The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016
The 11 Providers That Matter Most And How They Stack Up
by Jeff Pollard
August 30, 2016

Why Read This Report
In our 36-criteria evaluation of the managed security services market, we identified the 11 most significant providers — Alert Logic, AT&T, BAE Systems, CenturyLink, Hewlett Packard Enterprise, IBM, SecureWorks, NTT Security, Symantec, Trustwave, and Verizon — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals choose the right partner to meet their unique business needs.

Key Takeaways
Alert Logic, SecureWorks, And IBM Lead The Pack

Security Pros Look To Augment Skills, Reduce Complexity, And Improve Quality Of Protection
Companies face a staff shortage and an expertise gap. MSSPs represent a mitigation mechanism for both problems, with superior talent and domain-specific skills that the organization can’t find or can’t justify retaining.

Alignment, Customization, And Flexibility Are Key Differentiators
As legacy managed security services capabilities become outdated and less effective, improved business alignment, customization, and flexibility dictate which providers lead the pack.
The Forrester Wave™: Managed Security Services Providers, North America, Q3 2016

The 11 Providers That Matter Most And How They Stack Up

by Jeff Pollard
with Christopher McClean, Joseph Blankenship, Claire O’Malley, Trevor Lyness, and Peggy Dostie
August 30, 2016

Table Of Contents

2 MSSPs Abound With Talent While Security Teams Struggle
2 MSSPs Remain Relevant With Integration, Flexibility, And Customization
3 Managed Security Services Provider Evaluation Overview
   Evaluated Vendors And Inclusion Criteria
6 Vendor Profiles
   Leaders
   Strong Performers
   Contenders
12 Supplemental Material

Notes & Resources

Forrester conducted services provider evaluations in May 2016 and interviewed 44 vendor and user companies, including: Alert Logic, AT&T, BAE Systems, CenturyLink, Hewlett Packard Enterprise, IBM, NTT Security, SecureWorks, Symantec, Trustwave, and Verizon.

Related Research Documents

Get Your Managed Security Services In Order
Plan Your Security Sourcing Strategy For The Next Five Years
The State Of Security Services 2016
MSSPs Abound With Talent While Security Teams Struggle

Customers commit to MSSPs seeking three outcomes: reduced complexity, improved quality of protection, and greater competency within specialized skillsets.\textsuperscript{1} The security labor shortage means that quality of protection and specialized skills will remain drivers for the foreseeable future, while the accelerating business technology agenda will continue to increase the complexity necessitating outside help. Other key industry trends assure that MSSP engagement will continue to grow:

\begin{itemize}
  \item \textbf{The security vendor landscape is beyond unwieldy.} An explosion in security innovation has yielded so many emerging technologies that security leaders struggle to find reality within the dream of security promises. The overwhelming number of security conference exhibitors reflects how bad the problem is getting: RSA 2016 had more than 550, Black Hat 2016 had 256, and Infosec Europe 2016 had 378.\textsuperscript{2} MSSPs can help customers navigate this maze by blessing and supporting the technologies that are ready for prime time.
  \item \textbf{MSSPs are starting to get their heads in the clouds, and that's a good thing.} Organizations continue to expand their use of cloud services, and security leaders need to reap the benefits of cloud as their business colleagues have. On-demand capacity, elasticity, and consumption-based pricing models can transform security operations and procurement. MSSPs now enter app marketplaces, allowing security leaders to receive the same benefits as their technology and business peers, shifting from long-term fixed-price enterprise service contracts to variable cost models with shorter commitments.
  \item \textbf{MSSPs offer solutions that rise above the limitations of customer products.} The new competing priorities in security budgets sit between detect-and-respond and prevent-and-protect. Customer environments will feature selections of each. MSSPs can augment preventive solutions with detection via analytics and act as an advisor for mitigation strategies when detection-only controls find a threat. This is a unique fusion of capabilities that creates actual value by reducing fragmentation from technologies ignorant to the existence of anything other than their own isolated feature set. Through the MSSP, customers can avoid expense-in-depth spending strategies by getting more value from better use of existing investments.
\end{itemize}

MSSPs Remain Relevant With Integration, Flexibility, And Customization

The MSSP market faces pressures as customers demand more, competitors offer more, and vendors in adjacent industries join the fray. Customization requests threaten traditional MSSP economies of scale, and vendors that cling to outdated approaches see customer satisfaction dip. Changing customer expectations are causing many changes in MSSP strategies and portfolios:

\begin{itemize}
  \item \textbf{Customers will consume services how they want, not how MSSPs order them to.} Customers expect highly customized and tailored delivery to meet their individual needs. This may include the ability to opt out of services from certain geographic regions, demands for specialized vertical or
functional expertise, and preferences to interact via phone, email, text, ticket, or instant message. Customers are willing to pay a premium for this kind of white-glove service, and when it's done right, they find it uninteresting to explore other providers.

› **Security orchestration initiatives require more data from MSSPs.** MSSPs can’t be a place to just store logs. They also can’t offer restrictive time frames for access to collected data or excessive fees to provide it on-demand. Customer expectations require MSSPs to receive, retain, and provide access that doesn’t differ from the experience of storing them onsite. The rapid adoption of orchestration and automation technologies means that MSSPs must offer more data and more API functions to customers so they can initiate their own response workflows.

› **MSSP portals are getting much-needed cosmetic surgery.** MSSPs now understand the value of making their user interface user friendly for customers. Many providers completed a facelift of their user interface in the past 18 months, and others are on the way. These new interfaces include visualizations, link analysis, and investigation workflows to increase customer engagement and break the habit of customers waiting for a ticket or an alert.

› **Two legacy MSSP pricing models still dominate, while a third is rising.** Service providers remain comfortable with two ways for customers to pay: an expensive, yearly, all-inclusive contract, or a low-cost initial agreement based on volume, with upcharges based on interaction, changes, and/or investigative scope. Consumption-based models similar to cloud-based services exist for a growing subset of MSSP vendors as well.

› **MSSPs are intermingling their service offerings.** Customers now find vendors that combine traditional consulting, software-as-a-service products, and managed security services. The best MSSPs are coming to market with an approach that clearly defines customer involvement and responsibility, transfers security knowledge to the customer's security team, and helps customers strategize an exit from MSSP services in the future should they desire.

› **Customers will trade neutrality for greater efficacy.** Instead of simply managing whatever products their customers demanded, MSSPs are now endorsing particular products. This sends a message to customers that the MSSP will provide the best possible service through that product because they built the service around it. As added benefit, customers don’t mind shedding the burden of product selection.

**Managed Security Services Provider Evaluation Overview**

To assess the state of the managed security services market, Forrester evaluated the strengths and weaknesses of the top providers. After examining past research, user needs, and vendor and expert interviews, we developed a comprehensive set of 36 evaluation criteria, which we grouped into three high-level categories:
Current offering criteria measure the providers’ capabilities. We evaluated the ability of MSSPs to provide: 1) business technology agenda alignment; 2) service delivery of security operations; 3) available security services; 4) threat detection and security operations enhancement; 5) expertise and competency; 6) service onboarding and optimization; 7) user interface and integrations; and 8) customer experience.

Strategy criteria evaluate go-to-market competency. We evaluated: 1) product and service vision; 2) R&D investment in 2015 or latest completed fiscal year; and 3) MSSP employee growth in 2015 or latest completed fiscal year.

Market presence criteria gauge size and relevance. We evaluated: 1) North American client growth rate for 2015 or latest completed fiscal year; 2) North American revenue for 2015 or latest completed fiscal year; and 3) North American revenue growth rate for 2015 or latest completed fiscal year.

Evaluated Vendors And Inclusion Criteria

Forrester included 11 vendors in the assessment: Alert Logic, AT&T, BAE Systems, CenturyLink, Hewlett Packard Enterprise, IBM, SecureWorks, NTT Security, Symantec, Trustwave, and Verizon. Each of these vendors has (see Figure 1):

- **A complete suite of managed security services.** We included vendors that offer a complete suite of managed and monitored solutions that enhance existing security investments and workflows.

- **A strong MSSP presence in North America.** To be included, a significant portion of the vendor’s managed security service revenue had to come from clients in North America, including a minimum of 400 clients.

- **Significant interest from Forrester customers.** Forrester considered the level of interest from our clients based on inquiries, advisories, consulting engagements, and other interactions.

- **Redundant and resilient security operations centers (SOCs).** Vendors needed to have at least two SOCs to participate, and they must provide redundant failover if a disaster makes a SOC inoperable. The vendor also needed to demonstrate that it can provide physical redundancy as well as system, network, and personnel redundancy.

- **A critical mass of dedicated SOC analysts and engineers.** All included providers have more than 100 SOC analysts or engineers who spent at least 80% of their time dedicated to managed security services.
The 11 Providers That Matter Most And How They Stack Up

### FIGURE 1 Evaluated Vendors: Managed Security Services Provider Information And Selection Criteria

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Evaluated product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Logic</td>
<td>Alert Logic Cloud Defender</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>AT&amp;T Security Services</td>
</tr>
<tr>
<td>BAE Systems</td>
<td>BAE Systems Managed Security Services</td>
</tr>
<tr>
<td>CenturyLink</td>
<td>CenturyLink MSS 2.0</td>
</tr>
<tr>
<td>Hewlett Packard Enterprise</td>
<td>HPE Managed Security Services</td>
</tr>
<tr>
<td>IBM</td>
<td>IBM Managed Security Services</td>
</tr>
<tr>
<td>NTT Security</td>
<td>The NTT Security federated Global Service Platform (GSP)</td>
</tr>
<tr>
<td></td>
<td>ActiveGuard Security and Compliance Portal v4.14.17</td>
</tr>
<tr>
<td>SecureWorks</td>
<td>SecureWorks Managed Security Services</td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Managed Security Services</td>
</tr>
<tr>
<td>Trustwave</td>
<td>Trustwave Managed Security Services</td>
</tr>
<tr>
<td>Verizon</td>
<td>Verizon Managed Security Services</td>
</tr>
</tbody>
</table>

### Vendor selection criteria

- **A complete suite of managed security services.** We included vendors that offer a complete suite of managed and monitored solutions that enhance existing security investments and workflows.

- **A strong MSSP presence in North America.** To be included, a significant portion of the vendor’s managed security service revenue had to come from clients in North America.

- **Significant interest from Forrester customers.** Forrester considered the level of interest from our clients based on our various interactions, including inquiries, advisories, and consulting engagements.

- **Redundant and resilient security operation centers (SOCs).** Vendors needed to have at least two SOCs to participate, and they must provide redundant failover if a disaster makes a SOC inoperable. The vendor also needed to demonstrate that it can provide physical redundancy as well as system, network, and personnel redundancy.

- **A critical mass of dedicated SOC analysts and engineers.** The provider had more than 100 SOC analysts or engineers who spent at least 80% of their time dedicated to the provider's managed security services.
Vendor Profiles

This evaluation of the managed security services market is intended to be a starting point only. We encourage clients to view the detailed product evaluations and adapt criteria weightings to fit their individual needs using the Forrester Wave Excel-based vendor comparison tool (see Figure 2).

FIGURE 2 Forrester Wave™: North American Managed Security Services Providers, Q3 ’16

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.
Alert Logic has a head start in cloud, and it shows. As one of the first MSSPs to build on-demand and usage-based models ready for cloud environments, Alert Logic possesses an advantage for clients migrating toward off-premises solutions. More than any other provider, Alert Logic offers API-based integrations with clear and robust documentation, setting the stage for improved automation and orchestration. The company’s UI is clean and easy to use, and its dashboards are cloud native.
While Alert Logic excels in the cloud, it has a lower number of SOCs worldwide than top competitors. Clients working with the company will also need to contract with other providers for full-scale incident response needs. Despite these limitations, Alert Logic is an excellent fit for clients looking to secure their current or planned cloud migrations, clients requiring a provider than can span seamlessly between hybrid architectures, and those that demand strong API capabilities for integrations.

SecureWorks continues to blend exceptional threat research and incident response. Many providers use machine learning to produce security rules, which they then test and deploy for customers; SecureWorks is one of the first to apply machine learning in real time, enhancing protection and minimizing false positives. The company has also unified the Counter Threat Unit research team and Security Operations team into a single organizational chart with defined processes for information sharing and escalations. Client events and incidents are worked by SOC analysts and CTU team members in tandem when necessary, resulting in a differentiated experience for their customers.

Unfortunately, SecureWorks finds itself late to the cloud market, with its current offerings best suited for on-premises environments. The company has fallen behind in developing its own intellectual property, relying on partnerships that may be at risk if and when acquisitions occur. Additionally, being one of the largest MSSPs in revenue and client count can make change difficult. SecureWorks is best for clients looking for a steady and knowledgeable MSSP with over a decade of experience deploying and delivering managed security services. Clients that need a wide range of managed and professional services will also find SecureWorks a good option.

IBM balances a deep product portfolio with technology-neutral services. IBM’s presence as a strategic vendor across every vertical and region gives the company tremendous opportunity. With a few false starts in integrating prior acquisitions like ISS, IBM now seems to have the leadership, buy-in, and vision to execute. The company also exhibits flexibility, for example offering the log ingestion and analytic capabilities of QRadar in a multitenant or on-premises delivery model. Global SOCs and multilanguage support are strengths of IBM. The acquisition of Resilient Systems and an expanded use of Watson for security analytics could also position IBM as a leader in analytics and automation-based services.

IBM’s acquisition-heavy history comes with technical architecture challenges and multiple interfaces. For example, QRadar and other interfaces are more modern; however, other services have antiquated interfaces that are difficult to navigate and have limited features. Not all IBM SOCs provide all services, which limits clients’ flexibility should they want to opt out of a geographic region. Existing IBM customers, globally diverse organizations that require diverse language support, and fans of a large portfolio of services and products from a single vendor will see value in IBM’s approach to managed security.
Strong Performers

› **CenturyLink emerges with an innovative approach to architecture.** Not content to merely provide managed security services as a value-added option, CenturyLink made a substantial investment in its user interface and the method by which it collects log data. A consumption-based pricing model lets customers select what logs to send and in what volume, and dictate when additional assistance is needed for resolution. The company’s modern user interface with APIs is complemented by robust log collection capability.

While CenturyLink is a global service provider, its managed security services are specific to US-based SOCs. Continued refinement and integration of security operations staff, threat research, and incident response capabilities are needed for a holistic portfolio. Security leaders needing transparency from their service provider for cost control will prefer CenturyLink’s pricing model. Security operations staff will enjoy the full-text indexing and interaction with log data that CenturyLink facilitates in its user interface.

› **Symantec pressures competitors with multiple pricing options.** Symantec has a long history in managed security services and distinguishes itself with an array of pricing options for customers to choose from. Symantec offers clients the ability to send any and all log data, which they accept as part of their enterprise services agreement. Recent diversification of its product portfolio adds malware analysis, improved threat intelligence, and incident response capabilities. Symantec also provides cybersimulation and training to SOC personnel, which enhances client teams and creates an exit strategy should the client choose.

Symantec’s pricing model remained its primary innovation in the managed security services space until the launch of additional services like incident response and threat intelligence. Numerous executive changes at the company amid spin-offs and acquisitions should give customers pause. However, clients needing to send lots of logs to one provider that have found other MSSPs’ pricing options prohibitive, organizations looking to obtain security services and build the skills of their internal team, and those requiring a vendor with a rich history of managed security should consider Symantec.

› **NTT Security accelerates road map plans and global delivery capability.** NTT’s acquisition of Solutionary seemed to have little customer impact until recent announcements including a name change to NTT Security and formation of the security services arm of NTT. The company is one of the strongest at expressing business and technical value through white papers, return-on-investment calculations, and extensive content on the benefits of managed security. Strong correlation and security analytics are available through its MSS platform. The ability to deliver globally across territories and expand the partner ecosystem are significant improvements that came from the acquisition.
NTT Security still faces challenges gaining traction among large enterprise organizations. There’s a deep professional services portfolio that includes technical hands-on work as well as strategic consulting; however, the company struggles to produce the quantity and quality of research of its larger competitors. Customers looking for strong correlation and analytics capabilities, global scale, and help articulating the benefits of managed security services should evaluate NTT Security.

› **Trustwave continues to expand its offering, but compliance remains its strength.** Trustwave understands customers struggling with diverse requirements from PCI and has built its services and portal around that segment. However, it has also diversified its managed security services offering, consulting, and intellectual property. The company’s acquisition by Singtel opens up new geographies to expand delivery as well. Trustwave clients vary in sophistication but primarily use the company’s services through the SOC, relying on the expertise of analysts to guide them through events and incidents.

Trustwave’s user interface is aged and lacks customizations, visuals, and data exports. It also lacks APIs for integration with ticketing systems and customer technologies for automation and orchestration. Customers with franchises in the hospitality, retail, and restaurant verticals will find Trustwave a strong potential partner. Those organizations that want to work with an MSSP that has extensive experience in compliance-focused managed security services, those with limited security expertise preferring live interactions, and those without deep engineering requirements for integrations should explore Trustwave.

› **BAE Systems has breathed life into Silversky’s portfolio.** BAE Systems’ acquisition of Silversky brought enterprise resources and capital it lacked prior to the acquisition. BAE Systems also added advanced threat research and intelligence to Silversky’s nascent capabilities in that area. A deep and wide range of security services — including legacy managed and monitoring services — combined with advanced analytics offers customers a range of options.

An aging user interface with substantial limits underwhelms in comparison with newer MSSP portals. Customers won’t find APIs or advanced report features available, either. Teams that aren’t planning on customized integrations or those that prefer to work directly with SOC teams rather than user interfaces will see benefits from BAE Systems’ offering.

**Contenders**

› **Hewlett Packard Enterprise (HPE) specializes in ITO engagements.** A willingness to offer flexible delivery models, including security within IT outsourcing contracts, management of customers’ on-premises infrastructure, or multitenant managed security services, defines HPE’s current approach to solving client problems. An obvious area of expertise is augmenting clients’ existing Arcsight installations. The ability to keep all data on-premises and rely on SOC personnel to assist in security operations is particularly attractive and not a model many competitors match.
Managed application security services is also a distinctive element for HPE — where the company goes beyond simple application scanning and testing to full static and dynamic analysis services using the Fortify product.

The future of HPE became less murky following the merger with CSC. As a services provider, HPE’s primary challenge is that it’s highly product-centric, requiring an existing or planned investment in Arcsight or Fortify. While its cloud platform removes the physical infrastructure from that equation, it’s still an Arcsight-based offering. Clients that want to keep all data onsite, those with existing Arcsight investments, or those that like the Arcsight technology but want to remove the pain of managing SIEM infrastructure could find the approach HPE offers appealing. Before companies start working with HPE, they should have a full understanding of the approach CSC will take, including how HPE will transition from a reliance on intercompany intellectual property to an external entity.

› **AT&T has diversified its portfolio with services but remains network-centric.** With a deep history of working with complicated regulatory requirements in the enterprise, AT&T removes complexity for customers with a bundled network and MSSP offerings. With insights from the traffic that passes across its wired and wireless networks, AT&T has access to a rich data set on threat actor traffic from command-and-control and DDoS activities. A solid user interface with planned enhancements delivers a good user experience — although the lack of APIs will hold back more sophisticated teams.

Clients not using AT&T for existing network services will find less value in the company as an MSSP. Understanding how clients benefit from the network data AT&T collects is challenging (having lots of data isn’t the same as using it for security insights). The company also has a gap in application security expertise for assessment, mitigation, and protection outside of DDoS and web application firewall. Enterprises struggling with vendor complexity or challenged by large-scale global projects will find AT&T a capable partner.

› **Verizon has invested in new MSSP integrations and applications.** Core managed security services, including log analysis and alerting, had resided on Verizon’s aging platform until the 2016 integration between Verizon and Splunk, which now allows clients to apply managed security services to data resident in an on-premises platform via the application. Customers can also choose to send log data to Verizon directly. The company has strength in transport-specific functions like managed DDoS, and its Security Management Program is differentiated in the space in how well it handles compliance, regulatory frameworks, and security services.

Lack of customization for security alerts and a lack of APIs for its ticketing system and user interface limit clients’ ability to integrate with other systems. Optimization of client technologies is not a core part of Verizon’s services and instead requires professional services engagement. Organizations working with Verizon for bandwidth services, as well as those wanting expertise in regulatory requirements, should investigate the company’s managed security services offering.
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

**Online Resource**
The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

**Data Sources Used In This Forrester Wave**
Forrester used a combination of four data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by August 16, 2016:
Hands-on lab evaluations. Vendors spent one day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology. We evaluated each product using the same scenario(s), creating a level playing field by evaluating every product on the same criteria.

Vendor surveys. Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

Product demos. We asked vendors to conduct demonstrations of their products’ functionality. We used findings from these product demos to validate details of each vendor’s product capabilities.

Customer reference calls. To validate product and vendor qualifications, Forrester also conducted reference calls with one of each vendor’s current customers.

The Forrester Wave Methodology

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

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

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

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

1 Security leaders cede control of capabilities they offer the enterprise by misallocating resources and putting too much emphasis on technology. See the “Plan Your Security Sourcing Strategy For The Next Five Years” Forrester report.

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.