FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Vendor Landscape: Security Analytics (SA)

Tools And Technology: The Security Architecture And Operations Playbook

by Joseph Blankenship
November 15, 2016

Why Read This Report

Enabling their teams to quickly detect and respond to internal and external cyberthreats is critical for security leaders. Security analytics (SA) solutions promise to provide an array of functionality to give security professionals better visibility, improved detection, and enhanced workflows. This report examines the critical capabilities of SA solutions and provides security and risk pros with an overview of the key vendors that make up the SA ecosystem.

Key Takeaways

SA Is Paving The Way For Automation

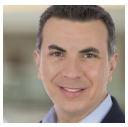
The increasing speed and accuracy of SA solutions is making it possible to automate security processes.

Multiple Technologies Make Up The SA Ecosystem

As standalone SA players become competitive, traditional security information management (SIM) vendors are adding analytics capabilities to their existing platforms. Meanwhile, specialized solutions for user behavior analytics and network analytics provide insight into behavior inside the network.

Vendor Landscape: Security Analytics (SA)

Tools And Technology: The Security Architecture And Operations Playbook



by Joseph Blankenship
with Stephanie Balaouras, Andras Cser, John Kindervag, Claire O'Malley, Bill Barringham, and Peggy Dostie

November 15, 2016

Table Of Contents

Notes & Resources

Forrester interviewed 18 vendor companies: AlienVault, BAE Systems, Damballa, E8 Security, EMC (RSA), FICO, Fidelis Cybersecurity, FireEye, FireMon, Forcepoint, Huntsman Security, IBM, LogRhythm, PwC, SAS Institute, Splunk, SS8, and Vectra Networks.

Related Research Documents

Counteract Cyberattacks With Security Analytics

TechRadar™: Zero Trust Network Threat Mitigation Technologies, Q4 2016

Vendor Landscape: Security User Behavior Analytics (SUBA)

FORRESTER®

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

© 2016 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

Security Teams Need Data For Better Decision-Making, Faster Response

Reducing time-to-detect and increasing speed-of-response are critical for security teams. According to our surveys, a whopping 96% of enterprise security decision-makers rate improving security monitoring capabilities as a priority.[1] Security analytics (SA) solutions built on big data infrastructure and using data science techniques like machine learning are taking the place of older rules-based and signature-based technologies, increasing detection accuracy and providing security pros with better data with which to make decisions. SA is the evolution of SIM, which in its first incarnation, failed to live up to its expectations because it lacked the ability to ingest, correlate, and analyze large amounts of data from a variety of sources, including other security solutions like tools for in-depth network analysis and visibility (NAV).[2] SA solutions can also deliver more robust security context in alerts and provide workflow tools to accelerate response.

SA Solutions Make Sense Of Diverse Data

Detecting and defending against cyberattacks requires fast analysis of large, diverse data sets. Legacy rules-based technologies are unable to keep pace, delivering a deluge of alerts to be validated or being ignored by security pros altogether. SA solutions use data science techniques in conjunction with rules-based techniques to recognize behavior patterns that could indicate malicious activity. Security teams reap benefits with higher detection rates and lower false positives. Security pros are turning to SA solutions because these solutions can:

- **Identify previously unknown threats.** Rules-based technologies like legacy SIM solutions are only able to detect known threats. The data-science-based detection in SA is able to detect anomalous behavior that is indicative of cyberthreats.[3] For example, an attacker who has compromised user credentials may not be detected via rules, but may demonstrate malicious behavior when attempting to access sensitive information or upload data to an unknown destination.
- **Support better decision-making.** Security pros have long complained about the accuracy of alerts from traditional rules-based SIMs. Security analytics helps increase detection accuracy and provide the context needed for analysts to make faster decisions. Increased confidence levels in the alerts generated by SA is paving the way for automation.[4]
- **Provide visibility to activity inside the network.** Gaining visibility is a key benefit of security analytics tools. The ability of SA tools to 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 provides insight into user and device activity.
- **Enable investigations.** SA tools combine and index inputs from disparate sources into big data environments, giving investigators and threat hunters the ability to search and make sense of large quantities of data. Case management, workflows, and playbooks built into SA tools make investigations more efficient.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Prioritize alerts based on risk.** Effectively triaging alerts based on risk allows analysts to address high-priority threats first. Malicious activity targeting high-value assets like cardholder data networks gets a higher risk score than assets containing less sensitive data.
- **Enable quick interception.** Merely investigating alerts isn't enough. Stopping incidents before they become data breaches is critical.[5] SA solutions quickly recognize malicious activity, enabling automated actions to quarantine a device, drop a network connection, or block a URL. Automation vendors like Ayehu, Demisto, Phantom, ServiceNow, and Swimlane are integrating with SA solutions and security vendors to automate response.

Modernizing Security Operations Depends On SA

Security teams rely on manual processes to do the majority of their work. Analysts who research alerts or conduct threat hunting rely on multiple tools that don't always work together. The lack of automation compounds problems like the cybersecurity skills shortage. In most security operations centers (SOCs):

- **Diverse security tools require a swivel chair.** Commonly known as "swivel chairing," analysts commonly access multiple security tools to investigate incidents and pull together needed context. SA platforms pull this contextual data into one place and provide workflows, reducing the need for analysts to access multiple tools.
- **Spreadsheets remain the leading productivity tool.** Instead of using workflow tools, many security teams rely on spreadsheets and email to track investigations and communicate. Our survey reveals that 64% of enterprise security decision-makers and influencers say their teams spend too much time on day-to-day tactical activities.[6]
- **Many analysts lack the requisite skills.** Qualified security professionals are difficult to find and retain. In our 2016 survey, 65% of enterprise security decision-makers and influencers report that finding security pros with the right skills is a challenge for them.
- **Automation is still a four-letter word.** Most security pros remain reticent to employ automation in security operations, believing human analysts are necessary to make security decisions. Better decision-making through improved analytics and tuning is making it possible to automate some security processes like investigations. Automated response is the next logical step as the technology continues to build confidence.[7]

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

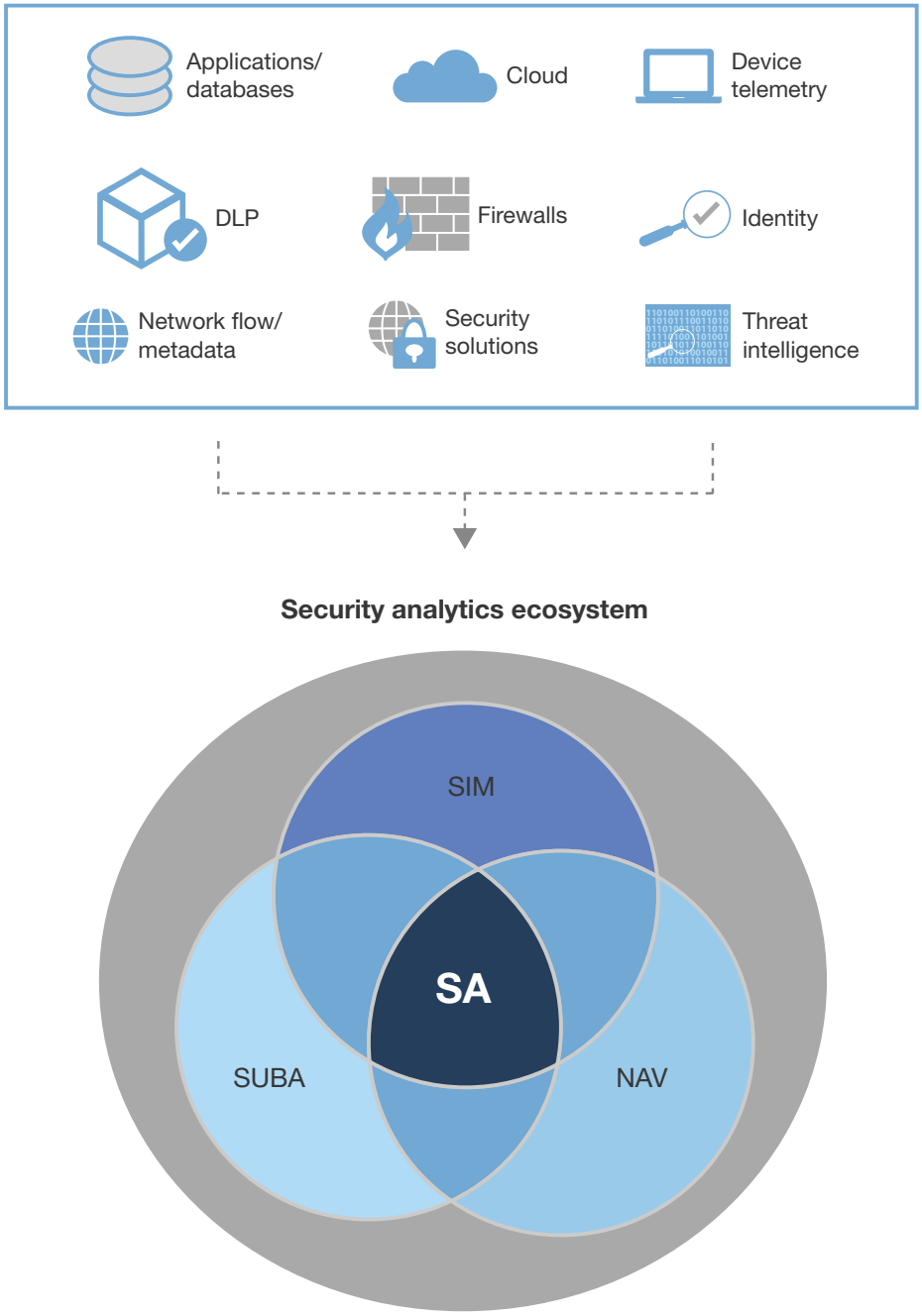
Security Analytics Is An Ecosystem And Tool Set, Not A Single Product

Forrester envisions security analytics as a single platform, built on big data infrastructure, that ingests relevant data from a wide variety of sources. The SA platform then uses this information along with machine-learning techniques to provide real-time monitoring and to facilitate rapid incident detection, analysis, and response.[8]

Unfortunately, no vendor is currently delivering on that vision completely. Instead, the security analytics market consists of multiple technologies that can work together or exist independently (see Figure 1). SA is a technology at a crossroads, and many vendors are co-opting the term SA. As a result, it has become a catchall for any security solution that uses data science to detect threats. In the future, the SA market will stabilize, and SA will become an integrated platform that provides security visibility and reporting and that enables automated breach response.[9]

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 The Security Analytics Ecosystem



© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

SIM Vendors Deliver SA, But Standalone Options Exist

The major SIM vendors such as EMC (RSA), IBM, LogRhythm, and Splunk are pivoting toward SA by adding NAV and security user behavior analytics (SUBA) capabilities to their existing solutions. Standalone SA, NAV, and SUBA solutions can exist independently from SIM or as a complementary technology. As the vendor landscape expands, security teams will find that (see Figure 2):

- **SIM provides rules-based correlation, log management, and robust compliance.** Since SIMs first emerged in the late 1990s, security teams have used them to collect and analyze logs. Compliance guidelines like PCI DSS made them must-have technologies for log monitoring, log management, and compliance reporting. While SIMs still rely on rules-based detection, they're evolving with the addition of security analytics, NAV, threat intelligence, and improved workflow. Large enterprises with complex security needs and compliance requirements should still choose SIM for monitoring.
- **Standalone SA uses data science to identify anomalies.** As security teams struggled to get value from SIMs, standalone SA solutions have emerged to provide threat detection that uses an underlying big data platform and data science techniques to detect unknown threats instead of relying solely on rules. Originally designed to work in conjunction with SIMs, some, such as Bay Dynamics, E8 Security, Securonix, and SS8, are emerging to become SIM competitors. Most, however, lack features like PCI-compliant log management. If your current SIM lacks security analytics, you don't have a SIM, or you don't have to comply with PCI but need threat monitoring, standalone SA is a viable alternative.
- **NAV provides deep insight into network activity.** NAV is a diverse set of tools designed to provide network-based situational awareness. NAV tools perform many functions, including: malicious behavior detection, network discovery, flow analysis, full packet capture, and network forensics. The need for NAV emerged when security teams were mainly focused on network perimeter monitoring.[10] NAV solutions such as Cisco (Lancope), Damballa, Fidelis Cybersecurity, and Vectra Networks examine network communications to understand network behavior and detect threats. SIM vendors and standalone SA vendors are adding NAV capabilities, but standalone solutions still exist. Choose NAV for increased visibility into network traffic and behavioral-based threat detection.
- **SUBA offers focused understanding of user behavior.** Since users are often the source of data breaches, security leaders need better visibility into how users behave on the network and interact with data. Instead of monitoring network traffic like NAV, SUBA takes in log data from endpoints, identity and access management (IAM) systems, data loss prevention systems (DLPs), and applications and databases to understand user behavior. SUBA identifies abnormal behavior patterns that are indicative of malicious user behavior.[11] SIM vendors are adding SUBA as a feature to their platforms, and standalone SA vendors typically offer SUBA as part of their solutions. Security leaders should pick a SUBA solution for specific use cases like insider threat hunting or if their current SIM doesn't provide SUBA.[12]

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 SA Vendors And Product Versions

SIM	Product	GA
AlienVault	Unified Security Management (USM) 5.2	October 2015
EMC	RSA NetWitness Suite	Q1 2016
Huntsman Security	Enterprise SIEM and Analyst Portal	November 2015
IBM	Qradar Security Intelligence 7.2.6	2012
LogRhythm	Security Intelligence Platform 7.1.6	April 2016
Splunk	Enterprise Security v4.1 and UBA	April 2016
Standalone SA		
BAE Systems	Threat Analytics 2.0	April 2016
E8 Security	Behavioral Intelligence Platform 1.3	October 2015
FICO	Falcon Cyber Security Analytics	February 2015
FireEye	Threat Analytics Platform (TAP)	February 2014
PwC	PWC's Secure Terrain	January 2016
SAS Institute	SAS Cybersecurity 1.1	November 2015
SS8	BreachDetect 2.3	March 2016
NAV		
Damballa	Failsafe 6.2	March 2016
Fidelis Cybersecurity	Fidelis Network	2015
FireMon	Immediate Insight	April 2016
Vectra Networks	X-Series Platforms and S-Series Sensors 2.5	April 2016
SUBA		
Forcepoint	SureView Insider Threat 8.0.1	March 2016

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

SA Vendors Deliver Diverse Solutions

The SA ecosystem is developing and evolving rapidly.[13] These technologies are highly desired, but both vendors and security pros struggle with precise definitions of these technologies and their place in the security stack. For example, some vendors like E8 Security identified themselves as SUBA, when their solution goes beyond user behavior. Below, we've listed 18 SA vendors with their diverse capabilities (see Figure 3):

- **AlienVault.** The AlienVault Unified Security Management (USM) platform collects and correlates event data from security controls (asset discovery, vulnerability assessment, network and host IDS, and file integrity monitoring) and third-party devices for threat prioritization. Its threat intelligence capabilities are powered by a mix of the USM's correlation engine, the AlienVault Lab Research team, and the AlienVault Open Threat Exchange (OTX). The solution is built for smaller deployments (100 to 10,000 employees) and caters to small security teams. The vendor has a large, loyal user base.
- **BAE Systems.** BAE Systems Threat Analytics is delivered as an on-premises solution or managed service to detect threats across the kill chain via delivery, exploitation, installation, and command and control (C2). Multiple analytics are written for each kill chain step in order to determine the different attack types per step. The solution analyzes a variety of endpoint and network data for alerting and to provide context via an investigator tool analysts can use for investigations. The UI provides graphical visualizations to illustrate how entities are connected, but no reporting is available.
- **Core Security (Damballa).** Core Network Insight (previously Damballa Failsafe) provides deep packet inspection to detect compromised systems. Core Network Insight is an on-premises NAV offering that discovers and provides visibility to active infections within a customer's network based on the communication behavior and activity of the devices within the network. Deep packet inspection sensors analyze network traffic for statistical similarities to machine learning models and threat intelligence to indicate evidence of infection. The company integrates with inline devices or on device software to facilitate remediation. While effective at detecting infected devices, Core Network Insight doesn't offer insight into user behavior or data exfiltration.[14]
- **E8 Security.** E8 Security Behavioral Intelligence Platform uses machine learning and multidimensional modeling to examine user, device, and network behaviors to identify anomalous activity. Analysts can use the solution to analyze current and historical behaviors, patterns, and anomalies across multiple data siloes. The solution also provides native visualizations between hosts, users, and behaviors to visually understand relationships. It integrates with Cisco Systems Identity Services Engine (ISE) to enable mitigation actions like quarantining. A fairly new company (it emerged from stealth mode in March 2015), only delivers as on-premises enterprise software that can be installed on an appliance or hosted in a private cloud.
- **EMC (RSA).** RSA NetWitness Suite (formerly RSA Security Analytics) provides SIM capabilities in combination with network forensics, endpoint detection and response, and advanced analytics.[15] The solution supports over 350 event sources and captures insights from network packets and

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

endpoint processes to analyze and identify suspicious files, processes, IOCs, and other behavior that could reveal malicious activity. The solution includes incident response workflow that provides capabilities to prioritize, triage, investigate, and remediate security alerts. An RSA NetWitness SecOps module with advanced incident management workflow, breach response playbooks, management dashboards, and reporting is available for more advanced security teams. The solution is delivered via on-premises software, hardware, or a mixed deployment. It monitors cloud environments, although cloud and SaaS deployment are not supported.[16]

- **FICO.** Falcon Cyber Security Analytics system is deployed as an on-premises solution or as part of the iBoss web security platform for cloud deployment. The solution ingests flows, DNS, HTTP, ICMP, and device ID from DHCP messages or logs then streams that data through its real-time analytics engine where it uses layered machine learning to detect anomalies. Events are then tagged with a threat score and associated reason codes and then passed along to a decision module for appropriate action. Alerts can be pushed to a SIM based on policy, but there is no built-in workflow or remediation capability. As it's intended to be a feeder for client SIMs or other SOC tools, its capabilities are limited, with no included workflow, visualizations, or remediation.
- **Fidelis Cybersecurity.** Fidelis Network monitors the network bidirectionally in real time to detect threats and data theft. It does not ingest logs from other devices but ingests feeds from Fidelis network sensors that inspect and analyze network traffic and deliver structured metadata, login, and IP/ID mapping logs from domain controllers and DHCP servers. The vendor provides Fidelis-curated threat intelligence to the system and can incorporate customer-provided feeds. Remediation actions are supported through Fidelis Endpoint to isolate endpoints, lock down a client NIC, or delete a specific file from the endpoint. It integrates with HPE ArcSight and other SIM providers to deliver alerts.
- **FireEye.** FireEye Threat Analytics Platform (TAP) is delivered as a SaaS service. It uses rules-based matching to evaluate events against FireEye-produced and third-party threat intelligence as well as heuristic and statistical approaches to identify potentially malicious behaviors. Prioritized notifications with context are generated in the UI with customizable alerting based on severity. Generated events and raw logs are indexed and stored in a scalable archive hosted in AWS. Guided workflows help analysts search events during investigations and threat hunting. FireEye purchased security orchestration vendor Invotas in February 2016 but has not yet fully integrated automation capabilities into TAP.[17]
- **FireMon.** FireMon Immediate Insight focuses on human/data interaction using natural language to provide real-time security analytics to discover and triage correlated, enriched security events. It ingests structured and unstructured data from a variety of sources like malware detection, endpoints, applications, network devices, and security solutions. The solution employs a natural-language system to interpret and perform entity extraction, full-text indexing, and enrichment for a human interaction-centric approach to data analysis and threat hunting that doesn't require coding.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

It is delivered as a hardened virtual appliance that can be deployed on-premises or in an IaaS environment. FireMon Immediate Insight doesn't detect threats on its own but correlates events from detection solutions like FireEye and searches for anomalies.

- **Forcepoint.** Forcepoint SureView Insider Threat uses an endpoint agent to monitor user behavior, detect anomalous behavior, and assign each user a risk score. The collected data can be sent immediately to the server or cached locally on the endpoint in an encrypted disk partition for later review. Analysts can investigate risk scores and examine the data through desktop video, captured files, and metadata. It integrates with other parts of the Forcepoint family of products, including Triton AP-Data DLP for data exfiltration detection. The solution only focuses on insider threats, so external dangers, apart from malware indicators, are not detected.
- **Huntsman Security.** Huntsman Enterprise SIEM combines SIM capabilities with an SA solution, the Huntsman Analyst Portal. The solution collects and processes security data in real time and uses correlation, rules, machine learning, and behavioral techniques to identity threats and misuses. The Analyst Portal includes SA technologies and automation capabilities that can be used for threat verification, elimination of false positives, and delivery of casefiles for threat resolution. Enterprise SIEM can be deployed on-premises or delivered via SaaS. The solution is multitenant, making the platform suited for managed security service providers (MSSPs) to use for client monitoring. Based in Australia with European headquarters in the UK and offices in Japan, Huntsman Security is not widely known in North America and caters primarily to government ministries, intelligence agencies, and defense departments.
- **IBM.** IBM QRadar Security Intelligence Platform is a family of offerings that includes QRadar and has a unified architecture that integrates security information, event management (SIM), log management, anomaly detection, incident forensics, incident response, and vulnerability management. QRadar takes feeds from 450 data sources and can be deployed on-premises, in the cloud, and via SaaS. The Sense Analytics engine is included as part of the base offering to detect advanced threats. QRadar User Behavior Analytics is available as an app to monitor user behavior. Some case management workflows are included, and additional automation is available through IBM's recent acquisition of Resilient.
- **LogRhythm.** LogRhythm delivers SA on a platform that also offers built-in SIM and log management, network forensics and analytics, endpoint monitoring, file integrity monitoring, and compliance automation. The solution promises a single-pane-of-glass view for SA, investigation, and correlation, with support for over 750 data sources. UBA is included with the solution through the User Threat Detection module. The solution is available for on-premises deployment using LogRhythm appliances, customer-provided hardware, virtual infrastructure, or private cloud.
- **PwC.** PwC's Secure Terrain provides SA as a managed service. The solution is not deployed on the premises of the client but is delivered as a cloud-hosted managed service. It focuses on threat intelligence, advanced analytics, and business risk assessment. PwC's Terrain Operation Centers (TOCs) manage the solution and monitors, respond to, and hunt for threats. UBA capabilities are

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

limited to access, network usage, and application usage. Some internal workflow management for functions like adding threat intelligence and alert routing is available, and integrations with third-party incident management systems is available via API.

› **SAS Institute.** SAS Cybersecurity includes data management, data streaming and enrichment, in-memory analytics, investigation, discovery, and visualization. The solution aims to provide network visibility and identify threats by enriching the network flow data with authentication, web proxy, business context, threat feed, and other security data in real time. The data is continually evaluated to understand machine and user behavior, as well as relationships. Risk scores are generated for each entity and then prioritized in the user interface for triage. The solution is delivered as an on-premises solution and doesn't include any workflow or remediation tools.

› **Splunk.** Splunk Enterprise Security provides real-time security monitoring, aids incident investigations, and offers user- and entity-based analytics from supervised and unsupervised machine learning techniques. Splunk Enterprise Security can be deployed on-premises, in public or private clouds, or as a hybrid configuration. Over 400 security-relevant apps are available through Splunkbase for use cases and data sources that aren't supported out of the box. Splunk UBA is a separate product for user behavior monitoring that integrates with Splunk Enterprise Security.[18] Built-in workflow is customizable and integrates with third-party ticketing systems.

› **SS8.** SS8 BreachDetect focuses on network communication and decoding protocols, using communication analytics to find suspects of interest and the associated compromised devices. Application-aware software sensors generate high-definition records (HDRs) that can be stored for years. Learning analytics enriches, analyzes, learns, and matches HDR data with user, device, and threat intelligence information. Automated discovery provides simplified workflows and visualization to support investigations. The solution can be deployed in the cloud or as on-premises software running on client-provided hardware.

› **Vectra Networks.** Vectra uses a combination of behavioral analysis, machine learning, and other mathematical models to identify a range of threats and human-driven attacks. The solution focuses on direct analysis of network traffic as opposed to consuming NetFlow or log data to identify attacker behaviors. Analysts are able to use visualizations to see relationships between hosts and risk scores associated with hosts. Workflow and remediation actions are supported through automated rules and integration with third-party solutions like SIMs and firewalls. The solution can monitor private cloud infrastructure, but there is no public cloud or IaaS support.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 3 Functional Comparison Of SA Vendors

Capabilities	Big data infrastructure	Advanced threat detection	Data exfiltration detection	Rules-based correlation	Ability to leverage third-party threat intelligence	PCI-compliant log archival	Built-in workflow and investigation	Network analysis and visibility	SUBA
AlienVault	✓	✓	✓	✓	✓	✓	✓	✓	
BAE Systems	✓	✓	✓		✓		✓		✓
Damballa	✓	✓					✓	✓	
E8 Security	✓	✓	✓		✓		✓		✓
FICO		✓	✓						✓
Fidelis Cybersecurity	✓	✓	✓	✓	✓		✓	✓	
FireEye	✓	✓		✓	✓		✓		✓
FireMon	✓			✓	✓		✓	✓	
Forcepoint			✓				✓		✓
Huntsman	✓	✓	✓	✓	✓	✓	✓		✓
IBM/Qradar	✓	✓	✓	✓	✓	✓	✓	✓	✓
LogRhythm	✓	✓	✓	✓	✓	✓	✓	✓	✓
PwC	✓	✓	✓	✓	✓	✓			✓
RSA	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAS Institute	✓	✓	✓		✓			✓	✓
Splunk	✓	✓	✓	✓	✓	✓	✓	✓	✓
SS8	✓	✓	✓		✓		✓	✓	✓
Vectra Networks		✓	✓					✓	

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Recommendations

Enable Security Operations With Security Analytics

Security monitoring is a critical part of a security strategy. Traditional monitoring technologies like legacy SIM have proven unable to detect more-advanced threats and malicious behaviors inside networks. SA solutions promise to detect cyberthreats and enable security teams to respond before they cause a data breach. Increased context, built-in workflows, and included remediation capabilities can improve operations. To enable your security operations, we recommend that you:

- **Consider alternatives to your current monitoring solution.** You are likely already using a SIM or MSSP for monitoring. If that solution is not living up to your expectations, it may be time to consider a change. Giving your team access to better tools can have a significant impact on performance and morale.
- **Evaluate where you may already have SA as a feature.** Are you making the most of the tools you already own? With features like NAV and SUBA now offered as part of SIM, ask your current vendor what functionality is available through your current solution. If you can avoid adding yet another product or interface, your operations will thank you.
- **Determine the best deployment model for your business.** If much of your business has already moved to the cloud, a cloud deployment may be a better fit for you, especially if your security team is already overtasked. On-premises deployments could be a better fit in sensitive environments or where data volumes are a concern. Hybrid deployments where some monitoring is done in the cloud and some is conducted with on-premises equipment are also a popular alternative.
- **Assess and tune your processes.** Manual SOC processes are a drag on security teams. Look for opportunities to streamline processes and automate where possible. You may be surprised to learn how many steps your analysts go through to conduct an investigation or close a ticket. Utilize the workflow and case management tools in your SA solution to get the most out of your investment.
- **Look for a vendor that will move you down the automation path.** SA vendors are building automation into their solutions and integrating with tools such as IAM, firewalls, IDS/IPS, and EVC to give analysts the ability to initiate remediation steps from the SA console. The next step is automating remediation to take immediate action based on confidence level and business impact.[19] Challenge your vendor to demonstrate how they are automating SOC processes.
- **Understand complex pricing models before you compare with other vendors and negotiate.** SA solutions may be priced based on log volume, amount of data analyzed, number of users, or number of nodes. If the vendor is using a consumption-based pricing model, your costs can increase significantly as you add new feeds. Get clarity about how adding new data sources or increasing volumes will affect you. Negotiate discounts once you understand the vendor's pricing mechanics and have a detailed estimate.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Survey Methodology

Forrester's Global Business Technographics® Security Survey, 2016 was fielded in 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. ResearchNow fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

AlienVault
BAE Systems
Damballa
E8 Security
EMC (RSA)
FICO
Fidelis Cybersecurity
FireEye
FireMon
Forcepoint
Huntsman Security
IBM
LogRhythm
PwC
SAS Institute
Splunk
SS8
Vectra Networks

Endnotes

[1] Source: Forrester's Global Business Technographics Security Survey, 2016.

[2] Business executives demand data for decision-making. Security professionals want situational awareness. Security information management (SIM) tools are seen as a solution to fulfill both needs, but today's reality is that SIM creates more fog than clarity, doing little more than providing compliance reporting. Big data and network analysis and visibility (NAV) tools for security analytics will provide the necessary additional ingredients to overhaul SIM and move it from merely compliance reporting to providing situational awareness for both the business and IT security. For more on how to effectively gain actionable output from security tools, see the "Dissect Data To Gain Actionable INTEL" Forrester report.

[3] S&R leaders frequently struggle with deploying the right mix of technologies to detect and respond to attacks. Four technologies should form the pillars of your breach detection capabilities: malware analysis, network analysis and visibility, endpoint visibility and control, and security analytics. For each technology, we provide you with key evaluation criteria, considerations, and both commercial and open source solutions to help you select the right solution. See the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Advanced Capabilities" Forrester report.

[4] The decision-making ability of security analytics is at the heart of Forrester's Declarative Security Model. For more information, see the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

[5] A massive breach of customer data can cost firms hundreds of millions in remediation costs, lost customers, and lost revenues. IP theft can lead to a permanent loss of competitive advantage. Today, CEOs and boards care about security more than ever and worry about the potential impact of a breach on the company. Automation is the answer. See the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

[6] Source: Forrester's Global Business Technographics Security Survey, 2016.

[7] Security has not caught up to other areas of the business that employ automation. Given the consequences of data breaches, businesses can no longer rely on passive, manual procedures to defend against them. The only way to protect the exfiltration of data by hackers and cybercriminals is to provide security teams with a set of rules that will incentivize automated response. For more, see the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

[8] Monitoring applications, databases, and endpoints, in addition to network devices, creates enormous log volumes that traditional security information management (SIM) systems have struggled to manage. The advent of big data and advanced analytical techniques has ushered in a new era for security monitoring and a new solution category — security analytics platforms. SA platforms use big data technology and machine learning to rapidly examine events, looking for anomalous activity that could be indicative of a breach, active malware, or other malicious activity. For more, see the "Counteract Cyberattacks With Security Analytics" Forrester report.

[9] For more, see the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

[10] In order to provide Zero Trust insight into internal and external networks, Forrester has defined a functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals. For the full NAV report, see the "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" Forrester report.

[11] Security user behavior analytics (SUBA) solutions promise to provide security and risk professionals with a unified view of employee activity across networks, devices, and apps and the ability to detect suspicious activity — quickly. For an overview of vendors in the space, see the "Vendor Landscape: Security User Behavior Analytics (SUBA)" Forrester report.

[12] Insider threats are a real risk to business because they threaten both customer and employee trust. Accidental or malicious misuse of the firm's most sensitive and valuable data can result in customer identity theft, financial fraud, intellectual property theft, or damage to infrastructure. Because insiders have privileged access to data in order to do their jobs, it's difficult for security pros to detect suspicious activity. For the full story, see the "Hunting Insider Threats" Forrester report.

[13] The cutoff date for this vendor landscape was May 20, 2016. While the market has changed since then, Forrester used information that was true on or before the cutoff date.

[14] Damballa was acquired by Core Security in July of 2016. Source: "Core Security Combines Identity, Vulnerability, and Now Network Detection and Response as The Industry's First Complete Actionable Insight Platform," Core Security press release, July 22, 2016 (http://www.coresecurity.com/press/core-security-combines-identity-vulnerability-and-now-network-detection-and-response-industry).

[15] 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 27, 2016 (http://www.rsa.com/en-us/company/newsroom/rsa-announces-rsa-netwitness-suite-designed-to-deliver-the-fastest-most-comprehensive-response).

[16] In September 2016, Dell and EMC, the parent company of RSA, combined their operations to become Dell EMC. Source: "Historic Dell and EMC Transaction Set to Close on September 7, 2016," Dell EMC press release, August 30, 2016 (http://www.emc.com/about/news/press/2016/20160830-01.htm).

[17] FireEye's acquisition of automation specialist Invotas International comes just 10 days after its acquisition of threat intelligence specialist iSight Partners. With these and prior acquisitions, FireEye continues its evolution from a malware analysis specialist to an enterprise security vendor with solutions for prevention, detection, and remediation. The Invotas acquisition also shines a spotlight on the emerging market for security automation solutions. For more, see the "Brief: FireEye Is Evolving Into An Enterprise Security Vendor" Forrester report.

[18] Splunk UBA is based on Splunk's 2015 acquisition of SUBA firm Caspida. Source: "Splunk Acquires Caspida," Splunk press release, July 9, 2015 (http://www.splunk.com/en_us/newsroom/press-releases/2015/splunk-acquires-caspida.html).

[19] Security analytics is the decision-making layer for Forrester's declarative security model. Using a response index based on confidence level and impact, security systems can take automated actions to stop malicious behavior, saving precious time in the event of an incident. See the "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.