FORRESTER®

For: Security &
Risk Professionals

The Forrester Wave™: Managed Security Services: North America, Q4 2014

by Ed Ferrara, November 18, 2014 | Updated: November 21, 2014

KEY TAKEAWAYS

IBM, Dell SecureWorks, And AT&T Lead The Pack

Forrester's research uncovered a market in which the Leaders are IBM, Dell SecureWorks, AT&T, SilverSky, Verizon, Solutionary, Trustwave, Wipro, and CSC. Leidos, HP, Symantec, and CenturyLink are Strong Performers, but all the vendors have important strengths and the potential to be a strategic partner.

Device Management And Continuous Monitoring Are Foundational

At its core, an MSSP must provide two kinds of basic services. These foundational services are security device management and continuous threat and breach monitoring. All of the vendors reviewed do these functions very well, and it shows in the clustering of vendors in the Leader and Strong Performer categories.

Portals, Threat Intelligence, And Security Analytics Differentiate The Vendors

Security information and event management (SIEM) technology has become outdated. Vendors can no longer rely on traditional SIEM solutions to detect and stop cyberbreach. New security analytics and threat intelligence will make the difference going forward for MSSPs and their customers in defending against cyberbreach.

Access The Forrester Wave Model For Deeper Insight

Use the detailed Forrester Wave model to view every piece of data used to score participating vendors and create a custom vendor shortlist. Access the report online and download the Excel tool using the link in the right-hand column under "Tools & Templates." Alter Forrester's weightings to tailor the Forrester Wave model to your specifications.

NOVEMBER 18, 2014
UPDATED: NOVEMBER 21, 2014

The Forrester Wave™: Managed Security Services: North America, Q4 2014

Thirteen Vendors That Have What It Takes To Take On Your Biggest Security Challenges

by Ed Ferrara
with Christopher McClean and Michael Caputo

WHY READ THIS REPORT

Forrester's 26-criteria evaluation of managed security service providers (MSSPs) included the 13 most significant vendors in the North American market that security and risk professionals can turn to for solving some of their most important security challenges — AT&T, CenturyLink, CSC, Dell SecureWorks, HP, IBM, Leidos, SilverSky, Solutionary/NTT, Symantec, Trustwave, Verizon, and Wipro. This report details how well each vendor met our criteria and where they stand in relation to each other. This report will help you refine your selection criteria and choose the right partner for your outsourced security needs.

Table Of Contents

Notes & Resources

Forrester conducted service evaluations in June, July, and August 2014 and interviewed over 40 vendor and user companies, including: Ameriprise Financial, AT&T, CenturyLink, CSC, Dell SecureWorks, Deltec Information Solutions, HP, IBM, Kentucky Department of Education, Leidos, Mondelez International, SilverSky, Smashburger, Solutionary/NTT, Symantec, Trustwave, Verizon, and Wipro.

Related Research Documents

Detecting Cyberthreats With Fraud-Based Advanced Analytics Technology
August 4, 2014

Market Overview: Managed Security Services, Europe, Q2 2014
April 22, 2014

Security Operations Center (SOC) Staffing
August 2, 2013

THE MSSP MARKET IS GROWING MORE SOLID AND STABLE

The challenges facing security and risk professionals this year are all too similar to the challenges faced 16 months ago when we last looked at enterprise-class managed security service providers (MSSPs). The difference is the volume of issues they face, including close senior management scrutiny, an increasing number of threats and attacks, limited staff, difficulty recruiting, a bewildering number of technology choices, and a clear move by many enterprises to the cloud.

MSSPs have responded nobly to these challenges, and the market is showing many signs of maturity:

- **Vendor revenue continues to grow, but not as rapidly.** The managed security market continues to grow because security and risk professionals see MSSPs as one way to address their biggest challenges. Although MSSP revenue growth rates have shown a slight decline, the growth rate in the number of contracts is increasing. This is a sign that large companies that could outsource security have already done so and now smaller companies with lower overall contract values are moving some or all of the security services to MSSPs.

- **Many MSSPs have comparable services and approaches.** Differentiation between MSSPs is hard. All of the firms offer similar or identical services, often using the same technology. Also, when comparing staff experience and expertise, we find similar profiles from all the vendors. They have similar training programs and recruit similar candidates. As the market matures, these firms will differentiate themselves in new areas of security analytics, threat intelligence, information portals, and customer service.

- **Smaller MSSPs have great capabilities and can compete with their larger cousins.** The managed security market remains very competitive, with all the firms reviewed providing comparable offerings in both device management and continuous monitoring. Smaller vendors are scoring as well as their larger counterparts in many criteria, showing strong investment in technology and staffing. Size does matter for many security and risk professionals, but smaller firms can hold their own.

THE ENTERPRISE MSSP MARKET REQUIRES SOPHISTICATED CAPABILITIES

Forrester divides the MSSP market into three divisions based on the size of the service provider: Enterprise MSSPs are the largest, and they serve the biggest and most complex customers.[1] Size, however, is just one criterion of many, and it may not be the most important. We looked at a number of different factors to determine which firms should be included in the North American Enterprise MSSP Forrester Wave, choosing 13 firms based on their ability to offer:

- **Security analytics and threat intelligence.** The traditional approach to security monitoring has been security information and event management (SIEM). This approach — even with technology enhancements — has proven to be too slow; detecting an attack could take weeks if

not months in some cases. The process and science of threat detection is changing quickly with the introduction of new and more sophisticated technologies. For example, new approaches based on fraud detection techniques now provide much more real-time and predictive intelligence.[2] The best MSSPs have embraced this technology to upgrade their continuous monitoring capabilities. Firms that have a strong focus on security analytics include Dell SecureWorks, HP, IBM, SilverSky, Solutionary, and Symantec.

- **Business value.** We had high hopes that all firms included in this Forrester Wave would have a strong understanding of their clients' business needs. What we found was "not so much." The industry is still very focused on the technical issues and challenges of security. The ability to help CISOs develop a strong business case for their services still remains elusive for most MSSPs. IBM, SilverSky, Solutionary and Trustwave — all of which came out as Leaders — are notable exceptions to this rule. These firms were able to describe how they helped clients reduce costs, improve revenue, financially manage risk, and protect their customers' data. This is a welcome and much needed change, critical for the industry's continued growth.

- **Technical value.** All the reviewed firms use both proprietary and licensed technology to provide a suite of services to outsource security operations. They also secure their clients' business by providing the necessary technical skills many companies lack today. Vendors in this space have to bring strong staff technical training, experience, and certifications, as well as device management, security information/event management (SIEM), security analytics, and threat intelligence capabilities using state-of-the-art technology.

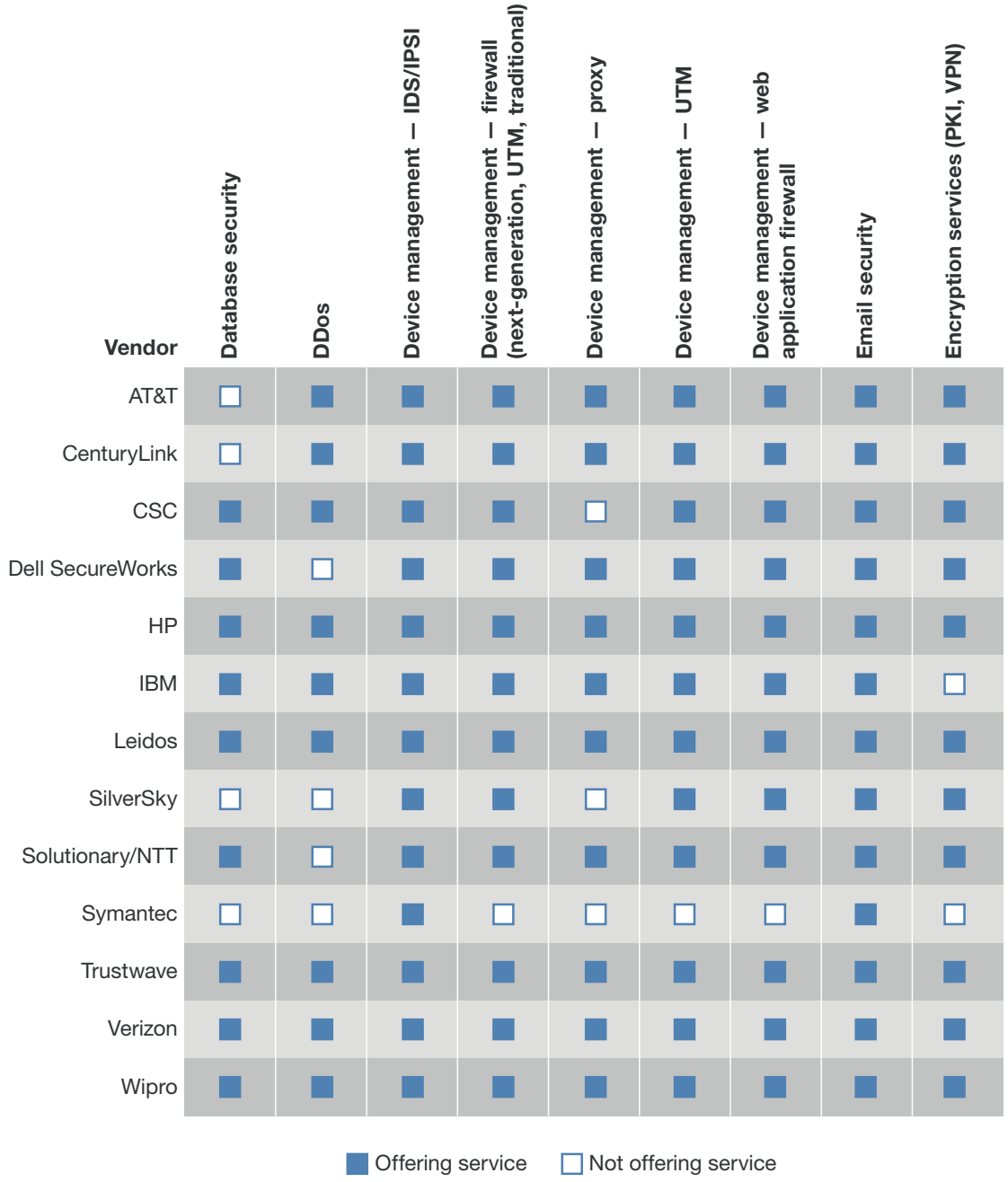
- **Effective information portals.** An MSSP's portal is the de facto communication channel for most customer support issues, event management, and status reporting. We evaluated the vendors' portals on how well they meet clients' information needs and how easily they integrate with the customer environment. The vendors have made significant advancements with these portals over the past two years. The best ones enable customers to customize information by role, group security devices by type and business function, drill down on security events to look at the raw log data and threat intelligence, build custom reports, and compare their events with events across the vendor's broader network of customers.

- **Broad service offerings.** The MSSPs we looked at offer a broad variety of different security services in two categories: security IT outsourcing (ITO) and security business process outsourcing (BPO). ITO offerings, such as device, endpoint, and server management, are now considered commodity services performed most cost-effectively by MSSPs' offshore locations in India or Eastern Europe, where labor costs are lower. BPO offerings are more sophisticated and require stronger process integration between the client and vendor. Examples of BPO include continuous monitoring, data loss prevention, insider threat detection, event detection and management, and threat intelligence services (see Figure 1 and see Figure 2).

- **Experienced and trained staff.** The firms reviewed here, in general, all have very capable staff. The majority of the firms employ analysts and engineers with at least five years of experience and at least one advanced security certification. They rely on this experience to identify and address cyberthreats in different ways, ranging from simple monitor-and-alert services all the way to complete incident response management.

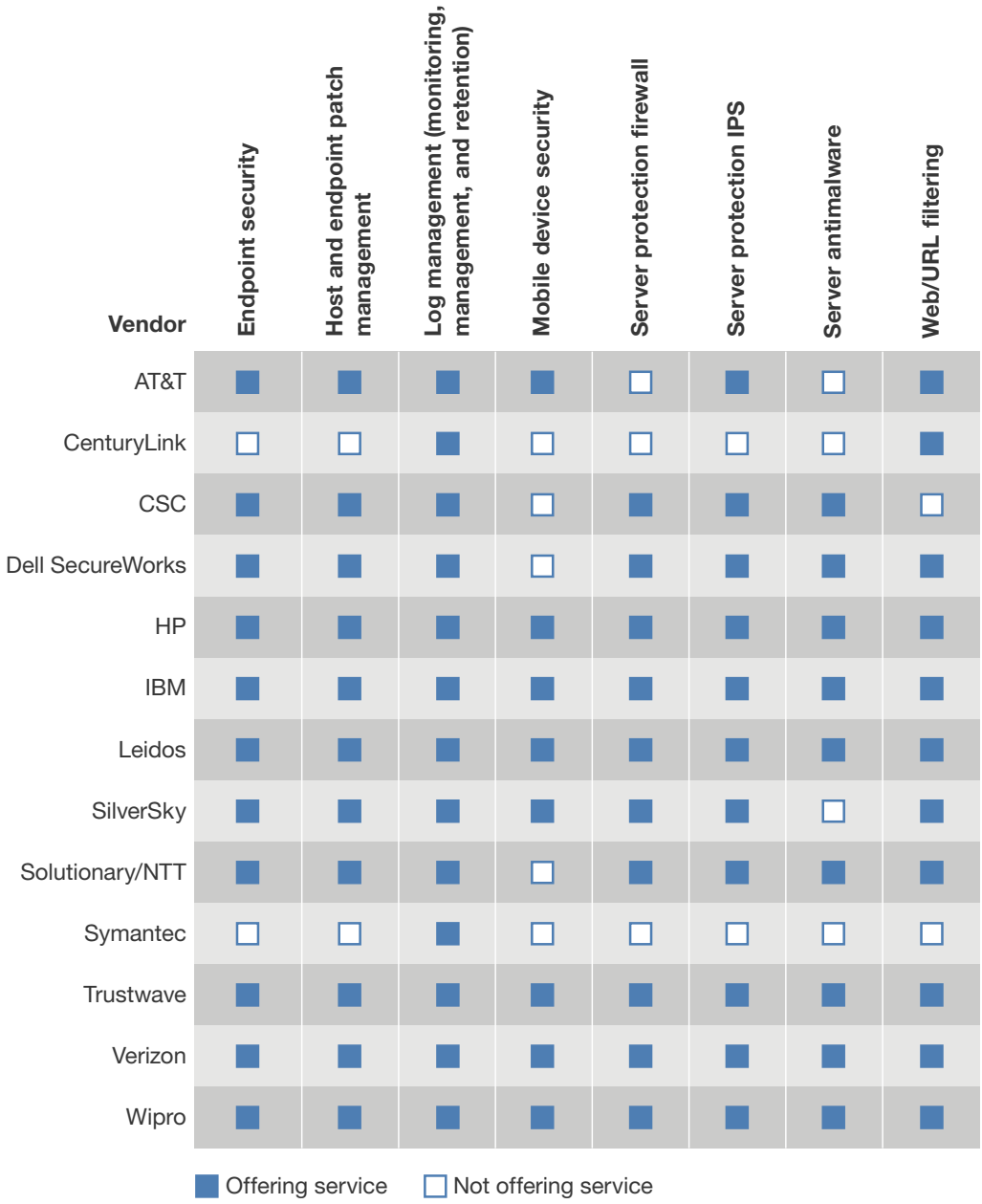
- **Strong focus on customer service.** There was variability in the client responses, but, overall, the MSSPs in this Forrester Wave did well in the customer satisfaction category. Clients gave their providers especially positive feedback on their pricing and quality of service. When the clients needed help, the best MSSPs didn't simply point to the contract to set service boundaries, but demonstrated flexibility and worked with their clients to resolve the issue.[3]

Figure 1 Managed Security ITO Services



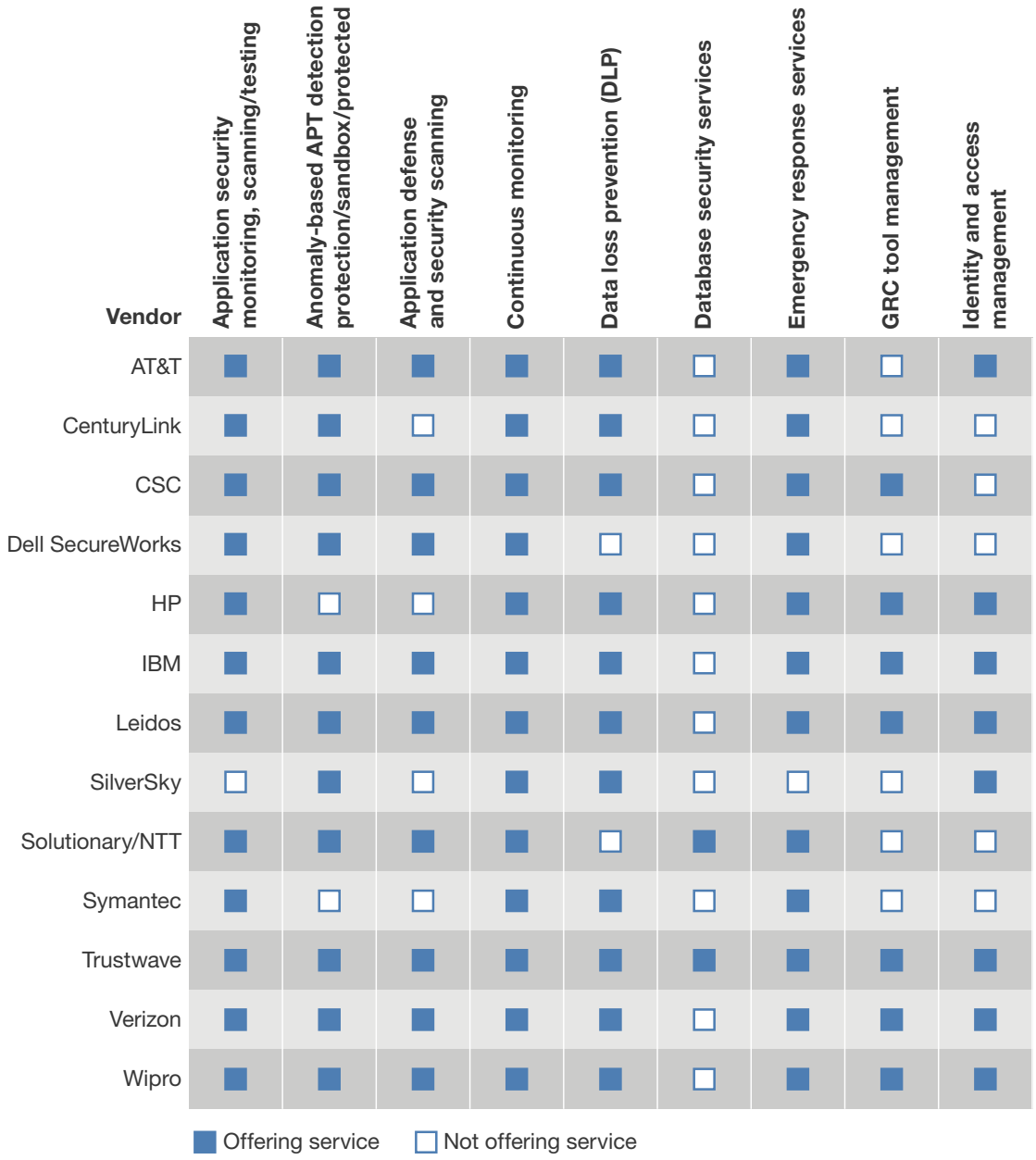
113183 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 1 Managed Security ITO Services (Cont.)



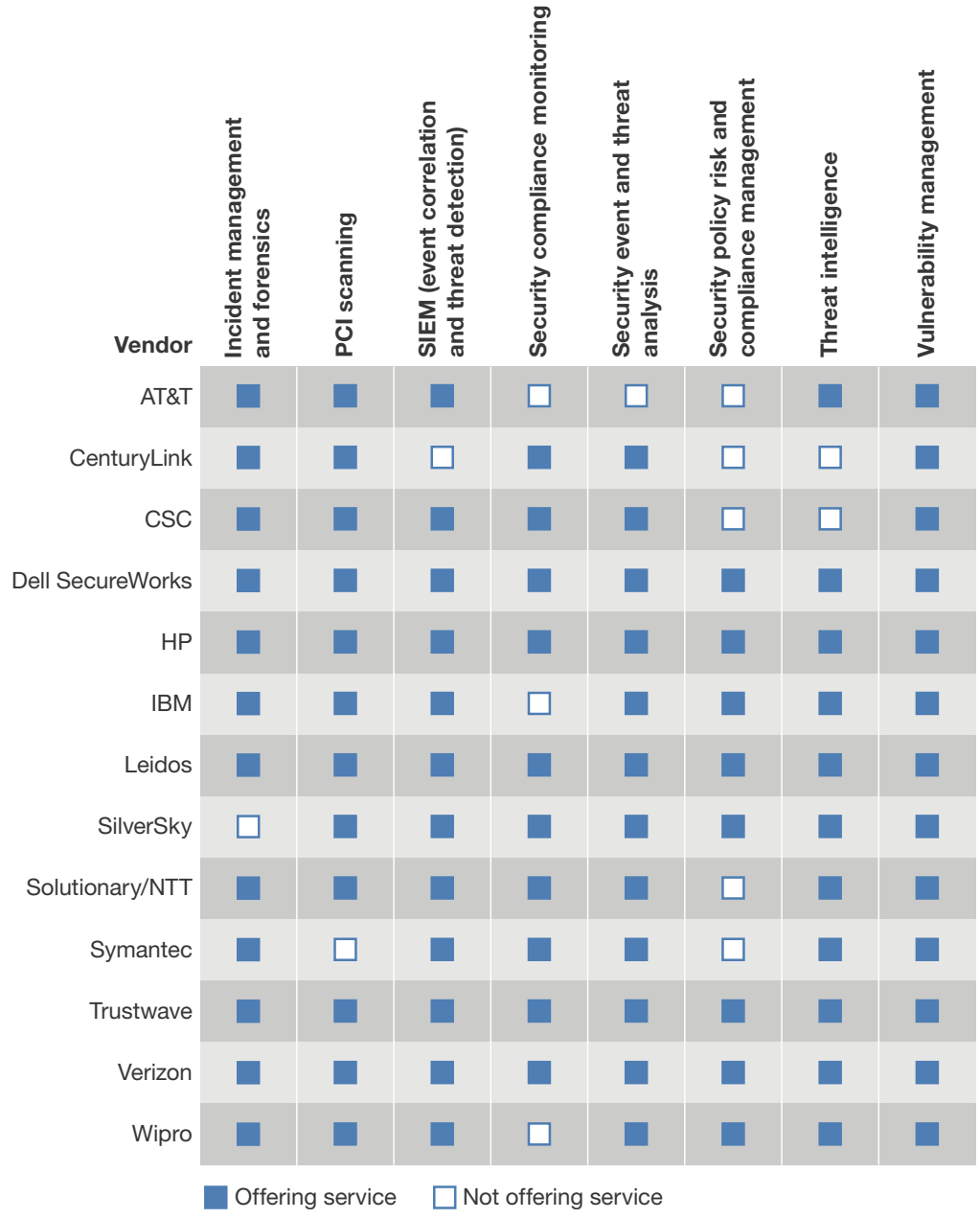
113183 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 2 Managed Security BPO Services



113183 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 2 Managed Security BPO Services (Cont.)



113183 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

ENTERPRISE MANAGED SECURITY SERVICE PROVIDERS: EVALUATION OVERVIEW

To assess the state of the North American managed security service provider market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top MSSPs with a substantial client base in the North American region.

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation 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 MSSP product offering. The sets of capabilities evaluated in this category are: value proposition, customer satisfaction, delivery capabilities, cloud and hosted services, infrastructure and perimeter, value-added services, content and application security, and staff dedicated to MSSP services.

- **Strategy.** A vendor's position on the horizontal axis indicates the strength of its MSSP strategy, specifically focused on customer satisfaction, quality of staff, quality of the company's information portals, SOC certifications, and growth plans.

- **Market presence.** The size of the vendor's bubble on the chart indicates its market presence, which Forrester measured based on the company's North American client base and North American revenue.

Evaluated Vendors Offer A Full Suite Of Managed Security Services

Forrester included 13 vendors in the assessment: AT&T, CenturyLink, CSC, Dell SecureWorks, HP, IBM, Leidos, SilverSky, Solutionary/NTT, Symantec, Trustwave, Verizon, and Wipro. We selected these vendors to participate in the Forrester Wave based on their ability to demonstrate (see Figure 3):

- **A complete suite of managed security services.** We included providers that offer a complete suite of IT outsourcing and business process outsourcing security services.

- **A strong MSSP presence in North America.** To be included, a significant portion of the vendors' 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. Also the vendor needs to demonstrate that it can provide physical redundancy as well as system, network, and personnel redundancy.[4]

- **Substantial annual MSSP revenues.** The annual revenue from the vendor's managed security services was a large part of their business.
- **A high total number of locations and/or IP addresses managed.** Forrester considered the number of locations, and in some cases, the number of IP addresses, the provider managed.
- **A critical mass of dedicated SOC analysts and engineers.** The provider had more than 50 SOC analysts or engineers who spent at least 80% of their time dedicated to the provider's managed security services.

EVALUATION ANALYSIS

All of the MSSPs reviewed for this research have the capabilities to become a strategic partner for their clients, and we saw a great deal of parity across the evaluated categories. The Leaders were notably close in their scoring; all clearly understand what enterprise clients need for security services and have built their programs to directly address these requirements. The Strong Performers also had their list of strengths but did not rate as consistently well across key areas such as business value, client references, customer services, information portals, security analytics, and threat intelligence.

Value For MSSPs Is Both A Business And A Technical Question

In order to be a true partner, MSSPs need to demonstrate they can create business value as well as technical value for their clients. MSSPs are assuming more and more of an active role in defending their clients, which requires forward thinking, excellent execution, and an understanding of the client's security business drivers. These qualities will determine the ability of the MSSP to meet current and future demands that clients will ask of these service providers.

The evaluation uncovered a market in which (see Figure 4):

- **Many vendors are in the Leader category.** IBM, Dell SecureWorks, AT&T, SilverSky, Verizon, Solutionary, Trustwave, Wipro, CSC, Leidos, HP, and Symantec are Leaders. These vendors demonstrated a variety of strengths in their service portfolio. They also demonstrated effective portals, good client and revenue growth, and a focus on customer service. Each of the Leaders offered a robust set of capabilities in both the ITO and BPO security service categories. All of the Leaders invest heavily in their security offerings to make sure they remain competitive and advance in the marketplace.
- **CenturyLink is a Strong Performer.** Strong Performers offer solid security services and are able to compete by virtue of their content expertise and price. In fact, they often compete against the Leaders and win. While not all of their capabilities are at the level of the Leaders, if you are looking to outsource security to a competent partner, you should consider CenturyLink.

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

Figure 3 Evaluated Vendors: Managed Security Services

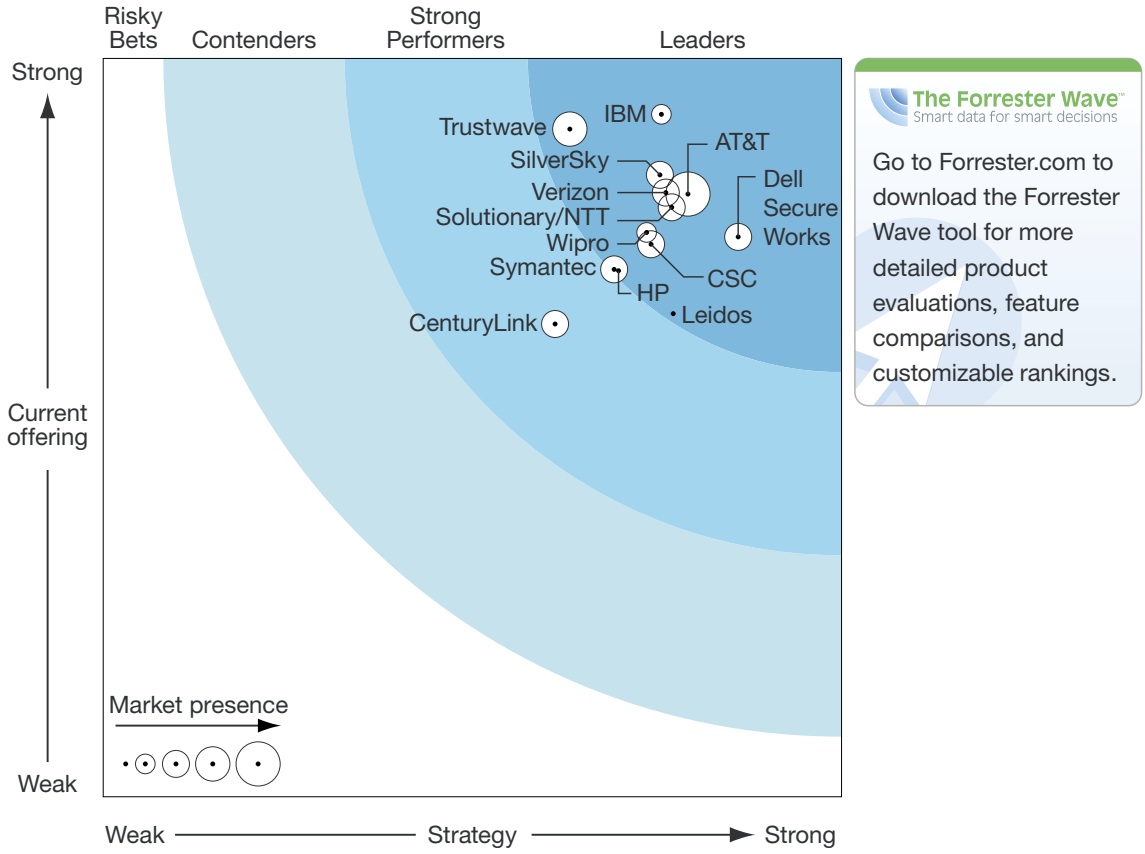
Vendor	No. of SOCs	SOC locations	No. of large MSS clients (deal size $50k+)
AT&T	8	New Jersey, US; N.C., US; Virginia, US; Brazil; Czech Republic; Bangalore, IN; MY	Forrester estimate: 2,500+
CenturyLink	4	Colorado, US; Minnesota, US; UK; IN	Forrester estimate: >1500<2000
CSC	9	Delaware, US; Maryland, US; New Jersey, US; UK (2); AU, MY, IN (2)	Forrester estimate: Between 50 and 500
Dell SecureWorks	7	Atlanta, Ga., US; Chicago, Ill., US; Myrtle Beach, S.C., US; Plano, Texas, US; Providence, R.I., US; Edinburgh, UK; Noida, IN	Forrester estimate: 2,500+
HP	8	Texas, US; Virginia, US; Costa Rica; UK; Bulgaria; IN; MY; Australia	Forrester estimate: Between 500 and 1,000
IBM	10	Atlanta, Ga., US; Boulder, Colo., US; Southfield, Missouri, US; Toronto, CA; Brussels, BE; Hortolandia, BR; Wroclaw, PL; Bangalore, IN; Tokyo, JP; Brisbane, AU	Forrester estimate: Between 500 and 1,500
Leidos	3	Arkansas, US; California, US; Maryland, US	Forrester estimate: between 50 and 500
SilverSky	4	Colorado, US; Florida, US: North Carolina, US; Philippines	Forrester estimate: more than 2,500
Solutionary/NTT	13	Nebraska, US; Pennsylvania, US; BE; PL; SA; AU; IN; JP; BR; CR;	Forrester estimate: between 1,500 and 2,000
Symantec	5	Herndon, Va., US; Reading, UK; Chennai, IN; Sydney, AU; JP	Forrester estimate: 2,500+
Trustwave	5	Chicago, Ill., US; Denver, Colorado, US; Minnesota, US; Warsaw, PO; PH	Forrester estimate: 2,500+
Verizon	8	Ashburn, Va., US; Carey, N.C., US; Miami, Fla., US; Leuven, BE; Luxembourg, LU; Canberra, AU; Chennai, IN	Forrester estimate: between 1,500 and 2,000
Wipro	7	Atlanta, Ga., US; Bangalore, IN; Chennai, IN (2); Greater Noida, IN; Mysore, IN; Pune, IN; Bucharest, RO	Forrester estimate: 150+

Figure 3 Evaluated Vendors: Managed Security Services (Cont.)

Vendor selection criteria
Complete suite of managed security services. We looked for providers that offered a complete suite of managed security services.
Strong MSS presence in North America. A significant portion of their managed security service revenue had to come from their 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 RFPs.
Large number of SOCs and their location. Forrester considered the number of SOCs providers had globally.
Substantial annual MSS revenues. The annual revenue from their total managed security services must have been a large part of their business.
Total number of locations and/or IP addresses managed. Forrester considered the number of locations, and, in some cases, the number of IP addresses the provider managed.
A host of dedicated SOC analysts. The number of analysts or engineers that spent at least 80% of their time dedicated to the provider's managed security services.

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 4 Forrester Wave: Managed Security Services, Q4 2014



Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 4 Forrester Wave: Managed Security Services, Q4 2014 (Cont.)

	Forrester's Weighting	AT&T	CenturyLink	CSC	Dell SecureWorks	HP	IBM	Leidos	SilverSky	Solutionary/NTT	Symantec	Trustwave	Verizon	Wipro
CURRENT OFFERING	50%	4.08	3.20	3.74	3.79	3.56	4.62	3.27	4.21	3.99	3.57	4.52	4.09	3.82
Value proposition	25%	4.00	3.00	3.50	2.50	2.50	5.00	3.50	4.50	4.50	4.00	4.50	3.50	3.50
Delivery capabilities — SOCs	15%	4.30	2.60	3.40	3.30	2.60	4.30	2.30	2.60	3.70	3.30	3.00	3.30	3.30
Delivery capabilities — services	20%	5.00	4.60	4.60	5.00	5.00	5.00	5.00	5.00	4.40	3.00	5.00	5.00	5.00
Delivery capability — offshore	5%	1.60	3.80	2.70	0.30	0.90	4.40	0.00	3.80	1.50	4.40	3.80	4.40	5.00
Delivery capability — service-level agreements	10%	4.00	3.00	4.00	4.00	4.00	4.00	1.00	4.00	1.00	0.00	5.00	4.00	2.00
Delivery capability — continuous monitoring	25%	3.80	2.60	3.60	5.00	4.40	4.40	3.80	4.40	5.00	5.00	5.00	4.40	4.00
STRATEGY	50%	3.96	3.06	3.71	4.30	3.49	3.78	3.86	3.77	3.85	3.46	3.16	3.81	3.68
Customer satisfaction	50%	4.20	3.40	4.20	4.40	3.20	3.00	5.00	4.60	4.60	2.80	3.80	4.00	3.80
MSS staff	20%	4.75	2.30	2.90	3.85	3.75	4.30	2.80	2.55	2.55	5.00	1.75	4.05	3.75
Portal	20%	2.40	2.20	3.40	5.00	4.20	5.00	2.60	3.00	4.00	3.20	3.00	3.20	3.60
SOC certifications and company innovation	5%	4.00	4.20	3.60	2.60	2.60	4.40	1.60	3.00	1.60	4.40	2.20	3.20	4.60
Growth plans and R&D investment	5%	4.60	5.00	3.40	4.00	3.40	4.00	4.00	4.20	3.20	4.00	4.00	4.00	1.60
MARKET PRESENCE	0%	4.25	2.90	2.90	2.90	0.70	1.20	0.85	2.25	2.65	2.95	3.60	2.85	1.60
North American clients for 2013	35%	5.00	3.00	1.00	5.00	2.00	2.00	1.00	5.00	3.00	5.00	5.00	3.00	1.00
North American client growth rate for 2013	15%	4.00	5.00	5.00	1.00	0.00	0.00	0.00	0.00	5.00	0.00	5.00	4.00	3.00
North American revenue for 2013	35%	5.00	1.00	3.00	2.00	0.00	1.00	1.00	1.00	2.00	3.00	1.00	3.00	1.00
North American revenue growth rate for 2013	15%	1.00	5.00	5.00	2.00	0.00	1.00	1.00	1.00	1.00	1.00	5.00	1.00	3.00

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

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

VENDOR PROFILES

Leaders

- **IBM, as the largest MSSP reviewed, provides true global leadership.** IBM's strengths are its focus on the client's business and the significant technical value it offers. IBM operates 10 SOCs globally, including three in Asia, and it had plans to add additional sites in 2014. The company has significant threat intelligence capabilities leveraging research from its X-Force team. Its portal is excellent, providing a complete view for security and risk professionals to understand their organization's security posture. IBM's SIEM and event correlation capabilities are built on the company's QRadar platform. IBM's customer reference was generally positive about IBM's services.

- **Dell SecureWorks is a leader in security analytics and threat intelligence.** Dell SecureWorks' strongest assets are the company's technical value and threat intelligence. Dell operates seven SOCs and has a strong global presence with over 2,500 clients. Dell also has one of the best threat intelligence teams in the industry; the company's Counter Threat Unit has many firsts, especially in zero-day discovery. The company's SIEM-related services are very effective, and Dell demonstrated good SLA adherence rates. Dell's portal is a key strength, with a majority of clients preferring to use it rather than their own portal and ticketing system. Dell SecureWorks struggled to articulate the company's business value, which hurt its score. Dell's customers, however, gave Dell the highest scores in all categories.

- **AT&T provides threat detection through the power of the company's network.** AT&T has one of the largest customer bases of the participating firms, with an estimated base of over 3,000 customers in worldwide and good client growth. AT&T is also building a respectable presence in Asia, with three SOCs in the region currently. AT&T's SIEM capabilities are strong; however, the company's threat intelligence and advanced analytics capabilities are still evolving.[5] The company's portal has a heavy emphasis on device management but lacks some of the features of other vendors' portals, including role customization and threat event drilldown. AT&T's business value proof points were not effectively demonstrated, but the company continues to invest in its MSSP business, and customers like and respect the power of AT&T's network. Overall, customers were pleased with AT&T's services and would recommend the firm to others.

- **SilverSky capabilities rival those of larger companies.** SilverSky operates four SOCs with a staff of approximately 120 engineers. SilverSky demonstrated strong business value and technical value, citing cost reduction, protecting client revenue streams, providing resource augmentation to allow customers to refocus internal resources, and helping protect clients' customers. SilverSky's SIEM and event correlation capabilities are effective at identifying complex attacks. The company has just created its own threat intelligence research group which will be a great benefit for the company's customers. SilverSky leverages one Asian SOC and has good service-level adherence. The company's portal is very device-centric and lacks some

of the most desired features, including a custom report writer. SilverSky's customer references reported that they are pleased with SilverSky's services, and they provided strong endorsements of the company's services.

- **Verizon's offers a broad set of BPO and ITO security services.** Verizon is a top telecommunications provider with more than 1,800 MSSP clients in the North American region. Verizon's strengths are the technical values it provides clients, built on the strength of the company's network. The company offers a full breadth of security BPO and ITO services, and its SIEM and event correlation are excellent. Verizon's portal allows customers to customize information by role, categorize devices, drill down on events to the raw log data, and compare their incidents with incidents seen on the broader Verizon network. Verizon lacks certain SOC security certifications. The company did achieve ISO certification for all SOCs in October 2014, and the company now has SOC 1 and SOC 2 reports available as well; however, Safe Harbor and PCI are still works in progress.[6] The clients we spoke to gave Verizon high scores with just a few concerns.

- **Solutionary/NTT excels with respect to continuous monitoring.** Solutionary is a member of the NTT Security Group, which also includes two other service providers.[7] Solutionary operates two SOCs in the United States but can provide services from 11 additional NTT-affiliated SOCs distributed globally from other NTT Security Group facilities. Solutionary's strengths are in the company's business and technical value. The company's portal is very effective, offering the ability to tailor information by role, comprehensive information on managed devices, and the ability to compare client events against those seen in the broader Solutionary network. The portal lacks a custom report writer but has good integration capabilities with a customer's environment. Solutionary's SIEM and event correlation is effective, and the company has very good threat intelligence capabilities. Solutionary's service-level adherence rate and customer retention rate was lower than some of the company's peers; however, clients interviewed were very satisfied with the company's services, giving the company very good to excellent reviews.

- **Trustwave provides a correct blend of MSS solutions.** Trustwave continues to prove that it's a Leader in the MSSP marketplace. Trustwave operates five SOCs and demonstrates very good business as well as technical value. The company operates a proprietary Trustwave SIEM, and its continuous monitoring capabilities are effective. The company's SpiderLabs threat intelligence research team provides excellent threat intelligence, and the company's SLA adherence is impressive. Trustwave's portal is effective and provides a comprehensive view of security devices under management, but it lacks a custom report writer and requires custom coding to make changes. Trustwave provides portal integration into the client's environment using a portal API. The company's customers were very positive and praised the company's responsiveness.

- **Wipro moves onshore while leveraging its considerable offshore capabilities.** Wipro operates seven SOCs globally, with one in North America, one in Europe, and five in Asia. The company has strong technical value, with effective SIEM and security monitoring. Wipro's threat intelligence capabilities include both internal and external information sources. The

company provides a broad list of capabilities, including a complete set of BPO and IT security services. Wipro delivers a large percentage of these services from its Asian SOCs. Wipro's portal presents information from a number of different information sources. Information can be tailored by role, and comprehensive information on devices managed is available. Customer references were positive, but the company's average SLA adherence rate was lower than for other companies in the Forrester Wave.

- **CSC provides great technical value.** CSC's estimated 300 SOC engineers provide fluent support in nine languages. The company operates nine SOCs, with two in Asia, and Forrester estimates that 45% to 55% of CSC's customers use services delivered from those Asian facilities. CSC has effective SIEM and continuous monitoring as well as threat intelligence capabilities using a linked infrastructure that allows clients to share information across the broader CSC network. CSC's SLA adherence is very good. The company's portal provides a detailed view of SOC operations and demonstrates tight integration with client environments. Customers have access to raw event data with excellent drill-down capabilities; however, the portal is not customizable by role and does not have a custom report writer. CSC's customers were very positive about CSC's services, although some were concerned about CSC's responsiveness, especially related to the deployment of new services.

- **Leidos shows its defense industry heritage when delivering MSS.** Leidos is a new entry in the market, having spun off from SAIC as an MSSP focused on the commercial market. Leidos has a defense industry heritage, and it shows in the company's approach to managed security. Leidos as the successor to the large US defense contractor SAIC, is a relatively new entrant into the commercial market for MSSPs. Leidos spun off SAIC to allow Leidos to focus on commercial business while SAIC remains focused on servicing the defense industrial base (DIB).[8] Leidos operates three SOCs, all in North America. The company did not report how many customers it has, but it's a relatively small number, between 50 and 500. The company has effective SIEM and event correlation capabilities based on HP ArcSight and McAfee Enterprise Security Manager, and its information portal also leverages technology from RSA. The company's portal provides comprehensive information on devices managed for customers, but the portal does not have a custom report writer and requires custom programming to make changes. Leidos' threat intelligence capabilities are behind many competitors' but evolving with the use of internally sourced information as well as Leidos' internal malware research team. Leidos customers gave the company highest scores for the services provided.

- **HP uses its technology solution portfolio to deliver MSS.** HP is one of the largest players in the MSSP market and continues to provide a solid and complete set of managed security services. The company operates eight SOCs, with two in North America, two in Europe, one in Latin America, and three in Asia. HP's Virginia and United Kingdom locations have ISO 27001 certification, and HP is working hard on ISO 27001 certification for the rest of its SOCs. Not all SOCs are certified, although the company is working toward ISO 7001 certification for all

these facilities. The company's SIEM and security analytics capabilities are effective, drawing on its own ArcSight platform. The company's threat intelligence team is very effective at providing situational awareness for customers, and the company reported a very good SLA adherence rate. HP's portal allows customization by role and provides an effective view of the security devices under management. HP's portal also has a custom report writer and allows customers to compare their specific security events with similar events on the broader HP network. HP's customers were generally happy with HP's service with minimal complaints. Some customers observed that HP could be more proactive with respect to change requests.

- **Symantec focuses on security BPO.** Symantec has an innovative engagement model offering customers fixed rate contracts. The company serves an estimated 2,500 clients in North America. Symantec as a very technically focused company had difficulty articulating the business value of their service offerings; however, the company's technical value is obvious. Symantec has effective SIEM and continuous monitoring capability, offering a full portfolio of security BPO services. The company's large security research organization works closely with the company's SOCs to provide detailed intelligence and early warning of emerging threats. Portal functionality is very good. The portal provides API access to allow integration into the customer's environment. The portal allows customers to tailor information by role and provides comprehensive information on all managed devices. Customers can drill down to the raw event log data by clicking on events of interest. The portal, however, does not have a custom report writer. Symantec's clients had minimal complaints and were impressed by Symantec's responsiveness.

Strong Performer

- **CenturyLink.** CenturyLink provides good technical value and was able to provide several examples of where it improved top-line revenue as well as allowing clients to refocus security resources on other tasks. The company offers a technically focused risk managed approach to its managed security service offerings. The company operates four SOCs globally, with one SOC located in Asia. CenturyLink's SIEM and continuous monitoring services are effective, and the company's portal provides the basic functionality most often needed for security and risk professionals to understand their risk posture. The portal cannot be customized by role, however, and it lacks a custom report writer. All client interviews were scheduled, and clients gave highest scores. Customers reported that CenturyLink has a high quality of analysts and SOC engineers, but they listed responsiveness as a concern.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 4 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 data sources to assess the strengths and weaknesses of each solution:

- **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.

- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with one to 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 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 document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we 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

All of Forrester's research, including Forrester Waves, is conducted according to our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

ENDNOTES

[1] Division 1 includes the largest enterprise-class providers. These MSSPs offer multiple security operations centers (SOCs) in multiple geographies, employ from 100 to more than 1,500 engineers, and have revenues between $70 million and $400 million. Division 2 includes the emerging MSSPs. These companies have from 20 to 100 engineers, one or two SOCs, and revenues between $25 million and $70 million. Division 3 includes many smaller firms that serve the small business market. These companies have a single SOC and a small staff of security analysts numbering no more than 10. Revenues for these firms are less than $25 million. For more information, please see the January 8, 2013, "The Forrester Wave™: Emerging Managed Security Service Providers, Q1 2013" report.

[2] Protecting company data is a critical function and the centerpiece of any continuous monitoring program. There are many strategies for protecting customer data, and each helps in threat defense. The use of big data is now seen as a key component of better and more comprehensive threat detection. Using advanced security analytics tools detection can now become more predictive and proactive. For more information, please see the August 4, 2014, "Detecting Cyberthreats With Fraud-Based Advanced Analytics Technology" report.

[3] In order to measure customer services, Forrester evaluated participating vendors on how well they met their SLA commitments and interviewed the vendor's customers to determine customer satisfaction.

[4] All of the vendors did well in this category. Forrester includes this here because this area of MSS operations is often overlooked in MSS contracting.

[5] AT&T and IBM announced in February 2014 a strategic alliance to provide comprehensive security services including a broad range of application and network security services that simplify security operations in the areas of threat intelligence, event correlation, and detection. This indicates the AT&T (and IBM) are willing to cooperate to develop better threat detection and intelligence capabilities. For more information on this partnership, please see the June 30, 2014, "Brief: AT&T And IBM Accelerate The Move To Utility-Based Security" report.

[6] This score is based on the state of the company's certification efforts as of August 15, and we scored on that basis.

[7] NTT Security includes Solutionary, Dimension Data, NTT Com Security, NTT Data, and the NTT Innovation Institute. Source: NTT Group (http://nttgroupsecurity.com/).

[8] Leidos split from Science Applications International Corp. (SAIC) in 2013 to allow Leidos to focus on commercial business. SAIC remains focused on US federal government contracting. Source: Amrita Jayakumar, "One year later: The tale of SAIC and Leidos," The Washington Post, September 28, 2014 (http://www.washingtonpost.com/business/capitalbusiness/one-year-later-saic-and-leidos/2014/09/26/d1fefd68-4273-11e4-b437-1a7368204804_story.html).

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

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 Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals