Critical Capabilities for Security Information and Event Management

7 May 2013 ID:G00246887

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

VIEW SUMMARY

SIEM technologies vary widely in capabilities that are needed for threat detection and compliance reporting. To avoid deployment failures, evaluate how capabilities match to your requirements.

Overview

Key Findings

The threat management use case is supported by capabilities that enable high-performance event processing, and iterative analysis of event data that includes contextual data and threat intelligence, in combination with profiling/anomaly detection.

Log management and reporting are the primary capabilities for the compliance use case.

Deployment and support simplicity is an important capability for all use cases because of the resource constraints of most IT security organizations.

Recommendations

Those developing SIEM requirements should:

Include stakeholders from IT security, IT operations internal audit and compliance.

Develop a two- to three-year road map for the SIEM deployment to ensure that all functional and scalability requirements are considered with the initial buying decision. This will allow you to evolve the deployment as change occurs with threats, information technology and business requirements.

Select a technology whose deployment and support requirements are a good match to the IT organization's project and support capabilities. Organizations may also need to consider services to cover project and operational capability gaps.

What You Need to Know

Organizations evaluating security information and event management (SIEM) tools should begin with a requirements definition effort that includes IT security, IT operations internal audit and compliance. Organizations must determine deployment scale, real-time monitoring, and postcapture analytics and compliance reporting requirements. In addition, organizations should identify products whose deployment and support requirements are good matches to internal project and support capabilities. Gartner recommends developing a set of requirements that resolve the initial problem; however, there should also be some planning for the broader implementation of SIEM capabilities in subsequent project phases. Developing a two- to three-year road map for all functions will ensure that the buying decision considers longer-term functional and scaling requirements. Be ready to evolve the plan in response to changes in IT, business requirements and threats.

Return to Top

Analysis

Introduction

SIEM technology is an important element of an organization's security strategy, because it establishes a consolidation point for all forms of security monitoring and can be used to detect a targeted attack in its early phases to minimize damage. SIEM tools provide user activity and data access monitoring and reporting for threat detection, and to satisfy audit requirements. Many Gartner clients need to implement SIEM technology to satisfy regulatory requirements — for example, log management for the Payment Card Industry (PCI) or privileged user reporting for Sarbanes-Oxley (SOX). IT security organizations generally recognize that these compliance-funded projects are opportunities to improve security monitoring and incident response.[1] This research will help IT security organizations define their requirements and select technology.

Return to Top

Product Class Definition

SIEM technology supports threat management and security incident response through the collection and analysis of security events from a wide variety of event and contextual data sources in real time. It also supports incident investigation and security policy compliance monitoring

EVIDENCE

[1] Based on 375 inquiries during 2012 from end-user clients with funded SIEM projects.

[2] Based on surveys of 24 SIEM vendors.

CRITICAL CAPABILITIES METHODOLOGY

"Critical capabilities" are attributes that differentiate products in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

This methodology requires analysts to identify the critical capabilities for a class of products. Each capability is then weighted in terms of its relative importance overall, as well as for specific product use cases. Next, products are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities overall, and for each use case, is then calculated for each product.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor: most or all defined requirements not achieved

2 = Fair: some requirements not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

Product viability is distinct from the critical capability scores for each product. It is our assessment of the vendor's strategy and its ability to enhance and support a product over its expected life cycle; it is not an evaluation of the vendor as a whole. Four major areas are considered: strategy, support, execution and investment. Strategy includes how a vendor's strategy for a particular product fits in relation to its other product lines, its market direction and its business overall. Support includes the quality of technical and account support as well as customer experiences for that product. Execution considers a vendor's structure and processes for sales, marketing, pricing and deal management. Investment considers the vendor's financial health and the likelihood of the individual business unit responsible for a product to continue investing in it. Each product is rated on a five-point scale from poor to outstanding for each of these four areas, and it is then assigned an overall product viability rating.

The critical capabilities Gartner has selected do not represent all capabilities for any product and, therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making an acquisition decision.

through the analysis of and reporting on historical data from these sources. The core capabilities of SIEM technology are the broad scope of event collection and the ability to correlate and analyze events across disparate information sources. The technology is typically deployed to:

- Discover external and internal threats
- Monitor the activities of privileged users
- Monitor server and database resource access
- Monitor, correlate and analyze user activity across multiple systems and applications
- Provide compliance reporting
- Provide analytics and workflow to support incident response

SIEM technology aggregates and analyzes the event data produced by devices, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data to obtain network context about users, IT assets, data, applications, threats and vulnerabilities. The data is normalized, so that events from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring and user activity monitoring for the early detection of breaches or misuse.

Return to Top

Critical Capabilities Definition

SIEM technology provides a set of common core capabilities that are needed for all cases. Other SIEM capabilities are more critical for the threat management use case or the compliance use case. Many organizations will apply SIEM technology broadly across their IT infrastructures and will implement most SIEM capabilities, but they typically start with a narrow deployment that implements a subset of functions to resolve a specific compliance gap or security issue.

Organizations should evaluate the following set of SIEM capabilities:

Scalable architecture and deployment flexibility: These are derived from vendor design decisions in the areas of product architecture, data collection techniques, agent designs and coding practices. Scalability can be achieved by:

- A hierarchy of SIEM servers — tiers of systems that aggregate, correlate and store data
- Segmented server functions — specialized servers for collection correlation, storage, reporting and display
- A combination of hierarchy and segmentation to support horizontal scaling

During the planning phase, many organizations underestimate the volume of event data that will be collected, as well as the scope of analysis reporting that will be required. An architecture that supports scalability and deployment flexibility will enable an organization to adapt its deployment in the face of unexpected event volume and analysis.

Real-time event data collection: SIEM products collect event data in near real time in a way that enables immediate analysis. Data collection methods include:

- Receipt of a syslog data stream from the monitored event source
- Agents installed directly on the monitored event source or at an aggregation point, such as a syslog server
- Invocation of the monitored system's command line interface
- APIs provided by the monitored event source
- External collectors provided by the SIEM tool

Note: The technology should also support batch data collection for cases where real-time collection is not practical or is not needed.
Filtering options at the source also are important methods of data reduction, especially for distributed deployments with network bandwidth constraints. Agent-based collection options and virtualized SIEM infrastructure options will become more important as organizations move workloads to virtualized and public infrastructure as a service cloud environments. A growing number of organizations that have deployed SIEM technology must integrate data sources that aren't formally supported by the SIEM vendors. SIEM products should provide APIs or other functions to support user integration of additional data sources. This capability becomes more important as organizations apply SIEM technology for application-layer monitoring.

Event normalization and taxonomy: This is a mapping of information from heterogeneous sources to a common event classification scheme. A taxonomy aids in pattern recognition, and also improves the scope and stability of correlation rules. When events from heterogeneous sources are normalized, they can be analyzed by a smaller number of correlation rules, which reduces deployment and support labor. In addition, normalized events are easier to work with when developing reports and dashboards.

Real-time monitoring: Event correlation establishes relationships among messages or events that are generated by devices, systems or applications, based on characteristics such as the source, target, protocol or event type. There should also be a library of predefined correlation rules and the ability to easily customize those rules. A security event console should provide the real-time presentation of security incidents and events.

Behavior profiling: Behavior profiling employs a learning phase that builds profiles of normal activity for various event categories, such as network flows, user activity, server access, and so on. The monitoring phase alerts on deviations from normal. Profiling and anomaly detection are emerging capabilities in SIEM that complement rule-based correlation.

Threat intelligence: Intelligence about the current threat environment exists in a variety of sources, including open-source lists, the threat and reputation content developed and maintained by security research teams within security vendors, and data developed by managed security and other service providers. Threat intelligence data can be integrated with an SIEM in the form of watch lists, correlation rules and queries in ways that increase the

success rate of early breach detection.

Log management and compliance reporting: Functions supporting the cost-effective storage and analysis of a large information store include collection, indexing and storage of all log and event data from every source, as well as the capability to search and report on that data. Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools.

Analytics: Security event analytics is composed of dashboard views, reports and ad hoc query functions to support the investigation of user activity and resource access in order to identify a threat, a breach or the misuse of access rights.

Incident management support: Specialized incident management and workflow support should be embedded in the SIEM product primarily to support the IT security organization. Products should provide integration with enterprise workflow systems, and should support ad hoc queries for incident investigation.

User activity and data access monitoring: This capability establishes user and data context, and enables data access and activity monitoring. Functions include integration with identity and access management (IAM) infrastructure to obtain user context and the inclusion of user context in correlation, analytics and reporting. Data access monitoring includes monitoring of database management systems (DBMSs), and integration with file integrity monitoring (FIM) and data loss prevention (DLP) functions. DBMS monitoring can take three forms — parsing of DBMS audit logs, integration with third-party database activity monitoring (DAM) functions or embedded DAM functions. FIM can be provided by the SIEM product directly or through integration with third-party products.

Application monitoring: The ability to parse activity streams from packaged applications enables application-layer monitoring for those components, and the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house-developed applications. Integration with packaged applications, an interface that allows customers to define log formats of unsupported event sources, and the inclusion of application and user context are important capabilities that enable the monitoring of application activities for application-layer attack detection, fraud detection and compliance reporting.

Deployment and support simplicity: Deployment and support simplicity is achieved through a combination of embedded SIEM use-case knowledge, and a general design that minimizes deployment and support tasks. Embedded knowledge is delivered with predefined dashboard views, reports for specific monitoring tasks and regulatory requirements, a library of correlation rules for common monitoring scenarios, and event filters for common sources. There should also be an easy way to modify the predefined functions to meet the particular needs of an organization.

Return to Top

Use Cases

Although the majority of SIEM projects have historically been funded to resolve compliance issues, most organizations also know that they need to improve security monitoring and incident response. IT security organizations evaluate and deploy SIEM tools for three primary use cases:

Threat management: The IT security organization has obtained funding for an SIEM deployment by making the case for improved threat management, breach detection and incident response capabilities. There's higher weighting to real-time event management and correlation, threat intelligence, anomaly detection, and support for high-performance and large-scale historical data analysis.

Compliance: The SIEM technology deployment is tactical, focused on log management, specific compliance reporting requirements, and a subset of servers that is material to the regulation. Log management is weighted heavily, because it provides the basic "check box" that a superficial audit would require. User and resource access reporting is important because SIEM technology is commonly deployed as a compensating control for weaknesses in user or resource access management. The implementation time frame is typically short, so simplicity and ease of deployment are valued over advanced functions and the capability to customize heavily.

General SIEM deployment: In this use case, there is a need to improve breach detection and incident response capabilities, and also a need for reporting to close compliance gaps. The SIEM technology must support rapid deployment for compliance reporting, and provide for subsequent deployment steps that implement security event management (SEM) capabilities.

Return to Top

Critical Capabilities

Of the 12 capabilities previously defined, eight of these are critical capabilities that differentiate vendor offerings for the three use cases (see Figure 1):

Real-time monitoring: This is important for threat management (to track and analyze the progression of an attack across components and systems) and for user activity monitoring (to track and analyze the activity of a user across applications, or to track and analyze a series of related transactions or data access events).

Data and user monitoring: User and data activity monitoring that includes user and data context is needed for breach and misuse discovery. Privileged user and sensitive data access monitoring is also a common requirement for compliance reporting.

Application monitoring: This is critical because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity.

Threat intelligence: Up-to-date information on threats and attack patterns can help an organization recognize abnormal activity. For example, a small amount of outbound activity to an external IP address might look normal and would be easily overlooked. Everything changes

if there is threat intelligence that indicates that the destination is associated with a botnet command and control center .

Behavior profiling: When abnormal conditions are well-defined, it's possible to define correlation rules that look for a specific set of conditions. It is very difficult to cover all the conditions that are abnormal with a rule-based approach. Anomaly detection can complement rule-based approaches, because it alerts organizations to deviations from normal. Profiling and anomaly detection are emerging capabilities in SIEM that complement rule-based correlation.

Analytics: When suspect activity is surfaced by security monitoring or activity reporting, it is important to be able to analyze user and resource access in using an iterative approach to start with a broad query about an event source, user or target, and to then initiate increasingly focused queries to identify the source of the problem.

Log management and reporting: Log management has become part of the standard of due care for many regulations. Compliance-oriented deployments are simplified when the SIEM technology includes predefined and modifiable reports for user activity, resource access and model reports for specific regulations.

Deployment and support simplicity: Compliance and security requirements have extended the SIEM market to organizations that have smaller security staffs and more-limited system support capabilities. For these buyers, predefined functions and ease of deployment and support are valued over advanced functionality and extensive customization.

Figure 1. Weighting for Critical Capabilities in Use Cases

Critical Product Capabilities	Overall	Compliance	Threat Management	SIEM
Real-Time Monitoring	12.5%	2.0%	18.0%	15.0%
Threat Intelligence	12.5%	2.0%	9.0%	10.0%
Behavior Profiling	12.5%	2.0%	10.0%	7.0%
Data and User Monitoring	12.5%	10.0%	10.0%	8.0%
Application Monitoring	12.5%	2.0%	10.0%	6.0%
Analytics	12.5%	2.0%	23.0%	8.0%
Log Management and Reporting	12.5%	55.0%	10.0%	26.0%
Deployment and Support Simplicity	12.5%	25.0%	10.0%	20.0%
Total	100.0%	100.0%	100.0%	100.0%

Source: Gartner (May2013)

Inclusion Criteria

In this research, we've included software products for evaluation, based on the following criteria:

The products must cover the core SIEM functions.

The products must have been in general availability and deployed in customer environments as of March 2013.

The products must target the SIEM market segment and the security buying center.

Gartner must have determined that the participants are the largest players in the market, based on Gartner estimates of the SIEM customer base size and SIEM revenue.[2]

Return to Top

Critical Capabilities Rating

Each of the products has been evaluated on the critical capabilities on a scale of 1 to 5. A score of 1 indicates a low level of capability, while a rating of 5 indicates a high level of capability (see Figure 2).

Figure 2. Product Rating on Critical Capabilities

Product Rating	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Real-Time Monitoring	2.80	3.2	2.8	4.1	3.9	3.53	3.55	3.90	2.6	3.03	3.0	3.40	2.85
Threat Intelligence	3.30	3.0	4.0	4.0	4.0	3.00	4.00	1.00	3.5	1.00	3.5	4.70	1.00
Behavior Profiling	3.50	3.3	3.0	3.8	4.5	3.50	3.25	3.50	3.3	2.00	3.3	2.00	3.40
Data and User Monitoring	2.60	3.0	3.2	4.2	3.5	3.58	3.54	3.08	3.6	3.06	3.1	2.92	2.79
Application Monitoring	3.17	3.0	3.3	4.1	3.5	3.58	3.83	2.40	3.7	3.00	3.7	3.08	2.42
Analytics	3.28	2.9	3.5	3.7	3.9	3.00	3.70	2.69	3.7	2.25	3.7	3.00	2.87
Log Management and Reporting	3.04	3.3	2.9	3.8	3.5	3.62	3.68	3.31	3.5	3.29	3.4	3.48	4.00
Deployment and Support Simplicity	3.53	3.2	2.5	3.3	4.0	4.00	3.50	3.80	2.3	5.00	2.9	3.00	3.85

Enlarge

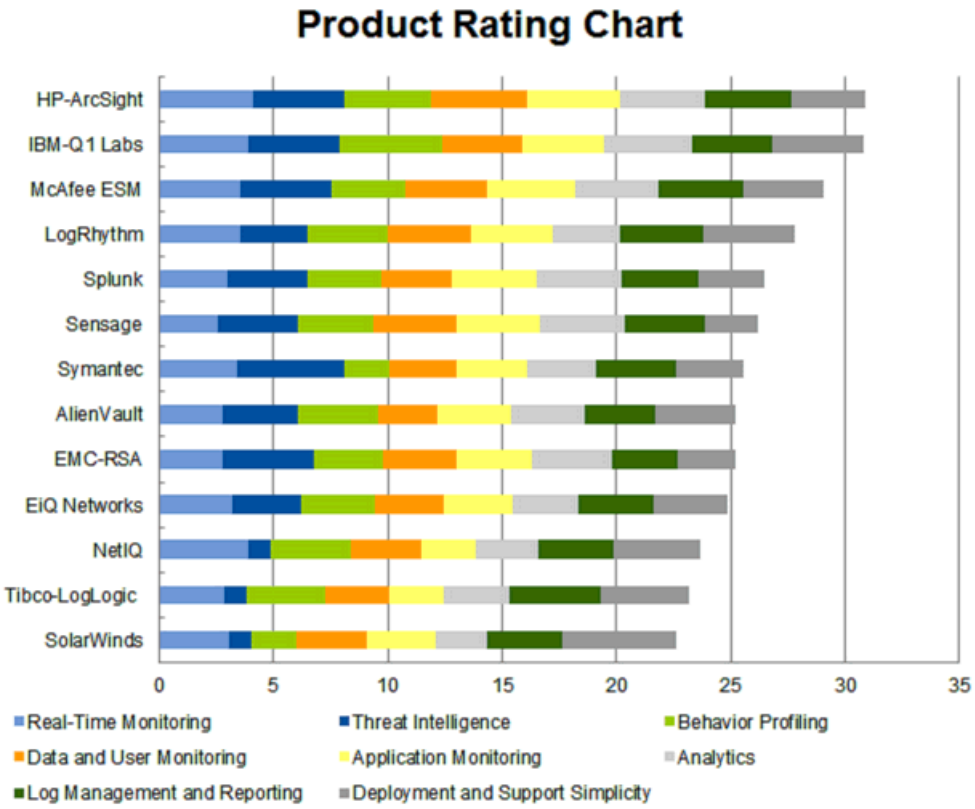
As of May 2013

Source: Gartner (May2013)

Return to Top

To determine an overall score for each product in the use cases, the ratings in Figure 2 are multiplied by the weightings shown in Figure 1. These scores are shown in Figure 3, which also provides our assessment of the viability of each product.

Figure 3. Overall Score for Each Vendor's Product Based on the Nonweighted Score for Each Critical Capability



As of May 2013

Source: Gartner (May2013)

Return to Top

Figure 4 shows the product scores for each use case.

Figure 4. Product Score in Use Cases

Use Cases	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Overall	3.2	3.1	3.1	3.9	3.9	3.5	3.6	3.0	3.3	2.8	3.3	3.2	2.9
Compliance	3.1	3.2	2.9	3.7	3.7	3.7	3.6	3.3	3.2	3.6	3.2	3.3	3.7
Threat Management	3.1	3.1	3.2	3.9	3.9	3.4	3.6	3.0	3.3	2.8	3.3	3.2	2.9
SIEM	3.2	3.2	3.0	3.8	3.8	3.6	3.6	3.2	3.1	3.2	3.3	3.3	3.2

Enlarge

As of May 2013

Source: Gartner (May2013)

Return to Top

Product viability is distinct from the critical capability scores for each product. It is our assessment of the vendor's strategy and the vendor's ability to enhance and support a product throughout its expected life cycle; it is not an evaluation of the vendor as a whole. Four major areas are considered: strategy, support, execution and investment. Strategy includes how a vendor's strategy for a particular product fits in relation to the vendor's other product lines, its market direction and its business overall. Support includes the quality of technical and account support, as well as customer experiences with that product. Execution considers a vendor's structure and processes for sales, marketing, pricing and deal management. Investment considers the vendor's financial health and the likelihood of the individual business unit responsible for a product to continue investing in it. Each product is rated on a five-point scale from poor to outstanding for each of these four areas, and it is then assigned an overall product viability rating (see Figure 5).

Figure 5. Product Viability Rating

Vendor/ Product Name	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Product Viability	Good	Good	Good	Excellent	Excellent	Good	Excellent	Good	Good	Good	Good	Fair	Good

Enlarge

As of May 2013

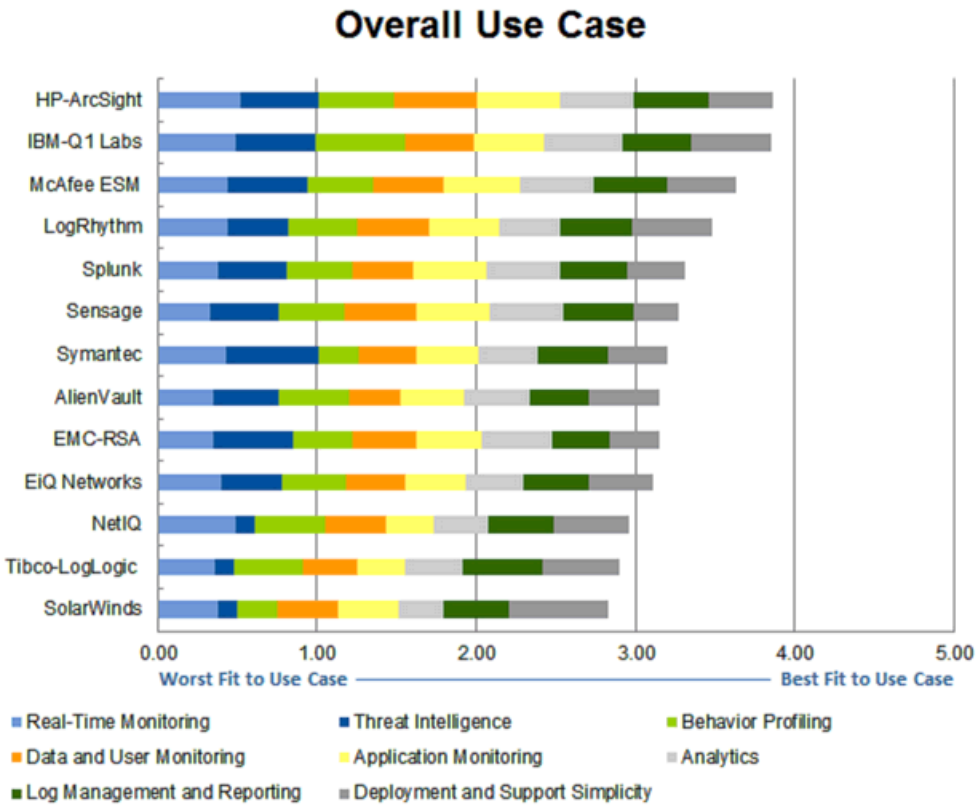
Source: Gartner (May2013)

Return to Top

The weighted capabilities scores for all use cases are displayed as components of the overall score.

The overall use case is in Figure 6. See Figures 7, 8 and 9 for the vendor scores for specific use cases.

Figure 6. Vendors' Product Scores for the Overall Use Case

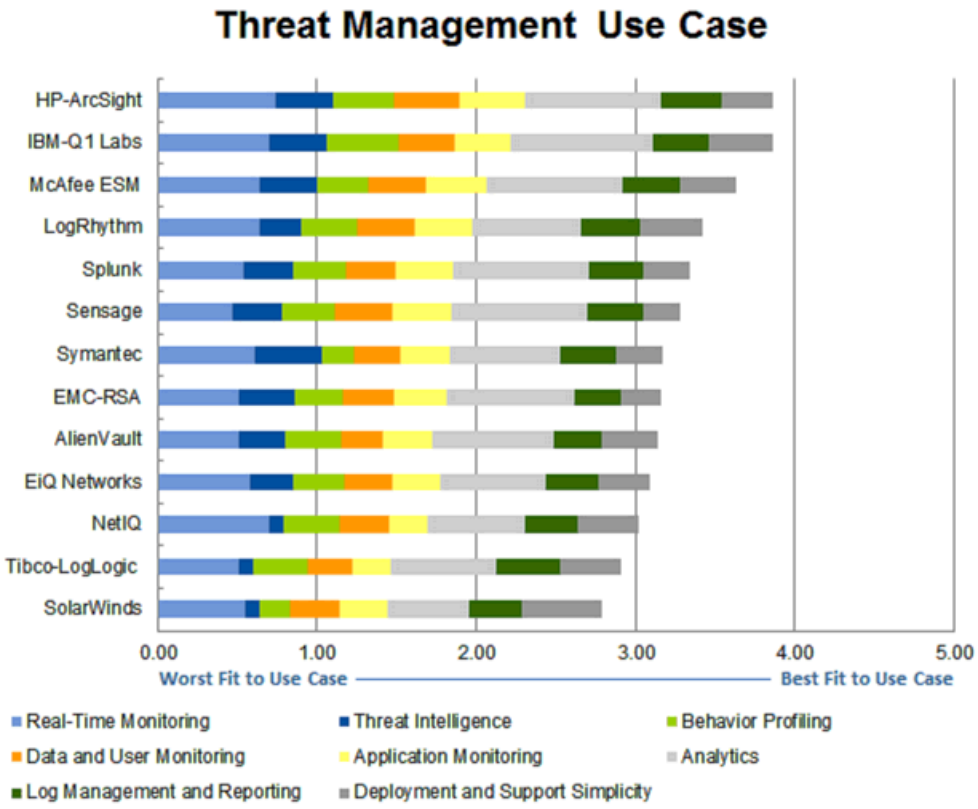


As of May 2013

Source: Gartner (May2013)

Return to Top

Figure 7. Vendors' Product Scores for the Threat Management Use Case

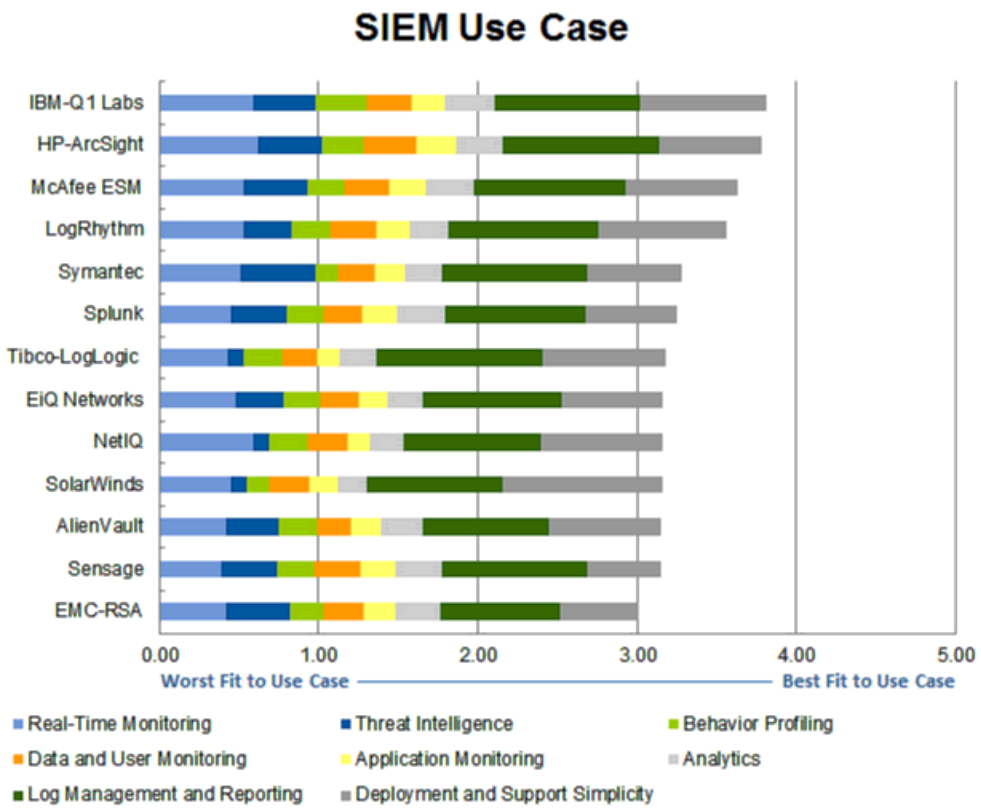


As of May 2013
The weighted capabilities scores for all use cases are displayed as components of the overall score.

Source: Gartner (May2013)

Return to Top

Figure 8. Vendors' Product Scores for the SIEM Use Case

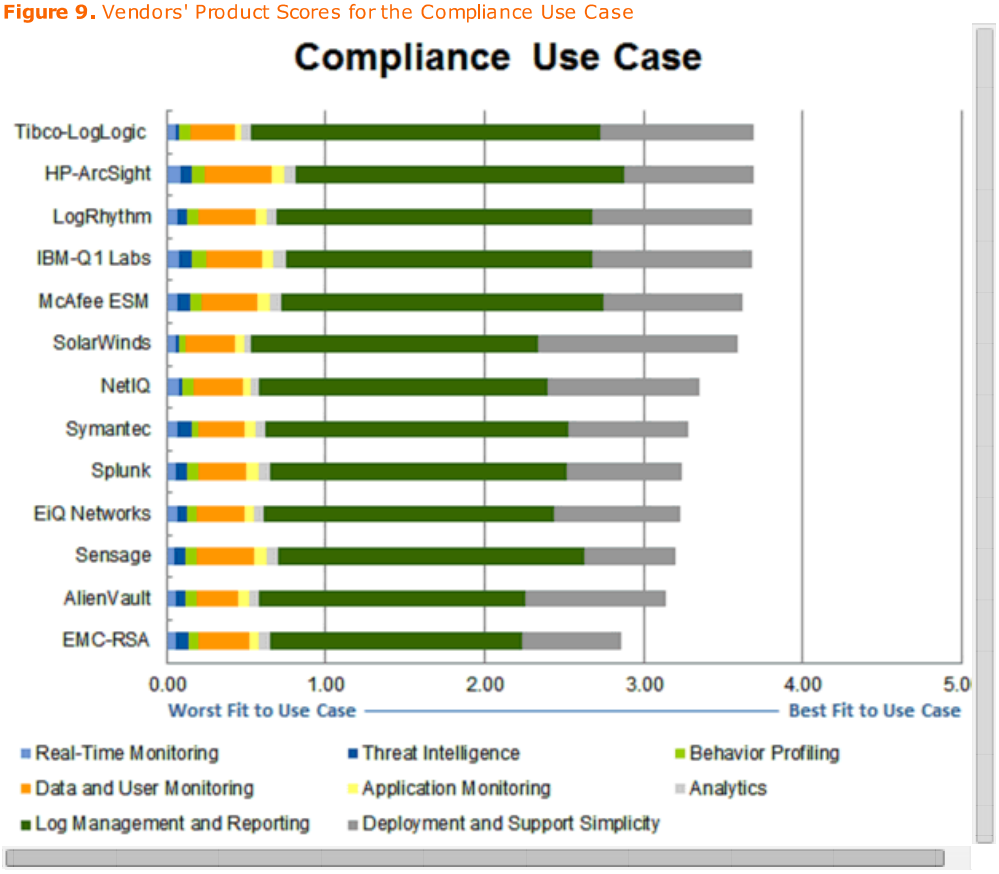


As of May 2013
The weighted capabilities scores for all use cases are displayed as components of the overall score.

Source: Gartner (May2013)

Return to Top

Figure 9. Vendors' Product Scores for the Compliance Use Case



As of May 2013
The weighted capabilities scores for all use cases are displayed as components of the overall score.

Source: Gartner (May2013)

Return to Top

Vendors

AlienVault

AlienVault's security management software and appliance offerings provide SIEM, vulnerability assessment, network and host intrusion detection, and file integrity monitoring. The commercial offerings extend the Open Source SIM (OSSIM) foundation with scaling enhancements, log management, consolidated administration and reporting, and multitenanting for managed security service providers (MSSPs). AlienVault packages its offering, the AlienVault Unified Security Management platform, into three tiers to match the size of the end-user's environment. In every offering provided by AlienVault, all features are enabled.

Real-time monitoring: The AlienVault Correlation Engine provides real-time monitoring and correlation. Predefined correlation rules for third-party intrusion detection system (IDS) and intrusion prevention system (IPS) sources are very limited, and are focused primarily on the suite's snort sensor data.

Threat intelligence: AlienVault Labs provides threat intelligence content on a subscription basis. The company also hosts and supports Open Threat Exchange, which enables sharing of IP and URL reputation information.

Behavior profiling: Statistical analysis can be applied to about 50 parameters. This capability complements rule-based correlation.

Data and user monitoring: The AlienVault identity management (IdM) component is included as part of the suite, and it enables integrated monitoring with identity context. There is no integration with commercial identity and access management (IAM) systems, beyond basic Active Directory monitoring. Local account changes can be monitored if AlienVault's host-based intrusion detection (HIDS) agent is installed. There is no productized integration with third-party FIM and data loss prevention (DLP) products, but the HIDS agent provides FIM and some basic and limited DLP functions. Database activity monitoring (DAM) is supported through direct monitoring of major DBMS logs. The Nagios component provides database activity monitoring that requires native audit functions enabled, and there is an integration with Imperva.

Application monitoring: There is integration with major Web application firewall and Web server technologies. Application integration is limited to open-source applications.

Analytics: Search and structured analysis are provided from the alert investigation panel (the primary console) and the raw event panel, and operate against the primary event data store.

Log management and reporting: Log management capability is provided as a function of the logger component. Reporting is provided via an interface from the SIEM server, and customers indicate that the report customization interface is easy to use.

Deployment and support simplicity: AlienVault has been working to simplify deployment and support. Recent improvements include AlienVault Center, which provides centralized configuration and management of all AlienVault components. There is also an Auto-Deploy Dashboard, which leverages asset discovery capabilities to guide log integration.

Use cases: The AlienVault Unified SIEM solution should be considered by organizations that need a broad set of integrated security capabilities, and by organizations that want a commercially supported product that is based on open source.

Return to Top

EiQ Networks

EiQ Networks' SecureVue provides SEM, SIM, security configuration policy compliance, FIM, operational performance monitoring functions and network behavior analysis capabilities. SecureVue's architecture includes a hierarchy of server and collector components, with a minimal deployment consisting of a global central server and a data collector. Additional tiers of optional servers (regional, local and data processing) and optional agents can be added to scale deployments. The server components and collectors are available as software images or appliances; agents are software only. EiQ Networks also provides SIEM technology packaged and configured for small and midsize business (SMB) and midmarket customers, called SecureVue NGS, which is available as software or an appliance.

Real-time monitoring: SecureVue functions can be horizontally scaled for large deployments.

Threat intelligence: SecureVue can integrate with threat intelligence data from Cisco and Symantec. Data from these sources can be updated in user-defined intervals.

Behavior profiling: The company has recently introduced behavior profiling capabilities, and enhancements are planned.

Data and user monitoring: SecureVue has predefined integration with Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) directories. Integration with IAM technologies from CA, IBM, Oracle, Novell, and RSA, The Security Division of EMC (EMC-RSA) is also supported. SecureVue integrates with the major DLP and DAP products. An optional host agent provides FIM, but there is no integration with third-party FIM tools

Application monitoring: Integration with Web application servers and ERP applications from Oracle and SAP is provided. Integration with FairWarning supports healthcare packaged application monitoring.

Analytics: The company's reporting and analytics include security configuration assessment and

policy-oriented reporting. The ForensicVue analytical tool is an integrated component of SecureVue that supports keyword search and forensic analysis.

Log management and reporting: SecureVue provides log management functions that are integrated with the overall offering. The company's compliance reporting is distinguished by the scope of SecureVue, which includes security configuration assessment and policy-oriented reporting.

Deployment and support simplicity: Customers indicate EiQ Networks offers flexibility and many customization options, but configuration and customization tasks can become complex. Users indicate strong satisfaction with technical support interactions, but there are some issues with the completeness and accuracy of written documentation. Customer feedback has been mixed in areas such as ease of correlation rules and report customization.

Use cases: SecureVue is appropriate for SIM and SEM deployments where security configuration assessment and FIM functionality are also required. The product offers configuration and customization options for those organizations with sufficient resources to enable and manage them.

Return to Top

EMC-RSA

RSA, The Security Division of EMC, has almost completed the transition from enVision to RSA Security Analytics (SA), which is an SIEM solution that is based on the NetWitness platform. RSA SA provides log and full packet data capture, basic security monitoring and basic security analytics. RSA will support the enVision platform until mid-2016. The SA reporting system can pull data from both the SA data structures as well as the IPDB in enVision, helping to accommodate the transition from enVision to SA within the RSA installed base.

RSA SA is composed of the following components:

- Decoders perform network capture or log ingestion
- Concentrators index the collected data in real time
- Brokers provide aggregate results from multiple Concentrators for analytics and reporting.

This data is further enhanced through a live-feed cloud service incorporating intelligence feeds from RSA and industry security providers. This enrichment feed can also be used for homegrown and custom data feeds providing security awareness.

Real-time monitoring: Threshold-based monitoring is currently supported. During 2Q13, RSA plans the release of a new correlation engine for the SA platform. Compound correlation rules are not supported currently, but will be supported with the release that is planned for 2Q13.

Threat intelligence: RSA Live provides aggregated threat intelligence from multiple sources including RSA's own intelligence, and other commercial and open-source feeds. This can be used to populate watch lists for contextual analysis. RSA also offers the Private Live service, which enables community-driven intelligence to groups of companies that are willing to share threat data.

Behavior profiling: RSA has indicated that it is still in the process of developing profiling capabilities for its SA offering.

Data and user monitoring: RSA SA integrates with many third-party IAM technologies to enable the monitoring of identity-centric events, and provides more than 140 predefined user activity monitoring reports. For data monitoring, SA integrates with RSA, McAfee and Symantec DLP technologies. There is support for direct monitoring of database audit logs and integration with a few DAM products.

Application monitoring: RSA SA integrates with a wide variety of Web server and Web application firewalls, and has a specific integration with SAP. There is also integration with SAP/Secude Security Intelligence for enhanced SAP activity monitoring, and with FairWarning to support third-party packaged applications used by the healthcare industry.

Analytics: enVision customers that have accumulated a large amount of event data behind enVision frequently complain about performance issues related to ad hoc queries and reporting. At the end of 2012, RSA provided an initial release of SA Warehouse — which supports long-term storage and access for compressed log data and network security metadata. The initial release has limitations on analytics (limited to keyword search into raw data), but the 1H13 release will provide a new engine that enables dynamic analytics of logs, metadata and other business context data.

Log management and reporting: Log management functions are provided by its Decoders and Concentrators. SA provides about 200 predefined reports for compliance, user activity and suspicious activity.

Deployment and support simplicity: SA is based on the NetWitness platform, which has been oriented to well-staffed security organizations in large companies that have the resources to support complex technology deployment. During 1Q13, RSA released an all-in-one appliance for SA that is a packaging option for the midmarket.

Use cases: RSA SA is ideally suited to organizations that want forensics analysis and reporting for both log data and packet capture data.

Return to Top

HP-ArcSight

HP-ArcSight provides three SIEM offerings:

Enterprise Security Manager software for large-scale event management

The ArcSight Express appliance for SIEM functions for small and midsize deployments

The Logger line of appliances, software and connectors for log management and reporting

The capability to deploy Logger in combination with ArcSight connectors provides additional options for normalized data analysis and application-layer data collection. HP is using ArcSight to unify event management across its security technologies, and to provide an integrated view of operations and security events. There is integration among ArcSight, Fortify, TippingPoint, and IT Performance Suite (Operations Manager and Network Node Manager) products. ArcSight is also integrated with HP EnterpriseView, which provides a business-centric view of IT that includes security assessment, security event and compliance data.

Real-time monitoring: ArcSight Enterprise Security Manager provides the capabilities needed for large-scale, SEM-focused deployments, but it has been complex to implement and manage. Enterprise Security Manager (ESM) version 6.0c (released 1Q13) replaces a major source of complexity and cost — the Orade Database, with the purpose-built Correlation Optimized Retention and Retrieval Engine. ArcSight Express is an appliance-based offering for Enterprise Security Manager that's designed for the midmarket, with preconfigured monitoring and reporting, as well as simplified data management.

Threat intelligence: ArcSight provides its own content and threat categorization model. There is also integration support for third-party feeds, such as iDefense and DeepSight. HP RepSM is an optional component that receives near-real-time reputation feeds from HP research labs.

Behavior profiling: ArcSight provides two functions for behavior analysis. IdentityView ships with a set of detection rules to issue alerts when any particular user performs actions that are a configurable deviation from what is normal for a group. The second is ThreatDetector, which performs historical analysis of logs to detect and graphically display statistically significant patterns (groupings of events). The engine offers the option of autocreating a rule to detect future forming of this pattern.

Data and user monitoring: In addition to typical integrations with Active Directory and network authentication sources, IdentityView is a separately chargeable module that provides prebuilt connectors to IAM systems to import users and roles, as well as specialized reports for activity-based role modeling, access violations and separation-of-duties tracking. ArcSight maintains connectors with major DLP, FIM and DAP products, and supports direct collection from database audit logs. There is no native FIM or DLP capability.

Application monitoring: Connectors are provided for major packaged and service as a software (SaaS) applications, including Oracle, SAP and salesforce.com. There is support for event collection from custom online applications and correlation across other fraud products to evaluate device, destination, account and transaction risks. HP Fortify RunTime detects application layer security events and user activity in real-time, and logs events in CEF format, which provides integration with ArcSight. Transaction activity monitoring is possible with customization.

Analytics: ESM provides trend analysis functions. ESM query performance has been raised as an issue by clients. The CORR-Engine has been implemented in ArcSight Logger, Express and most recently in ESM 6.0c, and is now the primary information store for analytics. Early adopters of ESM 6.0c report substantial performance improvements and lower resource consumption. HP has recently released integrations with Business Service Management and ArcSight connectors for Hadoop and Autonomy.

Log management and reporting: The ArcSight Logger line of appliances, software and collectors provide log management as a discrete component. ArcSight Logger can be implemented stand-alone or in combination with ArcSight connectors and/or ESM software or appliances. ArcSight provides more than 250 predefined and configurable reports. In addition, there are separately chargeable Compliance Insight Packages, which provide rules, reports and dashboards for specific regulations (such as SOX, PCI, North American Electric Reliability Corp. [NERC] and U.S. Federal Information Security Management Act [FISMA]). These packages are installed on top of Logger or ESM.

Deployment and support simplicity: ArcSight Express provides predefined monitoring rules and reports, as well as a simplified data model. With the implementation of CORR-Engine across its entire product line, ArcSight is better positioned to resolve complexity issues that have become competitive issues in the midmarket and barriers to deployment expansion in larger accounts.

Use cases: ArcSight provides comprehensive coverage for the compliance, threat management and SIEM use cases. Organizations that do not require full-function event management may be able to deploy a simpler and less expensive alternative. Users of HP security and operations technologies should expect an ongoing expansion of integrations with ArcSight.

Return to Top

IBM-Q1 Labs

The IBM-Q1 Labs' QRadar line of appliances can be deployed as all-in-one solutions for smaller environments or can be horizontally scaled in larger environments with specialized event collection, processing and console appliances. A distinguishing characteristic of the technology is the collection and processing of NetFlow data to provide network and application behavioral analyses, and behavior analysis capabilities for all events collected from any source. Q1 Labs also provides an optional component, QRadar Risk Manager, which adds network and firewall configuration monitoring and configuration context to event analysis.

Real-time monitoring: The QRadar technology provides an integrated view of the threat environment using NetFlow and direct network traffic monitoring, in combination with log-based event sources.

Threat intelligence: QRadar includes an autoupdate service that maintains current threat information (such as top targeted ports, botnets, emerging threats, bogon IPs, hostile nets, darknets and anonymous proxy). In addition, IBM provides an integration of X-Force IP Reputation data into QRadar that can be refreshed in a weekly schedule.

Behavior profiling: Behavior analysis capabilities can be applied to all data parsed from log sources. This capability complements rule-based correlation. We have validated customer deployments that utilize behavior analysis for log and NetFlow event sources. QRadar network anomaly detection complements Site Protector deployments by adding netflow and anomaly detection to the Site Protector IDS

Data and user monitoring: QRadar provides predefined, user-oriented activity reports and console views. In addition to standard integration with Active Directory and network authentication devices, QRadar also integrates with IAM technologies from IBM, CA, Novell and others. DAM is supported through direct monitoring of major DBMS logs and through integration with third-party database monitoring products from IBM Guardium, Imperva, McAfee and Application Security. This also integrates with third-party FIM and DLP products.

Application monitoring: There is integration with a variety of applications, including major Web application firewall and Web server technologies. There is also an integration with the SAP audit log, and a capability to monitor application behavior from the network using Q1 Labs' QFlow sensors.

Analytics: Analytics are supported directly from QRadar distributed event data. Customers report acceptable query response times in large deployments. During 1H13, IBM has released an integration of QRadar with InfoSphere BigInsights (IBM's commercialized Hadoop offering) and also with IBM's analytics and data visualization technologies (InfoSphere BigSheets and i2 Intelligence Analysis).

Log management and reporting: This capability is provided as a function of a general-purpose SIEM appliance, as a specialized function in a tiered deployment or as a stand-alone capability via the QRadar Log Manager appliance (which can be upgraded to QRadar SIEM via a license key upgrade). Included in the base technology are 1,300 predefined reports covering all major regulations. This can be augmented with security configuration compliance reporting via Risk Manager.

Deployment and support simplicity: Customer feedback reveals that the technology is relatively straightforward to deploy and maintain across a wide range of deployment scales.

Use cases: QRadar can support a wide set of common compliance and threat management use cases at a wide range of scale. In addition, the technology supports security-oriented use cases that benefit from network flow analysis and threat detection via broad-scope network, server, user and application behavior analysis.

Return to Top

LogRhythm

LogRhythm provides SIEM appliance and software technology to midsize and large enterprises. The SIEM technology can be deployed as a single appliance or software instance in smaller environments — configured to provide log management and event management — or it can be scaled as a set of specialized appliances (log management, event management and centralized console). The technology also includes optional agents for major OSs that can be used for filtering at the source.

Real-time monitoring: General feedback on correlation capabilities from existing LogRhythm customers has been positive. LogRhythm's 6.1 release includes an expansion of predefined monitoring rules to include the application layer. There is also enhanced support for Web application monitoring and attack response.

Threat intelligence: LogRhythm provides an integration interface for open-source threat intelligence sources, and integration support was expanded during 2012. Threat intelligence data can be referenced in alarm rules and reports. LogRhythm monitors all supported threat intelligence sources, and stages updates that can be pulled by customers. There is not specific support for commercial feeds in the product.

Behavior profiling: During 2H12, the company introduced behavioral profiling functions. Monitoring against whitelists, average trends, rate trends and histogram trends is supported. Network behavioral analysis is planned.

Data and user monitoring: In addition to integration with Active Directory and standard network authentication sources, there are integrations with IAM technologies from CA, IBM, NetIQ and Oracle. Identity cross-referencing is planned. An agent upgrade is available that provides file integrity and system process monitoring for Windows and Unix. There is integration with Symantec's DLP technology. LogRhythm can directly monitor database audit logs, and there is integration with third-party DAM technologies.

Application monitoring: LogRhythm integrates with a large number of packaged applications, including SAP, Oracle/PeopleSoft, and a variety of other ERP and HR applications. There are also integrations with Web application servers and firewalls. Application monitoring rules were added in version 6.1.

Analytics: Search and structured analysis are provided from the primary console and operate against the primary event data store. Customer feedback concerning the level of function and performance has been positive, with some caveats about the need to manage scope of queries to avoid performance issues.

Log management and reporting: LogRhythm's appliances provide horizontally scalable log

management functions. Knowledge Base has more than 950 predefined security monitoring and compliance reports, plus more than 170 additional report templates that can be used to create custom reports.

Deployment and support simplicity: There has been a consistent pattern of positive feedback from LogRhythm customers in areas such as the high level of predefined function, the ease of deployment, and the presence of straightforward interfaces for tasks such as customizing reports and developing customized correlation rules.

Use cases: LogRhythm is optimal for organizations with limited resources that require a balance of log management, reporting, event management, privileged user and FIM to support security operations and compliance use cases.

Return to Top

McAfee ESM

The McAfee ESM (formerly NitroView) line of appliances combines event collection and real-time monitoring functions with in-line network monitors, which implement deep packet inspection to obtain user, data and application context, and content for security events. In addition, the company provides integrated DAM technology, and continues its IDS and IPS business.

Real-time monitoring: Customer references validate that SEM functions are effective and can be scaled for very large deployments.

Threat intelligence: During 2012, McAfee released ESM version 9.1, which has an integration with the McAfee Global Threat Intelligence feed.

Behavior profiling: At the time of this evaluation, McAfee ESM supported risk-based and rule-based correlation. The risk-based correlation that was available in version 9.1 is more basic than what is available from competitors that provide behavior profiling. McAfee recently added statistical correlation in version 9.2 (April 2013 release), but capabilities have not been validated with customer references.

Data and user monitoring: ESM provides policy monitoring of Active Directory and LDAP, and uses integration with Securonix to provide identity cross-referencing and behavior profiling from major identity management products. The Application Data Monitor (ADM) component can extract identity information from monitored network traffic. Identity and access policy data can be automatically polled and imported for use in correlation rules and in reporting. The ESM Database Event Monitor and McAfee DAM component provides network- and agent-based DAM functions. McAfee ESM can also directly monitor database audit logs, and ESM is integrated with database vulnerability manager (DVM), McAfee database VPatch solution, as well as Guardium and Imperva using CEF. There is integration with FIM from McAfee and from several third-party products. The McAfee ESM ADM component provides network-based monitoring of data access, and there is also integration with all major third-party DLP products.

Application monitoring: The McAfee ESM ADM component provides network-based activity monitoring for an extensive list of applications. Direct Web server log integration is limited to Apache and Microsoft IIS. SAP and Oracle/PeopleSoft are supported via a direct integration. There are several integrations with major applications in use by the power generation industry, and an integration with FairWarning for monitoring of packaged healthcare applications.

Analytics: ESM includes proprietary high-speed event storage and query technology. Customer references give high marks for ad hoc query performance, even for deployments that must support high data acquisition rates and storage volumes. Development plans include connectors to technologies such as Hadoop and TeraData.

Log management and reporting: The McAfee ESM Receiver component is an event log collector, and McAfee ESM ELM provides log management. A large number of customizable predefined reports are provided.

Deployment and support simplicity: References have validated that ESM is relatively easy to deploy and maintain. Users indicate excellent premium support experiences, and less satisfaction with standard support interactions.

Use cases: McAfee ESM provides very good support for the compliance, threat management and SIEM use cases. ESM capabilities are well matched with deployments that require DAM, basic network-oriented DLP capabilities or monitoring of industrial control systems. The technology should also be evaluated for use cases that require heavy ad hoc query and historical analysis.

Return to Top

NetIQ

NetIQ Sentinel version 7 is composed of three components: the core Sentinel Server, Sentinel Log Manager and Sentinel Agents. Sentinel and Sentinel Log Manager are offered as software as well as virtual appliance deployments. NetIQ Sentinel integrates with other NetIQ products, including AppManager Identity Manager, Access Manager, Directory and Resource Administrator, and Secure Configuration Manager.

Real-time monitoring: Sentinel Server's real-time monitoring and incident management capabilities are scalable, highly customizable and suitable for large-scale security operations center deployments.

Threat intelligence: There are no specific integrations with IP reputation or other external threat intelligence feeds.

Behavior profiling: Sentinel 7 detects anomalies through the analysis of baseline deviations, and provides visual representation of baselines and deviations.

Data and user monitoring: Sentinel is integrated with NetIQ's IAM technologies, which enables policy-based user activity monitoring, and provides competitive differentiation for use cases where NetIQ IAM products are deployed. In addition to standard Active Directory integration, Change Guardian for Active Directory (an optional component) provides agent-based, real-time monitoring that augments native audit functions.

Sentinel provides database audit functions and also integrates with major third-party DAM products, such as Imperva and IBM Guardium. Sentinel provides integration with NetIQ Change Guardian for real-time FIM for Windows Unix and Linux, plus Active Directory, and there is also integration with third-party FIM products.

Application monitoring: Sentinel integrates with SAP for monitoring of identity and access policy changes in SAP, and also integrates with Oracle/PeopleSoft. Sentinel can monitor several Web application servers.

Analytics: Sentinel provides a Web-based interface into full-text indexed search functions. Sentinel 7 has replaced the relational database used in prior versions to store event data, and users report substantial improvements in ad hoc query performance with version 7 data store.

Log management and reporting: Sentinel Log Manager provides log data collection, storage, archiving and reporting. Log Manager can be used with Sentinel Agents to normalize, filter, compress and encrypt an event stream to the Sentinel event manager.

Deployment and support simplicity: Sentinel 7 introduced major improvements in install packaging and report customization. However, users report the upgrade effort includes revising connectors for custom applications, which can extend the time needed to migrate to the new version. NetIQ's plans to introduce a common administrative interface for the multiple components of Sentinel in late 2012 have been delayed and not yet generally available. NetIQ's granular and shifting licensing and pricing packages have introduced complexity and uncertainty into the acquisition and upgrade process.

Use cases: Sentinel is a very good option for large-scale SEM deployments for threat monitoring. There is also a good fit for compliance use cases when Sentinel Log Manager provides adequate coverage of compliance reporting use cases and there is a focus on Windows Active Directory and multiplatform FIM — especially when additional NetIQ technologies and modules are deployed.

Return to Top

Sensage

KEYW's Sensage solution is optimized for analytics and compliance reporting against a large log event data store, and the technology has been successfully deployed in many large environments that require this capability. The technology has also been successfully deployed for use cases that require application-layer and/or user-oriented monitoring.

Real-time monitoring: Although Sensage is known primarily for its analytics capabilities, we have been able to validate real-time event collection in a very large environment (10,000 server and network event sources) without real-time correlation, and real-time monitoring (multiple correlation rules) in an environment with more than 2,000 server, security and network sources. There is only a very basic native incident management capability, but integration with major third-party products is provided.

Threat intelligence: KEYW has integrated its threat intelligence with Sensage, and deploys a daily update to a distribution server from which customers can schedule pulls into Sensage watch lists. The threat intelligence feed is a consolidation of KEYW data in combination with intelligence from open sources.

Behavior profiling: The product provides basic profiling capabilities through statistical correlation and analytics.

Data and user monitoring: In addition to integration with Active Directory and network authentication sources, Sensage also has integration with IAM technology from CA, Novell and Sun. Sensage has done extensive integration with SAP, and provides the most comprehensive SAP user activity monitoring of all SIEM vendors. Sensage supports FIM through integration with Tripwire and McAfee. The technology lacks any DLP technology integration. Sensage can directly monitor database activity logs and also integrates with multiple DAM technologies.

Application monitoring: Sensage provides explicit audit support for many packaged applications — including SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and others — and pursues businesses that require application integration. The technology supports precise analytics needed for use cases, such as fraud detection.

Analytics: Sensage technology has been widely deployed for use cases that require analytics for a large log event data store. Distinguishing characteristics are very high compression rates, the ability to access the information store via standard SQL queries and Sensage connectors for a variety of mainstream analytics applications that use this query method. In addition, at query time, the technology dynamically applies a taxonomy that was associated with the event record at the time of collection. This enables flexible support for a wide range of event sources as they change over long periods of time. The vendor now supports integrations with Hadoop.

Log management and reporting: Sensage is capable of very high ingest rates of log data and has some of the largest deployments in the industry, as measured by ingest rates and the size of event data storage. There are more than 400 predefined compliance and security reports.

Deployment and support simplicity: Early in 2012, Sensage introduced Sensage Swift, a rapid deployment option, The majority of Sensage sales are to large companies that can support projects that include software product installation and customization. Customers that have deployed the current release of Sensage indicate that the install process is much simpler than previous releases.

Use cases: Sensage is a good fit for use cases that require large-scale security analytics and compliance reporting. The technology can also support use cases that include real-time monitoring; however, it is not the best fit for use cases that are focused primarily on that capability.

Return to Top

SolarWinds

SolarWinds Log and Event Manager (LEM) software is packaged as a virtual appliance. The software is targeted to SMBs, and provides real-time monitoring and log management. An optional Windows endpoint agent provides endpoint monitoring and control functions that are in widespread use within the installed base.

Real-time monitoring: SolarWinds LEM provides SEM functions that are easy to customize and deploy. Customers indicate that the library of predefined correlation rules is very close to what is needed, and that the needed light customization is straightforward.

Threat intelligence: SolarWinds LEM does not integrate with threat intelligence feeds.

Behavior profiling: There are baseline rules that can provide data about variations from historical norms, and results can be tested by correlation rules.

Data and user monitoring: SolarWinds LEM can derive user context from Active Directory and standard network authentication technologies. These limited IAM sources are dominant in the SMB space. The USB defender agent provides file access audit functions, and there is also integration with third-party FIM solutions. The endpoint agent provides some DLP capabilities, and there is integration with a few third-party products. The SQL auditor agent provides DAM capabilities, and SolarWinds LEM can directly monitor database audit logs. There is also integration with third-party DAM products.

Application monitoring: The vendor indicates that SolarWinds Server and Application Monitor (SAM) or SolarWinds Web Performance Monitor (WPM) can provide application activity data to SolarWinds LEM. SolarWinds LEM also integrates with a variety of Web infrastructure technologies, but provides very limited integration with packaged applications.

Analytics: Support for analytics is provided through visualization and investigation tools that are built into the SolarWinds LEM console, and also through the reporting interface.

Log management and reporting: Log management capabilities are provided. Users indicate that predefined reports are very close to what is needed for compliance reporting, and that, when light customization is needed, it is easy to accomplish.

Deployment and support simplicity: SolarWinds provides technology that is well-suited to its target market, requiring only light customization through easy-to-use interfaces. SolarWinds does not provide on-site implementation support services to its customers, but is working to certify deployment service partners on SolarWinds LEM.

Use cases: SolarWinds LEM is well-suited to smaller enterprises that require effective threat monitoring and compliance reporting, with a technology that is easy to deploy and maintain. There is an especially good fit for small organizations that also need endpoint control functions.

Return to Top

Splunk

Splunk Enterprise provides log management, analytics and statistical commands that facilitate real-time correlation, and the Splunk App for Enterprise Security provides predefined dashboards, searches, reports and alerts to support security monitoring and analytics use cases. Splunk is most often deployed by IT operations and application support areas to gain log management and analytics for availability-oriented use cases and, because of these deployments, the vendor is often on SIEM shortlists as an incumbent vendor.

Real-time monitoring: The Splunk App for Enterprise Security includes predefined mapping for security event sources, security-specific correlation searches, reporting and security monitoring dashboards.

Threat intelligence: The Splunk App for Enterprise Security can ingest a variety of external threat data feeds and perform searches of external data sources for known malicious spyware and adware IP address ranges, malicious IP addresses and bogon lists. Users can add additional threat intelligence sources. On-demand look-up is supported for DShield and CentralOps Domain Dossier.

Behavior profiling: Splunk's statistical analysis functions (over 100 commands) can be used to identify anomalies and deviations from normal behavior.

Data and user monitoring: Splunk provides a Windows Management Instrumentation collector for Active Directory, integration with LDAP, and specific support for a few other IAM event sources. As with any SIEM technology that supports keyword search, users with knowledge of log source formats can define their own keyword searches to develop identity context. Splunk's agent provides FIM functions, and there is also integration with Tripwire, OSSEC, and Filetrek. There is no predefined mapping support for third-party DLP products. For DAM, the Splunk App for Enterprise Security provides predefined mapping support for the Oracle common audit log, and support for the SQL server system log. There is no predefined mapping support for third-party DAM products at this time.

Application monitoring: A common use case for Splunk is monitoring in-house-developed and commercial applications through keyword searches to correlate data from multiple sources. Splunk provides specialized add-ons for a number of commercial applications, but only a few of these sources are supported with event mapping, predefined searches and reports.

Analytics: The Splunk App for Enterprise Security provides predefined dashboards that support drill-down to intermediate data aggregations, drill-down to the raw data, and pivoting to look at the data from different perspectives. Users report significant improvement in dashboard refresh rates in the latest version of Splunk and the Splunk App for Enterprise Security.

Log management and reporting: We note increased deployment of, and interest in, Splunk both as a companion technology to existing SIEM deployments, and as an SIEM. Security organizations use Splunk to provide log management functions for SIEM deployments, ad hoc query and compliance reporting. The Splunk App for Enterprise Security provides functionality to enable deployment as an SIEM, including predefined reports to support security monitoring and compliance reporting use cases.

Deployment and support simplicity: Splunk continues to add predefined security content and more external security feeds to the Splunk App for Enterprise Security. Splunk provides a wide range of configuration and customization options, but Splunk SIEM deployments typically require more customization effort than more mature SIEM products. Splunk security customers tend to be expert users with detailed knowledge of event sources that also value user-defined over predefined function.

Use cases: Splunk is a good fit for security organizations with sufficient deployment and customization expertise that need log management, keyword search, ad hoc query, real-time monitoring and correlation, and that have users with knowledge of event formats. Splunk supports a wide range of additional use cases, which include application monitoring, data analytics and IT operations management. Splunk has improved the predefined security use case support in the Splunk App for Enterprise Security, and the product can be extensively customized by expert users.

Return to Top

Symantec

Symantec Security Information Manager (SSIM) is delivered as a software appliance providing SIM, SEM and log management. Symantec has integrated SSIM with its Security Endpoint Protection (SEP), IT governance, risk and compliance management (IT GRCM) and DLP technologies. Symantec also has managed security service offerings that use the software appliance for on-site data collection and analysis. Dynamically updated threat and vulnerability data content is available to SSIM from Symantec's DeepSight security research and managed security services. During the past 12 months, Symantec enhancements included support for deployment in a VMware environment, improved analytics of user activity, and greater flexibility in archive/restore policy control. Development plans indude a unified collection architecture for all Symantec products.

Real-time monitoring: SSIM is suitable for SEM use cases, including large deployments. The product ships with a reasonable set of predefined correlation rules. SSIM's built-in incident response workflow is suitable for smaller deployments, and Symantec has added integration with external workflow products.

Threat intelligence: Symantec DeepSight real-time security intelligence provides monitoring content for external threats. The external threat monitoring content is pushed to SSIM and incorporated into event monitoring watch lists for activity related to malicious IP addresses.

Behavior profiling: SSIM provides no direct capability. Support for behavior analysis is limited to what is provided via the integration with Symantec Critical System Protection (CSP) or other event sources.

Data and user monitoring: SSIM integration is limited to Active Directory and a few other minor sources. Symantec offers basic capabilities, centered on dynamic watch lists, sufficient for many compliance-driven use cases but limiting for security monitoring use cases. SSIM integrates with Symantec and McAfee DLP technologies. FIM is provided through integration with Symantec CSP and other third-party technologies. SSIM can directly monitor database activity logs, and there is integration with major third-party DAM products.

Application monitoring: SSIM monitors SAP security audit log and has integrations with FairWarning, major Web servers, and with network and gateway security applications. Some customers have also employed customized collection to implement application-layer monitoring for use cases such as fraud detection.

Analytics: SSIM supports event forwarding to data to external data warehouses such as Hadoop, and SSIM external queries can be extended to those data stores. We have validated ad hoc query scalability in large deployments.

Log management and reporting: An SSIM instance can be configured as a specialized log collector, or to provide log management and event management capabilities. Agent-based and agentless log collection methods are supported. SSIM provides flexible archiving options to support multiple retention requirements. Symantec provides a large number of predefined, customizable security- and compliance-oriented queries to generate reports. There are more than 150 compliance report templates that cover all major regulations included with SSIM.

Deployment and support simplicity: The all-in-one appliance model is relatively easy to deploy. Symantec and its service provider partners provide basic implementation support, but there is a lack of resources to support customers that want assistance with application of the technology to more-advanced use cases.

Use cases: SSIM is capable of supporting a wide range of log management, compliance reporting and basic event management requirements. However, SSIM is not a good fit for implementations that require a high degree of customization or integration with specific IAM technologies beyond the narrow set of directory and network authentication technologies that are supported.

Return to Top

Tibco-LogLogic

Tibco Software acquired LogLogic in 2012. LogLogic's core log management appliances provide log management, searching and alerting functions, reporting for regulatory compliance, and for some security and operations use cases. The log management appliances have been frequently installed as a data collection and analysis tier, in conjunction with other SEM-focused products and, more recently, with LogLogic's SEM technology. LogLogic also provides the Security Event Manager appliance (real-time SEM and correlation), and the Database Security Manager appliance (agent-based activity monitoring and virtual patch capabilities for databases). Virtual appliances are available, and Compliance Manager is now packaged as a software offering.

Real-time monitoring: The log management appliances provide alert functions based on characteristics of the log event stream. The Security Event Manager appliance provides real-time monitoring and event correlation. We have validated successful deployments that do not expose the LogLogic Security Event Manager to high event rates, but clients that are considering the technology for real-time correlation functions at high event rates should request references that have deployed at similar levels of scale.

Threat intelligence: LogLogic does not integrate threat intelligence data.

Behavior profiling: Behavior profiling is not supported, but LogLogic supports simple rate/ratio-based alerting. LogLogic creates and maintains an historical traffic baseline profile for each log source based on time of day. Alerts can be triggered if rates deviate more than a given percentage above or below the baseline.

Data and user monitoring: LogLogic covers the standard set of identity sources (major directories and network authentication sources) and a few third-party identity management systems. DAM is provided directly from database audit logs or from LogLogic's optional Database Security Manager agent/appliance. LogLogic has integrated with a number of DLP solutions, including Symantec, RSA, McAfee and CA. There is an integration with Tripwire for file integrity monitoring.

Application monitoring: LogLogic's supported application sources can best be described as "infrastructure level" (Web application servers, application gateways and so on). There is a limited file pull integration with SAP. Customers have complained about the complexity of Log Labels, which provide an interface to define log source formats for unsupported event sources.

Analytics: Analytics are supported directly from LogLogic's LX, MX and ST appliances, from the Enterprise Virtual Appliance, and from software offerings such as Compliance Manager. Customers report acceptable ad hoc query performance, as long as a query can be constructed in a way that uses the prebuilt indexes. Long-running queries result if indexes are not referenced. Integration with SpotFire provides high-scale advanced analytics.

Log management and reporting: The LogLogic LX, ST and MX appliances provide very good core log management functions, and are widely deployed by organizations whose primary need is log management. Virtual appliances are also available. LogLogic offers its optional Compliance Suite (CS) reporting packages for all major regulations. Each CS contains a set of customizable reports and alerts, each mapped to one of the control objectives of its target mandate. Each CS contains about 200 reports and 100 alerts, and also provides compliance dashboards and workflow functions.

Deployment and support simplicity: Log management appliances are straightforward to deploy, but LogLogic now has four discrete appliance types (log management, event management, DAM and compliance workflow). There have been customer complaints about sparse documentation and the complexity of the event source integration interface. The company needs to continue standardizing administrative interfaces and making changes to improve appliance versatility.

Use cases: LogLogic's log management appliances are a good choice for organizations that want to deploy a consistent log management infrastructure across their environments in combination with other event management and analytics solutions for security and operations. The technology offers very good support for the log management and compliance reporting use case. We have validated successful deployments that do not expose the LogLogic Security Event Manager to high event rates.

Return to Top