Magic Quadrant for Security Information and Event Management

25 June 2014 ID:G00261641

Analyst(s): Kelly M. Kavanagh, Mark Nicolett, Oliver Rochford

VIEW SUMMARY

Broad adoption of SIEM technology is being driven by the need to detect threats and breaches, as well as by compliance needs. Early breach discovery requires effective user activity, data access and application activity monitoring. Vendors are improving threat intelligence and security analytics.

Market Definition/Description

This document was revised on 1 July 2014. The document you are viewing is the corrected version. For more information, see the on gartner.com.

The security information and event management (SIEM) market is defined by the customer's need to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for incident response, forensics and regulatory compliance. The vendors included in our Magic Quadrant analysis have technologies that have been designed for this purpose, and they actively market and sell these technologies to the security buying center.

SIEM technology aggregates event data produced by security devices, network infrastructures, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as NetFlow and packet capture. Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data is normalized, so that events, data and contextual information from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time security monitoring, historical analysis and other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management

Gartner (June 2014)

Vendor Strengths and Cautions

AccelOps

EVIDENCE

[1] Based on 500 inquiries during 2013 and 2014 from end-user clients with funded SIEM projects

[2] Based on surveys of 24 SIEM vendors

[3] 2013 Data Breach Investigations Report from Verizon Enterprise Solutions

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.

AccelOps is one of the few vendors that have capabilities that are directed at both IT security and IT operations. AccelOps provides log management, search, alerting, real-time correlation, and a dashboard environment for unified security, availability, and performance monitoring and analytics. The vendor's primary focus is its SIEM solution for security practitioners and managed security service providers (MSSPs), but AccelOps also provides a tightly integrated performance and availability monitoring (PAM) solution that is oriented to the IT operations area. MSSP customers typically use both the SIEM and PAM capabilities in order to provide a broad monitoring service to their customers. For end-user customers, the focus in most cases is SIEM, but about 25% of end-user customers have added the PAM component.

Over the past 18 months, the vendor has experienced rapid growth from a relatively small installed base, and is becoming increasingly visible on SIEM evaluation shortlists. Over the past 12 months, AccelOps updates have included integration for dynamically updated external threat intelligence feeds and support for statistical anomaly detection. Development plans include advanced and cloud-based threat visualization analytics.

AccelOps is a good fit for enterprises and MSSPs that require a combination of security monitoring and PAM, and integrated configuration management database (CMDB) capability.

Strengths

- AccelOps' combination of SIEM and PAM capabilities can be used to implement unified security and operations monitoring from log-based event sources, and can provide the security organization with additional operations support for a security-focused deployment.
- AccelOps provides strong support for deployment in a virtualized environment as well as public, private and hybrid clouds.
- Customers report that the technology is relatively easy to deploy, especially given the support for both security and operations monitoring.

Cautions

- Reporting capabilities are very flexible, but some users indicate that ease-of-use improvements in report customization are needed.
- The AccelOps design places a heavy reliance on high-quality CMDB data in order to accurately place each device into an asset category. Organizations must validate the accuracy of the automated discovery and classification activities.
- While AccelOps provide a UI for the simpler integration of unsupported data sources, out-of-the-box support for third-party applications is limited.
- IAM integration is limited to Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP).

AlienVault

The foundation of AlienVault's security management solution is Open Source SIEM (OSSIM), which provides SIEM, vulnerability assessment, NetFlow, network and host intrusion detection, and file integrity monitoring. AlienVault offers SIEM in two products, one open source and one commercial. AlienVault sells and supports Unified Security Management (USM) as software or appliance, and USM extends OSSIM with scaling enhancements, log management, consolidated administration and reporting, and multitenanting for MSSPs. The sensor, logger and server components of USM are available as all-in-one or separate servers in several tiers to match the size of customer environments. The vendor's target market is enterprises with smaller security staffs and limited security programs that need multiple integrated security technologies at a lower cost and with greater simplicity. AlienVault's Open Threat Exchange community enables sharing of Internet Protocol (IP) and URL reputation information. AlienVault Labs provides an integrated threat intelligence feed to its commercial products that includes updates to signature, vulnerability, correlation, reporting and incident response content. AlienVault has added several wizard and dashboard features to support easier deployment, configuration and maintenance of network and host-based sensors and controls. AlienVault's USM platform provides centralized configuration and management of all AlienVault components.

The AlienVault USM platform should be considered by organizations that need a broad set of integrated security capabilities at relatively low cost compared with other commercial offerings, and by organizations that want a commercially supported product that is based on open source.

Strengths

- AlienVault USM provides integrated capabilities for SIEM, file integrity monitoring, vulnerability assessment, NetFlow and both host-based and network-based intrusion detection systems.
- Customer references indicate that the software and appliance offerings are much less expensive than corresponding product sets from most competitors in the SIEM space.

Cautions

- Although AlienVault has recently expanded the number of predefined correlation rules for third-party commercial products, some existing customers identify this as an area that needs further improvement.
- Identity and access management (IAM) integration is limited to Active Directory and LDAP monitoring, and application integration is primarily with open-source applications.
- AlienVault's workflow capabilities do not include integrations with external directories for workflow assignments.

BlackStratus

BlackStratus has two offerings, Log Storm and SIEM Storm. Log Storm provides log management capabilities aimed at MSSPs and small to midsize enterprises, and is available as virtual and hardware appliances. SIEM Storm provides features such as multitenancy and security event management (SEM) capabilities, such as analytics, historical correlation and threat intelligence integration, and is deployable as software or virtual images. SIEM Storm can be deployed in combination with Log Storm, utilizing it as the storage and collection tier, or it can be deployed stand-alone with an HP Vertica Analytics Database back end.

Log Storm and SIEM Storm provide an integrated incident management and ticketing system guided by the SANS seven-step incident remediation process, and SIEM Storm also allows the tracking of SLA metrics to accommodate MSSP and service-centric environments. A Web services API providing two-

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.

way integrations with third-party systems offers powerful integrative capabilities, but out-of-the-box support for third-party data sources is limited compared with competitor offerings.

In the past 12 months, BlackStratus added a co-branded portal, integrations with FireEye, Mandiant and EMC's RSA NetWitness, and support for the Vertica Analytics Database to be used as the back end for SIEM Storm.

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

Strengths

- Log Storm and SIEM Storm provide a two-way integration API to enable custom-built service architectures.
- Both offerings include a fully integrated incident and ticket management system based on the SANS seven-step remediation process.
- SIEM Storm can be deployed with a Vertica Analytics Database back end.

Cautions

- Out-of-the-box support for third-party data sources is limited and requires custom scripting.
- BlackStratus has few technology integration partnerships or deep third-party integrations.
- Advanced security capabilities such as commercial threat intelligence feeds, network forensic/deep packet inspection (DPI) and identity and access management (IAM) integrations are not supported.
- BlackStratus has focused on sales to security service providers, and has not been very visible in competitive evaluations for end-user deployments.

EMC (RSA)

RSA, The Security Division of EMC (including enVision, NetWitness and Security Analytics), has a large SIEM installed base. However, during 2013, RSA completed its transition from enVision and NetWitness to the Security Analytics platform as Gartner customers continued to identify RSA enVision as the most frequently displaced SIEM technology, RSA Security Analytics (based on the NetWitness platform) provides log and full packet data capture, security monitoring forensic investigation, and analytics. RSA will support the enVision platform until the end of 2017. The Security Analytics reporting system can pull data from both the Security Analytics data structures and the Internet Protocol Database (IPDB) in enVision, helping to accommodate the transition from enVision to Security Analytics within the RSA installed base. The Security Analytics Archiver provides long-term storage and access for compressed logs and log metadata. Security Analytics Warehouse provided big data analytics. The initial release of Security Analytics had limitations on analytics (keyword search into raw data), but a 2013 release provided an analytics engine as an integral component of the Security Analytics Warehouse.

The initial release of Security Analytics lacked complex correlation rule support and a customization interface. RSA has released the Event Stream Analysis appliance, which provides real-time alerting for logs and packets, and includes a rule customization interface. In 2013, RSA released the Security Analytics All-in-One appliance that is a packaging option for smaller deployments. Near-term development plans include native incident management and more behavioral profiling capabilities related to outbound connections.

RSA Security Analytics should be considered by organizations with high-security environments and the staffing resources to support a complex technology that requires extensive customization, and that have a need for a combination of both log-based monitoring and network-level monitoring for threat detection and investigation.

Strengths

- RSA's Security Analytics platform offers a combination of analytics and basic event monitoring for both full packet capture and log data.
- RSA Security Analytics can be deployed by organizations that have implemented another vendor's SIEM in cases where full packet capture capabilities are needed

Cautions

- Security Analytics' support for complex correlation is very recent, and it has very little production experience in this area.
- Security Analytics displays are basic. The user interface lacks predefined dashboard views and requires extensive customization.

EventTracker

EventTracker targets its SIEM software and service offering primarily at midsize commercial enterprises and government organizations with security and operations event management and compliance reporting requirements. The EventTracker agent provides support for file integrity monitoring and USB control. Basic profiling capabilities are provided via a behavior module that can establish a baseline of a user-configurable period of time and can issue alerts on deviations from normal. During 2013, the vendor expanded its SIEM Simplified remote monitoring service (incident log and configuration review, incident investigation, and audit assistance) through an integration with OpenVAS vulnerability assessment scanning and Snort intrusion detection. EventTracker also introduced basic incident response workflow support. Development plans include support for monitoring packaged applications that are prevalent in midsize enterprises and a SaaS offering hosted in Amazon Web Services, which will be directed to managed service provider (MSP) partners. EventTracker is suited for midsize businesses that require log management, SEM, compliance reporting and operations monitoring via a software-based solution, and midsize businesses that have a requirement for on-premises or cloud-hosted SIEM in combination with basic monitoring services

Strengths

- EventTracker is easy to deploy and maintain, with compliance and use-case-specific knowledge packs that provide prebuilt alerts, correlation rules and reports.
- EventTracker supports centralized agent deployment and management in Windows environments.
- EventTracker includes a behavior analysis module that provides profiling and anomaly detection functions.

Services such as periodic log review, audit assistance and health check are available from the vendor at a low cost.

Cautions

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

EventTracker's capabilities for application monitoring are more limited than other SIEM products targeting enterprise deployments, as it lacks integration with major packaged applications.

The embedded incident ticketing capability is limited in the area of response workflow.

HP

HP's ArcSight line of SIEM solutions resides within HP's Enterprise Security Products (ESP) business unit, which also includes HP TippingPoint and HP Fortify. ArcSight Enterprise Security Manager (ESM) software is oriented to large-scale, SEM-focused deployments. ArcSight Express is an appliance-based offering for ESM that is designed for the midmarket with preconfigured monitoring and reporting. ArcSight Logger appliances and software provide log data collection and management functions that can be implemented stand-alone or in combination with ESM.

During 2013, ArcSight remained among the most visible SIEM competitors on Gartner client shortlists, but the introduction of competitive SIEM technologies within large ArcSight accounts continued, with customers citing ESM complexity and cost as inhibitors to expansion. With ArcSight ESM version 6, HP replaced the ESM Oracle Database with the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) and implemented a simplified events per second (EPS)-based pricing model. We have validated significant improvements in event-handling capacity on the same hardware with reference customers. In late 2013, HP introduced ArcSight Risk Insight for ESM, which provides risk rating and management dashboards for security event data. HP also introduced ArcSight Application View, which enables application activity monitoring that is not dependent on log data. HP also released enhancements to ArcSight Express to simplify deployment and customization. Development plans include further integrations with HP's Vertica Analytics Platform and additional improvements in ease of deployment.

ArcSight Express should be considered for midsize SIEM deployments. ESM is appropriate for larger deployments, as long as sufficient in-house support resources are available.

Strengths

ESM provides a complete set of SEM capabilities that can be used to support a security operations center.

ArcSight Express provides a simplified option for midsize SIEM deployments.

ArcSight Logger can provide an inexpensive log management capability for two-tier deployment architectures that require long-term event archiving.

Optional modules provide advanced support for user activity monitoring, IAM integration and fraud management.

ArcSight continues to be very visible in competitive evaluations of SIEM technologies.

Cautions

ArcSight provides real-time statistical correlation, but profiling and anomaly detection operate against historical data only.

While the CORR-Engine has eliminated a major source of deployment and support complexity, customers will still find ESM to be more complex than other leading solutions.

IBM Security

IBM Security's QRadar SIEM technology provides log management, event management, reporting and behavioral analysis for networks and applications. QRadar can be deployed as appliance or software (running on Red Hat Enterprise Linux Server appliances) in an all-in-one solution for smaller environments, or it can be horizontally scaled in larger environments using specialized event collection, processing and console appliances. A distinguishing characteristic of the technology is the collection and processing of NetFlow data, DPI, full packet capture, and behavior analysis for all supported event sources.

Enhancements to QRadar during the past 12 months included the introduction of QRadar Incident Forensics, which extends flow analysis, adding DPI and full packet capture capabilities. In addition, IBM Security introduced integrated vulnerability scanning via QRadar Vulnerability Manager (using technology licensed from Critical Watch), as well as new graphing/charting capabilities, improved search performance and API enhancements. IBM has developed two-way integration between QRadar and IBM's InfoSphere BigInsights, and also with IBM's analytics and data visualization technologies. IBM also provides additional connectors to Hadoop instances.

IBM offers a co-managed service option for QRadar, which combines an on-premises QRadar deployment with remote monitoring from IBM's managed security services operations centers. QRadar is a good fit for midsize and large enterprises that need general SIEM capabilities, and also for use cases that require behavior analysis, NetFlow analysis and full packet capture.

Strengths

QRadar provides an integrated view of the threat environment using NetFlow DPI and full packet capture in combination with log data, configuration data and vulnerability data from monitored sources.

Customer feedback indicates that the technology is relatively straightforward to deploy and maintain in both modest and large environments.

QRadar provides behavior analysis capabilities for NetFlow and log events.

Cautions

QRadar provides less-granular role definitions for workflow assignment compared with competitors' products.

QRadar's multitenant support requires a master console in combination with distributed QRadar instances. The number of third-party service providers that offer QRadar-based monitoring services is limited when compared with vendors that lead in this area.

LogRhythm

LogRhythm sells its appliance- and software-based SIEM solutions to midsize and large enterprises. The SIEM offering can be deployed in smaller environments with a single appliance or software instance that provides log management and event management, or it can be scaled as a set of specialized appliances or software instances (log management, event management and centralized console). Network forensic capabilities such as DPI flow monitoring and full packet capture are supported via LogRhythm's Network Monitor, which can be integrated as a network sensor. The technology also includes optional agents for major OSs that can be used for filtering at the source. LogRhythm's System Monitor Agents include host activity monitoring capabilities such as system process monitoring and file integrity monitoring for Windows and Unix.

New features and improvements in the latest 6.2 release of Security Intelligence platform include Active Directory group-based authentication for LogRhythm users, System Monitor Agent and collector load balancing, and a new capability designed to infer missing user information from event data called the Identity Inference Engine. Other enhancements in the past 12 months include a new UI release in 1Q14 that provides tablet support. Moreover, predefined correlation rules have increased to more than 500, and predefined modules containing correlation rules, saved searches and reports covering topics such as privileged user monitoring, network anomaly detection and targeted attack detection have been added. LogRhythm also released Network Monitor in 2013, a network forensic solution that provides flow analysis, deep packet inspection and full packet capture capabilities that can be seamlessly integrated with LogRhythm SIEM as a network sensor.

Plans for the next 12 months include enhancements to case and incident management support, the user interface, and data storage efficiency.

LogRhythm is an especially good fit for organizations that require a combination of SIEM, file integrity monitoring (FIM), and network monitoring, and those organizations that value ease of deployment and predefined function over a "build your own" approach to monitoring.

Strengths

- LogRhythm provides a balance of log management, reporting, event management, privileged-user and file integrity monitoring, and network forensic capabilities to support security operations and compliance use cases.
- Its appliance format and configuration wizards allow for fast deployment with minimal resources.
- Gartner receives consistent user feedback stating that LogRhythm's predefined correlation rules and reporting templates provide coverage for the most useful and important use cases and ease initial implementation.
- LogRhythm continues to be very visible in competitive SIEM technology evaluations of Gartner clients.

Cautions

- Users report that email alert template content can only be minimally customized.
- In order to continue to support older versions of devices, legacy log processing rules are not removed. Feedback has indicated that this can cause confusion among users.

McAfee

McAfee, part of Intel Security, provides McAfee Enterprise Security Manager (ESM), which combines security information management (SIM) and SEM functions, and is available as a stand-alone, all-in-one, virtual appliance and delivered as a managed service by partners. Capabilities can be extended and enhanced with a range of specialized add-on products, such as Database Event Monitor (DEM), which provides database activity monitoring and analysis, Application Data Monitor (ADM) for application monitoring, and Global Threat Intelligence (GTI). McAfee is further developing integration of ESM with its wider security portfolio to enable context about vulnerabilities, endpoint state and threats, and to enable automated response and blocking.

Among the enhancements released in the past 12 months were a new suite of regulatory compliance reports, the capability to use flow data and statistical anomaly tracking in correlation rules, and big data connectors for Hadoop integration. Data obtained via the Hadoop connectors can be used to populate watchlists for correlation and to enrich SIEM data. Plans for the next 12 months include deeper integrations with McAfee's own portfolio to enable autoresponse capabilities such as policy changes on end-user devices, the quarantining and blacklisting of malicious activity, a software development kit (SDK) for external data queries and system management, enhanced threat detection utilizing Data Exchange Layer and Threat Intelligence Exchange, and additional data obfuscation for enhanced compliance in privacy laws.

McAfee Enterprise Security Manager is a good choice for organizations that require high-performance analytics under high-event-rate conditions, as well as organizations with advanced requirements for monitoring database applications and industrial control systems.

Strengths

- Some of the highest event ingest rates and query performance levels that we have been able to validate have been with McAfee Enterprise Security Manager customers.
- Database and application monitoring, as well as network-based packet inspection, are provided for via McAfee Enterprise Security Database Event Monitor and Application Data Monitor.
- McAfee Enterprise Security Manager has strong industrial control system (ICS) and supervisory control and data acquisition (SCADA) device support.

Cautions

- Users have indicated that vendor support is good, but it can be difficult reaching the right point of contact.
- McAfee's advanced SIEM features and capabilities in areas such as endpoint intelligence and automated response require integrations with, or further investments in, other McAfee portfolio products.
- NetFlow filtering and alerting capabilities are limited. For example, there is no easy way to include all the packet data from an event that caused an alert in an email notification.

NetIQ

During 2013, NetIQ focused on completing the consolidation of NetIQ Sentinel (acquired from Novell) with its existing SIEM technology, as well as with its Change Guardian host monitoring. NetIQ's SIEM offering is based primarily on the Sentinel platform, in combination with agent technology and content from Security Manager. NetIQ Sentinel is composed of three packages: Sentinel, Sentinel Log Manager and Change Guardian. Optional host monitoring agents are also available. Sentinel and Change Guardian are offered both as software and virtual appliance deployments. NetIQ Sentinel integrates with other core NetIQ technologies (AppManager, Identity Manager, Access Manager, Directory and Resource Administrator, and Secure Configuration Manager). Enhancements in 2013 included a common administration interface for Sentinel and Security Manager components, initial support for NetFlow analysis, initial support for user import of threat intelligence feeds, and visualizations and point improvements in other areas. Development plans include improvements in scalability, usability and MSSP support.

Sentinel is a good fit for organizations that require large-scale security event processing in highly distributed environments (such as retail). and is an especially good choice for organizations that have deployed NetIQ IAM infrastructure and need security monitoring with an identity context.

Strengths

- Sentinel and Sentinel Log Manager are appropriate for large-scale deployments that are focused on SEM and threat monitoring.
- The Change Guardian product line provides policy-based privileged, user activity monitoring and change detection for Active Directory, Windows, Unix and Linux, as well as file integrity monitoring for host systems.
- NetIQ agent technology can provide guaranteed delivery mechanisms over and above native platform audit functions or agentless methods for use cases that require user and data access monitoring for servers.

Cautions

- NetIQ Sentinel has relatively low visibility in competitive evaluations of security monitoring technology.
- There are no specific integrations with IP reputation or other external threat intelligence feeds, although the vendor indicates the intention to release initial support during 2014.
- Remote monitoring services for Sentinel are provided by a smaller number of third-party service providers when compared with major competitors.
- Sentinel lacks the ability to replay historical event data against current correlation rules for threat detection use cases.

SolarWinds

SolarWinds packages its Log and Event Manager (LEM) software as a virtual appliance. LEM has integrations with SolarWinds' other products for operations monitoring to support activities such as change detection and root cause analysis. SolarWinds' development road map is focused on increasing ease of deployment and ease of ongoing operations for resource-constrained security groups. SolarWinds LEM is a good fit for small or midsize companies that require SIEM technology that is easy to deploy and those that use other SolarWinds' operations monitoring components.

Strengths

- SolarWinds LEM is easy to deploy and provides extensive content in the form of dashboards, predefined correlation rules and reports.
- The technology is also well-suited for organizations that have already invested in the vendor's other technology solutions.
- An agent for Windows systems can be used to exert endpoint control, including USB devices, and network quarantine functions in response to events observed by the SIEM offering.

Cautions

- SolarWinds LEM is optimized for small to midsize deployments, while other SIEM solutions are a better fit for large-scale deployments.
- SolarWinds LEM provides basic statistical and behavior analytics, but has no integration with data warehouse technologies.
- Customers requiring more extensive user and application or Web monitoring must acquire other SolarWinds products to extend the capabilities available in LEM.
- Although LEM includes a native flow capture and display capability, flow data is not available for real-time correlation in LEM.

Splunk

Splunk Enterprise provides log management, search, alerting, real-time correlation and a query language that supports visualization using more than 100 statistical commands. Splunk is widely deployed by IT operations and application support teams for log management analytics, monitoring and advanced search and correlation. Analytics on batch data stored in Hadoop/NoSQL Stores and relational databases is provided by a separate product called Hunk, and the DB Connect App for bidirectional support for relational databases. The Splunk App for Enterprise Security provides predefined reports, dashboards, searches, visualization and real-time monitoring to support security monitoring and compliance reporting use cases. During 2014, the vendor has remained very visible on SIEM evaluation shortlists. In many cases, Splunk has already been deployed by IT operations groups. However, there has also been an expansion in the number of customers deploying the Splunk App for Enterprise Security for stand-alone SIEM use cases.

Over the past 12 months, Splunk has released many new functions directed at a major competitive issue — deployment complexity. Splunk App for Enterprise Security now ships with 68 predefined security indicators that can be used to construct a custom dashboard, and there are now 40 predefined dashboards in the security domain menu. Splunk released a report builder with 200 predefined reports/panels. Splunk now aggregates 18 threat intelligence feeds to enable consolidation into common watchlists.

Development plans include improved threat detection through trending, anomaly detection, expanded use of predictive analytics, and discovery of behavioral outliers for assets and users. Splunk is a good fit for security organizations that require customizable security monitoring and analytics, and is an

especially good fit for use cases that span security and operations, and for deployments with a focus on application monitoring.

Strengths

- Splunk's strong presence in IT operations groups can provide the security organization with early hands-on exposure to its general log management and analytics capabilities, "pre-SIEM" deployment by operations for critical resources, and in-house operations support for an expanded security-focused deployment.
- Splunk's dashboarding and analytics capabilities provide a flexible framework for customization to meet a variety of event management and log management requirements.
- Splunk has built-in support for a large number of external threat intelligence feeds from commercial and open sources.

Cautions

- Splunk provides predefined parsing to a more limited set of IAM vendors than some competitors' products. Potential buyers should anticipate customization work to handle the parsing of IAM logs outside Active Directory, LDAP and selected other IAM technologies.
- Predefined reporting, while improved in the current release, is still more basic than that of many competitors.
- In cases where operations teams are not using Splunk for operations monitoring (to share deployment costs), Splunk is often significantly more expensive than competing SIEM solutions.

Tenable Network Security

Tenable Network Security's focus in this market is evolving to emphasize continuous compliance monitoring based on endpoint state (vulnerabilities, configuration), file activity, network activity and log data. This evolving emphasis is to augment or complement a broad SIEM deployment, although there are overlapping use cases. Tenable Network Security supports SIEM use cases through the SecurityCenter Continuous View (SCCV) console, Nessus, Log Correlation Engine (LCE), and Passive Vulnerability Scanner (PVS) as a capability of its Integrated Vulnerability, Threat and Compliance Platform. LCE provides log and event collection, NetFlow monitoring, normalization, analysis, and reporting. SCCV adds the ability to correlate events with data from Nessus and PVS, in addition to threat list intelligence from third-party providers. Windows and Unix log collection agents can also provide basic file integrity and change monitoring. Tenable's SIEM customers tend to use the vulnerability scanning and configuration assessment capabilities as components of their SIEM deployments.

SCCV, LCE, Nessus and PVS are available as software, and SCCV, Nessus and PVS are also available as hardware or virtual appliances. Network monitoring is available via the NetFlow and raw traffic monitoring capabilities of LCE, or is enhanced through integration with LCE and the passive network traffic monitoring provided by PVS. Recent enhancements include packaged content for specific use cases and policy creation wizards for use cases such as threat management. Development plans include enhanced user activity monitoring and the introduction of support for business application monitoring. The combination of SCCV and LCE for SIEM use cases and scanning and monitoring via PVS and Nessus provides unified management, monitoring, reporting and vulnerability assessment. Tenable's SIEM solution is a good choice for organizations that want to implement continuous monitoring based on the assessment of vulnerabilities, security configuration and log data.

Strengths

- The integration of SCCV, LCE, Nessus and PVS provides a single-vendor solution for customers addressing security and compliance requirements that span event and log analysis, vulnerability assessment, and security configuration auditing.
- SCCV and LCE provide statistical analytics, including notification of first-time events and deviations from baseline activity levels.

Cautions

- LCE does not provide support for co-managed SIEM offerings.
- LCE does not provide integration with IAM policy sources, but the vendor indicates there is current development activity in this area.
- LCE does not integrate with major packaged applications.
- SecurityCenter lacks workflow integration with enterprise directories.
- Organizations that require a broad-scope SIEM implementation should consider alternative solutions.

Tibco Software

Tibco Software's LogLogic Log Management Intelligence line of solutions provides log collection and management capabilities. Tibco also offers additional extensions such as LogLogic Compliance Manager and LogLogic Analytics. LogLogic is available as a line of physical and virtual appliances, as well as software-based options. Tibco is pursuing a general development strategy that will provide its large customers with high-end analytics, and complex-event processing through the integration of LogLogic with the Tibco portfolio. Since Tibco's acquisition of LogLogic in 2012, the solution has been integrated with the wider Tibco portfolio, notably Tibco Spotfire for advanced analytics, Tibco Iris for anomaly detection and forensics, and Tibco Business Events for complex-event processing.

The LogLogic Database Security Manager and Security Event Manager are not offered anymore, with some of the Database Activity Monitoring functionality now integrated with LogLogic Analytics, and event management and functionality divided between Tibco Iris and Tibco Business Events. By itself, LogLogic is designed as an organizationwide logging as a service (LaaS) platform to gather log, event and machine data, with only basic SIEM functionality included. In a threat management use case, it is intended to be used in conjunction with external solutions providing advanced capabilities.

LogLogic is a good fit for use cases focused primarily on log management, providing organizationwide LaaS, or those that involve log management and event forwarding to an MSSP or a third-party event manager. In addition, customers already using or planning to use other Tibco solutions will benefit from the integration with LogLogic.

Strengths

The LogLogic line of log management appliances provides competitive log management capabilities that can be integrated with a wide variety of third-party event managers.

LogLogic offers on-premises log management and reporting for deployments that also use an MSSP for real-time monitoring.

LogLogic, in combination with the greater Tibco portfolio, can provide high-scale advanced analytics, event processing and management, and operational workflow integration.

Cautions

LogLogic lacks advanced security capabilities, such as advanced correlation rules and endpoint protection technology integration, requiring the purchase of other Tibco products that do not have a security-specific focus, or of an additional third-party SIEM technology.

LogLogic does not support threat intelligence integration.

Feedback from some users has indicated that the LogLogic transition and integration with the Tibco portfolio is not fully complete.

LogLogic was not very visible in competitive evaluations, and we have seen more displacements by SIEM vendors during 2013.

Trustwave

Trustwave's primary business is services for compliance, vulnerability assessment, managed security and security consulting. Its threat and research capability includes SpiderLabs, which provides research on security threats and vulnerabilities in support of service delivery and product development. Trustwave also offers a broad portfolio of security products, including secure Web and email gateways, data loss prevention (DLP), a Web application firewall, network access control, unified threat management (UTM), security scanning, and encryption technologies. The core of this portfolio is an SIEM deliverable in several configurations to meet diverse requirements, from large enterprise, SEM-oriented deployments to midsize deployments with more modest SEM needs.

Trustwave SIEM products are provided as hardware or virtual appliance offerings and can be deployed as Log Management Enterprise or full function SIEM Enterprise. Trustwave's legacy SIEM Operations Edition (OE) is deployed as software only with additional optional components such as Advanced Analytics and Enterprise View. The vendor also offers traditional managed security services through its security operations centers running the SIEM OE product, and the Managed SIEM offering that includes customer premises Log Management appliances.

In 2013, Trustwave integrated the Trustwave Threat Correlation threat intelligence service with its SIEM offerings and added out-of-the-box NetFlow collection and analysis capabilities. Trustwave also released its self-healing network offering that leverages its SIEM to integrate with a number of other Trustwave security products to provide security automation and active response functionality.

Trustwave is a good fit for midsize organizations that require a combination of compliance-oriented services and SIEM technology.

Strengths

The Trustwave SIEM products include a broad range of deployment formats and service options, including hybrid options that support customers with limited internal resources for technology management or analysis.

SIEM OE offers analytics, capacity and customization capabilities appropriate for customers with large-scale event monitoring requirements.

Trustwave's self-sealing network offering leverages Trustwave SIEM to provide autoresponse capabilities such as quarantining and blacklisting.

Cautions

The variety of options available to mix and match SIEM with other security products and managed services means that potential SIEM buyers must carefully scope their requirements to enable like-to-like competitive evaluations.

Trustwave SIEM OE users have reported that the custom report wizard can be cumbersome to use, and manual custom report creation requires SQL and XML skills.

SIEM buyers with requirements to incorporate security technologies from Trustwave's competitors (for example, IPS, DLP and Web application firewall technologies) must monitor the vendor's ability to maintain timely support for these technologies with the Trustwave SIEM products and services.

Trustwave is not very visible in competitive evaluations of SIEM among Gartner clients.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope 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

AccelOps

BlackStratus

Dropped

Sensage was acquired by KEYW, which is no longer actively selling an SIEM solution.

Symantec has withdrawn from the SIEM market but will continue support of Symantec Security Information Manager until November 2017.

EiQ Networks is now focusing on providing co-managed solutions that deliver a combination of security controls assessment, configuration auditing and event monitoring.

Inclusion and Exclusion Criteria

The following criteria had to be met for vendors to be included in the 2014 SIEM Magic Quadrant:

The product must provide SIM and SEM capabilities.

The product must support data capture from heterogeneous data sources, including network devices, security devices, security programs and servers.

The vendor must appear on the SIEM product evaluation lists of end-user organizations.

The solution must be delivered to the customer environment as a software- or appliance-based product (not a service).

Vendors were excluded if:

They provide SIEM functions that are oriented primarily to data from their own products.

They position their products as an SIEM offering, but the products do not appear on the competitive shortlists of end-user organizations.

They had less than $13.5 million in SIEM product revenue during 2013.

The solution is delivered exclusively as a managed service.

SIEM is a $1.5 billion market that grew 16% during 2013 — with an expected growth rate of 12.4% during 2014. For exclusion, Gartner considers revenue and relative visibility of vendors in the market. The revenue threshold is $13.5 million per year for 2013 (net new license revenue plus maintenance). Visibility is calculated from the following factors: presence on Gartner client shortlists, presence on vendor-supplied customer reference shortlists, mentions as a competitor by other SIEM vendors and search references on gartner.com.

Evaluation Criteria

Ability to Execute

Product or service evaluates the vendor's ability and track record to provide product functions in areas such as log management, compliance reporting, SEM and deployment simplicity.

Overall viability includes an assessment of the organization's financial health, the financial and practical success of the overall company, and the likelihood that the business unit will continue to invest in the SIEM technology segment.

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 or service within production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed by conducting qualitative interviews of vendor-provided reference customers in combination with feedback 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

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

Source: Gartner (June 2014)

Completeness of Vision

Market understanding evaluates the ability of the technology provider to understand 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 log management, simplified implementation and support, and compliance reporting, while also meeting SEM 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 the vendor's approach to product development and delivery that emphasizes functionality and feature sets as they map to current requirements for SIM and SEM. Development plans during the next 12 to 18 months are also evaluated. Because the SIEM market is mature, there is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and consolidated administration capabilities. In this evaluation, we neutralized the relative ratings of vendors with capabilities in these areas, but there is a severe vision penalty for the few vendors that continue to have shortcomings in this

area. As in last year's SIEM vendor evaluation, we place greater weight on current capabilities that aid in targeted attack detection:

Vendor capabilities and plans for profiling and anomaly detection to complement existing rule-based correlation.

Threat intelligence integration, which includes automated update, filtering, and usage within rules, alerts and reports.

User activity monitoring capabilities, which include monitoring of administrative policy changes and integration with IAM technologies, for automated import of access policy (user context) for use in monitoring.

Data access monitoring capabilities, which include direct monitoring of database logs and integration with database audit and protection products, DLP integration, and file integrity monitoring (native capability and integration with third-party products).

Application layer monitoring capabilities, including integration with third-party applications (for example, ERP financial and HR applications, and industry vertical applications), for the purpose of user activity and transaction monitoring at that layer; the external event source integration interface that is used to define the log format of an organization's in-house-developed applications; and the ability to derive application context from external sources.

Analytics are 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 the SIEM technology, and this is the approach that most SIEM customers will use. 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 "back stores" designed to hold very large amounts of security event, content and contextual data, optimized for analysis. A number of SIEM vendors have also built connectors from the SIEM technology to general purpose big data repositories. Initial deployments of the "separate analytics back store" approach have been implemented by a small number of Type A companies.

Integration with advanced threat detection, network monitoring and packet capture technologies for more effective early breach detection.

Despite the vendor focus on expansion of capability, we continue to heavily weight deployment simplicity. Users still value this attribute over breadth of coverage beyond the core use cases. There is a danger of SIEM products (which are already complex) becoming too complex as vendors extend capabilities. Vendors that are able to provide deployment simplicity as they add function will be the most successful in the market.
We include an evaluation of hybrid or co-managed options, because a growing number of clients are asking about the possibility of limited monitoring services for their SIEM technology deployments.

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

Innovation evaluates the vendor's development and delivery of SIEM technology that is differentiated from the competition in a way that uniquely meets critical customer requirements. Product capabilities and customer use in areas such as application layer monitoring, fraud detection and identity-oriented monitoring are evaluated, in addition to other capabilities that are product-specific and are needed and deployed by customers. There is a strong weighting of capabilities that are needed for security monitoring and targeted attack discovery — user and data access monitoring, application activity monitoring, ad hoc query and analytics, capabilities/plans for profiling and anomaly detection, and threat intelligence. We added an evaluation of technology capabilities/vendor plans for monitoring cloud workloads.

For **geographic strategy,** although the North American and European SIEM markets produce the most revenue, growth rates in Latin America and the Asia/Pacific region are much higher (albeit coming from a much smaller base), driven primarily by threat management and secondarily by compliance requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for those geographies.

Table 2. Completeness of Vision
Evaluation Criteria

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

Source: Gartner (June 2014)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a good 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 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 a large revenue stream (typically because the vendor has 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. Vendors in this quadrant 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 as rich a capability or track record for their SIEM technologies as vendors in the Leaders quadrant.

Visionaries

The Visionaries quadrant is composed of vendors that provide products that are a good 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 smaller vendors that provide SIEM technology that is a good match to a specific SIEM use case, a subset of SIEM market requirements. Niche Players focus on a particular segment of the client base or a more limited product set. Their ability to outperform or innovate may be affected by this narrow focus. 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 the more narrowly focused service spectrum.

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:

- Threat management — Real-time monitoring and reporting of user activity, data access and application activity, in combination with effective ad hoc query capabilities
- Compliance — Log management and compliance reporting
- A deployment that provides a mix of threat management and compliance capabilities

Although many SIEM deployments have been funded to address regulatory compliance reporting requirements, the rise in successful targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection. The SIEM market is composed of technology providers that support all three use cases; however, there are variations in the relative level of capability for each use case — in deployment and support complexity, in the scope of related functions that are also provided, and in product support for capabilities related to targeted attack detection (such as user activity monitoring, data access monitoring, application activity monitoring, the use of threat intelligence and anomaly detection). This year's evaluation continues to more heavily weight capabilities that support targeted attack detection. As a companion to this research, we evaluate the SIEM technologies of 13 vendors with respect to the three major use cases noted above (see "Critical Capabilities for Security Information and Event Management").

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

Security managers considering SIEM deployments should first define the requirements for SEM and reporting. The requirements definition effort should include capabilities that will be needed for subsequent deployment phases. The project will benefit from the input of other groups, including audit/compliance, identity administration, IT operations and application owners (see "How to Deploy SIEM Technology"). Organizations should also describe their network and system deployment topology, and assess event rates, so that prospective SIEM vendors can propose solutions for company-specific deployment scenarios. The requirements definition effort should also include phase deployments beyond the initial use case. This Magic Quadrant evaluates technology providers with respect to the most common technology selection scenario — an SIEM project that is funded to satisfy a combination of threat monitoring/response and compliance-reporting requirements.

Market Overview

During the past year, demand for SIEM technology has remained strong. During this period, the number of Gartner inquiry calls from end-user clients with funded SIEM projects increased by 12% over the previous 12 months, and most vendors have reported increases in customers and revenue. During 2013, the SIEM market grew from $1.34 billion to approximately $1.5 billion, achieving a growth rate of about 16%. The primary drivers that were in place at the start of 2013 remain in effect. Breach detection is the primary driver, and compliance remains a secondary driver. In North America, there continues to be many new deployments by smaller companies that need to improve monitoring and breach detection. Compliance reporting also continues as a requirement, but most discussions are security-focused. There continue to be new deployments by larger companies that are conservative adopters of technology. Both of these customer segments 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 partial, marginal or failed deployments. During this period, we have continued to see a stronger focus on security-driven use cases from new and existing customers. Demand for SIEM technology in Europe and the Asia/Pacific region remains strong, driven by a combination of threat management and compliance requirements. Growth rates in Asia and Latin America are much higher than those in the U.S. and Europe. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for those geographies.

The SIEM market is mature and very competitive. We are in a broad adoption phase, in which multiple vendors can meet the basic log management, compliance and event monitoring requirements of a typical customer. The greatest area of unmet need is effective targeted attack and breach detection. Organizations are failing at early breach detection, with more than 92% of breaches undetected by the breached organization. The situation can be improved with stronger threat intelligence, the addition of behavior profiling and better analytics. Most companies expand their initial SIEM deployments over a three-year period to include more event sources and greater use of real-time monitoring. SIEM vendors have large existing customer bases, and there is an increasing focus on the expansion of SIEM technology deployments within existing accounts. In general, SIEM vendors are continuing to develop product capabilities in areas related to breach detection — threat intelligence, anomaly detection and activity monitoring from the network.

SIEM Vendor Landscape

Fifteen vendors met Gartner's inclusion requirements for the 2014 SIEM Magic Quadrant. Six are point solution vendors, and nine are vendors that sell additional security or operations products and services. There were two notable acquisitions in the SIEM market since the last SIEM Magic Quadrant: KEYW acquired Sensage, and Tibco Software acquired LogLogic. The SIEM market is now dominated by relatively few large vendors — HP, IBM, McAfee, EMC (RSA) and Splunk — that command about 60% of market revenue. Other large vendors such as Tibco are also present. A few small vendors continue to do well, but there will be increasing stress on many of the small remaining vendors. There has been some additional market consolidation over the past 18 months. Symantec announced the end of sale of its SIEM technology as of 2 September 2013, and the end of support as of November 2017. EiQ Networks has shifted its focus away from SIEM technology to security monitoring services and security configuration assessment. KEYW will no longer sell a full-function SIEM product, removing the Sensage technology from the market. Last year, we updated revenue thresholds and requirements for the relative visibility of vendors in the market. The revenue threshold is $13.5 million per year for 2013 (net new license revenue plus maintenance). Visibility is calculated from the following factors: presence on Gartner client shortlists, presence on vendor-supplied customer reference shortlists, mentions as a competitor by other SIEM vendors and search references on gartner.com.

SIEM technology is now deployed by a broad set of enterprises. SIEM vendors are increasingly focused on covering additional use cases, so they can continue to sell additional capabilities to their customer bases. Some SIEM technology purchase decisions do not include a competitive evaluation, because the technology is sold by a large vendor in combination with related security, network or operations management technologies. Many SIEM vendors continue to develop sales channels that can reach the midsize market in North America. Sales effectiveness in Latin America and Asia/Pacific is becoming more important as security spending and SIEM deployments increase in these locations.

SIEM vendors have responded to the customer focus on targeted attack and breach detection by continuing the development of SIEM capabilities in areas such as threat intelligence, analytics, profiling and anomaly detection, and network activity monitoring (both NetFlow analysis and full packet capture). Some vendors (IBM, HP and RSA) are also developing integrations with their own big data technologies, while others (McAfee and Splunk) have described integration plans with third-party technologies. A number of vendors with in-house security research capabilities (IBM, HP, McAfee, RSA and Trustwave) provide an integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (HP, IBM, Trustwave and EventTracker) are marketing co-managed SIEM technology deployments that include varying levels of monitoring services. RSA is executing a strategy to provide a common platform for log management and packet capture, and also to integrate with its IT governance risk and compliance management (GRCM) technology. McAfee's strategy is increasingly focused on technology integration within its own security portfolio and selling SIEM to large enterprises that use its endpoint security products Several vendors are not included in the Magic Quadrant because of a specific vertical market focus and/or SIEM revenue and competitive visibility levels:

- CorreLog is an SIEM vendor that no longer meets our more stringent revenue and visibility thresholds.
- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer.
- Lookwise is an SIEM vendor that was spun out of S21sec and has a market presence primarily in Spain and South America. The distinguishing characteristic of Lookwise is the threat intelligence feeds from S21sec, which are focused on the banking and critical infrastructure sectors. Lookwise does not meet our more stringent revenue and visibility thresholds.
- Tripwire Log Center is focused on augmenting Tripwire capabilities to provide greater system state intelligence.
- Tango/04 provides operational event correlation, business process monitoring and SIEM solutions to customers in Europe and South America. The vendor no longer meets our more stringent revenue and visibility thresholds.
- Tier-3 is an SIEM vendor with a presence primarily in the U.K. and Australia. The distinguishing characteristic of the technology is its profiling and anomaly detection capabilities. The vendor no longer meets our more stringent revenue and visibility thresholds.

A few vendors sell solutions that are based on licensed SIEM technology. IBM licenses its technology to vendors (Juniper Networks and Enterasys Networks) that implement its technology on their own appliances, and add specific integrations with their respective management infrastructures.

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

During the past year, Gartner clients deploying SIEM technology have continued to be primarily focused on security use cases, even though compliance continues to be an important driver. The primary focus continues to be targeted attack and breach detection. The security organization often wants to employ SIEM to improve capabilities for external and internal threat discovery and incident management (see "Using SIEM for Targeted Attack Detection"). As a consequence, there are requirements for user activity and resource access monitoring for host systems and applications (see "Effective Security Monitoring Requires Context"). In this year's SIEM vendor Magic Quadrant evaluation, we continue to place greater weight on capabilities that aid in targeted attack detection, including support for user activity monitoring, application activity monitoring, profiling and anomaly detection, threat intelligence, and effective analytics.

Demand from North American and European clients has remained steady, while the number of Asia/Pacific SIEM inquiries has been rising. Adoption of SIEM technology by a broad set of companies has fostered a demand for products that provide predefined security monitoring and compliance reporting functions, as well as ease of deployment and support. Log management functions have become an expected and standard component of an SIEM technology architecture.

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 with SIEM deployments. For an SIEM technology to meet the requirements for a given deployment, it must be able to collect, process, store and analyze all security-relevant events. Events that need to be monitored in real time have to be collected and processed in real time. Event processing includes parsing, filtering, aggregation, correlation, alerting, display, indexing and writing to the back store. Scalability also includes access to the data for analytics and reporting — even during peak event periods — with ad hoc query response times that do not preclude the use of an iterative approach for incident investigation. Query performance needs to hold up, even as the event store grows over time. We characterize the size of a deployment based on three principal factors:

- The number of event sources
- The sustained events per second (collected after filtering, if any)
- The size of the event back store

We assume a mix of event sources that are dominated by servers but also include firewalls, intrusion detection sensors and network devices. Some deployments also include a large number of PC endpoints, but these are not typical, and PC endpoint counts are not included in our totals. The boundaries for small, midsize and large deployments are not absolute, because some deployments may have a large number of relatively quiet event sources, while others will have a smaller number of very busy event sources. For example, a deployment with several busy log sources may exceed the EPS limits set below for a small deployment, but will still be small architecturally.

Gartner has updated its SIEM deployment size definitions to reflect the increasing scope and scale of security-focused deployments. We define a small deployment as one with 300 or fewer event sources, a sustained EPS rate of 1,500 events per second or less, and a back store sized at 800GB or less. Gartner defines a medium deployment as one with 400 to 800 event sources, a sustained event rate of 2,000 to 7,000 events per second and a back store of 4TB to 8TB. A large deployment is defined as one with more than 900 event sources, a sustained event rate of more than 15,000 events per second, and a back store of 10TB or more. Some very large deployments that have many thousands of event sources, sustained event rates of more than 25,000 EPS and a back store of more than 50TB. We may indicate that a vendor's SIEM technology is ideally suited for a small, midsize or large deployment, which means that the size is a typical or most common successful deployment for that vendor. Every vendor will have outliers.

SIEM Services

Real-time monitoring and alerting, as well as log collection, query and reporting, are available as a service offering from MSSPs. Gartner clients indicate a growing interest in using MSSPs to monitor a customer-deployed SIEM. These services are still relatively new, and MSSPs will evolve service offerings in two ways. We expect lower-cost template offerings, where the MSSP will configure and tune the SIEM system based on a limited number of use cases, with MSSP analysts providing monitoring for selected events and predefined reporting. We also expect custom offerings, where the MSSP will take over (or share with the customer) the monitoring and management of SIEM systems, and where the customer has established extensive alerting and reporting. These more customized services may be delivered with shared resources or with customer-specific resources working remotely or on-site. We do not include an evaluation of the service delivery capabilities of MSSPs in this Magic Quadrant. However, we do note SIEM product vendors that offer remote management or monitoring of their SIEM products. Service providers such as Alert Logic and Sumo Logic offer SIEM infrastructure as a service for organizations that do not want to deploy their own SIEM technology.