Gartner Licensed for Distribution

Magic Quadrant for Security Information and Event Management

Published 18 February 2020 - ID G00381093 - 72 min read

By Analysts Kelly Kavanagh, Toby Bussa, Gorka Sadowski

Security and risk management leaders increasingly seek security information and event management solutions with capabilities that support early attack detection, investigation and response. Users should balance advanced SIEM capabilities with the resources needed to run and tune the solution.

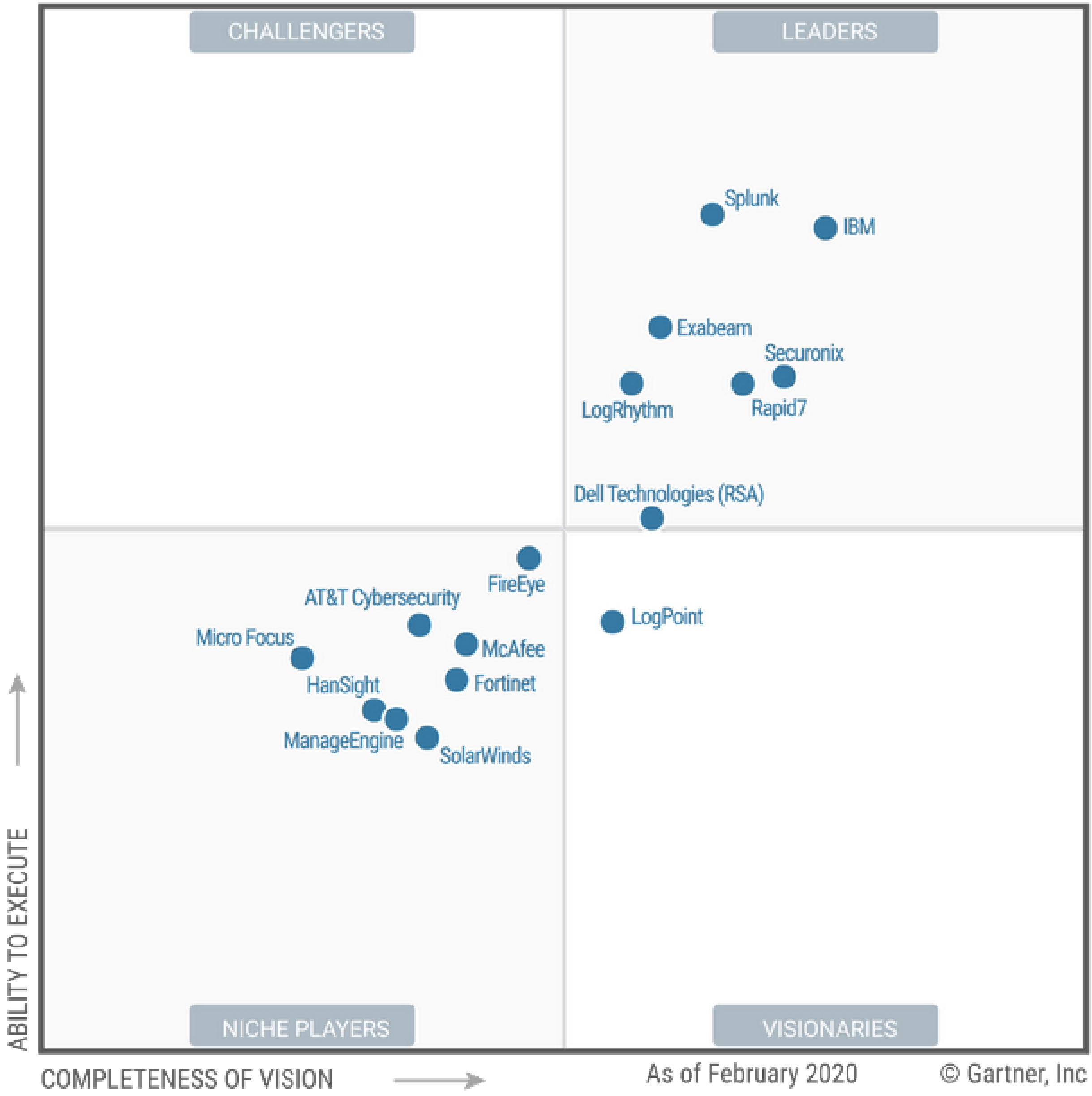
Market Definition/Description

The security information and event management (SIEM) market is defined by customers' need to analyze security event data in real time, which supports the early detection of attacks and breaches. SIEM systems collect, store, investigate, support mitigation and report on security data for incident response, forensics and regulatory compliance. The vendors included in this Magic Quadrant have products designed for this purpose, which they actively market and sell to the security buying center.

SIEM technology aggregates event data produced by security devices, network infrastructure, host and endpoint systems, applications and cloud services. The primary data source is log data, but SIEM technology can also process other forms of data, such as network telemetry (i.e., flows and packets). Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data may be normalized, so that events, data and contextual information from disparate sources can be analyzed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time analysis of events for security monitoring, query and long-range analytics for historical analysis, and other support for incident investigation and management, and reporting — e.g., for compliance requirements.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (February 2020)

Vendor Strengths and Cautions

AT&T Cybersecurity

AT&T Cybersecurity, part of the AT&T Business portfolio, is headquartered in Dallas, Texas. AT&T Cybersecurity's SIEM solution is Unified Security Management (USM) Anywhere, which is delivered as a software as a service (SaaS) solution. It packages several other security elements with SIEM, including asset discovery, vulnerability assessment, an intrusion detection system (IDS) for network and cloud, and endpoint detection and response (EDR). An on-premises software deployment, USM Appliance, is available and is still supported; however, the vendor continues to focus more on the USM Anywhere SaaS offering. USM customers can connect to the Alien Labs Open Threat Exchange

The AlienVault USM Appliance and Anywhere products are licensed on the amount of data analyzed (gigabyte per month) and are offered as subscription-only. There is also licensing for managed security service provider (MSSP) partners who want access to USM's central management console, USM Central, which provides unified dashboards across multiple USM Anywhere deployments.

Advancements during the past 12 months include the addition of an EDR agent to the USM portfolio to provide threat visibility and automated response actions for the major OSs. USM Anywhere now has threat visibility and response capabilities for Google Cloud, as well as enhanced case management features for analysts performing investigations.

Small and midsize businesses (SMBs) in financial services and healthcare verticals, which need SIEM as a service (SaaS SIEM) delivery models with bundled security controls that don't require extensive database or application monitoring or advanced analytics, should consider AT&T Cybersecurity's USM Anywhere.

Strengths

- **Deployment:** The SaaS form factor, combined with predefined content for detections and dashboards, offers relatively quick deployment and initial operation, compared with on-premises SIEM.
- **Operations:** Detection content is updated frequently by the vendor. The USM Anywhere detection rules and dashboards are updated weekly, based on the findings of the AT&T Alien Labs threat intelligence team.
- **Product:** AT&T Cybersecurity offers strong integrations with its own technologies for endpoint agent deployment/management, network intrusion detection, vulnerability scanning/asset discovery and threat intelligence. Native file integrity monitoring (FIM) and EDR capability is above average, although support for third-party solutions is more limited than that of many of its competitors.
- **Product:** Customers that must manage data residency requirements for multiple geographic regions can monitor 13 Amazon Web Services (AWS) regions, with central management available via the USM Central App. Data residency is supported in nine countries: the U.S., Ireland, Germany, Japan, Australia, U.K., Canada, India and Brazil.

Cautions

- **Market Understanding:** AT&T Cybersecurity must manage a complex go-to-market approach for security monitoring. AT&T Cybersecurity offers SaaS SIEM and a managed security offering to end users; however, it competes with a large number of third-party service providers that offer managed services to end users via USM Appliance. AT&T Cybersecurity must create clear relevant to MSE buyers with those relevant to managed services providers, because these target markets typically have differing priorities for features and functions.

- **Product**: Out-of-the-box integrations relevant to enterprise SIEM deployments are missing or limited. USM Anywhere does not integrate with identity repositories for user authentication, nor is there integration with ERP solutions or third-party, big data platforms or security orchestration, automation and response solutions. Other integrations, via the AlienApps ecosystem, are limited. Support for infrastructure as a service (IaaS) monitoring depends on the deployment of USM Anywhere sensors in AWS and Azure, and Google Cloud Platform (GCP). Monitoring of SaaS via AlienApps is limited to Microsoft Office 365, Google G Suite, Box and Okta, and a handful of others.

- **Product**: USM Anywhere support for user monitoring is basic, compared with many of its competitors. The product does not have native user and entity behavior analytics (UEBA) capability, nor does it provide integrations with third-party UEBA solutions.

- **Product**: There is no feature parity between USM Appliance and USM Anywhere, with more development funding being invested in USM Anywhere.

- **Customer Experience:** AT&T Cybersecurity received clearly mixed reviews for service and support, log management/reporting, and for real-time monitoring from customers, based on Gartner customer feedback via inquiry, and Peer Insights and vendor references.

Dell Technologies (RSA)

RSA is a business within Dell Technologies, which is headquartered in Round Rock, Texas. Its main offices are in Bedford, Massachusetts, as well as Bracknell, U.K.; Singapore; Tokyo, Japan; and Brazil.

The RSA NetWitness Platform (RSA NWP) is composed of several components: RSA NetWitness Logs, RSA NetWitness Endpoint, RSA NetWitness Networks, RSA NetWitness UEBA, and RSA NetWitness Orchestrator. UEBA competencies derive from the 2018 acquisition of Fortscale, while the RSA NetWitness Orchestrator security orchestration automation and response (SOAR) is an OEM of Demisto's SOAR solution.

Licensing is based on the nature of the tool, with pricing for RSA NetWitness Logs, including all components to run the SIEM, based on data volume. (Metered licensing on a perpetual or term basis is the default for all new customers.) Its legacy pricing model can be licensed by appliance capacity (for physical appliances). Clients can add other for-pay components, such as:

- RSA NetWitness Endpoint — based on the number of endpoints

- RSA NetWitness UEBA — based on the number of users monitored

- RSA NetWitness Orchestrator (Demisto OEM reviewed in this research) — based on the number of security analysts

Customers can mix appliance and metered licensing to enable granular capacity growth across the deployment architecture.

RSA NWP Version 11.3, introduced in April 2019, offers some improvements in the RSA NetWitness Endpoint, the introduction of RSA NetWitness Endpoint-specific UEBA models, and a tighter integration between the SIEM and the UEBA solutions.

Enterprises with a mature security operations capability seeking a single-vendor SIEM platform, with native endpoint, network and UEBA modules, as well SOAR capabilities, and support for analytics, forensics/hunting and reporting/compliance, should consider RSA NetWitness Platform.

Strengths

- **Deployment:** Organizations can mix and match appliances, virtual appliances and software to build functional stacks, enabling flexible deployments and horizontal scalability capabilities.
- **Product:** This is mature technology that's well-suited to advanced threat defense (ATD) use cases, thanks to multistage analytics encompassing RSA NWP's wide portfolio of additional, natively integrated solutions for ubiquitous view and analytics across endpoints and networks.
- **Product:** RSA NWP offers a multistage analytics engine with interesting, unsupervised modeling capabilities across endpoints, network and users.
- **Product**: RSA NWP has a strong feature set in support of forensics and threat hunting, with ubiquitous access of forensics artifacts across a wide RSA technology stack — e.g., fetch running process list from endpoints, or packet capture (PCAP) analysis natively inside the NWP user interface (UI).
- **Deployment/Support:** RSA offers RSA Live accessible directly from the NWP console, for access to all RSA NWP content.
- **Sales Execution:** RSA has an extensive worldwide ecosystem of channel partners and service providers offering local support for NWP, for integration, management and/or operations.

Cautions

- **Product Strategy:** RSA's NWP SOAR strategy is based on OEM relationships in a dynamic market (Demisto before the Palo Alto Networks acquisition, and Threat Connect after. RSA indicated they will support Demisto for several years). Clients should validate that RSA's SOAR partner fits their

- **Product:** The UEBA capabilities offer fewer models than some of its competitors. RSA NetWitness's Network UEBA models are slated for release in 1Q20.

- **Deployment/Support:** RSA NWP is not available from the vendor as a SaaS offering, although some RSA partners offer that capability. Organizations that want a vendor-delivered SaaS SIEM may find limitations in the product and should be comfortable with its cloud security roadmap.

- **Product:** Compared with competitors targeting the midmarket, the RSA NetWitness Platform is more complex to deploy and operate for less-mature buyers.

Exabeam

Exabeam's Security Management Platform (SMP) is composed of seven products: Exabeam Data Lake, Exabeam Cloud Connectors, Exabeam Advanced Analytics, Exabeam Threat Hunter, Exabeam Entity Analytics, Exabeam Case Manager and Exabeam Incident Responder. The SMP is available as software for on-premises deployments, and is offered as a cloud-based SIEM, hosted and managed by Exabeam. There are several form factors for on-premises deployments: hardened physical appliances, virtual appliances, dockerized containers, and private or public cloud deployments (in Amazon, Google and Azure). Moreover, an on-premises deployment can consist of multiple form-factor (i.e., physical, virtual and cloud) options.

Exabeam's licensing and pricing models are straightforward. Each of the SMP products is sold as a one- or three-year subscription, and priced by the number of employees in the organization, with the exception of Entity Analytics, which is priced by the number of assets monitored.

During the past 12 months, Exabeam has made several enhancements to SMP:

- A single UI for Advanced Analytics, Threat Hunter, Case Manager and Incident Responder

- Threat intelligence services delivered via the cloud

- Better alignment with the MITRE ATT&CK framework

- Improved alert triaging, allowing for richer user and entity context with alerts

- Risk-score-based activities related to an alert

Enterprises with security operations teams looking for a modular SIEM capable of delivering on simple through complex security use cases, using a pricing structure not based on volume, with native UEBA and SOAR (both for-pay) capabilities should consider Exabeam SMP.

Strengths

SOAR or Cloud Connectors for SaaS and IaaS use cases.

- **Product:** Exabeam SMP provides a strong foundation for monitoring users, entities and identities. This is performed by the core analytics module (Advanced Analytics) via the native UEBA features in the application (e.g., peer group analysis and monitoring for deviations in behavior).
- **Product:** Exabeam's Smart Timelines supports less-experienced SIEM users by leveraging machine learning (ML) to organize relevant logs and events in a timeline view, which simplifies investigation and response activities.
- **Sales:** Exabeam's pricing model is simple. It reduces the buying friction, because it's not based on volume, but rather on the number of employees in the organization per product, except for Entity Analytics, which is licensed by number of assets.
- **Market Understanding:** Exabeam has demonstrated strong growth and increased visibility with Gartner clients, primarily in North America, through its marketing efforts.
- **Customer Experience:** In Gartner customer inquiry, Peer Insights and vendor references, customers give positive evaluations of several elements, such as deployment and support services, evaluation and contract negotiation, and stronger-than-typical marks for behavior analytics.

Cautions

- **Market Understanding:** Although it has sales operations in multiple geographies, Exabeam is still predominantly purchased by buyers in North America. Buyers outside of North America should validate coverage for sales, professional services and support (whether direct or through partners) for their organizations' locations.
- **Market Understanding:** Exabeam is still building out its partner network, especially for services such as managed SIEM. Buyers looking for an SIEM-plus-services engagement should confirm the companies Exabeam has identified as partners that are trained/certified, and can address operational and use-case development requirements.
- **Marketing Execution:** Exabeam should better define capabilities relevant to buyers in vertical industries in which the challenges may be different from those of the general buying public (e.g., energy and utilities). Buyers looking for vertical-specific capabilities should confirm that there is appropriate coverage with Exabeam SMP — e.g., content specific to their verticals in the form of out-of-the-box detections and compliance report templates.
- **Customer Experience:** Based on Gartner inquiry feedback, Peer Insights and vendor references, Exabeam can improve on its integration and deployment, and ease of customization of existing

FireEye

FireEye is headquartered in Milpitas, California. FireEye Helix is the core component of the FireEye SIEM. Helix integrates with other, separately licensed, solutions from FireEye for email, network, endpoint and cloud security. FireEye also offers Expertise On Demand, services for tuning rules, investigating alerts, complementing security teams and responding to breaches. FireEye Helix is offered as SaaS SIEM, hosted in AWS and managed by FireEye. Integrated FireEye security solutions also run in the cloud, but can be optionally operated on-premises, either on physical or virtual systems in a hybrid environment. FireEye Helix is available as subscription-only, and pricing is based on events per second (EPS) in tiers as low as 100 EPS or as high as 150,000 EPS.

During the past 12 months, FireEye has added several enhancements, such as IoC context enrichment, orchestration capabilities for detection and response, and Expertise On Demand. In addition, the cloud integrations portal for cloud-to-cloud direct API integrations requires no customer-deployed appliances.

Organizations leveraging FireEye email, network, endpoint and/or cloud security products, or looking for end-to-end detection and response capabilities in one security solution, with the option for managed services, should consider FireEye.

Strengths

- **Product:** Helix includes packaged queries, curated by FireEye, to provide next-step guidance for investigations. More-extensive playbooks and response integrations are available with the FireEye Security Orchestrator.
- **Product:** FireEye provides an extensive, open API that enables access to all elements available through the UI, which enables users to develop integrations and programmatically interact with the solution.
- **Deployment/Support:** The Helix platform has an extensive set of threat detection rules managed by FireEye and updated daily based on the vendor's strong threat intelligence data acquisition capabilities.
- **Product:** Integrations with the FireEye Endpoint (formerly HX), Network (formerly NX) and Email products for endpoint, network and email forensics provide extensive capabilities for investigations based on forensic data. FireEye threat intelligence is fully integrated, and additional FireEye utilities support evidence collection (Evidence Collector) and response actions (FireEye Security Orchestration).
- **Deployment/Support:** FireEye's Managed Detection and Response service offering enables customers to use the Helix platform to perform their own searches and investigations, with 24/7

- **Product:** FireEye references give positive marks for most capabilities of the product. There is limited feedback from Gartner customers via inquiry or Peer Insights.

Cautions

- **Product:** Support for IaaS and SaaS threat detection is less mature than several competitors. Helix provides detection rules for AWS and Microsoft Office 365, but not yet for other popular IaaS and SaaS applications.
- **Deployment/Support:** Helix's event acquisition features are not as mature as those of many of its competitors. Helix lacks autodiscovery of event sources, and there is no capability for end users to develop new parsers. Log management capabilities depend on the features available from the underlying AWS platform. Customers should validate that the data management available on the AWS platform is sufficient for their requirements.
- **Product:** Compliance reporting capabilities are limited, compared with those of more-established competitors — e.g., there are dashboards only for Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) mandates.
- **Product:** FireEye is growing its technology partner ecosystem, but not all integrations are available throughout the FireEye portfolio. Potential customers should validate that the third-party integrations available with FireEye products — through Security Orchestration, the Helix platform, or the FireEye Network, FireEye Endpoint or other products — support the use cases required.

Fortinet

Fortinet is headquartered in Sunnyvale, California, with 58 offices globally and regional headquarters in Sunrise, Florida; Sophia, France; Sydney; Singapore; and Tokyo.

The Fortinet SIEM solution FortiSIEM includes:

- FortiSIEM Advanced Agent — an agent for Windows and Linux, with some FIM and EDR capabilities
- FortiGuard IoC — a for-pay threat intelligence subscription feed
- FortiInsight — a for-pay, pure-play UEBA tool derived from the ZoneFox acquisition

Fortinet FortiSIEM is part of Fortinet's Security Fabric. This allows enhanced collaboration and integration among several of Fortinet's portfolio solutions (e.g., Fortinet FortiSandbox) for additional, multitool use cases.

FortiSIEM is licensed on the number of assets in scope (number of IP addresses), as well as total

Fortinet FortiSIEM Version 5.2.1, introduced in March 2019, presented the concept of Explorer View that helps security analysts pivot from results to searches when doing forensics and threat hunting, support for IPv6, and additional pseudonymization features to help General Data Protection Regulation (GDPR) customers.

Fortinet FortiSIEM has strong support for organizations with existing Fortinet solutions, or managed service providers (MSPs) supporting Fortinet products, and MSSPs looking to offer Fortinet FortiSIEM as a service, using a low-friction/risk approach.

Strengths

- **Product Strategy:** Fortinet FortiSIEM will appeal to Fortinet-centric organizations, because it directly integrates with several of Fortinet's technologies (e.g., endpoint, sandbox, mail and deception) via the Fortinet Security Fabric for bidirectional automated remediation actions.
- **Product:** Fortinet FortiSIEM offers a solid set of compliance packages natively out of the box (e.g., PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13 and SANS), as well as IT operations and network operations use cases via packaged content.
- **Product:** Fortinet FortiSIEM has powerful asset discovery features and can automatically build an organization's configuration management database (CMDB) by actively scanning the environment and passively listening to network traffic.
- **Product:** Fortinet FortiSIEM delivers on most nonadvanced security use cases, but can also be used as an IT operations and network operations tool, due to its performance and availability monitoring and CMDB capabilities.
- **Customer Experience:** Overall customer satisfaction with FortiSIEM in Gartner inquiry feedback and Peer Insights is generally positive, and aligned with that of many competitors, with higher marks than several competitors for the product's threat intelligence capabilities.
- **Sales Strategy:** Fortinet has a partner program for MSSP with pay as you go (PAYG) partnership models that can encourage MSSPs to deliver FortiSIEM as a service.

Cautions

- **Product Strategy:** Fortinet customers planning to support OT/Internet of Things (IoT) monitoring will need to use partner products to parse events and integrate CMDB information.
- **Product Strategy:** Fortinet FortiSIEM's cloud security functional coverage is not as strong as other competitors — e.g., it lacks support for GCP and IBM Cloud.
- **Product:** Fortinet FortiSIEM's real-time advanced analytics capabilities lag those of some

- **Product:** Organizations looking to use Fortinet FortiSIEM as a case and incident management platform for forensics or threat hunting will find that the case creation and management is less intuitive than other tools, and there are no native integrations with threat-hunting tools.
- **Sales Strategy:** Fortinet does not offer SaaS SIEM. Clients seeking it will need to use Fortinet's MSSP partner.
- **Customer Experience:** Customers express lower satisfaction with FortiSIEM sales/support-related areas. This may indicate that Fortinet's partner-led go-to-market strategy is not as strong for SIEM as for other products.

HanSight

HanSight is a vendor with headquarters in Beijing, China. HanSight primarily sells in China, as well as other areas of the Asia/Pacific (APAC) region (e.g., Japan and Singapore) and Latin America through channel partners. HanSight Enterprise SIEM is the core product. It is part of an ecosystem of solutions that includes UEBA; network traffic analytics (NTA), with IDS capabilities; vulnerability management; asset discovery; data loss prevention (DLP); and threat intelligence management. EDR and cloud workload protection platform (CWPP) capabilities are provided through partnerships with several Chinese security technology vendors.

The platform is available as software, a hardware appliance (for smaller deployments) or as a hosted platform. HanSight's on-premises solutions are licensed as perpetual plus annual maintenance. Enterprise SIEM is priced by data velocity (EPS), with a tiered discount. Other modules are priced by the number of users (UEBA), the sensors deployed and bandwidth (NTA), and assets (VM and Assets). Hosted Enterprise SIEM is based on the standard pricing, plus an uplift for hosting the application, and is licensed on a subscription model.

During the past 12 months, HanSight added its HanSight Query Language (HQL) for search capabilities, introduced the DLP add-on, and added event aggregation and incident timeline visualizations.

Organizations in China — particularly those in the banking and financial sectors looking for an SIEM with an ecosystem for their security operations focused on supporting technologies in the region — should consider HanSight.

Strengths

- **Product:** HanSight offers a strong ecosystem of technologies that complement its core SIEM solution, which will appeal to organizations looking to instrument a modern security operations center (SOC) from a single vendor.

- **Product:** HQL and the search function include features such as an integrated development environment (IDE)-style analysts' notebook capability, as well as the ability to share saved searches via quick response (QR) code.

- **Customer Experience:** Based on Gartner Peer Insights and vendor customer references, users give above-average scores for service and support, compared with the competition, especially for support.

Cautions

- **Operations:** HanSight primarily competes in the Chinese market and has limited visibility outside that market. Channel partners outside the APAC region are limited to Latin America. There is no direct sales channel in North America or Europe.

- **Product:** Monitoring coverage is still variable. There is good coverage for cloud environments, including AWS and Alibaba; however, support for virtual environments, such as VMware and Hyper-V, is not yet available, nor is data collection from Azure.

- **Product Strategy:** Some features and functionality (e.g., threat intelligence management) are localized to Chinese and are unavailable in other languages.

- **Customer Experience:** Based on feedback from Gartner Peer Insights and vendor references, log management and incident management capabilities are areas for improvement.

IBM

IBM Security provides a range of security technologies and services, and is headquartered in Cambridge, Massachusetts. The QRadar Security Intelligence Platform is primarily built around the QRadar SIEM solution and composed of several other separately priced components:

- IBM QRadar Vulnerability Manager — integration of vulnerability assessment data

- IBM QRadar Network Insights — QFl application visibility and packet content inspection

- QRadar Risk Manager — network device configuration monitoring and threat simulation capabilities

- IBM QRadar User Behavior Analytics (UBA) — a free add-on module that addresses some insider threat use cases

- IBM QRadar Incident Forensics — forensic investigation support

- IBM QRadar Advisor with Watson — advanced analytics-based root cause identification and

IBM also offers the Security App Exchange, which enables QRadar customers to download curated content developed by IBM or third parties to extend IBM QRadar’s coverage or value proposition. Other relevant IBM solutions include the IBM QRadar Network Packet Capture appliance, for stronger network forensics capabilities, and IBM Resilient, a SOAR solution that has supported, bidirectional integration between Resilient and the QRadar SIEM solution. This can help organizations streamline their security incident workflow processes.

IBM QRadar SIEM can be deployed on-premises, via hardware virtual appliances and software packages, or it can be hosted in the cloud via IBM’s cloud-based SIEM solution, QRadar on Cloud (QROC). Core SIEM licensing is based on the customer’s event velocity (number of EPS across the data sources in scope) and flows per minute (FPM). It can be procured via a perpetual license or subscription — the latter is offered only if the customer is purchasing QROC. Pricing for other components in the IBM QRadar Security Intelligence Platform depends on their respective metrics, e.g.:

- The number of flows for IBM QRadar Network Insights
- The number of assets in scope for IBM QRadar Vulnerability Manager
- The number of systems from which configuration data is pulled for IBM QRadar Risk Manager

QRadar Network Insights is available only in hardware appliance format, and QRadar Incident Forensics is only sold as a perpetual license.

During the past 12 months, IBM has improved alert efficiency via its Tuning App, simplified data ingestion from various sources, whereby extracting event properties from a common log format can be accomplished with little or no customization required. IBM has also mapped its QRadar Advisor with Watson to the MITRE ATT&CK framework.

IBM has a wide customer base on the end-user and MSSP side, and tends to appeal to larger organizations, by offering a robust platform to build a threat detection and response function. However, smaller organizations can also benefit from the QRadar SIEM solution, with its relative ease of use and extensive out-of-the-box content for less-advanced security use cases.

Strengths

- **Sales Strategy:** IBM has extensive internal resources and partnerships to support sales, deployment and operational support, including managed services for QRadar, across multiple geographic regions.
- **Deployment/Support:** QRadar offers users extensive options in deployment architecture, with a

license for cloud deployment. The exception is the Network Insights component, which is available as a physical appliance only.

- **Operations:** QRadar has extensive open API to enable customers and partners to develop integrations with the platform. The app marketplace has extensive integrations provided by IBM and by third parties.

- **Product:** QRadar offers strong capabilities for managing the collection of events. Users can configure logging to automatically detect multiple event formats, with options to filter them, forward them to real-time analytics or to bypass the analytics tier and send to the data store. Direct forwarding of events to the data store does not contribute to the EPS licensing metric.

- **Sales Strategy:** QRadar includes UBA in the base licensing for QRadar, so there is no additional cost to acquire UBA.

- **Product:** The QRadar Advisor with Watson offers strong support for incident investigation by providing context enrichment from internal and external sources, suggesting next steps based on attacker actions and prioritizing alerts for further action.

Cautions

- **Pricing:** The several licensing models and pricing schemes for the various components associated with the QRadar platform present a complex set of choices for potential customers. Models include perpetual and term licensing, based on several factors that include data velocity, number of assets, and whether the technology is deployed on-premises or in the IBM cloud. A QRadar solution might include a mix of perpetual and term licensing, depending on the technology and deployment choices.

- **Product Strategy:** QRadar offers limited options for data collection for forensics from endpoints/hosts. IBM’s lack of native EDR capability is in contrast with the fuller capabilities for network monitoring. Customers must deploy third-party products or rely on its WinCollect agent or Sysmon for Windows collection.

- **Operations:** The modernization of the user experience (UX) for QRadar is still a work in progress, and the UI is not consistent across the various components of the platform.

- **Pricing:** IBM is demonstrating increasing reliance on their add-on products, available for additional cost, such as Resilient and QRadar Advisor for incident response capabilities, such as prioritization, investigation, context assembly and other response actions.

- **Innovation:** The components of the QRadar platform are at differing levels of maturity and

- **Customer Experience:** Based on Gartner customer feedback via inquiries, Peer Insights reviews and vendor references, QRadar's analytics and behavior profiling, and the vendor's sales/contracting processes are areas for improvement.

LogPoint

LogPoint is headquartered in Copenhagen, Denmark, with offices in Europe, The Middle East and Africa (EMEA; e.g., London, Paris and Munich); in the U.S. (Boston); and the APAC region (e.g., Kathmandu). LogPoint SIEM solution is composed of the following modules:

- LogPoint Core SIEM
- LogPoint UEBA
- LogPoint Director (which includes Console and Fabric)
- LogPoint Applied Analytics

LogPoint's core SIEM license is a subscription based on the number of assets (number of IP addresses), and includes all modules, except LogPoint UEBA, which is licensed for additional cost, based on the number of employees and assets.

LogPoint SIEM and all of their components can be deployed on-premises via a physical or software appliance (based on a hardened version of Linux Ubuntu), while the UEBA solution is delivered as a SaaS model. LogPoint Version 6.6.1 introduced in June 2019 offered improvements in incident investigation via data mining and visualizations, while UEBA Version 2.1.0 can detect anomalies across users and entities.

LogPoint will appeal to enterprises and MSSPs looking for a European vendor, and to privacy-conscious organizations looking for an SIEM with predictable, asset-based licensing, and basic incident response capabilities.

Strengths

- **Pricing:** LogPoint will appeal to organizations looking for an SIEM vendor with predictable pricing based on number of assets. LogPoint offers special pricing models for selected verticals. As an example, LogPoint offers hospitals a fixed fee based on the number of beds, municipalities a fixed fee based on the number of inhabitants, and universities a fixed fee based on the number of students.
- **Product Strategy:** LogPoint is an EMEA-based SIEM provider with an acute appreciation of privacy requirements that delivers advanced features in data masking and obfuscation for GDPR and

- **Product:** LogPoint offers two stages of enrichment of data: at ingest time for static data (e.g., IP to MAC) and at time of search, with latest available threat intelligence.
- **Sales/Partner Strategy:** LogPoint has developed a dense ecosystem of channel and MSSP partners in Europe, making LogPoint widely available as a product or a service.
- **Product:** LogPoint is natively multitenant through a federated model in which each tenant is connected to a management fabric, facilitating adoption by MSSPs.
- **Market Understanding:** LogPoint has carved some niche markets with interesting capabilities and security use cases for organizations extensively using SAP, or utilities using specific IoT equipment, such as Siemens wind turbines.

Cautions

- **Sales Execution:** LogPoint's U.S. expansion remains nascent; LogPoint has less visibility among Gartner's North American clients, and outside EMEA generally.
- **Product Strategy:** Although LogPoint is natively available as ready-to-run images for AWS and Azure, the SIEM is not available as SaaS from LogPoint, but UEBA is only available as SaaS.
- **Product Strategy:** LogPoint makes extensive use of query languages for rules, dashboards and alerts, which require training and familiarity with the syntax.
- **Product:** Case management and SOC collaboration features are basic and might not support all aspects of SOC operations. Integrations are provided with several SOAR products.
- **Product:** Clients looking to get advanced analytics capabilities for typical UEBA use cases, such as user monitoring need to be ready to purchase the additional UEBA module as the core SIEM's native ML capabilities are limited.
- **Product:** Collection and parsing for custom-made data sources (e.g., custom business applications) is done via "plug-ins," which need to be developed by LogPoint or configured by the customer. Cloud monitoring feature set is emerging — for example, there is no support for GCP or IBM Cloud.

LogRhythm

LogRhythm is headquartered in Boulder, Colorado, and brands its SIEM solution as LogRhythm NextGen SIEM Platform. The core SIEM component is the XDR Stack, which is made up of DetectX, AnalytiX and RespondX. Add-on modules include UserXDR, LogRhythm's rebranded UEBA product, and NetworkXDR, which provides NTA capabilities, as well as System Monitor (SysMon Lite and Pro)

(LogRhythm Enterprise) and midsize (LogRhythm XM) enterprises. It can be deployed on-premises as software, a physical appliance or a virtual appliance, in IaaS or hybrid environments.

LogRhythm's cloud-based SIEM offering, LogRhythm Cloud, is also available, and hosted and administered by the vendor. The XM solution is an all-in-one appliance; horizontal scalability is possible as the various discrete components that make up the LogRhythm platform can be deployed as stand-alone as required. Multitenancy is also natively supported.

LogRhythm's core product, the XDR Stack, is licensed based on data velocity (aka messages per second [MPS]). Although UserXDR is licensed based on the number of users being monitored, and NetworkXDR (or NDR) and Network Monitor are licensed based on gigabits per second (Gbps), System Monitor is priced per agent. Licenses are available as perpetual or term, along with enterprisewide agreements. At the beginning of October 2019, LogRhythm announced its Unlimited Data Plan (ULP) offering to help eliminate consumption-based capacity tracking and improve budget predictability.

During the past 12 months, LogRhythm has introduced its cloud-based version, branded as LogRhythm Cloud. It has introduced a software-license model decoupled from their physical hardware (allowing the solution to be installed on customer hardware, in IaaS or a hybrid model across LogRhythm appliances, customer infrastructure and IaaS). It has also added enhanced automation, integrations and case management features, and its Echo and LogWars features leverage its SIEM as a training tool for users.

Organizations that prefer a single-vendor ecosystem to instrument their security operations team for threat monitoring and response, and compliance use cases, along with flexible deployment options, should consider LogRhythm.

Strengths

- **Product Strategy:** LogRhythm offers a single-vendor-ecosystem approach for buyers that want a unified solution that includes core SIEM, network monitoring, endpoint monitoring and UEBA.
- **Deployment/Operations:** The range of professional services, from onboarding to ongoing support, is extensive. LogRhythm customers can take advantage of various co-pilot products to provide additional support for initial implementation, and for ongoing operations and use of the solutions.
- **Deployment:** LogRhythm has a strong set of options for running its core SIEM solution, including physical hardware, software (for installation on-premises or in IaaS, such as AWS, Azure and Google Cloud), and as SaaS.
- **Product:** LogRhythm offers an extensive range of compliance reports across a variety of industries and regulations worldwide

- **Customer Experience:** LogRhythm customers offer generally positive feedback on product capabilities.

Cautions

- **Product Strategy:** LogRhythm continues to lag competitors in areas such as moving the platform toward a modern SIEM architecture (e.g., it's still a mix of Windows Server, MS SQL and Linux OS), and the lack of a dedicated SOAR offering.
- **Market Understanding:** Support for monitoring in IaaS is lagging, compared with competitors. It's unclear whether API, Sysmon or other agents (e.g., Beats) may be the preferred mechanism to collect data out of cloud services provider (CSP) environment.
- **Marketing Execution:** LogRhythm has added new branding on top of its product names, with the XDR Stack branding. However, this adds more complexity into an existing mix of product names and features (Next Gen SIEM, CloudAI [for UEBA], Sysmon, Netmon, LogRhythm Cloud, AI Engine, etc.). Buyers should validate what is being proposed to them and determine whether the products and components meet their use cases and requirements.
- **Product:** Customers that require on-premises-only deployments will need to address the cloud-only delivery of CloudAI capabilities.
- **Customer Experience:** Feedback from Gartner customer inquiries, from Peer Insights review and from vendor references on capabilities, such as the usefulness of predefined reports and the effectiveness of predefined rules represent opportunities for improvement. Customers offer mixed feedback on deployment and support ease.

ManageEngine

ManageEngine has headquarters in India (Chennai), as well as in the U.S. (Austin, Texas). ManageEngine's core SIEM product is Log360, but also includes several other modules — at an additional cost — that can integrate with Log360 and address security and IT operations use cases. These include:

- ManageEngine ADAudit Plus — Active Directory (AD) change auditing and reporting
- ManageEngine EventLog Analyzer — central log management
- ManageEngine Cloud Security Plus — central log management (CLM) and SIEM for AWS and Azure
- ManageEngine Log360 UEBA

- ManageEngine Exchange Reporter Plus — Exchange Server change audits and reporting

ManageEngine Log360 is a software SIEM solution that can be deployed on-premises on physical or virtual systems. It is offered as a perpetual or term license, and pricing is based on the number of event sources or assets in scope. Individual components are licensed based on the number of assets (which varies depending on the specific component). A web-based, cloud-hosted log storage platform, ManageEngine Log360 Cloud, is available. It stores the data collected by the log management module, EventLog Analyzer. However, it is not a SaaS-based SIEM tool. Log360 Cloud is available as a subscription, with pricing based on the storage space required. Cloud Security Plus' pricing is based on the number of cloud accounts in scope, with upsell pricing for additional AWS S3 buckets.

During the past 12 months, ManageEngine has made the following advancements for the Log360 SIEM solution:

- The ability to create and manage incident workflows
- Integration with ManageEngine Log360 UEBA — providing user activity anomaly detection capabilities, storage optimization and the indexing of performance improvements
- The addition of the DataSecurity Plus module — providing data discovery, file storage analysis and Windows file server auditing capabilities

SMBs with Windows-centric and AWS/Azure environments that want to address IT operations, in addition to basic security event monitoring and threat detection use cases, should consider ManageEngine.

Strengths

- **Product**: ManageEngine provides above-average compliance reporting, including PCI DSS, HIPAA, FISMA, SOX, GLBA, GDPR, and several other industry- and region-specific mandates that are included out of the box.
- **Product**: Log360 supports automatic discovery of syslog devices on a customer network, which can be added to the event sources monitored by the solution.
- **Operations:** Several response workflows are included with Log360. Actions associated with these include blocking USBs, disabling users and killing processes. Some actions may require other ManageEngine products.
- **Customer Experience:** ManageEngine customers, based on Gartner Peer Insights data and vendor-

Cautions section, such as integrations with other products, and user, data and application monitoring.

Cautions

- **Product Strategy:** Several integrations relevant to enterprise SIEM deployments are missing or limited. There is no support for security orchestration, automation and response solutions, FIM or EDR products, UEBA products, or ERP solutions. Log360 does not have open APIs to support customer integrations.
- **Product:** Data monitoring support is limited to MS SQL and Oracle logs, with no support for DLP or database audit and protection (DAP). Network-based monitoring is only supported via third-party solutions.
- **Product:** Support for management of log data is limited. For example, Log360 does not support multiple log data retention policies.
- **Product:** User monitoring is a work in progress. The ADAudit Plus product provides AD monitoring, and ManageEngine has added basic anomaly detection and risk scoring. However, richer UEBA capabilities are not available.
- **Product:** Support for ATD is limited. Payload detection, network traffic analysis and forensics support require third-party products.

McAfee

McAfee is headquartered in Santa Clara, California, with main offices in Slough, U.K.; Singapore; Tokyo, Japan; and Sao Paulo, Brazil.

McAfee Enterprise Security Manager (ESM) is composed of the Event Receiver (ERC), Enterprise Log Search (ELS), Enterprise Log Manager (ELM), and the Advanced Correlation Engine (ACE). In addition, McAfee ESM can be extended and enhanced with McAfee Direct Attached Storage (DAS) for additional log storage capacity, or McAfee Global Threat Intelligence (GTI) for IP reputation. Other use cases require additional modules such as McAfee Application Data Monitor (ADM) for Layer 7 application monitoring, or McAfee MVISION Cloud (McAfee's CASB product) for UEBA features on cloud access.

McAfee ESM is sold as perpetual licenses for physical or virtual appliances. Its pricing model is based on velocity (EPS, aka MPS). It is sized according to the expected EPS in the given customer environment. Customers can increase EPS capacity and/or data source volume until the capacity of their appliance is reached, and can cluster appliances for additional horizontal scalability. McAfee

McAfee ESM's version 11.2.1, which was introduced in July 2019, is the one analyzed in this research. This version leverages McAfee's Data Streaming Bus (DSB) architecture, which enables resiliency for hierarchical ESMs, and message routing/forwarding to internal or third-party modules.

Organizations with mature, complex environments and significant investment in McAfee technology for data protection and endpoint security should consider McAfee ESM.

Strengths

- **Product Strategy:** McAfee offers integration among its broad portfolio of solutions addressing security operations and can complement McAfee ESM (e.g., McAfee Threat Intelligence Exchange, or McAfee Active Response for advanced orchestration capabilities).
- **Product:** McAfee ESM offers powerful bidirectional integrations for automated responses with McAfee MVISION EDR, Advanced Threat Defense (ATD), Network Security Platform (NSP) and Web Gateway (MWG).
- **Product Strategy:** McAfee's ecosystem of technology alliances (McAfee SIA) offers more than 115 active partners, of which 44 are direct ESM integrations or content contributors.
- **Product:** McAfee ESM data acquisition and management feature set is particularly strong — for example, implementing McAfee's Data Streaming Bus scalability, and support for federated organizations with complex governance requirements.
- **Sales Strategy:** McAfee enjoys a strong global presence — for example, in EMEA, with a dense ecosystem of channel and services partners available to organizations requiring consulting, implementation, operations and/or managed services.

Cautions

- **Product:** McAfee ESM lacks UEBA, and its UBA content pack affords a limited set of use cases. There is no dynamic peer grouping done by the tool.
- **Product:** Although McAfee ESM can provide analytics-based risk scores for suspicious events, the product lags competitors in mapping of these events against frameworks such as Cyber Kill Chain or MITRE ATT&CK to create a timeline of an attack.
- **Product:** McAfee's ESM native SOAR capabilities for response and playbook automation outside McAfee's portfolio (e.g., MVISION EDR, McAfee Active Response, McAfee Advanced Threat Defense) lag those of competitors.
- **Product:** Clients should validate that ESM will support their data governance requirements. There is no native encryption for the data stored (data at rest) in ESM. Masking/obfuscation capabilities

Micro Focus

Micro Focus, headquartered in Newbury, U.K., offers its ArcSight platform as its SIEM solution. The ArcSight solution is composed of the core SIEM solution, data collection and management components, UEBA, and incident investigation and management. Other add-ons include content-specific packages for compliance, application monitoring and other use cases. Other products in the Micro Focus portfolio also support security use cases, including Application Defender and Voltage data protection solutions. Micro Focus also offers ArcSight Marketplace as the source for customers to identify and implement content packages and technology integrations. ArcSight can be deployed via physical appliances or as software. Pricing for the ArcSight platform is primarily based around EPS, except for Interset UEBA, which is priced by the number of employees.

During the past 12 months, Micro Focus acquired Interset for UEBA, and split the ArcSight Data Platform (ADP) solution into two stand-alone components: Logger and Security Open Data Platform (SODP) with the Transformation Hub. It also introduced new pricing models for the ArcSight portfolio, based around only EPS (e.g., removing volume-pricing elements).

Enterprises with mature security monitoring operations that require high data ingestion capabilities and scalable options, along with the flexibility to route data to various sources, should consider ArcSight.

Strengths

- **Product Strategy:** Micro Focus acquired Interset UEBA in February 2019, adding an in-house UEBA capability that may be integrated more tightly with the ArcSight SIEM. The Interset technology replaces the OEM version of Securonix previously sold with ArcSight.

- **Product Strategy:** The ArcSight platform supports large enterprises and service providers with environments that require scalable and distributed architectures that can prefilter, and then ingest data at high velocities, along with flexible data-routing options — e.g., Logger, Investigate or a stand-alone Elasticsearch environment.

- **Product:** ArcSight has a comprehensive set of out-of-the-box compliance use cases and support for mapping events to MITRE ATT&CK.

- **Customer Experience:** Reference customers give above-average marks to ArcSight’s real-time monitoring capabilities and its ease of customizing correlation rules.

Cautions

- **Product:** Micro Focus must invest in capability upgrades to the ArcSight platform, such as improving the UI/UX and further integrating the Interset product. Buyers and existing ArcSight

- **Innovation:** Micro Focus is lagging competing vendors offering native SOAR capabilities, a SaaS offering, and deeper support for monitoring IaaS and SaaS and other new environments of concern to customers, such as OT and IoT.

- **Deployment:** Deployment options for the solution vary by component. Connectors, Logger and ESM are available as software and physical appliances. There are images available for ArcSight Management Center, ESM and Logger in AWS and Azure. Investigate and Transformation Hub have completed the containerization process. No SaaS options are available to buyers.

- **Sales Execution:** Based on Gartner customer inquiry, Micro Focus ArcSight rarely appears on shortlists for new SIEM deployments outside the Middle East and India.

- **Customer Experience:** Based on Gartner customer inquiries, Peer Insights reviews and vendor references, Micro Focus needs improvement in sales/contracting and technical support. The same sources indicate that product functions that lag those of competitors include deployment and support simplicity, behavior profiling, analytics, query/investigation capabilities, workflow, and case management.

Rapid7

Rapid7 is based out of Boston, Massachusetts. The company's Insight platform is composed of InsightIDR (its core SIEM/UEBA offering), InsightVM (vulnerability assessment), InsightAppSec (application security), InsightConnect (SOAR) and InsightOps (log management for IT operations). Rapid7 offers Insight Agent as its preferred endpoint agent to enable telemetry gathering and basic bidirectional response integration capabilities with Rapid7 InsightIDR, Rapid7 InsightVM and Rapid7 InsightOps. InsightIDR also offers integration with InsightVM, which allows customers to deploy one agent across the environment to instrument and collect vulnerability assessment data, while performing detection and response functions.

Rapid7 InsightIDR is a SaaS SIEM solution deployed in AWS, leveraging Insight Collectors or Insight Agents deployed in the customer's organization to collect, centralize and transmit logs. Rapid7 offers 24/7 threat monitoring and investigation and response functionality via its Managed Detection and Response (MDR) service offering.

Rapid7 InsightIDR's licensing is subscription-based and is priced by the number of assets in scope (typically servers, desktops and laptops) in a customer's environment, with tiered pricing for larger numbers of assets.

In April 2019, Rapid7 acquired NetFort, a small NTA company, with the intent to use its network sensor to collect, analyze and send network data to the Insight platform. Other enhancements during the past year include new FIM capabilities, cloud detections and support for AWS and Azure

SMBs that have limited security operations resources looking for a SaaS-based SIEM solution should consider Rapid7, given the breadth of the Insight platform offerings and option to outsource 24/7 detection and response to the same vendor.

Strengths

- **Deployment and Support:** InsightIDR is a SaaS offering, and requires only the deployment of endpoint agents or collectors on-premises. The architecture provides for relatively easy customer proof of concept (POC) engagements, and fast rollover into production use. Rapid7 manages all patches and platform updates, as well as detection, response and report content updates.

- **Product Strategy:** Rapid7's portfolio of complementary technologies (e.g., vulnerability management and SOAR) helps organizations address several aspects of security operations, including threat detection and response. For those clients still concerned with 24/7 monitoring of their Rapid7 environment, Rapid7 can offer managed services for threat detection and response based on InsightIDR.

- **Product:** InsightIDR offers strong support for UBA, with out-of-the-box use cases based on anomalous activities. In general, there is a user-centric lens in the incident identification and investigation features of the product, because context and risk scores for users are available to analysts throughout.

- **Product**: Native support for FIM and endpoint is strong, compared with that of competitor vendors. The endpoint agent can also be used to deploy deceptive credentials, a differentiator among SIEM products.

- **Customer Experience:** Based on feedback from Gartner customer inquiry, Peer Insights reviews and vendor references, Rapid7 users give the vendor generally strong marks, and especially strong for simplicity of deployment (and POC engagements).

Cautions

- **Product Strategy:** InsightIDR has integrations among the technology components of the Insight platform, but a relatively small technology alliance ecosystem. Bidirectional integrations with third-party detection, analytics and response technologies are limited, and there are no integrations with big data platforms. The InsightConnect product is required to enable additional integrations with response and bidirectional technologies.

- **Product Strategy:** Reliance on agents for log collection limits support for OT/IoT use cases to InsightIDR's honeypot deployments. The acquisition of Netfort may bring additional capabilities to these use cases via network monitoring.

analysis features support compliance with specific privacy requirements.

- **Product:** InsightIDR runs on top of AWS, and log management, encryption and archiving depend on the capabilities of that platform and are subject to the licensing conditions of the platform. Customers should validate that the log archiving/management capabilities of InsightIDR align with their own requirements.
- **Customer Experience:** Feedback from Gartner customers via inquiry, Peer Insights reviews and vendor references indicate that application monitoring and the availability of third-party resources for services are areas for improvement.

Securonix

Securonix is headquartered in Addison, Texas. Securonix's SIEM platform consists of the following components: Securonix SIEM, Security Data Lake, UEBA, SOAR, NTA, Threat Intelligence and Apps that provide support and packaged content for addressing specific use cases.

In 2019, Securonix moved to a SaaS SIEM, based in AWS, as the standard deployment model, and most new customers use that model. Customers deploy Remote Ingestor Nodes (RINs) for data collection and transport to the cloud. The solution is offered as a term-based subscription (perpetual licenses are available on an exception basis), and the Securonix pricing model is based on the number of customer employees. There is an additional cost element for hosting, which is based on EPS, plus data storage volume and duration requirements.

Capabilities introduced during the past year include shared multitenant architecture, the SNYPR-EYE deployment and management console, a new OEM, resell and technology-based capabilities for NTA and SOAR, endpoint and database monitoring, and cloud and identity monitoring.

Mature security organizations looking for full-featured, analytics-driven SaaS SIEM, capable of powering an SOC for threat detection and response across complex use cases (e.g., insider threat); hybrid environments (e.g., multiclouds); threat hunting; and compliance, should consider Securonix SIEM.

Strengths

- **Product Strategy:** Securonix has strong cloud support and commitment. Its SIEM is cloud-native and is offered as a service, with three different tenant models (shared, dedicated and isolated).
- **Product:** Securonix offers multilayer analytics, with UEBA capabilities for advanced analytics and behavior modeling across both users and entities, support for complex and advanced use cases (e.g., APT, insider threat and fraud), and mapping of detected attacks to common frameworks, such as the MITRE ATT&CK framework.

- **Product Strategy:** Securonix provides extensive out-of-the-box content, organized in vertical packages (most for an additional cost). It includes complete use cases, analytics, alerts, dashboards and even response playbooks.

- **Product Strategy:** The introduction of SNYPR-EYE provides SIEM managers isolation from the Hadoop technologies, while enabling those with sufficient resources to access underlying Hadoop infrastructures.

- **Product:** Securonix offers advanced obfuscation features, with role-based access control (RBAC) workflows, as well as native encryption features that go beyond those provided natively by AWS.

- **Customer Experience:** Based on Gartner customer inquiry, Peer Insights reviews and vendor reference data, Securonix receives high marks for analytics and user-monitoring capabilities.

Cautions

- **Deployment/Support**: Securonix's approach to filling functional coverage gaps by OEM, resell and technology partnerships introduces risks, because dependencies are created. Clients should understand both parties' roadmaps and longer-term commitments, and assess support and maintenance structures.

- **Marketing Execution:** Securonix's efforts in marketing its brand and tools need continued investment, and should better leverage its technology alliance, partner and OEM relationships (such as those mentioned above).

- **Product Strategy:** Securonix has introduced SNYPR-EYE to improve the platform management experience, and content packages for faster time to value for specific use cases and verticals. However, it will be difficult for Securonix SIEM to continue addressing complex use cases and mature organizations, while remaining simple enough to appeal to nonmature organizations.

- **Deployment and Operations:** The enablement of the full functional coverage of Securonix SIEM, especially features that address advanced use cases, such as multiproduct insider threat, requires effort and expertise.

SolarWinds

SolarWinds is headquartered in Austin, Texas, and offers its SolarWind Security Event Manager (SEM) SIEM solution. SEM includes core SIEM features that provide data management, real-time correlation and log searching to support threat and compliance monitoring, investigations and response. SolarWinds SEM is composed of the Manager and Console, and also includes a multifunction endpoint agent. As a complement to SEM's core features, SolarWinds portfolio includes products for

Licenses are perpetual with annual maintenance. SolarWinds has announced plans to introduce subscription-based pricing in 2020.

SEM is deployed as a self-contained virtual appliance that includes all components (e.g., database and correlation engine). SEM can also be deployed in Microsoft Azure or Amazon AWS.

During the past 12 months, SolarWinds has rebranded Log and Event Manager (LEM) to SEM, along with a new versioning scheme introduced in November 2019. It has also begun to support HTML5-based UIs and UX (migrating away from Flash), and has introduced the ability to deploy SEM into AWS.

SMBs with compliance-focused use cases looking for a simplified overall SIEM experience, as well as existing SolarWinds customers looking to integrate security monitoring into their environments, should consider SolarWinds SEM.

Strengths

- **Deployment/Operations:** SolarWinds emphasizes a do-it-yourself (DIY) approach through a combination of self-service POC (via a 30-day trial version), simplified pricing model, ease of deployment and operation, and a robust peer user community called THWACK. It has received high scores from reference customers.

- **Product:** SolarWinds SEM offers a large, out-of-the-box repository of threat detection rules and compliance content, as well as FIM capabilities included with the solution that support a wide variety of operating systems (e.g., Windows, Linux, macOS and IBM AIX).

- **Customer Experience:** Reference customers give real-time monitoring capabilities high marks, compared with the product’s other capabilities, and ease of deployment, integration and support simplicity are above average, compared with the competition.

Cautions

- **Marketing Strategy:** SolarWinds SEM is predominantly sold in North America and Europe; however, it lacks marketing visibility and channel partners outside these two regions.

- **Pricing:** Licensing models are limited to perpetual only, and deployment options are limited to just virtual appliances for SEM.

- **Product:** SolarWinds lacks features built into many competing SIEMs — for example, native case management/incident management functionality and support for monitoring cloud environments. Customers can leverage other products in the SolarWinds portfolio to complement SEM — for example, Service Desk for case management, and Papertrail and Loggly for log collection and

Splunk

Splunk is headquartered in San Francisco, California. The company's Security Operations Suite includes core products, Splunk Enterprise or Splunk Cloud. There are three security-specific solutions: Splunk Enterprise Security (ES), which Gartner considers mandatory for SIEM; Splunk UBA; and Splunk Phantom. All three are sold as premium, stand-alone products. Splunk Enterprise and Splunk Cloud provide event and data collection, search, and visualizations for various uses in IT operations and some security use cases. ES delivers most of the security content and event-monitoring capabilities, including security-specific queries, visualizations and dashboards, and some case management, workflow and incident response capabilities. UBA adds unsupervised ML-driven, advanced analytics. Phantom provides SOAR capabilities and is designed to provide automated remediation and mitigation of security incidents. Additional apps for security use cases are available through Splunkbase, such as Splunk App for PCI Compliance.

There are multiple deployment options: software on-premises, in IaaS and as a hybrid model. Splunk hosts and operates Splunk Cloud, which is a SaaS solution using AWS infrastructure. Splunk Enterprise and Splunk Cloud components consist of Universal Forwarders, Indexers and Search Heads supporting n-tier architectures.

Splunk Enterprise and Cloud licensing is based on the amount of data ingested into the platform (or gigabytes per day). The only difference is Splunk Cloud includes pricing based on the amount of data retained as storage in Splunk's AWS environment. Lower pricing is available for data coming from high-volume, low-value log sources, such as Domain Name System (DNS) and NetFlow. ES is also licensed on a consumption basis and is priced as a percentage of Splunk Enterprise. UBA is licensed by the number of user accounts in an organization. However, if customers prefer to coordinate UBA licensing with their other Splunk licenses, they can choose to purchase a consumption-based license for UBA, with pricing as a specified percentage of ES. All of Splunk's Security Operations Suite products are now only available as term licenses, with various options for enterprisewide pricing and true-ups. Phantom has two different licensing models. One is priced by the number of events on which users take action, and the other is priced by the number of licensed seatholders, or users of the tool.

Splunk's most important enhancements during the past 12 months include enhanced, real-time monitoring via ES Event Sequencing, the ability to implement security automation with threat intelligence, healthcare-specific vertical content to address prescription theft and patient privacy violations. In late October 2019, Splunk released a cloud-based solution called Mission Control, to more tightly integrate the Enterprise Security, Phantom and UBA products. Mission Control was not GA, and thus not evaluated, during the research phase of the Magic Quadrant.

Organizations seeking an SIEM solution that can grow from basic use cases to more-advanced use data and analysis requirements beyond security and across their organizations should also consider Splunk.

Strengths

- **Deployment:** Multiple delivery options for Splunk Enterprise and Enterprise Security include software (which can be deployed on-premises, in IaaS or in a hybrid mode); cloud-hosted; and via appliances (leveraging third parties).

- **Product Strategy:** Splunk's approach to providing centralized data collection and analysis, with premium solutions on top of the core product, appeals to organizations that want one solution that can support multiple teams (e.g., IT operations, security operations, data and analytics). Buyers can start with one use case or team and then expand into others with limited friction.

- **Market Understanding:** Splunk has fostered a dense ecosystem of partners and technology alliances capable of extending Splunk's native value via Apps that are use-case- or vendor-specific. Splunkbase is a strong example of how application marketplaces can be used to deliver content and product integrations in a single UX.

- **Customer Experience:** Splunk customers give high marks for ease of integration, quality and availability for end-user training, and the quality of the peer community, compared with their competition.

- **Marketing Execution:** Splunk's marketing approach and cross-organization selling opportunities have made it highly visible with Gartner clients, ranging from midsize to large, global, multinational enterprises.

Cautions

- **Customer Experience:** Reference customer overall scores for evaluation and contract negotiation, service and support, pricing and contract flexibility, and value for money spent are below most of its competitors. This reflects ongoing concerns raised by Gartner clients about the cost of Splunk. Splunk has introduced several new pricing options, but it's too soon to evaluate whether those changes will improve Splunk's lagging perception on pricing, licensing and cost.

- **Product Strategy:** Splunk's lack of endpoint and network sensors will require buyers to find complementary third-party solutions to fill out the requirements of a modern SOC (e.g., SIEM + UEBA + SOAR + EDR + NTA). Integrations with leading vendors are supported through Splunkbase apps.

- **Product Strategy:** Although Splunk has aligned the pricing model of UBA with that of Splunk Enterprise and Splunk Enterprise Security, Splunk UBA is on a separate technology stack. It is not

- **Operations:** Splunk's content is available across several platforms, must be licensed separately to access that content, and requires multiple mechanisms for organizing and updating the content — e.g., across premium apps and solutions (such as ES, UBA and Phantom).

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may reflect a change in the market and, therefore, different evaluation criteria, or a change in that vendor's focus.

Added

FireEye and HanSight were added to the Magic Quadrant this year, based on meeting the inclusion criteria.

Dropped

BlackStratus, Netsurion-EventTracker and Venustech were dropped from the Magic Quadrant this year, because they did not meet the inclusion criteria for revenue or geographic presence.

Inclusion and Exclusion Criteria

To qualify for inclusion, vendors need:

- A product that provides SIM and SEM capability to end-user customers via software and/or appliance and/or SaaS.
- SIEM features, functionality and add-on solutions that were generally available as of 31 July 2019.
- A product that supports data capture and analysis from heterogeneous, third-party sources (that is, other than from the SIEM vendor's products/SaaS), including market-leading network technologies, endpoints/servers, cloud (IaaS or SaaS), and business applications.
- SIEM (product/SaaS license and maintenance, and excluding managed services) revenue exceeding $32 million for the 12 months prior to 30 June 2019, or have 100 production customers as of the end of that same period. Production customers are defined as those that have licensed the SIEM and are monitoring production environments with the SIEM. Gartner will require that you provide a written confirmation of achievement of this requirement and others that stipulate revenue or customer thresholds. The confirmation must be from an appropriate finance executive in your organization.

production customers in each of at least two of the following geographies: North America, EMEA, the APAC region and Latin America.

- Sales and marketing operations (via print/email campaigns, local language translations for sales/marketing materials) targeting at least two of the following geographies as of 30 June 2019: North America, EMEA, the APAC region and Latin America.

Exclusion criteria includes capabilities that are available only through a managed services relationship. That is, SIEM functionality that is available to customers only when they sign up for a vendor's managed security or managed detection and response or managed SIEM or other managed services offering. By managed services, we mean those in which the customer engages the vendor to establish, monitor, escalate and/or respond to alerts/incidents/cases.

Evaluation Criteria

Ability to Execute

Product or Service evaluates the vendor's ability and track record to provide product functions in areas such as real-time security monitoring, security analytics, incident management and response, reporting, and deployment simplicity.

Overall Viability includes an assessment of the technology provider's financial health, the financial and practical success of the overall company, and the likelihood that the technology provider will continue to invest in SIEM technology.

Sales Execution/Pricing evaluates the technology provider's success in the SIEM market and its capabilities in presales activities. This includes SIEM revenue and the installed base size, growth rates for SIEM revenue and the installed base, presales support, and the overall effectiveness of the sales channel. The level of interest from Gartner clients is also considered.

Market Responsiveness/Record evaluates the match of the SIEM offering to the functional requirements stated by buyers at acquisition time, and the vendor's track record in delivering new functions when they are needed by the market. Also considered is how the vendor differentiates its offerings from those of its major competitors.

Marketing Execution evaluates the SIEM marketing message against our understanding of customer needs, and also evaluates any variations by industry vertical or geographic segments.

Customer Experience is an evaluation of product function and service experience in production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed by conducting surveys of

Operations is an evaluation of the organization's service, support and sales capabilities, and includes an evaluation of these capabilities across multiple geographies.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria	**Weighting**
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (February 2020)

Completeness of Vision

Market Understanding evaluates the ability of the technology provider to understand current and emerging buyer needs, and to translate them into products and services. SIEM vendors that show the highest degree of market understanding are adapting to customer requirements in areas such as early targeted attack and breach detection, as well as simplified implementation and operation, while also meeting compliance reporting requirements.

Marketing Strategy evaluates the vendor's ability to effectively communicate the value and competitive differentiation of its SIEM offering.

Sales Strategy evaluates the vendor's use of direct and indirect sales, marketing, service, and communications affiliates to extend the scope and depth of market reach.

Offering (Product) Strategy is an evaluation of the vendor's approach to product development and delivery that emphasizes functionality and feature sets as they map to current requirements. Development plans during the next 12 to 18 months are also evaluated. The SIEM market is mature devices, security devices, OSs and consolidated administration capabilities. We weight more strongly coverage for emerging event sources, such as IaaS and SaaS, and environmental context.

Despite the vendor focus on expansion of capabilities, we continue to heavily weight simplicity of deployment and ongoing support. Users, especially those with limited IT and security resources, still value this attribute over breadth of coverage beyond basic use cases. SIEM products are complex and tend to become more so as vendors extend capabilities. Vendors able to provide effective products that users can successfully use as a service, or deploy, configure and manage with limited resources will be the most successful in the market.

We evaluate options for co-managed or hybrid deployments of SIEM technology and supporting services, because a growing number of Gartner clients are anticipating or requesting ongoing service support for monitoring or managing their SIEM technology deployments.

Vertical/Industry Strategy evaluates vendor strategies to support SIEM requirements that are specific to industry verticals.

Innovation evaluates the vendor’s development and delivery of SIEM technology that is differentiated from the competition in a way that uniquely meets critical customer requirements. Product capabilities and customer use in areas such as application layer monitoring, identity-oriented monitoring and incident investigation are evaluated, in addition to other capabilities that are product-specific, and needed and deployed by customers. There is a strong weighting of capabilities that are needed for advanced threat detection (ATD) and incident response: user, data and application monitoring; ad hoc queries; visualization; orchestration and incorporation of context to investigate incidents; and workflow/case management features.

For **Geographic Strategy,** although the North American and European markets produce the most SIEM revenue, Latin America and the APAC region are growth markets for SIEM and are driven primarily by threat management and secondarily by compliance requirements. Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for those geographies, as well as product features to support local and regional compliance requirements regarding data residency and privacy.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium

Evaluation Criteria ↓	Weighting ↓
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (February 2020)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a strong functional match with general market requirements, and have been the most successful in building an installed base and revenue stream in the SIEM market. In addition to providing technology that is a good match with current customer requirements, Leaders also show evidence of superior vision and execution for emerging and anticipated requirements. They typically have relatively high market share and/or strong revenue growth, and have demonstrated positive customer feedback for effective SIEM capabilities and related service and support.

Challengers

The Challengers quadrant is composed of vendors that have multiple product and/or service lines, at least a modest-size SIEM customer base, and products that meet a subset of the general market requirements. As the SIEM market continues to mature, the number of Challengers has dwindled. Vendors in this quadrant would typically have strong execution capabilities, as evidenced by financial resources, a significant sales and brand presence garnered from the company as a whole, or from other factors. However, Challengers have not demonstrated a complete set of SIEM capabilities, or they lack the track record for competitive success with their SIEM technologies, compared with vendors in the Leaders quadrant

Visionaries

Leaders. This lower rating is typically due to a smaller presence in the SIEM market than the Leaders, as measured by installed base, revenue size or growth, smaller overall company size or general viability.

Niche Players

The Niche Players quadrant is composed primarily of vendors that provide SIEM technology that is a good match with a specific SIEM use case or a subset of SIEM functional requirements. Niche Players focus on a particular segment of the client base (such as the midmarket, service providers, or a specific geographic region or industry vertical) or may provide a more limited set of SIEM capabilities. In addition, vendors in this quadrant may have a small installed base or be limited, according to Gartner's criteria, by other factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant does not reflect negatively on the vendor's value in more narrowly focused markets or use cases.

Context

SIEM technology provides:

- **SIM —** Log management, analytics and compliance reporting
- **SEM —** Real-time monitoring and incident management for security-related events from networks, security devices, systems and applications

SIEM technology is typically deployed to support three primary use cases:

- **ATD —** Monitoring, alerting in real time, and longer-term analysis and reporting of trends and behaviors regarding user and entity activity, data access, and application activity. Threat detection includes the incorporation of threat intelligence and business context, in combination with effective ad hoc query capabilities.
- **Basic Security Monitoring —** Log management, compliance reporting and basic real-time monitoring of selected security controls.
- **Investigation and Incident Response —** Dashboards and visualization capabilities, as well as workflow and documentation support to enable effective incident identification, investigation and response.

Organizations should define their specific functional and operational requirements, and consider SIEM products from vendors in every quadrant of this Magic Quadrant. Product selection decisions

- Budget constraints
- The scale of the deployment
- The complexity of product (deploying, running, using and supporting)
- The IT organization’s project deployment and technology support capabilities
- Integration with established applications, data monitoring and identity management infrastructure

(See “Toolkit: Security Information and Event Management RFP” for more details.)

Organizations that plan to use external service providers (ESPs) for deployment, configuration or ongoing operations of the SIEM should consider products that have adequate service availability from the SIEM vendor or third-party providers.

Security and risk management leaders considering SIEM deployments should first define the requirements for SEM and reporting. The project will benefit from the input of other groups, including audit/compliance, identity administration, IT operations and application owners. Organizations should also describe their network and system deployment topology, and assess event volume and rates, so that prospective SIEM vendors can propose solutions for company-specific deployment scenarios. The requirements definition effort should also include phased deployments and enhancements — new use cases, which might require new investigation and response capabilities — beyond the initial use cases. This Magic Quadrant evaluates technology providers with respect to the most-common technology selection scenario: an SIEM project that is funded to satisfy a combination of threat monitoring/detection/response and compliance reporting requirements.

Market Overview

Demand for SIEM technology remains strong. The SIEM market grew from $2.319 billion in 2017 to $2.597 billion in 2018 (see “Market Share: All Software Markets, Worldwide, 2018”). Threat management (and specifically threat detection and response) remains the primary driver, and general monitoring and compliance are secondary. In North America, there continue to be many new deployments by organizations with limited security resources that need to improve monitoring and breach detection, often at the insistence of larger customers or business partners. Compliance reporting also continues as a requirement; however, most buyers regard it as “table stakes.”

There continue to be new deployments by larger companies that are conservative adopters of technology. Large, late adopters and smaller organizations place high value on deployment and operational support simplicity. We continue to see organizations of all sizes that are reevaluating SIEM vendors to replace SIEM technology associated with incomplete, marginal or failed

The SIEM market is mature and competitive. During this broad adoption phase, multiple vendors can meet the basic requirements of typical customers. The greatest area of unmet need is effective detection of and response to targeted attacks and breaches. The effective use of threat intelligence, behavior profiling and analytics can improve detection success. SIEM vendors continue to increase their native support for behavior analysis capabilities as well as integrations with third-party technologies, and Gartner customers are increasingly expressing interest in developing use cases based on behavior.

SIEM deployments tend to grow in scope over a three-year period to include more use cases and more event sources. As the number and complexity of use cases increase, there is typically greater demand for resources to run, tune and operate the SIEM, and to respond to incidents.

SIEM Vendor Landscape

The vendor landscape for SIEM is still evolving, with recent entrants bringing technologies that deliver higher levels of sophistication for analytics use cases and, in several cases, cloud-native SaaS offerings. Vendors with more-mature SIEM technologies are moving swiftly to update their architecture and introduce cloud-based models. Almost all vendors continue to enhance investigation capabilities and introduce integrations for response actions via native capabilities or acquired/third-party SOAR solutions. The SIEM market is characterized by a relatively small number of vendors that have large customer bases, and others with smaller, but rapidly increasing customer bases.

Splunk, Micro Focus, IBM, and LogRhythm command a significant share of market revenue, but several vendors with smaller shares command strong interest among Gartner customers, due to their strength supporting analytics-focused use cases, or their SaaS consumption model, or both. Smaller SIEM vendors are typically focused on specific market segments, such as buyers of their other products, buyers seeking SIEM plus monitoring services, or MSSP or MSP partners.

Notable developments in the market include the announcement of a preview version and, in August, general availability of Microsoft Azure Sentinel, and the availability of Backstory from the Alphabet company Chronicle (which was brought in under Google Cloud). Although these SaaS offerings did not meet the deadline date for inclusion in this research, Gartner customers have expressed interest in how they might affect their existing SIEM deployments and their longer-term SIEM plans.

Elastic, Graylog, Sumo Logic, Devo and other vendors that have previously targeted log collection and analysis for IT operations use cases are adding more support for security use cases. In some cases, they’re marketing them as SIEM. Although they didn’t meet the inclusion criteria for the research, Gartner customers have expressed interest in whether they might be able to satisfy security use cases and enable a single log and event collection architecture for security and for IT operations.

Several SIEM vendors are not included in the Magic Quadrant because of a specific vertical market

- Odyssey Consultants, based in Cyprus, and several vendors based in China — including DBAPPSecurity, Venustech, Qi An Xin Group — offer SIEMs based on modern, big data and analytics architectures, but have limited visibility among Gartner customers.

- Netsurion-EventTracker is focused on MSEs, and offers a central log management solution, as well as more full-featured SIEM, with optional services available for deployment, tuning and security monitoring.

- BlackStratus supplies SIEM to MSSP, and offers a cloud-based CyberShark SaaS SIEM focused on midsize buyers.

- Huntsman Security (the operating name of Tier-3 Pty Ltd.) is an SIEM vendor with a presence primarily in the U.K. and Australia, focused on governments and critical infrastructure organizations.

- Lookwise has a market presence primarily in Spain and South America. The distinguishing characteristic of Lookwise is the threat intelligence feeds from S21Sec, which are focused on the banking and critical infrastructure sectors.

- HelpSystems, with its Vityl product suite, provides operational event correlation, business process monitoring and SIEM solutions to customers in Europe and South America.

SIEM Services

Gartner customers increasingly indicate that they are seeking external service support for their SIEM deployment, or are planning to acquire that support in conjunction with an SIEM product (see “How and When to Use Co-managed Security Information and Event Management”). Motivation to seek external services includes lack of internal resources to manage an SIEM deployment, lack of resources to perform real-time alert monitoring or lack of expertise in expanding deployment to include new use cases (e.g., for ATD). We expect demand by SIEM users for such services to continue to grow, driven by more customers adopting 24/7 monitoring requirements and implementing use cases that require deeper SIEM operational and analytics expertise. We also expect increased interest in acquiring use-case content via third-party vendors, such as SOC Prime.

SIEM vendors may support these needs via managed services with their own staff or outsourcing services, or by using partners. SaaS SIEM includes vendor support and maintenance of the platform, often in a public cloud environment. However, customers need to use their own resources (or other service providers) to configure content and monitor and investigate events. MSSPs, which offer real-time monitoring and analysis of events, and collect logs for reporting and investigation, are another option for SIEM users (see “Innovation Insight for SIEM as a Service”). Customer-specific requirements for event collection and storage, alerting, investigation, and reporting may prove

SIEM Alternatives

The complexity and cost of buying and running SIEM products, as well as the emergence of other security analytics technologies, have driven interest in alternative approaches to collecting and analyzing event data to identify and respond to advanced attacks. The combination of Elasticsearch, Logstash and Kibana (aka the ELK Stack or Elastic Stack) is a leading example. There has also been an emergence of alternatives to broad-based SIEM solutions that are focused primarily on the log collection and security analytics elements. Vendors competing in this space include Elastic.io, Cybraics, Empow, Elysium, Jask (acquired by Sumo Logic), MistNet, PatternEx, Qomplx, Rank Software and Seceon.

Organizations with the resources to deploy and manage these, and develop and maintain analytics to address security use cases, may be able to get a solution that addresses enough of their requirements for lower cost, compared with commercial technologies. Gartner continues to track the development of this approach. There is some feedback from clients that the workload involved in engineering these solutions to scale and the development effort needed to support the required event sources and analysis are significant, despite the software being free. This may affect total cost of ownership (TCO) and negate the objective of being less expensive than a commercial SIEM deployment.

Several providers offer MDR services that differ from those of MSSPs, with the goal of identifying and responding to advanced threats in the customer environment. This is typically achieved through the analysis of selected network and endpoint data (see "Market Guide for Managed Detection and Response Services"). The scope of services and event sources is typically smaller than those available from an MSSP, or covered by an SIEM deployment. They do not typically compete directly against the SIEM vendor or MSSP, where customers have broader use-case requirements. However, the MDR services claim effective ATD capabilities, and may compete for SIEM budgets in organizations with sufficient resources to support those use cases. Gartner will continue to monitor the space to assess how MSS, MDR, logging and SIEM interact and intersect.

Evidence

Automated social media listening tools were used to track users' responses on social media and public discussion forums. The time period for the analysis was from 1 November 2016 through 30 September 2019. "Social media mentions" or "conversations volume" denote the inclusion of a monitored keyword in a textual post on a social media platform. High counts of mentions should not be considered an indication of "positive sentiment" or a measure of "adoption" by default.

Social media sources considered for this analysis included Twitter, Facebook (publicly available information only), Instagram, images (comments only), aggregator websites, blogs, news, mainstream media, forums and videos (comments only). All geographical regions of the world were

Social media analytics study results are not “market representative,” but largely “indicative.” They reflect the aggregate crowdsourced opinion about a topic on social media.

Additional research contributions were provided by Ritesh Srivastava, from the Gartner Social Media Analytics team.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.