Critical Capabilities for Security Information and Event Management

25 June 2014 ID:G00261642

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

VIEW SUMMARY

SIEM technologies vary widely in capabilities because of the focus vendors have on their products. This research helps IT security organizations align their particular needs with one of the three most common use cases to pick the best solution.

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. It can be achieved by vendor-supplied correlation rules, alerts, reports and other content that requires only light customization to provide early value. It is also supported by providing the means to scale the deployment and incorporate more advanced analysis without requiring substantial additional resources.

Recommendations

IT security organizations 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. The SIEM deployment can then evolve as change occurs with use in anticipation of and response to changing 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. For example, project-based services may be needed to expand monitoring scope and depth to address additional use cases. Managed services may be needed to allow 24/7 monitoring, analysis and response.

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, 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.

Analysis

Critical Capabilities Use Case Graphics

Figure 1. Vendors' Product Scores for Compliance Use Case

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

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services 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 for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services 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.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

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

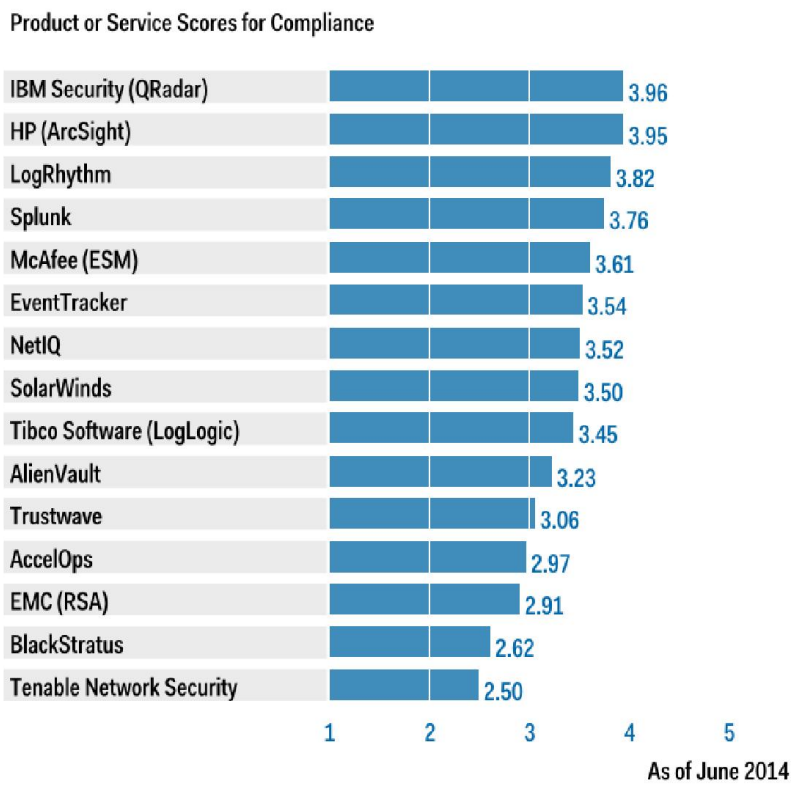
3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

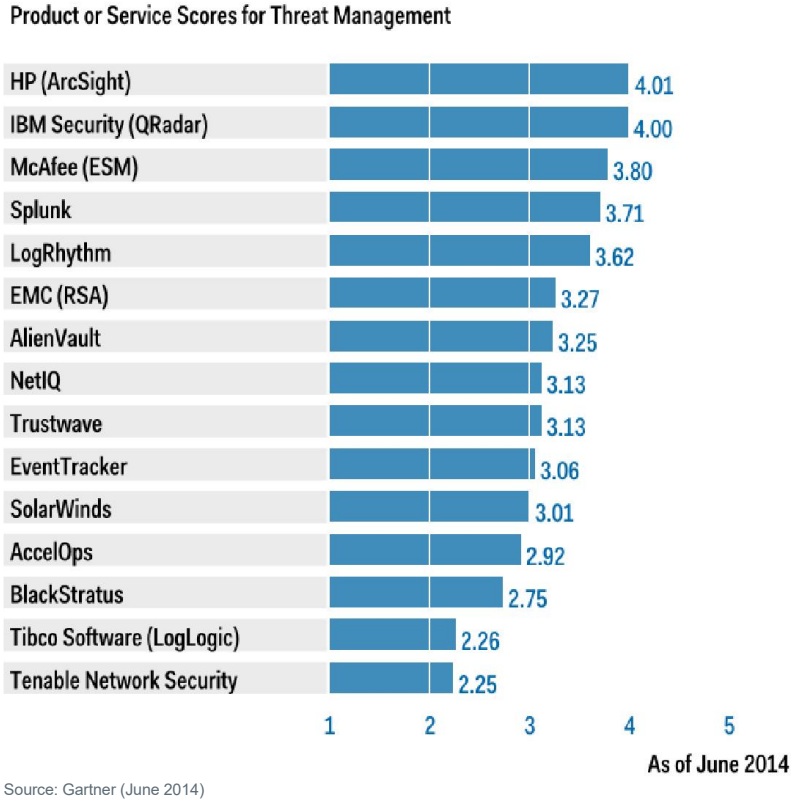
To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; 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 a product/service decision.



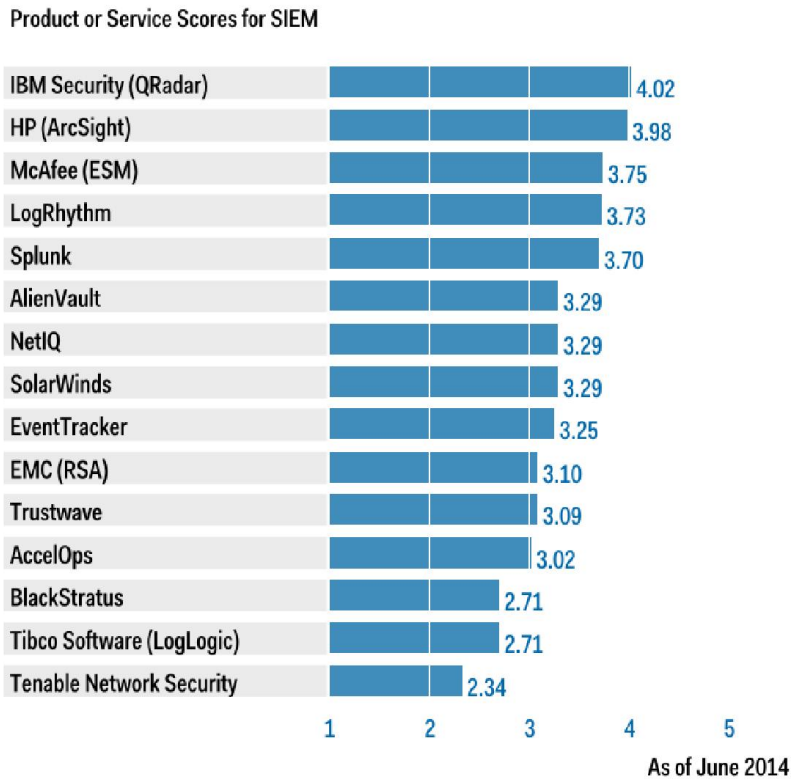
Source: Gartner (June 2014)

Figure 2. Vendors' Product Scores for Threat Management Use Case



Source: Gartner (June 2014)

Figure 3. Vendors' Product Scores for SIEM Use Case



Source: Gartner (June 2014)

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

Vendors

AccelOps

AccelOps primarily provides SIEM capabilities to the security organization and secondarily provides performance/availability monitoring (PAM) to IT operations. SIEM and PAM functions are delivered via a unified collection infrastructure and a common dashboarding environment. AccelOps is most often deployed by IT security areas to gain log management monitoring and analytics for security-oriented use cases. Because of the PAM capability, the technology is sometimes also championed and selected by the operations area as well.

Real-time monitoring: The AccelOps correlation rule language provides a unified framework for detecting patterns across security, performance, availability, compliance and change management scenarios.

Threat intelligence: AccelOps can ingest a variety of external threat data feeds, and can evaluate DNS look-ups and outbound flows to known malicious IP address ranges. There is also support for scheduled updates of external IP reputation data.

Behavior profiling: AccelOps provides statistical analysis that can be used to identify anomalies and deviations from normal behavior.

Data and user monitoring: Identity and access management (IAM) integration is limited to a collector for Active Directory, but user and group information is appended to events. AccelOps provides basic change detection functions via its own file integrity monitoring (FIM) and through integration with the Honeycomb FIM agent, but there is no integration with third-party FIM solutions. Basic support for database activity monitoring is provided, but it is oriented to availability and performance monitoring. There is no integration with database activity monitoring tools.

Application monitoring: AccelOps lacks specific support for application monitoring and does not support integration with third-party packaged applications.

Analytics: AccelOps provides standard support for the drill-down and display of event data in the context of event analysis, including data visualizations via heat maps, tree maps and scatter plots.

Log management and reporting: AccelOps uses a relational database to store structured data (such as device configuration and network topology) and indexed flat files for events. The log management function is designed to be tightly integrated with the SIEM and cannot be installed stand-alone. A large number of predefined reports are provided, covering security, availability and performance use cases. Some users indicate that the interface for report customization needs further development to improve usability.

Deployment/support simplicity: The product ships with a large number of predefined reports and correlation rules. The correlation rules are categorized as access/authentication, exploits, anomaly, policy violation and vulnerabilities.

Use cases: AccelOps is a good fit for end-user organizations and managed security service providers (MSSPs) that require a combination of security monitoring and PAM, and integrated CMDB capability.

AlienVault

AlienVault's security management software and appliance offerings provide SIEM, vulnerability assessment, NetFlow, network and host intrusion detection, and file integrity monitoring. AlienVault's commercial offering — the Unified Security Management (USM) platform — extends 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 the USM platform into three tiers to match the size of the end-user's environment.

Real-time monitoring: The AlienVault Correlation Engine provides real-time monitoring and correlation. Predefined correlation rules are provided for the suite's intrusion detection system (IDS) sensor data, and the company has recently expanded predefined rule content for third-party commercial products. However, some customers identify a need for an expansion of content for third-party commercial products.

Threat intelligence: AlienVault Labs provides threat intelligence content on a subscription basis for the commercial offering. 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 IAM systems, beyond basic Active Directory and LDAP monitoring. Local account changes can be monitored if AlienVault's host-based intrusion detection system (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 primarily with 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.

Deployment/support simplicity: AlienVault provides wizards and dashboards to support initial deployment, configuration and ongoing management of the included controls and sensors. Content updates for signatures for sensors, correlation rules, reports and incident response templates are available through the threat intelligence feed.

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.

BlackStratus

BlackStratus offers Log Storm and SIEM Storm, providing log management and security event management (SEM) capabilities to small and midsize businesses and MSSPs. SIEM Storm can be deployed in combination with Log Storm, utilizing it as the storage and collection tier, or it can be deployed stand-alone with a Vertica Analytic Database back end. Log Storm is available as a line of virtual or hardware appliances. SIEM Storm is available as software or a virtual image.

Real-time monitoring: Log Storm provides 66 predefined correlation rules, SIEM Storm 21, covering high-level categories such as access/authorization, exploits and suspicious activity. A wizard can be used to create custom correlation rules, and nonevent data such as threat intelligence watch lists and vulnerability scan data can be included. SIEM Storm contains a built-in incident management system based on the SANS seven-step incident remediation process that has received positive feedback from users. The integrations are provided by the vendor with Remedy and Service Desk. Active Directory and LDAP can be used to populate workflow assignments. NetFlow collection is supported, for nonevent data collection from the network, but feedback has indicated it is only a basic implementation.

Threat intelligence: Open-source threat intelligence feeds such as DShield, Shadowserver and Spamhaus are supported.

Behavior profiling: Log Storm and SIEM Storm provide basic statistical anomaly detection capabilities.

Data and user monitoring: Integrations with McAfee, Fortinet, Sophos and GFI Software DLP solutions, as well as with Tripwire, Sophos and McAfee FIM, are supported. DB2, Oracle and SQL database can be monitored via audit trail logs and database collector agents, but third-party DAM integrations are not available.

Application monitoring: Log Storm and SIEM Storm can monitor Apache and IIS Web server logs. Integrations with FireEye and Mandiant, as well as Web application firewalls from F5, Barracuda Networks and Imperva, are supported. Nonsupported third-party applications can be included via custom API scripts.

Analytics: Tabular views can be filtered by event fields and support nested conditional expressions. Visualizations are provided in the form of bar and pie charts, and network maps. SIEM Storm can also replay and apply correlations to historical data.

Log management and reporting: Log Storm is a full-fledged log management solution, with features including chain-of-custody compliance and digital signing**.** Both Log Storm and SIEM Storm are shipped with over 500 predefined report templates covering compliance standards and common security use case, and Crystal Reports templates can be imported.

Deployment/support simplicity: SIEM Storm and Log Storm can be deployed as virtual machines, and include an installation wizard and a passive autodiscovery feature for data source integration. A Web Services API is available to import user, contact, asset and similar information. The Vertica Analytics Database also required installation and maintenance if used for back-end storage for SIEM Storm.

Use cases: MSSPs and users looking for a customizable, service-orientated SIEM solution should consider BlackStratus.

EMC (RSA)

RSA, The Security Division of EMC, has almost completed the transition from enVision to RSA Security Analytics (SA), which is a SIEM solution that is based on the NetWitness platform. RSA SA provides log and full packet data capture, security analytics and basic security monitoring. RSA will support the enVision platform until the end of 2017. 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: During 2Q13, RSA released Event Stream Analysis (ESA), a correlation engine for the SA platform. There are 198 application rules and 75 complex correlation rules provided, and there is a user interface for rule customization. SA currently lacks native support for remediation workflow, but there is an integration with the Archer Security Operations Management module. A generic email integration interface can be used for third-party incident management systems.

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 watchlists for contextual analysis.

Behavior profiling: Support for behavior profiling is limited to basic deviation from a moving average.

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: During 2013, RSA augmented keyword search into raw data with basic data visualization capabilities.

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. Initial support for language localization is planned for 2013.

Deployment/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, but feedback from clients, prospects and current RSA customers indicates that a high degree of deployment complexity remains.

Use cases: RSA SA is ideally suited to organizations that have high-security requirements, have a need for forensics analysis and reporting for both log and packet capture data, and possess a well-staffed security organization capable of configuring and maintaining a complex monitoring technology.

EventTracker

EventTracker's SIEM software solution is targeted to SMBs and provides real-time monitoring and log management. The EventTracker Windows agent provides support for file integrity monitoring and USB control. Agents are also available for Solaris and AS/400. EventTracker also offers SIEM Simplified, a set of services (daily incident review, daily or weekly log review, weekly configuration assessment review, incident investigation, and audit assistance), delivered via remote access to the EventTracker instance running on customer premises. There is an option for continuous monitoring via a service provider partner.

Real-time monitoring: EventTracker provides SEM functions that are easy to customize and deploy. While the primary focus is security monitoring, there is also support for basic availability and performance monitoring as well.

Threat intelligence: EventTracker provides basic integration with threat intelligence feeds through a scripting interface that enables acquisition and import into watch lists.

Behavior profiling: EventTracker includes a behavior analysis module that provides profiling and anomaly detection functions.

Data and user monitoring: EventTracker provides an Active Directory Knowledge Pack that contains real-time alerts for user administration events. There is also integration with standard network authentication technologies. These limited IAM sources are dominant in the SMB space. The Windows agent provides USB device audit and control functions. File integrity monitoring is provided for the Windows platform via an optional Change Audit function. Integration with multiple third-party FIM solutions is also provided. EventTracker can directly monitor database audit logs. There is also integration with Imperva.

Application monitoring: Integration with packaged applications is not currently provided but is in development.

Analytics: Support for analytics is provided through keyword search functions and via a datamart feature called EventVault Explorer, where the user can export selected data into an external Microsoft SQL database and then query via the search interface or directly via SQL.

Log management and reporting: Log management capabilities are provided, and they are integrated with the solution. A large number of predefined reports are provided for compliance reporting.

Deployment/support simplicity: EventTracker provides technology that is well-suited to its target market, requiring only light customization through easy-to-use interfaces. In addition, EventTracker offers SIEM Simplified, a low-cost, co-managed SIEM service offering that provides basic remote monitoring and incident management.

Use cases: EventTracker is well-suited to smaller enterprises that require basic 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 or co-managed services.

HP (ArcSight)

HP ArcSight provides three SIEM offerings:

- ArcSight Enterprise Security Manager (ESM) software for large-scale event management
- ArcSight Express: Appliance for SIEM functions for small and midsize deployments
- ArcSight 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 ESM provides the capabilities needed for large-scale, SEM-focused deployments, but it has been complex to implement and manage. ESM version 6.0c (released 1Q13) replaced a major source of complexity and cost — the Oracle Database — with the purpose-built Correlation Optimized Retention and Retrieval (CORR) Engine. ArcSight Express is an appliance-based offering for ESM 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 Reputation Security Monitor (RepSM) is an optional component that receives near-real-time reputation feeds from HP research labs. Threat response manager is an add-on component that can perform network threat mitigation based on event triggers from ArcSight RepSM and other third-party security solutions.

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 database audit and protection (DAP) products, and supports direct collection from database audit logs. There is no native FIM or DLP capability. An integration with Autonomy Intelligent Data Operating Layer (IDOL) enables risk evaluation of data access observed by ArcSight.

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. In 4Q13, HP introduced Application View 1.0, which enables application activity monitoring that is not dependent on log data. HP Fortify Runtime technology is used

and implements a JAR file that runs with the application on the application server. It monitors method calls by the application, with over 40 discrete activities monitored out of the box. There is also a customization interface for transaction monitoring.

Analytics: ESM provides trend analysis functions. ESM query performance and resource efficiency has been improved via the CORR-Engine. ArcSight has integrations with Business Service Management, and there are ArcSight connectors for Hadoop and Autonomy. Risk Insight 1.0 is an ESM add-on and is a visualization tool for security event analysis.

Log management and reporting: The ArcSight Logger line of appliances, software and collectors provides 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 Sarbanes-Oxley Act [SOX], PCI, North American Electric Reliability Corp. [NERC] and the U.S. Federal Information Security Management Act [FISMA]). These packages are installed on top of Logger or ESM.

Deployment/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.

HP released ArcSight Express 4.0, which integrates SIEM, RepSM threat intelligence, IdentityView and connector management in a single appliance. This release focused on simplifying the installation and setup process to reduce deployment and operational complexity.

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 Security (QRadar)

IBM Security QRadar can be deployed as all-in-one solutions for smaller environments, or it 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. IBM Security 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 auto update 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 Security provides an integration of X-Force IP Reputation data into QRadar that can be refreshed on a daily 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 SiteProtector deployments by adding NetFlow and anomaly detection to the SiteProtector 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 Technologies, Novell and others. DAM is supported through direct monitoring of major DBMS logs and through integration with third-party database monitoring products from IBM InfoSphere 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 QFlow sensors.

Analytics: Analytics are supported directly from QRadar distributed event data. Customers report acceptable query response times in large deployments. QRadar has two-way integration 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. These reports can be augmented with security configuration compliance reporting via Risk Manager and vulnerability reporting with Vulnerability Manager (or third-party vulnerability-scanning products).

Deployment/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 threat management and compliance use cases for modest, as well as large-scale, deployments. 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.

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, event management and real-time analytics. In larger environments, it can be scaled as a set of specialized appliances and/or software instances (log management, event management and real-time analytics).Network forensic capabilities such as deep packet inspection and flow monitoring are supported via LogRhythm's Network Monitor. The technology also includes optional agents for major OSs that can be used for filtering at the source and to provide capabilities such as file and host activity monitoring.

Real-time monitoring: General feedback on correlation capabilities from existing LogRhythm customers has remained positive. Predefined monitoring rules doubled in 2013 to more than 500, and new modules providing specialized correlation rules, saved searches and dashboards for specific threats and topics such as privileged user monitoring, network anomaly detection and advanced persistent threats (APTs) were added. Network Monitor adds network traffic monitoring and forensic capabilities and allows correlation with log-based sources. Case and incident management for computer incident response team (CIRT)/security operations center (SOC) environments are planned for release in 2014.

Threat intelligence: LogRhythm provides an integration interface for open-source as well as commercial threat intelligence sources, but no specific support for commercial feeds. LogRhythm also provides its own threat intelligence via the LogRhythm Advanced Intelligence (AI) Engine, and the size of the in-house research team was increased twofold in the past year. Threat intelligence data can be referenced in analytics rule sets, alarm rules and reports. LogRhythm monitors all supported threat intelligence sources, and stages updates that can be pulled by customers.

Behavior profiling: Behavioral profiling and anomaly detection are supported via event and log sources, as well as network monitoring via Network Monitor. Monitoring against whitelists, average trends, rate trends and histogram trends is supported, as is the ability to create behavioral whitelists and baselines from host, application and user data, as well as Network Monitor session data.

Data and user monitoring: In addition to integration with Active Directory and standard network authentication sources, there are integrations with IAM technologies from CA Technologies, IBM, NetIQ and Oracle. The recently added Identity Inference Engine adds missing identity information to anonymous log data. 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's PeopleSoft, and a variety of other ERP and HR applications. There are also integrations with Web application servers and firewalls. Network Monitor adds application awareness via deep packet inspection and application identification for more than 2,000 applications.

Analytics: Search and structured analysis can be done directly via query language, or by drilling down from dashboard widgets. These can be customized to provide use-case specific views, visualizations and analytics, and can accommodate data point pivoting and filtering.

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 160 additional report templates that can be used to create custom reports.

Deployment/support simplicity: 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 has remained positive after the new UI design.

Use cases: LogRhythm is optimal for organizations that require balanced SIEM capabilities combined with privileged user monitoring, FIM, and network monitoring to support security operations and compliance use cases.

McAfee (ESM)

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

Real-time monitoring: McAfee ESM supports rule-based and risk-based correlation. Data from event and log sources, dynamic watch lists and threat intelligence can be used for correlation. The McAfee Advanced Correlation Engine (ACE) adds the capability to correlate NetFlow and event data, and run correlations against historic data.

Threat intelligence: McAfee Global Threat Intelligence for ESM provides threat context and is available as an additional module. McAfee ESM also supports the integration of third-party threat intelligence services via dynamic watchlists.

Behavior profiling: The McAfee ESM correlation engine supports statistical and baseline anomaly detection, as well as risk-based correlations. McAfee Application Data Monitor provides network anomaly detection, and McAfee Advanced Correlation Engine can be used to correlate and profile network and event data.

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 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 DEM provides network- and agent-based database activity monitoring functions. McAfee ESM can also directly monitor database audit logs, and ESM is integrated with McAfee Vulnerability Manager for databases, McAfee Virtual Patching for Databases, as well as Guardium and Imperva using Common Event Format. For FIM, there is integration with McAfee Application Control and with several third-party FIM products. The McAfee 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 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's PeopleSoft are supported via a direct integration. Support for industrial control systems and SCADA servers is also provided.

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. A Hadoop connector is available.

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

Deployment/support simplicity: References have validated that ESM is relatively easy to deploy and maintain. Deployment complexity can be increased when using multiple add-on products, but all-in-one appliances are offered for smaller deployments. User feedback regarding support has generally been good, but some have indicated challenges reaching the right point of contact.

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 database activity monitoring, 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. Users already using McAfee ePolicy Orchestrator (ePO) and other McAfee products should also consider McAfee ESM.

NetIQ

NetIQ Sentinel is composed of three packages: the Sentinel Server, Sentinel Log Manager and Change Guardian. All three packages are offered as software as well as virtual appliance deployments. Optional host agents are also available. 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: At the time of this review, there were no specific integrations with IP reputation or other external threat intelligence feeds, although the vendor introduced packaged threat intelligence feeds in the 7.2 version of Sentinel released in June 2014.

Behavior profiling: Sentinel, starting with version 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 InfoSphere 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's PeopleSoft. Sentinel can monitor several Web application servers.

Analytics: Sentinel provides a Web-based interface into full-text indexed search functions. The relational database used in prior versions was replaced in Sentinel 7 with a more efficient data store. Users report substantial improvements in ad hoc query performance.

Log management and reporting: Sentinel Log Manager provides log data collection, storage, archiving and reporting as a subset of Sentinel. NetIQ offers a package that includes only Log Manager to address stand-alone log management use cases.

Deployment/support simplicity: Sentinel 7 introduced major improvements in install packaging and report customization. During 2H13, NetIQ introduced a common administrative interface for the multiple components of Sentinel with version 7.1.

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.

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 provides a small number of watch lists, such as known bad/good process names and common administrative account names. These are included with product updates. LEM users can import threat feed and watchlist information for use in correlation rules, real-time monitoring or queries.

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. LEM provides no support for integration with external data warehouse or big data technologies, as SolarWinds reports that its SMB customers have not expressed demand for these capabilities.

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/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.

Use cases: SolarWinds LEM is well-suited to smaller organizations 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.

Splunk

Splunk provides log management, analytics and statistical commands that facilitate real-time correlation and visualization. Running on Splunk Enterprise, 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 and internal 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 databases, including DShield and CentralOps.net's Domain Dossier. Since the last evaluation, Splunk released the threat intelligence framework, which maps multiple feeds into a single framework to enable deployment into common watchlists. There is a filter parser to enable elimination of noisy entries, and a Norse intelligence feed is included.

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 basic FIM functions (essentially change detection), and there is also integration with Tripwire, OSSEC and FileTrek. In 2013, Splunk released predefined mapping support for third-party DLP products from RSA and Symantec. For DAM, the Splunk DB Connect app provides predefined mapping support for Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase and others. During 2013, Splunk released predefined mapping support for the major third-party DAM products.

Application monitoring: A common use case for Splunk is application management — monitoring in-house-developed and commercial applications through keyword searches to correlate and visualize 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. During 2013, Splunk introduced new visualizations for security metrics, threat analytics and predictive analytics. Hunk: Splunk Analytics for Hadoop and NoSQL Stores uses batch loading and does not require Splunk event collection infrastructure.

Log management and reporting: We note increased deployment of, and interest in, Splunk both as a companion technology to existing SIEM deployments, and as a 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 a SIEM, including predefined reports to support security monitoring and compliance reporting use cases. Reporting has been improved through predefined data models and pivot tables.

Deployment/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 have typically required more customization effort than other SIEM products. During 2013, Splunk has improved ease of use by increasing the number of predefined correlation rules and by implementing a customization interface that is an alternative to the search command line. There are now more than 20 predefined data models that correspond to common event sources, and a data model builder function has been added. With data models, a user can now build reports without knowledge of the Splunk query language. Splunk has 68 prebuilt security indicators and 200 predefined reports/panels that can be used to construct a custom dashboard. There are now 40 predefined dashboards in the security domains menu.

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 continues to improve the predefined security use-case support in the Splunk App for Enterprise Security, but the product can still be extensively customized by expert users.

Tenable Network Security

Tenable Network Security's focus in this market is evolving to emphasize continuous compliance monitoring based on endpoint state (vulnerabilities and configuration), file activity, network activity and log data. This evolving emphasis is to augment or complement a broad SIEM deployment, although there are overlapping use cases. Tenable Network Security delivers SIEM as a component of its suite of security products that also include vulnerability and configuration assessment and basic file integrity monitoring. Log Correlation Engine (LCE) provides log and event collection, NetFlow monitoring, normalization, analysis and reporting. The Nessus Vulnerability Scanner provides active vulnerability assessment, and the Passive Vulnerability Scanner (PVS) provides passive network traffic monitoring. Windows and Unix log collection agents can also provide basic file integrity and change monitoring. SecurityCenter Continuous View (SCCV) provides a console environment and the ability to correlate events with data from Nessus and PVS. SCCV, LCE, Nessus and PVS are available as software, and SCCV, Nessus and PVS are also available as hardware or virtual appliances.

Real-time monitoring: SCCV provides the framework for monitoring by integrating log collection and correlation with vulnerability scan and network monitoring technologies. Network monitoring is available via the NetFlow and raw traffic monitoring capabilities of LCE, or is enhanced through integration with LCE and the passive network traffic monitoring provided by PVS.

Threat intelligence: Tenable Network Security's threat intelligence integration includes support for parsing and import of a small number of specific IP reputation data feeds directly into watchlists and also includes vulnerability assessment scan or PVS detection of sessions with malicious hosts.

Behavior profiling: SCCV profiles events and will alert on statistically significant changes in activity.

Data and user monitoring: Tenable Network Security does not provide integration with IAM policy sources, but is able to extract user identity information from logs. Windows and Unix log collection agents can provide basic file integrity and change monitoring, and integration with a few third-party FIM solutions such as Tripwire. Tenable Network Security supports direct monitoring of database audit logs, but there is no integration with third-party database activity monitoring technologies.

Application monitoring: Integration with packaged applications is not currently provided but is in development.

Analytics: Support for analytics is provided through SCCV keyword search functions and an optional visualization module. Integration with external data warehouses is not currently supported.

Log management and reporting: Log management capabilities are provided by LCE. A moderate number of user-configurable predefined reports are provided for security use cases, and major regulations are covered with a modest number of predefined compliance reports.

Deployment/support simplicity: Tenable Network Security provides SIEM technology that is well-suited to its target market, namely customers that are already Nessus users and are comfortable with some tasks that require edits of parameter files.

Use cases: Tenable Network Security's SIEM solution is a good choice for organizations that want to extend the scope of a Nessus deployment to include security monitoring. Tenable Network Security offers a combination of very capable vulnerability assessment and basic SIEM and file integrity monitoring capabilities integrated under a single administration and reporting interface at a low cost.

Tibco Software (LogLogic)

Tibco Software's (Tibco's) LogLogic Log Management Intelligence solution provides log management, searching and alerting functions, and reporting for regulatory compliance and 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. Tibco also offers additional extensions such as LogLogic Compliance Manager and LogLogic Analytics. Virtual appliances are available, and LogLogic Compliance Manager is also packaged as a software offering.

Real-time monitoring: The log management appliances provide alert functions based on characteristics of the log event stream. LogLogic Analytics provides real-time monitoring and event correlation. More advanced capabilities require Tibco Iris or Tibco BusinessEvents.

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 a historical traffic baseline profile for each log source based on the 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 via integrations with McAfee Vulnerability Manager for Databases and IBM InfoSphere Guardium, and with LogLogic Analytics directly from database audit logs. LogLogic has integrated with a number of DLP solutions, including Symantec, RSA, McAfee and CA Technologies. There is an integration with Tripwire for file integrity monitoring.

Application monitoring: LogLogic's supported application sources can best be described as "infrastructure level" (such as Web application servers and application gateways). There is a limited file pull integration with SAP. NetFlow v.5 and v.9 are supported, and there are integrations with third-party Web application firewalls such as Cisco IronPort, Palo Alto Networks and Fortinet.

Analytics: Basic analytics are supported directly from LogLogic's LX, MX and ST and virtual appliances, and from software offerings such as Compliance Manager. Integration with Tibco SpotFire (LogLogic Analytics) 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 150+ reports and 100 alerts, and also provides compliance dashboards and workflow functions.

Deployment/support simplicity: Log management appliances are straightforward to deploy, and virtual appliance images are also available. Additional components and add-ons such as Compliance Manager and LogLogic Analytics can be deployed as software only. 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. Customers already using or planning to use other Tibco offerings will also benefit from using LogLogic as the log collection and management tier.

Trustwave

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

Trustwave has three primary offerings: SIEM Enterprise and Log Management Enterprise, each available as virtual or hardware appliance lines; and SIEM Operations Edition (OE), a software-only offering aimed at large organizations and MSSPs. The vendor also offers traditional managed security services through its security operations centers running the SIEM OE product, and the Managed SIEM offering that includes customer premises Log Management Appliances.

Real-time monitoring: Trustwave SIEM Enterprise and OE support event and log data via agent and agentless collection, NetFlow data, as well as contextual information such as threat intelligence and vulnerability assessment results for real-time correlation and alerting. Trustwave SIEM Enterprise ships with 79 customizable correlation templates.

Threat intelligence: Trustwave Threat Correlation Services is available as an add-on product for Trustwave SIEM Enterprise, SIEM OE and Log Management Enterprise. The service provides threat intelligence from a mix of open-source and commercial feeds, and also includes contributions from Trustwave SpiderLabs research.

Behavior profiling: SIEM Enterprise and OE both provide basic statistical analysis, trending, profiling and deviation from baseline anomaly detection capabilities.

Data and user monitoring: Trustwave SIEM Enterprise and SIEM OE can integrate with Microsoft Active Directory and Oracle Identity Analytics to support user and identity mapping, and IAM policy

change monitoring. Trustwave DLP can be integrated, and FIM is included on the Log Management appliance line. DAM is supported via JDBC connectors and audit trail logs.

Application monitoring: Third-party application monitoring capabilities are based on syslog and flat file ingestion, with the Active Response API available for deeper integrations.

Analytics: Customizable dashboards and visualization, and investigation tools such as the LogExplorer and EventExplorer, provide access to raw and normalized log and event data. SIEM Enterprise and SIEM OE also support posthoc statistical analysis, trending and profiling.

Log management and reporting: Trustwave's Log Management Appliances, Log Management Enterprise, Log Management Operations, and Log Collector are available as virtual and physical appliances. Agent and agentless collection are supported, with FIM capabilities included in the agent. Reporting is also included, with templates provided for common compliance standards.

Deployment/support simplicity: Trustwave SIEM Enterprise and Log Management are available as virtual and physical appliances, with SIEM OE available as software only. Deeper third-party integrations require usage of an API, but Trustwave also provides appropriate professional services.

Use cases: Users deploying SIEM for compliance use cases, especially in conjunction with PCI requirements, should consider Trustwave. Use cases where automated response capabilities are required should also review Trustwave SIEM and Trustwave's self-healing network offering.

Context

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 PCI or privileged user reporting for 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 their technology.

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.

In addition to the eight critical capabilities described in this research, organizations should evaluate the following four additional 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.

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.

Product/Service 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 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.

Critical Capabilities Definition

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).

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.

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.

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 a SIEM in the form of watchlists, correlation rules and queries in ways that increase the success rate of early breach detection.

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.

Behavior profiling employs a learning phase that builds profiles of normal activity for various event categories, such as network flows, user activity and server access.

The monitoring phase alerts on 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.

This capability establishes user and data context, and enables data access and activity monitoring. Functions include integration with IAM infrastructure to obtain user context and the inclusion of user context in correlation, analytics and reporting.

Data access monitoring includes monitoring of DBMSs and integration with FIM and DLP functions. DBMS monitoring can take three forms — parsing of DBMS audit logs, integration with third-party DAM functions or embedded DAM functions. FIM can be provided by the SIEM product directly or through integration with third-party products.

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.

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.

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.

Security event analytics are 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.

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.

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.

Deployment/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.

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: compliance, threat management and SIEM.

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.

Threat Management

The IT security organization has obtained funding for a 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.

SIEM

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 SEM capabilities.

Vendors Added and Dropped

Added

- AccelOps
- BlackStratus
- EventTracker
- Tenable Network Security

Dropped

- EiQ Networks
- Sensage
- Symantec

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]

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Compliance	Threat Management	SIEM
Real-Time Monitoring	2.0%	18.0%	15.0%
Threat Intelligence	2.0%	9.0%	10.0%
Behavior Profiling	2.0%	10.0%	7.0%
Data and User Monitoring	10.0%	10.0%	8.0%
Application Monitoring	2.0%	10.0%	6.0%
Analytics	2.0%	23.0%	8.0%
Log Management and Reporting	55.0%	10.0%	26.0%
Deployment/Support Simplicity	25.0%	10.0%	20.0%
Total	**100.0%**	**100.0%**	**100.0%**
			As of June 2014

Source: Gartner (June 2014)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated (see Table 2) on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Product or Service Ratings	AccelOps	AlienVault	BlackStratus	EMC (RSA)	EventTracker	HP (ArcSight)	IBM Sec (QR
Real-Time Monitoring	3.5	3.0	3.0	3.3	2.9	4.1	
Threat Intelligence	3.0	3.5	2.5	4.0	2.0	4.0	
Behavior Profiling	2.5	3.5	2.5	3.0	2.8	4.0	
	3.0	2.4	2.2	3.5	3.2	4.2	

Product or Service Ratings	AccelOps	AlienVault	BlackStratus	EMC (RSA)	EventTracker	HP (ArcSight)	IBM Secur (QRa
Data and User Monitoring							
Application Monitoring	2.9	3.6	2.9	4.0	3.2	4.5	4.
Analytics	2.4	3.2	2.9	3.3	2.9	3.8	3.
Log Management and Reporting	2.8	3.0	2.5	3.1	3.4	4.0	3.
Deployment/Support Simplicity	3.5	4.0	3.0	2.0	4.3	3.7	4.

Source: Gartner (June 2014)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	AccelOps	AlienVault	BlackStratus	EMC (RSA)	EventTracker	HP (ArcSight)	IBM Security (QRadar)	L
Compliance	3.00	3.23	2.62	2.91	3.54	3.95	3.96	
Threat Management	2.92	3.24	2.74	3.27	3.06	4.01	4.00	
SIEM	3.03	3.29	2.71	3.10	3.26	3.99	4.02	

Source: Gartner (June 2014)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1