The Forrester Wave™: Security Analytics Platforms, Q3 2018

The 13 Providers That Matter Most And How They Stack Up

by Joseph Blankenship
September 21, 2018

Why Read This Report

In our 30-criteria evaluation of security analytics platforms providers, we identified the 13 most significant ones — AlienVault, Exabeam, Fortinet, Gurucul, Huntsman Security, IBM, LogRhythm, McAfee, Micro Focus, Rapid7, RSA, Securonix, and Splunk — and researched, analyzed, and scored them. This report shows how each provider measures up and helps S&R professionals make the right choice.

Key Takeaways

LogRhythm, IBM, Splunk, And RSA Lead The Pack

Forrester's research uncovered a market in which LogRhythm, IBM, Splunk, and RSA are Leaders; Securonix, Exabeam, McAfee, Gurucul, Huntsman Security, and Micro Focus are Strong Performers; Fortinet and Rapid7 are Contenders; and AlienVault is a Challenger.

S&R Pros Are Looking To Make SA Platforms The Centerpiece Of Their Operations

The security analytics platform market is growing because more S&R professionals see these platforms as a way to address their top cybersecurity challenges. This market growth is in large part due to security teams using security analytics platforms as the centerpiece of their security operations.

Customization, Integrations, And Data Security Are Key Differentiators

As legacy security information management (SIM) technology becomes outdated and less effective, improved customization and flexibility will dictate which providers will lead the pack. Vendors that can provide customization, integrations, and data security position themselves to successfully deliver flexibility, increased coverage, and data protection to their customers.

The Forrester Wave™: Security Analytics Platforms, Q3 2018

The 13 Providers That Matter Most And How They Stack Up

by Joseph Blankenship
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie

September 21, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Security Analytics Platforms, Q1 2017

Reduce Risk And Improve Security Through Infrastructure Automation

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 Platforms Are The New Generation Of SIM

Forrester has covered security information market (SIM) technology under the umbrella of security analytics (SA) for years. However, legacy SIM (AKA SIM 1.0) largely failed to deliver on expectations due to growing data volumes and infrastructure complexity.[1] Today's solutions have expanded from purely rules-based detection to include data science methods like machine learning and artificial intelligence.

Vendors call this SIM 2.0, next-generation SIM, or evolved SIM. We call it security analytics, to signify how much the technology has evolved from its days as a log management and rules-based detection platform. Enterprises continue to invest in SA platforms: 57% of global network path security decision makers at enterprises of more than 1,000 employees say they have already implemented, are in the process of implementing, or are expanding/upgrading their implementation of SIM and SA (see Figure 1). S&R pros invest because today's SA platforms:

- **Speed detection and response.** SA platforms give S&R pros the ability to detect, investigate, and respond to cybersecurity threats more quickly.[2] Speeding detection and hastening the investigation process enables faster response, lessening the impact of cyberattacks.
- **Detect previously unknown threats.** Advanced detection AI and data science techniques 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 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 SA vendors have focused much of their development efforts here over the past several years.
- **Enable threat hunting and forensics.** S&R pros can use analytic tools for threat hunting in archived logs. As vendors release new analytics and as new indicators of compromise (IOCs) emerge in threat intelligence, S&R pros can apply them to existing data to surface those threats. In the event of a security incident, forensics teams can leverage the data captured by SA platforms to determine what happened and what systems were impacted.
- **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.
- **Accelerate investigations.** Added context, visibility, and threat intelligence give security analysts more information on which to act. Workflow and automation tools 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

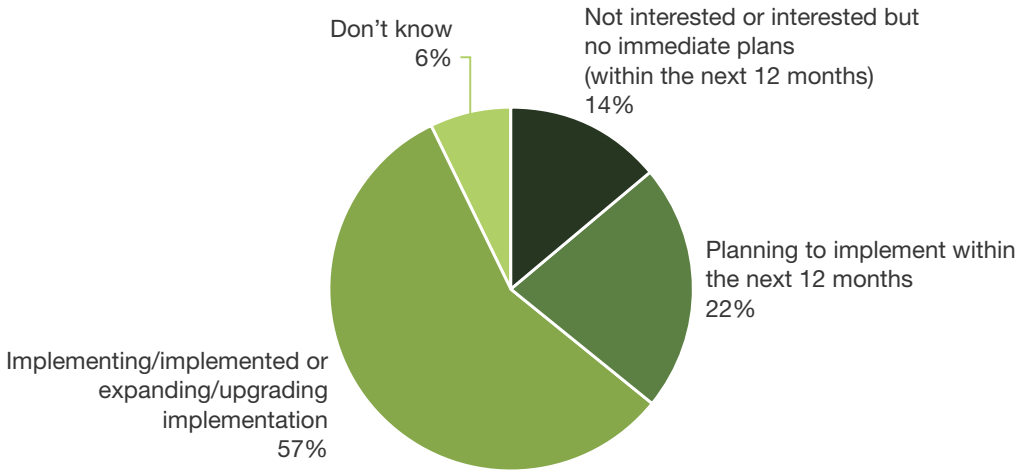
alert and a link graph showing other systems with which the device is communicating. Built-in workflow and automation can recommend next steps and automate actions to speed investigations and remediation.

› **Improve operations.** Many enterprises employ SIM solutions at the heart of their security operations center (SOC). Older tools lack workflow management and automation, forcing analysts to use spreadsheets, email, and collaboration tools like Slack to track investigations and communicate. With security talent at a premium, S&R teams have to increase analyst productivity. SA platforms are including and integrating with security automation and orchestration (SAO) tools, making operations more efficient and moving toward automated response.[4]

› **Support compliance efforts.** Compliance support for standards and regulations like the Payment Card Industry Data Security Standard (PCI DSS), ISO 27002, and many 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 adequately address this use case, focusing on detection instead. This means that S&R pros who invest in these tools will need separate compliance solutions.

FIGURE 1 Enterprise Security Analytics Implementation

"What are your firm's plans to adopt security information management (SIM)/security analytics?"



Base: 540 global network path security decision makers (working at enterprises of 1,000-plus employees)
Note: Results may not add up to 100% because of rounding.
Source: Forrester Analytics Global Business Technographics® Security Survey, 2018

Understand Security Analytics Platform Characteristics

Rules-based SIM systems have been around since the mid-1990s, gaining widespread market acceptance in the mid-2000s 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 and changing nature of threats. SIM vendors added security analytics features such as:

- **Network analysis and visibility (NAV).** NAV provides 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 (SUBA).** Understanding user behavior is key for finding malicious insiders and compromised accounts. SA platforms include SUBA as a feature or value-added offering or are partnering with third-party SUBA vendors to deliver the capability.
- **Big data infrastructure.** SA platforms leverage big data infrastructure to handle the massive volume of events and data sources they process. SA vendors have updated their solutions to incorporate big data infrastructure, and some work with customer-provided, third-party big data platforms.
- **Security automation and orchestration (SAO).** SAO tools orchestrate processes and automate many of the mundane tasks performed by SOC analysts, saving time and improving productivity. SA platforms include SAO as a feature or separate but integrated product or are partnering with third-party standalone SAO vendors.

Security Pros Demand More SA Flexibility

Describing his iconic Model T, Henry Ford famously said, “Any customer can have a car painted any color that he wants, so long as it is black.” Inflexibility may have worked for cars in 1919 but does not work for SA platforms in 2018. Computing models are changing as more enterprises adopt a cloud-first philosophy and require more deployment options. Licensing and pricing also have to change to fit budgets that are becoming better suited to buying SaaS services and subscription software licenses. Increasing data volumes mean that consumption-based pricing is difficult to predict and can lead to excessive costs. As a result:

- **Solutions can be deployed in a variety of ways.** Once only available on-premises, delivered as hardware appliances, SA solutions are now available in multiple deployment scenarios — on-premises hardware, software, virtual machine, and SaaS. Customers can choose the deployment scenario that best fits their needs.

- **Data is decoupled from analytics.** Enterprises are collecting vast quantities of log data for compliance, threat hunting, and forensics. Much of this data resides in SA platforms while enterprises build their own data lakes for long-term storage due to processing and storage costs. Data is not useful without analytics, so enterprises are looking for solutions that work with customer-supplied data stores. SA vendors integrate analytics with these third-party data stores, making log data storage a commodity.
- **Multiple licensing options become the norm.** Perpetual licenses were once the norm for software purchases, but the majority of customers are now demanding subscription licensing, which more closely aligns to the way they buy cloud services. Some customers, however, still prefer perpetual licensing, so vendors now offer a choice.
- **Consumption-based pricing remains a pain point.** The majority of SA platforms have a consumption-based pricing model of events per second (EPS) processed, data volume processed, or data volume stored. EPS and amount of data processed pricing models cause much consternation for customers; they are a disincentive for customers to add more data sources to the solution and can be unpredictable, making budgeting difficult. Some vendors are adding an option for enterprise pricing based on the number of users or assets being monitored, removing the variability of events and data.

Security Analytics Platforms Evaluation Overview

To assess the state of the security analytics platforms market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top security analytics platforms 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 30 criteria, which we grouped into three high-level buckets:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave™ graphic indicates the strength of its current offering. Key criteria for these solutions include data architecture, deployment options, data connectors, customization, correlation rules, real-time monitoring, advanced detection techniques, risk scoring and prioritization, user behavior analytics, cloud security, endpoints, integrated network analysis and visibility, data security, log management, threat intelligence, vulnerability data, investigation and incident management, dashboards and reporting, compliance, scalability, security automation and orchestration, and end user experience.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, planned enhancements, technology partners, implementation size, delivery/implementation model, and pricing and licensing.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise customer base and product line revenue.

Evaluated Vendors And Inclusion Criteria

Forrester included 13 vendors in the assessment: AlienVault, Exabeam, Fortinet, Gurucul, Huntsman Security, IBM, LogRhythm, McAfee, Micro Focus, Rapid7, RSA, Securonix, and Splunk (see Figure 2). Each of these vendors:

- **Has advanced detection capabilities.** The solution must utilize the technology building blocks of AI, machine learning, or behavioral anomaly detection as a supplement to or replacement for rules-based detection.
- **Has an enterprise client base.** Vendors must have significant enterprise customers using the solution as part of their security monitoring strategy. For the purposes of this Forrester Wave, enterprise customers had to have 5,000 or more employees.
- **Delivers two or more SA components.** Vendors must deliver multiple SA components, such as big data infrastructure, SIM, SUBA, or NAV as part of the SA solution.
- **Delivers as a productized commercial offering.** The offering can be on-premises or cloud delivered, but it cannot be a custom managed or professional service. The vendor must offer a product version of the solution that was generally available prior to March 31, 2018. We only evaluated suite capabilities that were released and generally available to the public by this cutoff date.
- **Has log archiving that supports PCI DSS compliance.** The solution must provide log storage in a format that supports compliance with PCI DSS.
- **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 2 Evaluated Vendors And Product Information

Vendor	Product	Version number
AlienVault	USM Anywhere	
Exabeam	Exabeam Security Intelligence Platform	2.0
Fortinet	FortiSIEM	5.0
Gurucul	Gurucul Risk Analytics	6.2
Huntsman Security	Huntsman Enterprise SIEM	6.01
IBM	IBM QRadar Security Intelligence Platform	7.3.1
LogRhythm	LogRhythm NextGen SIEM Platform	7.3
McAfee	McAfee Security Operations solution	
Micro Focus (NetIQ/ArcSight — formerly HPE)	ArcSight	7.0
Rapid7	Rapid7 InsightIDR	
RSA	RSA NetWitness Platform	11.2
Securonix	SNYPR Security Analytics	6.1
Splunk	Splunk Enterprise Splunk Enterprise Security Splunk UBA	7.0 5.0 4.0

Vendor Profiles

We intend this evaluation of the security analytics platform market to be a starting point only and 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 3 and see Figure 4). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 3 Forrester Wave™: Security Analytics Platforms, Q3 2018

FIGURE 4 Forrester Wave™: Security Analytics Platforms Scorecard, Q3 2018

	Forrester's weighting	AlienVault	Exabeam	Fortinet	Gurucul	Huntsman Security	IBM	LogRhythm	McAfee	Micro Focus	Rapid7	RSA	Securonix	Splunk
Current offering	50%	1.92	3.14	2.62	3.10	2.68	4.00	4.22	3.34	2.96	1.66	3.86	3.24	3.80
Data architecture	5%	1.00	3.00	3.00	5.00	3.00	5.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
Deployment options	2%	1.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00	1.00	3.00	5.00	5.00
Data connectors	3%	3.00	3.00	3.00	3.00	3.00	5.00	5.00	5.00	5.00	1.00	3.00	3.00	5.00
Customization	6%	1.00	5.00	1.00	3.00	3.00	3.00	5.00	5.00	3.00	1.00	5.00	3.00	5.00
Correlation rules	5%	3.00	3.00	5.00	3.00	3.00	5.00	5.00	3.00	5.00	1.00	5.00	3.00	3.00
Real-time monitoring	6%	1.00	3.00	3.00	3.00	3.00	5.00	5.00	5.00	3.00	1.00	3.00	3.00	5.00
Advanced detection techniques	3%	1.00	3.00	3.00	5.00	3.00	3.00	5.00	3.00	3.00	3.00	3.00	5.00	3.00
Risk scoring and prioritization	6%	1.00	5.00	3.00	5.00	3.00	5.00	5.00	3.00	3.00	1.00	3.00	3.00	3.00
User behavior analytics	5%	1.00	5.00	3.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00
Cloud security	6%	3.00	3.00	3.00	5.00	1.00	3.00	5.00	1.00	1.00	1.00	5.00	3.00	3.00
Endpoints	6%	3.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00	5.00
Integrated network analysis and visibility (NAV)	6%	3.00	1.00	3.00	1.00	1.00	3.00	3.00	3.00	3.00	1.00	5.00	3.00	3.00
Data security	6%	1.00	5.00	3.00	5.00	3.00	3.00	3.00	3.00	1.00	1.00	5.00	3.00	3.00
Log management	5%	1.00	3.00	1.00	1.00	3.00	3.00	3.00	3.00	3.00	1.00	3.00	3.00	5.00
Threat intelligence	4%	3.00	3.00	3.00	1.00	3.00	5.00	3.00	5.00	3.00	1.00	5.00	3.00	3.00
Vulnerability data	3%	3.00	1.00	3.00	1.00	3.00	5.00	5.00	5.00	3.00	3.00	3.00	3.00	3.00
Investigation and incident management	4%	1.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00	3.00	1.00	5.00	5.00	5.00
Dashboards and reporting	5%	3.00	1.00	3.00	1.00	3.00	5.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00
Compliance	5%	3.00	1.00	3.00	1.00	5.00	5.00	5.00	3.00	3.00	3.00	3.00	1.00	3.00
Scalability	3%	1.00	3.00	3.00	3.00	3.00	5.00	5.00	5.00	5.00	1.00	3.00	3.00	5.00
Security automation and orchestration	3%	1.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00	1.00	3.00	3.00	3.00	3.00
End user experience	3%	3.00	5.00	3.00	3.00	1.00	5.00	5.00	5.00	1.00	3.00	3.00	5.00	3.00

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

FIGURE 4 Forrester Wave™: Security Analytics Platforms Scorecard, Q3 2018 (Cont.)

	Forrester's weighting	AlienVault	Exabeam	Fortinet	Gurucul	Huntsman Security	IBM	LogRhythm	McAfee	Micro Focus	Rapid7	RSA	Securonix	Splunk
Strategy	50%	1.20	3.80	1.20	3.00	3.20	4.60	4.60	3.20	2.40	2.80	3.40	3.80	4.20
Product vision	30%	1.00	3.00	1.00	3.00	3.00	5.00	5.00	3.00	3.00	3.00	5.00	3.00	5.00
Planned enhancements	30%	1.00	5.00	1.00	3.00	3.00	5.00	5.00	3.00	1.00	3.00	3.00	5.00	5.00
Technology partners	10%	1.00	3.00	3.00	1.00	3.00	5.00	5.00	3.00	3.00	1.00	3.00	3.00	5.00
Implementation size	10%	1.00	3.00	1.00	3.00	5.00	5.00	5.00	3.00	5.00	1.00	3.00	3.00	5.00
Delivery/implementation model	10%	3.00	3.00	1.00	5.00	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	1.00
Pricing and licensing	10%	1.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00	1.00	3.00	1.00	5.00	1.00
Market presence	0%	4.00	1.00	2.00	1.00	1.00	5.00	5.00	3.00	5.00	2.00	3.00	3.00	5.00
Installed base	50%	5.00	1.00	3.00	1.00	1.00	5.00	5.00	3.00	5.00	1.00	3.00	3.00	5.00
Product line revenue	50%	3.00	1.00	1.00	1.00	1.00	5.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00

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

Leaders

› **LogRhythm.** LogRhythm remains the largest standalone pure-play security analytics platform provider in the market, although it was acquired by private equity firm Thoma Bravo in July 2018.[7] LogRhythm provides a feature-rich platform, largely developed in-house, that includes SIM capabilities, SUBA, file integrity monitoring (FIM), SAO, endpoint monitoring, and NAV functionality. These may not have the same functionality as standalone solutions. The solution is available for on-premises deployment using LogRhythm appliances, virtual appliances, or software. SaaS services are available through LogRhythm partners, although aspects of the LogRhythm platform, like the CloudAI SUBA functionality, are delivered from the cloud.

LogRhythm includes its SAO capability and core SUBA functionality as part of the base license, although additional SUBA capability is licensed separately as CloudAI. Customers remark that reporting needs an update. Midmarket and enterprise customers seeking a full-featured security analytics platform should consider LogRhythm.

› **IBM.** IBM has placed its QRadar Security Intelligence Platform as the centerpiece of its security portfolio. The company continues to pursue an ambitious strategy for security analytics and automation that includes cognitive security capabilities from its Watson initiative and SAO from IBM Resilient. QRadar includes SUBA functionality as part of its standard license, although it's not as

full-featured as standalone offerings from competitors. NAV is delivered as part of QFlow, Network Insights, which is included as part of the base license, and Incident Forensics, which is sold as a separate license. IBM delivers QRadar on-premises via hardware, software, or virtual appliances. IBM also offers QRadar as a SaaS service, hosted in the IBM Cloud, and as a managed service.

Numerous integrations and apps are available through IBM App Exchange. QRadar is scalable for large installations but can be costly as additional resources are added and more data is consumed in the consumption-based pricing model. 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 SIM functionality with available add-ons for SUBA and SAO (through its acquisition of Phantom earlier this year). 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. Splunk is highly customizable and gives users the ability to build their own rich reports, dashboards, and visualizations, but out-of-the-box functionality is not as deep as competitive offerings.

Splunkbase, Splunk's app exchange, offers numerous apps and integrations for third-party technologies. Customers appreciate Splunk's scalability and degree of customization, but the solution may require extensive services for larger or more complex implementations. Splunk's consumption-based pricing model continues to be a pain point for customers, although the company has introduced enterprise pricing. S&R pros planning to deploy Splunk should pay attention to estimating the amount of data they plan to process so they aren't surprised by the consumption-based pricing. Enterprises seeking a high degree of customization and those with advanced security teams and complex logging requirements should consider Splunk.

› **RSA.** RSA, part of Dell Technologies, provides SIM, NAV, and UBA through its RSA NetWitness Platform offering. RSA NetWitness provides threat detection and visibility through a combination of log and packet data analysis. SUBA is offered in two tiers: RSA UEBA Essentials, which is part of the standard license, and RSA NetWitness UEBA, offered as a separate license. RSA announced its acquisition of SUBA vendor Fortscale in April 2018, but those capabilities are not included in this Forrester Wave.[8] SAO is delivered via RSA NetWitness Orchestrator, based on an OEM agreement with Demisto, which is available as a separate license. The solution is delivered via on-premises software, hardware, or in a mixed deployment. The software version can be hosted in private or public cloud environments but is not available as a SaaS offering. RSA NetWitness offers a unique blend of log and network analytics that allows full reconstruction of network sessions.

RSA integrates RSA NetWitness with its own EDR functionality, offering a "light" functionality as part of the standard license, but support for third-party endpoint solutions is lacking. Customers noted that the solution is complex and that the UI is not intuitive. Recent organizational changes caused some business disruption, but RSA now seems focused on growing its security business. Organizations looking for a high level of visibility into their network traffic should consider RSA.

Strong Performers

- **Securonix.** Securonix launched in 2008 primarily as a SUBA vendor and added SIM functionality in 2016 to compete as a security analytics platform. The company's solution is made up of SNYPR Security Analytics, SNYPR Security Big Data Lake, and Securonix UEBA. SNYPR Security Big Data Lake, built on Hadoop, is designed to meet the need for platform independent log data storage. Security analytics uses a combination of rules and machine learning to detect threats, and the solution provides built-in SAO as part of the standard license, although it is not as full-featured as standalone SAO tools. The solution is delivered via software, appliance, virtual appliance, and SaaS. The software version can be hosted in public or private cloud environments. Securonix offers a flexible pricing model based on the number of identities in the customer environment.

  Customers appreciate SNYPR's open data model, user behavior analysis, and use case customization. Some customers claim that solution setup and tuning can be difficult. Available out-of-the-box reports and custom report creation are also weak points cited by customers. Midmarket companies and enterprises looking for a flexible security analytics platform that can work as a standalone solution or in conjunction with current SIM implementations should consider Securonix.

- **Exabeam.** Exabeam launched in 2014, originally focusing on SUBA, and launched its SIM and SAO offerings in 2017. Exabeam Security Intelligence Platform is a combination of integrated analytics, log management, and SAO offerings that operate as a platform in combination or as standalone solutions. Incidents are largely based on user behavior and assets, and users are able to view events in timelines for investigation. Although Exabeam has only been in the market for a relatively short time, the company appears in numerous enterprise purchasing opportunities and has made significant progress with its platform. Exabeam deploys as hardware or software which can be hosted in cloud environments. SaaS is available through MSSP partners.

  Exabeam's pricing is flat rate, based on the number of employees, not on number of assets monitored or amount of data ingested. Customers note usability and insight into individual user behaviors as strengths. Weaknesses include limited available reporting, integration with vulnerability management tools, and integrated threat intelligence. Midmarket companies and enterprises seeking a modular yet integrated SA platform should consider Exabeam.

- **McAfee.** McAfee provides SA through its McAfee Enterprise Security Manager (ESM) SIM solution. McAfee's security portfolio is focused on endpoint, security management, and cloud security, with ESM making up the security management portion. The solution is delivered via physical appliance, virtual appliance, or as a hybrid deployment. Integrated SUBA (McAfee Behavior Analytics) is delivered via an OEM partnership with Interset. McAfee Active Response provides EDR capabilities, while McAfee Investigator is available to aid in forensic investigations and threat hunting. Both capabilities are licensed separately. ESM is licensed as a perpetual license, while add-ons like behavior analytics, investigator, and active response are sold as annual subscriptions. The solution doesn't price by data ingestion, although collection appliances are sold by their EPS capacity.

Customers cite the high degree of customization and integration with other McAfee products as strengths. Reporting and dashboards are noted as weaknesses. Despite an updated UI, a portion of the administrator interface remains Flash-based. McAfee has spun out of Intel as a standalone entity but remains partially owned by Intel and private equity firm TPG.[9] McAfee leadership indicates that it will continue to invest in ESM, but customers should pay special attention to road map announcements to ensure they are delivered as scheduled. Enterprises and midmarket organizations, especially those using McAfee for other parts of their security stack, should consider McAfee.

- **Gurucul.** Gurucul originally emerged as a big data security analytics vendor in 2010, later focusing on its SUBA capabilities. The company has more recently added features like real-time threat monitoring and compliance support to its Gurucul Security Analytics platform, allowing it to compete against legacy SIM solutions as an SA platform. Gurucul offers its own big data stack and can also add its analytics to customer-provided, third-party big data deployments via Gurucul Risk Analytics. Customers can customize Gurucul's behavior models or build their own via GuruculSTUDIO. The vendor built on its SUBA heritage, combining robust risk categorization with data classification to prioritize alerts and detect exfiltration of sensitive data. Gurucul deploys as software that can run on customer-supplied hardware or virtual infrastructure, appliance, or as a SaaS offering. The vendor offers subscription, perpetual, and SaaS licensing. Solution pricing is based on the number of identities/entities being monitored.

  Gurucul doesn't fully address all SIM use cases. Compliance reporting, for example, is weak compared with other solutions, as is support for NAV, threat intelligence, and vulnerability data. Customer feedback indicates that Gurucul's machine learning models, risk scoring, and flexibility are strengths. Weaknesses mentioned by customers include the user interface and the vendor's sales and marketing efforts. Enterprises looking for a robust security analytics tool with strong SUBA and data protection should consider Gurucul.

- **Huntsman Security.** Huntsman Security, a private Australian company, is building on its legacy as a SIM for government and defense. Its customers include government ministries, intelligence agencies, defense departments, and enterprises. Huntsman Enterprise SIEM combines SIM capabilities with behavioral anomaly detection. The add-on Huntsman Analyst Portal provides threat verification, investigation, and automated resolution. The solution is delivered as a software application or virtual machine, deployable via customer-supplied hardware or in a cloud environment. Licensing options include subscription and perpetual licenses with pricing determined by EPS and data volume. Options for multitenant licensing and per-user pricing are also available.

  Huntsman Security is not yet widely known in North America, with most of its customer base in Asia Pacific, Japan, and Europe. Elements of the user interface are a little dated — likely a hangover of the solution's original government client base. Customer references indicate that alert context and automation are strengths. Weaknesses noted by customers include the speed of product development and the number of OOTB rulesets. Enterprises and government agencies with presence in Asia Pacific and Europe that want to combine the strengths of security analytics and SIM should evaluate Huntsman Security.

› **Micro Focus.** Micro Focus is working to breathe new life into its once market-leading ArcSight SIM solution, which it acquired when HPE spun out its Software Business Segment in a merger with Micro Focus that closed in 2017. Long-term ArcSight customers were frustrated with HPE's inability to keep pace with innovations in the market and are hopeful that Micro Focus will invest in the solution. Some of the largest enterprises in the world and government agencies continue to rely on ArcSight for security monitoring and logging, although many customers are seeking alternatives. Micro Focus is making some progress but has plenty of ground to make up. ArcSight deploys as hardware appliances and as software that can be deployed in virtual and cloud environments. The solution is priced based on EPS or GB per day, and an enterprise pricing model is also available.

The future of the ArcSight platform is uncertain, although plans call for investment in bringing it up to date through enhancements, acquisitions, and partnerships. For example, Micro Focus has an OEM agreement with Securonix to provide its SUBA solution. Enterprises should continue watching the product road map closely during the integration process to see if planned updates slip or if the new ownership loses focus on the product. Micro Focus has another SIM solution, NetIQ Sentinel, which it continues to support and market. The company plans to blend aspects of both solutions, starting with data collection and reporting.

Contenders

› **Fortinet.** Fortinet entered the SA market with its acquisition of AccelOps in June 2016, rebranding the solution as FortiSIEM.[10] FortiSIEM offers SIM capability with some lightweight SUBA capability and an included CMDB. Fortinet gives customers a choice of event database, a proprietary NoSQL database, or Elastisearch. The solution is delivered as an appliance and as a virtual machine. SaaS is available through partners. Pricing is based on EPS and the number of devices monitored in the CMDB.

Fortinet recently updated the solution's UI, and users noted ease-of-use, correlation rules, and alert customization as strengths. Customers report product support and updates as shortcomings. The majority of FortiSIEM customers are midsize enterprises, although the solution does have some enterprise customers. Midsize enterprises looking for strong SIM capabilities should consider FortiSIEM.

› **Rapid7.** Rapid7 entered the SA market in 2016 with its cloud-based InsightIDR offering, combining SUBA capabilities with log management. InsightIDR includes SUBA as part of the base license along with SIM and lightweight EDR capabilities. The included EDR agent is also leveraged by Rapid7's endpoint management and vulnerability management solutions. SAO is supported as a separately licensed product through the acquisition of SAO provider Komand in 2017. Rapid7 has a unique detection feature with integrated deception technology included as part of the subscription. InsightIDR is delivered as SaaS, with no on-premises version available.

As a SaaS offering, licensing is a subscription model, and pricing is based on the number of assets monitored. Customer feedback indicates ease of deployment and operation as strengths. Rapid7 is a relatively new entrant to the SA market. As a result, InsightIDR lacks the feature depth that its more mature competitors offer. Shortcomings mentioned by customers include lack of customization and limited reporting. Small and midsize enterprises as well as larger, resource-constrained enterprises looking for a SaaS-based SA solution should consider Rapid7.

Challengers

› **AlienVault.** AlienVault, recently acquired by AT&T, offers AlienVault Unified Security Management (USM) as a combined security platform that includes multiple security tools like vulnerability assessment, intrusion detection, endpoint security, and SIM as part of the base license.[11] AlienVault has transitioned from an appliance-based model to SaaS delivery, so new customer implementations will be delivered in the cloud, not on-premises. The solution's SUBA capabilities are confined to events where user context can be extracted. Limited SAO capability is delivered through AlienApps which integrates with third-party technologies. AlienVault has a unique approach to threat intelligence with its community-oriented Open Threat Exchange (OTX) and includes threat intelligence from AlienVault Labs as part of the subscription. The solution is licensed as a subscription, and pricing is based on monthly data consumption.

AlienVault focuses on small and midsized enterprises and has a large, loyal customer base. Customers value getting multiple security technologies in a single solution. Other strengths mentioned by customers include price and ease of deployment and management, which make it a good fit for small security teams. Customers list reporting, NetFlow analysis, and lack of integrations as shortcomings. It's unsure what the AT&T acquisition means for AlienVault at this point, so customers and prospects should watch the integration and road map promises closely. Small and midsize enterprises looking for a SaaS-based security platform with SA should consider AlienVault.

Supplemental Material

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

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 August 20, 2018.

- **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.** To validate product and vendor qualifications, Forrester also conducted reference surveys with three of each vendor's current customers and one customer reference call for each vendor.

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 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. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the 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. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2018, was fielded between May and June, 2018. This online survey included 3,089 respondents in Australia, Canada, China, France, Germany, the UK, and the US. Forrester Analytics 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.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] Forrester introduced the concept of security analytics in a 2012 report. See the Forrester report "Dissect Data To Gain Actionable INTEL."

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

[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 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] See the Forrester report "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility."

[7] Source: "Thoma Bravo Completes Majority Investment in LogRhythm," Thoma Bravo press release, July 2, 2018 (https://thomabravo.com/2018/07/02/thoma-bravo-completes-majority-investment-in-logrhythm/).

[8] Source: "RSA Announces Intent to Acquire Fortscale, Expanding RSA NetWitness Evolved SIEM Platform With UEBA Capabilities," RSA press release, April 5, 2018 (https://www.rsa.com/en-us/company/news/rsa-announces-intent-to-acquire-fortscale).

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

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

[11] Source: "AT&T to Acquire AlienVault," AT&T press release, July 10, 2018 (http://about.att.com/story/att_to_acquire_alienvault.html).

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.