

# The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018

The 14 Providers That Matter Most And How They Stack Up

by Jeff Pollard and Claire O'Malley

August 20, 2018

## Why Read This Report

In our 23-criteria evaluation of global managed security services providers (MSSPs), we identified the 14 most significant ones — Accenture, Alert Logic, AT&T Business, BAE Systems, CenturyLink, Deloitte, IBM, NTT, Optiv Security, Secureworks, Symantec, Trustwave, Verizon, and Wipro — and researched, analyzed, and scored them. This report shows how each provider measures up to help security leaders make the right choice.

## Key Takeaways

### **Secureworks, Alert Logic, IBM, And Symantec Lead The Pack**

Forrester's research uncovered a market in which Secureworks, Alert Logic, IBM, and Symantec are Leaders; Deloitte, NTT, Trustwave, CenturyLink, and Wipro are Strong Performers; Optiv Security, Accenture, BAE Systems, and AT&T Business are Contenders; and Verizon is a Challenger.

### **Security Pros Are Looking For Context, Criticality Scoring, And Prioritization**

The global MSSP market is growing because security professionals see services as a way to address their top challenges, and they increasingly trust providers to act as strategic partners based on a shared understanding of business needs.

### **Machine Learning, Automation, And Mobile Apps Are Key Differentiators**

As hybrid cloud deployments and increasingly complex technology exacerbate information security challenges, the best MSSPs are distinguishing themselves by using machine learning to detect and prioritize events; security automation to resolve incidents; and user interfaces that are easy to navigate.

# The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018

## The 14 Providers That Matter Most And How They Stack Up

by [Jeff Pollard](#) and [Claire O'Malley](#)  
with [Christopher McClean](#), [Elsa Pikulik](#), and [Peggy Dostie](#)  
August 20, 2018

---

### Table Of Contents

- 2 **MSSPs Are Rescuing Security Teams Drowning In New Technology**
    - The MSSP Market Will Continue To Grow And Will Begin To Look Different
  - 3 **Global Managed Security Services Providers Evaluation Overview**
    - Evaluated Vendors And Inclusion Criteria
  - 4 **Vendor Profiles**
    - Leaders
    - Strong Performers
    - Contenders
    - Challengers
- 
- 11 **Supplemental Material**

### Related Research Documents

- [The Forrester Wave™: Information Security Consulting Services, Q3 2017](#)
- [The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016](#)
- [Lessons From The Forrester Wave™: MSSPs, North America, Q3 2016](#)



**Share reports with colleagues.**  
Enhance your membership with  
[Research Share.](#)

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

## MSSPs Are Rescuing Security Teams Drowning In New Technology

For every problem that a technology investment solves, it introduces a new one. And just like with medication, the side effects can sometimes be worse than the original ailment. The amount of cybersecurity innovation taking place at the moment is unprecedented, but each innovation requires new skills, new workflows, and extra capacity to handle all the alerts and remediation actions it produces. These factors encourage security pros to turn to MSSPs to solve problems of complexity, obtain needed expertise, and increase the global reach of their program.

### The MSSP Market Will Continue To Grow And Will Begin To Look Different

There is a race to enter the managed security services market, and the explosion of vendors taking aim at recurring services revenue models will make it challenging for security pros to assess which vendors offer the right services, delivery model, and price. When assessing potential providers, it's vital to understand how familiar they are with top of key trends:

- › **Customers crave context.** Far too many MSSPs still pride themselves on the quantity of log data they collect, alerts they produce, and escalations they send to a client. But customers want to understand the threat intelligence associated with the events, including potential attribution, motivation, and next steps of an adversary. They need system criticality scores to understand the business risk of potential response actions and the vulnerability context to understand what happened and how to stop it from happening again. “Alert-factory” MSSPs are no longer valuable.
- › **Automation, remediation, and chat capabilities have revamped escalations.** Longtime MSSP customers know that most incident response workflows used to start with an email, then included a ticket, and possibly a phone call when necessary. Now, federated chat capabilities offer a virtual war room for collaboration during critical events, automation allows customers to preprogram response actions and escalation procedures, and some providers are offering comprehensive investigation and remediation capabilities by combining traditional managed services with managed detection and response.<sup>1</sup>
- › **Mobile applications are now a critical element of the MSSP user experience.** MSSPs are more often engaging with customers through easy-to-use mobile apps and responsive web portals. Mobile applications allow security teams to adjust the priority of an event, initiate a deeper investigation, or choose a preprogrammed response action with just a few touches on a smart phone screen. This capability removes the MSSP's reliance on ticketing systems, emails, and phone calls, and it speeds up the resolution time for security issues.

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

## Global Managed Security Services Providers Evaluation Overview

To assess the state of the global MSSP market, Forrester evaluated the strengths and weaknesses of the most significant vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors using 23 criteria, which we grouped into three 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 alert and event analysis and prioritization for networks, endpoints, and applications; proactive detection; solution usability; business and technical value; incident management; artificial intelligence and machine learning; automation capabilities; and dashboard, user interface, and reporting capabilities.
- › **Strategy.** Placement on the horizontal axis indicates the strength of each vendor's strategy, which includes product road map, user experience road map, and go-to-market approach.
- › **Market presence.** Represented by the size of the markers on the graphic, the market presence scores reflect each vendor's number of clients and service revenue.

### Evaluated Vendors And Inclusion Criteria

Forrester included 14 vendors in the assessment: Accenture, Alert Logic, AT&T Business, BAE Systems, CenturyLink, Deloitte, IBM, NTT, Optiv Security, Secureworks, Symantec, Trustwave, Verizon, and Wipro. Each of these vendors has (see Figure 1):

- › **At least \$100 million in annual revenue from its managed security services business.** Each participant has a large, globally available business offering a combination of managed and monitored security services.
- › **At least 300 managed security services clients.** Each participant has a large base of clients headquartered in North America, Europe, and Asia Pacific.
- › **At least 100 dedicated security operations center (SOC) personnel.** Each participant has a minimum of 100 staff members providing services in a multitenant customer support model.
- › **Mindshare with Forrester clients.** Forrester clients often discuss the participating vendors during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, have warranted inclusion because of technical capabilities and market presence.

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

**FIGURE 1** Evaluated Vendors And Product Information

<b>Vendor</b>	<b>Product evaluated</b>
Accenture	Accenture Managed Security Services
Alert Logic	Alert Logic Cloud Defender
AT&T Business	AT&T Cybersecurity Solutions
BAE Systems	BAE Systems Managed Security Services
CenturyLink	CenturyLink Global Security Services
Deloitte	Deloitte Managed Vigilant Services
IBM	IBM Managed Security Services
NTT	NTT Managed Security Services
Optiv Security	Optiv Managed Security Services
Secureworks	Secureworks Managed Security Services
Symantec	Symantec Managed Security Services
Trustwave	Trustwave Managed Security Services
Verizon	Verizon Managed Security Services
Wipro	Wipro Managed Security Services

## Vendor Profiles

We intend this evaluation of the global MSSP 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 2 and see Figure 3). Click the link at the beginning of this report on Forrester.com to download the tool.

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

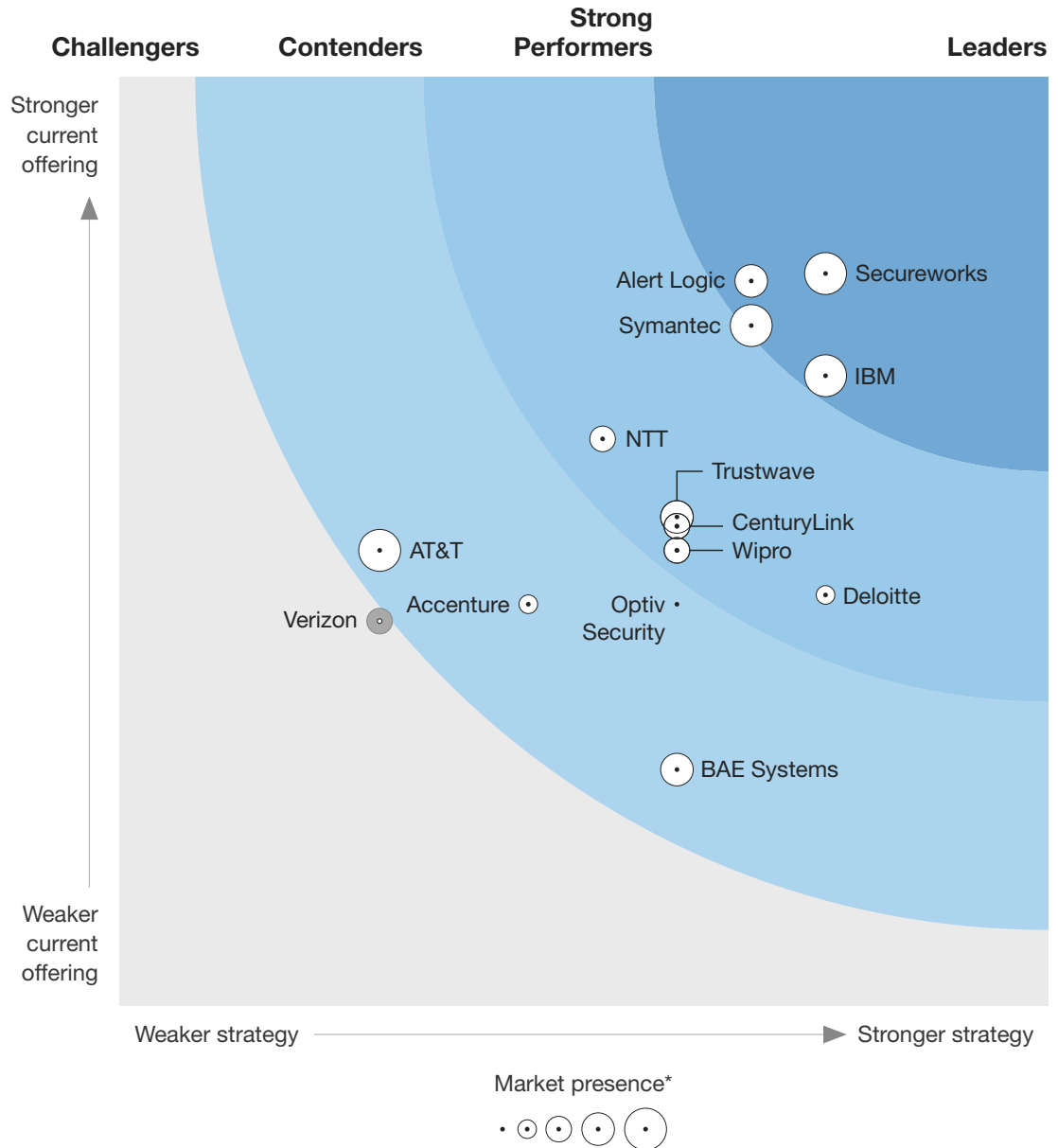
The 14 Providers That Matter Most And How They Stack Up

**FIGURE 2** Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018

**THE FORRESTER WAVE™**

Global Managed Security Services Providers (MSSPs)

Q3 2018



\*A gray marker indicates incomplete vendor participation.

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

**FIGURE 3** Forrester Wave™: Global Managed Security Services Providers (MSSPs) Scorecard, Q3 2018

	Forrester's weighting	Accenture	Alert Logic	AT&T Business	BAE Systems	CenturyLink	Deloitte	IBM
<b>Current offering</b>	50%	2.16	3.90	2.45	1.27	2.58	2.21	3.39
Analysis and priority: network/endpoint	14%	2.31	3.63	1.65	0.99	2.97	1.65	2.97
Analysis and priority: applications/hunting	14%	2.31	3.63	1.65	0.99	2.97	1.65	2.97
Solution usability	14%	2.00	4.00	3.00	3.00	2.00	1.00	4.00
Business and technical value	14%	3.00	5.00	2.00	1.00	1.00	3.00	3.00
Incident management process	14%	2.33	3.00	3.00	1.00	3.67	3.00	3.00
AI, ML, and automation	14%	1.00	4.00	3.00	1.00	2.00	3.00	5.00
Reporting capabilities	14%	2.33	4.33	3.00	1.00	3.67	2.33	3.00
<b>Strategy</b>	50%	2.20	3.40	1.40	3.00	3.00	3.80	3.80
Service provider road map	40%	1.00	3.00	1.00	3.00	3.00	5.00	3.00
User experience road map	40%	3.00	3.00	1.00	3.00	3.00	3.00	5.00
Go-to-market approach	20%	3.00	5.00	3.00	3.00	3.00	3.00	3.00
<b>Market presence</b>	0%	2.00	4.00	5.00	4.00	3.00	2.00	5.00
Number of clients	50%	1.00	5.00	5.00	5.00	3.00	1.00	5.00
Service revenue	50%	3.00	3.00	5.00	3.00	3.00	3.00	5.00

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

**FIGURE 3** Forrester Wave™: Global Managed Security Services Providers (MSSPs) Scorecard, Q3 2018 (Cont.)

	Forrester's weighting	NTT	Optiv Security	Secureworks	Symantec	Trustwave	Verizon*	Wipro
<b>Current offering</b>	50%	3.05	2.16	3.94	3.66	2.63	2.07	2.45
Analysis and priority: network/endpoint	14%	3.63	1.65	3.63	4.29	1.65	1.65	2.31
Analysis and priority: applications/hunting	14%	3.63	1.65	3.63	4.29	1.65	1.65	2.31
Solution usability	14%	2.00	4.00	3.00	4.00	3.00	3.00	3.00
Business and technical value	14%	3.00	3.00	5.00	3.00	3.00	1.00	1.00
Incident management process	14%	2.33	1.00	3.67	4.33	3.67	3.00	1.00
AI, ML, and automation	14%	4.00	1.00	4.00	3.00	2.00	2.00	4.00
Reporting capabilities	14%	3.00	3.00	5.00	3.00	3.67	2.33	3.67
<b>Strategy</b>	50%	2.60	3.00	3.80	3.40	3.00	1.40	3.00
Service provider road map	40%	3.00	3.00	3.00	3.00	3.00	1.00	3.00
User experience road map	40%	3.00	3.00	5.00	5.00	3.00	1.00	3.00
Go-to-market approach	20%	1.00	3.00	3.00	1.00	3.00	3.00	3.00
<b>Market presence</b>	0%	3.00	1.00	5.00	5.00	4.00	3.00	3.00
Number of clients	50%	3.00	1.00	5.00	5.00	5.00	3.00	3.00
Service revenue	50%	3.00	1.00	5.00	5.00	3.00	3.00	3.00

**Leaders**

- › **Secureworks combines an overhauled user interface with its superior threat research.** In recent years, Secureworks has set itself apart from other MSSPs by bringing its Counter Threat Unit to the forefront of its service delivery. After years of investments in back-end capabilities, Secureworks turned its attention to client experience. Secureworks has always been able to articulate the technical value of managed security services, and it now can clearly articulate the business value as well. Clients expressed frustration at long response times to nonsecurity issues such as device health alerts, and they complained about the lack of detail SMS escalations provided.
- › **Alert Logic sets itself apart by expediting client deployments on any infrastructure.** Alert Logic offers one of the most comprehensive deployments of supervised machine learning among all MSSPs, with SOC analysts continually refining rulesets and detection algorithms. Alert



**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

## The 14 Providers That Matter Most And How They Stack Up

Logic applies system criticality measurements to prioritize incident management efforts, using automation, asset grouping and tagging, and machine learning to determine the sensitivity of users and systems. Alert Logic can also help clients make a business or technical case for the value of managed security services during the presales process. Clients expressed that Alert Logic services become expensive when they try to scale them across the business and that the portal needs to provide better business metrics alongside its technical metrics.

- › **IBM uses its product portfolio with great effect to strengthen service delivery.** While IBM offers a vendor-neutral version of its managed security services, client satisfaction soars when the services rely on IBM products. Managed security services based on QRadar are a real differentiator for IBM, with clients specifying that the tight integration between product management, development, SOC, and support teams reduces complexity for them. IBM's size does create weaknesses, though, with clients mentioning that the do-it-all approach did not always work well and that front-end sales teams did not always take the time to understand a client's needs before prescribing a solution.
- › **Symantec accelerates decision making by providing excellent context for alerts.** Symantec incorporates threat intelligence and vulnerability context information into its workflow, user interface, and escalation processes, differentiating itself from other MSSPs in the Forrester Wave. Symantec's incident governance process and escalation methods provide clear details on how events will be handled, and they offer numerous customization options for clients. Reference clients mention strong responsiveness, prioritization, and analysis as key benefits of Symantec's services. However, they described the company's channel-only go-to-market strategy as complicating the purchase process and serving as a negative aspect of working with it. Symantec customers were more likely than other MSSP customers to say that their provider was slow to adopt and support newer technologies.

**Strong Performers**

- › **Deloitte brings its global delivery capabilities to managed security services clients.** Deloitte's geographically distributed SOCs offer in-region (and in many cases in-country) delivery options, which better equips Deloitte to satisfy clients' data residency and transit requirements compared with other providers. Clients also cite security maturity, expertise, and flexibility of service delivery as high-value benefits of working with Deloitte. Clients reported lengthy deployment timeframes as a problem, and while many praised the company's localized delivery, the geographic distribution sometimes means that experts are not available in-region to meet immediate client needs.
- › **NTT offers a broad portfolio with MSS for Oracle and SAP environments.** After acquiring Solutionary, NTT pledged to integrate its security capabilities under one umbrella, and the company has executed on that vision. The widened portfolio incorporates managed security services for critical enterprise software implementations such as SAP HANA and Oracle ERP suites. NTT clients

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

## The 14 Providers That Matter Most And How They Stack Up

noted that the blended approach of consulting and managed security services is a strength during the onboarding process. Clients also reported that NTT sometimes failed to incorporate threat intelligence into alerts and struggled with securing cloud infrastructure.

- › **Trustwave has entered rapid growth mode as it eyes international markets.** The Singtel acquisition has been good for Trustwave, creating inroads into international markets and providing capital to accelerate Trustwave's plans to grow abroad. Trustwave has built or expanded a number of international SOCs and is ahead of most other MSSPs when it comes to user interface localization. Trustwave clients noted rapid response capabilities and global delivery as key strengths of the service but expressed concerns about the lack of APIs for integration and the lack of mobile support.
- › **CenturyLink experiences growing pains as it merges with Level 3 Communications.** CenturyLink and Level 3 Communications coming together muddies the water for clients of both companies. CenturyLink brings granular, role-based access control based on geography, role, region, or service as a key differentiator from other MSSPs, and the company provides substantial detail to help clients understand what steps it has taken for incidents and alerts. Clients indicated that they valued the strong event correlation and advanced warnings that CenturyLink provides as part of its services but noted that the company doesn't always have the expertise needed to handle events and that the deployment of services was complex and time consuming.
- › **Wipro's managed services maintain a strong link to IT infrastructure and operations.** Customers can see Wipro's legacy in IT operations in the company's custom dashboards and metrics, which include a heavy focus on IT assets and log sources. Wipro has made strategic venture capital investments in a number of security technologies that it incorporates into its service portfolio. While Wipro can deliver services using a variety of client technologies, QRadar features prominently in its sales demonstrations. Clients value Wipro's flexible operating models and expertise deploying and managing specific technologies. However, clients also stated that inconsistent delivery experiences and the inability to replace staff quickly were particularly problematic.

## Contenders

- › **Optiv Security leans on expertise more than technology to create value.** Optiv Security has a mature approach to threat intelligence, incident response, and escalations, but it requires manual interactions from experts to deliver these capabilities to clients. Optiv Security clients feel that the accuracy and level of detail provided are strengths of the company's services. However, as Optiv Security continues to invest in its MSS portfolio, it will need to enhance its client experience. Clients complained about the lack of integrations and the inability to customize reports as issues Optiv Security needs to address.
- › **Accenture packs onshore, offshore, and multitenant MSS into a single package.** Accenture's comprehensive set of offerings requires more coordination and project management from clients than offerings from other firms, but it allows the company to create a highly customized and

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

## The 14 Providers That Matter Most And How They Stack Up

variable-cost delivery model that clients can tailor to their preferences. With the exception of threat intelligence, Accenture is heavily reliant upon the technology investments clients make, with limited in-house technologies to support its services. Clients stated that Accenture's threat hunting maturity and responsiveness to issues are key strengths, but they complained that Accenture struggles to replace onshore resources quickly and is slow to resolve contractual issues.

- › **BAE Systems balances legacy services with innovations in threat detection.** BAE Systems struggles with a dated portal and poor user experience for its legacy security services, but the company has begun to revamp its reporting features and has plans for an updated user interface. New reports feature comparisons, baselines, and metrics to support CISO-level decisions. Clients mentioned that the level of threat research and technical analysis are the things they value most from the service; however, they repeatedly mentioned the poor user interface and lack of consistency in the security operations teams as problems BAE Systems needs to solve.
- › **AT&T Business is working to become a primary security partner for enterprise clients.** AT&T Business understands its enterprise buyers and uses its expertise in large, complex global deployments as part of its value. The company has also made a number of investments in security platforms and its service delivery organization, resulting in higher levels of client satisfaction. AT&T Business emphasizes the size of its network as a key value proposition for its services, but the company fails to distinguish itself from any other telecom that offers managed security services. Clients expressed that AT&T Business provides value by integrating managed security with managed network services, but conversely, many AT&T Business clients are ambivalent about the company's services, noting that they are bundled as part of a broader telecom purchase.

## Challengers

- › **Verizon clings to its network and data breach investigation report to remain relevant.** While Verizon's partnership with Splunk gives clients an avenue to escape its dated and underinvested platform, it also makes Verizon reliant upon Splunk to make the service better. Verizon has doubled down on its partnership approach for service delivery, adding services with third-party scoring platforms as part of a new Verizon Risk Rating service. Unfortunately, Verizon fails to add much value. The company has made some small investments in intellectual property, acquiring Needl, a threat-hunting company, which should improve the company's analytics and threat-hunting services when fully integrated. Verizon declined to participate in our research. Scores are based on Forrester estimates.

## The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018

### The 14 Providers That Matter Most And How They Stack Up

## 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 iOS and Android.**

Stay ahead of your competition no matter where you are.

## Supplemental Material

### Online Resource

The online version of Figure 2 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 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 May 18, 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.

**The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018**

The 14 Providers That Matter Most And How They Stack Up

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

### The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we 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.

### Endnotes

<sup>1</sup> Security and risk professionals use MDR services to offer assurance that the business is not currently compromised, to turn internal investigations over to efficient experts, and to get on-demand access to a seasoned incident response team. Security leaders should use Forrester's Now Tech report to understand the value they can expect from an MDR provider and select vendors based on size and functionality. See the Forrester report "[Now Tech: Managed Detection And Response \(MDR\) Services, Q2 2018.](#)"

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](mailto:clientsupport@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.