圳六地研发中心建立研发团队，能够满足快速支持本地化的研发工作。天融信在全国设有 60 多家分支机构，拥有 1300 多名技术人员，可以实现态势感知方案本地化快速交付，具备大型成熟交付案例。近 10 年来，天融信大数据产品线团队一直专注在态势感知及大数据领域，凭借自身实践和技术积累参与了 14 项态势感知及大数据相关标准及白皮书，其中 2 项国家标准，8 个部委行业标准，2 个部委白皮书，2 个政府机关标准。

挑战

- 与云平台的融合：各大企业和组织网络安全建设逐渐向云端迁移，网络边界被重新定义，态势感知方案需要适应环境变化，与不同类型的云计算平台进行高度融合，具备云化交付能力。
- 与新兴技术的融合：随着 5G、工业互联网、车联网能等新兴技术领域的发展，态势感知需要应对新领域的特定安全态势感知特点，满足客户不断新增的网络安全态势感知需求。

厦门服云

厦门服云信息科技有限公司（品牌名：安全狗）在 2021 年中国态势感知解决方案市场评估中处于主要厂商位置。

厦门服云信息科技有限公司成立于 2013 年，致力于提供云安全领域相关产品、服务及解决方案。公司目前拥有云安全、Web 应用安全、安全大数据三大核心产品线。在云安全领域，厦门服云依托（云）主机安全产品、公有云 SaaS 产品、私有云安全平台，结合容器安全、微隔离等最新技术，为公有云、私有云、混合云等各种复杂云环境下的用户提供整体解决方案及服务。在 Web 应用安全领域，厦门服云信息科技通过新一代混合式 WAF 产品及防篡改系统，为用户的网站安全上云提供了全面的保障。在安全大数据领域，公司基于已安装部署产品所获取的海量攻防数据，融合 AI 学习能力，构建多领域、多维度的安全态势感知平台，帮助用户有效预测风险、精准感知威胁、提升响应效率。

优势

安全狗啸天态势感知平台由安全大数据中台、纵深联动响应与自动化编排引擎、云工作负载保护平台（CWPP）探针、网络流量分析（NTA）探针和日志探针组成，具备集采集、监测、溯源、响应和预防于一体的新一代网络安全智能分析与联动处置平台。在产品形态上分别推出面向公有云的云磐 SaaS 平台、面向混合云的私有化部署设备，帮助用户实现安全数据可视化，发现潜在的内、外部风险，预测即将发生的安全威胁，并基于纵深联动响应技术体系联动相关安全产品，将安全控制点形成一道道控制面，实现自动化统一快速处置目标。

安全狗啸天态势产品在设计之初就针对云安全和云原生安全态势感知关键技术遇到的瓶颈问题做了相应的研究，并取得了以下技术优势：

- 针对传统方案在云原生场景下无法有效防护网页后门、无文件或无恶意软件攻击等新型云威胁，提出了基于 AI 算法的网页后门查杀技术、基于多维度运行时监控算法的云工作负载新型攻击检测技术，解决了变种、加密型网页后门检出率低和误报大的问题，实现对内存木马等新型攻击的准确发现和实时阻断。
- 针对传统方案无法满足混合云和云原生场景下所需的流量完整可视化和访问控制微隔离的需求。提出了一种基于流量跟踪算法的网络流量可视化绘制技术和一种基于业务策略模型的网络流量控制技术，支持基于应用、身份和威胁定制综合性的微隔离策略进行访问控制。
- 针对现有云上安全防护组件堆叠部署，以及组件自身的资源占用缺乏控制，可能影响业务应用正常运行的问题，提出了“N 合 1”轻代理开放式技术架构和一种基于云上安全防护组件的资源控制技术，实现了一个代理软件即可覆盖全栈安全需求，且自适应调节云安全组件的中央处理器（CPU）和内存占用情况，保障关键业务能够分配到足够的资源。
- 针对现有整体态势感知方案缺乏合理的度量指标和算法，往往停留在对攻击、访问、漏洞进行可视化展现层面的问题，创新提出基于“四色”分级预警机制的网络安全整体态势度量分析算法和一种基于 Hbase 行键的高性能查询方法,实现了在海量安全数据的基础上近实时计算出网络安全态势指数对应的整体安全态势等级，可为领导快速决策和安全管理所需可视化分析和指挥调度提供支撑服务。
- 针对安全威胁联动响应无法形成联合发现和抵御的问题，采用“大基座”开放方式设计思路，以“统一纵深联动响应 API 接口层开放体系”为技术基础，构建覆盖主机侧、网络侧和容器侧的纵深联动响应技术体系，联动主机安全模块、容器安全模块、网络微隔离模块和漏洞补丁模块形成联合发现和联合抵御高级威胁的效果。

安全狗态势感知产品线在厦门、成都两地设有研发中心，产品已应用于包括国家部委、央企、世界 500 强等在内的上百家大型客户，以及数千家中小企业客户，涵盖了能源、金融、教育、医疗、互联网、电信运营商等多个行业。

挑战

面对各种各样的网络攻击，在防御上实现攻击入侵自动化联动响应是企业安全自始至终的核心诉求，这就需要与众多安全产品进行“跨厂商、跨产品”的对接协同，其面临的最大挑战就是生态体系丰富程度难以形成规模。安全狗自身重点专注与主机侧和容器侧的自动化响应能力的建设，以及部分网络侧第三方安全产品的联动驱动的供应，更多的希望通过探索一条技术体系开放、标准规范统一、商业模式创新的道路，吸引各个生态厂商主动参与并积极拥抱协同对接，才能形成较为丰富的联动响应生态体系，这项工作的推动极其艰巨。

新华三

新华三在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

新华三集团深耕网络安全领域近二十年，致力于为国家网络安全领域提供完善的产品、解决方案及专业安全服务，同时为各行业搭建优质安全人才培养体系。新华三拥有网络安全专业人才千余人，为客户提供从顶层设计到底层基础设施的“云-网-边-端”一体化安全解决方案，基于全球网络安全的最新发展趋势，在业界提出从被动防御向主动防御的主动安全理念。新华三正面向未来打造新一代网络安全产业链，构建网络安全主动防御体系，为中国的数字经济发展保驾护航。

优势

新华三依托态势感知平台强大的数据分析、通报溯源、运维管理能力，打造了“云网安”一体的综合安全防护体系。其主要特点包括：

- 基于 AI 的安全风险分析能力：利用人工智能技术，可以对海量的网络日志、威胁情报等信息进行自动分析处理与深度挖掘，对隐藏在网络流量、资产设备及系统日志中的正向样本和恶意样本进行分类统计，从海量数据中提取出真正有用的信息，针对全过程攻击链中攻击者留下的任意线索进行多维拓展，可视化绘制出完整的攻击链条，从而提前进行防范，实现对威胁全过程的可视化溯源追踪。
- 自动化、全闭环响应处置能力：新华三态势感知致力于打造智能安全运营平台，针对风险的各个维度，通过剧本自定义编排与不同的网络、安全、终端、平台类产品实现自动化联动，实现安全的精准防御。针对网络中普遍存在的漏洞，内置专门的漏洞管理引擎实现漏洞发现、漏洞处理、漏洞验证三个阶段的闭环管理，极大减轻安全运营团队运维压力。具备完整的工单流程，安全事件自动触发产生工单，自动提醒责任人处理超期工单，处理过程全部存档，保证流程的规范性。
- 云安全大脑能力：云安全大脑是面向云端安全管理场景的安全 SaaS 服务，将安全设备通过云通道一键接入云端，实现实时设备状态监控、配置管理、策略管理，配合云安全大脑后端的态势感知分析模块，收集设备侧的各类信息实现威胁分析、安全态势呈现以及事件闭环处理。极大节约安全设备运维成本、缩短事件处置时间、快速定位威胁风险，实现“安全大脑”闭环决策，助力企业快速高效地将安全能力落地。

新华三能够提供 7*24 小时的远程服务，并拥有上百人的专业安全服务团队，涵盖网络安全、云安全、移动安全、应用安全、大数据安全、工控安全、可信计算及物联网安全等各领域。新华三坚持以总部专家对项目进行交付，并在 7 大区域（杭州、北京、合肥、成都、沈阳、广州、郑州）设置安全服务专员，总部专家保证了项目的交付质量，区域服务工程师能够对用户的需求进行及时响应。

挑战

- 态势感知尚无统一的标准定义：不同的行业对态势感知的认知各异；不同的用户对态势感知的认知更是大相径庭。这样的认知导致态势感知实现上的不统一，只能基于厂商自己的理解与客户调研进行产品开发，对客户来说无法标准交付。

- 态势感知生态建设需长时间磨合：企业网络中存在大量资产，且资产类型、协议、端口多种多样，如果要实现全方位的监测及防御，就必须采集所有资产的数据，指挥所有能联动的设备。因此，建立完善的生态圈很重要，通过生态建设破除壁垒，实现不同资产的“合纵连横”。

亚信安全

亚信安全在 2021 年中国态势感知解决方案市场评估中处于领导者位置。

亚信安全作为“懂网、懂云”的安全公司，致力于护航产业互联，成为在 5G 云网时代，守护云、网、边、端的安全智能平台企业。以安全数字世界为愿景，以护航产业互联为使命，亚信安全在云安全、身份安全、终端安全、安全管理、高级威胁治理和威胁情报等领域拥有核心技术。同时基于“安全定义边界”的发展理念，亚信安全以身份安全为基础，以云网安全和端点安全为重心，以安全中台为枢纽，以威胁情报为支撑，构建“全云化、全联动、全智能”的产品技术战略，赋能企业在 5G 时代的数字化安全运营能力。

优势

亚信安全态势感知采用先进的大数据架构，基于模块化、松耦合、灵活组装及快速定制四类要求，不断研发上层应用能力，面临层出不穷的安全威胁，借助大数据安全分析技术、机器学习和数据挖据算法，能够克服海量数据的存储、索引和运算的瓶颈，智能洞悉信息与网络安全的态势，主动、弹性地去应对新型复杂的威胁和未知多变的风险。亚信安全拥有众多自主创新态势感知技术与能力，在大数据分布式监测、智能格式解析、统一数据超集、UEBA 流式行为识别、攻击透视轨迹视图、安全威胁情报云、场景化集成框架等领域持续耕耘，并拥有多项专利技术，保持在安全态势感知技术的行业创新性。

亚信安全态势感知平台是集安全运营与态势感知为一体的全能平台，以安全大脑为核心，为用户带来进阶式安全赋能。平台能够全面采集企业各类安全数据，形成安全数据湖，并应用内置智能引擎对安全数据进行统一处理分析，实现对网络攻击行为、安全威胁事件等网络安全问题的发现和告警。针对潜伏性高级持续威胁及新型组合式网络攻击，提供集“检测—预警—监测—响应—防护—分析—溯源”为一体的立体式防御能力。

亚信安全态势感知平台立足于企业网络安全业务场景，结合最新的信息安全检测技术，协助用户构建安全监测中心、安全分析中心、安全响应中心、安全资产中心、知识情报中心等中台能力，形成以安全数据为中心的安全运营一体化工作落地。

- 全网资产测绘管理：采用“主动扫描+被动获取”的模式，对网络空间资产数据进行全面、高效、精准的识别和梳理，能够结合资产的漏洞、脆弱性信息，帮助客户准确评估企业资产安全风险，高效应对潜在威胁，为后续安全态势分析、响应处置提供有力支撑。
- 融合建模智能分析：通过提炼安全要素信息，对各类安全数据进行情境关联，建立日志、流量、告警、漏洞、行为、情报等数据模型，融合高级统计、数据挖掘、行为分析、机器学习、人工智能等新兴技术，依托于平台强大的分析能力，帮助客户实现全业务分析场景落地。
- 主动出击威胁狩猎：通过典型的攻击链模型对攻击的全过程进行监测，能够分别对攻击者与受害者画像进行刻画，同时结合亚信安全全球化的威胁情报数据进行云网端的联合溯源分析，为客户提供安全管理主动式防御战略。
- 剧本编排自动响应：基于安全剧本的自动化编排能力，实现人员、流程、技术的无缝融合，充分结合人机能力，广泛集成全行业安全防护基础设施，构筑企业自动化运维体系，打造智能安全响应生态。

亚信安全围绕着中长期战略和行业增长机会，看好未来网络安全态势感知平台发展机遇，主动进行研发体系和服务体系的建设拓展。团队持续加大对大数据分析前沿技术的应用，加强安全服务及运营团队建设，以技术输出为导向，保障项目的整体交付效果，提升安全管理产品能力及客户价值实现。

挑战

目前客户普遍采用传统的网络安全需求指导态势感知平台建设，与云安全、零信任等新型安全体系相适应相对滞后。对各行业客户或企业客户而言，由于各行业建设标准、技术规范等没有形同统一规范，导致客户建设目标差异化极大，需要构建多线版本才能应对建设需求，但同时部分项目存在非合理的个性化需求，对厂商而言，在提高建设交付难度，成本增加的同时容易给人带来“产品无用”的印象。

附录

解读 IDC MarketScape 图

基于该分析的目的，IDC 将成功的潜在关键因素分为两大类：能力和战略。

Y 轴反应了厂商目前的能力、服务菜单、及该厂商如何满足客户需求。能力范畴集中讨论企业和产品此时此刻的能力。在该范畴中，IDC 的分析师将着眼于那些使厂商能够实现其在该市场中已确定的发展战略的发展/交付能力。

X 轴或策略轴分析了厂商未来的战略将如何满足客户未来 3 到 5 年的需要。战略范畴集中讨论基于未来 3 到 5 年的产品、细分用户、业务和市场推广的高层决策和基本假设。

气泡的圆心位置反映了企业在能力和战略两方面的综合实力，气泡的大小反应了该企业 2020 年网络安全态势感知标准平台类产品的直接收入，不包括安全探针、定制化开发收入和安全服务收入，但企业具体营收数字并不会直接体现在本次报告中。

IDC 认为，全球企业正在积极推进数字化转型进程，云计算市场（包括公有云、私有云）发展迅速，尤其是国内市场对云计算的认可度持续提升，越来越多的企业将业务迁移到云端，云安全的重要性以及软件即服务（SaaS）模式的态势感知解决方案受到企业级客户的更多关注。因此，在本次厂商评估中，无论是缺少云平台支持能力的传统安全厂商，还是缺少传统网络环境支持能力的云服务提供商，都将由于各自部分能力或战略的缺失，影响其在本次评估中的最终整体表现。

IDC Marketscape 研究方法

IDC MarketScape 的选择标准、权重和厂商得分代表了 IDC 对市场和特定厂商的判断。IDC 的分析师通过与市场领导者、参与者和最终用户进行有组织的讨论、调查和访谈，来评估厂商，并制定了一系列标准特征。市场权重是基于用户访谈、买方调查、以及 IDC 专家审查组对各个市场的意见。基于各厂商的得分，IDC MarketScape 中的厂商位置，对厂商的详细的调查和访谈，公开信息和最终用户反馈等，IDC 的分析师提供了针对各个厂商特征、行为和能力的，精确的、一致的评估。

市场定义

网络安全态势感知解决方案是由网络安全分析、情报、响应和编排（AIRO）四类技术组成的，是安全和漏洞管理（SVM）市场的演变，是一套专注于允许组织确定、解析和改进公司风险态势的全面的解决方案，是成熟安全架构的基本组成部分。该市场中的产品（无论是硬件，软件还是服务）包括那些创建、监控和实施安全策略的产品以及确定给定设备的配置、结构和属性的产品。网络安全 AIRO 产品还包括执行评估和漏洞扫描、提供漏洞修复和补丁管理、聚合和关联安全日志以及提供综合安全管控类的产品。这个市场包含三个独立但共生的市场：

- 分析和情报（输入）
- 响应（行动）
- 编排（自动化）

这三个子市场可以是独立的，但它们在企业使用方式上也存在相当大的重叠。

分析和情报子市场包括安全情报和事件管理（SIEM）解决方案、威胁分析产品、威胁情报产品、蜜罐产品。响应子市场包括取证和事件响应产品、策略和合规解决方案、GRC（治理、风险管理、法律遵从）。编排子市场由编排和自动化相关工具集组成。

战略和能力标准

本节中提出的标准用于评估本次研究中的参与供应商。权重反映了每个标准对终端安全检测与响应产品/工具买家的相对重要性。表 1 侧重于厂商战略（即未来能力的规划），表 2 侧重于厂商目前的能力。同时，战略和能力构成了 IDC MarketScape 图表的两个轴（参见图 1）。

表 1

关键能力指标：中国态势感知解决方案市场

能力指标	具体定义	权重
客户满意度	厂商具备完善的项目交付流程、制度和售后服务评价体系；行业客户对厂商售后服务质量和延续性的评价。	8%
客服交付	厂商具备 24 小时售后服务能力，并具备全面的区域覆盖；建立全面的客户分级体系。	7%
服务范围	厂商具备良好的最终客户品牌认知；能够为客户进行整体安全建设规划；具备多样化的托管安全服务模式和内容。	16%
客服产品	厂商具备完善的客户服务团队建设和售后技术支持能力，能够为重点行业客户提供定制化支持。	8%
产品或解决方案及其功能特性	厂商态势感知产品/解决方案具备对传统网络、云计算、工业互联网、5G、智慧城市等不同业务场景的支持能力；在分析、情报、响应、编排等基础能力方面有良好的展现；具备强大的管理能力且界面友好。	52%
投资组合优点	厂商态势感知相关技术专利及第三方评测成绩的情况，能够通过自主研发、生态合作等方式打造全面的安全防护体系，实现态势感知平台与其他终端安全、网络安全、威胁情报等相关产品的协调联动，为客户打造安全闭环。	9%
合计		100%

来源: IDC, 2021

表 2

关键战略指标：中国态势感知解决方案市场

战略指标	具体定义	权重
交付	厂商产品/解决方案在国内外能够获取充足的资源支持，以保障产品的可交付性；需要具备强大的扩展能力以适配不同规模用户的安全态势需求；对国内外主流云计算平台进行有效适配，并能够为用户提供多种形式的托管安全服务。	27%
产品或解决方案及其功能特性	厂商产品/解决方案在分析、情报、响应、编排能力等方面具备清晰且可行的发展规划；在新兴技术和业务场景安全需求方面的规划具备前瞻性和创新性。	27%
创新	对厂商技术创新性的综合评价。	6%
增长	厂商产品/解决方案在研发、营销、生态建设等方面的资源投入和增长。	15%
研发速度、生产效率	厂商态势感知相关产品及研发团队的建设规划和发展预期；需要具备深厚的技术和经验积累，在行业内具备广泛的影响力和口碑。	20%
其他	厂商在监管态势感知、企业运营态势感知的市场布局。	5%
合计		100%

来源: IDC, 2021

进一步研究

相关研究

- *Market Analysis Perspective: Worldwide Cybersecurity, 2021*（IDC #US48165821, August 2021）
- *Worldwide Cybersecurity AIRO and Tier 2 SOC Analytics Forecast, 2021 – 2025: Is the Pathway to XDR Paved with Good Intentions?*（IDC #US45384920, August 2021）
- *中国网络安全市场新趋势——零信任市场研究*（IDC #CHC47929221，2021 年 6 月）
- *Worldwide Cybersecurity Analytics, Intelligence, Response, and Orchestration Forecast, 2021 – 2025: Legacy SIEM and Vulnerability Management Tech — How They Will Survive and Hopefully Continue to Thrive*（IDC #US47081021, June 2021）
- *IDC MarketScape：中国态势感知解决方案市场 2019 年厂商评估*（IDC #CHC44880419, 2019 年 10 月）

大纲

本次研究对象包含了在中国态势感知解决方案/平台市场具备一定技术水平和市场规模，并且在该领域有持续投入规划，具备不断完善产品和服务能力的主流厂商。厂商类型涵盖国内综合型安全厂商、云服务提供商及新兴态势感知解决方案/平台提供商等。IDC 针对入选的态势感知解决方案/平台安全厂商的能力和战略进行综合评估，评估标准包括收入规模、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方面。各维度根据市场情况进一步划分为若干细分项，并配以不同权重，从而形成 IDC MarketScape 综合评分体系，通过 IDC 分析师针对各个厂商和大量最终用户的深入访谈，综合分析并确定各厂商在 IDC MarketScape 中的相对位置，并探讨厂商的特点和战略，总结发展趋势，为终端用户选择态势感知解决方案/平台提供商提供参考。

“近些年，态势感知解决方案受到中国网络安全市场的持续关注，并成为驱动中国 IT 安全市场快速增长的重要因素之一。经过大量项目的不断打磨，无论是企业级客户还是技术提供商都对态势感知解决方案的核心能力和应有价值有了更清晰和理性的认识。基于安全分析、情报、响应和编排能力构建的态势感知解决方案/平台正在成为众多企业主动安全防御体系的“智慧大脑”。虽然态势感知相关的诸多技术和功能模块，特别是自动化响应和编排能力还有待完善，但随着市场需求的持续火热，态势感知解决方案/平台必将快速成熟，并在企业整体网络安全防护中体现更高价值。IDC 希望通过本次研究帮助技术买家明确态势感知解决方案的核心能力和发展方向，并综合展示目前中国市场主要态势感知解决方案提供商的各自特点和优势。”——IDC 中国网络安全市场研究经理赵卫京表示。

关于 IDC

国际数据公司（IDC）是在信息技术、电信行业和消费科技领域，全球领先的专业的市场调查、咨询服务及会展活动提供商。IDC 帮助 IT 专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略。IDC 在全球拥有超过 1100 名分析师，他们针对 110 多个国家的技术和行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。在 IDC 超过 50 年的发展历史中，众多企业客户借助 IDC 的战略分析实现了其关键业务目标。IDC 是 IDG 旗下子公司，IDG 是全球领先的媒体出版，会展服务及研究咨询公司。

IDC China

IDC 中国（北京）：中国北京市东城区北三环东路 36 号环球贸易中心 E 座 901 室
邮编：100013
+86.10.5889.1666
Twitter: @IDC
blogs.idc.com
www.idc.com