The Forrester Wave™: Security Analytics Platforms, Q1 2017

Tools And Technology: The Security Architecture And Operations Playbook

by Joseph Blankenship

March 6, 2017

Why Read This Report

In our 36-criteria evaluation of security analytics (SA) providers, we identified the 11 most significant ones — BAE Systems, E8 Security, Fortinet, Hewlett Packard Enterprise (HPE), Huntsman Security, IBM, Intel Security, LogRhythm, RSA, Securonix, and Splunk — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

IBM, Splunk, LogRhythm, And RSA Lead The Pack

Forrester's research uncovered a market in which IBM, Splunk, LogRhythm, and RSA lead the pack. HPE, Securonix, E8 Security, Fortinet, and Intel Security offer competitive options, while BAE Systems and Huntsman Security have developing solutions that show great promise.

S&R Pros Are Looking For Better Threat Detection And Improved Operations

The security analytics market is growing because S&R pros increasingly trust security analytics providers to solve key challenges and act as strategic partners, advising them on top S&R decisions.

Vendors Have Improved Detection; User Behavior And Endpoint Analytics Differentiate

First-generation security information management (SIM) solutions never lived up to their promise to detect threats. Traditional SIM vendors are increasing the variety of data sources and integrations while adding advanced detection technologies.

The Forrester Wave™: Security Analytics Platforms, Q1 2017

Tools And Technology: The Security Architecture And Operations Playbook

by Joseph Blankenship
with Stephanie Balaouras, Bill Barringham, and Peter Harrison
March 6, 2017

Table Of Contents

Related Research Documents

Counteract Cyberattacks With Security Analytics

Market Overview: Security User Behavior Analytics (SUBA), 2016

Vendor Landscape: Security Analytics (SA)

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Security Analytics Is Essential For Monitoring, Alerting, And Operations

Security analytics platforms give S&R pros the ability to detect, investigate, and respond to cybersecurity threats.[1] Speeding detection and hastening the investigation process enables faster response, lessening the impact of cyberattacks. Forrester surveys indicate that 74% of global enterprise security technology decision makers rate improving security monitoring as a high or critical priority.[2] Vendors are adding security analytics features to existing solutions, and newer vendors are building SA solutions that leverage newer technologies without the baggage of legacy solutions. SA solutions enable S&R pros to:

- **Detect previously unknown threats.** Advanced detection technologies like machine learning and behavioral anomaly detection identify threats without the need for rules or signatures. Rules are still used to detect known threats, but the added detection capabilities of machine learning and behavioral anomaly detection can identify and alert on potentially malicious activity. For example, an external attacker may use compromised user credentials to access a system, but once the system starts to exhibit abnormal behavior, it will be flagged as suspicious. The need for more advanced detection capabilities has been so great that this is where SA vendors have focused much of their development efforts, and, today, detection capabilities have increased dramatically across the vendor landscape.
- **Search for threats in archived logs.** S&R pros can use analytic tools for threat hunting in archived logs. As vendors release new analytics in response to newly discovered malware and other threats, S&R pros can apply them to existing logs to identify those threats.
- **Monitor activities inside the network.** SA solutions ingest and correlate data from multiple disparate sources such as applications, data loss prevention (DLP), endpoints, identity and access management (IAM), and network flow data, providing necessary insight into user and device activity. Features like security user behavior analytics (SUBA) provide insight into user activity to identify malicious users and compromised accounts.[3] Carefully examining network traffic helps to identify signs of malicious behavior like compromised accounts or infected endpoints. This is one area where a high degree of differentiation still remains among vendor solutions.
- **Investigate alerts more quickly.** Added context, visibility, and threat intelligence give security analysts more information on which to act. And added workflow and automation provide a necessary productivity boost to understaffed security teams. When opening an alert, the solution may provide an analyst with context about the alert, the device, and the user as well as threat intelligence related to the alert and a link graph showing other systems with which the device is communicating. Built-in workflow and automation can recommend next steps and automate actions to speed investigations and remediation. Surprisingly, not all vendors we evaluated could integrate vulnerability management data.
- **Improve operations.** Many enterprises employ SIM solutions at the heart of their security operations center. Current tools lack workflow management and automation, forcing analysts to use spreadsheets and email to track investigations and communicate. With security talent at a

premium, S&R teams have to increase analyst productivity. SA solutions are employing security automation and orchestration (SAO) tools, helping make operations more efficient and move toward automated response.[4] However, our analysis shows that SA vendors still have a lot of work to do in SAO, as no vendor scored highly in our evaluation criteria. This is indicative of just how nascent the technology and capabilities still remain, and it's likely that specialized solutions will have room to grow.

› **Comply with regulations and standards.** Compliance support for standards and regulations like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), ISO 27002, North American Electric Reliability Corporation standards for critical infrastructure protection (NERC CIP), Federal Information Security Management Act (FISMA), and others is still a required use case for S&R pros responsible for compliance initiatives. Despite the perennial requirement for compliance, some of the newer SA vendors don't address this use case, preferring instead to focus on detection. This means that S&R pros who invest in these solutions will need separate solutions for compliance.

SIM Is Evolving Into Security Analytics

Traditional rules-based SIM systems have been around since the mid-1990s. To keep up with compliance mandates like the PCI DSS, S&R pros largely employed SIM solutions as log management and reporting tools.[5] When S&R pros did use them for monitoring and alerting, they did so primarily to look for outside intrusions. With the surge of cyberthreats and the accompanying proliferation of security tools, legacy SIM solutions were forced to evolve to keep up with the volume (see Figure 1). Forrester surveys indicate that 64% of global network security decision makers at enterprises have implemented or are expanding their implementation of SIM and SA (see Figure 2). SIM vendors are adding security analytics features such as:

› **Network analysis and visibility (NAV).** SIM vendors added NAV functionality to provide visibility into activity inside the network. NAV is a diverse tool set that includes network discovery, flow data analysis, network metadata analysis, packet capture and analysis, and network forensic tools.[6]

› **Security user behavior analytics.** Understanding user behavior is key for finding malicious insiders and compromised accounts. SIM vendors are adding SUBA as a feature or are partnering with SUBA vendors to deliver the capability. It's a key area of differentiation.

› **Big data infrastructure.** Originally built using relational databases, SIM solutions are evolving to include big data infrastructure to handle the massive volume of events and data sources they process and to remain competitive with standalone SA vendors that have built their platforms using big data infrastructure. Infrastructure, scalability, and the size of the largest deployment are key areas of differentiation among vendor solutions.

FIGURE 1 SIM Moves Toward SA

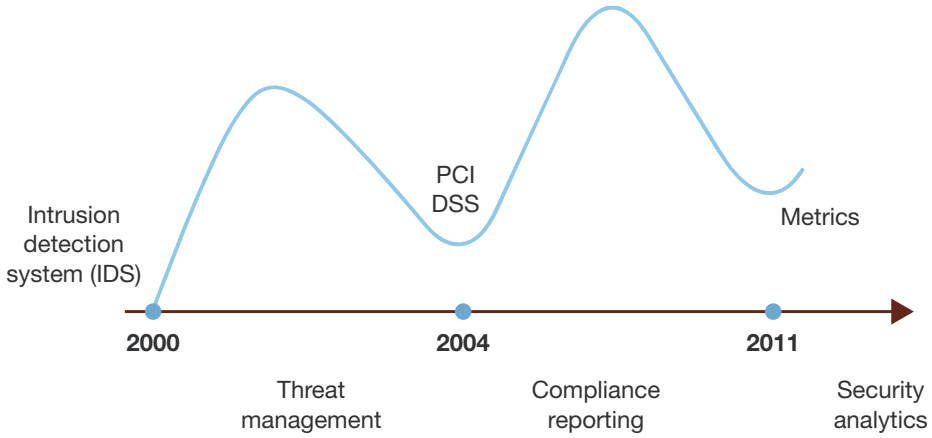
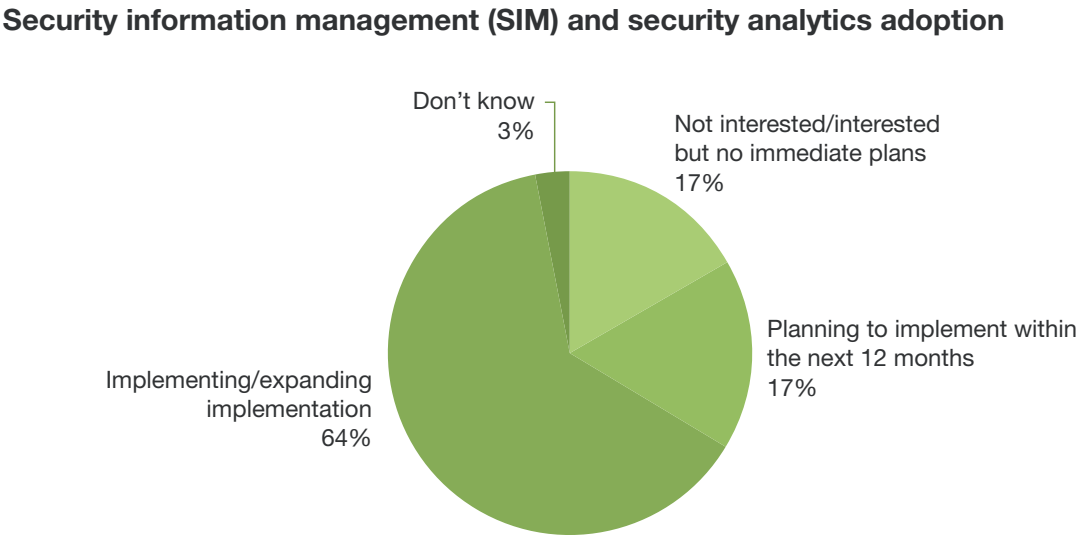


FIGURE 2 A Majority Of Firms Have Adopted SA



Base: 579 global network security decision makers (1,000+ employees)
Source: Forrester Data Global Business Technographics® Security Survey, 2016

Security Analytics Platforms Evaluation Overview

To assess the state of the SA market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top SA vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 36 criteria, which we grouped into three high-level buckets:

- **Current offering.** The vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current SA offering. We evaluated criteria such as infrastructure, deployment options, detection capabilities, risk prioritization, log management, threat intelligence, visibility, dashboards and reporting, flexibility, compliance support, workflow, security automation, end user experience, and customer satisfaction.
- **Strategy.** A vendor's position on the horizontal axis indicates the strength of its strategy. Factors we considered include product strategy, planned enhancements, technology partners, implementation size, delivery model, and pricing structure.
- **Market presence.** The size of each vendor's bubble on the chart indicates the vendor's market presence. We evaluated each vendor's installed base, staffing, and product line revenue.

Evaluated Vendors And Inclusion Criteria

Forrester included 11 vendors in the assessment: BAE Systems, E8 Security, Fortinet, HPE, Huntsman Security, IBM, Intel Security, LogRhythm, RSA, Securonix, and Splunk. Each of these vendors (see Figure 3):

1. **Has advanced detection capabilities.** The solution must utilize artificial intelligence, machine learning, or behavioral anomaly detection as a supplement to or replacement for rules-based detection.
2. **Has an enterprise client base.** Vendors must have enterprise customers using the solution as part of their security monitoring strategy.
3. **Delivers two or more SA components.** Vendors must deliver multiple SA components, such as big data infrastructure, SIM, SUBA, and NAV, as part of the SA solution.
4. **Delivers primarily as a product, not a service.** The vendor must offer a product version of the solution that was generally available prior to August 24, 2016. We only evaluated suite capabilities that were released and generally available to the public by this cutoff date.
5. **Has log archiving that supports PCI DSS compliance.** The solution must provide log storage in a format that supports compliance with PCI DSS.
6. **Has significant interest from Forrester customers.** Forrester considered the level of interest from our clients based on our various interactions, including inquiries, advisories, and consulting engagements.

FIGURE 3 Evaluated Vendors: Vendor Information And Selection Criteria

Vendor	Product evaluated
BAE Systems	BAE Systems Threat Analytics 2.0
E8 Security	Behavioral Intelligence Platform 1.6
Fortinet	FortiSIEM 4.7
Hewlett Packard Enterprise	HPE ArcSight User Behavior Analytics 5.0
Huntsman Security	Huntsman Analyst Portal 5.96
IBM	IBM Security QRadar 7.2
Intel Security	McAfee Enterprise Security Manager 9.6.0
LogRhythm	LogRhythm Security Intelligence and Analytics Platform 7.1
RSA	RSA NetWitness Suite 10.6.1
Securonix	Enterprise 5.0, SNYPR 5.0
Splunk	Splunk Enterprise 6.5, Splunk Enterprise Security 4.5

FIGURE 3 Evaluated Vendors: Vendor Information And Selection Criteria (Cont.)

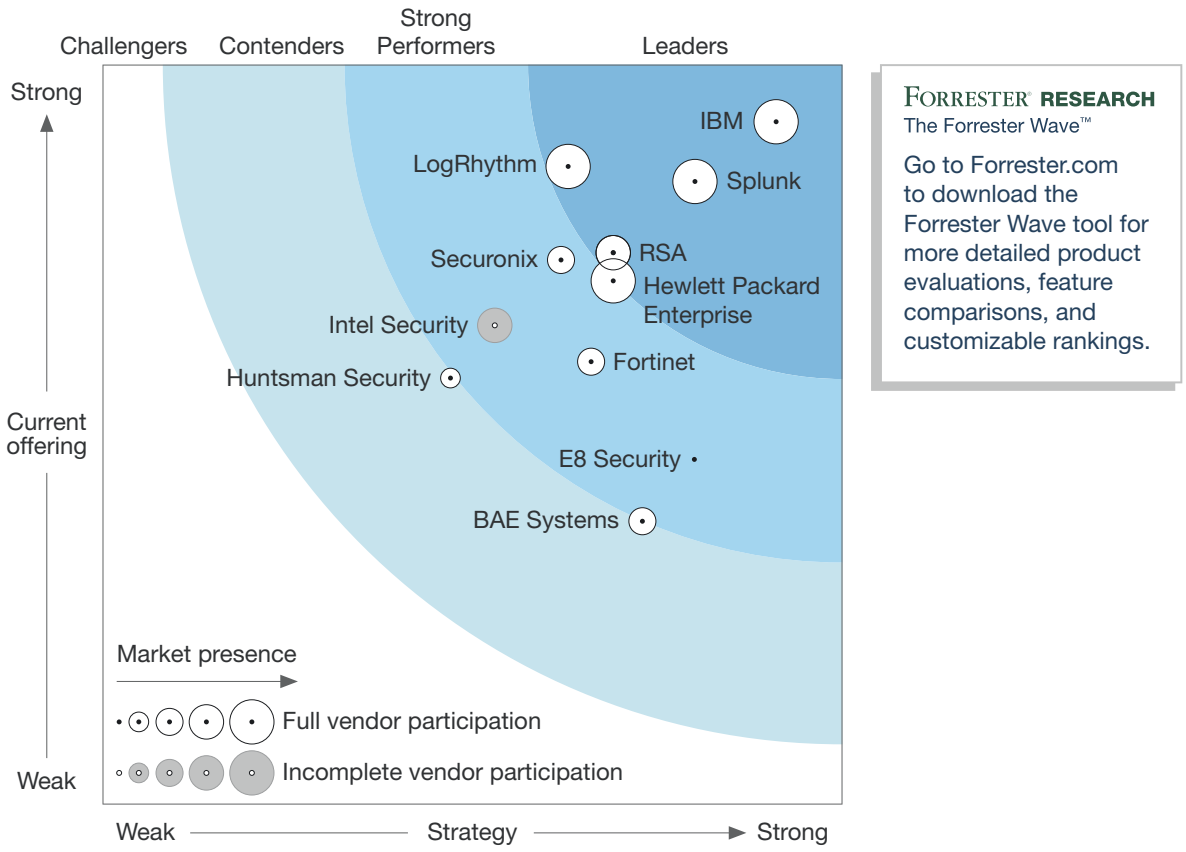
Vendor inclusion criteria

Each of these vendors:
1. **Has advanced detection capabilities.** The solution must utilize artificial intelligence, machine learning, or behavioral anomaly detection as a supplement to or replacement for rules-based detection.
2. **Has an enterprise client base.** Vendors must have enterprise customers using the solution as part of their security monitoring strategy.
3. **Delivers two or more SA components.** Vendors must deliver multiple SA components, such as big data infrastructure, SIM, SUBA, and NAV, as part of the SA solution.
4. **Delivers primarily as a product, not a service.** The vendor must offer a product version of the solution that was generally available prior to August 24, 2016. We only evaluated suite capabilities that were released and generally available to the public by this cutoff date.
5. **Has log archiving that supports PCI DSS compliance.** The solution must provide log storage in a format that supports compliance with PCI DSS.
6. **Has significant interest from Forrester customers.** Forrester considered the level of interest from our clients based on our various interactions, including inquiries, advisories, and consulting engagements.

Vendor Profiles

This evaluation of the SA market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 4).

FIGURE 4 Forrester Wave™: Security Analytics Platforms, Q1 '17



FORRESTER® **RESEARCH**
The Forrester Wave™

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

FIGURE 4 Forrester Wave™: Security Analytics Platforms, Q1 '17 (Cont.)

	Forrester's weighting	BAE Systems	E8 Security	Fortinet	Hewlett Packard Enterprise	Huntsman Security	IBM	LogRhythm	RSA	Securonix	Splunk
Current Offering	50%	1.90	2.32	2.98	3.53	2.87	4.61	4.30	3.72	3.67	4.20
Infrastructure	5%	5.00	5.00	3.00	3.00	1.00	5.00	5.00	3.00	5.00	5.00
Deployment options	2%	3.00	3.00	2.00	3.00	3.00	5.00	5.00	3.00	4.00	5.00
Supported data types	1%	3.00	5.00	3.00	5.00	3.00	5.00	5.00	4.00	4.00	3.00
Data connectors	2%	3.00	1.00	3.00	5.00	3.00	3.00	5.00	3.00	3.00	3.00
Custom data sources	5%	3.00	1.00	3.00	3.00	5.00	5.00	3.00	3.00	5.00	5.00
Correlation rules	11%	1.00	1.00	5.00	5.00	1.00	5.00	5.00	3.00	5.00	5.00
Real-time monitoring	12%	0.00	3.00	3.00	3.00	5.00	5.00	3.00	3.00	3.00	5.00
Detection technologies	1%	3.00	3.00	3.00	3.00	5.00	5.00	3.00	5.00	5.00	5.00
Risk scoring and prioritization	1%	3.00	3.00	2.00	4.00	2.00	3.00	5.00	3.00	4.00	4.00
User behavior analytics (UBA)	4%	3.00	5.00	1.00	3.00	3.00	3.00	5.00	5.00	5.00	3.00
Endpoints	10%	1.00	3.00	1.00	3.00	1.00	3.00	5.00	5.00	3.00	3.00
Integrated network analysis and visibility (NAV)	4%	3.00	3.00	1.00	3.00	3.00	5.00	5.00	5.00	3.00	3.00
Data exfiltration	1%	2.00	3.00	1.00	3.00	3.00	3.00	4.00	3.00	5.00	4.00
Log management	1%	3.00	4.00	4.00	3.00	3.00	5.00	4.00	4.00	4.00	5.00
Threat intelligence	1%	4.00	1.00	3.00	3.00	3.00	4.00	4.00	5.00	4.00	3.00
Vulnerability data	7%	0.00	0.00	3.00	3.00	3.00	5.00	5.00	3.00	3.00	3.00
Investigation and incident management	1%	3.00	2.00	3.00	2.00	3.00	5.00	4.00	4.00	3.00	3.00
Workflow	1%	3.00	2.00	3.00	3.00	2.00	4.00	4.00	4.00	4.00	4.00
Visibility	1%	3.00	3.00	3.00	3.00	3.00	5.00	3.00	3.00	5.00	3.00
Dashboards and reporting	4%	1.00	2.00	3.00	4.00	4.00	5.00	5.00	4.00	4.00	5.00
Flexibility	1%	5.00	3.00	3.00	3.00	3.00	5.00	3.00	3.00	5.00	5.00
Compliance	7%	0.00	0.00	3.00	5.00	3.00	5.00	5.00	3.00	1.00	3.00
Scalability	4%	3.00	1.00	3.00	5.00	3.00	5.00	3.00	5.00	3.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 4 Forrester Wave™: Security Analytics Platforms, Q1 '17 (Cont.)

	Forrester's weighting	BAE Systems	E8 Security	Fortinet	Hewlett Packard Enterprise	Huntsman Security	IBM	LogRhythm	RSA	Securonix	Splunk
Current Offering	50%	1.90	2.32	2.98	3.53	2.87	4.61	4.30	3.72	3.67	4.20
Geographic support	4%	5.00	1.00	5.00	5.00	3.00	5.00	5.00	5.00	3.00	5.00
Security automation	1%	2.00	2.00	3.00	2.00	3.00	4.00	4.00	3.00	1.00	4.00
End user experience	1%	2.00	3.00	4.00	2.00	4.00	5.00	3.00	4.00	3.00	5.00
Customer satisfaction	7%	3.00	5.00	4.00	2.00	3.00	5.00	3.00	4.00	5.00	5.00
Strategy	50%	3.65	4.00	3.30	3.45	2.35	4.55	3.15	3.45	3.10	4.00
Product strategy	5%	3.00	3.00	3.00	4.00	3.00	5.00	4.00	4.00	3.00	4.00
Planned enhancements	5%	3.00	3.00	3.00	4.00	3.00	5.00	5.00	4.00	4.00	4.00
Technology partners	15%	5.00	5.00	5.00	3.00	5.00	5.00	3.00	3.00	3.00	5.00
Implementation size	35%	3.00	3.00	1.00	5.00	1.00	5.00	3.00	3.00	3.00	5.00
Delivery/implementation model	35%	4.00	5.00	5.00	2.00	2.00	4.00	3.00	4.00	3.00	3.00
Pricing structure	5%	3.00	3.00	3.00	3.00	5.00	3.00	3.00	3.00	4.00	1.00
Market Presence	0%	2.20	1.00	2.20	5.00	1.40	5.00	4.60	4.60	3.00	4.60
Installed base	40%	3.00	1.00	2.00	5.00	2.00	5.00	4.00	4.00	2.00	4.00
Development, sales, and technical support staffing	20%	3.00	1.00	5.00	5.00	1.00	5.00	5.00	5.00	5.00	5.00
Product line revenue	40%	1.00	1.00	1.00	5.00	1.00	5.00	5.00	5.00	3.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

IBM, Splunk, LogRhythm, And RSA Are Leaders

› **IBM.** IBM has invested and continues to invest heavily in security with its QRadar Security Intelligence Platform as one of the key pieces of its portfolio. IBM has an ambitious strategy for security analytics that includes cognitive security capabilities from its Watson initiative and security automation from its Resilient Systems acquisition. IBM delivers security analytics on-premises, in the cloud, and as a managed service.

IBM continues to expand its offerings based on QRadar. While customers may realize benefits from integrated tools, they may not be as full-featured as standalone offerings from competitors. Large enterprises and those looking for advanced capabilities and a flexible deployment model should consider IBM.

› **Splunk.** Splunk Enterprise Security is a highly customizable add-on to Splunk Enterprise that delivers traditional SIM functionality with available add-ons for SUBA (through its Caspida acquisition) and analytics. The solution can be deployed on-premises, in public or private clouds, or as a hybrid configuration.

Enterprises widely deploy Splunk as a log management and search tool for infrastructure and operations use cases in addition to security use cases. Pricing and cost are frequent pain points for customers. S&R pros planning to deploy Splunk should pay special attention to estimating the amount of log data they plan to process so they aren't surprised by the consumption-based pricing model. Enterprises with advanced security teams and complex logging requirements should consider Splunk.

› **LogRhythm.** LogRhythm is the largest of the standalone pure-play SIM providers in the market. While its competitors have been acquired, reacquired, or spun off, LogRhythm remains independent, and it raised $50 million in new funding in August 2016.[7] LogRhythm provides a feature-rich platform that includes traditional SIM capabilities along with SUBA, file integrity monitoring (FIM), SAO, endpoint monitoring, and NAV functionality. The solution is available for on-premises deployment using LogRhythm appliances, customer-provided hardware, virtual infrastructure, or private cloud.

Although it's used by numerous enterprise and government organizations, we advise the very largest customers to ask the vendor to prove the solution can meet their desired scale. Midmarket and enterprise customers seeking visibility into their networks should consider LogRhythm.

› **RSA.** RSA, now part of Dell Technologies, provides SIM capabilities in combination with NAV, endpoint detection and response, and advanced analytics through its RSA NetWitness Suite (formerly RSA Security Analytics).[8] It provides threat detection and visibility through a combination of log and packet data analysis. The solution is delivered via on-premises software, hardware, or a mixed deployment. It monitors cloud environments, although cloud and software-as-a-service (SaaS) deployment are not supported.

The recent change of ownership may cause some disruption, although the ability to focus on its security and risk businesses may prove beneficial in the long run. Organizations looking for a high level of visibility into their network traffic should consider RSA.

HPE, Securonix, E8 Security, Fortinet, And Intel Security Are Strong Performers

› **HPE.** HPE is working to breathe new life into its once market-leading SIM solution as it prepares to spin off its Software Business Segment into a merger with Micro Focus that's expected to close in 2017.[9] HP acquired ArcSight in 2010, but it was unable to keep pace with innovations in the market, leaving long-term customers frustrated. Some of the largest enterprises in the world rely on ArcSight for security monitoring and logging, although many customers are looking for alternatives.

The future of the ArcSight platform is uncertain, although plans call for investment in bringing it up to date through enhancements and partnerships. For example, HPE has an OEM agreement with Securonix to provide its SUBA solution. Enterprises should watch the product road map closely to see if planned updates slip or if the new ownership loses focus on the product.

› **Securonix.** Securonix shows strength as a standalone security analytics provider. Its solution is delivered as Securonix SNYPR, which runs natively on Hadoop or as Securonix Enterprise for customers who want to deploy analytics on their own big data infrastructure or SIM deployment. The solution applies unsupervised machine-learning-based analytical techniques to detect anomalies and identify threat patterns to risk-rank insider threats and cyberthreats. It offers investigation capabilities using link analysis and visualization dashboards to explore linkages in data. The solution is delivered via software, appliance, virtual machine, or cloud deployment.

A smaller vendor with most of its customers in North America, Securonix is able to support some compliance use cases, although it doesn't have the depth of reporting and compliance support of a SIM solution. Users note complexity and pricing as issues, although customer satisfaction is well above average. Midmarket companies and enterprises looking for a flexible security analytics platform that can work as a standalone solution or in conjunction with current tools should consider Securonix.

› **E8 Security.** E8 Security is a standalone vendor that delivers SA via its Fusion Behavioral Intelligence Platform. The solution uses machine learning and multidimensional modeling to examine user, device, and network behaviors to identify anomalous activity. It also provides native visualizations between hosts, users, and behaviors to help analysts visually understand relationships. Users praise the solution for its time-to-value, detection accuracy, and product support. The solution is delivered as on-premises enterprise software that can be installed on an appliance or hosted in a private cloud.

E8 Security is a smaller vendor, with most of its customer base in the US. While the solution provides log management and long-term retention, it doesn't include reporting to support compliance use cases. Enterprises that need a robust analytics solution but don't require compliance reporting or localized support outside North America should evaluate E8 Security.

› **Fortinet.** Security vendor Fortinet purchased AccelOps in June 2016 and quickly rebranded the solution as FortiSIEM.[10] FortiSIEM delivers SIM functionality using in-memory event analytics and a distributed, real-time event correlation engine. Users give the solution high marks for its flexibility and reporting capabilities. The solution is delivered as a virtual appliance or as SaaS.

The acquisition by Fortinet will likely mean good things for FortiSIEM, as the solution lags behind competitors in areas like machine learning, visualization tools, and UI. FortiSIEM customers are mostly midsize enterprises. Midsize enterprises and those that need compliance support with a high degree of flexibility should consider FortiSIEM.

› **Intel Security.** Intel Security provides SIM through its McAfee Enterprise Security Manager (ESM) solution. ESM has a large customer base and integrates well with other parts of the Intel Security portfolio. It is delivered via physical appliance, virtual appliance, or hybrid deployment options. The optional McAfee Advanced Correlation Engine provides correlation without the need for rules, risk-based alerting, and historical data analysis.

With numerous enterprise customers, ESM has fallen behind other SIM solutions as part of Intel Security. Now that Intel Security has announced that it will spin out of Intel under its former moniker, McAfee, it will once again be a dedicated cybersecurity vendor.[11] With a much smaller enterprise security portfolio, Intel Security leadership indicates that it will be investing in ESM to bring it up to date. The road map calls for numerous enhancements, including a UI refresh, the addition of Elasticsearch, expanded analytics options, and improved workflow. Current ESM customers should watch road map announcements closely to take advantage of planned enhancements and ensure that they are being delivered as scheduled.

Forrester included Intel Security as a nonparticipating vendor in this evaluation.

BAE Systems And Huntsman Security Are Contenders

› **BAE Systems.** BAE Systems delivers the security analytics expertise it gained as a managed security services provider (MSSP) as a product in its threat analytics offering. The solution detects threats through correlation and analysis of endpoint and network data, giving analysts context via an investigation console. It provides unique graphical visualizations to show how entities are connected. BAE Systems Threat Analytics is delivered as on-premises software or as a managed service.

BAE Systems does not provide real-time security monitoring; it uses stored data for analysis instead. It also does not support any compliance use cases or supply reporting. Enterprises looking for an effective threat-hunting and investigation tool should evaluate BAE Systems.

› **Huntsman Security.** Australia-based Huntsman Security is building on its legacy as a government and defense solution. Many of its customers include government ministries, intelligence agencies, and defense departments. Huntsman Enterprise SIEM combines SIM capabilities with an SA solution — the Huntsman Analyst Portal. The Analyst Portal includes SA technologies, behavioral anomaly detection, and automation capabilities that can be used for threat verification, elimination of false-positives, and delivery of case files for threat resolution. A behavioral anomaly detection feature is available as an add-on to the base capability. The solution is delivered as a software application or virtual appliance, deployable via customer-supplied hardware or in a cloud environment.

Huntsman Security is not yet widely known in North America, with most of its customer base in Asia Pacific and Europe, the Middle East, and Africa (EMEA). Elements of the user interface are a little dated — likely a legacy of the solution's original government client base. Enterprises and government agencies with presence in Asia Pacific and EMEA that want to combine the strengths of security analytics and SIM should evaluate Huntsman Security.

Supplemental Material

Online Resource

The online version of Figure 4 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2016, was fielded from March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by January 2017.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls and surveys.** To validate product and vendor qualifications, Forrester also conducted or attempted to conduct reference calls or surveys with three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool.

The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] For a definition of security analytics platforms, see the Forrester report "Counteract Cyberattacks With Security Analytics."

[2] Source: Forrester Data Global Business Technographics Security Survey, 2016.

[3] See the Forrester report "Market Overview: Security User Behavior Analytics (SUBA), 2016."

[4] See the Forrester report "Rules Of Engagement: A Call To Action To Automate Breach Response."

[5] The PCI DSS was largely responsible for the growth of SIM in the mid-2000s. While compliance is not as strong of a driver for SA solutions, it remains an important use case for S&R pros. See the Forrester report "Market Overview: Security Information Management (SIM)."

[6] For more on NAV tools and how they detect threats inside networks, see the Forrester report "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility."

[7] Source: "LogRhythm Closes $50 Million Financing to Extend Global Leadership in Security Intelligence and Analytics," LogRhythm press release, August 30, 2016 (http://logrhythm.com/about/press-releases/logrhythm-closes-50-million-financing/).

[8] Source: "Historic Dell and EMC Merger Complete; Forms World's Largest Privately-Controlled Tech Company," Dell Technologies press release, September 7, 2016 (http://www.delltechnologies.com/en-us/press/dell-technologies-combination-announcement.htm).

In July 2016, RSA rebranded RSA Security Analytics to RSA NetWitness Suite. Source: "RSA Announces RSA NetWitness Suite Designed to Deliver the Fastest and Most Comprehensive Response to Advanced Attacks," RSA press release, July 28, 2016 (http://www.rsa.com/en-us/company/newsroom/rsa-announces-rsa-netwitness-suite-designed-to-deliver-the-fastest-most-comprehensive-response).

[9] Source: "HPE Accelerates Strategy With Spin-Off and Merger of Software Assets With Micro Focus," Hewlett Packard Enterprise press release, September 7, 2016 (http://www.hpe.com/us/en/newsroom/news-archive/press-release/2016/09/1276021-hpe-accelerates-strategy-with-spin-off-and-merger-of-non-core-software-assets-with-micro-focus.html).

[10] Source: "Fortinet Announces Acquisition of AccelOps," Fortinet press release, June 7, 2016 (http://www.fortinet.com/corporate/about-us/news-events/press-releases/2016/fortinet-announces-acquisition-of-accelops.html).

[11] See the Forrester report "Quick Take: Intel Spins Off McAfee As Synergies Fail To Materialize."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.