G00227900

Critical Capabilities for Security Information and Event Management

Published: 21 May 2012

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

This research assesses 12 security information and event management technologies by evaluating the capabilities that are critical for the support of threat management, compliance reporting and SIEM deployment use cases.

Key Findings

- Many security information and event management (SIEM) vendors are releasing or developing SIEM capabilities — such as behavior profiling and anomaly detection, threat intelligence, and more effective analytics — to support the early detection of targeted attacks.
- High-performance event processing and data retrieval are needed to support the iterative analysis of historical data required for breach detection.
- Deployment and support simplicity is an important attribute for all use cases because of the resource constraints of most IT security organizations.

Recommendations

- Product selection decisions should be driven by organization-specific requirements in areas such as deployment scale, real-time security monitoring, compliance reporting, analytics, and integration with system and application infrastructures.
- Organizations should 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 capability gaps.
- When developing requirements, include stakeholders from internal audit, compliance, IT security and IT operations.
- Develop a two- to three-year road map for all functions that will influence buying decisions for the initial implementation.

What You Need to Know

Organizations evaluating SIEM tools should begin with a requirements definition effort that includes IT security, internal audit, compliance and IT operations. Organizations must determine deployment scale, real-time monitoring and postcapture analytics requirements, and compliance reporting requirements. In addition, organizations should identify products whose deployment and support requirements are a good match to internal project and support capabilities. Gartner recommends developing a set of requirements that resolve the initial problem, but 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 influence the buying decision for the initial implementation.

Analysis

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.

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 security policy compliance monitoring and incident investigation 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 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.

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 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 device 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 large percentage 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 discrete event sources, such as NetFlow data, users, servers 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.

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 and incident response capabilities. There's higher weighting to real-time event management and correlation, threat intelligence, anomaly detection, and support for security event 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, security has funding to close compliance gaps, but there's also a need to improve threat management and incident response capabilities. The SIEM technology must support rapid deployment for compliance reporting, and provide for subsequent deployment steps that implement security event management (SEM) capabilities.

Critical Capabilities

Eight critical capabilities 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).
- **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 botnet control.
- **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.
- **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.
- **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%	15.0%	15.0%
Threat Intelligence	12.5%	2.0%	8.0%	10.0%
Behavior Profiling	12.5%	2.0%	8.0%	7.0%
Data and User Monitoring	12.5%	10.0%	9.0%	8.0%
Application Monitoring	12.5%	2.0%	10.0%	6.0%
Analytics	12.5%	2.0%	30.0%	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 (May 2012)

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 2012.
- 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]

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.

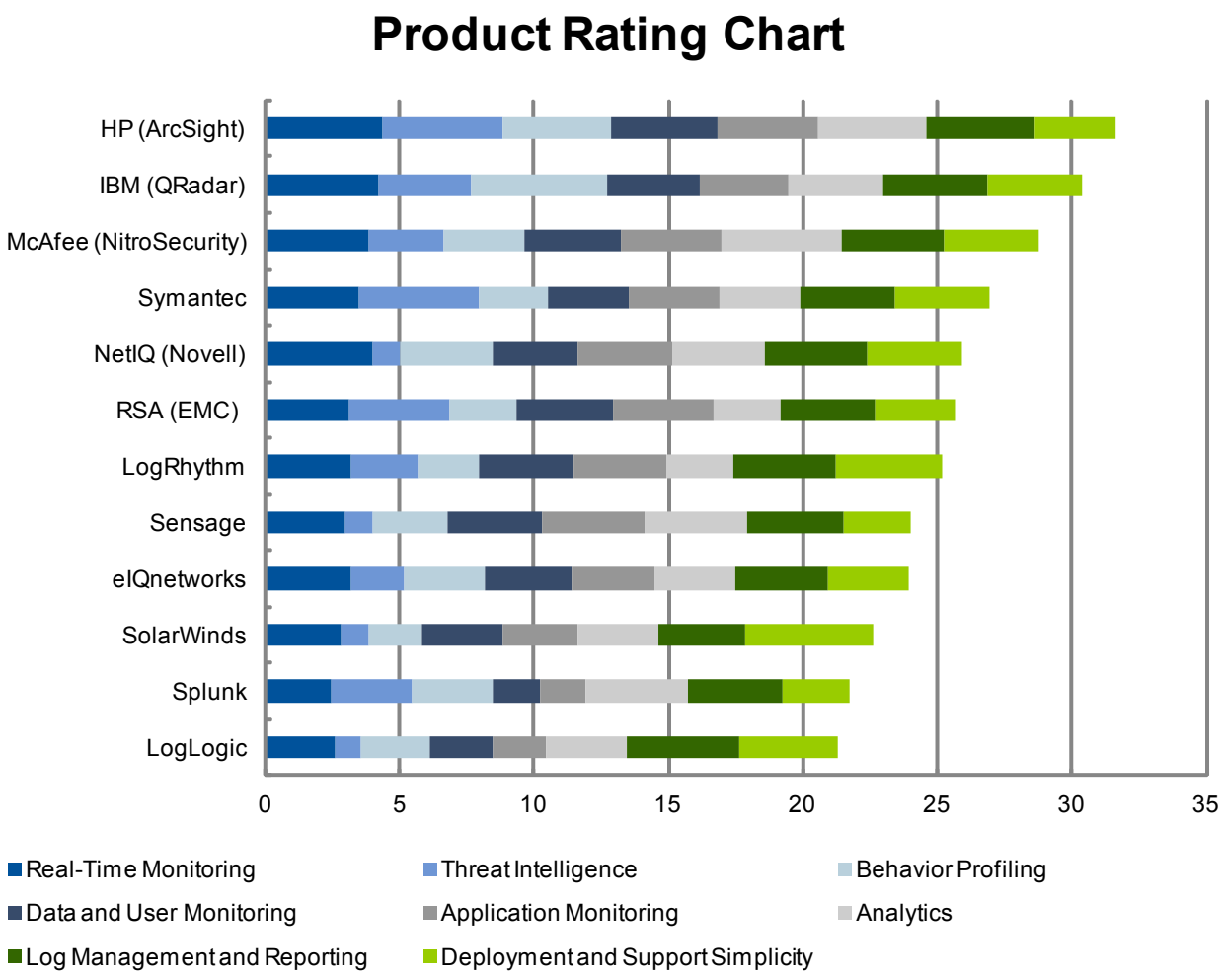
Figure 2. Product Rating on Critical Capabilities

Product Rating	elQnetworks	HP (ArcSight)	IBM (QRadar)	LogLogic	LogRhythm	McAfee (NitroSecurity)	NetIQ (Novell)	RSA (EMC)	Sensage	SolarWinds	Splunk	Symantec
Real-Time Monitoring	3.2	4.4	4.2	2.6	3.2	3.9	4.0	3.1	3.0	2.9	2.5	3.5
Threat Intelligence	2.0	4.5	3.5	1.0	2.5	2.8	1.0	3.7	1.0	1.0	3.0	4.5
Behavior Profiling	3.0	4.0	5.0	2.5	2.3	3.0	3.5	2.5	2.8	2.0	3.0	2.5
Data and User Monitoring	3.2	4.0	3.5	2.4	3.5	3.6	3.1	3.6	3.5	3.0	1.7	3.0
Application Monitoring	3.1	3.8	3.3	2.0	3.5	3.7	3.5	3.8	3.8	2.8	1.8	3.3
Analytics	3.0	4.0	3.5	3.0	2.5	4.5	3.5	2.5	3.8	3.0	3.8	3.0
Log Management and Reporting	3.4	4.0	3.9	4.2	3.8	3.8	3.8	3.5	3.6	3.3	3.5	3.5
Deployment and Support Simplicity	3.0	3.0	3.5	3.7	4.0	3.5	3.5	3.0	2.5	4.8	2.5	3.5

Source: Gartner (May 2012)

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



Source: Gartner (May 2012)

Figure 4 shows the product scores for each use case.

Figure 4. Product Score in Use Cases

Use Cases	elQnetworks	HP (ArcSight)	IBM (QRadar)	LogLogic	LogRhythm	McAfee (NitroSecurity)	NetIQ (Novell)	RSA (EMC)	Sensage	SolarWinds	Splunk	Symantec
Overall	3.0	4.0	3.8	2.7	3.2	3.6	3.2	3.2	3.0	2.8	2.7	3.4
Compliance	3.2	3.8	3.8	3.7	3.7	3.7	3.6	3.3	3.2	3.5	3.0	3.5
Threat Management	3.0	4.0	3.7	2.8	3.1	3.8	3.4	3.1	3.2	2.9	2.9	3.3
SIEM	3.1	3.9	3.8	3.0	3.4	3.6	3.4	3.2	3.0	3.1	2.8	3.5

Source: Gartner (May 2012)

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).

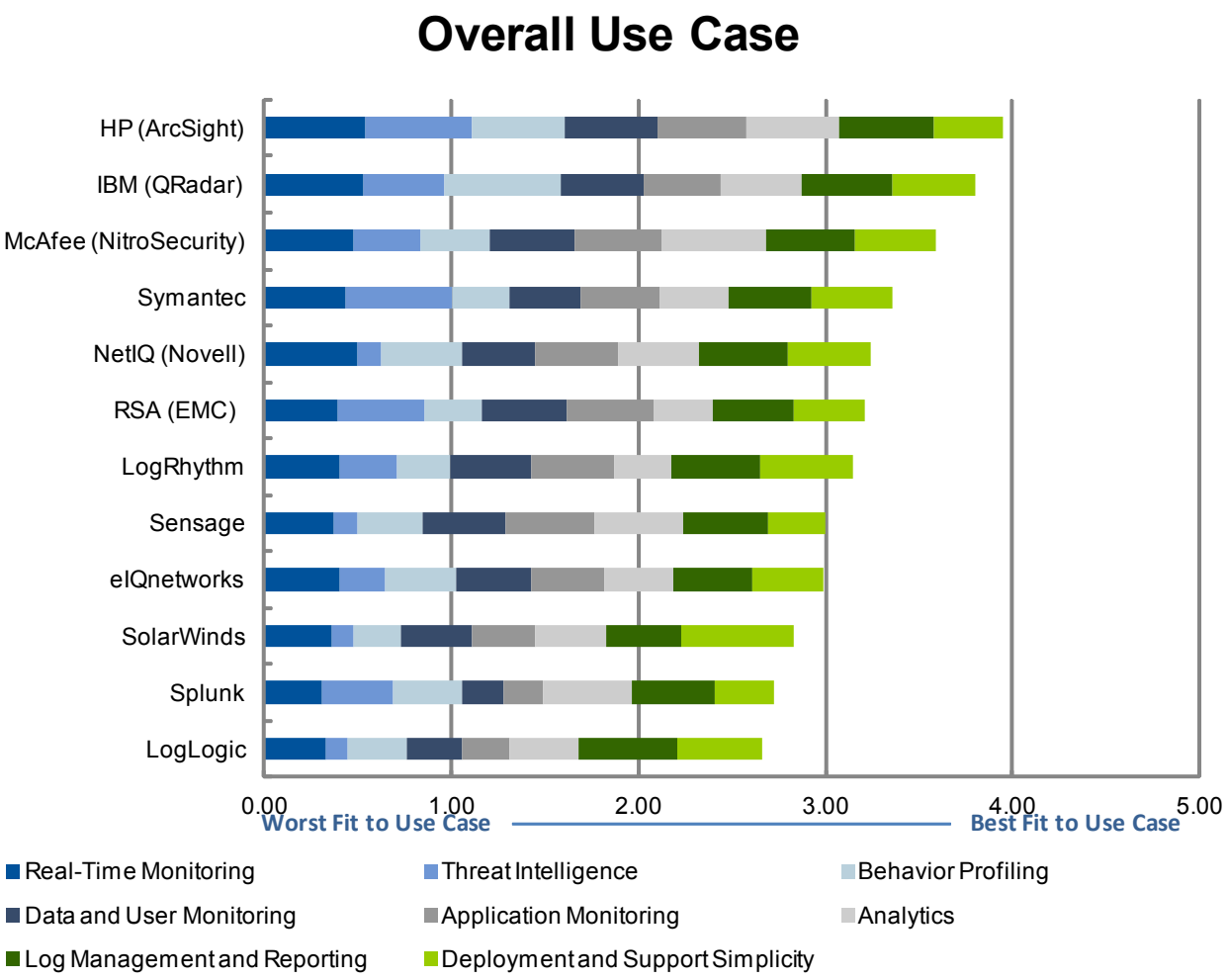
Figure 5. Product Viability Rating

Vendor/Product Name	elQnetworks	HP (ArcSight)	IBM (QRadar)	LogLogic	LogRhythm	McAfee (NitroSecurity)	NetIQ (Novell)	RSA (EMC)	Sensage	SolarWinds	Splunk	Symantec
Product Viability	Good	Excellent	Excellent	Good	Good	Excellent	Good	Good	Good	Good	Good	Good

Source: Gartner (May 2012)

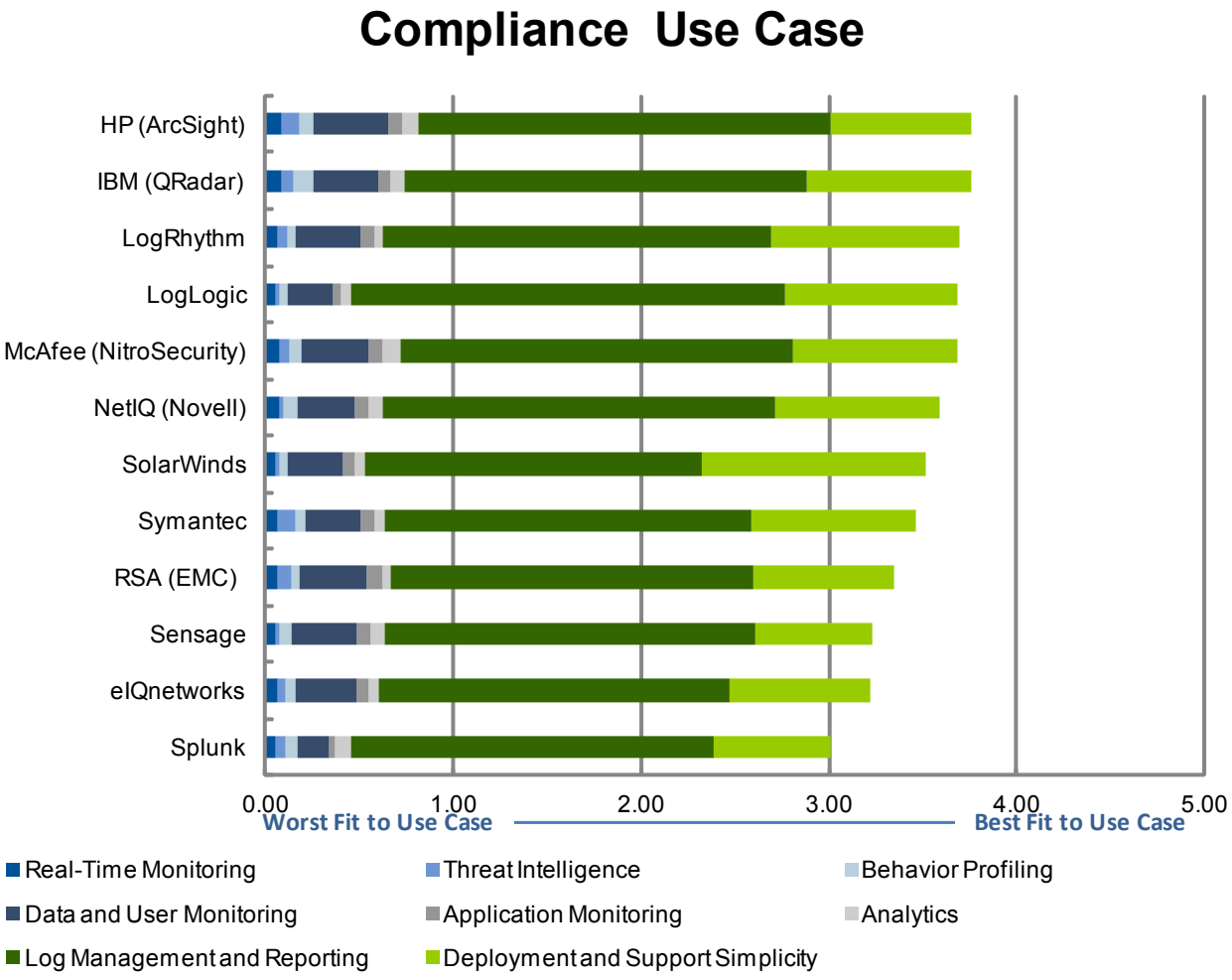
The overall use case is in Figure 6. See Figures 7, 8 and 9 for the vendor scores for specific use cases.

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



Source: Gartner (May 2012)

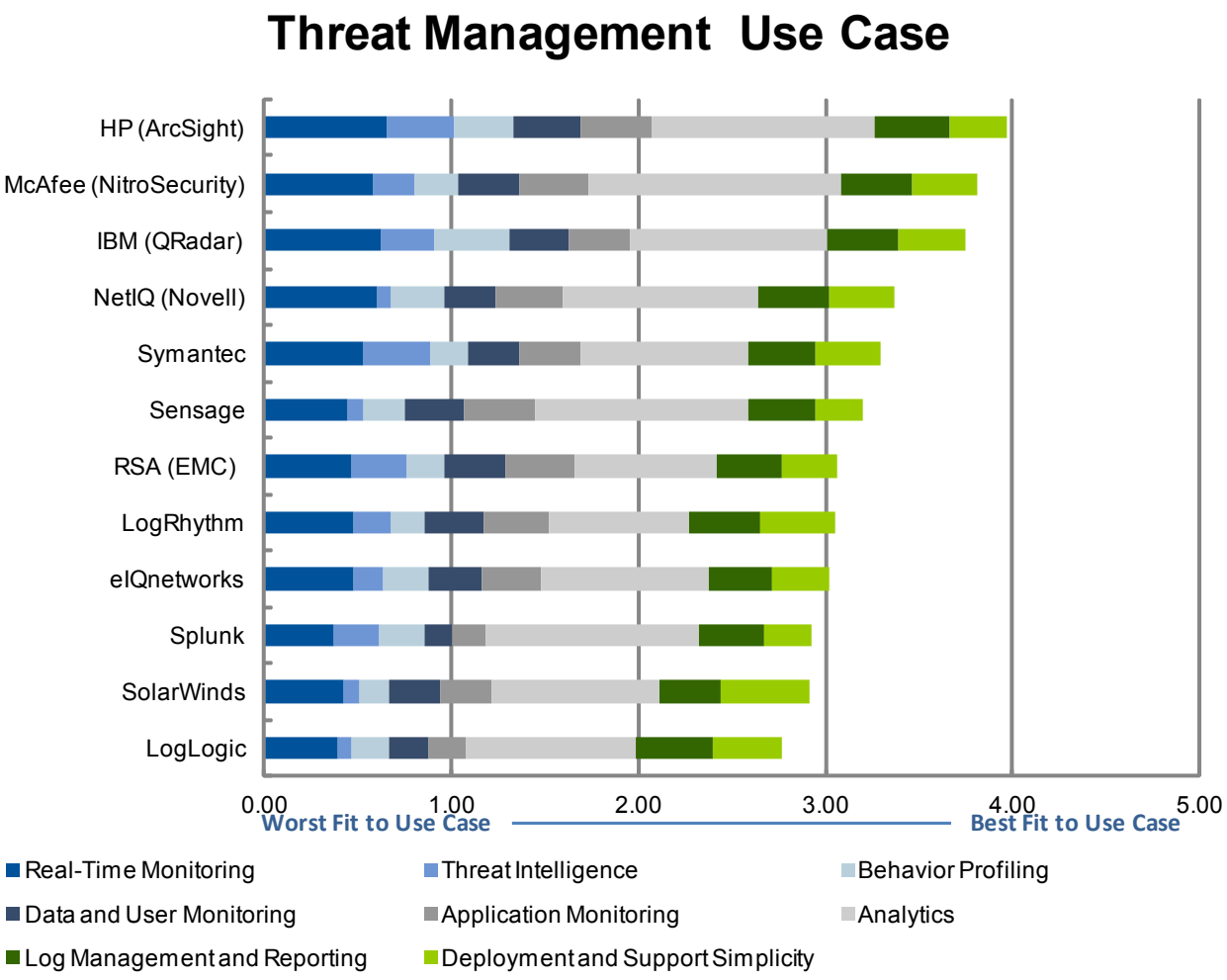
Figure 7. Vendors' Product Scores for the Compliance Use Case



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

Source: Gartner (May 2012)

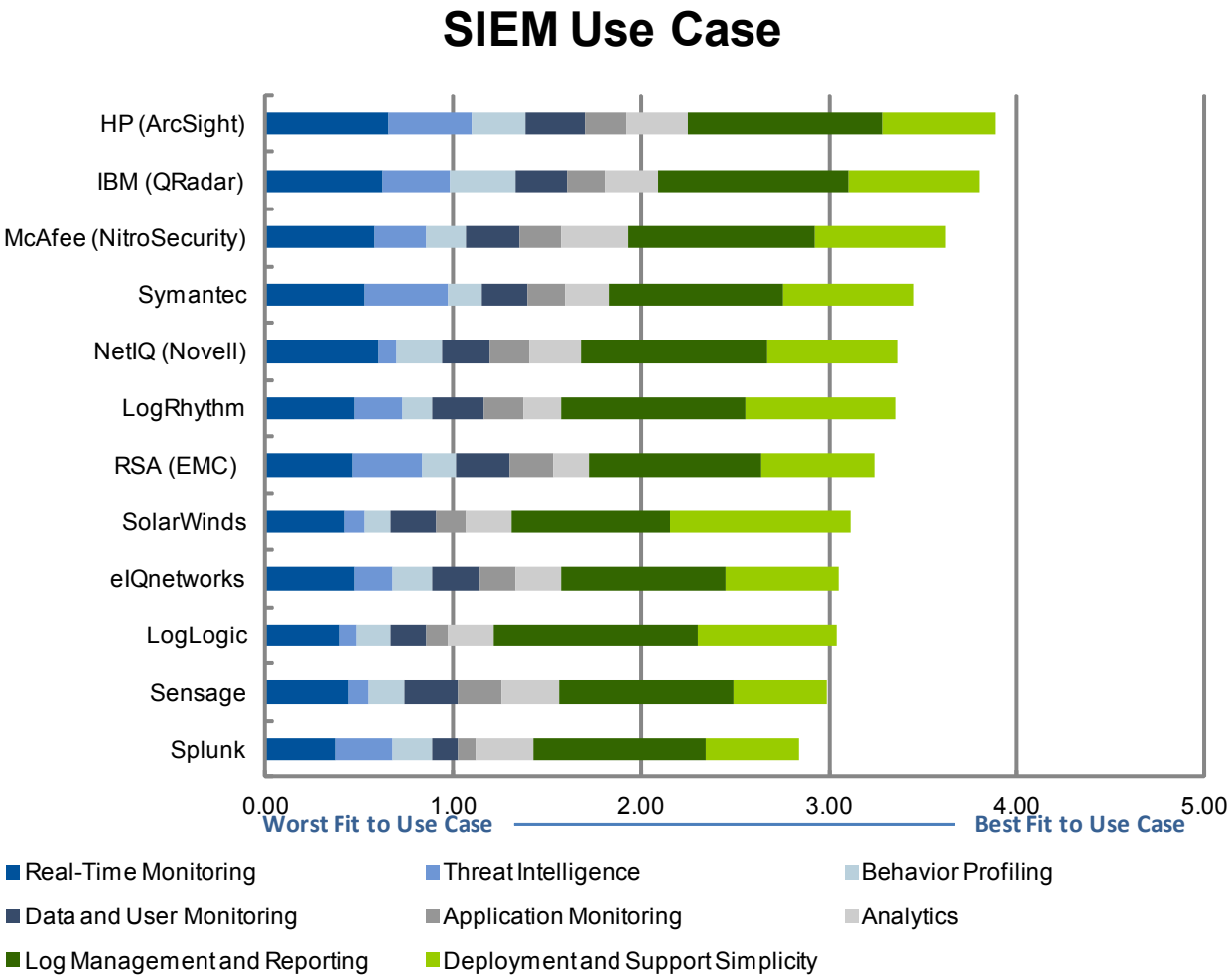
Figure 8. Vendors' Product Scores for the Threat Management Use Case



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

Source: Gartner (May 2012)

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



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

Source: Gartner (May 2012)

Vendors

eIQnetworks

eIQnetworks' SecureVue provides SEM, security information management (SIM), security configuration policy compliance, FIM, operational performance monitoring functions, and some network behavior analysis capabilities. SecureVue is composed of 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, while agents are software only.

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

Threat intelligence: SecureVue has built-in integration with threat intelligence data from Cisco and Vigilant. Data from these sources can be updated in user-defined intervals.

Behavior profiling: The company has recently introduced basic behavior profiling capabilities and reputation database support, with development plans to enhance the capability.

Data and user and monitoring: IAM integration includes Microsoft Active Directory and IAM technologies from CA, IBM, Oracle, Novell and RSA (EMC). SecureVue integrates with the major DLP and DAM products. An optional host agent provides FIM. There is also integration with third-party FIM tools from Tripwire and nCircle.

Application monitoring: SecureVue integrates with major Web application servers and ERP applications from Oracle and SAP, and some packaged applications in some industry verticals, such as healthcare. There is also an integration with FairWarning to extend support of 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. Customer feedback on ad hoc query performance has been mixed, with some customers indicating good performance and others indicating performance issues for queries against distributed log data stores.

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: Customer feedback has been positive in areas such as ease of correlation rule and report customization.

Use cases: In addition to providing a solution for typical deployments that require a mix of SIM and SEM functions, SecureVue is optimal for organizations that also need security configuration assessment functions.

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 log management appliances and collectors for log management and reporting

The capability to deploy Logger in combination with ArcSight agents 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 already a good deal of existing 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's complex to implement and manage. 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. As part of the HP Enterprise Security Products business unit, there is development work with DVLabs (earlier TippingPoint) to integrate reputation data feeds into ArcSight SIEM offerings.

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 and 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 DAM 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 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. During 1Q12, HP announced Application Security Monitor — an ArcSight connector that monitors authentication and authorization activity. The connector can be deployed on any physical or virtual server running the application. Transaction activity monitoring is possible with customization, and real-time application vulnerability detection is provided (using technology derived from Fortify).

Analytics: The Correlation Optimized Retention and Retrieval Engine (CORR-Engine) currently implemented in ArcSight Logger and Express — and soon to be implemented in Enterprise Security Manager — is becoming the primary information store for analytics. Enterprise Security Manager query performance has been raised as an issue by clients. The replacement of relational databases

with the CORR-Engine (planned for later in 2012) should improve Enterprise Security Manager query performance.

Log management and reporting: The ArcSight Logger line of appliances and collectors provides log management as a discrete component. ArcSight Logger can be implemented stand-alone or in combination with ArcSight agents and/or Enterprise Security Manager 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 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 Enterprise Security Manager.

Deployment and support simplicity: ArcSight Express provides predefined monitoring rules and reports, as well as a simplified data model. During 3Q11, HP eliminated the Oracle Database from Express, which simplifies the offering. A similar update is planned for Enterprise Security Manager in 3Q12. With these enhancements, ArcSight hopes to solve 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.

IBM (QRadar)

IBM's acquisition of Q1 Labs provides strong SIEM technology as a replacement for IBM's marginal Tivoli SIEM offering. The 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 the expansion of behavior analysis capabilities to include all the 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). During 2Q12, IBM plans to release an integration of X-Force IP Reputation data into QRadar for real-time risk identification.

Behavior profiling: Behavior analysis capabilities were extended beyond NetFlow data early in 2011 to include all data parsed from log sources. This capability complements rule-based correlation. We have validated multiple large-scale deployments that incorporate a combination of

log and NetFlow event sources, and IBM is developing extensive integrations with ISS packet capture and attack detection data.

Data and user and 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. Enhancements during the past 12 months included indexing and query improvements to support keyword search, and improvements in event storage scalability. Customers report acceptable query response times in large deployments.

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.

LogLogic

Tibco Software announced the intention to acquire LogLogic as the research process for this document was drawing to a close. We evaluated LogLogic based on capabilities that were generally available from LogLogic preacquisition. LogLogic's core log management appliances provide log management functions and reporting for regulatory compliance, and for some 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 Security Event Manager appliance (from the Exaprotect acquisition) 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 indicates that behavior profiling capabilities are in development.

Data and user and 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. FIM is provided via an integration with Tripwire.

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, 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.

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, 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.

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, even though support for compound correlation rules is relatively recent. LogRhythm's latest 6.0 release includes performance improvements that the vendor indicates will triple the events-per-second capacity of existing appliances.

Threat intelligence: LogRhythm provides an integration interface for open-source threat intelligence sources (such as abuse.ch, malwaredomainlist.com, projecthoneypot.org and mtc.sri.com/live_data/attackers), but the customer is responsible for obtaining the data and orchestrating list table update. The same interface can be used by the customer to pull commercial feeds, but there is not specific support for commercial feeds in the product.

Behavior profiling: Technology deployed in customer environments at the time of this evaluation lacked the capability. During 2H12, the company plans to introduce statistical analysis improvements and profiling for users and hosts. Development plans include an expansion of behavioral analysis capabilities and the introduction of network behavioral analysis.

Data and user and 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. An agent upgrade is available and 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.

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 500 predefined security monitoring and compliance reports, plus more than 100 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. Although LogRhythm has some large deployments, the majority of its customers have deployed the technology for less than 800 event sources.

McAfee (NitroSecurity)

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 intrusion detection system (IDS) and intrusion prevention system (IPS) business with a common platform for SIEM and IPS.

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

Threat intelligence: McAfee indicates that ESM version 9.1 (expected to be released in 2Q12) will have an integration with the McAfee Global Threat Intelligence feed.

Behavior profiling: The current version of McAfee ESM supports statistical correlation. The 9.1 release (planned for 2H12) will introduce profiling capabilities.

Data and user and monitoring: In addition to standard policy monitoring of Active Directory, there has been an expansion of support to include major identity management products. The Application Data Monitor (ADM) component is also able to extract identity information from monitored network traffic. There is support for the automated import of identity and access policy data for reference in correlation rules and reporting. The NitroView Database Monitor component provides network- and agent-based DAM functions. McAfee ESM can also directly monitor database audit logs, and there is integration with the IBM/Guardium, Imperva and McAfee DAM products. There is integration with many third-party FIM 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 monitoring of application activity. Direct Web server log integration is limited to Apache and Microsoft IIS. SAP is the only major packaged application that is supported via a direct integration, but the ADM component supports a long list of network-monitored applications. NitroSecurity has also done significant integrations with major applications in use by the power generation industry. There is also an integration with FairWarning for monitoring of packaged healthcare applications.

Analytics: The platform includes proprietary high-speed event storage and query technology. Customer references consistently point at ad hoc query performance as a strong point, even with very high event rates and a large back store.

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: We have spoken with multiple references that have validated that NitroView is relatively easy to deploy and maintain.

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

NetIQ (Novell)

NetIQ's 2Q11 acquisition of Novell's SIEM technology brings together two software offerings that are largely synergistic. Sentinel is the "go forward" SIEM platform for NetIQ, The company has made rapid progress in integrating the best of NetIQ security monitoring functions into the Sentinel v.7 platform, which was released in 4Q11. There is a lightweight interface that allows Sentinel users to integrate data from Change Guardian and Security Manager server monitoring agents. An event-forwarding interface enables Security Manager customers to deploy Sentinel to gain road scope security monitoring.

Real-time monitoring: Sentinel's core real-time monitoring and incident management capabilities are fully developed, scalable, highly customizable and suitable for large-scale security operations center deployments. Security Manager is not optimized for deployments that are focused on this use case. Security Manager's installed base is focused primarily on host and user activity monitoring, and we expect a gradual transition to the Sentinel technology base.

Threat intelligence: Limited support for threat intelligence is provided by Sentinel Advisor, which is a subscription service that pushes updated threat signatures to Sentinel. Advisor cross-references the signatures from third-party IDSs, IPSs and vulnerability scanners.

Behavior profiling: Sentinel 7 introduced an anomaly detection engine that detects anomalies through the analysis of baseline deviations, and provides visual representation of baselines and deviations.

Data and user and monitoring: Sentinel is integrated with NetIQ's IAM technologies, which enables policy-based user activity monitoring, and provides competitive differentiation for use cases involving NetIQ IAM technology. In addition to standard Active Directory integration, Change Guardian for Active Directory (an optional component) provides agent-based, real-time monitoring that does not depend on native audit functions.

Sentinel supports DAM through native database audit functions and also integrates with major third-party DAM products, such as Imperva SecureSphere and IBM Guardium. Change Guardian provides real-time FIM for Windows and Unix systems, as well as Active Directory, and is integrated with Sentinel and Security Manager. There is also integration with third-party FIM products.

Application monitoring: Sentinel integrates with a few packaged applications. Its distinguishing characteristic in this area is the integration with SAP, which enables the monitoring of identity and access policy change activities within SAP. There is also an integration with Oracle/PeopleSoft. A variety of Web application servers can also be monitored.

Analytics: Sentinel provides a Web-based interface into full-text indexed search functions. Sentinel 7 eliminates the need for a relational database to store event data, and early adopters of the release report drastic improvements in ad hoc query performance.

Log management and reporting: Sentinel Log Manager provides log data collection, storage, archiving and reporting. The component can be used in combination with Sentinel agents to normalize, filter, compress and encrypt an event stream to the Sentinel event manager. Security Manager provides integrated log management and archive components. Both products provide user and resource access monitoring reports for compliance reporting.

Deployment and support simplicity: Sentinel 7 introduced major improvements in install packaging and report customization that we have been able to verify with multiple Sentinel 6 customers that have done "from scratch" deployments of the new release. Although NetIQ's two SIEM technologies are synergistic, organizations need to deploy multiple components that are managed by two different administrative interfaces. A deployment of log management and event management functions still requires the installation of multiple software components. Additional NetIQ integrations will be rolled out during 2012.

Use cases: Sentinel provides SEM capabilities that support large-scale deployments for threat monitoring. The compliance reporting use case is adequately covered with Log Manager. The SIEM technology is an especially good fit for organizations that have also deployed NetIQ's IAM technology. Security Manager provides coverage for compliance use cases when there is a focus on Windows Active Directory and multiplatform FIM — especially when additional NetIQ technologies and modules are deployed.

RSA (EMC)

RSA, The Security Division of EMC, is in a period of transition for its security monitoring technologies. The vendor positions its recently introduced NetWitness for Logs offering as the scalable solution for log analytics and reporting for its larger customers, but still needs to maintain the enVision platform for real-time monitoring for all customers and as a general SIEM solution for smaller deployments. In the long term, we expect the introduction of a full-function correlation engine for NetWitness, a transition to NetWitness as the primary SIEM platform and support of enVision, as long as customers require it.

Real-time monitoring: We have validated a few large-scale enVision deployments that use real-time monitoring capabilities, but there has been a long-standing pattern of mixed customer feedback in this area. In the long term, we expect RSA to develop a real-time correlation engine for NetWitness as a replacement for enVision for security use cases.

Threat intelligence: NetWitness Live provides aggregated threat intelligence from multiple sources to log event data for contextual analysis. RSA continues to integrate additional intelligence feeds, such as its CyberCrime Intelligence and FraudAction services.

Behavior profiling: RSA has indicated that it is developing profiling capabilities for its SIEM technologies.

Data and user and monitoring: enVision 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, enVision 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: enVision 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. RSA now positions a second component — NetWitness for Logs — as a solution to this issue. NetWitness has a reputation for providing strong analytics capabilities for packet capture data, and these capabilities should carry forward to log analysis as well.

Log management and reporting: Log management and reporting are provided by two technologies — enVision and NetWitness. enVision provides appliance-based log management capabilities. High ingest rates are possible, but reporting performance issues become more common as the back store grows in size There are more than 1,300 predefined reports, including a large number of predefined reports for all major regulations. NetWitness for Logs also provides log management and reporting functions. RSA has implemented about 100 of the most commonly used compliance reports on NetWitness.

Deployment and support simplicity: enVision is easier to deploy than most software-based SIEM technologies, but query and report performance issues have complicated ongoing operational support in moderate and large deployments. During this period of transition, RSA is offering two loosely coupled technologies for security monitoring. Until RSA develops a correlation engine for NetWitness, customers will need to deploy enVision. Customers that need scalable reporting and analytics will also need to deploy NetWitness for Logs.

Use cases: NetWitness for Logs is ideally suited to organizations that want forensics analysis and reporting for log data and packet capture data. enVision's mix of capabilities provides coverage of the compliance and SIEM use cases, and support for many threat management use cases, in midsize environments. Organizations that need to access a large event store for ad hoc queries should evaluate the cost and complexity of a two-technology solution from RSA (NetWitness and enVision) versus competing solutions for security monitoring.

Sensage

The Sensage solution is optimized for analytics and compliance reporting against a large log event data store, and the company has successfully pursued large deployments that require this capability. Sensage has also successfully pursued 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 its streaming of 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 500 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: Sensage does not integrate with threat intelligence feeds.

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

Data and user and 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 precision 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.

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: Although the company has just introduced Sensage Swift, a rapid deployment option, it was not evaluated for this critical capabilities research, and customer feedback during the evaluation period continued to indicate that the enterprise version of Sensage is complex to deploy and maintain. The majority of Sensage sales are to large companies that can

support projects that include software product installation and customization. Customers have indicated that there is still a need for Linux expertise to support a Sensage deployment.

Use cases: Sensage is a good fit for use cases that require large-scale compliance reporting or security analytics. 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.

SolarWinds

SolarWinds entered the SIEM market with the 3Q11 acquisition of TriGeo. The company repackaged TriGeo's appliance and now sells SolarWinds Log and Event Manager (LEM) software as a virtual appliance. The software is targeted to small and midsize businesses, 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 and monitoring: LEM can derive user context from Active Directory and standard network authentication technologies. These limited IAM sources are dominant in the small and midsize business 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 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 or Synthetic End User Monitor can provide application activity data to LEM. 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 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 LEM.

Use cases: SolarWinds Log and Event Manager is well-suited to midsize 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 organizations that also need endpoint control functions.

Splunk

Although Splunk is most often deployed by IT operations and application support areas to gain log management and analytics for availability-oriented use cases where a "build your own" approach is valued, the vendor has been building the predefined functions that are often valued by the security buying center. Splunk provides real-time correlation, and the Splunk App for Enterprise Security provides predefined functions to support security monitoring and analytics use cases.

Real-time monitoring: Splunk provides real-time alerting and correlation. We have been able to validate this capability with customer references. Splunk App for Enterprise Security provides predefined mapping for security event sources, and security monitoring dashboards.

Threat intelligence: Splunk App for Enterprise Security includes predefined support for the periodic collection of external threat intelligence feeds that include known malicious spyware and adware IP address ranges, malicious IP addresses and bogon lists. On-demand lookup is supported for DShield and CentralOps Domain Dossier.

Behavior profiling: Splunk provides statistical analysis of search results that can be used to identify anomalies and deviations from normal behavior.

Data and user and monitoring: Splunk provides a Windows Management Instrumentation collector for Active Directory, but does not provide specific support for any other IAM event or policy source. 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. There is no predefined mapping support for third-party DLP products. For DAM, 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.

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

Analytics: 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.

Log management and reporting: The technology is widely deployed by IT operations and application support teams. Within the past 18 months, there's been a larger uptake by IT security organizations to provide log management functions for SIEM deployments, ad hoc query and

compliance reporting, and converged use cases. Splunk App for Enterprise Security provides predefined reports to support security monitoring and compliance reporting use cases. The Splunk App for Enterprise Security provides predefined reports to support security monitoring and compliance reporting use cases.

Deployment and support simplicity: The traditional Splunk customer has been an expert user with detailed knowledge of event sources that values user-defined over predefined function. Splunk is broadening embedded product knowledge of security use cases, but the technology still requires more customization than mature commercial SIEM products.

Use cases: Splunk is a good fit for organizations that need log management, keyword search, ad hoc query and monitoring, and that have users with knowledge of event formats. Support for security use cases has improved with core Splunk capabilities for real-time monitoring and correlation, and the predefined functions provided by Splunk App for Enterprise Security. Splunk supports a wide number of additional use cases, which include application monitoring, data analytics and IT operations management.

Symantec

The Symantec Security Information Manager (SSIM) appliance provides SIM and SEM capabilities, and can be used to implement log management functions. Symantec provides integrations with its security endpoint protection, IT GRCM (governance, risk and compliance management) and DLP technologies. Symantec has managed service offerings that can potentially use the soft appliance for on-site data collection and analysis (but this is sometimes discouraged by the Symantec MSSP business unit). We have seen a pattern of customer complaints about a lack of progress in long-standing Symantec development plans for improvements in areas such as user activity monitoring, and support for co-managed deployments.

Real-time monitoring: The technology is capable for SEM use cases, and we have validated event processing in large deployments. The product ships with a reasonable set of predefined correlation rules. SSIM provides security incident response workflow, but no integrations with third-party products.

Threat intelligence: Symantec uses its DeepSight real-time security intelligence data to dynamically build monitoring content for external threats. The external threat monitoring content is pushed to SSIM customers.

Behavior profiling: There is no native capability within the product. Support for behavior analysis is limited to what is provided via the integration with Symantec Critical System Protection or other event sources.

Data and user and monitoring: IAM policy source integration is limited to Active Directory and a few other minor sources. The product provides basic capabilities that will be adequate for many compliance-driven use cases but inadequate for security-oriented monitoring. SSIM integrates with Symantec and McAfee DLP technologies. FIM is provided through integration with Symantec

Critical System Protection and other third-party technologies. SSIM can directly monitor database activity logs, and there is integration with major third-party DAM products.

Application monitoring: There are specific integrations with major Web servers, and there is also basic SAP monitoring support (the SAP security audit log). Monitoring of packaged applications for the healthcare industry is provided through an integration with FairWarning. Some customers have also employed customized collection to implement application-layer monitoring for use cases such as fraud detection.

Analytics: 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. Symantec provides a large number of predefined security- and compliance-oriented queries that are customizable and are used to generate reports. There are more than 150 compliance report templates that cover all major regulations and are included in the base product.

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 provides good support for a wide variety of use cases that require a mix of log management, compliance reporting and basic SEM functions. 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.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Planning for an SIEM Technology Deployment"

"How to Deploy SIEM Technology"

"Toolkit: Security Information and Event Management RFP"

"Effective Security Monitoring Requires Context"

Evidence

[1] Based on 300 inquiries during 2011 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 the defined requirements are not achieved.

2 = Fair: Some requirements are not achieved.

3 = Good: This meets the requirements.

4 = Excellent: This meets or exceeds some requirements.

5 = Outstanding: This significantly exceeds the 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.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Atago Green Hills MORI Tower 5F
2-5-1 Atago, Minato-ku
Tokyo 105-6205
JAPAN
+ 81 3 6430 1800

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600