# 安全信息和事件管理魔力象限分析报告

发布日期：2020 年 2 月 18 日 - ID：G00381093 - 阅读时间约 72 分钟

作者：Kelly Kavanagh、Toby Bussa、Gorka Sadowski



---

安全和风险管理的领导者越来越多地寻求支持早期攻击检测、调查和响应的安全信息和事件管理解决方案。用户应在高级 SIEM 功能与运行和调优解决方案所需的资源之间实现平衡。

## 市场定义/描述

安全信息和事件管理（SIEM）市场根据客户实时分析安全事件数据的需求而定义，有助于及早发现攻击和数据泄露。SIEM 系统能够对安全数据进行收集、存储和调查，并支持威胁缓解和报告功能，以实现事件响应、取证及监管合规性。本魔力象限分析报告中所含供应商的产品旨在实现这一目的，他们会主动向安全购买中心推销和出售其产品。

SIEM 技术集合了由安全设备、网络基础架构、主机和端点系统、应用及其他服务生成的事件数据。主要数据源为日志数据，但 SIEM 技术也可处理其他形式的数据，如网络遥测数据（即数据流和数据包）。可将事件数据与用户、资产、威胁和漏洞方面的情境信息结合起来。数据可能是标准化的数据，因此可分析各种来源的事件、数据和情境信息，以实现网络安全事件监控、用户活动监控和合规性报告等特定目的。该技术可实时分析相关事件，以针对历史分析进行安全监控、查询和长期分析，同时还支持事件调查、管理和报告 - 比如为满足合规需求而进行的调查、管理和报告。

# 魔力象限

图 1. 安全信息和事件管理魔力象限


来源：Gartner（2020 年 2 月）

## 供应商优势和注意事项

## AT&T Cybersecurity

AT&T Cybersecurity 是 AT&T Business 的子公司，总部位于德克萨斯州达拉斯。AT&T Cybersecurity 的 SIEM 解决方案是 Unified Security Management (USM) Anywhere，它作为软件即服务（SaaS）解决方案提供。该解决方案与 SIEM 一起打包了其他几个安全元

素，包括资产发现、漏洞评估、面向网络和云的入侵检测系统（IDS）以及端点检测和响应（EDR）。作为内部软件部署的 USM Appliance 也可提供，而且仍旧受支持；不过，该供应商会继续将更多的精力放在 USM Anywhere SaaS 产品上。USM 客户可以通过 API 密钥连接到 Alien Labs Open Threat Exchange (OTX)，以获得其他威胁指示器（IoC）和威胁情报共享功能。

AlienVault USM Appliance 和 Anywhere 产品按分析的数据量(每月 GB 数)获得许可，并且仅以订阅的形式提供。对于希望访问 USM 中央管理控制台 - USM Central 的托管安全服务提供商（MSSP）合作伙伴而言，也提供有相应的许可；该控制台可在多个 USM Anywhere 部署中提供统一的仪表板。

过去 12 个月的产品发展包括在 USM 产品组合中增加了 EDR 代理，旨在针对主要操作系统提供威胁可视性和自动响应操作。目前，USM Anywhere 可提供面向 Google Cloud 的威胁可视性和响应功能，而且为执行调查的分析师提供了增强的案例管理功能。

金融服务和医疗保健垂直行业的中小型企业（SMB）需要 SIEM 即服务（SaaS SIEM）交付模型（其中绑定的安全控件不要求使用庞大的数据库、应用监视或高级分析），应考虑 AT&T Cybersecurity 的 USM Anywhere 产品。

## 优势

- **部署：**以 SaaS 的形式部署，与内部部署的 SIEM 相比，加上用于检测和仪表板的预定义内容，可提供相对快速的部署和初始运营。
- **运营：**供应商会频繁更新检测内容。根据 AT&T Alien Labs 威胁情报小组的调查结果，USM Anywhere 的检测规则和仪表板每周会更新一次。
- **产品：**AT&T Cybersecurity 针对其自身技术提供了强大的集成功能，用以实现端点代理部署/管理、网络入侵检测、漏洞扫描/资产发现和威胁情报等。该公司产品的原生文件完整性监控（FIM）和 EDR 功能高于市场平均水平，不过，相比许多其他竞争对手，其对第三方解决方案的支持有限。
- **产品：**能够应对在多个地理区域有数据驻留要求的客户，可以监控 13 个 Amazon Web Services (AWS) 区域，而且可以通过 USM Central App 进行中央管理。在 9 个国家或地区支持数据驻留，包括美国、爱尔兰、德国、日本、澳大利亚、英国、加拿大、印度和巴西。

## 注意事项

- **对市场的了解：**AT&T Cybersecurity 针对安全监控，必须管理一个复杂的进入市场的方法。AT&T Cybersecurity 为最终用户提供了 SaaS SIEM 和托管安全产品；不过，该公司要与许多第三方服务提供商竞争，后者通过 USM Appliance 向最终用户提供托管服务。AT&T Cybersecurity 必须就其目标买家以及这些买家如何获得其监控解决方案的托管服务支持，发出明确的营销消息。此外，供应商必须平衡其在与 MSE 买方相关的功能以及那些与托管服务提供商相关的功能上的投资，因为这些目标市场通常在功能和特性上具有不同的优先级。
- **产品：**该供应商欠缺与企业 SIEM 部署相关的开箱即用集成功能，或者说这方面的功能比较有限。USM Anywhere 未与用于用户身份验证的身份存储库相集成，也未与 ERP 解决方案、第三方的大数据平台或安全编排、自动化和响应解决方案相集成。通过 AlienApps 生态系统实现的其他集成也较为有限。对基础设施即服务 (IaaS) 监控的支持取决于是否在 AWS、Azure 及 Google Cloud Platform (GCP) 中部署了 USM Anywhere 传感器。通过 AlienApps 监控 SaaS 的功能仅限于 Microsoft Office 365、Google G Suite、Box、Okta 及少数几家其他供应商。
- **产品：**与许多竞争对手相比，USM Anywhere 对用户监控的支持比较基本。该产品不提供原生用户和实体行为分析 (UEBA) 功能，也不提供与第三方 UEBA 解决方案的集成。
- **产品：**USM Appliance 和 USM Anywhere 的功能不对等，该供应商将更多的开发资金投入到了 USM Anywhere 上。
- **客户体验：**我们根据 Gartner 通过询问获得的客户反馈，以及 Peer Insights 和供应商的评论，对 AT&T Cybersecurity 所提供的服务、支持、日志管理/报告以及实时监控功能褒贬不一。

## Dell Technologies (RSA)

RSA 是 Dell Technologies 的子公司，其总部位于德克萨斯州朗德罗克。该公司在马萨诸塞州贝德福德、英国的布拉克内尔、新加坡、日本东京和巴西设有主要办事处。

RSA NetWitness 平台 (RSA NWP) 由几个组件组成：RSA NetWitness Logs、RSA NetWitness Endpoint、RSA NetWitness

Networks、RSA NetWitness UEBA 和 RSA NetWitness Orchestrator。该公司在 UEBA 方面的功能来自于 2018 年对 Fortscale 的收购，而 RSA NetWitness Orchestrator 安全编排自动化和响应（SOAR）则是 OEM 了 Demisto SOAR 的解决方案。

该公司的产品许基于工具的性质，RSA NetWitness Logs 定价（包括运行 SIEM 所需的所有组件）基于数据量来确定。（所有新客户默认采用永久性许可或基于一定期限的计量许可。）其传统定价模型可通过设备容量（物理设备的容量）进行许可。客户可以添加其他付费组件，例如：

- RSA NetWitness Endpoint - 基于端点数量
- RSA NetWitness UEBA - 基于所监控用户的数量
- RSA NetWitness Network - 基于计量的数据量或传统模式基于设备容量
- RSA NetWitness Orchestrator（此次调研中对 Demisto OEM 进行了评估）- 基于安全分析师的数量

客户可以混合使用设备许可与计量许可，以实现整个部署架构的精细化实现容量增长。

于 2019 年 4 月推出的 RSA NWP v11.3 针对 RSA NetWitness Endpoint 进行了一些改善，同时引入了 RSA NetWitness Endpoint 特定的 UEBA 模型，以及 SIEM 和 UEBA 解决方案之间更紧密的集成。

对于具有成熟安全运营能力的企业而言，如果希望部署具有端点、网络和 UEBA 模块以及 SOAR 功能，支持分析、取证/捕获和报告/合规性的单一供应商 SIEM 平台时，则应考虑使用 RSA NetWitness 平台。

## 优势

- **部署：**组织可以混合搭配使用设备、虚拟设备和软件来构建功能堆栈，以实现灵活的部署和水平可扩展性功能。
- **产品：**这是一项成熟的技术，非常适合高级威胁防御（ATD）用例，这要归功于其中的多阶段分析功能，其中包括 RSA NWP 广泛的其他原生集成解决方案组合，可提供端点和网络之间无处不在的视图和分析功能。
- **产品：**RSA NWP 提供了一个多阶段分析引擎，该引擎可跨端点、网络和用户提供令人关注的，无监督化建模功能。

- **产品：**RSA NWP 具有强大的功能集，支持取证和威胁捕获，可在任何位置访问广泛的 RSA 技术堆栈中的取证工件，例如：从端点获取运行进程列表，或者 NWP 用户界面 (UI) 中的原生数据包捕获 (PCAP) 分析。
- **部署/支持：**RSA 提供可直接从 NWP 控制台访问的 RSA Live，以访问所有的 RSA NWP 内容。
- **销售执行：**RSA 在全球范围内拥有广泛的渠道合作伙伴和服务提供商生态系统，可为 NWP 提供原生支持，以进行集成、管理和/或运营。

### 注意事项

- **产品战略：**RSA 的 NWP SOAR 战略基于不稳定市场中的 OEM 关系（在收购 Palo Alto Networks 之前为 Demisto，之后为 Threat Connect。RSA 表示他们将提供数年的 Demisto 支持)。客户应确认 RSA 的 SOAR 合作伙伴是否符合其要求。
- **产品：**相比其竞争对手，该公司产品的 UEBA 功能所提供的模型较少。RSA NetWitness 的 Network UEBA 模型预计在 2020 年第一季度发布。
- **部署/支持：**该供应商不提供作为 SaaS 产品的 RSA NWP，不过某些 RSA 合作伙伴可提供该功能。希望由供应商提供 SaaS SIEM 的组织可能会发现，该产品具有局限性，不过应会对其云安全发展路线图感到满意。
- **产品：**与面向中端市场的竞争对手相比，RSA NetWitness 平台对于不太成熟的买家而言，部署和运营更加复杂一些。

## Exabeam

Exabeam 的安全管理平台 (SMP) 由七个产品组成：Exabeam Data Lake、Exabeam Cloud Connectors、Exabeam Advanced Analytics、Exabeam Threat Hunter、Exabeam Entity Analytics、Exabeam Case Manager 和 Exabeam Incident Responder。SMP 可以作为内部部署软件提供，也可以作为基于云的 SIEM 提供，由 Exabeam 托管和管理。内部部署可采用多种外形规格：加固的物理设备、虚拟设备、Docker 化的容器，以及私有或公有云部署（在 Amazon、Google 和 Azure 中)。此外，内部部署也可以包含多个外形规格选项（即物理、虚拟和云)。

Exabeam 的许可和定价模型非常简单。每个 SMP 产品均以一年或三年的订阅期限出售，并按组织中的员工人数定价，但 Entity Analytics 除外，后者按所监控资产的数量定价。

在过去的 12 个月中，Exabeam 对 SMP 进行了一些增强：

- 通过单个 UI 集成了 Advanced Analytics、Threat Hunter、Case Manager 和 Incident Responder
- 通过云交付的威胁情报服务
- 与 MITER ATT&CK 框架更好地保持一致
- 改进了警报分类，通过警报支持更为丰富的用户和实体上下文
- 评分的活动与报警建立关联

对于拥有安全运营团队的企业而言，如果他们希望部署能够以简单方式交付复杂安全用例、定价结构不是基于数据量且具有原生 UEBA 和 SOAR 功能（均为付费功能）的模块化 SIEM，则应考虑使用 Exabeam SMP。

**优势**

- **部署/支持：**SMP 支持分阶段采用功能，这些功能可以从核心 SIEM（Data Lake、Advanced Analytics、Case Manager）开始，然后扩展到面向 SOAR 的 Incident Responder 或面向 SaaS 和 IaaS 用例的 Cloud Connector。
- **产品：**Exabeam SMP 为用户、实体和身份的监控提供了坚实的基础。这一基础借助核心分析模块（Advanced Analytics）通过应用中的原生 UEBA 功能（例如对等组分析和行为偏差监控）而实现。
- **产品：**Exabeam 的 Smart Timeline 利用机器学习（ML）在时间线视图中组织相关的日志和事件，进而可为经验不足的 SIEM 用户提供支持，从而简化了调查和响应活动。
- **销售：**Exabeam 的定价模式很简单。这种定价模式有助于减少购买摩擦，因为它不是基于数量，而是基于组织中使用每种产品的员工人数，但 Entity Analytics （按资产数量进行许可）除外。

- **对市场的了解：**通过市场营销活动，Exabeam 在 Gartner 客户群体（主要在北美）中表现出强劲的增长和知名度。
- **客户体验：**从 Gartner 客户问询、Peer Insights 和供应商样板客户的反馈来看，客户对该公司产品的几个方面给出了积极评价，例如部署和支持服务、评估和合同谈判，以及行为分析的超常规标记。

### 注意事项

- **对市场的了解：**尽管 Exabeam 在多个地区都开展有销售业务，但其买家主要来自于北美。北美以外的买家应验证其组织所在位置的销售、专业服务和支持覆盖情况（无论是该公司直接还是通过其合作伙伴提供）。
- **对市场的了解：**Exabeam 仍在持续构建其合作伙伴网络，尤其是在托管 SIEM 等服务方面。寻求“SIEM + 服务”支持模式的买家应确认 Exabeam 已将其确定为经过培训/认证的合作伙伴的公司，并且可以满足运营和用例开发要求。
- **营销执行：**Exabeam 应该更好地定义与特定垂直行业中的买家相关的功能，这些特定垂直行业中的挑战可能与一般购买组织（如能源和公用事业）所面临的挑战不同。寻求垂直行业特定功能的买家应确认 Exabeam SMP 是否具有适当的覆盖范围 - 例如，以开箱即用检测和合规报告模板的形式针对其垂直行业特定的内容。
- **客户体验：**基于 Gartner 客户问询、Peer Insights 和供应商样板客户的反馈，Exabeam 可以改善其产品的集成和部署、现有规则自定义的简洁性、预定义报告以及 SMP 中产品的质量和稳定性。

## FireEye

FireEye 的总部位于加利福尼亚州米尔皮塔斯。FireEye Helix 是 FireEye SIEM 的核心组件。Helix 与 FireEye 的电子邮件、网络、端点和云安全等其他单独许可的解决方案相集成。FireEye 还提供了 Expertise On Demand，该产品所提供的服务有助于调优规则、调查警报、补充安全团队能力、应对违规行为。FireEye Helix 作为 SaaS SIEM 提供，托管在 AWS 中，而且由 FireEye 负责管理。集成的 FireEye 安全解决方案也可以在云中运行，不过客户也可以选择在内部环境中运行，即在混合环境中的物理系统或虚拟系统上运行。FireEye Helix 仅可以以订阅的形式提供，价格基于每秒事件数（EPS）确定，最低为 100 EPS，最高为 150,000 EPS。

在过去的 12 个月中，FireEye 添加了一些增强功能，例如 IoC 情境丰富、用于检测和响应的编排功能，以及 Expertise On Demand。

此外，用于云到云直接 API 集成的云集成门户不需要客户部署的任何设备。

利用 FireEye 电子邮件、网络、端点和/或云安全产品的组织，或希望通过单个安全解决方案实现端到端检测和响应功能且可选配托管服务的组织，应考虑使用 FireEye 的产品。

## 优势

- **产品：**Helix 包含由 FireEye 预定义好的查询功能，该功能为调查提供了指导。FireEye Security Orchestrator 提供了更广泛的运行手册和响应集成功能。
- **产品：**FireEye 提供了广泛的开放式 API，这些 API 支持通过 UI 访问提供的所有元素，从而使用户能够开发集成功能并以编程的方式与解决方案进行交互。
- **部署/支持：**Helix 平台具有广泛的威胁检测规则集，这些规则由 FireEye 管理，并基于该供应商强大的威胁情报数据采集功能进行每天更新。
- **产品：**FireEye Endpoint（之前为 HX）、FireEye Network（之前为 NX）和 FireEye Email 产品的集成，将端点、网络和电子邮件取证进行了整合，为基于取证数据的调查提供了丰富的功能。FireEye 威胁情报已完全集成其中，而且其他 FireEye 工具能够支持证据收集（Evidence Collector）和响应操作（FireEye Security Orchestration）。
- **部署/支持：**借助 FireEye 的托管检测和响应服务产品，客户可以使用 Helix 平台执行自己的搜索和调查，同时能够获得供应商的 24/7 全天候监控和响应支持。
- **产品：**FireEye 的样板客户对其产品的大多数功能都给与了积极的评价。通过问询和 Peer Insights，从 Gartner 客户获得的反馈信息较为有限。

## 注意事项

- **产品：**在对 IaaS 和 SaaS 威胁检测的支持方面，该供应商产品的成熟度低于比多个竞争对手。Helix 为 AWS 和 Microsoft Office 365 提供了检测规则，但尚未为其他流行的 IaaS 和 SaaS 应用提供检测规则。

- **部署/支持**：Helix 的事件获取功能没有竞争对手的产品成熟。Helix 缺乏事件源的自动发现功能，而且不提供最终用户可用于开发新解析器的功能。日志管理功能取决于底层 AWS 平台的可用功能。客户应验证 AWS 平台上可用的数据管理功能是否足以满足他们的要求。
- **产品**：与较成熟的竞争对手相比，该供应商产品的合规性报告功能较为有限 - 举例来说，该供应商的产品仅提供了针对《支付卡行业数据安全标准》(PCI DSS) 和《医疗保险可移植性和责任法案》(HIPAA) 要求的仪表板。
- **产品**：FireEye 正在发展其技术合作伙伴生态系统，但并非所有集成都可以在整个 FireEye 产品组合中提供。潜在客户应验证 FireEye 的产品通过 Security Orchestration、Helix 平台或 FireEye Network、FireEye Endpoint 或其他产品提供的第三方集成，是否支持所需的用例。

## Fortinet

Fortinet 的总部位于加利福尼亚州桑尼维尔，在全球设有 58 个办事处，在佛罗里达州森赖斯、法国索菲亚、悉尼、新加坡和东京设有区域性办事处。

Fortinet 的 SIEM 解决方案 FortiSIEM 包括：

- FortiSIEM Advanced Agent - Windows 和 Linux 代理，具有 FIM 和 EDR 功能
- FortiGuard IoC - 付费威胁情报订阅源
- FortiInsight - 通过收购 ZoneFox 而获得的付费 UEBA 工具

Fortinet FortiSIEM 是 Fortinet Security Fabric 的一部分。这有助于提升多个 Fortinet 产品组合解决方案（如 Fortinet FortiSandbox）之间的协作和集成，以实现更多的多工具间集成的用例。

FortiSIEM 基于范围内的资产数量（IP 地址数量）、总 EPS 数及 FortiSIEM 代理数量进行许可。该产品的许可可以是永久许可，也可以是基于订阅（或基于期限）的许可。对于非虚拟设备部署，购买硬件设备需额外支付费用。

2019 年 3 月推出的 Fortinet FortiSIEM v5.2.1 提出了资源管理器视图（Explorer View）的概念，可帮助安全分析人员在进行取证和威胁捕获时，快速从发现的结果转向相关的搜索，同时提供了对 IPv6 的支持，以及隐私处理功能，可帮助需要遵守《一般数据保护法案》(GDPR) 的客户确保合规性。

Fortinet FortiSIEM 为目前使用 Fortinet 解决方案的组织或支持 Fortinet 产品的托管服务提供商（MSP），以及希望通过低摩擦/低风险方法以服务的形式提供 Fortinet FortiSIEM 的 MSSP 提供强大的支持。

## 优势

- **产品战略：**Fortinet FortiSIEM 对以 Fortinet 为中心的组织比较有吸引力，因为它通过 Fortinet Security Fabric 直接与 Fortinet 的多种技术（如端点、沙箱、邮件和欺诈防范）相集成，从而实现双向、自动化的响应操作。
- **产品：**Fortinet FortiSIEM 通过原生开箱即用的方式提供了一系列合规软件包（如 PCI、COBIT、SOX、ISO、ISO 27001、HIPAA、GLBA、FISMA、NERC、GPG13 和 SANS），同时还通过内置内容提供了诸多 IT 运营和网络运营相关的用例。
- **产品：**Fortinet FortiSIEM 具有强大的资产发现功能，而且可通过主动扫描环境以及被动监听网络流量来自动构建组织的配置管理数据库 (CMDB)。
- **产品：**Fortinet FortiSIEM 提供了大量的基本的安全用例，由于提供了性能、可用性监控以及 CMDB 功能，因此还可以用作 IT 运营和网络运营工具的场景。
- **客户体验：**从 Gartner 客户问询和 Peer Insights 来看，FortiSIEM 的总体客户满意度普遍不错，这方面与许多竞争对手保持一致，而且该产品的威胁情报功能的得分高于多个竞争对手。
- **销售战略：**Fortinet 推出了一个面向 MSSP 的合作伙伴计划，该计划采用账单到期即付 (PAYG) 合作伙伴模式，鼓励 MSSP 以服务的形式提供 FortiSIEM。

## 注意事项

- **产品战略：**计划支持 OT/物联网 (IoT) 监控功能的 Fortinet 客户将需要使用合作伙伴产品来解析事件并集成 CMDB 信息。

- **产品战略：**Fortinet FortiSIEM 的云安全功能覆盖范围不如其他竞争对手强大，比如它缺乏对 Google Cloud 和 IBM Cloud 的支持。
- **产品：**Fortinet FortiSIEM 的实时高级分析功能落后于某些竞争对手 - 比如它无法动态建立节点组。FortiInsight 提供了更多的 UEBA 功能，但仅适用于运行 FortiInsight 代理的端点。
- **产品：**将 Fortinet FortiSIEM 用作取证或威胁狩猎的案例和事件管理平台的组织会发现，该产品的案例创建和管理功能不如其他工具直观，并且没有与威胁狩猎工具的原生集成。
- **销售战略：**Fortinet 不提供 SaaS SIEM。部署该公司产品的客户将需要通过 Fortinet 的 MSSP 合作伙伴实现此功能。
- **客户体验：**客户对 FortiSIEM 销售/支持相关领域的满意度较低。这可能表明 Fortinet 以合作伙伴为主导的市场进入战略对于 SIEM 产品而言不及其他产品有效。

## HanSight

HanSight 是一家总部位于中国北京的供应商。HanSight 的产品主要在中国市场销售，另外也通过渠道合作伙伴，在亚太地区（APAC）（如日本和新加坡）和拉丁美洲进行销售。HanSight Enterprise SIEM 是该公司的核心产品。该产品是由一系列解决方案构成的生态系统的一部分，此类解决方案包括：UEBA 、带有 IDS 功能的网络流量分析（NTA）、漏洞管理、资产发现、数据防泄漏（DLP）和威胁情报管理。该公司通过与中国多家安全技术供应商的合作来提供 EDR 和云工作负载保护平台（CWPP）功能。

该平台可以作为软件、硬件设备（用于较小的部署）或作为托管平台来提供。HanSight 的内部部署解决方案采用永久性许可 + 年度维护的许可模式。Enterprise SIEM 按数据流速（EPS）定价，同时采用阶梯折扣制。其他模块按用户数量（UEBA）、所部署传感器的数量和带宽（NTA）及资产（VM 和资产）进行定价。Hosted Enterprise SIEM 以标准定价为基础，再加上托管应用的增加部分；该产品通过订阅模式进行许可。

在过去的 12 个月中，HanSight 在其搜索功能中添加了 HanSight 查询语言（HQL），引入了 DLP 插件，并添加了事件聚合和事件时间线可视化功能。

在中国市场的组织，尤其是银行和金融领域中，希望所部署的 SIEM，其提供商专注于所在区域的技术支持和安全运营生态系统构建，应考虑使用 HanSight 的产品。

### 优势

- **产品：**HanSight 提供了一个强大的技术生态系统，该生态系统是其核心 SIEM 解决方案的有效补充，这对于那些希望通过单个供应商配备整个现代化安全运营中心（SOC）的组织而言比较有吸引力。
- **产品：**该平台采用现代大数据技术和方法，还提供了作为服务交付的版本。
- **产品：**HQL 和搜索功能包括很多特性，如：集成开发环境（IDE），分析师笔记本风格的功能、通过响应（QR）代码共享已保存搜索的功能等等。
- **客户体验：**从 Gartner 客户问询、Peer Insights 和供应商样板客户的反馈来看，与竞争对手相比，该公司产品在服务和支持方面的用户评分均高于平均水平，尤其是在支持方面。

### 注意事项

- **运营：**HanSight 主要在中国市场与其他对手竞争，在中国市场之外的市场，该公司的知名度比较有限。亚太地区以外的渠道合作伙伴也仅限于拉丁美洲。北美或欧洲没有直接销售渠道。
- **产品：**该公司产品的监控覆盖仍然需要扩大和增强。对于包括 AWS 和阿里巴巴在内的云环境，该公司的产品都有很好的覆盖；但是，该公司的产品尚不支持虚拟环境（如 VMware 和 Hyper-V），也不能从 Azure 收集数据。
- **产品战略：**某些功能部件（如威胁情报管理）已本地化为中文，使用其他语言时带来了问题。
- **客户体验：**根据 Gartner Peer Insights 的反馈及供应商样板客户的反馈，日志管理和事件管理功能有待改善。

## IBM

IBM Security 可提供一系列安全技术和服务，其总部位于马萨诸塞州剑桥市。QRadar Security Intelligence Platform 主要围绕 QRadar

SIEM 解决方案构建，还包括其他几个单独定价的组件，这些组件包括：

- IBM QRadar Vulnerability Manager - 漏洞评估数据集成
- IBM QRadar Network Insights – 网络应用可视化和数据包全包内容检查
- QRadar Risk Manager - 网络设备配置监控和威胁模拟功能
- IBM QRadar User Behavior Analytics (UBA) - 一个免费的插件模块，实现用于检测内部人员威胁相关的用例
- IBM QRadar Incident Forensics – 通过全数据包捕获和留存，实现对调查取证的支持
- IBM QRadar Advisor with Watson – 利用人工智能技术，提供基于高级分析的根本原因识别和归因引擎

IBM 还提供了 Security App Exchange，旨在支持 QRadar 客户下载由 IBM 或第三方开发的安全 App，进而扩展 IBM QRadar 的功能覆盖面，提供更多的安全价值。其他相关的 IBM 解决方案包括：用于增强网络取证功能的 IBM QRadar Network Packet Capture 设备、IBM Resilient 是一款 SOAR 解决方案，可以实现与 QRadar SIEM 解决方案之间的双向集成，该产品可帮助组织简化其安全事件响应流程。

IBM QRadar SIEM 支持 on-premise 部署，是硬件、软件或者是虚拟机的形式，也可以通过 IBM 基于云的 SIEM 解决方案 QRadar on Cloud (QROC) 托管在云端。SIEM 的核心许可基于客户的日志流速（即涵盖范围内数据源的 EPS 数量）和每分钟流量 (FPM)。该产品可以通过永久许可或订阅的方式购买，而且只有在客户购买了 QROC 的情况下，才提供订阅。IBM QRadar Security Intelligence Platform 中其他组件的定价取决于它们各自的度量标准，例如：

- IBM QRadar Network Insights 基于网络流数量进行定价
- IBM QRadar Vulnerability Manager 基于范围内的资产数量进行定价
- IBM QRadar Risk Manager 基于从中提取配置数据的系统数量进行定价

QRadar Network Insights 仅以硬件设备的形式提供，而 QRadar Incident Forensics 则仅以永久许可证的方式出售。

在过去的 12 个月中，IBM 通过其调优 App 提高了报警效率，如何理解各种类型数据源变得更加简单，仅需要极少定制或几乎不需要定制的情况下，从通用日志格式中提取事件属性。IBM 还实现了将 QRadar Advisor with Watson 与 MITER ATT&CK 框架进行映射。

IBM 拥有广泛的客户群，包括最终用户和 MSSP 客户，而且可提供强大的平台来构建威胁检测和响应能力，因此倾向于吸引大型组织的客户。不过，小型组织也可以从 QRadar SIEM 解决方案中受益，因为该解决方案使用起来较为容易，而且提供了广泛的开箱即用的安全用例。

## 优势

- **销售战略：**IBM 拥有广泛的内部资源和合作伙伴关系，以支持销售、部署和运营，包括跨多个区域的 QRadar 托管服务。
- **部署/支持：**QRadar 可为用户提供广泛的部署架构选项，用户可选择不同的，各种组合的部署方式。其中包括物理设备和虚拟设备（可以是一体式设备，或独立组件形式），进行云部署，客户可以自带许可证。Network Insights 组件是一个例外，该组件仅可作为物理设备提供。
- **运维：**QRadar 具有广泛的开放式 API，可支持客户和合作伙伴开发与该平台的集成。该应用市场具有 IBM 及第三方提供的广泛集成。
- **产品：**QRadar 可提供强大的事件收集管理功能。用户可以配置日志记录，以自动检测多种事件格式，同时提供有诸多选项，用以过滤事件、将事件转发到实时分析，或绕过分析层并发送到数据存储。将事件直接转发到数据存储不会消耗 EPS 许可指标。
- **销售战略：**QRadar 的基本许可中包括 UBA，因此用户无需支付额外的成本便可使用 UBA 功能。
- **产品：**QRadar Advisor with Watson 可利用内部和外部源提供情境增强，基于攻击者的行为给出下一步操作建议，并对报警进行优先排序，以便未来采取行动，提供强大的事件调查支持。

## 注意事项

- **定价：**针对 QRadar 平台相关各个组件的多种许可模型和定价方案为潜在客户提供了一系列丰富的选择。许可模型包括永久性许可和期限性许可，基于多个因素来确定，这些因素包括：数据流速、资产数量，以及该技术是部署在内部还是部署在 IBM Cloud 中。QRadar 解决方案可混合采用永久性许可和期限性许可，具体取决于技术和部署选择。
- **产品战略：**QRadar 针对从端点/主机进行取证所需的数据收集提供了一些有限的选项。IBM 缺乏原生 EDR 功能，但可提供完整的网络监控功能。客户必须部署第三方产品或依靠其 WinCollect 代理或 Sysmon 来收集 Windows 系统的数据。
- **运维：**QRadar 仍在不断推动其现代化用户体验（UX），而且其 UI 在平台各个组件之间并不一致。
- **定价：**IBM 希望通过增值产品增加客户的粘性，这些产品需要额外付费才能使用；举例来说，客户需要部署 Resilient 和 QRadar Advisor，可以获得事件响应功能，包括：优先级排序、调查、情境构建和其他响应操作等。
- **创新：**QRadar 平台的组件处于不同的成熟度水平，而且其与其他组件以及新的 IBM 云管理产品的集成程度也不一。用户应确认与其自身运维相关的功能路线图承诺已按计划进行。
- **客户体验：**根据 Gartner 通过问询获得的客户反馈、Peer Insights 评论和供应商样板客户的反馈，QRadar 的分析功能和行为画像，以及供应商的销售/合同流程均有待改进。

## LogPoint

LogPoint 的总部位于丹麦哥本哈根，在欧洲、中东和非洲（EMEA；比如伦敦、巴黎和慕尼黑）、美国（波士顿）和亚太地区（如加德满都）设有办事处。LogPoint SIEM 解决方案由以下模块组成：

- LogPoint Core SIEM
- LogPoint UEBA
- LogPoint Director（包括控制台和结构）
- LogPoint Applied Analytics

LogPoint 的核心 SIEM 许可证采用基于资产数量（IP 地址数量）的订阅模式，而且包括除 LogPoint UEBA 之外的所有模块；LogPoint UEBA 按员工和资产数量进行许可，需支付额外费用。

LogPoint SIEM 及其所有组件可通过物理或软件设备（基于 Linux Ubuntu 的增强版本）在内部部署，而 UEBA 解决方案则以 SaaS 模型提供。2019 年 6 月推出的 LogPoint v6.6.1 通过数据挖掘和可视化功能增强了事件调查功能，而 UEBA v2.1.0 则可以检测用户和实体中的异常情况。

LogPoint 对于寻求欧洲 SIEM 供应商的企业和 MSSP，注重隐私保护，寻求预测型、基于资产的许可和基本事件响应功能的 SIEM 的企业和 MSSP 比较有吸引力。

## 优势

- **定价：**LogPoint 对于寻求采用基于资产数量的可预计定价模式的 SIEM 供应商的组织而言比较有吸引力。LogPoint 针对所选的垂直行业提供特殊的定价模型。举例来说，LogPoint 为医院提供基于床位数量的固定定价，为市政当局提供基于居民数量的固定定价，为大学提供基于学生数量的固定定价。
- **产品战略：**LogPoint 是一家基于 EMEA 的 SIEM 提供商，对隐私要求的理解非常敏锐，可针对 GDPR 和 CCPA 的法规要求提供数据屏蔽和模糊处理方面的高级功能。LogPoint 是唯一一家获得 Common Criteria EAL 3+ 认证的 SIEM 提供商。
- **产品：**LogPoint 提供了两个阶段来进行数据富集：通过最新可用威胁情报来扩充的阶段：第一个是在理解静态数据时（比如从 IP 到 MAC），第二个是在搜索时，提供了最新威胁情报的支持
- **销售/合作伙伴战略：**LogPoint 在欧洲开发了一个强大的渠道和 MSSP 合作伙伴生态系统，确保 LogPoint 的产品或服务可以得到广泛推广。
- **产品：**LogPoint 通过一个联合模型实现了原生多租户产品模式，在该模式中，每个租户都连接到管理结构，有利于 MSSP 的采用。
- **对市场的了解：**对于广泛使用 SAP 的组织或使用特定物联网设备（如西门子风力涡轮机）的公用事业公司，LogPoint 通过具有吸引力的功能和安全用例开拓了一些利基市场。

### 注意事项

- **销售执行：**LogPoint 在美国的市场扩张仍处于起步阶段；LogPoint 在 Gartner 的北美客户以及欧洲、中东和非洲以外地区的知名度较低。
- **产品战略：**尽管 LogPoint 的产品能以原生的方式作为 AWS 和 Azure 的现成映像使用，但其 SIEM 产品不能作为 SaaS 使用，而其 UEBA 则仅可以作为 SaaS 使用。
- **产品战略：**LogPoint 在规则、仪表板和警报方面大量使用了查询语言，这需要用户进行培训并熟悉语法。
- **产品：**案例管理和 SOC 协作功能比较基本，可能不支持 SOC 运营的所有方面。支持与多种 SOAR 产品的集成。
- **产品：**希望获得面向典型 UEBA 用例的高级分析功能（如用户监控）的客户，需要做好购买额外 UEBA 模块的准备，因为该公司核心 SIEM 的原生机器学习功能具有局限性。
- **产品：**定制化数据源（如定制业务应用）的收集和解析是通过“插件”完成的，这些插件需要由 LogPoint 开发或由客户配置。云监控功能集刚刚起步 - 举例来说，不支持 Google Cloud 或 IBM Cloud。

## LogRhythm

LogRhythm 的总部位于科罗拉多州的博尔德，其 SIEM 解决方案名为 LogRhythm NextGen SIEM Platform。该 SIEM 解决方案的核心组件是 XDR Stack，后者由 DetectX、AnalytiX 和 RespondX 组成。插件模块包括 UserXDR（LogRhythm 更名后的 UEBA 产品）、NetworkXDR（可提供 NTA 功能）、System Monitor（SysMon Lite 和 Pro）和 Network Monitor（NetMon 和 NetMon Freemium）。其产品 LogRhythm Enterprise 适用于大型企业配置，而产品 LogRhythm XM 则适用于中型企业配置。它可以作为软件、物理设备或虚拟设备在 IaaS 或混合环境中进行内部部署。

LogRhythm 基于云的 SIEM 产品 LogRhythm Cloud 也已上市，由供应商托管和管理。XM 解决方案是一种多合一设备； 由于构成 LogRhythm 平台的各种组件可以根据需要独立部署，因此可以实现水平可扩展性。原生支持多租户。

LogRhythm 的核心产品 XDR Stack 采用按数据流速（即每秒消息数 [MPS]）的许可方式。尽管 UserXDR 根据受监控的用户数量进行许可的，但 NetworkXDR（或 NDR）和 Network Monitor 是基于每秒 GB 数 (Gbps) 进行许可，而 System Monitor 则是按代理进行定价。该公司产品的许可证包括永久性或期限性许可证，以及企业范围内的协议。在 2019 年 10 月初，LogRhythm 推出了 Unlimited Data Plan (ULP) 产品，旨在消除基于消耗量的容量跟踪并提高预算的可预测性。

在过去的 12 个月中，LogRhythm 推出了基于云的 SIEM 产品，即 LogRhythm Cloud。该产品引入了与物理硬件相分离的软件许可模型（即：允许将解决方案安装在客户硬件上、IaaS 中或者 LogRhythm 设备、客户基础架构和 IaaS 的混合模型中）。它还增加了增强的自动化、集成和案例管理功能，其 Echo 和 LogWars 功能利用其 SIEM 产品作为用户的培训工具。

对于希望使用单一供应商生态系统来为其安全运营团队提供威胁监控和响应、合规性用例以及灵活的部署选项的组织，应考虑采用 LogRhythm 的产品。

## 优势

- **产品战略**：LogRhythm 为希望部署统一解决方案（包括核心 SIEM、网络监控、端点监控和 UEBA）的买家提供了一种单一供应商生态系统的方法。
- **部署/运营**：从注册到持续支持，该公司的专业服务范围非常广泛。LogRhythm 的客户可以利用各种辅助产品为初始实施以及解决方案的持续运营和使用提供额外的支持。
- **部署**：LogRhythm 提供有运行其核心 SIEM 解决方案所需的强大选项，包括物理硬件、软件（用于在内部或在 IaaS 中安装，例如 AWS、Azure 和 Google Cloud）和 SaaS。
- **产品**：LogRhythm 可针对全球范围内各个行业和法规提供广泛的合规性报告。
- **客户体验**：LogRhythm 的客户通常比较看好该公司的产品功能。

## 注意事项

- **产品战略：**LogRhythm 在将平台迁移到现代 SIEM 架构 (比如说，该公司仍旧采用的是 Windows Server、MS SQL 和 Linux OS 的组合）等方面仍然落后于竞争对手，并且缺少专用的 SOAR 产品。
- **对市场的了解：**该公司在 IaaS 监控支持方面落后于竞争对手。究竟 API、Sysmon 或其他代理（如 Beats）哪个才是从云服务提供商（CSP）环境中收集数据的首选机制，目前尚不明朗。
- **营销执行：**LogRhythm 在其产品名称中添加了新的品牌名称，即产品名称中加上了 XDR Stack 品牌。不过，这一举措给现有的产品名称和功能组合（Next Gen SIEM、CloudAI [for UEBA]、Sysmon、Netmon、LogRhythm Cloud、AI Engine 等）增加了更多的复杂性。买方应验证该公司向其提出的建议，并确定产品和组件是否满足其自身的用例和需求。
- **产品：**仅需要内部部署的客户将需要解决 CloudAI 功能的纯云交付问题。
- **客户体验：**Gartner 客户问询、Peer Insights 评论及供应商样板客户反馈均体现了该公司产品功能的改善机会（例如预定义报告的有用性、预定义规则的有效性)。客户针对部署和支持简便性提出了综合性反馈。

## ManageEngine

ManageEngine 在印度金奈和美国德克萨斯州奥斯汀均设有总部。ManageEngine 的核心 SIEM 产品是 Log360，不过该产品还包括其他几个模块（需要额外付费)，这些模块可与 Log360 集成，解决安全和 IT 运营用例。这些模块包括：

- ManageEngine ADAudit Plus - 活动目录（AD）变更审计与报告
- ManageEngine EventLog Analyzer - 中央日志管理
- ManageEngine Cloud Security Plus - 面向 AWS 和 Azure 的中央日志管理（CLM）和 SIEM
- ManageEngine Log360 UEBA
- ManageEngine DataSecurity Plus - 数据发现和文件服务器审计
- ManageEngine O365 Manager Plus - Office 365 安全与合规

- ManageEngine Exchange Reporter Plus - 交换服务器变更审计与报告

ManageEngine Log360 是一款软件 SIEM 解决方案，可以在物理系统或虚拟系统上内部部署。它采用永久性或期限性许可证，定价基于事件来源的数量或范围内的资产数量。各个组件均根据资产数量进行许可（具体取决于特定组件）。该公司提供基于 Web 的云托管日志存储平台 ManageEngine Log360 Cloud。该产品能够存储由日志管理模块 EventLog Analyzer 收集的数据。不过，该产品并非基于 SaaS 的 SIEM 工具。Log360 Cloud 可通过订阅的方式提供，价格根据所需的存储空间而定。Cloud Security Plus 的定价基于范围内云帐户的数量，而且可针对其他 AWS S3 存储段进行升级销售。

在过去的 12 个月中，ManageEngine 针对 Log360 SIEM 解决方案进行了以下增强：

- 构建和管理事件工作流的能力
- 与 ManageEngine Log360 UEBA 相集成 - 提供用户活动异常检测功能、存储优化和性能改进索引
- 增加了 DataSecurity Plus 模块 - 提供数据发现、文件存储分析和 Windows 文件服务器审核功能

对于拥有以 Windows 为中心的环境及 AWS/Azure 环境，而且除了基本的安全事件监控和威胁检测用例之外，还希望解决 IT 运营问题的 SMB 而言，应该考虑采用 ManageEngine 的产品。

## 优势

- **产品：**ManageEngine 可提供高于平均水平的合规性报告，包括 PCI DSS、HIPAA、FISMA、SOX、GLBA、GDPR 以及现成的其他一些行业和地区特定法规。
- **产品：**Log360 支持自动发现客户网络上的 syslog 设备，然后将其添加到解决方案监控的事件源中。
- **运营：**Log360 包含有一些响应工作流。与这些工作流相关的操作包括阻止 USB、禁用用户和终止进程等。某些操作可能需要使用 ManageEngine 的其他产品。

- **客户体验：**基于 Gartner 的 Peer Insights 数据以及供应商提供的样板客户数据，ManageEngine 客户普遍表示对 ManageEngine 和 Log360 的功能非常满意。需要改善的领域包括“注意事项”部分所确定的领域，例如与其他产品的集成以及用户、数据和应用监控。

### 注意事项

- **产品战略：**该供应商欠缺多个与企业 SIEM 部署相关的集成功能，或者说这方面的功能比较有限。该供应商不支持安全编排、自动化和响应解决方案、FIM 或 EDR 产品、UEBA 产品或 ERP 解决方案。Log360 没有开放的 API 来支持客户集成。
- **产品：**数据监控支持仅限于 MS SQL 和 Oracle 日志，不支持 DLP 或数据库审计和保护 (DAP)。仅通过第三方解决方案支持基于网络的监控。
- **产品：**对日志数据管理的支持较为有限。举例来说，Log360 不支持多个日志数据保留策略。
- **产品：**用户监控功能正在开发中。ADAudit Plus 产品可提供 AD 监视，而 ManageEngine 已经增加了基本的异常检测和风险评分功能。不过，该供应商不提供更丰富的 UEBA 功能。
- **产品：**该公司产品对 ATD 的支持较为有限。有效负载检测、网络流量分析和取证支持均需要借助第三方产品。

## McAfee

McAfee 的总部位于加利福尼亚州圣克拉拉，主要办事处设在英国斯劳、新加坡、日本东京和巴西圣保罗等地。

McAfee Enterprise Security Manager (ESM) 由 Event Receiver (ERC)、Enterprise Log Search (ELS)、Enterprise Log Manager (ELM) 和 Advanced Correlation Engine (ACE) 组成。此外，McAfee ESM 可以通过 McAfee Direct Attached Storage (DAS) 进行扩展和增强，以增加日志存储容量，还可以通过 McAfee Global Threat Intelligence (GTI) 实现 IP 信誉保护。若要实现其他用例，则需要借助其他模块，比如借助 McAfee Application Data Monitor (ADM)，可实现第 7 层应用监控，而借助 McAfee MVISION Cloud（McAfee CASB 产品)，则可实现云访问的 UEBA 功能。

McAfee ESM 采用永久性许可证，面向物理设备或虚拟设备销售。它采用基于流速（EPS，又称 MPS）的定价模型。该产品的规模根据给定客户环境中的预期 EPS 确定。客户可以增加 EPS 容量和/或数据源数量，直到达到其设备的容量为止，而且可以对设备进行集群处理，以实现额外的水平可扩展性。McAfee Global Threat Intelligence 采用年度订阅的方式出售，并根据所购 ESM 设备的型号（硬件）或内核数量（虚拟）进行定价。

此次研究分析了 McAfee ESM v11.2.1，该版本于 2019 年 7 月推出。该版本采用 McAfee 的数据流总线 (DSB) 架构，该架构可实现分层 ESM 的弹性，支持将消息路由/转发到内部或第三方模块。

拥有成熟、复杂环境而且在 McAfee 技术上投入大量资金来进行数据保护和端点安全的组织，应考虑 McAfee ESM。

## 优势

- **产品战略：**McAfee 在其安全运营解决方案产品组合中提供了集成，而且能够补充 McAfee ESM（如 McAfee Threat Intelligence Exchange 或旨在提供高级编排功能的 McAfee Active Response）。
- **产品：**McAfee ESM 提供了强大的双向集成，使用户可通过 McAfee MVISION EDR、Advanced Threat Defense (ATD)、Network Security Platform (NSP) 和 Web Gateway (MWG) 实现自动化响应。
- **产品战略：**McAfee 的技术联盟生态系统 (McAfee SIA) 涵盖了超过 115 个活跃的合作伙伴，其中有 44 个合作伙伴是 ESM 集成功能或内容的直接贡献者。
- **产品：**McAfee ESM 的数据获取和管理功能集特别强大 - 举例来说，实施 McAfee 的 Data Streaming Bus 可扩展性，并支持具有复杂治理需求的联合组织。
- **销售战略：**McAfee 拥有强大的全球覆盖 - 举例来说，McAfee 在 EMEA 地区拥有密集的渠道和服务合作伙伴生态系统，可为需要咨询、实施、运营和/或托管服务的组织提供产品和服务。

## 注意事项

- **产品：**McAfee ESM 缺少 UEBA 功能，其 UBA 内容包提供的用例集较为有限。该工具没有动态对等体分组。

- **产品：**尽管 McAfee ESM 能够针对可疑事件提供基于分析的风险评分，但该产品在将这些事件映射到诸如 Cyber Kill Chain 或 MITER ATT&CK 之类的框架，创建攻击时间线方面落后于竞争对手。
- **产品：**在 McAfee 的产品组合（如 MVISION EDR、McAfee Active Response、McAfee Advanced Threat Defense）之外，McAfee ESM 原生、用于响应和运行手册自动化的 SOAR 能力落后于竞争对手。
- **产品：**客户应确认 ESM 在将来是否能支持其数据治理需求。ESM 中存储的数据（静态数据）没有原生加密。静态数据的屏蔽/模糊处理功能仅限于事件数据库中所存储事件的 IP 地址。

## Micro Focus

Micro Focus 的总部位于英国纽伯里，所提供的 SIEM 解决方案即其 ArcSight 平台。ArcSight 解决方案由核心 SIEM 解决方案、数据收集和管理组件、UEBA 以及事件调查和管理组成。其他插件组件包括用于合规性、应用监控和其他用例的特定软件包。Micro Focus 产品组合中的其他产品也支持安全用例，包括 Application Defender 和 Voltage 数据保护解决方案。Micro Focus 还提供了 ArcSight Marketplace，用作客户选择和实施内容包和技术集成的来源。ArcSight 可以通过物理设备部署或作为软件进行部署。除 Interset UEBA 外，ArcSight 平台的定价主要基于 EPS，而 Interset UEBA 则是按员工数量进行定价。

在过去的 12 个月中，Micro Focus 通过收购 Interset 获得了 UEBA 功能，并将 ArcSight Data Platform (ADP) 解决方案分为两个独立的组件：Logger 及带有 Transformation Hub 的 Security Open Data Platform (SODP)。此外，该公司还针对 ArcSight 产品组合引入了仅基于 EPS 的新定价模型（比如删除了数据量定价元素）。

对于具有成熟的安全监控运营的企业而言，如果需要比较高的数据解读功能和可扩展选项，以及将数据路由到各种来源的灵活性，则应该考虑使用 ArcSight。

### 优势

- **产品战略：**Micro Focus 于 2019 年 2 月收购了 Interset UEBA，通过此次收购增加了内部 UEBA 功能，可与 ArcSight SIEM 更紧密集成。Interset 的技术替代了先前与 ArcSight 一起出售的 Securonix OEM 版本。

- **产品战略：**ArcSight 平台为大型企业和服务提供商提供支持环境，具有可扩展和分布式架构，可以预过滤数据，然后高速解读数据，同时具有灵活的数据路由选项（例如 Logger、Investigate 或独立的 Elasticsearch 环境）。
- **产品：**ArcSight 具有一整套开箱即用合规用例，而且支持将事件映射到 MITER ATT&CK。
- **客户体验：**样板客户对 ArcSight 的实时监控功能及其在自定义关联规则方面的易用性给出了高于平均水平的评分。

### 注意事项

- **产品：**Micro Focus 必须将更多资金投入到 ArcSight 平台的功能升级上，例如改善 UI/UX 并进一步集成 Interset 产品。买家和现有 ArcSight 客户应评估 Micro Focus 的路线图，以确认其是否能满足当前需求和规划的需求。
- **创新：**Micro Focus 在一些方面落后于竞争对手，这些方面包括：原生 SOAR 功能、SaaS 产品，以及 IaaS、SaaS 和客户关注的其他新环境（如 OT 和 IoT）的更深入支持。
- **部署：**该公司 SIEM 解决方案的部署选项因组件而异。Connector、Logger 和 ESM 均可作为软件和物理设备提供。在 AWS 和 Azure 中，有可用于 ArcSight Management Center、ESM 和 Logger 的映像。Investigate 和 Transformation Hub 已完成了容器化过程。该公司未向买家提供可用的 SaaS 选项。
- **销售执行：**从 Gartner 客户问询结果来看，Micro Focus ArcSight 很少出现在中东和印度以外地区企业的新 SIEM 部署项目候选清单之中。
- **客户体验：**基于 Gartner 客户问询、Peer Insights 评论及供应商样板客户的反馈，Micro Focus 需要改善其销售/签约和技术支持。同样是基于这些来源的反馈，该公司落后于竞争对手的产品功能包括：部署和支持的简单性、行为画像、分析、查询/调查功能、工作流和案例管理。

## Rapid7

Rapid7 的总部位于马萨诸塞州波士顿。该公司的 Insight 平台由 InsightIDR（其核心 SIEM/UEBA 产品）、InsightVM（漏洞评估）、

InsightAppSec（应用安全）、InsightConnect (SOAR) 和 InsightOps（IT 运营日志管理）组成。Rapid7 提供 Insight Agent 作为其首选的端点代理，它可通过 Rapid7 InsightIDR、Rapid7 InsightVM 和 Rapid7 InsightOps 实现遥测收集和基本双向响应集成功能。InsightIDR 还提供与 InsightVM 的集成，使客户可以在整个环境中部署单个代理，以检测和收集漏洞评估数据，同时执行检测和响应功能。

Rapid7 InsightIDR 是一款部署在 AWS 中的 SaaS SIEM 解决方案，它利用部署在客户组织中的 Insight Collector 或 Insight Agents 来收集、集中和传输日志。Rapid7 通过其 Managed Detection and Response (MDR) 服务产品提供 24/7 全天候威胁监控、调查和响应功能。

Rapid7 InsightIDR 采用基于订阅的许可模式，并根据客户环境范围内的资产数量（通常是服务器、台式机和笔记本电脑）进行定价，而更大数量的资产，则采用分级定价。

2019 年 4 月，Rapid7 收购了一家小型 NTA 公司 - NetFort，旨在使用其网络传感器来收集和分析网络数据并将其发送到 Insight 平台。该公司在过去一年中的其他增强功能包括：新的 FIM 功能、云检测及对 AWS 和 Azure 环境的支持、增强的端点自动化功能，以及与案例管理工具（如 ServiceNow 和 JIRA）的更紧密集成。

鉴于 Insight 平台产品的广度以及可以将 24/7 全天候检测和响应外包给同一供应商的选项，那些安全运营资源有限、正在寻求基于 SaaS 的 SIEM 解决方案的中小型企业，应该考虑使用 Rapid7 的产品。

## 优势

- **部署和支持：** InsightIDR 是一款 SaaS 产品，仅需要在内部部署端点代理或收集器。该架构提供了相对轻松的客户概念验证（POC）互动，而且可以快速过渡到生产使用。Rapid7 负责所有补丁程序和平台更新，以及检测、响应和报告内容的更新。
- **产品战略：** Rapid7 的补充技术组合（如漏洞管理和 SOAR）可帮助组织应对安全运营的多个方面，包括威胁检测和响应。对于那些仍然关注其 Rapid7 环境的 24/7 全天候监控问题的客户，Rapid7 可以基于 InsightIDR 提供威胁检测和响应所需的托管服务。

- **产品：**InsightIDR 通过基于异常活动的开箱即用案例为 UBA 提供强大的支持。通常来说，该产品的事件识别和调查功能以用户为中心，因为分析人员可以随时获得用户的情境和风险评分。
- **产品：**与竞争对手的供应商相比，它对 FIM 和端点的原生支持能力较强。端点代理还可以用于部署迷惑性凭据，这是其在 SIEM 产品方面的一个亮点。
- **客户体验：**从 Gartner 客户问询、Peer Insights 评论和供应商样板客户的反馈来看，Rapid7 的用户对该供应商的评价较高，尤其是在简化部署（和 POC 互动）方面表现突出。

### 注意事项

- **产品战略：**InsightIDR 可提供 Insight 平台的技术组件之间的集成功能，但是技术联盟生态系统相对较小。该公司的产品与第三方检测、分析和响应技术的双向集成较为有限，而且不提供与大数据平台的集成功能。需要借助 InsightConnect 产品来实现与响应和双向技术的其他集成功能。
- **产品战略：**依赖代理进行日志收集将对 OT/IoT 用例的支持限制为 InsightIDR 蜜罐部署。收购 Netfort 可能会通过网络监控为这些用例带来更多功能。
- **对市场的了解：**尽管可以对令牌进行标记，但 InsightIDR 不支持模糊处理所需的数据屏蔽。潜在客户应验证 InsightIDR 的数据收集和分析功能是否符合特定的隐私要求。
- **产品：**InsightIDR 在 AWS 之上运行，日志管理、加密和归档取决于该平台的功能，而且受该平台许可条件的约束。客户应验证 InsightIDR 的日志归档/管理功能是否符合其自身的需求。
- **客户体验：**Gartner 客户问询、Peer Insights 评论和供应商样板客户的反馈表明，应用监控和面向服务的第三方资源可用性有待改善。

## Securonix

Securonix 的总部位于德克萨斯州艾迪生。Securonix 的 SIEM 平台由以下组件构成：Securonix SIEM、Security Data Lake、UEBA、SOAR、NTA、Threat Intelligence and Apps，可提供支持和打包内容，以解决特定的用例。

2019 年，Securonix 迁移到基于 AWS 的 SaaS SIEM，以此作为标准部署模型，大多数新客户都使用该模型。客户部署 Remote Ingestor Node（RIN）收集数据并将数据传输到云。该解决方案以基于期限的订阅方式提供（个别情况下，也提供永久性许可），而且 Securonix 采用基于客户员工数量的定价模型。就托管而言，还有一个额外的成本要素，它基于 EPS 以及数据存储量和持续时间需求。

去年引入的功能包括：共享的多租户架构、SNYPR-EYE 部署和管理控制台、新的 OEM、基于转售和技术的 NTA 和 SOAR 功能、端点和数据库监控以及云和身份监控。

对于寻求功能全面、由分析驱动且能够针对复杂用例中的威胁检测和响应（如内部人员威胁）、混合环境（如多云）、威胁捕获及合规性为 SOC 提供支持的 SaaS SIEM 的成熟安全组织而言，应考虑 Securonix SIEM。

## 优势

- **产品战略：**Securonix 可提供强大的云支持和承诺。它的 SIEM 是云原生产品，而且作为服务提供，具有三种不同的租户模型（共享、专用和隔离）。
- **产品：**Securonix 可提供多层分析以及 UEBA 功能，可跨用户和实体进行高级分析和行为建模，支持复杂用例和高级用例（如 APT、内部人员威胁和欺诈），并将检测到的攻击映射到通用框架（如 MITER ATT&CK 框架）。
- **产品战略：**Securonix 可提供广泛的开箱即用内容，这些内容以垂直包装的形式进行组织（大多数情况下需要额外付费）。它包括完整的用例、分析、警报、仪表板，甚至是响应手册。
- **产品战略：**SNYPR-EYE 的引入使得 SIEM 管理器与 Hadoop 技术隔离开来，同时使拥有足够资源的人员可以访问底层的 Hadoop 基础架构。
- **产品：**Securonix 可提供高级模糊处理功能、基于角色的访问控制（RBAC）工作流以及原生加密功能，这些功能超出了 AWS 以原生方式所提供功能的范畴。

- **客户体验：**从 Gartner 客户问询、Peer Insights 评论和供应商样板客户反馈来看，Securonix 在分析和用户监控功能方面获得了很高的评价。

### 注意事项

- **部署/支持：**Securonix 通过 OEM、转售和技术合作伙伴来填补功能覆盖空白，这种方法会带来风险，因为它会产生依赖性。客户应了解双方的路线图和长期承诺，并评估该供应商支持和维护结构。
- **营销执行：**Securonix 在品牌和工具营销方面的投入需要持续投资，而且应更好地利用其技术联盟、合作伙伴和 OEM 关系（如上述关系）。
- **产品战略：**Securonix 引入了 SNYPR-EYE 来改善平台管理体验，同时引入了内容包，从而可以更快地帮助特定用例和垂直行业实现价值。不过，Securonix SIEM 很难继续解决复杂用例及成熟组织的需求，同时又要保持足够简单，以吸引不成熟的组织。
- **部署和运营：**若要实现 Securonix SIEM 的全部功能，尤其是实现解决高级用例（如多产品内部人员威胁）的功能，则需要大量的投入和专业知识。

## SolarWinds

SolarWinds 的总部位于德克萨斯州奥斯汀，提供 SolarWind Security Event Manager (SEM) SIEM 解决方案。SEM 包含有 SIEM 的核心功能，可提供数据管理、实时关联和日志搜索，进而支持威胁和合规监控、调查和响应。SolarWinds SEM 由管理器和控制台组成，还包括一个多功能端点代理。作为 SEM 核心功能的补充，SolarWinds 的产品组合包括用于票务和案例管理、网络和应用监控以及虚拟平台监控的产品。SolarWinds SEM 根据监控的数据源（也称为节点）和工作站的数量进行定价。该产品采用永久性许可证，提供年度维护。SolarWinds 宣布计划在 2020 年引入基于订阅的定价。

SEM 可部署为包含所有组件（如数据库和关联引擎）的独立虚拟设备。SEM 也可以部署在 Microsoft Azure 或 Amazon AWS 中。

在过去的 12 个月中，SolarWinds 将 Log and Event Manager (LEM) 重命名为 SEM，并于 2019 年 11 月推出了新的版本控制方案。它还开始支持基于 HTML5 的 UI 和 UX（从 Flash 迁移而来），并引入了将 SEM 部署到 AWS 中的功能。

具有专注于合规性的用例且希望简化 SIEM 整体体验的 SMB，以及希望将安全监控集成到其环境中的现有 SolarWinds 客户而言，应考虑 SolarWinds SEM。

### 优势

- **部署/运营：**SolarWinds 通过自助 POC（借助 30 天试用版）、简化的定价模型、轻松的部署和操作，以及强大的对等用户社区 THWACK 来强调自己动手（DIY）的方法。这种方法得到了样板客户的好评。
- **产品：**SolarWinds SEM 提供了一个大型的开箱即用威胁检测规则和合规内容存储库，以及该解决方案中所包含的 FIM 功能，这些功能支持多种操作系统（如 Windows、Linux、macOS 和 IBM AIX）。
- **客户体验：**与该产品的其他功能相比，样板客户对实时监控功能给予了很高的评价；与竞争对手相比，该产品部署、集成和支持的简洁性均高于平均水平。

### 注意事项

- **营销战略：**SolarWinds SEM 主要在北美和欧洲销售；不过，它在这两个地区之外的地区，市场知名度和渠道合作伙伴有所欠缺。
- **定价：**许可模式仅限于永久性许可，部署选项仅限于 SEM 虚拟设备。
- **产品：**SolarWinds 缺乏许多竞争性 SIEM 中内置的功能 - 例如原生案例管理/事件管理功能以及云环境监控支持。客户可以利用 SolarWinds 产品组合中的其他产品来补充 SEM，比如采用 Service Desk 来实现案例管理，或者采用 Papertrail 和 Loggly 来实现云环境的日志收集和监控。

## Splunk

Splunk 的总部位于加州旧金山。该公司的 Security Operations Suite 包括其核心产品 Splunk Enterprise 或 Splunk Cloud。该公司提供三种安全特定的解决方案，分别是：Splunk Enterprise Security (ES)（Gartner 认为这是 SIEM 的必备解决方案）、Splunk UBA 和 Splunk Phantom。所有这三种解决方案都是作为额外独立产品出售。Splunk Enterprise 和 Splunk Cloud 可提供事件和数据收集、搜

索和可视化功能，用于 IT 运营中的各种用途及部分安全用例。ES 提供了大多数的安全性内容和事件监控功能，包括安全特定的查询、可视化和仪表板，以及一些案例管理、工作流和事件响应功能。UBA 添加了无监督的机器学习驱动型高级分析。Phantom 可提供 SOAR 功能，旨在提供安全事件的自动补救和缓解功能。针对安全用例的其他应用可通过 Splunkbase 获得，例如用于 PCI 合规性的 Splunk 应用。

该公司可提供多种部署选项：内部部署软件、IaaS 和混合模型。Splunk 托管并运行 Splunk Cloud，它是一款使用 AWS 基础架构的 SaaS 解决方案。Splunk Enterprise 和 Splunk Cloud 组件由支持 n 层架构的通用转发程序、索引程序和搜索 header 组成。

Splunk Enterprise 和 Splunk Cloud 基于采集到平台中的数据量（或每天的 GB 数）进行许可。唯一的区别在于 Splunk Cloud 还可以基于 Splunk 的 AWS 环境中作为存储而保留的数据量进行定价。对于来自大量、低价值日志源，如：域名系统 (DNS) 和 NetFlow 的数据，可采用更低的价格。ES 也是按消费量进行许可，并且按 Splunk Enterprise 的百分比定价。UBA 按照组织中用户帐户的数量进行许可。不过，如果客户希望将 UBA 许可与其他 Splunk 许可进行协调，则可以选择购买基于消费量的 UBA 许可，价格以 ES 的指定百分比定价。目前，Splunk Security Operations Suite 的所有产品仅采用期限型许可方式，而且针对整个企业范围的定价和实际配置提供了多种选项。Phantom 具有两种不同的许可模式。一种是根据用户采取措施的事件数量来定价，另一种是根据许可的席位用户的数量来定价。

Splunk 在过去 12 个月中最重要的增强功能包括：通过 ES Event Sequencing 增强的实时监控功能、利用威胁情报实施安全自动化的功能、医疗保健行业特定的垂直内容 (旨在解决处方盗用和病患隐私侵害等问题)。2019 年 10 月下旬，Splunk 发布了一款名为 Mission Control 的基于云的解决方案，以更紧密地集成其 Enterprise Security、Phantom 和 UBA 产品。在本魔力象限报告的研究阶段，Mission Control 尚未正式推出，因此未做评估。

对于寻求可通过插件功能从基本用例扩展到更高级用例的 SIEM 解决方案的组织而言，应考虑使用 Splunk 的产品。希望通过单个供应商来支持其安全之外及整个组织范围内的数据和分析需求的买家，也应考虑使用 Splunk 的产品。

## 优势

- **部署：**Splunk Enterprise 和 Enterprise Security 具有多种交付选项，包括软件 (可以在内部部署，或采用 IaaS 或混合模式部署)、云托管，以及通过设备交付（利用第三方)。
- **产品战略：**Splunk 提供集中式数据收集和分析的方法，以及基于其核心产品的高级解决方案，吸引了那些希望通过单个解决方案支持多个团队（如 IT 运营团队、安全运营团队、数据和分析团队）的组织。买家可以从一个用例或团队开始，然后再扩展到其他用例。
- **对市场的了解：**Splunk 建立了一个完善的合作伙伴和技术联盟生态系统，能够通过用例或供应商特定的应用扩展 Splunk 的原生价值。Splunkbase 便是使用应用市场在单个 UX 中交付内容和产品集成的典型示例。
- **客户体验：**与竞争对手相比，Splunk 客户在集成的简洁性、最终用户培训质量和可用性，以及同行社区的质量方面获得了很高的评价。
- **营销执行：**Splunk 的营销方式和跨组织的销售机会使其受到了 Gartner 客户（大中型企业、全球性企业、跨国企业）的高度重视。

## 注意事项

- **客户体验：**在评估和合同谈判、服务和支持、定价和合同灵活性以及投资价值方面，样板客户对该供应商产品的总体评分要低于大多数竞争对手。这体现了 Gartner 客户对 Splunk 产品成本的持续关注。Splunk 引入了几个新的定价选项，但我们现在来评价这些更改是否会改善 Splunk 在定价、许可和成本方面的劣势，还为时过早。
- **产品战略：**Splunk 缺乏端点和网络传感器，这就需要买家寻找互补的第三方解决方案来满足现代 SOC 的需求（如 SIEM + UEBA + SOAR + EDR + NTA)。该公司的产品通过 Splunkbase 应用支持与领先供应商的集成。
- **产品战略：**尽管 Splunk 已将 UBA 的定价模型与 Splunk Enterprise 和 Splunk Enterprise Security 的定价模型进行了统一，但 Splunk UBA 位于单独的技术体系中。它尚未集成到核心 Splunk 中，并且仍然采用内部或托管模式，这可能会对 Splunk Cloud 的买家造成影响。
- **运营：**Splunk 的内容在多个平台上提供，必须分别获得许可才能访问相应的内容，并且需要多种机制来组织和更新内容，比如跨额外付费应用和解决方案（如 ES、UBA 和 Phantom）来组织和更新内容。

### 增加和撤除的供应商

随着市场的变化，我们检查并调整了魔力象限（Magic Quadrants）的纳入标准。调整后，任何魔力象限的供应商组合将随时间推移而发生变化。供应商第二年未继续出现在魔力象限中并不意味着我们对该供应商的看法发生改变。这可能体现了市场中发生的变化，因此也体现了不同的评估标准，或该供应商专注领域所发生的变化。

### 增加

按照纳入标准，FireEye 和 HanSight 于今年被纳入到本魔力象限中。

### 撤除

BlackStratus、Netsurion-EventTracker 和 Venustech 今年从本魔力象限中撤除，因为他们不符合收入和地理覆盖方面的纳入标准。

## 纳入和排除标准

供应商若要被纳入到魔力象限之中，需要达到以下要求：

- 其产品能够通过软件和/或设备和/或 SaaS 为最终用户客户提供 SIM 和 SEM 功能。
- 在 2019 年 7 月 31 日之前，其 SIEM 特性、功能和插件解决方案均已普遍可用。
- 其产品支持从异构的第三方来源（即不同于 SIEM 供应商的产品/SaaS，包括市场领先的网络技术、端点/服务器、云（IaaS 或 SaaS）及业务应用）进行数据捕获和分析。
- 在 2019 年 6 月 30 日之前的 12 个月中，SIEM 领域（包括产品/SaaS 许可和维护，不包括托管服务）的收入超过 3,200 万美元，或者在同一时期的期末拥有 100 个上生产系统的客户。该类客户是指已获得 SIEM 许可且正在使用 SIEM 监控其生产环境的客户。Gartner 将会要求您提供达成此要求的书面确认，以及达成其他收入或客户门槛规定的书面确认。此类确认必须由您组织中相应的财务主管出具。

- 在 2019 年 6 月 30 日之前的 12 个月内，在供应商总部所在地理区域以外的区域实现的 SIEM 产品/ SaaS 收入占比达到 15%。在以下至少两个地理区域的每个区域中，至少拥有 10 个上生产系统的客户：北美、欧洲、中东、非洲、亚太地区和拉丁美洲。
- 截至 2019 年 6 月 30 日，至少针对以下两个地域开展了相应的销售和营销运营（通过印刷品/电子邮件营销活动、采用本地语言翻译的销售/营销材料）：北美、欧洲、中东、非洲、亚太地区和拉丁美洲。

排除条件包括仅通过托管服务关系而提供的功能。换言之，如果只有在客户注册了供应商的托管安全或托管检测和响应或托管 SIEM 或其他托管服务产品之后才能提供 SIEM 功能，那么此类供应商应排除在外。此处所述的托管服务是指客户与卖方合作构建、监控、升级和/或响应警报/事件/案例的服务。

# 评估标准

## 执行力

**产品或服务：**评估供应商在以下领域提供产品功能的能力及其过往记录，包括实时安全监控、安全分析、事件管理和响应、报告，以及部署简化等领域。

**整体可行性：**用于评估技术提供商的财务状况、整个公司在财务和实践上的成功，以及持续投资于 SIEM 产品的可能性。

**销售执行/定价：**用于评估技术提供商在 SIEM 市场的成功及其开展销售准备活动的能力。其中包括 SIEM 收入和现有客户群的规模，SIEM 收入和现有客户群的增长率，售前支持，以及销售渠道的整体有效性。此外，Gartner 客户的关注水平同样在考虑范围之内。

**市场反应/过往记录：**评估 SIEM 产品与买家在求购时所述的功能需求的匹配程度，以及供应商在交付市场所需的新功能方面的过往记录。此外，我们还会评估供应商如何将自己的产品与主要竞争对手的产品区别开来。

**营销执行**：评估供应商根据对客户需求的理解所制作的 SIEM 营销信息，与面向不同垂直行业或地区所制作的 SIEM 营销信息。

**客户体验**：评估产品环境内的产品功能和服务体验。包括评估部署的便捷性、操作、管理、稳定性、可扩展性和供应商支持功能。此项标

准主要通过以下方式评估：对供应商提供的样本客户进行的调查，通过咨询获得的客户反馈意见，同行洞察力报告，以及与正在使用 SIEM 产品或者已经完成了 SIEM 产品竞争性评估的 Gartner 客户进行的其他互动。

**运营**：评估供应商的服务、支持和销售功能，包括在不同地区推出的服务、支持和销售功能。

**表 1：执行力评估标准**

| 评估标准 | 加权 |
| --- | --- |
| 产品或服务 | 高 |
| 整体可行性 | 中 |
| 销售执行/定价 | 高 |
| 市场响应/过往记录 | 高 |
| 营销执行 | 中 |
| 客户体验 | 高 |
| 运营 | 中 |

来源：Gartner（2020 年 2 月）

## 前瞻性

**对市场的了解：**评估技术提供商理解新老买家需求并将这些需求转变为产品和服务的能力。对市场的了解程度高的 SIEM 供应商能够一面满足合规报告要求，一面响应各个领域的客户需求，比如针对性攻击和漏洞的早期检测，以及简化的实施和运营等。

**营销战略**：评估供应商有效传播其 SIEM 产品的价值和差异化优势的能力。

**销售战略**：用于评估供应商如何使用直接和间接销售、营销、服务和通信分公司来扩展市场覆盖的广度和深度。

**产品/服务战略**：用于评估供应商开发和交付产品的方法，其强调的是映射至当前需求时的功能和特性集。未来 12 到 18 个月的开发计划也在评估范围内。SIEM 市场已经发展得相当成熟。大多数供应商已经很难在通用网络设备、安全设备、操作系统和整合型管理功能的支持上出奇出新。我们在评估时加大了新兴事件源（如 IaaS 和 SaaS）以及环境情境覆盖范围的权重。

除了供应商对功能扩展的关注度外，我们依然很看重部署的便捷性和持续支持。相比基础用例覆盖范围的广度，用户，尤其是 IT 和安全资源有限的用户还是更看重这些特性。SIEM 产品很复杂，并且随着供应商不断扩展其功能，这些产品将变得越加复杂。如果用户能够用有限的资源成功部署、配置和管理供应商提供的有效产品，或以服务的形式使用此类产品，那么这些供应商必将成为 SIEM 市场的大赢家。

此外，我们还评估了 SIEM 技术的联合托管或混合部署选项与支持服务，因为越来越多的 Gartner 客户希望或者要求供应商提供持续服务支持，用于监控或管理他们部署的 SIEM 技术。

**垂直/产业战略**：评估供应商为支持特定垂直行业的 SIEM 需求所制定的战略。

**创新**：评估供应商开发和交付 SIEM 技术的方式，这种方式要有别于竞争对手，能够以独特方式满足关键的客户需求。此外，我们还会评估应用层监控、基于身份的监控和事件调查等领域的产品功能和客户使用情况，以及客户需要且部署的其他产品特定功能。高级威胁检测 (ATD) 和事件响应所需的功能也占了很大的权重，比如用户、数据和应用监控、即席查询、可视化、统筹安排、为调查事件而进行的情境融合，以及工作流/案例管理功能。

**地区战略**：尽管北美洲和欧洲的市场创造的 SIEM 收入最多，但是拉丁美洲和亚太地区才是成长型 SIEM 市场，威胁管理是后两个市场的主要驱动因素，其次就是合规性要求。在整体评估魔力象限中的供应商时，我们会评估供应商在这些地区的销售和支持战略，以及产品在支持与本地和区域性数据驻留和隐私法规的合规性方面的功能。

**表 2：前瞻性评估标准**

| **评估标准** | **加权** |
| --- | --- |
| 对市场的了解 | 高 |
| 营销战略 | 中 |
| 销售战略 | 中 |
| 产品/服务战略 | 高 |
| 业务模式 | 未评估 |
| 垂直/产业战略 | 中 |
| 创新 | 高 |
| 地区战略 | 中 |

来源：Gartner（2020 年 2 月）

## 象限说明

## 领导者

入选 SIEM 领导者象限的供应商均为可提供功能强大且满足一般市场需求的产品，同时在 SIEM 市场的客户群和收入流方面表现最成功的供应商。除了提供与客户需求完美匹配的技术外，领导者还在满足新兴和预测的需求方面，拥有超凡的前瞻性和执行力。通常，他们拥有相对更高的市场份额和/或强劲的收入增长势头，并且在有效的 SIEM 功能及其相关的服务和支持方面，赢得了正面的客户反馈。

## 挑战者

入选 SIEM 挑战者象限的供应商必须满足以下要求：有多条产品和/或服务线、中等规模的 SIEM 客户群，以及能满足一系列一般市场需求的产品。随着 SIEM 市场日趋成熟，挑战者的数量开始减少。通常，该象限中的供应商的执行力很强 (他们的财务资源可以证明这一点)，销售业绩也很突出，并且整个企业或者其他因素让他们的品牌认知度变得很高。但是，挑战者尚未拥有一套完整的 SIEM 功能，或者他们的 SIEM 技术在与领导者的 SIEM 技术相比较时，还没有胜出的记录。

## 有远见者

入选 SIEM 有远见者象限的供应商必须满足以下要求：提供的产品功能能够很好地匹配一般市场需求，但是执行力比领导者逊色。这主要是因为他们在 SIEM 市场的份额要低于领导者，比如，他们的现有客户群或收入规模/增长势头要小于领导者，或者他们的整个企业规模或整体可行性比不上领导者。

## 特定领域者

入选 SIEM 特定领域者象限的供应商必须满足以下要求：提供的 SIEM 技术能够很好地匹配特定的 SIEM 用例需求或一部分 SIEM 功能需求。特定领域者重点关注某个特定的客户群体，比如，中端市场、服务提供商，或者某个特定地区或垂直行业。此外，受到其他因素的限制，根据 Gartner 的标准，该象限中供应商的客户群规模较小或有限。这些因素可能包括：有限的投资或功能，覆盖范围有限的足迹，或者在目前及未来 12 个月阻碍供应商向企业提供更广泛功能的因素。入选该象限并不会给供应商在更细化的市场或用例上的价值带来负面影响。

# 背景信息

SIEM 技术可提供：

- **SIM -** 日志管理、分析和合规性报告
- **SEM -** 实时监控和事件管理，面向网络和安全设备、系统及应用的安全相关事件

通常，企业部署 SIEM 技术是为了支持以下三大用例：

- **ATD -** 用户和实体活动、数据访问和应用活动相关趋势和行为的监控、实时警报以及长期分析和报告。威胁检测包括结合采用威胁情报和业务情境，以及有效的临时查询功能。
- **基础安全监控 -** 日志管理、合规性报告和针对所选安全控制措施的基础实时监控。
- **取证和事件响应 -** 仪表板和可视化功能，以及工作量和文档支持，用于实现有效的事件识别、调查和响应。

组织应定义其特定的功能和运营需求，并考虑本魔力象限的每个象限中所列供应商所提供的 SIEM 产品。产品选择决策应基于组织在以下方面的特定需求做出：

- 基本功能与高级功能的相对重要性
- 预算限制
- 部署规模
- 产品复杂性（部署、运行、使用和支持）
- IT 部门的项目部署和技术支持能力
- 与已构建应用、数据监控和身份管理基础架构的集成

（有关更多详情，参见“Toolkit:Security Information and Event Management RFP”。）

计划使用外部服务提供商（ESP）进行 SIEM 的部署、配置或持续运营的组织，应考虑可通过 SIEM 供应商或第三方提供商确保足够服务可用性的产品。

负责考虑 SIEM 部署项目的安全与风险管理领导者首先应该定义企业的 SEM 和报告需求。其他团队输入的信息也能让项目受益匪浅，包括审计/合规团队、身份管理团队、IT 运营团队和应用所有者。此外，企业还应该描述他们的网络和系统部署拓扑，并评估事件数量和级别。这样，候选的 SIEM 供应商就能根据企业的特定部署场景，推荐解决方案。需求定义工作还应包括阶段性部署和增强功能 - 超出

初始用例的新用例，此类新用例可能需要新的调查和响应功能。本魔力象限评估了技术提供商在最常见的技术选择场景中的表现，即，SIEM 项目获得资金，用于满足威胁监控/检测/响应需求和合规性报告需求。

# 市场概述

市场对 SIEM 技术的需求仍然强劲。SIEM 市场的价值从 2017 年的 23.19 亿美元增长到了 2018 年的 25.97 亿美元（参见“Market Share:All Software Markets, Worldwide, 2018”）。威胁管理（尤其是威胁检测和响应）仍然是主要驱动因素，而常规监控与合规性次之。在北美市场，安全资源有限的组织依然会启动许多新的部署项目，因为很多这类组织出于大型客户或业务合作伙伴的坚持，需要提升监控和漏洞检测能力。合规报告功能也将继续作为组织的需求之一；不过大多数买家将其视为“筹码”。

保守采用 SIEM 技术的大型组织也会继续启动新部署项目。大型的晚期采用者和小型组织非常重视部署和运营支持的简洁性。我们仍将会看到各种规模的组织重新评估 SIEM 供应商，以便替代不完整、无价值或者失败的部署项目中的 SIEM 技术。

SIEM 市场已经发展得相当成熟，并且竞争激烈。在这一广泛采用的阶段，市场上有多家供应商能满足普通客户的基本需求。最大的需求空白区域是面向针对性攻击和数据泄露的有效检测和响应。有效使用威胁情报、行为画像和分析有助于提高检测成功率。SIEM 供应商将继续增加对行为分析功能和第三方技术集成的本地支持，而 Gartner 客户也将会越来越多地着手开发基于行为的用例。

SIEM 部署的范围在三年内趋于增长，以包含更多用例和事件源。随着用例数量和复杂性的增加，通常会对运行、调优和运营 SIEM 以及响应事件所需的资源提出更高的要求。

## SIEM 供应商格局

SIEM 的供应商格局仍在不断演变，新进入者带来的技术给分析用例带来了更高的复杂性，而且在某些情况下，也会增加云原生 SaaS 产品的复杂性。具有更成熟 SIEM 技术的供应商正在迅速采取行动，以更新其架构并引入基于云的模型。几乎所有供应商都将继续增强其事件调查功能，并通过原生功能或收购的/第三方 SOAR 解决方案引入面向响应的集成功能。SIEM 市场的特点是相对较少一部分的供应商拥有大规模客户群，而其他供应商则拥有规模较小但快速增长的客户群。

Splunk、Micro Focus、IBM 和 LogRhythm 占据了大部分的市场收入份额，不过也有一些供应商，尽管他们所占的市场份额较少，但由于他们在支持以分析为核心的用例方面或 SaaS 消费模型方面比较有优势，因此也引起了一些 Gartner 客户的强烈兴趣。较小型的 SIEM 供应商通常专注于特定的市场细分领域，例如他们其他产品的买家、寻求 SIEM 及监控服务的买家、MSSP 或 MSP 合作伙伴。

市场中的显著发展包括预览版的推出、8 月发布了 Microsoft Azure Sentinel，以及 Alphabet 的子公司 Chronicle（收购并并入 Google Cloud 旗下）推出 Backstory。尽管这些 SaaS 产品是在此次调研截止日期之后推出的，但 Gartner 客户对这些产品会如何影响其现有 SIEM 的部署及其长期 SIEM 计划非常感兴趣。

Elastic、Graylog、Sumo Logic、Devo 及其他以前曾针对 IT 运营用例推出过日志收集和分析功能的供应商，正在增加其产品对安全用例的支持。在某些情况下，他们会将其作为 SIEM 产品进行营销。尽管这些供应商不符合此次调研的纳入标准，但 Gartner 客户对他们能否满足安全用例并支持面向安全和 IT 运营的单一日志和事件收集架构非常感兴趣。

有些 SIEM 供应商由于关注的是特定的垂直市场和/或纳入标准阈值及竞争曝光度方面的原因而没有入选本魔力象限：

- 总部位于塞浦路斯的 Odyssey Consultants 和中国的多家供应商（包括 DBAPPSecurity、Venustech、奇安信集团）均可提供基于现代大数据和分析架构的 SIEM 产品，但在 Gartner 客户中的知名度较为有限。
- Netsurion-EventTracker 专注于 MSE，而且可提供集中式日志管理解决方案以及功能更全面的 SIEM，还可提供诸多可选配的部署、调优和安全监控服务。
- BlackStratus 可向 MSSP 提供 SIEM，并针对中型规模的买家提供基于云的 CyberShark SaaS SIEM。
- Huntsman Security（Tier-3 Pty Ltd. 的经营名称）是一家 SIEM 供应商，主要在英国和澳大利亚开展业务，主要服务于政府和关键基础设施组织。
- Lookwise 的市场份额主要在西班牙和南美。S21Sec 提供的威胁情报资讯是 Lookwise 的独特优势，这些情报主要关注的是银行和关键基础设施行业。
- HelpSystems 及其 Vityl 产品致力于为欧洲和南美的客户提供运营事件关联、业务流程监控和 SIEM 解决方案。

## SIEM 服务

如今，越来越多的 Gartner 客户表示，他们正在为其 SIEM 部署项目寻求外部服务支持，或者计划获取此类支持来辅助 SIEM 产品（参见“How and When to Use Co-managed Security Information and Event Management”）。寻求外部服务的驱动因素包括：缺乏内部资源来管理 SIEM 部署项目，缺乏资源来执行实时报警监控，或者缺乏专业知识来扩展部署项目以纳入新用例（比如面向 ATD 的用例）。预计，随着越来越多的客户提出全天候监控需求，并实施需要更深入的 SIEM 运营和分析专业知识的用例，SIEM 用户对此类服务的需求会继续增加。我们还预计，组织通过第三方供应商（如 SOC Prime）获取用例内容的兴趣会增加。

SIEM 供应商可能会在内部员工、外包服务或合作伙伴的帮助下，利用托管服务满足这些需求。SaaS SIEM 包括供应商对平台的支持和维护（通常是在公有云环境中）。不过，客户需要使用其自身的资源（或其他服务提供商）来配置内容、监控和调查事件。MSSP 是 SIEM 用户的另一种选择，它能够实时监控和分析事件，并收集日志，以进行报告和调查（参见“Innovation Insight for SIEM as a Service”）。但是，让外部服务提供商来满足事件收集和存储、报警、调查和报告方面的客户特定需求，可能也会出现问题；因此，客户在寻找服务时，应该评估外部服务提供商是否满足当前及规划的用例。

## SIEM 备选方案

因为购买运行 SIEM 产品很复杂并且成本高昂，同时市场上还涌现了一些其他安全分析技术，这种情况下，客户越来越希望采用其他方法来收集和分析事件数据，以识别和响应高级攻击。Elasticsearch、Logstash 和 Kibana（又名 ELK Stack 或 Elastic Stack）的组合便是一个很好的例子。此外，还出现了可替代基础广泛的 SIEM 解决方案的替代方案，这些解决方案主要专注于日志收集和安全分析元素上。在这个领域展开竞争的供应商包括 Elastic.io、Cybraics、Empow、Elysium、Jask（被 Sumo Logic 收购）、MistNet、PatternEx、Qomplx、Rank Software 和 Seceon。

如果组织有资源来部署和管理这些服务，并开发和维护分析工具，以应对安全用例，那么他们可能就可以获得一款用更少的成本满足更多需求的解决方案（与商用技术相比）。Gartner 继续跟踪了这种方法的发展。一些客户的反馈表明，尽管软件本身是免费的，但在扩展这些解决方案时涉及的工作量以及支持所需事件来源及分析所需的开发投入却十分巨大。这可能会影响总体拥有成本（TCO），而且也不利于实现比商用 SIEM 部署成本更低的目标。

多家提供商可提供不同于 MSSP 的 MDR 服务，目的在于识别并响应客户环境中的高级威胁。这通常是通过分析选定的网络和端点数据来实现的（参见“Market Guide for Managed Detection and Response Services”）。通常，他们的服务和事件源范围要比 MSSP 或 SIEM 部署项目的范围要小。他们一般不会与 SIEM 供应商或 MSSP 直接竞争，因为后者的客户有更广泛的用例需求。但是，MDR 服务提供商也能提供有效的 ATD 功能，如果组织有充足的资源来支持这些用例，也可以考虑将 SIEM 预算投入在 MDR 服务上。Gartner 将继续关注该领域，评估 MSS、MDR、日志和 SIEM 之间的交互和交叉。

# 证据

我们通过自动化社交媒体倾听工具跟踪了用户在社交媒体和公共论坛上的回应。分析时段为 2016 年 11 月 1 日至 2019 年 9 月 30 日。“社交媒体提及量”或“对话量”表示的是所监控关键字在社交媒体平台的文本帖子中的包含情况。默认情况下，不应将大量提及视为“积极情绪”或“采用量”的衡量指标。

我们进行此次分析所用的社交媒体来源包括 Twitter、Facebook（仅限于公开信息）、Instagram、图像（仅评论）、聚合器网站、博客、新闻、主流媒体、论坛和视频（仅评论）。该项研究分析了全球除中国之外的所有地理区域。由于中国对外资社交媒体平台施加有相应的限制，因此此处的社交媒体数据无法代表中国的情况。

社交媒体分析研究结果并不“代表市场情况”，仅供“指导参考”之用。它们反映了大众对社交媒体上某个主题的观点。

其他研究结果由来自 Gartner 社交媒体分析小组的 Ritesh Srivastava 提供。

# 评估标准定义

## 执行力

**产品/服务：**供应商为细分市场提供的核心产品和服务。这包括现有的产品/服务功能、质量、功能包、技能等，无论是本地提供还是通过市场定义及子标准中规定的 OEM 协议/合作伙伴关系提供。

**整体可行性**：可行性包括整个企业财务健康、业务部门财务及实践成功、个别业务部门继续进行产品投资、提供产品、在企业产品组合中保持领先水平的可能性等方面的评估。

**销售执行/定价**：供应商在所有销售准备活动中的功能以及为其提供支持的结构。这包括交易管理、定价和协商、售前支持以及销售渠道的总体效率。

**市场反应/过往记录**：随着机遇的发展、竞争对手的行动、客户需求的演化和市场动态的变化，做出反应、改变方向、灵活调整并取得竞争成功的能力。这种标准还应考虑供应商的响应历史。

**营销执行**：设计用于推广企业信息，以影响市场、提升品牌和业务、提高产品知名度、建立产品/品牌及企业在买家心目中的正面形象的计划，其清晰性、质量、创造性和功效。这种“消费者心理占有率”可通过广告宣传、促销活动、思维领导力、口碑和销售活动得以提高。

**客户体验**：促使客户通过所评估产品取得成功的关系、产品和服务/计划。具体而言，这包括客户接受技术支持或客户支持的方式。这也可包括辅助工具、客户支持计划（及其质量）、用户群可用性、服务级别协议等等。

**运营**：企业实现其目标和承诺的能力。具体因素包括企业结构的质量，如支持企业持续有效且高效运营的技能、经验、计划、系统和其他工具。

## 前瞻性

**对市场的了解**：供应商了解买家需求并将其转化为产品和服务的能力。具有高度愿景的供应商能听取和了解买家的需求，并通过提升后的愿景形成或提升需求。

**营销战略**：在企业范围内持续传达并通过网站、广告、客户计划和定位声明对外说明的明确、独特的信息。

**销售战略**：使用直接或间接的销售、营销、服务、通信的适当网络，拓宽、加深市场覆盖范围、技能、专业知识、技术、服务和客户群，以进行产品销售的战略。

**产品/服务战略**：供应商的产品开发及交付方法，侧重于可映射到当前及未来要求的差异化、功能、方法和功能包。

**业务模型：**供应商设定商业主张的有效性和逻辑性。

**垂直/产业战略：**供应商用于指导资源、技能、产品，以满足包括垂直市场在内的个别细分市场的具体需求的战略。

**创新：**出于投资、整合、防御或先发制人目的而对资源、专业知识或资本进行的直接、相关、补充和协同布局。

**地区战略：**供应商用于指导资源、技能、产品，以满足“国内”或本土之外的区域的具体要求，无论是直接指导还是通过适用于该区域和市场的合作伙伴、渠道、子公司间接指导。