Magic Quadrant for Security Information and Event Management

Published 3 December 2018 - ID G00348811 - 68 min read

By Analysts Kelly Kavanagh, Toby Bussa, Gorka Sadowski

Security and risk management leaders increasingly seek SIEM solutions with capabilities that support early targeted attack detection and response. Users must balance advanced SIEM capabilities with the resources needed to run and tune the solution.

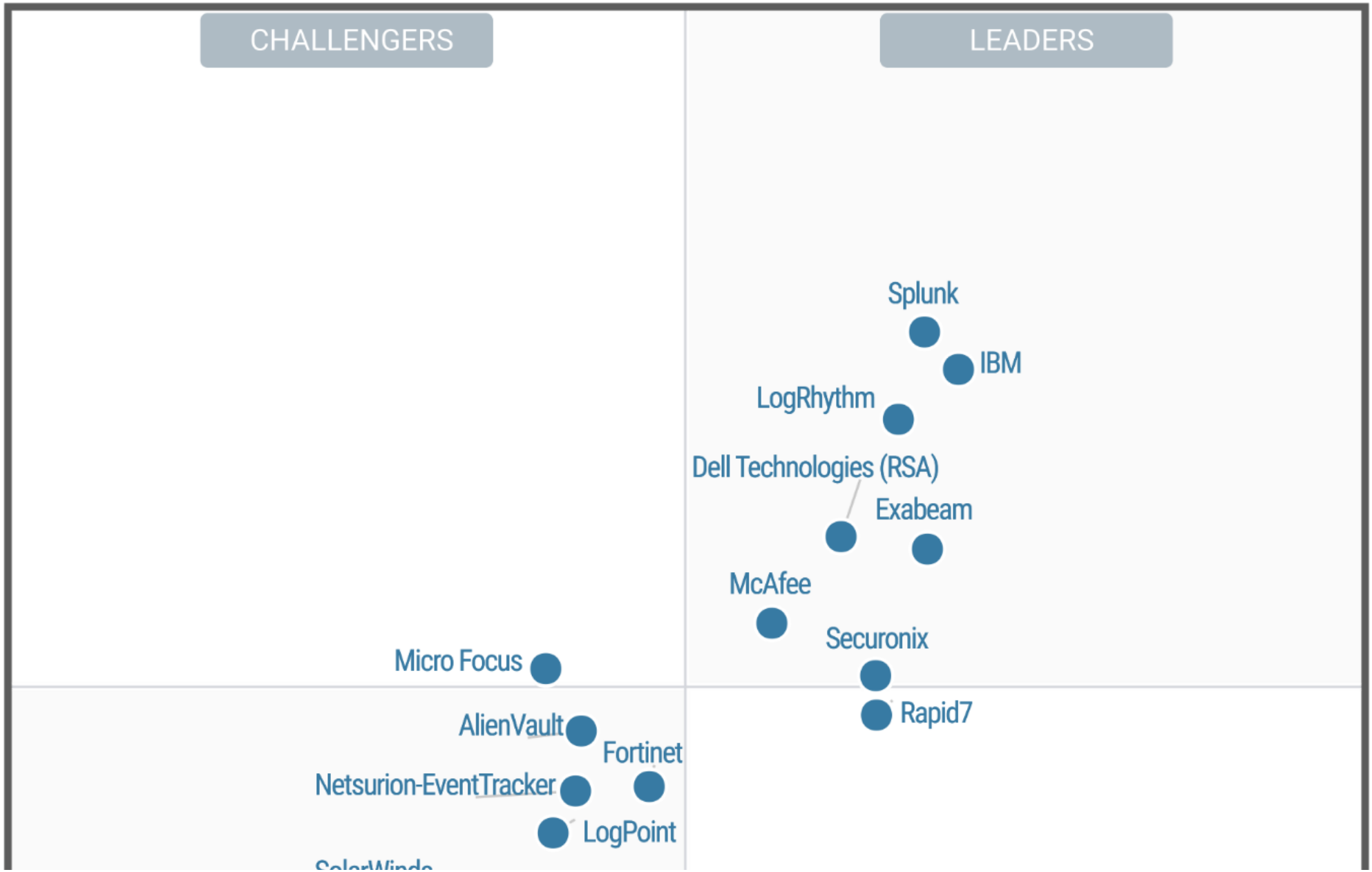
Market Definition/Description

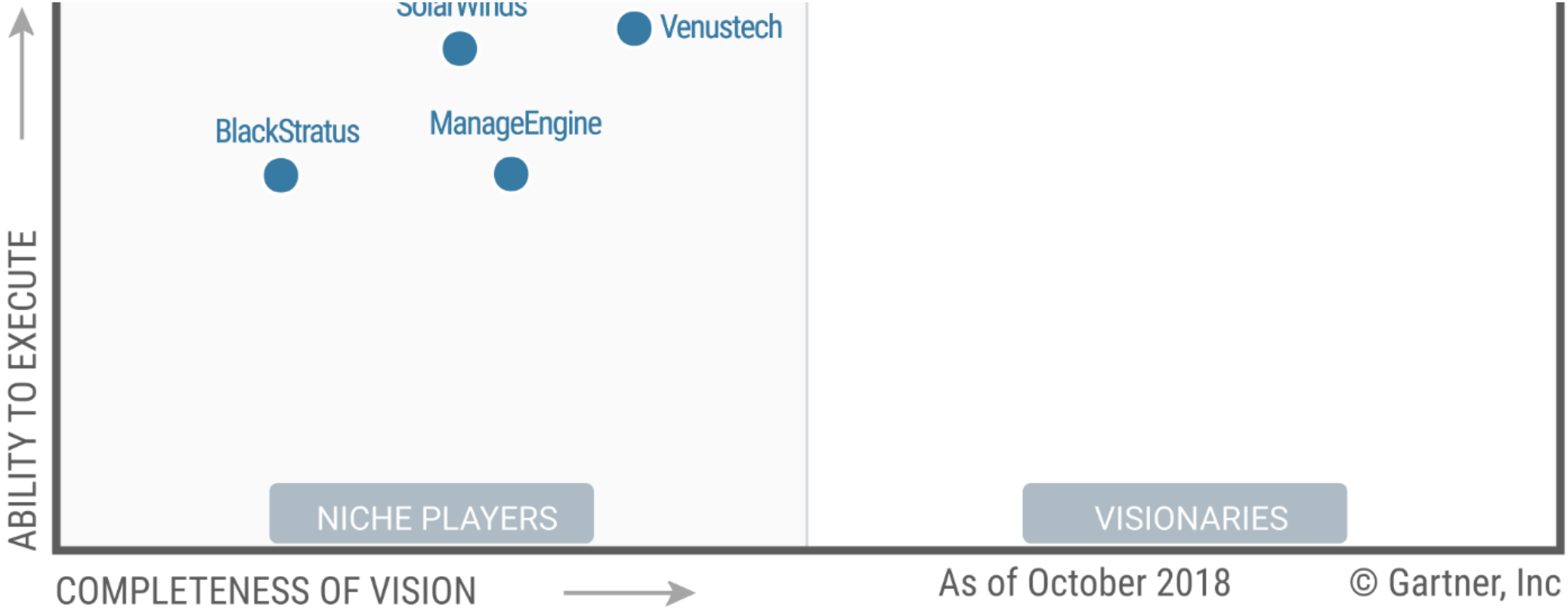
Gartner defines the security and information event management (SIEM) market by the customer's need to analyze event data in real time for early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics and regulatory compliance. The vendors included in our Magic Quadrant analysis have products designed for this purpose, and they actively market and sell these technologies to the security buying center.

SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as network telemetry (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 (December 2018)

Vendor Strengths and Cautions

AlienVault

AlienVault, an AT&T company, was acquired in August 2018, and is part of AT&T's newly created Cybersecurity Solutions division. The AlienVault SIEM product, Unified Security Management (USM) Anywhere, is delivered as SaaS, and includes several components for asset discovery; vulnerability assessment; and intrusion detection system (IDS) for network, host and cloud; as well as for core SIEM capabilities. USM Appliance (an on-premises software deployment) is still supported, but the vendor's emphasis is on the Anywhere SaaS offering. Additional offerings include the Open Threat Exchange (OTX) threat intelligence sharing capability and OTX Endpoint Threat Hunter service, both no-cost services. AlienVault also offers Open Source Security Information Management (OSSIM).

AlienVault targets end-user SIEM buyers, with an emphasis on financial services and healthcare as well as service providers. End-user customers are typically midmarket, not large, enterprises.

Notable capabilities that have been added since the last Magic Quadrant research include monitoring of Google G Suite and Office 365 SaaS, an API to support app integrations, and a central management console (USM Central) for managed security service (MSS) partners.

Midsize organizations seeking an SIEM-as-a-service delivery model with bundled security controls, but with little need for extensive database or application monitoring, or advanced analytics, should consider AlienVault.

Strengths

- USM Anywhere bundles several security controls, sensors and other capabilities like file integrity monitoring (FIM)/endpoint detection and response (EDR) and vulnerability scanning as components of the solution.
- The Anywhere SaaS solution has a straightforward architecture: cloud-based storage and analytics/reporting with on-premises endpoint agents and a network appliance for log aggregation and forwarding, NIDPS, and vulnerability scanning. Scalability requires adding more agents and network sensors as needed.
- Implementation is straightforward: Users request new sensors via the management interface for the specific hosting platform (on-premises virtual machine or a virtual instance in Amazon Web Services [AWS] or Microsoft Azure), and the sensor is made available to be deployed. Configuring the sensor to accept events is supported by a wizard.
- Product currency and scalability are handled on the cloud-based platform. New features and updates are automatically deployed. If a client exceeds its licensed capacity, it is notified so it can arrange to move to a higher-capacity service tier.

Cautions

- AT&T has not provided detailed plans for the future of AlienVault USM. Organizations considering AlienVault should get assurances from AT&T regarding the product roadmap. The vendor provides MSS and managed SIEM services, and is a potential competitor of managed security service providers (MSSPs) that deliver their services through the AlienVault solution. Service providers should get assurances from AT&T about the roadmap and ongoing availability of AlienVault products. Although USM Appliance is still supported, AlienVault's focus is now

primarily on Anywhere. Buyers wanting an on-premises version should carefully evaluate and understand the differences in feature parity and capabilities between the two products.

- Support for native user analytics is limited to the capabilities provided by the underlying graph database, along with monitoring for attacks against identity and directory services. Integrations with third-party user and entity behavior analytics (UEBA) solutions are not supported.
- Anywhere lags competitors in several areas, such as application and database monitoring, and integrations with third-party solutions such as cloud access security brokers (CASB), DAM, DAP and DLP.
- Data backup and archive are handled automatically by the Anywhere platform. Archive is, by default, one year, with options to purchase additional years. Organizations with data retention policies should evaluate whether the retention scheme meets their policy requirements.

BlackStratus

BlackStratus focuses on SIEM technology delivered on-premises and as a service, focused on MSSPs, managed service providers (MSPs), large enterprises and, increasingly, midsize enterprises (MSEs). The portfolio is composed of LOGStorm, SIEMStorm and CYBERShark. LOGStorm is a log and event management and reporting tool targeted at MSEs and MSSPs that require basic log collection, management and reporting. SIEMStorm is a natively multitenant platform that is delivered as software only and includes core SIEM capabilities like real-time event management, analytics, incident management and reporting. It is targeted at MSSPs that require multitenancy and large enterprises with federated monitoring requirements such as a hierarchical or parent/child model. CYBERShark is a cloud-based SIEM-as-a-service solution aimed primarily at MSPs and MSEs that can include 24/7 monitoring, analysis and alerting services delivered from the BlackStratus security operations center (SOC). A variety of pricing models are employed depending on the solution. For example, LOGStorm is a term model priced on storage required, SIEMStorm is priced on the volume of log events and CYBERShark is aligned to the number of employees in the organization

Version 4.3 of SIEMStorm was released in December 2017 and is mainly focused on platform and management enhancements, such as a new HTML5 user interface, the addition of contact tree management, and enhancements to the case management and multitenant features.

Midsize organizations seeking a cloud-based SIEM as a service solution with optional managed services, and MSSPs seeking multitenant SIEM to deliver monitoring services, should consider BlackStratus

Strengths

- LOGStorm and SIEMStorm offer native multitenancy support.
- SIEMStorm's underlying architecture for data management no longer uses an RDBMS. The use of Vertica provides a modern big data capability for data storage and management, and faster search capabilities.
- Buyers looking for an SIEM solution delivered as a service can purchase CYBERShark, along with the flexibility of adding 24/7 security monitoring and alerting as required.

Cautions

- BlackStratus has focused on a niche set of buyers, primarily large MSSPs and MSPs, so it lacks visibility with Gartner's enterprise and MSE end-user clients.
- BlackStratus has positioned itself as providing core SIEM capabilities, particularly where native multitenancy support is provided. SIEMStorm lacks other capabilities increasingly being asked for by SIEM buyers and being added by competing solutions, such as support for packaged analytics content, advanced analytics and user monitoring, as well as workflow, orchestration and automation.
- SIEMStorm lacks complementary technologies that could support host and network data collection and telemetry, such as native FIM, EDR or network monitoring via flow or deep packet inspection (DPI).

Dell Technologies (RSA)

The RSA NetWitness Platform (RSA NWP) consists of RSA NetWitness Logs, RSA NetWitness Network, RSA NetWitness Endpoint, RSA NetWitness UEBA and RSA NetWitness Orchestrator. These elements are composed of several components for data acquisition, forwarding, storage and analysis. RSA gained in-house UEBA capability with the acquisition of Fortscale in 2018, and security orchestration, automation and response (SOAR) capabilities are delivered via a white-label version of Demisto. These elements can be deployed as software, appliance or virtual appliance, in any combination. Pricing for RSA NetWitness Logs and RSA NetWitness Network is based on data volume per day. Pricing for RSA NetWitness UEBA is based on users monitored, and pricing for RSA NetWitness Orchestrator is based on number of analysts. RSA NetWitness Logs and RSA NetWitness Network can be licensed by appliance capacity (for physical appliances) or metered (data volume) license on a perpetual or term basis. Metered licensing provides entitlements to all required components. Customers can mix appliance and metered licensing to enable granular capacity growth across the deployment architecture.

The version 11 release of RSA NetWitness Logs and RSA NetWitness Network introduced or enhanced several capabilities, the most important being better investigation capabilities and workflow, stronger analytics capability via the Fortscale acquisition, and orchestration and response via Demisto.

Enterprises with a mature security operations capability seeking scalable SIEM with flexible deployment options, UEBA and SOAR capabilities should consider RSA.

Strengths

- The vendor can support enterprise buyers focused on advanced threat detection and looking for a single vendor that integrates capabilities including core SIEM, network monitoring and analysis, EDR, and UEBA.
- The combination of RSA NetWitness Network and NetWitness Endpoint provides strong coverage of the five styles of advanced threat defense: real-time network and endpoint monitoring, and forensic network and endpoint investigation.
- RSA NWP provides strong OT monitoring capability due to its ability to deploy RSA NetWitness Network to capture data in ICS/SCADA environments, and then process it using native support for common protocols.
- NWP customers indicate they find value in the platform's ability to correlate and analyze logs and network data (and other event sources) into a unified view. Customers provided positive, but limited, feedback on version 11.

Cautions

- RSA NWP integration with CASB includes SkyFormation, and support for Netskope, Forcepoint and McAffe-SkyHigh Networks was recently made available. Organizations using other CASB products should validate roadmap support for RSA NWP integrations with those products.
- The number of technical components of the RSA NWP solution and the licensing models provide extensive flexibility in designing the deployment architecture, but require understanding of the breadth of the options and the implications for cost, functionality and scalability.
- The RSA NetWitness Endpoint technology is partially integrated into NWP, with a separate management console and user interface. RSA NetWitness Orchestrator has a separate UI and relies on UI redirects with the core RSA NWP.

- RSAs' focus on larger customers and those with more mature security monitoring capabilities results in a poor match to the needs and resources of less mature buyers.
- RSA has modest visibility among Gartner customers inquiring about SIEM.

Exabeam

Exabeam's Security Management Platform (SMP) is composed of six products: Exabeam Data Lake, Exabeam Cloud Connectors, Exabeam Advanced Analytics, Exabeam Entity Analytics, Exabeam Threat Hunter and Exabeam Incident Responder. Each of these products has a release/update schedule, and some are more mature than others. They are available in several form factors: hardened physical appliances, virtual appliances, and private or public cloud deployments (Amazon, Google and Azure). A deployment can consist of multiple form factor (physical/virtual/cloud) options. The licensing and pricing model is straightforward: one- or three-year subscription, with Data Lake, Cloud Connectors, Advanced Analytics, Threat Hunter and Incident Responder priced by number of employees monitored, and Entity Analytics priced by the number of entities monitored. Exabeam targets larger organizations in the financial services, healthcare and energy verticals, among others. The modular packaging of the technology enables Exabeam to position elements such as Incident Responder or Advanced Analytics as companion technologies to a competitor's SIEM, and to add Data Lake and other elements as SIEM replacement. Midsize and smaller organizations typically engage with external service providers to monitor or run Exabeam SMP. The vendor received a $50 million infusion of funding in August 2018, which will be used to develop a multitenant SaaS offering.

Version 2 of SMP was released in March 2018. It included the introduction of Entity Analytics and flow collection, improvements to Incident Responder, support for more SaaS platforms, and stronger correlation rule management features and compliance reports. It also included content updates related to existing and new use cases, and a UW (ML) SDK/API.

Enterprises with behavior-focused use cases, and those that want integrated orchestration and response capabilities with SIEM, should consider Exabeam SMP.

Strengths

- The scalable architecture is based on Elasticsearch and Hadoop (HDFS), with Kafka message bus and Spark for ML processing.
- There is an easy-to-understand pricing model based on users and entities.

- Orchestration and response capabilities include automated playbooks available with Incident Responder.
- SMP provides granular (predefined and customizable) role-based data access and workflow to support privacy concerns.
- Advanced Analytics, along with solid out-of-the-box content and models, provides mature user behavior analytics (UBA) capabilities. This was the core of the UEBA product that Exabeam developed prior to entering the SIEM market.
- Customers offer good-to-high marks for Exabeam overall, with high marks for evaluation/contracting activities, and deployment and support services.

Cautions

- Organizations with low-maturity investigation and response capabilities will be less likely to get the full benefit from advanced features for those activities, and will need to use a service provider.
- Some users indicated that the incident response functionality lagged behind other custom-made incident response products.
- Some users report a slow response from their technical account manager and other support issues that they generally ascribe to growing pains.
- Exabeam has yet to provide its analytics solution in the cloud as a SaaS model, limiting applicability for some organizations.

Fortinet

Fortinet's FortiSIEM solution, currently at version 5, provides core SIEM capabilities in addition to complementary features that include a built-in configuration management database (CMDB), FIM, and application and system performance monitoring. FortiSIEM's solution is deployed via virtual appliances that can be installed on-premises in virtual environments or via IaaS platforms like AWS and Azure. The solution can be deployed as a single appliance or as individual, stand-alone components for scalability. Physical appliance options are also available. Licensing is primarily based on the number of data sources, events per second (EPS) and agents deployed.

Fortinet positions FortiSIEM for MSPs, telecommunications providers and MSSPs that use or support other Fortinet solutions, as the solution is part of Fortinet's Security Fabric framework, as well as for security operations buyers in large enterprises, government and education. FortiSIEM

has been adopted by organizations where security and network operations monitoring are delivered from a unified solution (e.g., in a combined NOC and SOC), as well as by MSPs and MSSPs that leverage multiple Fortinet solutions.

Version 5 delivered significant updates to FortiSIEM, including a productwide HTML5-based GUI, adoption of Elasticsearch for the event database, incident response enhancements that include automated response actions and workflows, and user risk scoring, among other enhancements. Fortinet now offers a physical appliance option in addition to its virtual appliances.

End-user organizations and MSPs with investments in Fortinet network technologies should consider FortiSIEM.

Strengths

- FortiSIEM offers functionality that appeals beyond just security operations (e.g., discovering assets, a built-in CMDB and asset context that appeals to teams beyond security operations).
- Enterprises where security operations and network operations are combined can leverage a common platform with native incident management features.
- The integration of FortiSIEM with the rest of the Fortinet portfolio through Fortinet Security Fabric may appeal to organizations leveraging a range of Fortinet products.
- FortiSIEM offers out-of-the-box features meant to help with faster installations and implementations (e.g., the native CMDB that can be populated through its asset discovery feature), as well as multiple delivery options via virtual and physical appliances.
- Overall customer satisfaction with FortiSIEM is positive based on feedback by reference customers as well as data collected via Gartner's Peer Insights.

Cautions

- Buyers focused on threat detection use cases should evaluate the out-of-the-box threat detection capabilities of FortiSIEM (e.g., package content and analytics), which lag behind compared to the support for compliance and reporting use cases.

- Analytics are still a work in progress and lag behind many competitors in the use of advanced analytics, such as using ML. Fortinet has indicated additional support for user behavior analytics, and the incorporation of ML is on its roadmap.
- Integration with commercial threat intelligence feeds is limited to Fortinet's own FortiGuard Indicators of Compromise (IOC) feed and Anomali. However, a number of open-source feeds are natively supported and any TAXII feed should be usable (just not natively supported).
- FortiSIEM has limited visibility with end-user SIEM technology buyers. Fortinet's focus tends to favor service providers that leverage other Fortinet products and require an SIEM solution that supports integrated IT and network operations capabilities, and offers native multitenancy features.

IBM

The IBM QRadar Security Intelligence Platform builds around IBM QRadar SIEM and includes several components. IBM QRadar Vulnerability Manager contextualizes event data with VM data. IBM QRadar Network Insights provides QFlow-based application visibility from network flows. IBM QRadar User Behavior Analytics is a free UBA module that addresses some insider threat use cases. IBM QRadar Incident Forensics provides forensic investigation support. IBM QRadar Advisor with Watson provides automated root cause research for identified threats. The vendor also offers the IBM Security App Exchange, where IBM QRadar customers can download 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 can help organizations streamline their incident management process.

IBM QRadar SIEM is available as hardware virtual appliances and software packages based on the customer's event velocity (number of EPS across the data sources in scope). It is also consumable from the cloud as SaaS SIEM hosted by IBM. Pricing for other components in the IBM QRadar Security Intelligence Platform depends on their respective metrics (e.g., number of flows for IBM QRadar Network Insights or number of assets in scope for IBM QRadar Vulnerability Manager). QRadar Network Insights is available only in hardware appliance format.

In 2018, IBM has iterated QRadar on its version 7.3.1 with several incremental updates and platform enhancements (e.g., data-at-rest encryption software installs, stronger multitenancy with tenant-aware properties), and more out-of-the-box content and use cases (e.g., GDPR, extensions to further support the NIST framework and cloud providers such as IBM Cloud, Azure, Office 365 and AWS, and additional UBA models and use cases).

IBM QRadar targets large organizations, by offering a robust platform to build a threat detection and response function, and smaller organizations, by offering extensive content out-of-the-box for simpler use cases. It enjoys a wide deployment base, and a wide availability of service providers that can help organizations procure, run, tune and monitor their IBM QRadar instance.

Strengths

- QRadar offers a flexible and powerful SIEM platform with extensive out-of-the-box content for a broad selection of use cases.
- There is a solid ecosystem of value-added integrations with other IBM security portfolio solutions (such as IBM QRadar Advisor with Watson, IBM Resilient or the free UBA module) and content developed by third parties (community, and security and IT vendors), easily accessible via IBM QRadar's marketplace.
- There is strong support for network data monitoring, with a large number of application flow signatures to parse flow data.
- QRadar has widespread visibility among Gartner clients seeking SIEM products.

Cautions

- User experience can lag behind some of the newer competitors, with a nonunified look and feel among the tabs and modules in IBM QRadar.
- Risk scoring in QRadar is represented as magnitude within offenses, and it can require a level of maturity in security processes to operationalize this. Risk scoring in UBA is provided out of the box, with no customization required.
- Gartner Peer Insights data indicates that IBM receives lower scores than other SIEM leaders for integration and deployment, and service and support. Reference customers for SIEM give IBM below-average scores for service and support. IBM has indicated that it has recently increased staffing levels for service and support.

LogPoint

The LogPoint SIEM and LogPoint Director software products are available in OVA format for virtual or physical appliance deployment, or a hybrid of both forms. The architecture is straightforward, consisting of collectors to acquire log and event data, NoSQL log and data storage, and search heads to provide alert and search functions. Customers deploy as many collectors, storage nodes and search heads as are required to

address data volumes. For large, federated deployments, LogPoint Director coordinates searches and analytics across data stores. The LogPoint licensing model is based on the number of nodes/users sending data. Enterprise license agreements are available.

Recent enhancements include improvements to the security analytics capabilities, LogPoint data privacy mode, which encrypts sensitive data as a GDPR compliance feature, and a cloud-based UEBA module with analytics and threat scoring on users and entity data.

Among other verticals, LogPoint targets healthcare providers and municipal governments subject to compliance requirements, and organizations that have deployed SAP for ERP. Customers tend to be midsize businesses.

Midsize organizations with monitoring requirements in Europe, or those seeking to include SAP in the scope of their security and compliance monitoring, should consider LogPoint.

Strengths

- A 90-day trial version with all features enabled, supporting up to 450 EPS from 10 nodes, is available to allow buyers to download and test the solution, even before deciding if they want to commit to a proof of concept (POC).
- LogPoint's node-based pricing for SIEM is straightforward and, unlike the models used by several competitors, encompasses all needed collectors, search and storage components. UEBA capabilities are available as an add-on, priced by users/nodes.
- Strong data protection and access control features are offered, and the architecture allows for data residency and local versus centralized use and management.
- There are UEBA capabilities that leverage prebuilt content, including rules and ML. Elements of the UEBA analytics are performed in the cloud, thus do not require additional resources on-premises.
- LogPoint has developed extensive SAP integrations for compliance, fraud detection and security use cases in ERP.

Cautions

- LogPoint is new to the North American market, with low visibility among Gartner clients and limited channels established. Marketing effort will be required to compete within the saturated North American market, especially considering vendors in tangential markets competing for

SIEM technology budget share.

- LogPoint has directed limited attention to the Asia/Pacific region, and none to Japan and Latin America. Prospective customers in these regions may not have access to channel partner options or resources.
- There is a heavy reliance on channel and partners for sales and initial deployment, and implementation of professional services support. There are several partners in Europe, but fewer in North America.
- Compared to the publicly visible marketplace or app store approach of other vendors, LogPoint provides third-party integrations via a service desk not visible to external parties. LogPoint claims more than 400 integrations are available.

LogRhythm

Thoma Bravo completed its acquisition of a majority interest in LogRhythm in July 2018. LogRhythm's SIEM solution, branded as LogRhythm NextGen SIEM Platform, is available in configurations for both large (LogRhythm Enterprise) and midsize (LogRhythm XM) enterprises. Add-on components to either are System Monitor (SysMon Lite and Pro), Network Monitor (NetMon and NetMon Freemium), and CloudAI. LogRhythm's SIEM can be deployed as software, a physical appliance or a virtual appliance. The XM solution is an all-in-one appliance and the various discrete components that make up the LogRhythm platform can be deployed as stand-alone as required. LogRhythm can be deployed on-premises, in IaaS and in hybrid models. Multitenancy is also natively supported. LogRhythm Enterprise and XM are licensed based on message per second (MPS) per day, and licenses are available as perpetual or term, along with enterprisewide agreements. System Monitor is priced per agent and Network Monitor is priced per gigabits per second throughput. UEBA is priced according to the number of identities monitored.

In December 2017, LogRhythm introduced a cloud-based add-on component to the existing UEBA capabilities of the platform, and also introduced its UEBA capabilities as a stand-alone UEBA product. Additionally, other enhancements include better identity detection and tracking across multiple sources, branded as TrueIdentity, as well as enhancements to its alarm and incident management features and a new generation of physical appliances.

Organizations seeking SIEM with native network monitoring, endpoint agent, and cloud-based analytics should consider LogRhythm.

Strengths

- LogRhythm offers a single vendor approach for buyers that want an SIEM solution that offers complementary and self-contained options for network and host-level monitoring, as well as UEBA capabilities.
- LogRhythm SIEM is focused on ease of deployment and use through its emphasis on UX and UI elements of the application, as well as through use of prepackaged content in frequent content updates and SmartResponse actions to aid in the incident management process. Ease of administration and use-case enablement are facilitated through Co-Pilot services for administration, analytics implementation and custom content creation.
- LogRhythm has seen an increase in interest from Gartner customers over the past 12 months, particularly as MSE and smaller enterprise clients are purchasing LogRhythm SIEM along with managed SIEM services. LogRhythm is leveraging and expanding its focus on the reseller channel, particularly in North America, which seems to be driving its increased visibility. LogRhythm is frequently shortlisted by Gartner customers.

Cautions

- LogRhythm does not have an app store for exposing its technology partnerships and integrations both for users and marketing purposes, compared to competing SIEM vendors with online app stores.
- LogRhythm includes some case management and response capabilities as part of its solution, but buyers looking for a stand-alone SOAR product will need to leverage third-party solutions. Integrations are available with Phantom (acquired by Splunk), Demisto, CyberSponse and ServiceNow. Buyers should confirm availability for their preferred SOAR solution.
- LogRhythm's marketing lacks clarity as its platform is simultaneously being referred to as its "NextGen SIEM Platform" as well as LogRhythm Threat Lifecycle Management (TLM) Platform, with both messages being used on the vendor's website and in marketing materials.
- Customers indicate lower satisfaction with the pricing and contract flexibility of LogRhythm relative to some competitors.

ManageEngine

ManageEngine's SIEM portfolio consists of its core ManageEngine Log360 SIEM offering and several modules that can integrate with it to extend its value proposition — particularly for Microsoft and cloud environments — and are capable of addressing security as well as IT operations use cases. These include ManageEngine EventLog Analyzer (central log management), ManageEngine ADAudit Plus (Active Directory

change auditing and reporting), ManageEngine Cloud Security Plus (CLM and SIEM for AWS and Azure), ManageEngine O365 Manager Plus (Office 365 security and compliance) and ManageEngine Exchange Reporter Plus (Exchange Server change audits and reporting).

ManageEngine Log360 is available for on-premises deployments as software for physical or virtual systems, with perpetual or term licensing, and pricing is based on the number of assets in scope. Individual components are licensed based on the volume of assets (which vary depending on the specific component). A notable outlier is ManageEngine Log360 Cloud, which is only offered as a web-based cloud-hosted service, available as a subscription with pricing based on the number of cloud accounts in scope, with upsell pricing for additional AWS S3 buckets.

Since August 2017, ManageEngine Log360 is at version 5.0, with the latest update in April 2018 offering deeper integration with ManageEngine Exchange Reporter Plus. Other notable enhancements this year include the update to ADAudit Plus 5.1 to support Azure Audit data, or EventLog Analyzer version 11.12 with column integrity monitoring to support GDPR.

Midsize organizations with Windows-centric and AWS/Azure environments that want to address IT operations and basic threat detection uses cases should consider ManageEngine.

Strengths

- The vendor’s focus is on cloud environments, with native and seamless integration with several IaaS/PaaS offerings (e.g., AWS and Azure), as well as some SaaS cloud applications (e.g., Salesforce).
- There is a focus on Microsoft environments with native and seamless integration with Windows infrastructures. Autodiscovery features for Windows systems and Microsoft SQL/IIS devices allow for faster deployment in Windows-centric environments.
- The ability to capture information is strong as a variety of capture methods are supported and automatic parsing of fields from new data sources is supported. The native ability to monitor hypervisor activities specifically is well-supported.
- Comprehensive out-of-the-box content is offered, with 700 parsers, 200 correlation rules, 2,000 dashboards and prebuilt reports for compliance requirements (e.g., GDPR, PCI-DSS, HIPAA, FISMA, ISO27001).

Cautions

- ManageEngine has very low visibility in the SIEM market with Gartner clients, and particular attention should be paid to reference checking for environments and use cases similar to those of your organization.
- Not all modules integrate seamlessly with ManageEngine Log360. For example, although ManageEngine Cloud Security Plus and ManageEngine O365 Manager Plus can be accessed via a unified interface, they are deployed separately and used as separate products.
- The lack of native advanced analytics and inability to bolt on a UEBA module on ManageEngine Log360 limits its applicability for use cases on insider threats and advanced threat detection.
- The lack of CASB integration is notable for a solution focused on cloud.
- There is limited availability of third-party support for deployment (run), ongoing operations, and evolution of the solution (tune) or 24/7 monitoring of the ManageEngine Log360 SIEM solution (monitor).

McAfee

McAfee's SIEM capabilities are delivered via an all-in-one device or discrete components. McAfee Enterprise Security Manager (ESM) is the core element of the platform. McAfee Event Receiver (ERC) is for collection and correlation of data. McAfee Enterprise Log Search (ELS) is for Elastic-based log search. McAfee Enterprise Log Manager (ELM) is for long-term log management and storage. McAfee Advanced Correlation Engine (ACE) is for dedicated correlation, including risk and behavior-based correlation, and statistical and baseline anomaly detection. Additional SIEM options include McAfee Application Data Monitor (ADM) for application monitoring, McAfee Direct Attached Storage (DAS) for additional capacity, and McAfee Global Threat Intelligence (GTI) for IP reputation. These can be augmented with other products from the McAfee Security Operations portfolio, including McAfee Behavioral Analytics (MBA), McAfee Investigator (MI), McAfee Active Response, McAfee Advanced Threat Defense (ATD) and McAfee Database Activity Monitoring (DAM). McAfee targets the public-sector and critical infrastructure sectors, healthcare, and higher education. The McAfee SIEM components are sold with perpetual licenses (MI is subscription-based) and the pricing models vary by type of component, and whether they are delivered as physical (EPS) or virtual (core count) appliances.

With the release of version 11, McAfee introduced a modern SIEM architecture. It also recently introduced MBA as a stand-alone UEBA/security analytics offering that integrates with McAfee ESM and third-party SIEMs.

Enterprises with mature security monitoring and operations capabilities, and those with OT/IoT use cases, should consider McAfee.

Strengths

- McAfee has implemented a modern SIEM architecture that leverages big data technologies, such as Kafka and Elasticsearch. The open nature of the data tier allows organizations looking to feed data into or out of ESM to have flexible options.
- User behavior capabilities are available through several options. In addition to basic user monitoring via a content pack for ESM, McAfee offers MBA as a UEBA/analytics offering, plus support for numerous third-party UEBA integrations.
- Application support is strong across databases, ERP solutions, OT and IoT, either leveraging native capabilities or enhanced through the use of its ADM and DAM solutions.
- MI (an add-on subscription product in the Security Operations product portfolio) provides guided incident investigation support for analysts, including context/evidence collection and recommended actions.

Cautions

- McAfee's visibility with end users has decreased year over year as it increasingly competes against other SIEM vendors. In the MSE and smaller enterprise space, McAfee's visibility in deals where SIEM solutions are considered for co-management by third-party service providers has decreased.
- The vendor does not have a native UEBA product and relies on a white-label partnership. The UEBA is recent, and does not arise in conversations or quotes from Gartner clients considering McAfee ESM.
- McAfee's underlying architecture and focus on its ESM, MI and Active Response products is more appropriate for large enterprises with mature security monitoring and response operations than for those without. Midsize and smaller enterprises interested in McAfee should carefully evaluate how the solution will fit their requirements.
- McAfee users providing feedback for product capability and support put the vendor in the middle of those evaluated, indicating room for improvement in features and support.
- McAfee's pricing model requires multiple data points to determine total cost, and is also affected by the choice of delivery method. Physical appliances are sized by EPS, and virtual appliances are licensed by the number of CPU cores employed. Related McAfee solutions have

different pricing models, such as the number of endpoints for MI and Active Response, and user identities for MBA. Some of the solutions are also sold as capital expenditures, while others, like MI, are subscriptions (operating expenditures).

Micro Focus

Micro Focus offers two SIEM technologies, Micro Focus ArcSight and Micro Focus Sentinel, as a result of the spin-merge in 2017 of Hewlett Packard Enterprise and Micro Focus. Sentinel SIEM is featured in the NetIQ brand, and Micro Focus appears to position ArcSight as its premier SIEM platform. Gartner clients have not shown interest in Sentinel, so our analysis is confined to the ArcSight platform. Micro Focus ArcSight is composed of Enterprise Security Manager (ESM), providing core SIEM functions of real-time analytics, incident management and reporting, and ArcSight Data Platform (ADP), providing event and data collection and management capabilities. ArcSight Investigate provides a dedicated solution for data searching and visualizations to support incident investigation and threat hunting use cases. ArcSight User Behavior Analytics provides advanced analytics to detect anomalous user and entity behaviors. ArcSight ESM Express is available as an all-in-one solution for smaller deployments. Other add-ons include Compliance Insight Package, Application View, Reputation Security Monitor Plus, Interactive Discovery and Micro Focus Application Defender. ArcSight Management Center (ArcMC) is the stand-alone utility used to manage ArcSight components. The ArcSight Marketplace is used to deliver content packages as well as integrations with third-party solutions. The solution can be deployed as a physical appliance or as software, with bare-metal, virtual and IaaS options supported. Multitenant functionality is native to the platform. Pricing for the solution varies according to components used; for example, ADP and Investigate prices are based on the amount of data indexed per day, ESM by the EPS ingested and UBA by the number of accounts monitored. Micro Focus now also offers an enterprise unlimited use license option.

In the past 12 months, Micro Focus has focused enhancements on the ArcSight platform with its 7.0 release that added new features to scale the correlation capabilities in ESM. ArcSight Investigate, currently at version 2.2, has added integrations with several third-party SOAR tools, support for DNS analysis and product fixes.

Enterprises with mature security monitoring operations should consider ArcSight.

Strengths

- Micro Focus is redefining its architecture to take advantage of new technologies (for example, using big data Kubernetes-driven Event Broker within ArcSight ADP).

- The ArcSight platform supports very large enterprises and service providers with environments that require scalable and distributed architectures that can ingest high velocities of events and provide flexibility in managing the data once ingested (e.g., routing to other ArcSight components or third-party solutions).
- ArcSight ESM is leveraged by many very large enterprises, government organizations and MSSPs. This is due to its correlation engine, which was upgraded in version 7 to support federated event ingestions that can handle 100k EPS per ESM cluster via horizontal scaling or 100k EPS per node in vertical scaling models.

Cautions

- The Micro Focus ArcSight platform relies on multiple databases, depending on the components and applications used (e.g., ESM uses CORR-Engine, Investigate uses Vertica and UBA leverages Microsoft SQL). The roadmap for a simplified storage tier based on Vertica has not been released.
- Buyers looking for an integrated UBA solution should confirm the status of Micro Focus' offering as the version is licensed from Securonix and, while recently updated, is an older version.
- Although Micro Focus ArcSight occasionally appears on shortlists for new SIEM deployments, inquiries about replacing ArcSight are common. Client interest in Micro Focus ArcSight Express specifically is minimal and is rarely mentioned or included on shortlists of MSEs and smaller enterprise clients.
- Customer feedback on the overall experience with Micro Focus is below average and lags behind most competitors in the market.

Netsurion-EventTracker

EventTracker offers two solutions in its portfolio. EventTracker Log Manager is a central log management solution. EventTracker Security Center is an SIEM offering. The vendor also offers several components used to extend EventTracker Security Center's value proposition, such as EventTracker Sensor to collect Windows endpoint events or EventTracker Change Audit Sensor to monitor changes to a system. These are available for deployment on-premises as software with an annual subscription license based on the number of assets in scope (number of IP addresses). The solutions are also available as a service through EventTracker's SIEMphonic, covering the three phases of co-managed SIEM service. Those are: (1) "run," for the initial deployment and ongoing management of the solution; (2) "tune," for the co-managed SIEM service for

fine-tuning the EventTracker solution; and (3) “monitor,” for the 24/7 security monitoring of the EventTracker Security Center instance for potential threats.

Version 9, released in December 2017, saw a major overhaul as the back end is now based on Elasticsearch version 5.5, offering scalable performance, and the user interface was updated.

MSEss looking for compliance requirements and basic threat detection in a simple package, and considering outsourcing their SIEM to the vendor for co-management, should consider EventTracker.

Strengths

- The product is a straightforward solution appropriate for core use cases such as compliance and forensics. For small and midsize buyers, compliance packages are available for PCI-DSS, NIST 800-171 and HIPAA, and more are available for enterprise buyers and a few more advanced use cases, such as basic threat detection.
- EventTracker Security Center provides a solid framework for inclusion of threat intelligence feeds via STIX and TAXII.
- The EventTracker SIEMphonic service is available for organizations looking for co-managed SIEM provided by the software vendor.
- SIEMphonic’s co-managed service offers transparency and collaboration opportunities by enabling customers to access the SOC incident and case management platform.

Cautions

- The user interface is clean, but some graphics look dated and investigation support, although intuitive, seems dependent on manual, user-driven activities, compared to competing products.
- EventTracker Security Center’s native case and incident management capabilities are minimal compared to other SIEM products.
- There is limited extensibility of EventTracker Security Center for more advanced use cases requiring advanced analytics.
- Netsurion, which acquired EventTracker in October 2016, has very low visibility among Gartner clients for SIEM.

Rapid7

Rapid7's Insight platform is composed of InsightIDR (its core SIEM offering), InsightVM (vulnerability management), InsightAppSec (application security), InsightConnect (SOAR) and InsightOps (log management for IT operations use cases). 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 seamless integration with InsightVM, providing interesting incident prioritization opportunities. Rapid7 InsightIDR is offered as a service, leveraging Insight Collectors deployed in the client's organization to centralize and forward all required logs to InsightIDR. Because Rapid7 InsightIDR is developed as a cloud-native application, the vendor can bring solution updates to market seamlessly and transparently. Rapid7 InsightIDR customers can outsource 24/7 threat monitoring and investigation and response to Rapid7 through its Managed Detection and Response (MDR) services. Rapid7 InsightIDR's pricing is based on the number of assets monitored for activity (typically servers, desktops and laptops), with tiered pricing for higher volumes.

Rapid7 InsightIDR, a cloud-native solution, has short and iterative release cycles, offering continuous improvements. In September 2018, Rapid7 announced InsightConnect — essentially Rapid7's SOAR module — which supports security use cases, as well as IT operations use cases (for example, by also integrating with InsightVM for automated support for vulnerability scanning and patching).

SMBs and midsize organizations looking for SIEM as a service with the option to outsource 24/7 monitoring and response to the vendor should consider Rapid7.

Strengths

- Rapid7 has a strong understanding of its target market and buyers. This is reflected in the straightforward pricing model, easy deployment via SaaS, inclusion of an endpoint agent and wide functional coverage, and the availability of MDR services delivered with the platform.
- InsightIDR can address the detection of complex insider threats and malware due to the advanced analytics engine and risk scoring developed for InsightIDR's initial target as a UEBA tool.
- There are value-added integrations with other Rapid7 solutions in the Rapid7 Insight platform, notably integration of its Rapid7 InsightVM vulnerability assessment offering as a first-class citizen in risk prioritization.

Cautions

- Rapid7 InsightIDR is delivered only as SaaS and will not be appropriate for organizations that require an on-premises solution, or that have data governance mandates that prevent logs from leaving the organization.
- Heavy prioritization of integrations with other Rapid7 solutions creates holes in InsightIDR's technology ecosystem. For example, there is no integration of VM data from Qualys or Tenable into InsightIDR, and there is limited ability to use endpoint agents outside of Rapid7 Insight Agent.
- SOAR capabilities leveraging the technology from the Komand acquisition in July 2017 were announced as InsightConnect in September 2018. There are not yet any details on how the product will look or be licensed, or any feedback from early adopters.
- Business and threat context is limited to solutions within Rapid7's portfolio, and to Rapid7's MDR teams and its own threat intelligence feed, along with some open-source feeds. Support for TAXII is not yet available, but is on the roadmap (along with YARA).

Securonix

The Securonix SNYPR Security Analytics Platform provides SIEM capabilities via an on-premises solution or as a SaaS-delivered option. SNYPR leverages a Hadoop platform to provide event and data collection and management, analytics that include rule-based and advanced analytics (also sold stand-alone as its UEBA solution), and operational functions such as dashboards, incident management and response, and reporting. SNYPR includes a variety of components in the platform that can be leveraged to scale based on buyer requirements and environments. Premium apps (and app bundles) provide prepackaged behavior models, rules, reports and dashboards across a variety of security monitoring use cases related to privileged accounts, data security, access, cyberthreats, patient data, fraud and trade surveillance. Incident investigation and threat hunting activities are supported by Securonix's Spotter feature. SNYPR can be deployed in a variety of ways, including software-only that includes the Hadoop environment, or as software that can use a buyer's existing Hadoop environment. Turnkey deployments are supported via a physical appliance that includes all required components. Securonix licenses are term-based, priced on the number of identities in an organization (per EPS pricing is also offered) for SNYPR. Premium apps and bundles are licensed by the number of identities monitored. SNYPR Hadoop support services are priced per node deployed.

Over the past 12 months, Securonix has focused on delivering two updates to the Security Analytics Platform (6.1 and 6.2). The emphasis has been on adding features to improve incident management and response via recommendations for response actions and automated plays, and enhancements to threat detection analytics focused on network traffic analysis. Securonix also introduced a tool to simplify customers' management and operations of the Hadoop platform. Securonix now also offers co-managed services that include a threat monitoring option.

Large enterprises seeking flexible deployment options and a range of security monitoring use cases with optional analytics add-ons oriented to specific vertical needs should consider Securonix.

Strengths

- Licensing options are decoupled from data volumes by using the number of identities as the metric for all elements of the solution — for Security Analytics Platform and individual and bundled apps. Securonix can license based on EPS as required, but it is not an option that Gartner clients are adopting.
- Securonix's data management tier is flexible and can ingest an extensive set of data sources and formats that are applied to both streaming and batch analytics. Support for archiving data to AWS S3 is available.
- The use cases supported out of the box and via premium content are extensive and support a variety of monitoring scenarios across security and risk management (e.g., insider threat, fraud analytics, medical apps and technologies).
- Securonix has flexible delivery models, including a SaaS option that removes the need to deploy and manage a Hadoop platform, as well as support organizations where a majority of its data is being generated within IaaS or PaaS.
- Customer feedback for Securonix is positive overall.

Cautions

- There is an improved visual/dashboard for monitoring the Hadoop components of the platform called SNYPREye, but Hadoop is still not a common platform in use for SIEM, and experience managing this platform is not common in SecOps. Potential buyers should confirm that SNYPREye provides an effective complement to their internal security operations resources, or consider the SaaS delivery option.
- Incident response capabilities, particularly around automation, are better than many SIEM solutions, but Securonix lacks the ease-of-use features that many competitors have added (e.g., a visual play/process creation tool, an app store for integrating third-party technologies).
- Securonix lacks native advanced threat defense solutions, relying on integrations with third-party solutions for those functions (e.g., host and network forensics).
- Securonix has moderate visibility relative to competitors in the SIEM technology market.

SolarWinds

Log & Event Manager (LEM) is the SIEM solution from SolarWinds. LEM includes the core SIEM solution that provides data management, real-time correlation and log searching to support investigations. The LEM solution is composed of the Manager and Console, deployed via a virtual appliance, and an endpoint agent. The agent provides log collection and forwarding, in addition to FIM, EDR (including active response functionality) and lightweight DLP capabilities. LEM is complemented with other products in the SolarWinds portfolio for ticketing and case management, network and application monitoring, and virtual platform monitoring. SolarWinds LEM is licensed using a perpetual model by number of event source nodes (like servers) and workstations (via a specialized price).

Version 6.5, released in September 2018, added support for raw log forwarding from LEM and the ability to deploy LEM in Microsoft Azure. Version 6.4, released in June 2018, added new features like the first elements of a new HTML5 user interface, focused on viewing and searching log data, as well as support for more than 2TB of storage and other administrative improvements.

Organizations with compliance-focused use cases that also want to support IT management use cases should consider SolarWinds.

Strengths

- Potential buyers can leverage a fully functioning 30-day trial to run their own POC at their leisure, with the ability to convert over to a licensed model post-POC. SolarWinds offers a robust online support capability to assist POCs and buyers with design, deployment, installation and operating support.
- SolarWinds leverages a simple architecture and pricing model, along with a large library of compliance reports and correlation rules that appeal to the MSE and smaller enterprise buyer.
- The functionality availability with the LEM agent will appeal to organizations looking to tightly integrate their SIEM with an agent for log collection, as well as seeking preventative and active response-type capabilities, rather than relying on separate solutions. The LEM agent supports a variety of platforms including Windows, Linux, macOS, IBM AIX, Oracle Solaris and others.
- The vendor has moderate visibility with Gartner clients, particularly among SMBs and MSEs.

Cautions

- SolarWinds lacks support for monitoring public cloud services' IaaS or SaaS. Buyers looking to collect logs (and perform visualizations) from IaaS environments, and make them available for search to aid incident investigation, could leverage SolarWinds' Papertrail and Loggly solutions for those use cases.
- SolarWinds LEM does not have native case or incident management functionality, which will require buyers to purchase that solution from SolarWinds or integrate with a third-party tool. A stand-alone ticketing or case management solution for incident management is needed, and integrations are limited to a single direction via email and SNMP.
- Custom report writing and customization of out-of-the-box compliance report templates are not supported with LEM and require the use of Crystal Reports.
- Buyers looking to integrate LEM with non-SolarWinds solutions will need to confirm what third-party solutions can be supported.

Splunk

Splunk's Security Intelligence Platform is composed of Splunk Enterprise and three solutions: Splunk Enterprise Security (ES), Splunk User Behavior Analytics (UBA) and Splunk Phantom. Splunk Enterprise provides event and data collection, search, and visualizations for various uses in IT operations and some security use cases. The premium ES solution delivers most of the security-monitoring-specific capabilities, including security-specific queries, visualizations and dashboards, and some case management, workflow and incident response capabilities. UBA adds ML-driven, advanced analytics. Phantom provides SOAR capabilities. Additional apps for security use cases are available through Splunkbase. There are multiple deployment options: software on-premises, in IaaS and as a hybrid model. Splunk Cloud is a Splunk-hosted and -operated SaaS solution using AWS infrastructure. Splunk Enterprise and Splunk Cloud components consist of Universal Forwarders, Indexers and Search Heads supporting n-tier architectures. Splunk is licensed based on the amount of data ingested into the platform, with pricing discounts for DNS and NetFlow data. ES is also licensed by gigabytes per day, whereas UBA is licensed by the number of user accounts in an organization, and all these are available either as perpetual or term licenses, with various options for enterprisewide pricing and true-ups. Phantom is priced by the number of events on which users take action.

Splunk's most important enhancements over the past 12 months are support for guided investigation via the Investigation Workbench UI in Splunk ES, rapid content updates for ES and UBA, and speed improvements.

Organizations seeking SIEM solutions that can share architecture and vendor management across SIEM and other IT use cases, and seeking a scalable solution with a full range of options from basic log management through advanced analytics and response, should consider Splunk.

Strengths

- Splunk's offerings provide organizations with multiple entry points into security monitoring with a path that can start with basic event collection and simple use cases with Splunk Enterprise through to richer SIEM functionality with ES, more advanced analytics with UBA and SOAR capabilities with Phantom.
- The vendor has a strong ecosystem of technology integrations available in the Splunk application marketplace, although users of other technologies that compete with Splunk (for example, in the user analytics space) should validate the depth of integration.
- PII protection features are strong; obfuscation and PII masking are supported down to the field level, and can be applied based on user identities, locations and other characteristics.
- Splunk is highly visible in the industry among Gartner clients interested in security monitoring solutions, among service providers that compete to provide Splunk services and among the workforce that offers widespread Splunk technical expertise.

Cautions

- Customers and prospective buyers continue to express concerns about pricing models and total cost. The addition of Phantom, and the introduction of the "nerve center" concept (separate SIEM, UBA and SOAR products), results in three pricing models with different measurement approaches.
- Splunk provides no native agent support for FIM or EDR, although there are integrations with numerous third-party solutions.
- Splunk support for OT/IoT is largely dependent on the capabilities of third-party apps, rather than on Splunk support for OT protocols.
- Splunk UBA is an on-premises or customer cloud-only solution at this point, which can create friction with Splunk Cloud customers wishing to remain in a SaaS model.

Venustech

Venustech's SIEM solution is composed of Venusense Unified Security Management (USM) as the core SIEM solution, and includes Security Analytics (SA), Network Traffic Analytics (NTA), Configuration Verification System (CVS), Log Analysis System (LAS) for user behavior analysis and Business Security Management (BSM). Venusense SA provides log collection, normalization and storage, and an analytics engine for threat detection and compliance use cases. It is based on a big data platform, with both Hadoop and Elasticsearch options available depending on the amount of events and data being collected. Venustech offers software, virtual appliances and physical appliances, except NTA, which is available as a physical appliance and software. Additional options for specific use cases, such as monitoring industrial control systems and asset collection and monitoring, are available as well (e.g., Venusense USM-ICS and Venusense-AEM). Venustech also offers a variety of security technologies in addition to its SIEM solution, focused on the China, Asia/Pacific and Middle East markets, with solutions covering firewalls and UTM, web application firewalls, intrusion detection, vulnerability scanning, VPNs, and other products. The solution is licensed by the core product version (back-end data tier), number of data source nodes and add-on functional modules.

Over the past year, Venustech added support for additional threat and business context data sources, enhanced its analytics capabilities, and added its own CASB product to the Venustech technology portfolio.

Organizations in the China and Asia/Pacific region seeking an analytics-focused SIEM solution with network monitoring should consider Venustech.

Strengths

- Venusense USM's support for a variety of sources of nonsecurity event data is extensive and includes network flow, vulnerability, configuration and performance via native data collection options using host- and network-based sensors.
- Monitoring of ICS/SCADA environments and OT devices is supported using a combination of preconfigured correlation rules (included natively with the core SIEM solution as of the version 3.1 release) when deployed with Venustech's NTA or ICS flow collectors. A scaled-down version of its SIEM product specific to ICS monitoring is also available (USM-ICS).
- The vendor offers a wide range of complementary security technologies for its SIEM solution for buyers that want a single vendor and platform for a variety of security operations, threat detection and risk management capabilities.
- Customer feedback on the overall experience with Venustech is above average, including service and support, and product capabilities.

Cautions

- Venustech has little visibility with Gartner clients compared to other competing SIEM solutions, as the vendor primarily sells to Chinese customers and in some other markets in the Asia/Pacific region, such as Singapore. Visibility elsewhere in the world is low due to the focus on Asia/Pacific markets, although Venustech has recently expanded into the European market.
- Buyers should confirm which version of the solution is appropriate for their requirements (and future growth, to avoid selecting the wrong option) because there are three versions of the core product, varying based on data collection and management and confidentiality requirements. The small deployment version leverages Elasticsearch, and the large deployment version leverages Hadoop along with Elasticsearch to support very large data collection and analysis requirements.
- There is no app store or marketplace for integrations and content. Buyers must download content updates from the Venustech website.
- USM and additional components and products are quite extensive, with many variations. Buyers should confirm the components required for their deployments and ensure that they understand how the various components are priced and licensed.

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 be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

LogPoint has been added to the Magic Quadrant this year, because it meets the criteria for inclusion.

Dropped

Trustwave has been dropped from the Magic Quadrant because the vendor is focused on selling managed security and managed detection and response (MDR) services, rather than actively pursuing the SIEM market.

Coverage of the Micro Focus (NetIQ) Sentinel product has been dropped due to vendor focus on its ArcSight product, and lack of Gartner customer interest in Sentinel.

FireEye has been dropped due to the vendor's focus on selling the solution primarily as a managed platform.

Inclusion and Exclusion Criteria

To qualify for inclusion, vendors need to meet the following criteria:

- The product must be generally available and provide SIM and SEM capabilities.
- The product must support data capture from heterogeneous data sources, including network devices, security devices, security programs and servers.
- The vendor must appear on the SIEM product evaluation lists of end-user organizations.
- The solution must be delivered to the customer environment as a software- or appliance-based product or in an as-a-service model.
- SIEM revenue (net new license revenue plus maintenance) must be at least $18 million for 2017. Gartner will require that you provide a written confirmation of achievement of this requirement. The confirmation must be from an appropriate finance executive within your organization.

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 within production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed by conducting surveys of vendor-provided reference customers, in combination with feedback via inquiry, Peer Insights and other interactions from Gartner clients that are using or have completed competitive evaluations of the SIEM offering.

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	High
Sales Execution/Pricing	High

Evaluation Criteria	Weighting
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (December 2018)

Completeness of Vision

Market Understanding evaluates the ability of the technology provider to understand current and emerging buyer needs, and to translate those needs 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, and 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. Because the SIEM market is mature, there is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and consolidated administration capabilities. In this evaluation, we do not weight heavily the relative capabilities of vendors in these areas,

but there would be a severe “vision penalty” (that is, a lower rating on the Completeness of Vision axis) for a vendor that has shortcomings in this area. We continue to place greater weight on current capabilities that aid in targeted attack detection and response.

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 that are able to provide effective products that users can successfully 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 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. There is also an evaluation of capabilities for monitoring cloud environments.

For **Geographic Strategy**, although the North American and European markets produce the most SIEM revenue, Latin America and the Asia/Pacific 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.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High

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

Source: Gartner (December 2018)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a strong functional match to general market requirements, and have been the most successful in building an installed base and revenue stream within the SIEM market. Leaders also have a relatively high viability rating (due to SIEM revenue or SIEM revenue in combination with revenue from other sources). In addition to providing technology that is a good match to 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 lack the track record for competitive success with their SIEM technologies, compared to vendors in the Leaders quadrant.

Visionaries

The Visionaries quadrant is composed of vendors that provide products that are a strong functional match to general SIEM market requirements, but have a lower Ability to Execute rating than the 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, or by 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 to 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 a number of 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:

- Advanced threat detection — 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 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 should be driven by organization-specific requirements in areas such as:

- Relative importance of basic capabilities versus advanced features
- Budget constraints
- Scale of the deployment
- 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 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

During the past year, demand for SIEM technology has remained strong. The SIEM market grew from $1.999 billion in 2016 to $2.180 billion in 2017 (see “Market Share Analysis: Security Software, Worldwide, 2017”). Threat management is the primary driver, and general monitoring and compliance remains 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, but most buyers regard it as “table stakes.”

Demand for SIEM technology in Europe and the Asia/Pacific region remains steady, driven by a combination of threat management and compliance requirements. New compliance requirements related to the privacy of specific information that might be in gathered in the course of using an SIEM is driving scrutiny to SIEM capabilities to meet those requirements through access control and data masking. Growth rates in the less mature markets of the Asia/Pacific region and Latin America are much higher than those in the more mature North American and European markets. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for those geographies.

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 re-evaluating SIEM vendors to replace SIEM technology associated with incomplete, marginal or failed deployments.

The SIEM market is mature and very competitive. We are in a broad adoption phase, in which multiple vendors can meet the basic requirements of a typical customer. 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 evolving, with recent entrants bringing technologies optimized for analytics use cases. Vendors with more mature SIEM technologies are moving swiftly to incorporate big data technology and analytics to better support detection and response. The SIEM market continues to be dominated by relatively few large vendors. Splunk, Micro Focus (including the ArcSight and Sentinel SIEMs) IBM, LogRhythm and McAfee command a significant share of market revenue. 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 providers.

Leading SIEMs have integrations with big data platforms (the vendors' own, where they have them or open-source options like Hadoop). A number of vendors with in-house security research capabilities (IBM, McAfee, Dell Technologies [RSA]) or customer-sourced threat intelligence (AlienVault) provide integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (EventTracker, IBM) are marketing co-managed SIEM technology deployments that include a range of monitoring services. Rapid7 offers as-a-service SIEM.

Several vendors are not included in the Magic Quadrant because of a specific vertical market focus and/or SIEM revenue and competitive visibility levels:

- Odyssey Consultants, based in Cyprus, and HanSight, based in China, offer SIEMs based on modern, big data and analytics architectures, but currently have very limited visibility among Gartner customers.
- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer, and has expanded to include security monitoring for Salesforce.

- Huntsman Security (part of Tier-3) is an SIEM vendor with a presence primarily in the U.K. and Australia. The Huntsman Enterprise SIEM can be augmented with modules to support behavioral anomaly detection and threat intelligence.
- Developed by S21sec, 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.

Customer Requirements — Security Monitoring and Compliance Reporting for Systems, Users, Data and Applications

Customers remain primarily focused on security use cases for SIEM, with compliance typically a secondary requirement. The security organization often wants to employ SIEM to improve capabilities for external and internal threat discovery and incident management (see “Use SIEM for Targeted Attack Detection”). As a consequence, there are requirements for user activity and resource access monitoring for host systems and applications (see “Market Guide for User and Entity Behavior Analytics”). In this year’s Magic Quadrant, we continue to place greater weight on capabilities that aid in targeted attack detection, including support for user activity monitoring, application activity monitoring, profiling and anomaly detection, threat intelligence, effective analytics, and incident response features.

Ongoing consideration of SIEM technology by companies with limited security resources results in demand for products that are easy to deploy and manage, and provide security monitoring content like correlation rules, queries, dashboards, reports, threat feeds that support basic security monitoring and compliance reporting functions.

SIEM solutions should:

- Support the real-time collection and analysis of events from host systems, security devices and network devices, combined with contextual information for threats, users, assets and data.
- Provide long-term event and context data storage and analytics.

- Provide predefined functions that can be lightly customized to meet company-specific requirements.
- Be as easy as possible to deploy and maintain.

Scalability

Scalability is a major consideration in SIEM deployments. For an SIEM technology to meet the requirements for a given deployment, it must be able to collect, process, normalize, store and analyze all security-relevant events and other context-relevant data. Minimal latency is necessary for real-time correlation and alerting. Event processing includes parsing, filtering, aggregation, correlation, enrichment, alerting, display, indexing and writing to the data store. Scalability also includes access to the data for analytics and reporting — even during peak event periods — with ad hoc query response times that enable iterative searching for incident investigation. Behavioral and analytics require the collection and analysis of data over longer time periods than typically used for real-time alerting. We characterize the size of a deployment based on three principal factors:

- Number of event sources
- Sustained events collected per second
- Size of the event data store

We assume a mix of event sources that are dominated by servers, but also include firewalls, intrusion detection sensors and network devices. The boundaries for small, midsize and large deployments are not absolute, because some deployments may have a large number of relatively quiet event sources, while others will have a smaller number of very busy event sources. For example, a deployment with several busy log sources may exceed the EPS boundary for a small deployment, but will still be small architecturally.

Gartner defines a small deployment as one with 300 or fewer event sources, a sustained EPS rate of 1,500 EPS or less, and a back store sized at 800GB or less. Gartner defines a midsize deployment as one with 400 to 800 event sources, a sustained event rate of 2,000 to 7,000 EPS and a back store of 4TB to 8TB. A large deployment is defined as one with more than 900 event sources, a sustained event rate of more than 15,000 EPS, and a back store of 10TB or more. Some very large deployments have many thousands of event sources, sustained event rates of more

than 25,000 EPS and a back store of more than 50TB. We may indicate that a vendor's SIEM technology is better-suited for a small, midsize or large deployment, which means that the size is a typical or most common successful deployment for that vendor. Every vendor will have outliers.

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 to expand the deployment to include new use cases (like those for advanced threat detection). We expect that demand by SIEM users for such services will grow, driven by more customers adopting 24/7 monitoring requirements and implementing use cases that require deeper SIEM operational and analytics expertise.

SIEM vendors may support these needs via managed services with their own staff or outsourcing services, or using partners. SIEM offered as a service (SIEMaaS) includes the maintenance of the platform by the vendor, often in a public cloud environment, with customers using 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 problematic for external service providers, and SIEM users exploring services should evaluate the fit of the service provider to meet current and planned use cases.

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 advanced attacks. The combination of Elasticsearch, Logstash and Kibana (aka the ELK Stack or Elastic Stack); Apache Spot; Apache Metron; and other tools leveraged with or natively using big data platforms like Hadoop offer capabilities for data collection, management and analytics. Organizations with sufficient 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 a sufficient number of their requirements for a lower cost compared to 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 negate the objective of being less expensive than a commercial SIEM deployment.

Vendors of central log management solutions (such as Graylog or Sumo Logic), typically targeted to log collection and analysis for IT operations use cases, are increasingly incorporating support for basic security use cases, and Gartner expects this trend to continue. These products may allow organizations with basic security and compliance use cases to share a common log collection architecture for IT operations and security, and avoid the cost and complexity of deploying and maintaining SIEM (see “Use Central Log Management for Security Event Monitoring Use Cases”).

There are a number of providers offering 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. As such, 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 advanced threat detection capabilities, and may compete for SIEM budget 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

Sources of information to support this analysis include feedback from Gartner clients gathered through inquiry calls, face-to-face meetings and survey/polling tools; vendor information supplied in response to a survey, product demonstration and/or briefings; and vendor reference opinions gathered via polling tools.

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.

Completeness of Vision

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.