Magic Quadrant for Security Information and Event Management

Published: 04 December 2017 **ID:** G00315428

Analyst(s):

Kelly M. Kavanagh, Toby Bussa

Summary

Security and risk management leaders are implementing and expanding SIEM to improve early targeted attack detection and response. Advanced users seek SIEM with advanced profiling, analytics and response features.

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, analyze, investigate and report on event 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 tools aggregate event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data, but SIEM tools can also process other forms of data, such as NetFlow and network packets, or contextual information about users, assets, threats and vulnerabilities that can be found inside or outside the enterprise and that can be useful to enrich logs and raw data. All these data are normalized so that events, data and contextual information from disparate sources can be correlated and analyzed for specific purposes, such as threat management, network security event monitoring (SEM), user activity monitoring and compliance reporting. The tools provide real-time correlation of events for security monitoring, enable query and analytics for historical analysis, and offer other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2017)

Vendor Strengths and Cautions

AlienVault

AlienVault competes in the SIEM market with two offerings: AlienVault Unified Security Management (USM) Appliance (physical or virtual) for on-premises deployment and AlienVault USM Anywhere, a cloud-based SaaS solution. USM Appliance includes file integrity monitoring (FIM) via the host intrusion detection system (IDS), NetFlow analysis and full-packet capture. USM Anywhere is designed to monitor cloud and on-premises environments from the AlienVault Secure Cloud. AlienVault also offers Open Threat Exchange (OTX), a free, community-supported threat intelligence sharing forum that integrates threat intelligence into USM. AlienVault Labs Threat Intelligence is a subscription service that updates correlation rules, reports, response templates, signatures for IDS and vulnerability checks in both USM Appliance and USM Anywhere. AlienVault is no longer offering its USM for Amazon Web Services (AWS) product, and customers of USM AWS have been migrated to USM Anywhere.

USM Anywhere became generally available in February 2017, and is the result of a from-scratch development effort. The focus of USM Anywhere is monitoring cloud environments, initially AWS and Microsoft Azure, although monitoring of on-premises technology is supported as well. The USM Anywhere architecture accommodates apps (AlienApps) to enable adding capabilities in a modular fashion. USM Anywhere and USM Appliance features and capabilities differ somewhat. AlienVault's current plans are to continue to offer both USM Appliance and USM Anywhere. The pricing model for USM Appliance is based on the number of appliances required, available as a perpetual license or monthly subscription. USM Anywhere is sold as a monthly subscription, priced by the volume of data consumed.

Strengths

- USM Appliance and USM Anywhere provide several integrated security capabilities, including asset discovery, FIM, vulnerability assessment, and both host-based and network-based intrusion detection systems.
- AlienVault provides content updates via its Threat Intelligence subscriptions, as well as community source intelligence, that are integrated into the monitoring, detection and reporting functions of USM Appliance and USM Anywhere.
- Customers report that the security monitoring technologies included with USM offer a lower cost for more capabilities compared with products from most competitors in the SIEM space.
- The pricing model for USM Anywhere and USM Appliance is straightforward and easy to understand, and the availability of monthly subscription pricing for USM Appliance offers flexibility.

Cautions

- There are differences in the capabilities of USM Appliance and USM Anywhere that may present potential buyers with trade-offs. For example, capturing NetFlow data is supported by USM Appliance, but not by USM Anywhere. USM Anywhere, however, can capture VPC flow logs from AWS. USM Appliance uses correlations to provide basic enrichment of event data with user context, and USM Anywhere uses a graph-based engine to support a basic user and entity behavior analytics (UEBA) capability focused on cloud environments.
- USM Appliance has more limited support for cloud environments than USM Anywhere. For example, in AWS, USM Anywhere monitors CloudTrail, CloudWatch Classic Load Balancer, Application Load Balancer and Simple Storage Service (S3) access, plus logs for installed software, and provides vulnerability assessments. USM Appliance provides monitoring of Windows and Linux guests on AWS via an HIDS agent.
- AlienVault's target market is midsize enterprises and smaller organizations. As a result, enterprise-oriented features, such as role-based workflow, ticketing integrations, support for multiple threat intelligence feeds and advanced analytics capabilities, lag behind those of competitors that focus on enterprise customers.

BlackStratus

BlackStratus is a SIEM technology and service-focused vendor with solutions aimed at large enterprises, small or midsize businesses (SMBs), managed security service providers (MSSPs), and managed service providers (MSPs). The portfolio is composed of LOGStorm, SIEMStorm and CYBERShark. LOGStorm is a log and event management and reporting tool

targeted at SMBs and MSSPs. It is available as a physical and virtual appliance. LOGStorm leverages a Vertica big data platform and stores both raw and normalized event data. SIEMStorm is a natively multitenant platform that is delivered as software, where components can be installed on a single physical or virtual server, or installed separately depending on the size and scope of the environment to be monitored. SIEMStorm includes core SIEM capabilities including real-time event management, correlation, analytics, workflow and incident response, and reporting. It is targeted at large enterprises or organizations with federated security monitoring requirements (e.g., across lines of business or child companies), as well as at MSSPs needing to support customers in a shared, multitenant environment. CYBERShark is a SIEM as a service aimed at MSPs and SMBs. It is delivered as a cloud-based solution, along with 24/7 Tier 1 security operations center (SOC) security monitoring and alerting services.

Recent enhancements of the platforms include a variety of new product integrations, in particular support for AWS, Azure, Office 365 and ServiceNow, as well as improvements to the user interface and back-end performance optimizations. Support for GE Digital (Wurldtech) OpShield was added to extend SIEMStorm to operational technology security monitoring use cases.

Strengths

- The architectures for SIEMStorm and LOGStorm are flexible for both deployment and expansion. All application components are multitenant out of the box.
- Integrations added over the past 12 months extend support for popular service desk solutions, as well as SaaS and IaaS environments.
- Support for OT data sources is now a native feature, albeit with limited support for OT security-based threat detection vendors, such as GE Digital (Wurldtech).
- SIEMStorm includes a fully integrated incident and ticket management system based on the SANS Institute's incident handling process.

Cautions

- Native advanced threat detection solutions, such as FIM, endpoint detection and response (EDR), network deep packet inspection, and network forensics, are not available. The vendor's open API does allow for integration with a variety of third-party solutions.
- Advanced analytics capabilities are very limited. BlackStratus indicates that expansion of analytics is planned over the next year.
- Support for identity and access management (IAM) solutions is limited. User-based event monitoring is provided for Active Directory (AD) and a variety of web access management (WAM) solutions.
- SIEMStorm's workflow capabilities lack orchestration and automation features.
- BlackStratus has a large MSSP and MSP customer base, but lacks visibility with Gartner's enterprise and SMB end-user clients.

Dell Technologies (RSA)

RSA (a Dell Technologies business since the acquisition of EMC by Dell in September 2016) competes in the SIEM market via its RSA NetWitness Suite. The suite is composed of RSA NetWitness Logs and Packets, RSA NetWitness Endpoint, and RSA NetWitness Security Operations (SecOps) Manager. RSA NetWitness Suite is focused on real-time threat detection, incident response, forensics and threat hunting use cases leveraging network full-

packet capture, security event and log data, NetFlow, and telemetry from endpoints. The architecture is composed of the RSA NetWitness Server along with Decoders (full-packet capture, logs, NetFlow and endpoint data collection); Concentrators (metadata aggregation and indexing); Event Stream Analytics (analytics for real-time monitoring and alerting); and Archivers (data and event archiving tier). There is a stand-alone management server for RSA NetWitness Endpoint. RSA NetWitness Suite offers flexible deployment options as it can be installed as software, physical and virtual appliances, and in hybrid configurations. On-premises as well as IaaS environments are supported. Scalability (both vertically and horizontally) is supported through the deployment of additional components (e.g., Decoders, Concentrators and Archivers). RSA NetWitness SecOps Manager, a module in the RSA Archer solution, adds advanced incident management workflow, operational playbooks, management dashboards and reporting. The solution is primarily licensed by volume (software model) or per appliance for Logs and Packets, and by number of agents for Endpoint. Both perpetual and term models are available.

Since mid-2016, RSA has added additional support for event and data collection within IaaS (AWS and Azure), support for deploying RSA NetWitness Suite components in AWS, and additional feature and functionality enhancements, such as the addition of RSA Live-delivered content packs focused on new users as well as advanced threat hunters, Trial Rules (allows rules to be demoed before being implemented in production), Endpoint agent support added for Linux and Mac, and expanded command-and-control behavior-based analytics. RSA NetWitness Suite 11, released in October 2017, provides a new user interface and enhancements to capabilities for investigation, incident management and identity insights.

Strengths

- RSA NetWitness Suite offers a single-solution approach for threat detection and event monitoring, investigation, and response across network traffic, endpoints and other security event and log data sources.
- RSA NetWitness Suite's focus on advanced threat detection, incident response, forensics and threat hunting makes it a viable solution for buyers with, or planning to deploy, a SOC and those looking for a single, integrated platform across teams.
- RSA Live, a cloud-based service, provides a marketplace-type interface for RSA NetWitness content packs (threat detection rules, parsers, reports), threat intelligence and third-party integrations. Threat intelligence and content updates can be automated so they are seamless to users.
- The RSA NetWitness Suite provides a flexible architecture that scales from a single appliance to complex n-tier deployments, which can span both on-premises and IaaS.
- Out-of-the-box threat intelligence includes access to over two dozen threat feeds, including intelligence from RSA's FirstWatch research team and incident response activities, and RSA Live provides crowdsourced threat intelligence from RSA NetWitness customers.

Cautions

- RSA NetWitness Suite's user interface is basic compared to competing SIEM solutions. RSA indicates that a new UI is included with version 11, released in October 2017.
- RSA NetWitness Logs and Packets lags behind similar SIEM solutions in UEBA capabilities. Integrations are available with third-party UEBA vendors.

- RSA NetWitness Suite's incident management capabilities are lightweight. Buyers looking for richer workflow capabilities need to purchase RSA NetWitness SecOps Manager.
- Native security orchestration and automation capabilities are limited, but out-of-the-box integrations with most third-party security operations, analytics and reporting (SOAR) solutions are available.

EventTracker

In October 2016, EventTracker merged with Netsurion, a provider of managed security services, and EventTracker continues as a subsidiary with its own brand. EventTracker targets its SIEM software and service offerings primarily at midsize and government organizations with security event management and compliance reporting requirements. EventTracker Enterprise software is available, 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, flow analyzer, honeynet, threat intelligence feeds and the analyst data mart. Service offerings include SIEMphonic co-managed SIEM aligned to run, watch, tune and comply with activities performed on schedules ranging from daily to weekly. Collection from and deployment in AWS and Azure are natively supported.

In the past year, EventTracker has added a security scorecard dashboard that provides a risk-prioritized view of security incidents and a deception component (honeynet) offered as a managed service. Support for NIST SP 800-171 and the EU's General Data Protection Regulation (GDPR), as well as 23 NYCRR 500 compliance, was also introduced.

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, and offers compliance and use-case-specific content with prebuilt alerts, correlation rules and reports.
- EventTracker's software pricing model is based on the number of event sources and is thus relatively straightforward for potential customers to understand. Perpetual license and annual subscription pricing are offered.
- EventTracker's SIEMphonic managed SIEM services aligned with run, watch, tune and comply activity are a differentiator, and address the needs of its target market.

Cautions

- EventTracker's SIEMphonic managed SIEM services offerings are based on data volume (not event source count, which is the model for the software), thus potential buyers comparing options will need to make different calculations when developing assumptions about the scope and growth of the monitored environment.
- 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 they lack integration with major packaged applications.
- Full incident management, including ticketing, requires an external solution. Several integrations via email and XML are supported.

Exabeam

Exabeam Security Intelligence Platform is a collection of components that collectively deliver the Exabeam SIEM solution that was introduced in February 2017. The platform is built on a variety of big data technologies, including Elastic, Hadoop, Kafka and Spark. Data management (collection, parsing, indexing and storage) is provided by Log Manager, which also includes agent-based collectors that can collect logs from local resources or from cloud-based applications using RESTful APIs. Advanced Analytics, also sold as Exabeam's stand-alone UEBA tool, provides analytics functionality via a collection of both expert rules as well as behavior- and machine learning (ML)-based analytics. Incident Responder provides workflow, case management, security orchestration and automation capabilities. Threat Hunter is a search and investigation tool oriented toward analysts doing incident investigations and analyses, or threat-hunting-oriented activities. Threat Hunter provides user-based timelines rather than focusing on standard query and search approaches. Customers requiring connecting to IaaS and SaaS can purchase Exabeam's Cloud Connectors, which are prebuilt API connectors for a variety of services, such as several AWS services, Office 365, SharePoint, Box and Salesforce. Exabeam's components can be run on dedicated appliances (two versions are currently available), and installed as software or virtual appliances.

Strengths

- Exabeam's licensing approach is based on the number of users in an organization, rather than the velocity or volume of event, log and contextual data analyzed.
- Exabeam has established itself as complementary to existing SIEM solutions through its UEBA solution, which forms the core of the vendor's solution portfolio. Advanced Analytics is included as part of the core platform, rather than as an add-on to complement traditional signature- and correlation-based rules.
- Customers can customize the SIEM platform by selecting the components to meet their requirements (e.g., starting out with Log Manager and Advanced Analytics and adding Incident Responder and Threat Hunter as buyer experience and maturity in security monitoring improve).
- Exabeam's architecture is big data-oriented and supports a variety of deployment options (physical and virtual, and on-premises, IaaS or hybrid) and offers easy horizontal scalability through the addition of more appliances.

Cautions

- Most of Exabeam's full platform, except for Advanced Analytics (which has been available for several years as a stand-alone UEBA tool, complementing SIEM), does not yet have widespread adoption and use compared to most SIEM solutions on the market.
- Predefined reporting capabilities against industry and regulatory requirements are nascent, given the focus on user-based monitoring. Reports can be created from searches and saved as dashboards, or created from visualization capabilities for viewing and exporting.

- Exabeam's platform lacks native network traffic analysis capabilities, although it supports a variety of third-party solutions. Flow data cannot yet be analyzed, but is available for ingestion and searches as part of incident investigations.

FireEye

FireEye is a new entrant in the SIEM Magic Quadrant. FireEye's SIEM offering is Threat Analytics Platform (TAP), which is delivered as a service leveraging AWS. TAP provides real-time security analytics, investigative threat hunting, monitoring and data management, and storage, with data segregated on a per-customer basis. Integrated threat intelligence is provided by in-house iSIGHT security researchers and Mandiant incident responders. Both multitenant as well as single-instance versions are supported.

TAP customers deploy a Cloud Collector appliance on their network to aggregate and securely transmit logs to TAP. Cloud Collector can also be deployed as a network security monitoring appliance that generates its own network metadata events as well as providing selective full-packet capture. Cloud Collector can be deployed as software, an ISO installer that supports bare-metal hardware or virtualized environments, or a physical appliance. Licensing is based on events per second (EPS) and data storage/retention requirements (13 months is the default.)

Strengths

- TAP's as-a-service delivery model gets strong marks for ease of deployment. There is no technology for customers to manage and only Cloud Collector appliances to deploy. There is out-of-the box support for a large variety of event sources. There are more than 2,300 predefined rules for alerting, which are updated or added continually.
- Threat intelligence from FireEye iSight, as well as curated open-source feeds, is included with the service.
- Guided investigation support for incidents and events includes best-practice suggestions and predefined searches.
- FireEye provides an optional 24/7 monitoring service (FireEye as a Service) for customers that lack the resource to staff full-time operations.

Cautions

- TAP currently includes a limited number of report templates, with PCI and HIPAA templates available for compliance reporting.
- Integrations with enterprise configuration management databases (CMDBs) and AD, support for STIX and TAXII, and more advanced orchestration and automation features are available only with the additional purchase of FireEye Security Orchestrator.
- Potential customers should closely evaluate TAP's current capabilities for advanced analytics against the use cases they want to support. User behavior analytics and analytics covering long time frames are not available.

Fortinet

FortiSIEM, acquired from AccelOps in 2016, is a component of Fortinet's Security Fabric framework that provides traditional SIM and SEM capabilities, complemented by a built-in CMDB, application and system performance monitoring capabilities, and agent-based FIM.

Fortinet positions FortiSIEM for MSPs, telecommunications providers and MSSPs that use or support other Fortinet solutions, in addition to 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, as well as by MSPs and MSSPs that take advantage of the full FortiSIEM stack.

FortiSIEM's architecture is composed of four components (Supervisors, Worker, Collector and Report Server) that are deployed via virtual appliances supported across a variety of on-premises (ESX, KVM, Hyper-V, Zen and OpenStack) and IaaS platforms (AWS and Azure), and can be deployed as a single appliance or stand-alone components for scalability. Data management leverages a mix of big data (NoSQL) and RDBMS. Managed SIEM as a service is also available to end users as well as to MSPs and MSSPs. Physical appliance options and a remediation library for integrations with third-party tools are expected later in 2017. Licensing is primarily based on the number of data sources, EPS and agents deployed.

Over the past 12 months, Fortinet has added additional integrations within the Fortinet Security Fabric, as well as adding risk-based scoring for devices; STIX and TAXII support for improved threat intelligence capabilities; user activity auditing for SaaS such as Office 365 and G Suite; and the initial move to an HTML5-based UI.

Strengths

- FortiSIEM provides a single platform for organizations looking to support multiple environments (on-premises physical and virtual, SaaS, and IaaS), use cases and teams across IT (network operations, security operations and application performance monitoring [APM]).
- A built-in autodiscovery feature and an integrated CMDB capability support use cases across IT, network operations and security operations.
- FortiSIEM's scope of reporting covers a wide variety of compliance requirements and best practices for both security operations and network operations across several geographies.
- Midmarket organizations, especially those leveraging other Fortinet products, where security responsibilities are federated out to teams like network operations, will benefit from the unified platform available with FortiSIEM, which includes native workflow and the ability to perform basic automated response activities.

Cautions

- FortiSIEM lags behind the competition in advanced analytics capabilities and easy integration (e.g., through an app store interface) with third-party technologies, such as EDR, UEBA, and security orchestration and automation tools.
- Out-of-the-box threat intelligence is not provided, but support for Fortinet's FortiGuard threat intelligence platform, as well as integrations with third-party threat feeds, is provided.
- FortiSIEM has limited visibility with Gartner clients procuring SIEM solutions.

IBM

IBM QRadar Security Intelligence Platform is composed of QRadar SIEM at the core, with additional components providing complementary security monitoring and operations capabilities, such as log management (Log Manager), network monitoring (QFlow, Network

Insights and Incident Forensics), vulnerability management (Vulnerability Manager) and risk management (Risk Manager). IBM positions QRadar as an on-premises solution available via a stand-alone or distributed architecture, SIEM as a service (QRadar on Cloud) or as co-managed QRadar in partnership with IBM Managed Security Services. QRadar's on-premises architecture is deployed via physical or virtual appliances (for on-premises or IaaS), software, and hosted cloud. The core components include Event Collectors and Event Processors, QFlow Collectors and Processors, Data Nodes, and Consoles, in addition to the premium components. Advanced threat detection and response capabilities include UEBA functionality (the QRadar UBA App) supported by ML-based analytics (QRadar Machine Learning Analytics app), threat intelligence provided by IBM's X-Force Threat Intelligence feed, QRadar Advisor with Watson app and Resilient Incident Response Platform for incident response and orchestration and automation capabilities. IBM QRadar is licensed primarily by EPS and flows per second (FPS), and premium modules and apps are charged separately.

Over the past 12 months, IBM has introduced a variety of new capabilities, including user behavior analytics (UBA), Machine Learning Analytics app, Advisor with Watson app, Network Insights and platform enhancements around user interfaces and usability features, and data storage compression and optimization. Integrations with partners have been expanded through additions to QRadar App Exchange. IBM Resilient (an incident response tool) is now being offered as a premium service alongside QRadar engagements.

Strengths

- QRadar supports both midsize and large enterprises that require core SIEM capabilities, in addition to those looking for a unified platform that covers a wide range of security monitoring and operational technologies.
- QRadar provides a flexible architecture that can support a variety of environments, including hybrid monitoring options across on-premises and IaaS.
- QRadar App Exchange provides an improved user experience for integrating premium content, content packs and third-party security controls into the QRadar Console and Security Intelligence Platform compared to many competitors.
- Buyers looking to implement advanced analytics and user-based monitoring will benefit from the free UBA and ML apps provided with the core SIEM product.
- QRadar offers a single view across real-time and historic network-based event sources through the correlation of log data, NetFlow, QFlow, deep packet inspection (via Network Insights) and full-packet capture.
- There is widespread availability of managed service support for on-premises QRadar deployments from third parties (and from IBM for large accounts), and QRadar is also available in a hosted SIEM model.

Cautions

- Endpoint monitoring for threat detection and response, or basic file integrity, requires use of third-party technologies. IBM has positioned its BigFix product as a component in this space, especially for security response activities, but there has been very little interest from Gartner clients for this approach.
- Gartner clients that have deployed or are considering QRadar have not expressed much interest in QRadar Advisor with Watson.
- While IBM has introduced its UBA and ML apps, UBA features lag behind the UEBA-centric SIEM vendors. Integrations with several UEBA vendors are supported through QRadar App Exchange.

- IBM Resilient still lacks native integration into the QRadar platform. Integration is available through QRadar App Exchange.
- Customer feedback on the QRadar architecture is generally positive, but for buyers requiring a multicomponent-based architecture, the number of licensable components and options required generates confusion as part of the acquisition and purchase process.

LogRhythm

LogRhythm Threat Lifecycle Management Platform provides core SIEM capabilities, in addition to optional add-ons for network and host monitoring. LogRhythm's SIEM solution consists of several components that can be run from a single appliance or separately as discrete components — Data Collector, Data Processor, Data Indexer, AI Engine, Platform Manager and WebUI Services. System Monitor Agents (available for Windows, Unix and Linux platforms and in two flavors — Pro and Lite) provide FIM functions, but can also act as event forwarders to Data Collectors. Network Monitor provides network and application traffic visibility, as well as selective packet capture for forensic purposes. LogRhythm's SIEM can be deployed in a variety of ways — as software, or as physical or virtual appliances, either as a single appliance solution or for the various discrete components to support a variety of architectural approaches. LogRhythm can be deployed on-premises, in IaaS and in hybrid operating models. Multitenancy for MSSP buyers is also natively supported. LogRhythm SIEM is a velocity-based license approach measured by messages per second (MPS), and licenses are available as perpetual or term. Enterprise license agreements are also available. Physical appliances are available for additional charge. System Monitor is priced per host and Network Monitor is priced per gigabits throughput.

In the past 12 months, LogRhythm has made usability improvements across a variety of functions and features, including case management, workflow and response with the SmartResponse feature, improved user monitoring analytics, delivered enhancements to System Monitor and Network Monitor (including expansion into OT environment monitoring), usability improvements for real-time monitoring, and content updates delivered via AI Engine.

Strengths

- LogRhythm provides a strong platform for organizations that want a contained platform that includes core SIEM capabilities enhanced by complementary host and network monitoring capabilities, in a solution that can scale from a single appliance up to n-tier architectures.
- LogRhythm's out-of-the-box content (and updates delivered to the AI Engine component), along with a powerful user interface, provides a strong real-time monitoring experience for users.
- SmartResponse allows users to integrate preconfigured automated response activities into their alert, investigation and response activities, either fully automated or semiautomated (e.g., manually initiated).
- Organizations considering security monitoring of ICS/SCADA or OT environments, or looking to merge security event monitoring of their IT and OT environments, should consider LogRhythm.
- Gartner clients, particularly midsize and smaller enterprise organizations, report that the simplified deployment model and support by LogRhythm via the Core

Deployment Service is useful. Customers with specific use cases indicate that the Analytics Co-Pilot Service is also useful to speed up implementation times.

Cautions

- LogRhythm lags the UEBA-centric SIEM vendors in ML-driven analytics. The vendor has announced a cloud-based advanced analytics capability called CloudAI, which was released to a limited number of users in early 2017, with general availability targeted for 4Q17.
- There is no application store for easily integrating third-party solutions like several other competing products, and the platform's APIs are less open to third parties to facilitate easier integrations, although LogRhythm has a partner program to facilitate custom integrations.
- LogRhythm supports a limited number of threat intelligence feeds out of the box, although users can add custom STIX/TAXI feeds with the LogRhythm TIS utility, and LogRhythm provides API-based support for other formats. Buyers with third-party threat intelligence feeds should confirm support with LogRhythm.
- A few customers have expressed concerns about LogRhythm's ability to scale to support very high event volume environments. Buyers with those environments should validate LogRhythm's ability to support anticipated event and data volumes.
- Some Gartner clients have raised concerns about the use of Windows as the underlying platform for components in the overall architecture (the Data Indexer is Linux-based), especially around maintaining patch and hotfix currency. Buyers should follow patching best practices and monitor LogRhythm for patch advisories.

ManageEngine

Log360 is the SIEM offering from ManageEngine, a division of Zoho. ManageEngine Log360 is composed of three components — EventLog Analyzer, which provides core SEM and SIM features including event log management, correlation-based analytics, and management/UI for reports, dashboards and log search functionality; ADAudit Plus, which provides real-time monitoring and auditing for AD; and Cloud Security Plus, which manages log event data from public cloud environments. EventLog Analyzer is offered in two versions: Premium is for single instance deployment, and Distributed, which uses a centralized admin server, is for large organizations or MSPs/MSSPs that need to scale horizontally beyond a single EventLog Analyzer instance (e.g., multitenant use cases or a single, geographically distributed organization). ADAudit Plus is offered in two versions — Standard and Professional — depending on the features required. Log360 is only available as a software version, but can be installed into virtual environments. It is licensed by the software components, version, and number of event log and data sources.

Over the past 12 months, ManageEngine has added support for monitoring AWS and Azure public cloud services, enhanced analytics with field-level correlation, improved incident response capabilities and integrations with service desk solutions. It has also added out-of-the-box threat intelligence feeds and improved auditing of AD (e.g., AD Federation Services [ADFS] and AD Lightweight Directory Services [ADLDS]), among other enhancements.

Strengths

- Either ManageEngine Log360 or EventLog Analyzer is a good choice for existing ManageEngine customers looking for an integrated solution, as well as for organizations looking for a simple, cost-effective SIEM solution.

- ManageEngine addresses heavy auditing and compliance capabilities. Over 1,200 predefined reports, including various compliance-focused ones, are available out of the box.
- ADAudit Plus provides stand-alone or integrated monitoring of AD for identity and access governance requirements.
- ManageEngine's architecture and deployment are straightforward and easier to deploy than many SIEM solutions. Log360 includes a wide range of out-of-the-box correlation rules as well as threat intelligence feeds. Organizations primarily using Windows are well-supported with built-in log source identification and integration capabilities.

Cautions

- EventLog Analyzer only provides basic SIEM threat detection functionality. Support is lacking for third-party threat intelligence endpoints and for network-based traffic (e.g., NetFlow).
- Log360 integrates EventLog Analyzer and ADAudit Plus; however, analysts are required to use two different interfaces to perform various activities, such as monitoring for new incidents, investigations and reporting.
- Scalability of the platform may present challenges for larger organizations. Buyers should confirm that event and data volumes, and AD sizes, are supported. Horizontal scaling is supported, but n-tier scalability may be a challenge.
- ManageEngine buyers report difficulty working with remote support staff after purchase.
- ManageEngine has little visibility with Gartner clients for SIEM use cases.

McAfee

McAfee Enterprise Security Manager (ESM) provides core SIEM functionality, including a web-based user interface, a parsed event database, reporting capabilities and central management of other components in the solution. The other components in the solution include Event Receiver (ERC), which provides event and flow collection, and event parsing and normalization; Enterprise Log Manager (ELM), which collects, manages and stores all raw events; Advanced Correlation Engine (ACE), which provides real-time analytics using four types of correlation approaches (rule-based, risk-based, statistical and historical); and Enterprise Log Search (ELS) for log search functionality. Buyers can also purchase the McAfee Database Event Monitor (DEM), which provides real-time discovery and transaction-level database monitoring; Application Data Monitor (ADM), which provides application-level (e.g., Layer 7) decoding and inspection of network traffic; and Global Threat Intelligence (GTI), a threat intelligence feed produced by McAfee Labs. The McAfee SIEM can be deployed as physical or virtual appliances, either as an all-in-one offering (where ESM, ELM and ERC components are on a single appliance) or as individual, discrete components. Physical and virtual appliances can be run together in hybrid-type deployments. The flexible deployment options support n-tier architectures. McAfee's SIEM solution is licensed as a perpetual model, primarily by maximum event volume per appliance as measured in EPS. Physical appliances are an additional charge. McAfee ADM is licensed by bandwidth in gigabytes per second and GTI is licensed per ESM server deployed.

Over the last year, McAfee has primarily focused on transitioning the ESM underlying architecture to a big data-based approach that leverages technologies like Elastic and Kafka, which is supported with the release of a new generation of physical appliances (although

many earlier appliance models support the new architecture too). Additionally, the user experience was also addressed via a new HTML5-based interface that included improved visualizations and workflow capabilities (although the interface is not yet 100% available across the entire solution). Forensics capabilities were improved via the release of ELS.

Strengths

- McAfee's architecture and licensing approach, especially for buyers looking for turnkey appliances (both physical and virtual), simplifies purchases and deployments.
- Customers of other McAfee products, as well as the large set of vendors that are part of the McAfee Security Innovation Alliance, will benefit from native integrations as well as interoperability provided by the Data Exchange Layer (DXL) framework.
- Organizations that require SEM of OT environments (ICS/SCADA) should consider ESM and ADM due to a long history of supporting OT environments (e.g., being able to run as a "one-way diode") and through specific prepackaged content (rules, dashboards and reports).
- Customer satisfaction, with both the product and support, over the past 12 months has improved compared to previous periods.

Cautions

- McAfee lacks advanced, machine-driven analytics capabilities, compared to leading competitors. The planned changes to the platform to run on a big data architecture should enable development of these capabilities.
- McAfee ESM has workflow and case management, but is lacking in automation and orchestration capabilities. Support for many third-party SOA tools is available.
- Customers report ongoing concerns about options for training and education on the ESM platform.

Micro Focus (ArcSight)

In September 2017, Hewlett Packard Enterprise (HPE) and Micro Focus closed a business transaction that resulted in the ArcSight SIEM product becoming part of the Micro Focus business. ArcSight Enterprise Security Manager (ESM) is the core component of ArcSight's SIEM solution. Data collection and management is enabled by ArcSight Data Platform (ADP) using HDFS, Kafka, and Logger and Connectors (both prepacked SmartConnectors and customizable FlexConnectors). The ArcSight Management Center (ArcMC) handles configuration management. ESM provides real-time analytics and monitoring, search, reporting, case management, and workflow. ArcSight ESM Express is available for single, all-in-one system implementations. ArcSight Investigate, built on top of Micro Focus Vertica, is a purpose-built big data and analytics platform that enables data search for incident investigation as well as threat hunting uses. UBA is possible via a repackaged version of Securonix Bolt that provides advanced analytics-based user monitoring capabilities (peer group analysis and ML). DNS Malware Analytics (DMA) is a SaaS-delivered solution that applies advanced analytics that use DNS events to detect malware-infected hosts. DMA will be incorporated into the next release of ArcSight Investigate. 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.

Strengths

- ArcSight has a large installed base of customers using the SIEM product for large, complex SOC environments and for more basic log collection use cases. There is widespread professional services and third-party monitoring support for ArcSight.
- ArcSight supports acquisition and parsing of data from a broad range of sources, connector customization that allows normalization of a broad range of event sources and an open platform that enables structured data to be used outside of the ArcSight solution.
- ArcSight can be extensively customized to support threat management and compliance-focused use cases. ArcSight's robust API enables extensive integrations in SOC environments.

Cautions

- Prior to the acquisition by Micro Focus, ArcSight was updating several elements of its architecture. ArcSight users and prospective customers should seek assurances that Micro Focus will meet commitments for product feature/function improvements and support. Since closing the merger with HPE, Micro Focus has stated that its current plan is to continue investment in ArcSight, leveraging the combined expertise and technology from the legacy companies for the foreseeable future.
- Licensing may be problematic for buyers, with volume-based (for ADP), velocity-based (for ESM) and user-based (for UBA) pricing schemes. Current customers that are converting from legacy licensing models to new licenses and the ADP architecture have reported issues with license conversion complexity and costs. To address these concerns, Micro Focus has implemented changes to its license model that include a pricing option that is free of data restrictions.
- The ArcSight architecture is undergoing changes, with the introduction of ADP, Investigate and other components to support scalable, richer analytics and response, while at the same time supporting legacy functionality. As a result, customer choices regarding the deployment of some elements of the solution can result in duplication of data.

Micro Focus (NetIQ)

NetIQ Sentinel is a SIEM solution from Micro Focus. Sentinel Enterprise is the full SIEM solution that provides SIM and SEM capabilities to support both threat detection- and compliance-oriented use cases. Sentinel for Log Management provides log management, search and reporting capabilities, and can be upgraded to Enterprise. Additional components in the platform include Identity Tracking (a combined solution of Micro Focus Identity Manager and Sentinel with user-monitoring-focused content), Change Guardian (for host-based change and file monitoring), Exploit Detection (a threat and vulnerability management intelligence subscription), Secure Configuration Manager, and Aegis (for enhanced automation to the native Sentinel iTrace workflow). Sentinel can be deployed as software on Linux or as a virtual appliance on VMware, Hyper-V and Xen, and allows for flexible horizontal scaling. Sentinel is licensed based on EPS, event sources and optional components. Multitenant capabilities are natively supported.

Over the past 12 months, Micro Focus introduced Sentinel version 8 that includes an optional big data storage back end built on Cloudera Hadoop and Threat Response Dashboard. Other functional and operational enhancements were also added.

Strengths

- Sentinel Enterprise supports organizations that have large-scale deployment requirements underpinned by core SIEM capabilities, along with native workflow and automation capabilities.
- Tight integration between Micro Focus' IAM, SIEM and IT operations tools provides organizations with a single view into user activity across the IT environment.
- Sentinel's Hadoop-based log management tier provides flexible and horizontally scalable data collection, along with support for third-party solutions that can integrate with data from Hadoop platforms (e.g., UEBA tools).
- Sentinel's architecture is one of the simpler solutions to deploy and manage compared to competing products. Scaling and distribution-only require installation of more Sentinel instances.

Cautions

- The merger of Micro Focus and the software business from HPE resulted in ArcSight SIEM technology becoming part of Micro Focus. Users and prospective buyers should seek assurances from Micro Focus regarding roadmaps. Since closing the merger with HPE, Micro Focus has stated that its current plan is to continue investment in Sentinel and ArcSight, leveraging the combined expertise and technologies from both for the foreseeable future.
- Advanced analytics in Sentinel are lagging compared to competing SIEM solutions. However, support for Hadoop-based event and data management should make integration with stand-alone UEBA solutions easier.
- Support for log and event data collection and monitoring for SaaS, such as Office 365, Salesforce and Box, is lacking.
- Integration of third-party solutions and content is provided, but the lack of an app store experience makes it less user-friendly than competitive products.
- Micro Focus NetIQ Sentinel has low visibility with Gartner clients in competitive evaluations of SIEM platforms.

Rapid7

InsightIDR is Rapid7's SIEM solution that is delivered as a service via the Insight platform. The solution consists of the InsightIDR service, EDR agents and honeypots. InsightIDR provides core SIEM features like log collection and management, threat detection rules and correlations, advanced analytics, dashboards, case management, and workflow and reporting. InsightIDR is built on Rapid7's UserInsight (now InsightUBA) UEBA solution and the acquisition of Logentries. Advanced analytics with a focus on user behavior is a core component of InsightIDR. Buyers deploying the solution will need to install Collectors, available for Windows server or Linux and usually deployed in a ratio of one per location (physical and IaaS), to collect, aggregate and forward logs to the InsightIDR platform. The EDR agents also support local event log forwarding. Scalability is managed by Rapid7. Rapid7's managed detection and response (MDR) service provides 24/7 SEM for buyers that require a service overlay. InsightIDR is licensed by annual subscriptions based on the number of monitored assets, which is any device connected to the buyer's network that generates security data (e.g., desktops, laptops, tablets and servers). Data retention is 90 days, but extended data storage can be added for an additional charge.

Strengths

- InsightIDR is delivered as a service, thus the architecture and implementation is simplified. Ongoing maintenance of the platform (performance management, upgrades, scaling) is not required of the user as it's fully managed by Rapid7.
- Advanced analytics, particularly UEBA, is provided as part of the core solution.
- Monitoring and responding to alerts is supported by the guided investigation feature, making it easier for less experienced users to leverage the solution.
- EDR and honeypot technology are included with the price of the solution, allowing users to leverage advanced threat detection technologies along with InsightIDR.

Cautions

- InsightIDR is relatively new to the SIEM solution market and is less feature-rich compared with more mature SIEM solutions in areas such as reporting and the number of supported log event and data sources (but popular SaaS vendors are natively supported).
- Workflow and case management is basic, and there is a lack of orchestration and response features. Rapid7 acquired an IT operations and security orchestration and automation company, Komand, in July 2017, which could address this gap in the future.
- The as-a-service model may not meet the requirements of all buyers. There is no on-premises version of the solution available to buyers that have concerns about transmitting data and that data being stored off-premises. If network connectivity to Rapid7 is impaired, availability to the solution will be affected.

Securonix

Securonix's SIEM platform is branded as Snypr Security Analytics and runs on top of a Hadoop big data platform. Snypr incorporates an event and data collection and management tier, advanced analytics that include native UEBA functionality as well as a threat library of traditional signatures and rules, and case management and workflow functions. Snypr components include the Console, which provides the UI and configuration functions; Search Service for indexing and searching across all stored data; Enrichment Service for handling data parsing, normalization and event enrichment; Correlation Service for correlation rules; Behavior Science for ML analytics; Risk Scoring Service for threat modeling and indicator-based analytics; Storage Service; Indexing Service; Centralized Ingestion Service; and Ingesters for collecting and forwarding data to the Centralized Ingestion Service. Premium apps include prepackaged behavior models, rules, reports and dashboards across a variety of security monitoring use cases, such as privileged account misuses, data security, cyberthreats, access, application security, cloud security and fraud. Advanced incident investigation and threat hunting requirements are supported by Securonix's Spotter capability. 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. For faster implementations, both physical appliance and hosted as-a-service options are available. Securonix licenses the solution as a term model based on the number of users in an organization for Snypr, premium content apps.

Over the past 12 months, Securonix added improvements around SEM, such as use-case-specific packaged content; enhancements in dashboard features and functionality that help address compliance-, threat- and operational-driven uses; the Securonix Threat Model Exchange for users to share use-case content from a central community-driven location; and the introduction of an as-a-service option.

Strengths

- Securonix Snypr provides both rule-based and UEBA capabilities as part of the core platform.
- The Securonix licensing model is straightforward and easy for buyers to understand.
- Securonix has a large set of partners and supports a wide variety of third-party solutions out of the box, including endpoint protection platforms, data loss prevention, cloud access security brokers, firewalls, healthcare solutions and access management solutions.

Cautions

- Native workflow and case management is relatively basic. More advanced orchestration and automation capabilities are available through API connection. Integrations with third-party solutions, such as ServiceNow, Jira and Remedy service desk solutions, are supported, as well as SOAR solutions like Microsoft-Hexadite and Phantom.
- Since Snypr runs on a commercial Hadoop platform, it introduces a different architecture compared to more traditional SIEM solutions, and may require a learning curve to understand how to manage, monitor and troubleshoot the various components running on the platform (e.g., Kafka, Solr, HBase, Spark, HDFS, etc.)
- Securonix lacks native advanced threat defense solutions, relying on integrations with third-party solutions for those functions (e.g., host and network forensics).

SolarWinds

SolarWinds Log & Event Manager (LEM) provides SEM and SIM functionality delivered as a virtual appliance for VMware and Hyper-V platforms. SolarWinds LEM is composed of Manager, which provides central management of the overall solution as well as log and event management and storage; Console, which provides the user interface; and Agents. The LEM Agents provide real-time event collection from endpoints, handle encryption and compression of data sent to the Manager, and also provide basic DLP (called USB Defender), FIM and automated, active response capabilities. Support for other security monitoring and context sources, such as network traffic, application and virtualized platform monitoring, is available through other SolarWinds solutions such as Virtualization Manager, Network Performance Monitor, and Server & Application Monitor. SolarWinds LEM is licensed per number of event source nodes and includes all components, including Agents and threat intelligence feeds.

Over the past 12 months, SolarWinds added multifactor authentication to the Console, along with feature and functionality upgrades for new device and application event sources. The vendor also improved capabilities for monitoring LEM health through other SolarWinds applications.

Strengths

- SolarWinds LEM provides a well-integrated solution across a variety of IT operation capabilities, making it a good option for SMBs where security operations responsibilities are federated across IT teams and staff.
- LEM supports a variety of event sources, including nonevent data sources that can be integrated into its analytics and correlation rules.

- SolarWinds' simple architecture, easy licensing, and robust out-of-the-box content and features — some found in more complex SIEM solutions — make it a good fit for SMB security operations and compliance use cases.
- The automated response capability based on the endpoint agent for Windows provides some threat containment and quarantine control capabilities not normally found with many competing SIEM solutions.
- SolarWinds has moderate visibility with Gartner clients, particularly midsize and smaller enterprise clients.

Cautions

- SolarWinds LEM is a closed ecosystem, limiting the ability to integrate it with third-party security solutions, particularly advanced threat detection, threat intelligence feeds and UEBA tools. Integrations with service desk tools are also limited to one-way connectivity via email and SNMP.
- LEM's architecture scales horizontally to support thousands of nodes, but it doesn't scale vertically and has an event data storage limit, which the vendor plans to address in a future release.
- Monitoring of SaaS is not supported, and monitoring of IaaS is limited. Buyers that wish to extend monitoring to networks and applications must purchase other SolarWinds solutions to address those requirements.

Splunk

Splunk's Security Intelligence Platform is composed of Splunk Enterprise and two premium solutions, Enterprise Security (ES) and Splunk User Behavior Analytics (UBA). Splunk Enterprise is the core component of the product, providing event and data collection, a variety of analytics capabilities, search, and visualizations. Splunk Enterprise (aka Core Splunk) and Splunk Cloud provide use-case-agnostic data analysis capabilities that are used for various purposes like IT operations, application and network performance monitoring, business intelligence, and some security use cases. The premium ES solution delivers most of the security-monitoring-specific capabilities, including prepackaged security-specific queries, visualizations and dashboards, as well as case management, workflow and incident response capabilities. UBA adds machine-driven, advanced analytics that complement the query-oriented approach of ES. Splunk offers a variety of complementary apps for security use cases, made available through Splunkbase. Example apps include App for PCI Compliance; Stream, which ingests network packet data directly off the wire; Analytics for Hadoop (formerly Hunk), which integrates Splunk with Hadoop environments; and Machine Learning Toolkit for users that want to create their own ML-driven analytics. Splunk supports a variety of deployment options, such as software that can be run on-premises, in IaaS and as a hybrid model. Splunk Cloud is a Splunk-hosted and -operated SaaS solution using AWS infrastructure. Core Splunk and Splunk Cloud components consist of Universal Forwarders, Indexers and Search Heads supporting n-tier architectures, as well as multiple use cases and premium solutions. Splunk is licensed based on the amount of data ingested into the platform, measured in gigabytes per day. 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 a perpetual or term license.

Over the past 12 months, Splunk has primarily delivered a variety of performance and usability enhancements to Core, ES and UBA. Splunk introduced a new open-visualization approach and the Machine Learning Toolkit app that supports user-generated, machine-based

analytics. Support for Okta, Azure AD and ADFS was added. Enhancements were also made to the incident response features in ES (called Adaptive Response), further enabling orchestration and automated response capabilities. Improved integration between ES and UBA events, alerts and identity resolution were also added.

Strengths

- Splunk provides a full suite of solutions oriented toward SEM that allow users to grow into the platform over time (e.g., starting with Core, then adding ES and UBA).
- Advanced analytics capabilities are available through a variety of means across the Splunk ecosystem (e.g., built into the core search capabilities, with Machine Learning Toolkit, prepackaged in UBA or via third-party app providers).
- Splunk has a large partner ecosystem that provides integration and Splunk-specific content that is made available through the Splunkbase application store.
- Many organizations start implementing Splunk for other use cases, easing the path for security teams looking to add a SIEM solution to their environment as the core infrastructure and event log sources are already in place.
- Splunk has significant visibility with Gartner clients, consistently appearing on buyers' shortlists.

Cautions

- Gartner clients that have implemented Splunk consistently raise concerns about the licensing model and overall cost to implement the solution. Splunk has introduced new licensing approaches, such as the Enterprise Adoption Agreement (EAA) as well as additional license headroom for new users with periodic license true-ups, to address these concerns.
- Splunk UBA is visible on shortlists of Splunk users seeking to add UEBA features, but competes with other UEBA solutions, some of which also offer SIEM functionality. Buyers considering using Splunk for SIEM and a third-party solution for UEBA must validate the degree of integration of the solutions and assess the commitment of the respective vendors to continued integration.
- Splunk does not offer an appliance version of the solution. Organizations that want an on-premises appliance version must work with a Splunk partner that provides the integration on supported hardware.

Trustwave

Trustwave's SIEM solution is composed of two versions — SIEM Enterprise and Log Management Enterprise (LME). Both products complement their broader security solution offerings across network, endpoint, and content and data security. Customers consuming SIEM Enterprise as a service leverage the local collector appliance (LCA). The SIEM Enterprise solution is composed of the following components: DA or LCA for event and data collection and normalization; Threat Detection and Threat Evaluation (TD&TE) for real-time analytics and alerting; and the Secure Data Warehouse (SDW) for data storage and historical analysis. SIEM Enterprise, LME and LCA can be deployed as physical or virtual appliances. The architecture can run as an all-in-one solution, and can scale both horizontally and vertically across on-premises and IaaS environments (e.g., a hybrid approach). Trustwave offers a variety of co-managed or hybrid, services augmenting its security management products. Trustwave's licensing is primarily based on appliance costs and velocity of events processed per day (EPD). Services are charged for based on the size of the SIEM environment, and number and types of event sources.

Over the past 12 months, Trustwave has made additions and enhancements to the core platform, primarily around event collection and parsing; connectivity to cloud-based services; added support for deployment in AWS, Azure and CenturyLink; and improved storage capabilities and security.

Strengths

- Trustwave has built integrations across its security product portfolio, making its SIEM a viable option for customers of other Trustwave security products.
- Trustwave offers flexible deployment and service options, including co-management and hybrid deployments, which is a good fit for midmarket organizations and buyers with diverse IT environments (across geographies, on-premises and IaaS).
- SIEM Enterprise has good out-of-the-box support for event and data sources, as well as reports across a variety of regulatory and security frameworks.
- SIEM Enterprise provides core SEM and SIM capabilities that can support both small environments and large organizations and MSSPs requiring multitenant support.
- Midmarket customers can adopt LME and then grow into SIEM Enterprise via a simple license key upgrade.

Cautions

- Trustwave SIEM Enterprise lags the competition in integration with third-party security solutions. The addition of RESTful API support, which Trustwave added this year, should make this easier in the future.
- SIEM Enterprise lacks advanced analytics and user-behavior-based analytics, as well as integration with big data solutions and stand-alone UEBA solutions.
- Threat intelligence feeds are not provided out of the box. Buyers must add on Trustwave SpiderLabs research team feeds as a premium. Native SIEM integration with third-party threat intelligence feeds is not directly supported.
- Trustwave has little visibility in competitive evaluations of SIEM solutions among Gartner clients.

Venustech

The Venustech SIEM solution is composed of various components under the Venusense Unified Security Management (USM) product, which includes modules for Security Analytics (SA), Network Behavior Analysis (NBA), Configuration Verification System (CVS) 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, that enables ML analytics in addition to standard correlation-based detection. The solution can be deployed via software, or as a virtual or physical appliance (the NBA solution is only available as a physical appliance). Venustech also offers a variety of security technologies in addition to its SIEM solution, focused on the Chinese and Asia/Pacific region markets, with solutions that cover firewalls and UTMs, web application firewalls, intrusion detection, vulnerability scanning, VPN, 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 introduced a number of new capabilities and enhancements, including its big data architecture and new UI based on HTML5, support for OT/ICS environments, and a new version of its NBA tool.

Strengths

- Venustech is a good solution for Chinese organizations, both midsize and enterprise-sized, and buyers in the Asia/Pacific markets where Venustech's security solutions are used. Both Chinese and English are supported out of the box.
- Venustech's SIEM solution provides core SEM and SIM functionality that can be expanded to address a variety of network-based monitoring, as well as other security operations and risk management capabilities.
- The Venustech SIEM architecture is straightforward and offers flexible, horizontal scaling.
- Venustech's SIEM solution provides a variety of data management tiers to fit different buyer types (e.g., midsize versus large enterprises).
- Advanced analytics using ML for modeling network-based entity behavior is provided out of the box.

Cautions

- Venustech's SIEM solution lacks the ability to monitor IaaS and SaaS solutions popular outside of the Chinese market, such as AWS, Azure, Office 365, Box and Salesforce. Support is provided for Alibaba Cloud and Tencent Cloud environments.
- Venustech offers three versions of data management to support small- to large-scale deployments. Potential customers must understand the use cases and data volumes they need to support in order to choose the appropriate data management architecture.
- The number of out-of-the-box parsers and report templates, especially regulatory reports outside those needed by Chinese organizations, is fewer than competing SIEM solutions.
- Venustech has little visibility with Gartner clients, including those in the Asia/Pacific region, relative to other competing SIEM solutions.

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

- Exabeam
- FireEye
- Rapid7
- Securonix
- Venustech

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion:

- 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 $15 million for 2016.

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

Source: Gartner (December 2017)

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 evaluations 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 FIM 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 normalizers and parsers for the log formats 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, endpoint and network traffic monitoring, and packet capture capabilities, and integration 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 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	
Market Understanding	
Weighting	High
Marketing Strategy	
Weighting	Medium
Sales Strategy	
Weighting	Medium
Offering (Product) Strategy	
Weighting	High
Business Model	
Weighting	Not Rated
Vertical/Industry Strategy	
Weighting	Medium
Innovation	
Weighting	High
Geographic Strategy	
Weighting	Medium

Source: Gartner (December 2017)

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 — Monitoring, alerting in real time, and longer-term analysis and reporting of trends and behaviors regarding user 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 the relative importance of basic capabilities versus advanced features; budget constraints; the scale of the deployment; complexity of product (deploying, 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 and risk management leaders 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 phased deployments and enhancements beyond the initial use cases. This Magic Quadrant evaluates technology providers with respect to the most common technology selection scenario — a 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 $2.001 billion in 2015 to $2.167 billion in 2016 (see "Forecast: Information Security, Worldwide, 2015-2021, 3Q17 Update"). Threat management is now 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 discussions with Gartner clients are security-focused, and compliance reporting is regarded 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. 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 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 detection of targeted attacks and breaches. Organizations are failing at early breach detection, with more than 80% of breaches undetected by the breached organization. The situation can be improved with threat intelligence, behavior profiling and effective analytics. 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 increases, 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 several new entrants to the Magic Quadrant this year. Exabeam, FireEye, Rapid7, Securonix and Venustech have been added, as these vendors have added support for SIEM functions, and compete for SIEM budget with other vendors in the Magic Quadrant. Venustech is based in China, with aims of expansion into Europe. Exabeam and Securonix have added SIEM functionality to their previously UEBA-focused products, and FireEye has evolved to add SIEM as a service to its advanced threat detection platform. The SIEM market continues to be dominated by relatively few large vendors — Micro Focus (including the ArcSight and Sentinel SIEMs) IBM, McAfee (previously Intel Security) and Splunk — that command more than 60% 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 SIEM vendors continue to focus on targeted attack and breach detection through incorporation of threat intelligence, analytics, profiling and anomaly detection, and endpoint and network activity monitoring.

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, RSA and Trustwave) provide integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (EventTracker, IBM and Trustwave) are marketing co-managed SIEM technology deployments that include a range of monitoring services. Rapid7 and FireEye offer as-a-service SIEM.

Customer's adopting SIEM solutions that have emerged from UEBA vendors need to plan for changes to the way analysts use the tools. The tools primarily emphasize a user-based approach to monitoring for threats, compared to traditional approaches of event-based monitoring oriented around IP addresses and hostnames. SIEM solutions delivered entirely on big data platforms are just emerging in the market and buyers should consider the potential operational impacts and expertise requirements as these platforms are more complex and newer than other SIEM solutions.

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 LogPoint, based in Denmark, 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 a 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.
- Lookwise (developed by S21sec) 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.
- Tango/04, with its Alignia product, 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 "Effective Security Monitoring Requires Context"). 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, and effective analytics, as well as on incident response features.

The ongoing consideration of SIEM technology by companies with limited security resources results in demand for products that are easy to deploy and manage and that provide security monitoring content such as 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 a 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 an iterative approach 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:

- The number of event sources
- The sustained events collected per second
- 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. 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 SIEM"). Motivation to seek external services includes lack of internal resources to manage a SIEM deployment, lack of resources to perform real-time alert monitoring or lack of expertise to expand the deployment to include new use cases (such as 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 includes the maintenance of the platform by the vendor, with customers using their own resources (or other service providers) to configure content and monitor and investigate events. 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. (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 Loggly, 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 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 (also known as the ELK stack or Elastic Stack); Apache Spot; 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 continues to track the development of this approach, and there is some feedback from customers that the workload involved in engineering these solutions to scale and the development effort to support the required event sources and analysis is significant, despite the software itself being free. This may negate the objective of being less expensive than a commercial SIEM deployment .

Organizations that lack the resources and process maturity for SIEM deployment and support, and that 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 (see "Use Central Log Management for Security Event Monitoring Use Cases").

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 a 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 customers gathered through inquiry calls, face-to-face meetings and survey/polling tools; vendor information supplied in response to a survey, product demonstration and briefings; and vendor reference opinions gathered via polling tool.

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.

- Privacy

  |

- Site Index

  |

- IT Glossary

  |

- Contact Gartner