The Forrester Wave™: Security Analytics Platforms, Q4 2020

The 11 Providers That Matter Most And How They Stack Up

by Joseph Blankenship and Claire O'Malley
December 1, 2020

Why Read This Report

In our 27-criterion evaluation of security analytics platform providers, we identified the 11 most significant ones — Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix, Splunk — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

IBM Security, Splunk, Securonix, Exabeam, And Microsoft Lead The Pack

Forrester's research uncovered a market in which IBM Security, Splunk, Securonix, Exabeam, and Microsoft are Leaders; LogRhythm, Gurucul, Micro Focus, Rapid7 and RSA are Strong Performers; and FireEye is a Contender.

Customization, MITRE ATT&CK Mapping, And SaaS Are Key Differentiators

As security information and event management (SIEM) technology becomes outdated and less effective, cloud-delivered security analytics platforms that provide custom detections will dictate which providers will lead the pack. Vendors that can provide customization, MITRE ATT&CK mapping, and SaaS delivery position themselves to successfully deliver improved detection, faster investigations, and flexibility to their customers.

The Forrester Wave™: Security Analytics Platforms, Q4 2020

The 11 Providers That Matter Most And How They Stack Up

by Joseph Blankenship and Claire O'Malley
with Stephanie Balaouras, Alexis Bouffard, and Peggy Dostie

December 1, 2020

Table Of Contents

Related Research Documents

The Forrester Wave™: Security Analytics Platforms, Q3 2018

Now Tech: Security Analytics Platforms, Q3 2020

The State Of Network Security: 2018 To 2019

FORRESTER®

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

The Future Of Security Analytics Is In The Cloud

In the past, vendors offered traditional SIEM systems as on-premises hardware or software deployments. As a result, security pros struggled to manage and update these systems and continually add storage for ever-increasing log volumes. In *The Empire Strikes Back*, Lando Calrissian tells Princess Leia, "You truly belong here with us among the clouds." The same can be said of security analytics platforms. As enterprises have moved their own workloads to the cloud to take advantage of its scale, flexibility, and availability, security vendors have finally started to follow suit with cloud-based delivery of their security analytics solutions. This transition and the entry of cloud native vendors are indicative that security analytics belongs in the cloud.

Most of the vendors included in Forrester's 2020 evaluation of the security analytics platform market deliver their products via SaaS or cloud-hosted models. This change has enabled vendors to more quickly roll out new capabilities to their customers and decrease the management overhead for these systems. Security pros looking to replace their legacy on-premises solutions should look for vendors that deliver most, if not all, of their capabilities from the cloud. As a result of these trends, security analytics platforms customers should look for providers that:

- **Provide customizability for customers.** Most vendors deliver out-of-the-box (OOTB) content that can be customized by enterprises to meet their individual needs. More advanced users also want to develop custom detections for specific scenarios. Some vendors make their machine learning models available to be customized by customers that want to create their own.
- **Offer true analytics and operations.** Many security analytics vendors offer basic analytics, focused on user behavior, and little to no automation. The strongest vendors offer analytics capabilities with multiple machine learning types and include security orchestration automation and response (SOAR). The combination of analytics and automation creates the opportunity for security analytics platforms to deliver intelligent operations with the capability of identifying threats and automatically responding to them.
- **Map to the MITRE ATT&CK framework.** Security pros were fast to adopt the MITRE ATT&CK framework as part of their security operations. SA vendors responded by mapping their solutions to the framework for detection, investigations, and threat hunting. Vendors with the most-advanced capabilities also show which parts of MITRE ATT&CK are covered in customers' environments.
- **Have a vision for extended detection and response (XDR).** Endpoint detection and response (EDR) and security analytics have long been on a collision course. The overlap of these capabilities combine EDR with analytics from other technologies, providing highly enriched telemetry, speedy investigations, and automated response actions.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our report Now Tech: Security Analytics Platforms, Q3 2020.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Security Analytics Platforms, Q4 2020

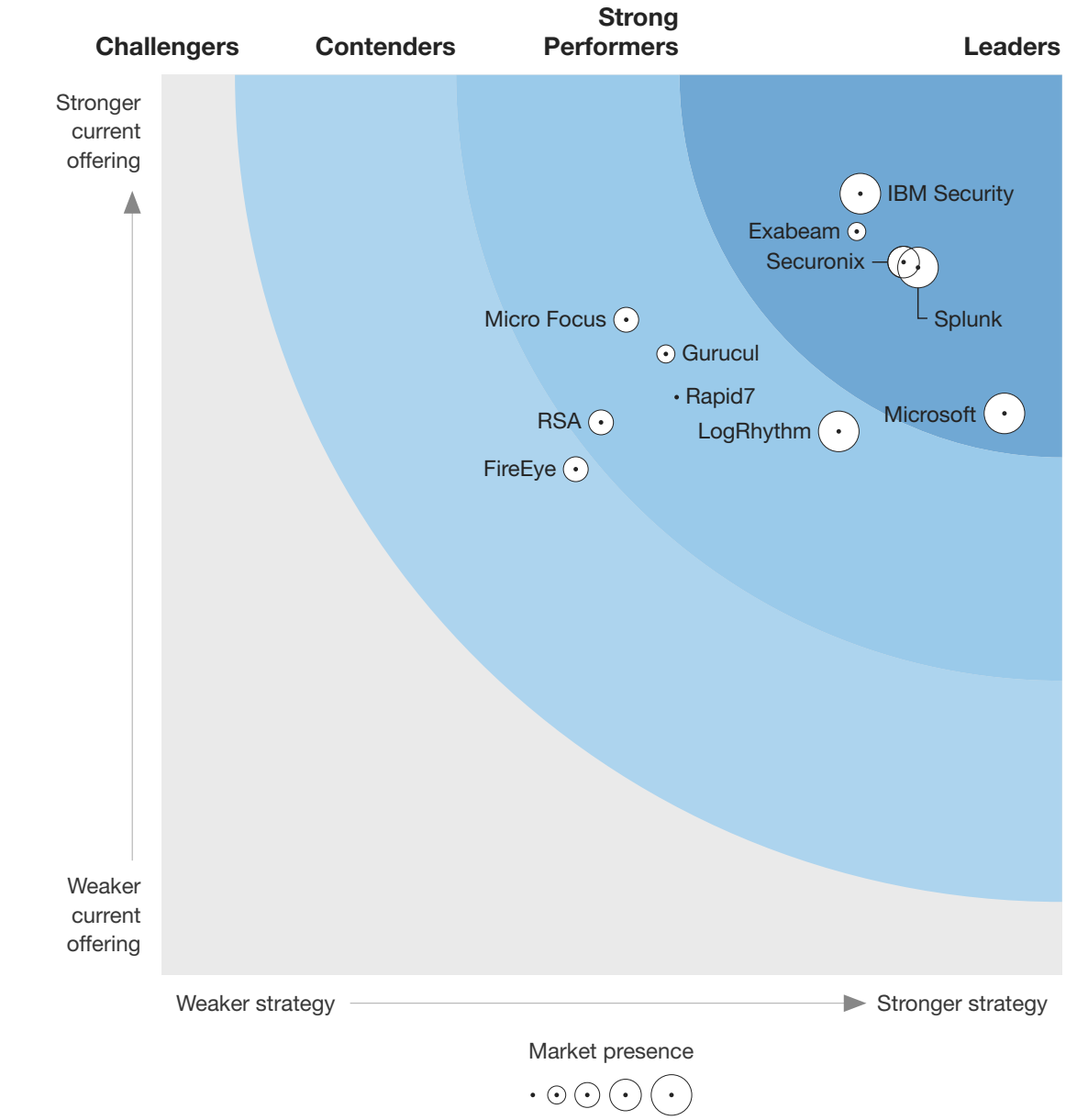

FIGURE 2 Forrester Wave™: Security Analytics Platforms Scorecard, Q4 2020

	Forrester's weighting	Exabeam	FireEye	Gurucul	IBM Security	LogRhythm	Micro Focus	Microsoft	Rapid7	RSA	Securonix	Splunk
Current offering	50%	4.13	2.81	3.45	4.34	3.02	3.64	3.12	3.21	3.07	3.96	3.93
Deployment and data architecture	5%	3.40	3.40	3.80	3.40	3.40	2.20	4.20	3.80	1.80	5.00	2.20
Visibility	10%	3.00	3.00	3.00	5.00	3.00	3.00	1.00	3.00	5.00	3.00	3.00
Correlation capabilities	10%	5.00	3.00	5.00	5.00	3.00	5.00	5.00	5.00	3.00	5.00	5.00
Threat detection	20%	4.60	3.00	3.40	4.60	4.20	4.20	2.60	4.20	3.00	3.80	4.20
ATT&CK mapping	10%	5.00	3.00	3.00	5.00	3.00	3.00	3.00	1.00	3.00	3.00	3.00
Custom detections	5%	5.00	3.00	5.00	5.00	3.00	3.00	3.00	1.00	3.00	5.00	5.00
Security orchestration	10%	3.00	5.00	1.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00	3.00
Compliance	5%	3.00	1.00	1.00	5.00	5.00	5.00	3.00	3.00	3.00	3.00	5.00
Platform experience	5%	3.60	3.60	1.60	3.00	3.00	3.00	3.00	3.60	1.60	3.00	4.40
Analytics	10%	3.60	1.60	5.00	3.00	1.60	4.40	4.40	3.00	3.00	5.00	3.60
Risk scoring and prioritization	10%	5.00	1.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00	5.00
Strategy	50%	3.86	2.30	2.80	3.88	3.76	2.58	4.68	2.86	2.44	4.12	4.20
Product vision	25%	3.00	3.00	3.00	5.00	3.00	3.00	5.00	3.00	3.00	5.00	5.00
Planned enhancements	25%	5.00	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
Performance	25%	5.00	1.00	3.00	3.00	3.00	1.00	5.00	3.00	1.00	5.00	3.00
Commercial model	15%	3.40	3.00	3.00	4.20	3.40	2.20	4.20	3.40	2.60	3.80	3.00
Technology partners	10%	1.00	1.00	1.00	5.00	5.00	5.00	3.00	1.00	3.00	3.00	5.00
Market presence	0%	1.40	3.00	1.80	4.60	4.60	3.00	4.20	1.00	3.00	3.40	5.00
Enterprise adoption	80%	1.00	3.00	1.00	5.00	5.00	3.00	5.00	1.00	3.00	3.00	5.00
Average deal size	20%	3.00	3.00	5.00	3.00	3.00	3.00	1.00	1.00	3.00	5.00	5.00

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

Vendor Offerings

Forrester included 11 vendors in this assessment: Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix, and Splunk (see Figure 3). We invited Fortinet and McAfee to participate in this Forrester Wave, but they chose not to participate, and we could not make enough estimates about their capabilities to include them in the assessment as nonparticipating vendors.

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Exabeam	Exabeam Security Management Platform 2020.1
FireEye	FireEye
Gurucul	Unified Security and Risk Analytics (USRA) 8.0
IBM Security	IBM Security QRadar 7.4.0; IBM Security Resilient v37
LogRhythm	LogRhythm NextGen SIEM Platform 7.5
Micro Focus	ArcSight 2020.2
Microsoft	Azure Sentinel
Rapid7	InsightIDR
RSA	RSA NetWitness Platform v11.4; RSA NetWitness Orchestrator v6.0
Securonix	Securonix Next-Gen SIEM 6.3
Splunk	Splunk Enterprise 8.0; Splunk Cloud; Splunk Enteprise Security (ES) 6.2; Splunk User Behavior Analytics (UBA) 5.0; Splunk Phantom 4.9; Splunk Mission Control (MC)

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

› **IBM Security is building an open security platform in the cloud.** The future of IBM's security analytics platform is based on its CloudPak For Security platform, built in on OpenShift cloud-native architecture and based on its RedHat acquisition, which seeks to deliver multiple security

services in the IBM Cloud. Capabilities like IBM QRadar Advisor with Watson, X-Force threat intelligence, and the integration with IBM's managed security services are differentiators. SOAR is delivered via IBM Security Resilient as an add-on. Pricing options include a consumption-based license determined by the quantity of events ingested into the system, or an unlimited license for ingestion, analytics, and storage based on the number of servers in the environment.

Customer references appreciate IBM's global reach, technical support, and innovation. They noted that many new capabilities are delivered as apps, not as improvements to the core product, and that some visualizations appear antiquated. Weaknesses mentioned include the complexity of on-prem installations and the ability to locate product documentation and support pages. Large, global enterprises with complex security needs should evaluate IBM.

› **Splunk is on a security analytics mission.** Most enterprises use Splunk in some capacity for infrastructure monitoring, application analytics, or security. For security, Splunk is building its future around its cloud-based unified security platform, Mission Control. Splunk has been slower to the cloud than others in this evaluation and cloud-native newcomers to the security analytics market, but the firm is now making cloud a focus for the future. Splunk offers a range of pricing options, including workload-based, use-case based, and the traditional consumption-based model determined by the volume of data the platform ingests.

Flexibility and the ability to conduct fast searches over large data volumes are key Splunk features. Reference customers state that speed, versatility, and customization are key strengths. They also laud Splunk for its tremendous and engaged user community. By contrast, pricing concerns continue to be an issue. Splunk has made efforts to improve its pricing and provide more flexibility, but customer references agree that cost is a weakness. Enterprises that want a highly customizable solution that enables fast searches across large data volumes should consider Splunk.

› **Securonix offers SaaS-based, multitenant security analytics.** Securonix initially launched as a SUBA vendor in 2008, adding SIEM functionality in 2016 to compete as a security analytics platform. The vendor has since added automation as an add-on feature or delivered via third-party integrations. Securonix has shifted to a cloud-first SaaS deployment strategy with flexible deployment options, including multitenancy, which makes it attractive for MSSP partners. The vendor's pricing approach is based on the number of identities monitored.

Customer references comment that Securonix's analytics-based approach, behavioral analytics, and real-time enrichment are strengths. On the downside, reference customers note delays with log ingestion and small bugs in the UI as weaknesses. Enterprises and midmarket companies seeking a flexible security analytics platform or multitenant solution should evaluate Securonix.

› **Exabeam excels on user experience.** Exabeam launched in 2014 with a focus on SUBA, launched its SIEM and SOAR offerings in 2017, and has grown quickly. Exabeam Security Management Platform combines integrated analytics, log management, and SOAR that operate as a platform in combination or as standalone solutions. Incidents are largely based on user behavior

and assets, and security analysts are able to view events in timelines for investigation. Exabeam offers multiple pricing models, including pricing based on the number of employees monitored or amount of data ingested.

Reference customers note usability and insight into individual user behaviors as strengths. They also view the vendor's pricing strategy as an attractive feature. Customer references caution that the vendor's fast growth may be detrimental to its ability to adequately support customers and commented that new features are often buggy on initial release. Midmarket companies and enterprises seeking a modular yet integrated SA platform with a focus on user behavior should consider Exabeam.

› **Microsoft roars into the security analytics market.** Microsoft Azure Sentinel, the vendor's SA solution, was announced at the 2019 RSA security conference, then launched in September 2019 to great fanfare. The vendor's entry into the security analytics space captivated security buyers. Microsoft's bold move to allow the ingestion of Microsoft Azure and Microsoft Office 365 activity logs into Sentinel at no cost makes the solution attractive to enterprises invested in Azure and Microsoft 365. Pricing for other data sources is consumption-based determined by the amount of data ingested into the platform. In only one year, Microsoft has gained a great deal of market traction.

While Azure Sentinel is innovative and takes full advantage of the Azure infrastructure, it is still a very new offering. This newness shows in areas like the ability to bring in third-party logs. Customer references note the ease of integration across other Microsoft products like Azure, Microsoft 365, and Windows Defender for Endpoint as a big benefit. Reference customers call out automation as another strength. Microsoft's push into security does present a problem for security pros who don't want a single vendor providing security at multiple layers, including the cloud, endpoint, and email. Those seeking a single-vendor solution, however, will appreciate the integrations across technologies. Enterprises of all sizes that are heavily invested in Microsoft Azure and Microsoft 365 should consider Microsoft.

Strong Performers

› **LogRhythm offers deployment flexibility for enterprise security analytics.** LogRhythm, acquired by private equity firm Thoma Bravo in July 2018, is a long-time player in the SIEM market. Long known as a midmarket solution, LogRhythm provides a feature-rich SA platform suitable for enterprises of all sizes. The vendor includes SIEM, analytics, and automation as part of the base license, but SUBA, delivered via its Cloud AI, is an add-on purchase. LogRhythm delivers as on-premises appliances, virtual appliances, software, and SaaS. In 2020, in an effort to give customers pricing flexibility, LogRhythm introduced its True Unlimited data plan pricing, a model that promises unlimited data usage as an alternative to its consumption-based model which prices determined by messages per second (MPS).

Customer references remark that the solution is easy to use and scales well for growth. They also note customer support as a strength. Reference customers mention that the included automation and Quick Response capabilities are not on par with standalone SOAR solutions and that support for third-party cloud and SaaS environments don't meet expectations. Midmarket and enterprise customers seeking a full-featured security analytics platform with flexible deployment options should consider LogRhythm.

- **Gurucul brings risk-based analytics to data.** Gurucul emerged as a big-data security analytics vendor in 2010 and evolved as a security analytics platform provider covering SUBA, SIEM, and SOAR. Gurucul offers its own big-data architecture and also supports customer-provided, third-party data stores. The vendor allows customers to customize its analytics models or build their own via Gurucul STUDIO. Gurucul provides customizable machine learning behavior profiling, predictive risk-scoring, and risk prioritized alerts. Gurucul deploys as software that can run on customer-supplied hardware or virtual infrastructure, appliance, or as SaaS. The vendor offers subscription, perpetual, and SaaS licensing. Pricing for the solution is modular, with separate modules for SIEM, SUBA, custom log storage, SOAR, and NAV with enterprise pricing available. Monitoring is priced based on the number of identities/entities monitored.

  Customer reference feedback indicates that Gurucul's machine learning models, risk scoring, and flexibility are strengths. Weaknesses mentioned by reference customers include solution complexity and the vendor's go-to-market efforts. Enterprises looking for a robust, customizable security analytics tool with risk-based prioritization should consider Gurucul.

- **Micro Focus puts the security analytics platform pieces together.** Micro Focus made strategic acquisitions of a SUBA vendor (Interset) and a SOAR vendor (Atar Labs), adding to its existing ArcSight SIEM which has lagged behind the rest of the market for several years. ArcSight was long the vendor of choice for some of the world's largest enterprises and government agencies, although many long-time customers moved away from the platform. Micro Focus is making some progress but is very late to embrace cloud delivery compared to others in this evaluation. ArcSight deploys as hardware appliances, containers, or software that can be deployed in virtual and cloud environments. Micro Focus is currently working to deliver a full SaaS version. The solution is priced based on EPS, and the SUBA capability is sold as an add-on and licensed by the number of managed entities.

  Micro Focus is investing in the security analytics space, adding capabilities to its platform, which is an encouraging sign. Reference customers mentioned integration with other products, correlation, and global support as strengths. They noted slow search performance, support, and the management console as shortcomings. Enterprises invested in other parts of the Micro Focus portfolio and those seeking a vendor with a long history in the SA space should evaluate Micro Focus.

- **Rapid7 combines multiple security capabilities in the cloud.** Rapid7's InsightIDR platform is entirely cloud delivered, providing log management, SIEM, SUBA, and SOAR that integrate with its vulnerability management platform. The vendor also bundles in endpoint visibility and detection, file

integrity monitoring, and deception capabilities. The acquisition of NetFort in 2019 gave the vendor NAV capabilities to provide visibility to network traffic and behaviors, which is available as an add-on. The vendor can add services to give customers access to delivery expertise and support for internal teams. As a SaaS offering, licensing is a subscription model, and pricing is based on the number of assets monitored.

Customer reference feedback indicates ease of deployment and operation as strengths. 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.

› **RSA provides a unified platform for security analytics.** RSA is now operating independently following a spinout from Dell Technologies and an acquisition by a consortium of investors in September 2020.[1] The vendor provides SIEM, NAV, SUBA, and SOAR through its RSA NetWitness Platform offering. RSA NetWitness provides threat detection and visibility through a combination of log, endpoint, and packet data analysis. SOAR is delivered via RSA NetWitness Orchestrator, built via an OEM agreement with Threat Connect, 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, although a full SaaS capability is on the roadmap. Pricing is determined by the various components through a combination of consumption-based pricing for RSA NetWitness Logs and RSA NetWitness Network and user-based pricing for RSA NetWitness UEBA, RSA NetWitness Endpoint, and RSA NetWitness Orchestrator.

RSA integrates RSA NetWitness with its own EDR functionality for detection and response in addition to supporting third-party EDR vendors. Customer references appreciate the unified platform and strengths like the combination of log and packet analysis. Reference customers noted that the solution is complex, the UI is not intuitive, and that the learning curve can be steep for new users. Organizations using RSA Archer for governance, risk, and compliance (GRC) and those looking for a high level of visibility into their network traffic and integrated EDR should consider RSA.

Contenders

› **FireEye provides an integrated approach with Helix.** FireEye combines its security analytics and automation capabilities in its Helix platform. Helix encompasses log retention, SIEM, threat intelligence, threat hunting, and SOAR. The vendor sells Helix as a standalone SaaS solution or they can package it with other FireEye solutions like network security, email security, endpoint security, and Cloudvisory. The acquisition of Verodin in 2019 gave the ability to visualize coverage to the MITRE ATT&CK framework as an add-on purchase, although Helix allows threat hunting and custom detections using ATT&CK. Mandiant services are also available to augment Helix, giving access to security expertise, or to provide managed services. The vendor's pricing is consumption-based, tied to EPS.

Customer references appreciate the inclusion of threat intelligence, ability to access FireEye experts, and the level of integration with other FireEye security tools. While the solution is well-integrated across the FireEye portfolio, there is no central admin console or dashboard for all FireEye products, which customer references noted as a weakness. Reference customers also mentioned that there is a lack of documentation for the SOAR component of Helix and that the availability of skilled resources to manage the platform is an issue. Enterprises that leverage the vendor for other parts of their security infrastructure should consider FireEye.

Evaluation Overview

We evaluated vendors against 27 criteria, which we grouped into three high-level categories:

- **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 deployment and data architecture, visibility, correlation capabilities, threat detection, ATT&CK mapping, custom detections, security orchestration, compliance, platform experience, analytics, and risk scoring and prioritization.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, planned enhancements, performance, commercial model, and technology partners.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise adoption, and average deal size.

Vendor Inclusion Criteria

Forrester included 11 vendors in the assessment: Exabeam, FireEye, Gurucul, IBM Security, LogRhythm, Micro Focus, Microsoft, Rapid7, RSA, Securonix, and Splunk. Each of these vendors has:

- **Product revenue.** Vendor must have $50 million in product-line revenue for their security analytics platform.
- **Core functionality.** Vendor must have a security analytics platform that includes mature SIEM and SOAR capabilities. Provided SOAR capabilities may be offered as a proprietary or white labeled part of the solution.
- **Forrester mindshare.** Forrester clients often discuss the participating vendors during inquiries and interviews. To ensure relevance to Forrester clients and the quality of the references being provided, it is required that the product has been generally available and not undergone significant changes in the past six months.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by August 18, 2020 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

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

Endnotes

[1] Source: "RSA® Emerges as Independent Company Following Completion of Acquisition by Symphony Technology Group," RSA press release, September 1, 2020 (https://www.rsa.com/en-us/company/news/rsa--emerges-as-independent-company).

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

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.