Magic Quadrant for Security Information and Event Management

10 August 2016 | ID:G00290113

Analyst(s): Kelly M. Kavanagh, Oliver Rochford, Toby Bussa

Summary

The need for early targeted attack detection and response is driving the expansion of new and existing SIEM deployments. Advanced users seek SIEM with advanced profiling, analytics and response features.

Strategic Planning Assumption

By the end of 2017, at least 60% of major SIEM vendors will incorporate advanced analytics and UEBA functionality into their products.

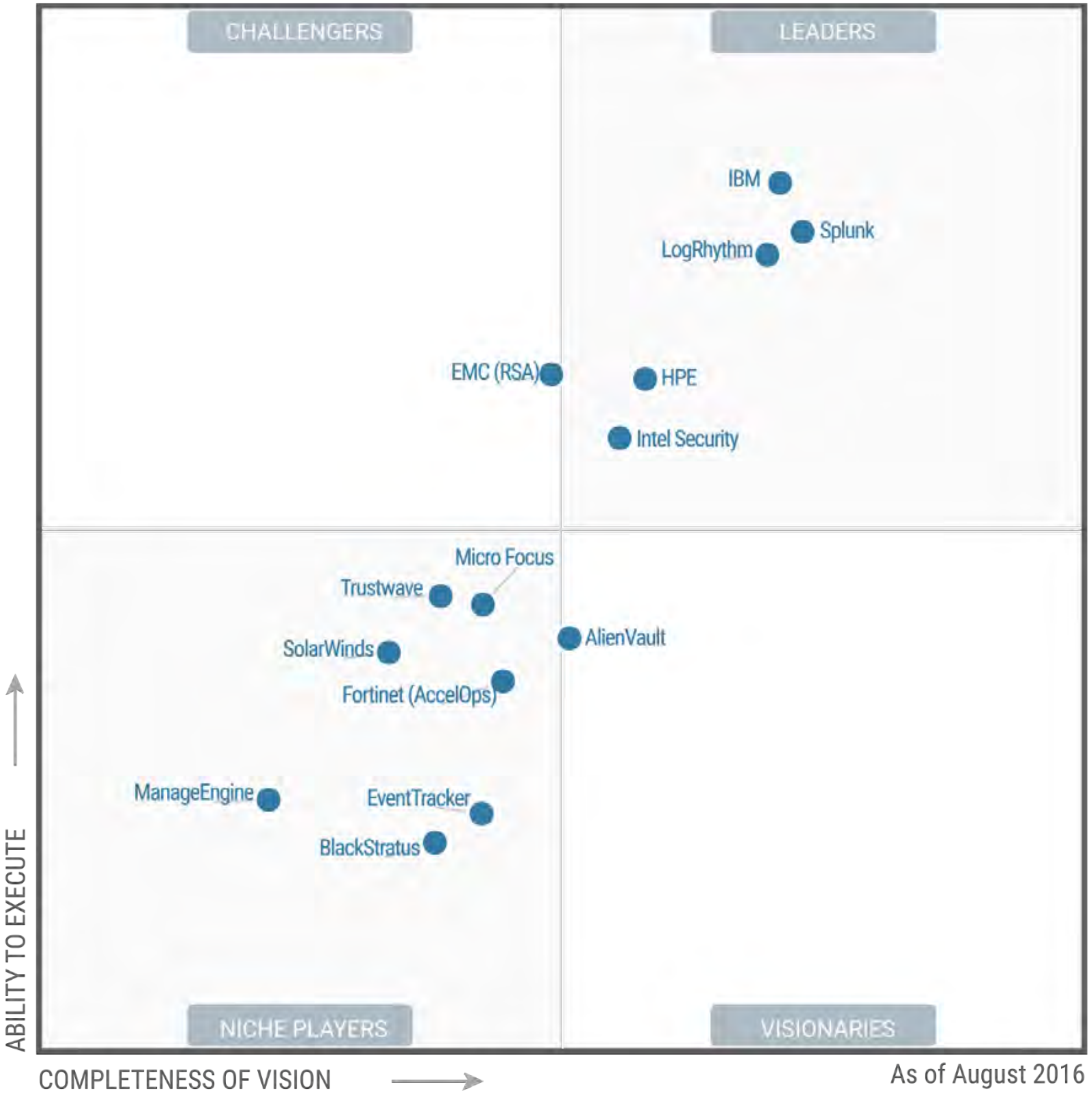
Market Definition/Description

The security information and event management (SIEM) market is defined by the customer's need to analyze event data in real time for the 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 NetFlow and network packets. Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data is normalized, so that events, data and contextual information from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time correlation of events for security monitoring, query and analytics for historical analysis and other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (August 2016)

Vendor Strengths and Cautions

AlienVault

The AlienVault Unified Security Management (USM) solution provides SIEM, vulnerability assessment (VA), asset discovery, network and host intrusion detection (NIDS/HIDS), flow and packet capture, and file integrity monitoring (FIM). AlienVault USM provides centralized configuration and management of all AlienVault components. AlienVault USM for Amazon Web Services (AWS) is an AWS-native version providing asset discovery; vulnerability assessment; monitoring and alerting for CloudTrail, Simple Storage Service (S3) and Elastic Load Balancing (ELB) access; log management; and event correlation. The AlienVault USM is composed of open-source components such as Open Vulnerability Assessment System (OpenVAS; VA), Snort, Suricata (intrusion detection system [IDS]), and OSSEC (HIDS/FIM), and combines these with SIEM to provide a unified security solution. USM buyers have access to a subscription-based threat intelligence service consisting of correlation directives, IDS signatures, vulnerability checks, reports and response templates. In addition, the free Open Threat Exchange (OTX) and its community enable discussion and sharing of threat information. AlienVault also offers open-source SIM (OSSIM), a free, open-source version of its solution with a reduced feature set. AlienVault USM extends OSSIM with scaling enhancements, log management, consolidated administration and reporting, and federation for managed security service providers (MSSPs).

AlienVault USM is available as both a virtual and hardware appliance. The sensor, logger and server components of USM can be deployed combined in one system (all-in-one architecture), or as separate servers in horizontal and vertical tiers to scale to diverse customer environments. Over the past 12 months, AlienVault feature updates included better asset visibility and agent management, faster reporting updates, and deeper integration with OTX. The AlienVault USM platform should be considered by organizations that need a broad set of integrated security capabilities at relatively low cost for on-premises and AWS environments.

STRENGTHS

- AlienVault USM provides a variety of integrated security capabilities, including SIEM, file integrity monitoring, vulnerability assessment, asset discovery, and both host-based and network-based intrusion detection systems.
- USM provides a well-designed interface for navigating events, assets and threat intelligence for investigating incidents based on the kill chain framework.
- Customers report the security monitoring technologies included with USM offer a lower cost for more capabilities compared with products from most competitors in the SIEM space.
- AlienVault offers a simplified licensing model based on utilized appliances, rather than based on event volume or the number of event sources.

CAUTIONS

- USM provides NetFlow capture, basic statistics and context for assets, but cannot generate alerts from NetFlow.
- Integration of unsupported data sources is cumbersome compared with competing products. Alternatively, users can request AlienVault develop a plug-in to enable the integration.
- Although identity activity can be linked with assets, USM provides only basic enrichment of event data with user context; and identity and access management (IAM) integration is limited to Active Directory and LDAP.
- AlienVault's workflow capabilities do not include integrations with external ticketing systems or role-based workflow assignments.

BlackStratus

BlackStratus has three offerings: LOGStorm, SIEMStorm and CYBERShark. LOGStorm provides log management capabilities aimed at MSSPs and small to midsize enterprises, and is available as virtual and hardware appliances. SIEMStorm provides features such as multitenancy and security event management (SEM) capabilities, including analytics, historical correlation and threat intelligence integration, and is deployable as software or virtual images. SIEMStorm can be deployed in combination with LOGStorm, utilizing it as the storage and collection tier. BlackStratus recently introduced CYBERShark, a cloud-based SIEM-as-a-service offering for small or midsize businesses (SMBs) based on LOGStorm and SIEMStorm.

LOGStorm and SIEMStorm provide an integrated incident management and ticketing system guided by the SANS seven-step incident remediation process, and SIEMStorm also allows the tracking of SLA metrics to accommodate MSSP and service-centric environments.

In the past 12 months, BlackStratus has added a new compliance reporting template set, the ability for service providers to brand the portal, and released a redesigned and updated HTML5 web user interface.

BlackStratus is a good fit for service providers requiring a customizable SIEM platform, and for service-centric end-user organizations looking for well-formed multitenancy support.

STRENGTHS

- SIEMStorm and LOGStorm can be deployed as virtual machines, and include an installation wizard and a passive autodiscovery feature for data source integration.
- LOGStorm and SIEMStorm provide a bidirectional integration API to enable custom-built service architectures.
- LOGStorm and SIEMStorm include a fully integrated incident and ticket management system based on the SANS incident handling process.
- BlackStratus support received praise from customers for speed of response and expertise.

CAUTIONS

- Out-of-the-box support for third-party data sources is limited and may frequently require custom scripting.
- Advanced security capabilities, such as network forensic and deep packet inspection (DPI), and IAM integrations, are currently not supported. Although Proofpoint is supported, other commercial threat feeds require vendor support to implement.
- Customer feedback indicates that ad hoc querying of log event data could be more granular and lacks Boolean logic.
- BlackStratus has focused on sales to security service providers, and has not been very visible in competitive evaluations for end-user deployments.

EMC (RSA)

In July, 2016, RSA, The Security Division of EMC rebranded its SIEM offering as the RSA NetWitness Suite, which includes RSA NetWitness Logs, RSA NetWitness Packets, RSA NetWitness Endpoint, and RSA NetWitness SecOps Manager — formerly RSA Security Analytics, RSA Enterprise Compromise Assessment Tool (ECAT) and RSA SecOps, respectively. RSA NetWitness Suite provides visibility of threats using data from security events and other log sources, network full-packet capture, NetFlow and endpoints (via NetWitness Endpoint). The RSA NetWitness system is focused on real-time monitoring, analysis and alerting, in addition to supporting proactive threat hunting, and incident response and forensic investigation. The platform leverages a combination of one or more physical or virtual appliances for log and packet capture (Decoder), querying and raw data retrieval (Concentrators), real-time analytics (Event Stream Analysis), and long-term log storage and reporting (Archiver). Hybrid appliances (combining Decoders and Concentrators into a single system) are available for smaller environments. Decoder and Concentrator appliances as well as Brokers are available to support large and regionally distributed architectures. The NetWitness server provides a unified interface for administration and analysis. It also provides an interface for reporting and to the malware analytics engines. RSA Live Connect is the cloud-based service (included with product support agreements) that provides automated content updates including detection rules, packet and log parsers, reports, and threat intelligence feeds. RSA NetWitness Suite users can also leverage RSA NetWitness SecOps Management (a module in the RSA Archer Governance, Risk, and Compliance [GRC] solution), which adds advanced incident management workflow, operational playbooks, management dashboards and reporting.

Over the past 12 months, RSA has added command-and-control communication detection using behavior analytics, selective log retention, enhancements to event source integration and grouping, and support for AWS monitoring by integrating CloudTrail logs.

RSA NetWitness Suite should be considered by organizations with dedicated security operations centers (SOCs) and incident response teams, or those organizations with a dedicated service provider that require security monitoring across logs and network traffic for threat detection and validation, and forensic investigation.

STRENGTHS

- RSA NetWitness platform combines threat detection analytics and event monitoring, investigation, and threat intelligence across network traffic, endpoints and other security event and log data sources.

- Modular deployment options enable customers to select network traffic monitoring, or event and log monitoring and analysis capabilities as needed.
- RSA Live provides an easy, automated approach to ensure threat intelligence, content and other updates are delivered and implemented seamlessly.
- Integration with RSA NetWitness SecOps Manager provides unified SOC capabilities. Existing Archer users will benefit from integration allowing for centralized risk management, metrics and reporting across an organization.

CAUTIONS

- Customers report RSA NetWitness Suite is a complex SIEM technology to implement and tune to achieve desired use cases.
- The RSA NetWitness user interface is basic compared with competing products. The out-of-the-box dashboards require greater customization compared with other SIEM solutions.
- RSA NetWitness provides only lightweight incident management capabilities. Richer workflow capabilities are available through RSA SecOps Manager.

EventTracker

EventTracker targets its SIEM software and service offering primarily at midsize and government organizations with security event management and compliance reporting requirements. EventTracker Security Center is available as software, with licensing based on the number of event sources. Standard components include correlation, alerting, behavior analysis, reporting, dashboards and a large number of event source knowledge packs. Options include configuration assessment, change audit FIM, ntopng, threat intelligence feeds (open source or commercial subscriptions) and the analyst data mart. Service offerings include annual subscriptions aligned to run, watch, tune and comply activities performed on schedules ranging from daily to weekly. Collection from and deployment in AWS and Azure are natively supported.

Capabilities added in the past year include unknown process detection and blacklisting/whitelisting, IP reputation integrations and alerting, threat analysis dashboards with third-party enrichment, as well as other threat intelligence feed options. Support for JSON and extraction, transformation and loading (ETL) format logs were added, and the user interface was rewritten to support touchscreen mobile devices.

Midsize businesses requiring a software-based solution for log and event management, compliance reporting, and operations monitoring via on-premises or cloud-hosted SIEM with optional, flexible monitoring services should consider EventTracker.

STRENGTHS

- EventTracker is easy to deploy and maintain, with compliance and use-case-specific knowledge packs that provide prebuilt alerts, correlation rules and reports.
- Reference customers and Gartner clients give EventTracker good marks for support and for packaged reports and new report creation features.
- EventTracker includes a behavior analysis module that provides basic profiling and anomaly detection functions.
- EventTracker's range of service offerings aligned with run, watch, tune and comply activity is a differentiator, and addresses the needs of its target market.

CAUTIONS

- The vendor targets the midmarket, but is not as visible on customer shortlists as other SIEM vendors that are also targeting this segment.

- EventTracker's advanced threat detection features are basic, Windows-centric, and in the case of flow and packet capture, not cleanly integrated into the core product. Integrations with third-party advanced threat detection/response technologies are not available.
- EventTracker's capabilities for application monitoring are more limited than SIEM products that target enterprise deployments, as it lacks integration with major packaged applications.
- Full incident management, including ticketing, requires an external solution. Several integrations via email and XML are supported.

Fortinet (AccelOps)

In June 2016, Fortinet announced it had acquired AccelOps, with plans to rebrand its SIEM product as FortiSIEM and integrate it into Fortinet Security Fabric; for example, integrating with Fortinet's APM solution focused on network and cloud environment monitoring. AccelOps SIEM provides SIM and SEM, file integrity monitoring, configuration management database (CMDB), and availability and performance monitoring (APM) capabilities. AccelOps had a primary focus on providing a solution for security operations and managed service providers (MSPs) and MSSPs.

AccelOps has a modest number of MSP and MSSP customers that use its SIEM, CMDB and FIM capabilities for security and network monitoring, and it is one of only a few vendors that has capabilities for both IT and network operations use cases. Fortinet now has the opportunity to expand the sale of AccelOps SIEM into its service provider and end-user customer base.

In the past year, AccelOps expanded its SIEM offerings to include a cloud-based SIEM-as-a-service offering with three tiers (Basic, Plus and Pro) targeted at MSPs and MSSPs, and organizations using AWS and Azure. Other enhancements include additional support for virtualization and public cloud services (Hyper-V, Xen, OpenStack and Azure), improved threat feed integration, and additional support for network and endpoint advanced threat detection solutions. AccelOps also updated its architecture with the introduction of Apache Kafka to better integrate with big data platforms.

AccelOps SIEM is a good fit for midmarket organizations, and MSPs and MSSPs that require a combination of security monitoring and APM with integrated CMDB capabilities. It is also well-suited for IT operations teams with combined IT, network and security operation functions, as well as organizations needing multitenancy capabilities for role and duty separation.

STRENGTHS

- AccelOps SIEM's combination of security and operational capabilities can be used by IT, network and security operational teams to provide a unified view across an organization's environment, including physical and virtualized environments, as well as public, private and hybrid clouds.
- Midmarket organizations with centralized monitoring and response accountability across the entire IT environment will benefit from AccelOps' integrations that enable a unified platform.
- AccelOps has a strong focus on integrating operational and security capabilities to support remediation and incident management.
- Customers report that the technology is relatively easy to deploy, with positive feedback for the depth and flexibility of customization.

CAUTIONS

- Existing AccelOps customers should request assurances from Fortinet that the development roadmap for SIEM and related platform products will continue or expand support for third-party technologies.
- AccelOps SIEM lags the competition in advanced analytics capabilities, direct integration with big data platforms like Hadoop, and integration of complementary solutions like user and entity behavior analytics (UEBA).
- AccelOps is only marginally visible in competitive evaluations of SIEM with Gartner clients. Fortinet's sales and deployment support capabilities in the SIEM market are unproven.

HPE

Hewlett Packard Enterprise (HPE) sells its ArcSight SIEM platform to midsize organizations, enterprises and service providers. The platform is available in three different variations: the ArcSight Data Platform (ADP), providing log collection, management and reporting; ArcSight Enterprise Security Management (ESM) software for large-scale security monitoring deployments; and ArcSight Express, an appliance-based all-in-one offering that's designed for the midmarket, with preconfigured monitoring and reporting, as well as simplified data management.

The ArcSight Data Platform (composed of ArcSight Connectors, ArcSight Management Center [ArcMC; a management console] and Logger) can be deployed independently as a log management solution, but is also used as the data collection tier for ArcSight ESM deployments. Premium modules, adding capabilities such as user and entity behavior analytics (ArcSight User Behavior Analytics [UBA]), DNS malware detection (ArcSight DNS Malware Analytics) and threat intelligence (ArcSight Reputation Security Monitor [RepSM]), can be used to extend the SIEM's capabilities.

HPE ArcSight can be deployed as an appliance, software or virtualized instance, and supports a scalable n-tier architecture with HPE ArcSight Management Center available to manage large and complex deployments. HPE ArcSight Express is available as an appliance only.

In 2015, HPE redesigned and simplified the ArcSight SIEM architecture and licensing model. Further enhancements include new features in the analyst user interface allowing more granular control over incoming events and incidents. New module releases included HPE ArcSight UBA (licensed from Securonix); HPE ArcSight DNS Malware Analytics, providing malware detection based on DNS traffic analysis; HPE ArcSight Marketplace, a community exchange for integration with other vendor solutions; and SIEM context such as dashboards and report templates.

ArcSight Express should be considered for midsize SIEM deployments requiring extensive third-party connector support. HPE ArcSight ESM is a good fit for large-scale deployments and for organizations seeking to build a dedicated SOC.

STRENGTHS

- ArcSight ESM provides a complete set of SIEM capabilities that can be used to support a large-scale SOC, including a full incident investigation and management workflow, and a dedicated deployment management console.
- HPE ArcSight User Behavior Analytics provides full UBA capabilities in conjunction with SIEM.
- HPE ArcSight has a wide variety of out-of-the-box third-party technology connectors and integrations.

CAUTIONS

- HPE ArcSight proposals routinely include more professional services than comparable offerings.
- Customer feedback indicates that HPE ArcSight ESM is found to be more complex and expensive to deploy, configure and operate than other leading solutions.
- Although ArcSight is among the top four vendors in competitive visibility with Gartner clients, the trend is decreasing visibility for new installs and increasing numbers of competitive replacements.
- HPE is undertaking a development effort to redo the core ArcSight technology platform. Customers and prospective buyers should track development plans to ensure the availability of features and functions needed to support existing or planned deployments.

IBM

IBM's QRadar Security Intelligence Platform comprises the QRadar Log Manager, Data Node, SIEM, Risk Manager, Vulnerability Manager, QFlow and VFlow Collectors, and Incident Forensics. QRadar can be deployed using physical and virtual appliances, and infrastructure as a service (IaaS; such as in public or private cloud services). QRadar is also available in an as-a-service solution (IBM QRadar on Cloud), which is fully managed by IBM along with optional event monitoring provided by the IBM Managed Security

Services team. Deployment options range from all-in-one implementations or scaled implementations using separate appliances for discrete functions. The QRadar platform enables collection and processing of security event and log data, NetFlow, network traffic monitoring using deep-packet inspection and full-packet capture, and behavior analysis for all supported data sources.

IBM introduced several new features and capabilities in the past 12 months, including IBM X-Force Exchange for sharing threat intelligence, and IBM Security App Exchange, supported by the QRadar Application Framework. IBM also acquired Resilient Systems in April 2016 to extend the incident response capabilities of the QRadar platform. Enhancements were made in the product's multitenant capabilities, system administration (health monitoring and patch management) and search performance.

Midsize and large enterprises with general SIEM requirements, as well as organizations looking for a single security event monitoring and response platform for their SOCs should consider QRadar. Midsize organizations looking for a solution with flexible implementation, hosting and monitoring options should also consider QRadar.

STRENGTHS

- QRadar provides an integrated view of log and event data, with network flow and packets, vulnerability and asset data, and threat intelligence.
- Network traffic behavior analysis can be correlated across NetFlow and log events.
- QRadar's modular architecture supports security event and log monitoring in IaaS environments, including native monitoring for AWS CloudTrail and SoftLayer.
- QRadar's technology and architectural approach makes it relatively straightforward to deploy and maintain, whether as an all-in-one appliance or a large-tiered, multisite environment.
- IBM Security App Exchange provides a framework to integrate capabilities from third-party technologies into the SIEM dashboards and investigation and response workflow.

CAUTIONS

- Endpoint monitoring for threat detection and response, or basic file integrity requires use of third-party technologies.
- Gartner clients report mixed success with the integration of the IBM vulnerability management add-on for QRadar.
- Gartner clients report the sales engagement process with IBM can be complex and requires persistence.

Intel Security

Intel Security provides McAfee Enterprise Security Manager (ESM) as a physical, virtual or software appliance. The three primary components that make up the SIEM offering are ESM, the Event Receiver (ERC) and the Enterprise Log Manager, which can be deployed together as one instance, or separately for distributed or large-scale environments. Optional components include Advanced Correlation Engine (ACE), Database Event Monitor (DEM), Application Data Monitor (ADM), and Global Threat Intelligence (GTI).

Enhancements introduced in the past 12 months include the ability to dynamically populate watch lists from additional internal or external sources, deeper two-way integration with Hadoop, and support for additional access to and management of threat intelligence feeds. Integration with McAfee Active Response now provides ESM with greater endpoint visibility. McAfee Enterprise Security Manager is a good choice for organizations that use other Intel Security technologies, as well as those seeking an integrated security framework that includes response capabilities

STRENGTHS

- Customers with Intel Security's McAfee ePolicy Orchestrator (ePO) value the deep integration with ESM.
- Enterprise Security Manager has good coverage of operational technology (industrial control systems [ICSs]), and supervisory

control and data acquisition (SCADA) devices.

- Intel Security's McAfee Data Exchange Layer (DXL) enables integrations with third-party technologies without the use of APIs. This approach shows promise for allowing the use of ESM as an SIEM platform.

CAUTIONS

- Intel Security's many advanced SIEM features and capabilities in areas such as endpoint intelligence and automated response require integrations with, or further investments in, other Intel portfolio products.
- Intel provides limited advanced analytics capabilities and integrations with third-party tools. Baselines and variances are identified, and risk-based analytics are available via the ACE. However, there are no predictive analytics, and other built-in features are not as strong as those of leading competitors.
- ESM provides strong workflow features. However, out-of-the-box integration is available only with Remedy. Support for other workflow products is limited to email, or through development with the ESM API.
- Feedback from users and Gartner clients about poor stability and performance with ESM has continued over the past 12 months.
- Users highlight a lack of satisfaction with technical support.
- McAfee ESM has slipped in visibility in Gartner client inquiries over the past year, and customer discussions about displacement have increased.

LogRhythm

LogRhythm sells its SIEM solutions to midsize and large enterprises. LogRhythm's SIEM can be deployed in an appliance, software or virtual instance format and supports an n-tier scalable decentralized architecture composed of the Platform Manager, AI Engine, Data Processors, Data Indexers and Data Collectors. Consolidated all-in-one deployments are also possible. System Monitor and Network Monitor can optionally be deployed to provide endpoint and network forensic capabilities such as system process, file integrity and NetFlow monitoring, DPI, and full-packet capture. LogRhythm combines event, endpoint and network monitoring capabilities with UEBA features, an integrated incident response workflow, and automated response capabilities.

In the past year, LogRhythm has separated out the log processing and indexing capabilities of its SIEM solution into two separate components, adding a storage back end based on Elasticsearch to provide unstructured search capabilities. Clustered full data replication was also added. Other enhancements include improvements to the risk-based prioritization (RBP) scoring algorithm; additional parsers for applications and protocols for Network Monitor; support for cloud services such as AWS, Box and Okta; and integrations with cloud access security broker (CASB) solutions including Microsoft's Cloud App Security (formerly Adallom) and Zscaler.

LogRhythm is an especially good fit for organizations that require integrated advanced threat monitoring capabilities in combination with SIEM. Those organizations with resource-restricted security teams requiring a high degree of automation and out-of-the-box content should also consider LogRhythm.

STRENGTHS

- LogRhythm combines SIEM capabilities with endpoint monitoring, network forensics, UEBA and incident management capabilities to support security operations and advanced threat monitoring use cases.
- LogRhythm provides a highly interactive and customizable user experience, with dynamic context integration and security monitoring workflows.
- LogRhythm provides emerging automated response capabilities to execute actions on remote devices.
- Gartner receives consistent user feedback stating that LogRhythm's solution is straightforward to deploy and maintain, and provides effective out-of-the-box use cases and workflows.

- LogRhythm continues to be very visible in the competitive SIEM technology evaluations of Gartner clients.

CAUTIONS

- Although LogRhythm's integrated security capabilities, such as System Monitor and Network Monitor, enable synergies across IT derived from the deeper integration with the SIEM, organizations with critical IT and network operations requirements in this area should evaluate them against related point solutions.
- User feedback indicates that the custom report engine is a feature that needs improvement.
- LogRhythm has fewer sales and channel resources compared with other leading SIEM vendors, and buyers in geographies outside of North America may have fewer choices for reseller and services partners.

ManageEngine

ManageEngine, a division of Zoho, provides SIEM capabilities using the ManageEngine EventLog Analyzer and ADAudit Plus products. Log360 integrates both tools into a single product. EventLog Analyzer provides log management, monitoring, analysis, correlation and archiving, as well as alerting and reporting capabilities. There are two versions — Premium for single instance deployment and Distributed for large organizations or MSPs that require the ability to scale beyond a single EventLog Analyzer instance. The Distributed Edition leverages an Admin server to manage and provide a single view across individual Managed servers. ADAudit Plus focuses on monitoring, alerting and auditing of Active Directory, providing the user context to EventLog Analyzer. ADAudit Plus is offered in two versions — Standard and Professional depending on the features required. Both products are provided as VMware images that include a PostgreSQL database for storage and primarily rely on an agentless approach for security event and log collection. EventLog Analyzer is licensed based on number of hosts, devices or applications generating security events or event logs.

ManageEngine is an established vendor in the IT service and IT operations and management spaces. Organizations that are already users of other ManageEngine tools and are looking for a simple, cost-effective approach to adding security event monitoring capabilities should consider EventAnalyzer or Log360.

STRENGTHS

- ManageEngine provides a single appliance that is easy to deploy, and quickly integrates logs either via syslog or via log import.
- Over 1,000 predefined reports, including various compliance-focused ones, are available covering a range of devices and applications in a typical IT environment.
- ADAudit Plus provides a comprehensive logging and auditing capability for organizations solely using Active Directory for identity and access control.

CAUTIONS

- EventAnalyzer provides basic SIEM functionality, but lags competitors in several key areas, such as security operations and monitoring dashboards, workflow for incident management, support for threat intelligence feeds and platforms, and network traffic and NetFlow monitoring.
- Although Log360 integrates EventAnalyzer and ADAudit Plus, analysts are required to leverage at least two different user interfaces to perform various activities, such as monitoring for new incidents, investigations and reporting.
- Since ADAudit Plus is directed at small and midsize organizations, larger organizations need to carefully evaluate against requirements for scalability, performance and support.
- ManageEngine has little visibility with Gartner clients for SIEM use cases.

Micro Focus

NetIQ was acquired by Micro Focus in 2014. Sentinel Enterprise is the core SIEM product from Micro Focus, complemented by Change Guardian (for host monitoring and FIM) and Secure Configuration Manager (for compliance use cases). Additional modules add a range of features covering threat intelligence feeds, exploit detection, and high-availability support. NetIQ Identity Manager and Aegis customers can also benefit from integration with Sentinel for enhanced identity tracking and workflow management capabilities. Log management is available as a stand-alone product (Sentinel Log Manager). Sentinel Enterprise is offered as software and as a virtual appliance.

Micro Focus made modest enhancements to Sentinel during the past 12 months, focusing on usability enhancements, platform health and management, visualizations, simplified deployment, and improved threat intelligence.

Sentinel is a good fit for organizations or MSSPs that require large-scale security event processing for highly distributed IT environments (for example, geographic or cloud), and is an especially good choice for organizations that have deployed NetIQ IAM and IT operations tools, which can provide enriched context to security events detected with Sentinel.

STRENGTHS

- Sentinel Enterprise is appropriate for large-scale deployments that are focused on SEM and SIM threat monitoring capabilities, where contextual information is automatically added to any correlated event.
- Integrations with other NetIQ technologies provide capabilities to support user monitoring, identity and endpoint monitoring, and enforcement/response use cases.
- NetIQ's architecture is one of the simpler available to deploy and manage. Scaling and distribution only require installation of more Sentinel instances.
- Sentinel supports monitoring of mainframe platforms in addition to standard Windows, Unix and Linux platforms.
- NetIQ customers give Sentinel above-average or average marks for scalability and performance, ease of customizing existing report templates, and support experience.

CAUTIONS

- NetFlow data can only be used to provide additional context for alerted events and cannot be used within correlation rules.
- Sentinel's threat intelligence capabilities still lag the competition. Customers can purchase threat feeds from NetIQ. Additionally, there is basic support for a few open-source feeds, but third-party feeds require a software development kit (SDK)-based plug-in to be created and there is no support for open standards like STIX and TAXII.
- Support and integration with UEBA tools are lacking, and advanced analytics capabilities are lagging compared to competitors' products.
- Usability and reporting of the results when replaying historical event data against correlation rules are limited when compared with some competitors.
- NetIQ Sentinel has low visibility in competitive evaluations of SIEM among Gartner clients.

SolarWinds

SolarWinds Log & Event Manager (LEM) software is available as a virtual appliance. The architecture is composed of the LEM Manager, providing centralized log storage and management, the LEM Console for data display and search, and optional agents. LEM includes basic data loss prevention (DLP), FIM and automated response capabilities for Windows hosts.

In 2015, SolarWinds added its "zero configuration" threat intelligence feed to provide regular threat intelligence updates for reputational IP blacklists.

SolarWinds positions LEM as an easy-to-deploy and use SIEM product for resource-constrained security teams that have no requirements for big data, advanced analytics or advanced threat detection capabilities. LEM has integrations with SolarWinds' other products for operation monitoring to support activities such as change detection and root cause analysis. SolarWinds LEM is a good fit for small or midsize companies that requires SIEM technology with a simple architecture, and for those that wish to combine SIEM use with other SolarWinds IT operations solutions.

STRENGTHS

- SolarWinds LEM has a simple architecture and provides extensive out-of-the-box content suitable for a variety of SMB compliance and security operations use cases.
- The technology is well-suited for organizations that have also invested in other SolarWinds technology solutions, and these integrations can also provide synergies.
- An automated response capability based on the endpoint agent for Windows provides some threat containment and quarantine control capabilities.
- SolarWinds offers a simplified licensing model based on asset count, not consumption.
- SolarWinds' customers report high levels of satisfaction with LEM, and praise the balance of costs versus features.

CAUTIONS

- SolarWinds LEM provides only basic statistical and behavior analytics and has no integrations with user behavior analytics or big data platforms.
- SolarWinds provides no dedicated support for third-party advanced threat defense technologies.
- Customers requiring more extensive user, application or web monitoring must acquire other SolarWinds products to extend the capabilities available in LEM.
- Although LEM includes a native flow capture and display capability, flow data is not available for real-time correlation in LEM, and packet capture is not supported.
- SolarWinds' SIEM architecture supports horizontal scaling of LEM instances, but does not support true distributed n-tier scaling.

Splunk

The Splunk Security Intelligence Platform is composed of Splunk Enterprise — the core product from Splunk that provides event and log collection, search and visualization using the Splunk query language — and Splunk Enterprise Security (ES), which adds security-specific SIEM features. Data analysis is the primary feature of Splunk Enterprise, and is used for IT operations, application performance management, business intelligence and, increasingly, for security event monitoring and analysis when implemented with Enterprise Security. Splunk Enterprise Security provides predefined dashboards, correlation rules, searches, visualizations and reports to support real-time security monitoring and alerting, incident response, and compliance reporting use cases. Splunk Enterprise and Splunk Enterprise Security can be deployed on-premises, in public or private clouds, or as a hybrid. Both products are also available as a SaaS offering. Splunk's architecture consists of streaming input and Forwarders to ingest data, Indexers that index and store raw machine logs, and Search Heads that provide data access via the web-based GUI interface.

In mid-2015, Splunk added native UEBA functionality with the acquisition of Caspida, which was rebranded Splunk UBA (Splunk works with a number of other UEBA products, as well). Tighter integration between the Enterprise Security and UBA products was introduced in early 2016. Additional improvements were made to incident management and workflow capabilities; and for lower data storage requirements, improved visualizations and expansion of monitoring to additional IaaS and SaaS providers.

Splunk continues to focus on security event monitoring and analysis use cases. Threat intelligence capabilities and security-product-specific apps in Splunkbase add further context and functionality. Organizations that require an SIEM platform with flexibility for a variety of data sources and analytics capabilities (such as machine learning and UEBA), as well as those that need a single data analysis platform across an organization should consider Splunk.

STRENGTHS

- Splunk's investment in security monitoring use cases is driving significant visibility with Gartner clients.
- Advanced security analytics capabilities are available from both native machine learning functionality and integration with Splunk UBA for more advanced methods, providing customers with the necessary features to implement advanced threat detection monitoring and inside threat use cases.
- Splunk's presence, and investment, in IT operations monitoring solutions provides security teams with in-house experience, as well as existing infrastructure and data to build upon when implementing security monitoring capabilities.

CAUTIONS

- Splunk Enterprise Security provides only basic predefined correlations for user monitoring and reporting requirements, compared with richer content for use cases provided by leading competitors.
- Splunk license models are based on data volume in gigabytes indexed per day. Customers report that the solution is costlier than other SIEM products where high data volumes are expected, and recommend sufficient planning and prioritization of data sources to avoid overconsuming licensed data volumes. In the past 12 months, Splunk introduced licensing programs to address high-volume-data users.
- Potential buyers of Splunk UBA should plan appropriately, as it requires a separate infrastructure and leverages a license model different from how Splunk Enterprise and Enterprise Security are licensed.

Trustwave

Trustwave offers a broad portfolio of security products covering security management in addition to network, content and data, endpoint, and application security. Trustwave's SIEM offering is part of the Security Management portfolio. Trustwave has two SIEM product options: SIEM Enterprise and Log Management Enterprise (LME), both available as physical or virtual appliances, with LME also available as an AWS advanced metering infrastructure (AMI). Trustwave LME and SIEM Enterprise provide a range of options suitable for both midmarket and enterprise-sized buyers. Additionally, Trustwave offers a variety of co-managed, or hybrid, services augmenting its security management products.

Over the past year, Trustwave has made improvements focused on core functions of the products, including improved storage options, user interface and search enhancements, and deployment enhancements focused on managed and multitenancy deployments.

Trustwave is a good option for buyers already invested in products and services from Trustwave's portfolio, or for midmarket buyers seeking an SIEM product to complement a broader set of security technologies from the same vendor, as well as those needing support via a co-managed service.

STRENGTHS

- Trustwave's Security Management products include a broad range of deployment and service options, including co-managed or hybrid services that support customers with limited internal resources for technology management, as well as security monitoring and analysis.
- Customers of other Trustwave security products will benefit from improved bidirectional integration across many technologies in its portfolio that supports automated response capabilities (active integration and response), like quarantining endpoints or locking accounts.
- SIEM Enterprise offers correlation, capacity and customization capabilities appropriate for customers with large-scale event monitoring and multitenant requirements, as well as geographically diverse locations.

- Trustwave has one of the simpler architectures that eases the burden on customers during deployment and any future expansion.

CAUTIONS

- Trustwave has little visibility in competitive evaluations of SIEM offerings among Gartner clients.
- Threat intelligence integration is limited to feeds provided by Trustwave's SpiderLabs (which include some third-party feed data). Direct integration of third-party feeds into the SIEM requires professional services support.
- Trustwave SIEM Enterprise lacks native capabilities to provide user behavior analytics and does not offer integration with leading UEBA vendors.
- On-premises SIEM Enterprise buyers who need integration with big data platforms will require customized approaches as Trustwave has focused on its big data capabilities for co-managed SIEM customers.

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

ManageEngine was added to the Magic Quadrant.

Dropped

No vendors were dropped from the Magic Quadrant this year.

Inclusion and Exclusion Criteria

The following criteria had to be met for vendors to be included in the 2016 SIEM Magic Quadrant:

- The product must 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 (not a service).

Vendors were excluded if:

- They provide SIEM functions that are oriented primarily to data from their own products.
- They position their products as an SIEM offering, but the products do not appear on the competitive shortlists of end-user organizations.
- They had less than $13.5 million in SIEM product revenue during 2015.
- The solution is delivered exclusively as a managed service.

For exclusion, Gartner considers revenue and relative visibility of vendors in the market. The revenue threshold is $13.5 million per year for 2015 (net-new license revenue plus maintenance). Visibility is determined from among the following factors: presence on Gartner client shortlists via client inquiries, Peer Insight reports, search references on gartner.com, presence on vendor-supplied customer reference shortlists and mentions as a competitor by other SIEM vendors.

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
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (August 2016)

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 neutralized the relative ratings of vendors with capabilities 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, including:
  - Vendor capabilities for profiling and anomaly detection to complement existing rule-based correlation.
  - Threat intelligence and business context integration, including automated updates, filtering, and usage within rules, alerts and reports.
  - User monitoring capabilities, including monitoring of administrative policy changes and integration with IAM technologies, for automated import of access policy (user context) for use in monitoring. We also evaluate predefined analytics for user behavior analysis.
  - Data access monitoring capabilities, which include direct monitoring of database logs and integration with database audit and protection products, DLP integration, and file integrity monitoring through native capability and integration with third-party products.
  - Application layer monitoring capabilities, including integration with third-party applications (for example, ERP financial and HR applications, and industry vertical applications), for the purpose of user activity and transaction monitoring at that layer; the external event source integration interface that is used to define the log format of an organization's in-house-developed applications; and the ability to derive application context from external sources.
  - Analytics, an important capability to support the early detection of targeted attacks and breaches. SIEM vendors have long provided query capabilities against the primary storage tiers of SIEM technology. In order to be effective for early breach detection, the analytics capability must incorporate context about users, assets, threats and network activity, and must also provide query performance that supports an iterative approach to investigation. Some SIEM vendors have introduced separate data stores to hold very large amounts of security event, content and contextual data, optimized for applying advanced analytics. A number of SIEM vendors have also built connectors from the SIEM technology to industry-standard big data repositories.
  - Inclusion of advanced threat detection, network traffic monitoring and packet capture capabilities, and integrations with third-party technologies that provide these functions for more effective early breach detection.

Despite the vendor focus on expansion of capability, 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, fraud detection and identity-oriented monitoring are evaluated, in addition to other capabilities that are product-specific and are 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 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 SIEM markets produce the most 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
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 (August 2016)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a strong functional match to general market requirements, have been the most successful in building an installed base and revenue stream within the SIEM market, and 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 they lack the track record for competitive success with their SIEM technologies, compared with 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 or 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 — Real-time monitoring and reporting of user activity, data access, and application activity, 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
- Forensics and incident response — Dashboards and visualization capabilities, as well as workflow and documentation support to enable effective incident identification, investigation and response

Although many SIEM deployments have been funded to address regulatory compliance reporting requirements, improving security monitoring and early breach detection is now the primary driver for SIEM. The SIEM market is composed of technology providers that support all three use cases; however, there are variations in the relative level of capability for each use case. This year's evaluation continues to more heavily weight capabilities that support advanced threat detection and response. As a companion to this research, we evaluate the SIEM technologies of the vendors in this Magic Quadrant with respect to the three major use cases noted above (see "Critical Capabilities for Security Information and Event Management").

Organizations should consider SIEM products from vendors in every quadrant of this Magic Quadrant, based on their specific functional and operational requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of basic capabilities versus advanced features; the scale of the deployment; complexity of product (deployment, running, using and supporting); the IT organization's project deployment and technology support capabilities; and integration with established applications, data monitoring and identity management infrastructure (see "Toolkit: Security Information and Event Management RFP").

Security managers considering SIEM deployments should first define the requirements for SEM and reporting. The requirements definition should include capabilities that will be needed for subsequent deployment phases. The project will benefit from the input of other groups, including audit/compliance, identity administration, IT operations and application owners (see "How to Deploy SIEM Technology"). Organizations should also describe their network and system deployment topology, and assess event rates, so that prospective SIEM vendors can propose solutions for company-specific deployment scenarios. The requirements definition effort should also include phase deployments beyond the initial use case. 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 $1.67 billion in 2014 to $1.73 billion in 2015 (see "Forecast Analysis: Information Security, Worldwide, 1Q16 Update"). The buying drivers that were in place at the start of 2015 remain in effect today. Threat management is the primary driver, and compliance remains secondary. In North America, there continue to be many new deployments by smaller companies 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 discussions with Gartner clients are security-focused. Demand for SIEM technology in Europe and the Asia/Pacific region remains steady, driven by a combination of threat management and compliance requirements. Growth rates in the less mature markets of Asia/Pacific 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 large companies 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 targeted attack and breach detection. Organizations are failing at early breach detection, with more than 80% of breaches undetected by the breached organization. [1] The situation can be improved with threat intelligence, behavior profiling and effective analytics. We are monitoring the emerging area of UEBA, and early adopters report effective detection of targeted attacks with limited deployment efforts. In 2015, Splunk acquired the UEBA vendor Caspida, and HPE announced an integration solution including ArcSight and Securonix. We expect SIEM vendors to continue to increase their native support for behavior analysis capabilities as well as integrations with third-party technologies over the next 18 months, as more enterprises develop use cases based on behavior.

Most companies expand their initial SIEM deployments over a three-year period to include more event sources, greater use of real-time monitoring and investigation to support incident response. The large SIEM vendors have significant existing customer bases, and there continues to be a focus on the expansion of SIEM technology deployments within existing accounts. In general, SIEM vendors are continuing to incrementally improve product capabilities in areas related to breach detection — threat intelligence, anomaly detection and activity monitoring from the network — as well as investigation workflow and case management.

SIEM Vendor Landscape

Fourteen vendors met Gartner's inclusion requirements for the 2016 SIEM Magic Quadrant. Six are point solution vendors, and eight are vendors that sell additional security or operations products and services. In June 2016, Fortinet announce the acquisition of AccelOps. The AccelOps SIEM product will be rebranded as FortiSIEM. The SIEM market continues to be dominated by relatively few large vendors — HPE, IBM, Intel Security and Splunk — that command more than 60% of market revenue. LogRhythm is an example of a point solution vendor that continues to do very well. There is increasing stress on many of the remaining small vendors, as small and midsize organizations seek managed services or SIEM-as-a-service options to reduce the internal resources needed for compliance or security requirements. As a result, we note that SIEM vendors both large and small are turning to third-party services providers to deliver operational services for their SIEM, or offering such services themselves.

SIEM technology is now deployed by a broad range of enterprises. SIEM vendors are increasingly focused on supporting additional use cases so they can continue to sell additional capabilities to their customer bases. Some SIEM technology purchase decisions do not include a competitive evaluation, because the technology is sold by a large vendor in combination with related security, network or operations management technologies; but most SIEM purchases are made on the merits of SIEM capabilities.

Leading SIEM vendors continue to focus on targeted attack and breach detection through incorporation of threat intelligence, analytics, profiling and anomaly detection, and network activity monitoring. Specialized UEBA products with advanced capabilities to support early breach detection are emerging and have gained awareness and acceptance in the market over the past 18 months. These are typically positioned by vendors as complementary to SIEM, with a higher fidelity in finding advanced attacks than SIEM. In practice, the technologies are often deployed to support distinct use cases, and complementary integrations between the tools can make analytic results and context available to each product.

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, HPE, Intel Security, RSA and Trustwave) provide integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (EventTracker, HPE, IBM and Trustwave) are marketing co-managed SIEM technology deployments that include a range of monitoring services. RSA provides a common platform for log management and network packet capture, and also integrates its SIEM with its IT GRC technology. Intel Security's strategy is increasingly focused on technology integration within its own security portfolio, and on selling SIEM to large enterprises that use its endpoint and other security products. Several vendors are not included in the Magic Quadrant because of a specific vertical-market focus and/or SIEM revenue and competitive visibility levels:

- 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 distinguishing characteristic of the technology is its profiling and anomaly detection capabilities. The vendor does not meet our more stringent revenue and visibility thresholds.
- Lookwise is an SIEM vendor that was spun out of S21sec and 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. Lookwise does not meet our more stringent revenue and visibility thresholds.
- Tango/04 provides operational event correlation, business process monitoring and SIEM solutions to customers in Europe and

South America. The vendor no longer meets our more stringent revenue and visibility thresholds.

- Tripwire's Log Center is focused on augmenting Tripwire capabilities to provide greater system state intelligence.
- Tenable's SecurityCenter Continuous View (SecurityCenter CV) provides Tenable customers with a central capability of analyzing vulnerability data along with event data from Tenable technology integration partners' solutions.

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

During the past year, Gartner clients deploying SIEM technology have continued to be primarily focused on security use cases. Even though compliance continues to be a secondary driver, the primary focus continues to be targeted attack and breach detection. 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 "Effective Security Monitoring Requires Context"). In this year's SIEM vendor Magic Quadrant evaluation, 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, and effective analytics, as well as on incident response features.

The continued adoption of SIEM technology by companies with limited security programs has fostered a demand for products that provide predefined content such as correlation rules, queries, dashboards, reports, threat feeds that support basic security monitoring and compliance reporting functions, as well as ease of deployment and support.

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, store and analyze all security-relevant events. Events that need to be monitored in real time have to be collected and processed with minimal latency. Event processing includes parsing, filtering, aggregation, correlation, 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 an iterative approach for incident investigation. Query performance needs to hold up, even as the event store grows over time. We characterize the size of a deployment based on three principal factors:

- The number of event sources
- The sustained events per second (collected after filtering, if any)
- The 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. Some deployments also include a large number of PC endpoints, but these are not typical, and PC endpoint counts are not included in our totals. 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 events per second (EPS) limits set below 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 events per second 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 events per second 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 events per second, 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 ideally 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 SIEM"). Drivers for external services include lack of internal resources to manage an SIEM deployment, lack of resources to perform real-time alert monitoring (as opposed to once a day or even less frequently), or lack of expertise to expand the deployment to include new use cases (such as endpoint detection monitoring and response). We expect demand by SIEM users for such services will grow, as more customers adopt 24/7 monitoring requirements and implement 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. Managed security service providers, which offer real-time monitoring and analysis of events, and collect logs for reporting and investigation, are another option for SIEM users. The number of hosted SIEM, or SIEM-as-a-service offerings (such as Splunk Cloud), is increasing to support customers opting to forgo SIEM technology management, but able to use internal resources for monitoring and investigation (see "Innovation Insight for SIEM as a Service"). For basic use cases, severely resource-constrained customers may opt for SaaS-type log management services from Logentries, Loggly, Papertrail, Sumo Logic or others that have some security utility but also cover operational use cases. 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 SIEM, as well as emerging security analytic technologies, have driven interest in alternative approaches to collecting and analyzing event data to identify advanced attacks. The combination of Elasticsearch, Logstash and Kibana (Elastic Stack), OpenSOC , Apache Metron and other tools leveraged with or natively using big data platforms like Hadoop offer data collection, management and analytics capabilities. 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 with commercial technologies. Gartner is tracking the development of this approach, as well as service providers offering Elastic Stack as a service (like Elastic) or managed security services (MSSs) for these technologies.

Organizations that lack the resources and process maturity for SIEM deployment and support, and cannot or choose not to engage an MSSP for monitoring can meet basic logging and review requirements with log management technologies (or services) such as Graylog or Sumo Logic with no, or very limited, security use cases supported out of the box.

There are a number of providers offering managed detection and response (MDR) services that differ from those of MSSPs, with the goal of identifying and responding to advanced threats in the customer environment — typically 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 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

Evidence used to prepare this report include information from briefings and structured data collection from vendors, discussions with Gartner customers during inquiries and other interactions, feedback provided by Gartner customers for Peer Insights, and data provided by vendor reference customers.

[1] "2016 Verizon Data Breach Investigations Report (DBIR)," Verizon. Figure 9, page 11, indicates the parties responsible for detecting a breach, with internal detection, is below 20% in 2015.

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.