IDC MarketScape

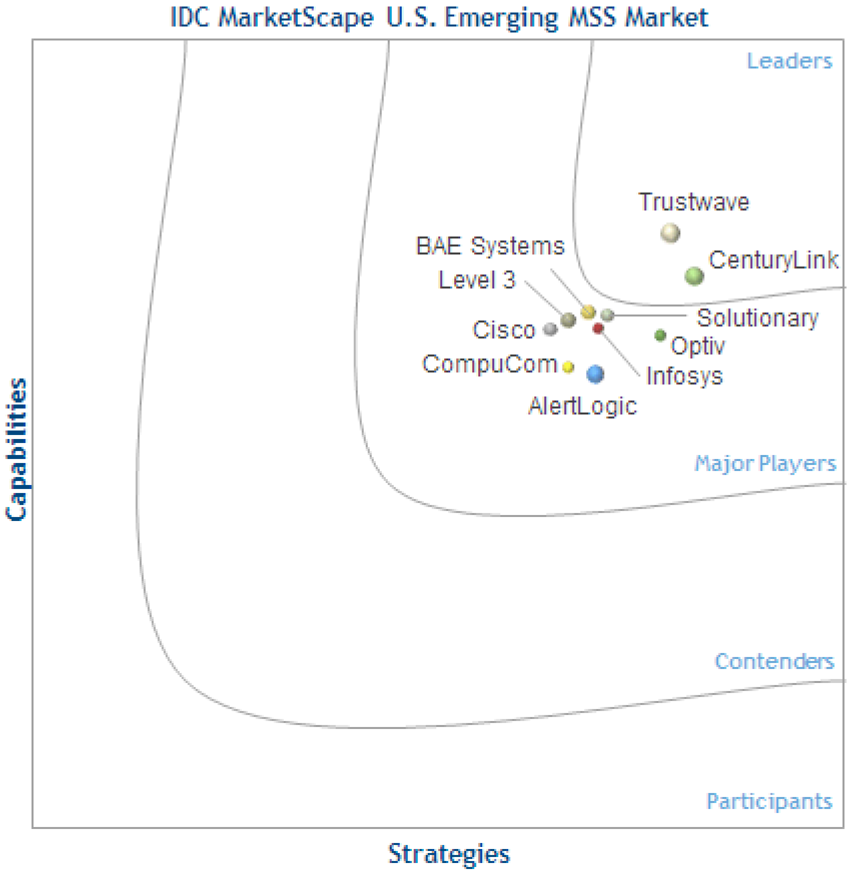
IDC MarketScape: U.S. Emerging Managed Security Services 2016 Vendor Assessment

Christina Richmond Martha Vazquez

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape U.S. Emerging Managed Security Services Vendor Assessment



Source: IDC, 2016

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

August 2016, IDC #US41320816

IDC OPINION

Using the IDC MarketScape model, IDC studied 10 organizations in the first quarter of 2016 that offer managed security services (MSS) in the United States, although several of the study participants deliver services worldwide. This study excludes the more established worldwide managed security services providers (MSSPs), which may also be considered the top providers in the United States. These companies were studied in 2014 and will be evaluated again in 2017 and are not included in this study. Through in-depth managed security services provider interviews and more than 25 interviews with providers' customers, IDC learned that the providers offer traditional (basic) MSS and advanced MSS capabilities in varying degrees. Through granular evaluation in early 2016, IDC found that each provider possesses some unique strengths and weaknesses when compared with its peer group. Major differences centered on both current capabilities and strategies for the next 12-18 months. As a result of IDC's evaluation, IDC found two Leaders — Trustwave and CenturyLink. The second group of Major Players consists of Alert Logic, BAE Systems, Cisco, CompuCom, Infosys, Level 3, Optiv, and Solutionary. As MSS continues to mature, it is incumbent upon these 10 emerging U.S. MSSPs to participate in the next generation of MSS, which IDC calls MSS 2.0. Buyers certainly face complex choices in selecting a vendor with which to partner. However, despite these complexities in vendor selection, buyers purchasing MSS have plenty of options. IDC believes the following areas will drive the MSS market forward and differentiate the providers:

- Complementary consulting services that provide customizable opportunities for customers to plan and enable their security journeys
- Flexible consumption models that match customer preferences for integrating MSSP expertise, processes, and technology
- Cloud management capabilities that seamlessly enable hybrid implementations
- Pricing models that align with customer preferences
- BYOD/mobile solutions
- Advanced detection and analytics techniques, including advanced detection and response capabilities, threat intelligence, and big data
- Robust customer support, including incident response (IR) and forensics, to assist with recovery from breaches
- Security operations centers (SOCs) and advanced methods of acquiring and retaining much sought-after security talent

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 10 MSSPs within the 2015 IDC MarketScape U.S. emerging managed security services market assessment. While the market arena for MSS is broad and there are many suppliers that offer these services, IDC narrowed the field of participants for this study based on the following criteria:

- **MSS capabilities.** Each service provider was required to offer at least five traditional MSS delivery capabilities that are viewed by IDC as basic. A majority of participants offer more than five capabilities. See the Situation Overview section for an explanation of traditional MSS.
- **Revenue.** Each service provider was required to have 2014 MSS revenue in the range of $25 million to $75 million in the United States.

- **Security operations center.** A minimum of one SOC in the United States.

ESSENTIAL BUYER GUIDANCE

Buyers face complex choices in selecting an MSSP due to the number of providers and a multitude of variables: breadth and depth of offerings; staffing, capabilities, and locations; complementary services; onboarding methods; service-level agreements (SLAs); payment options; customer portal capabilities; customer service delivery methods; partnerships; and more. Given the pace of technology change, buyers should evaluate current and future MSSP offerings, along with the MSSPs' product/service/investment road maps, to be sure that future offerings align with anticipated business and cost projections. It can be expensive and disruptive to change providers, so it is worthwhile for buyers to take the time to find the right fit, no matter how many security services are being outsourced. An MSSP's customer satisfaction surveys, pricing benchmarks, use cases, proofs of concept, and/or best practices can aid the decision process.

IDC suggests that buyer organizations pay particular attention to the following decision factors:

- **Investigate MSS research and development (R&D) focus areas.** Forward-looking MSSPs are paying attention to cloud evolution, threat intelligence, incident response, forensics, big data and analytics, and advanced detection techniques. It is important to evaluate the MSSP's future road map strategies to determine whether the MSSP will be able to offer future technology changes needed for your business. For example, some MSSPs are making investments in security related to Internet of Things, BYOD/mobility, big data analytics capabilities, user behavior analytics (UBA), secure web gateways, and cloud hosting providers like Amazon and Microsoft.
- **Clarify cloud adoption strategy and timeline.** Workloads are shifting to different cloud platforms, so it is important to select an MSSP that can deliver offerings that best fit your business needs and can be flexible to meet future changes occurring within your infrastructure. Typically, MSSPs have some equipment on-premises for log collection, but software-as-a-service (SaaS) and hybrid delivery are gaining momentum. A typical MSSP can manage/monitor on-premises equipment for the customer and/or correlate log aggregation or security events through SaaS/cloud services. MSSPs are using multiple delivery processes to manage, monitor, and correlate security. Given ongoing concerns about cloud security, however, buyers should evaluate offerings carefully. MSSPs are expanding cloud capabilities and expertise, perhaps opportunistically, through acquisition, organic development, and partnerships. Current and upcoming cloud-based managed security services include threat intelligence, analytics, threat detection, web security, identity, distributed denial of service (DDoS), mobile, and email security.
- **Embrace the necessity of threat intelligence and the use of big data.** Cyberattacks are only going to increase in frequency and severity. Organizations can no longer afford a "do the minimum" security strategy, which is simply not sufficient to thwart advanced persistent threats, distributed denial of service, identity theft, and other sophisticated attack strategies. The commonsense best practice is to acquire and use reliable, "predictive" intelligence that results from a robust combination of technology and expertise. Buyers may want to evaluate MSSP capabilities such as large databases (for long-term analysis), data aggregation and correlation, behavioral- and heuristic-based detection (versus signature-based detection), machine learning, emulation/sandboxing, virtual containerization, and forensic analysis/interpretation.

- **Evaluate customer portals.** Portals are the primary conduits of information between MSSPs and their customers, and they determine the scope and ease of visibility and control. Portals can be a competitive differentiator, and as such, they should be able to satisfy broad user requirements. Basic portals typically include some visibility of data, ticketing functions, limited reports, and contact links. Advanced portals are built with Web 2.0 tools and offer a rich customer experience that may include sophisticated analytics and visuals, real-time updating, and configurability/customization choices, especially for reports. Increasingly, portals include role-based access, querying of security and information event management (SIEM) data with broad correlation capabilities, and real-time chat or instant messaging. MSSPs should be able to demonstrate how their MSS are integrated into the portal and how the portal can be customized for different types of users (e.g., executives and security personnel). Portals can also be used for providing workflow analysis for the client to see what incidents are being addressed by the MSSP and the ticket status.
- **Consider complementary services.** MSSPs included in this study offer some or all of the following services that are complementary to MSS: assessment of architecture and design, breach management, incident response, forensics, and compliance services. Some MSSPs offer additional complementary services around advanced malware analysis or in other areas that will help strengthen a customer's security program. Enterprises must have a strategy to respond to incidents and collect forensic evidence for legal and/or compliance reasons. A preemptive strategy is even better — one that does not treat all security threats as equal and apportions budget based on a current-state/future-state risk analysis.
- **Evaluate SOC capabilities and security expertise.** Depending on organizational requirements, SOC staff certifications, which are relevant to specific industries, security regulations, and operating systems, may be crucial in a proactive, predictive security strategy.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Alert Logic

According to IDC analysis and buyer perception, Alert Logic is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Alert Logic provides a unique security-as-a-service model that protects customers' IT infrastructure where it resides: on-premises, hosted, or in a cloud environment. Alert Logic has developed proprietary technology for cloud providers and provides security for private and public cloud platforms. The security services offerings "work like the cloud," which makes it a very simple transition for customers that are moving to different cloud platforms.

Alert Logic has two SOCs globally, with one in the United States and the other in the United Kingdom. With over 700 employees, 106 are dedicated to MSS. Alert Logic provides security products and ActiveWatch, a managed security-as-a-service solution that provides 24 x 7 monitoring and management.

In the past two years, Alert Logic has experienced double-digit growth in the MSS space. Alert Logic's cloud-based delivery model enables the company's services to be largely focused around midsize cloud providers. In the past four years, Alert Logic has evolved its security services from being PCI focused to providing a more mature security practice overall. Alert Logic positions itself to be a security expert for cloud environments and continues to experience strong growth in this area. The service competes by delivering an end-to-end service that combines analytics-driven threat detection and prevention, compliance services, global threat intelligence, 24 x 7 security monitoring service, and incident remediation guidance.

Alert Logic offers a suite service called Cloud Defender, which provides web application, vulnerability assessment, log management, intrusion detection services (IDS), data analytics coupled with 24 x 7 monitoring, and experts on staff and security research and content. The service protects the IT infrastructure regardless where it resides – in the cloud, on-premises, or in a hybrid environment.

The services are differentiated by offering security solutions that are built in the cloud specifically to protect applications running on cloud platforms in which traditional, on-premises security solutions cannot provide protection. Also, Alert Logic maintains full-stack protection, which is different from point products solutions; the solution is integrated with its security operations, network operations, and analytics platform.

Alert Logic has the ability to protect dynamic applications and workloads running on cloud platforms, so organizations that are cloud native, advancing their DevOps or Cloud Security Operations practices, or looking to migrate workloads to cloud service providers such as Amazon Web Services or Microsoft Azure, should consider Alert Logic.

Strengths

Alert Logic's Cloud Defender service is a bundled, managed suite that covers network protection, vulnerability assessment, log management, log correlation, and web application security. The service is positioned well to offer enhanced detection capabilities based on a combination of security content, analytics, and human expertise. The company plans to continue developing more enhanced analytics by its data scientists and focusing on growth initiatives in big data. It also continues to invest in further integrations with public cloud service providers.

Alert Logic recently revamped its human resources strategy for acquiring and retaining employees. Specialty skills are in demand to be competitive in the MSS market today. In the past 24 months, the company has made some hefty investments in its talent management team by providing a multipronged approach to attracting and retaining talent that focuses on engaging with local universities, offering continuing education, and investing in its employees.

Challenges

Alert Logic does not manage other third-party vendor products. Therefore, it lacks the traditional flexibility that a typical MSS client is looking for, but it can be used as an augmented service with other MSSPs. The company could also improve in other areas such as complementary offerings and marketing initiatives. According to customer feedback, depending on the client environment, integration could be smoother when deploying services. The customer-facing portal provides real-time updating but lacks enhanced analytics, visualization, and reporting tools. Enhancements could be made to the portal in the future.

Alert Logic could offer usage-based pricing options that map more closely to cloud services pricing models. The market is not there just yet, but lots of thought is driving the adoption of this price model.

BAE Systems

According to IDC analysis and buyer perception, BAE Systems is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

BAE Systems' strategy aims to be a trusted provider of managed security services, helping thousands of customers simplify how they safeguard their critical information assets. BAE provides advanced technology, threat intelligence, compliance, and customer support that allow its customers to focus on core business activities. BAE has two SOCs in the United States, located in Fort Lauderdale, Florida, and Raleigh, North Carolina. One SOC is located in Manila, Philippines, which handles triage and level 1 support for the U.S. customer base.

In 2014, BAE Systems acquired SilverSky, an MSSP that provided cloud-based email and network security. The acquisition of SilverSky enabled BAE Systems to expand its MSS portfolio and target U.S. businesses. BAE Systems targets markets where it can leverage its success, which include highly regulated midmarket customers and smaller enterprises. BAE is also focusing on larger enterprises in the United States and other parts of the world.

BAE Systems has been successful in providing threat intelligence for highly regulated providers such as financial institutions. Another successful market for BAE Systems also includes other highly regulated cloud service provider datacenters and telecommunication providers. Customers choose BAE Systems as their MSSP because of the quality provided by the security expertise analysts, engineers, consultants, and data scientists.

BAE Systems' top strategic focus centers around the company's Threat Analytics, which combines two main core competencies: security expertise and big data analytics. The Threat Analytics is offered in two flavors today: as an on-premises solution for companies with internal SOCs (threat analytics) and as a managed service (managed threat analytics). More investments will be made in these areas to improve its use of analytics through security research, threat intelligence, and data science.

Enterprise-level organizations such as financial institutions, telecommunication providers, and datacenters in highly regulated environments should consider partnering with BAE Systems.

Strengths

BAE Systems has a comprehensive portfolio that covers the entire security life cycle. Its threat intelligence and research cover competitive amounts of data analytics. Also, BAE Systems has extensive experience for working with companies in highly regulated areas. BAE Systems provides basic security monitoring services but also is differentiated because of its threat intelligence capabilities and high-touch, white-glove alert response policies. The advanced services, Managed Threat Analytics include advanced threat detection and big data analytics. The company also provides incident response, Active Compromise Assessments, and threat intelligence, which integrate into its MSS solutions, but also offers premium options to add on for highly security-conscious customers.

According to customer feedback, although the company has gone through a number of changes, it continues to stay attentive to customers' needs and the services/products have improved over time. The company continues to reach out to customers consistently with any known escalated security issues. BAE Systems has been very proactive in supplying feedback to the customer on a regular basis.

Challenges

BAE Systems has no formal retention program for its employees and does not provide any multiple security career path methods to its employees, but it started offering leadership development programs to executives to drive retention. As a large defense contractor company, BAE Systems could enhance in diversifying its security talent acquisition and retention methods.

BAE Systems could also utilize more methods in its R&D efforts today. The portal capabilities could provide more advanced functionality other than enhanced reporting such as visualization.

CenturyLink

According to IDC analysis and buyer perception, CenturyLink is an IDC MarketScape Leader in the U.S. Emerging Managed Security Services market.

CenturyLink is currently the third-largest telecom company in the United States. Since 2008, CenturyLink has transformed its business by acquiring some strategic companies, each of which has given CenturyLink new capabilities. This transformation included the acquisition of Qwest Corp. and Savvis Communications in 2011, which helped broaden CenturyLink's services portfolio by adding in managed security services as well as domestic and international enterprise networking, hosting, colocation, and cloud infrastructure and services.

Along with the acquisition of Savvis and many others such as AppFog, Tier 3, Cognilytics, and netAura, CenturyLink has demonstrated its commitment to strengthening its security services as well as supporting its customers' transition from a traditional networking infrastructure to a hybrid IT world. In 2016, CenturyLink expanded its managed security service portfolio with the announcement of five key enhancements and a new customer portal.

In 2016, CenturyLink relaunched its customer-facing portal, which is built on the elastic search stack ELK. This architecture allows customers to access their data by using this elastic ELK stack and then do detailed searches, analytics, and visualization of their data. The portal also provides clients with complete transparency into what the CenturyLink analysts are doing for them in real time. They can see what incidents or alerts are open and active, can interact with the SOC analysts in real time, and can change the status of open incidents in real time.

CenturyLink has three SOCs in the United States, with two others located in the United Kingdom and India. The MSS business focuses on midmarket and enterprise customers but also has a breadth of government customers. CenturyLink has been providing security services for over a decade and has a number of offerings that are customizable to its customers. CenturyLink sells security in two ways: as an add-on to core company offerings such as network and hosting (mainly basic services) and/or as a standalone network-agnostic service for larger organizations that desire a true MSS partner.

Federal government entities and/or compliance-driven midmarket and enterprise organizations will find CenturyLink MSS a good option.

Strengths

CenturyLink has a strong foothold in delivering services to the federal and government entities and can provide custom-based security services for enterprises. CenturyLink also delivers advanced services such as DDoS, web application scanning, web application firewall, managed SOC, penetration testing, and file integrity monitoring and is providing advanced detection and analytics techniques. Also, the company added five new services in its SIEM platform, which were log monitoring, threat analysis, incident response, vulnerability management, and managed protection services.

CenturyLink also offers different price models and payment options for customers. The company has a strong channel program, with seven channels to support the implementation of service sales. Also, the go-to-market plan consists of vertically focused sales teams. CenturyLink has a senior leadership team with security expertise that act as advisors to multiple federal agencies and contributors to the NIST cybersecurity framework and a team of 30+ security consultants and 250 researchers and testers in its SOCs that are GIAC Certified Intrusion Analysts covering multiple security domains.

CenturyLink received solid marks for its talent acquisition and retention programs. Century Link employees are offered numerous academic programs to attend in the United States. For example, Innovations in Communications, Information and Cyberspace (IC3) at Louisiana Tech University is a unique and innovative certificate program in information technology that is offered to students and employees of CenturyLink.

Customer feedback applauded CenturyLink for its responsiveness to customers' RFP and its service management group.

Challenges

Portal capabilities were lacking in 2015, but moving into 2016, the portal is now enhanced, and many customers are trying out its new capabilities. Before the new integrated portal, there were two separate portals, in which the Savvis portal did not have any capabilities such as real-time updating, enhanced analytics, reporting, or visualization tools. Unfortunately, there will be more challenges to work through as these portals are integrated. To compete competitively, CenturyLink should also look at enhancing its MSS capabilities with threat intelligence services and BYOD/mobility.

Cisco

According to IDC analysis and buyer perception, Cisco is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Cisco, a well-known networking company, is based in San Jose, California, and has 140 employees dedicated to its MSS business. For over 10 years, Cisco has had Remote Management Services (RMS), an offering that has been offered to customers but has not been aggressively marketed. The RMS offering is a basic MSS offering where the customer owns the equipment, and then the design, implementation, and so forth are provided by the customer, or the customer can purchase a traditional plan, design, and implementation type of service from Cisco and then hand it off to RMS starting at day 2 operation. Cisco can provide remote management and fault and performance testing, review security events that are coming in from the security devices, and provide an instant response based on the telemetry that is provided to Cisco. In 2014, Cisco launched MTD, a managed security services offering that applies real-time, predictive analytics to detect attacks and protect customers' networks. In 2015, the service was rebranded to be called Active Threat Analytics (ATA).

Cisco has strong market traction in the enterprise, so as a result, offering MSS to its large existing base of customers is a natural fit. Cisco believes customers are at different stages of their security maturity. Therefore, Cisco can utilize its portfolio to create different entry points. Cisco offers three distinct offerings for MSS customers: Essential, Enhanced, and Premier. Customers that are just looking for device monitoring and management, Cisco offers its Active Threat Analytics Essential offering, where the customer can add more services as its security maturity evolves. Essential provides security device management and log collection and event correlation. The Enhanced solution offers more in-depth capabilities such as statistical anomaly detection and netflow generation. For customers that are more mature and looking for big data and advanced analytics solutions, Cisco can offer ATA Premier, which includes proactive threat hunting and machine-learning capabilities. Customers also have the opportunity for Cisco to take over the management and monitoring of their devices.

Healthcare and financial organizations looking for a comprehensive approach to security services and also looking for advisory services to assist in their security journey should consider Cisco.

Strengths

Cisco has a broad portfolio of security services that complement its MSS portfolio. This includes both the advisory services portfolio and the integration services portfolio. Given Cisco's broad portfolio of security services, the company can offer the customer a comprehensive service that aligns with its goals. According to customer feedback, Cisco was given positive remarks for integrating all their components and managing these devices for them. Customers also sited a key differentiator for Cisco is the telemetry data that Cisco is gathering; customers feel that they are getting a lot more information than just security analysis. Customers can produce queries and gain more insight from Cisco.

Cisco's advanced detection method is a key strength and provides a solid road map in expanding in this area. Cisco also has a breadth of complementary services that include breach management, incident response, forensics, compliance, and assessment of architecture and design.

Challenges

Although Cisco has a solid brand name and reputation, it is not well known as an MSSP. The company has not focused its marketing efforts of its MSS offering until recently. It will take some time for Cisco to build a reputation and market share in this area. Cisco should also look at providing more pricing and payment options to customers for flexibility. Customer feedback stated that the customer-facing portal could be improved. Customers are not able to run queries against the data that is coming in from the solution that they have. Customers would like to have more interaction with the portal than what they currently have today.

CompuCom

According to IDC analysis and buyer perception, CompuCom is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

CompuCom entered the MSS space over 10 years ago and since then has undergone significant business transformations. CompuCom revamped its security portfolio and marketing strategy to align with and fall under its cloud technology service business unit. With the implementation of its new security services, the MSS for CompuCom has experienced double-digit growth. CompuCom is reengineering its portfolio and reinventing its services.

CompuCom offers basic and advanced MSS such as managed firewall, intrusion prevention services (IPS), web email security and antimalware, managed SIEM, file integrity, and penetration testing. CompuCom's complementary services include incident response, compliance, and assessment of architecture and design. Compliance reporting and PCI reporting have been and still are the core focuses for CompuCom.

CompuCom will continue its focus on large enterprise customers and plans to expand its reach into the medium-sized enterprise and into SMB's using stores under the Tech Zone brand.

Small to midsize companies in retail and healthcare and financial organizations that have a strong focus on compliance will benefit in partnering with a company such as CompuCom.

Strengths

CompuCom's significant business changes and investments in the future will enable the company to grow its portfolio and capabilities. The company already has a number of basic MSS capabilities but was not representing itself as a more comprehensive MSSP. It is now working toward collaborating with the other lines of business to educate each about the security services offering.

In addition, CompuCom is working toward modernizing its MSS portfolio and integrating its security capabilities. The investments are in line to produce a more comprehensive solution to provide effective services. In regard to partnerships, the company is working with software and hardware vendors that are enabling it to leverage and enhance its SIEM and cloud-based security services.

Challenges

CompuCom is at a turning point where it is rebranding and reworking its new strategies and focus; although this is positive for the long term, there are still bumps that can occur along the way. At this point, its onboarding process is slower than the other competitors, and its road map lags behind as well. There is a renewed focus, but it will take time to play catch-up.

In the past, CompuCom has taken a conservative approach to MSS but is now working on integrating other services such as compliance automation, cloud security, and cyberanalytics in the future.

CompuCom offers complementary services such as incident response, compliance, and some forensics, but the company understands the need to move to an MSS 2.0 with more consulting services and is looking to invest more in these areas.

The portal is relatively dated, where only real-time updates are being provided. CompuCom could provide better end-user experience for the customer through the portal.

Infosys

According to IDC analysis and buyer perception, Infosys is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Infosys provides technology and consulting services to organizations in more than 50 countries. With 1,250 MSS employees and 350 SOC analysts, Infosys offers MSS from two SOCs located in Bangalore, India, and Milwaukee, Wisconsin. Infosys has a flexible business model that utilizes the "follow the sun" approach in an effective and efficient manner and supports its clients by ensuring that the incident management process is not interrupted because of business hours or employment constraints in one region.

The value proposition of Infosys for its Information and Cyber Risk Management (iCRM) practice is to provide the best-fit framework in securing a borderless enterprise of today and tomorrow. From basic regulatory compliance to futuristic converged security solutions, Infosys offers complete end-to-end solutions in the areas of data, application, infrastructure, and cloud security. The iCRM solutions are using artificial intelligence analytics and automation to help drive security transformations to prevent security breaches and enable collaboration across dispersed security teams.

Infosys' segments include manufacturing, insurance, life sciences, financial services, utilities, retail, and healthcare. To acquire its customers, Infosys cross-sells to its large base of Infosys enterprise customers. Infosys focuses on target markets by participating in relevant forums and also has joint go-to-market campaigns with strategic partners. To retain its customers, Infosys has client engagement and program teams that support defined service metrics measured against SLAs. Infosys also utilizes transformation partners, an advisory layer of architects, to facilitate client landscape transformation and continuous improvements through innovation.

The iCRM practice provides MSS advanced service offerings such as managed SIEM, DDoS, web application firewall, identity and access management (IAM) services, managed SOC, penetration testing, file integrity monitoring, and threat intelligence and uses advanced detection analytic techniques such as big data analytics. Some complementary services are offered such as architecture assessment and design and compliance.

Large and medium-sized enterprises that have compliance restrictions, or are undergoing digital transformation programs could benefit from Infosys' MSS.

Strengths

Infosys has an solid list of advanced services and has received high marks for being very engaged with its customers. Infosys' advanced services include analytical and tool-based services that address evolving threats and rely on big data from multiple threat intelligence sources. Threat intelligence utilizes artificial intelligence and signaling to detect indicators of compromise and a holistic cloud security assessment framework enables visibility and control. Solutions feature AI-driven analytics and automation to drive security transformations to work toward preempting security breaches.

Infosys also has a robust talent development program for security analysts. Infosys believes in the philosophy of continuous learning and has a large corporate training facility that enables employees to continue their education. Also, the talent development program consists of a plethora of training ranging from initial employment to security and leadership management training.

Infosys has an onboarding process that uses a standardized methodology for accelerating the service setup. The company also received very positive feedback from customers regarding migrating from one vendor to Infosys. Customers stated that the transition of support and services for IAM was very easy and went very well. The duties, expectation, and timelines were all met. The smooth transition was also due to Infosys being very organized and having dedicated project managers. Customer feedback also gave positive reviews for providing support and keeping lines of communication open where the staff will respond quickly and escalate issues appropriately.

Challenges

Areas of opportunity include providing additional routes to purchase, channel support, pricing flexibility, and more complementary offerings. Also, the MSS portal is basic with only enhanced reporting but lacks real-time updating, enhanced visualization, and analytics.

Level 3

According to IDC analysis and buyer perception, Level 3 is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Level 3 is a global internet service provider based in Broomfield, Colorado. Level 3 offers a multilayered approach at the edge through its network-based security method versus using a point solution architecture. The company has a strong threat research team that provides visibility into the threat landscape to proactively detect threats and alert its customers. With a network-based security, Level 3 believes it offers an improved multilayer security design at the edge, which is closer to the attack vectors.

Level 3 targets large enterprises and federal government entities. Today, the company is building out more security services specifically for the federal sector, but SMB and midmarket customers make up the bulk of its revenue. Level 3 continues to focus on growing upmarket and most of its security development is aimed at serving the large enterprise customers.

Level 3 operates a total of six SOCs, of which three are located outside the United States — in the United Kingdom, Brazil, and Argentina. The three U.S. SOCs are located in Colorado, Arizona, and California and provide 24 x 7 x 365 global coverage, which is integrated with Level 3's Threat Research Labs intelligence. The Threat Research Labs of Level 3 proactively analyze threats globally and share the information to help defend its customers and its network. With over 200,000 route miles of global fiber, Level 3 sees around 1.3 billion security events and 48 billion netflow sessions daily.

Level 3's security portfolio includes basic MSS 1.0 for cloud- and premise-based firewalls, IDS/IPS, mobility, content filtering, antimalware, and real-time security reporting, but the company has launched other security capabilities such as DDoS and Adaptive Network Security, which begin its entry into the MSS 2.0 arena.

Small and midmarket buyers interested in a network-based security approach will find Level 3 to be a good option with many future enhancements committed.

Strengths

Level 3 has a good MSS portfolio and a solid road map for adding more capabilities. The company offers hybrid capabilities (cloud- and premise-based services). Level 3 has developed services that go beyond MSS 1.0 such as threat intelligence, malware sandboxing, secure gateway via NFV, and DLP. In 2016, Level 3 launched a new threat intelligence service that gathers netflow data globally.

In 2015, the Black Lotus acquisition provided Level 3 with a strong foothold in the DDoS market, and the company will continue to invest aggressively in DDoS mitigation offerings throughout 2016. Also, its new service, Adaptive Network Security, offers a next-generation firewall/intrusion detection and prevention, web content filtering, antimalware, DLP, and endpoint protection, and it is carrier agnostic.

The company provides an integrated support model that addresses the entire life cycle of the customer experience from shop, buy, get, use, pay, and renew. Key focus areas include driving global consistency on service delivery and assurance processes; enhancing customer communications and expectations setting, with frontline employee training; improving network reliability and maintenance; evolving digital self-service capabilities via portal, mobile, and APIs; creating a customer-centric culture and measurement/incentive system; and building quantitative and qualitative survey platforms to provide better customer intelligence. For complex implementations and migrations, Level 3 offers dedicated security professional services engagements.

Level 3 plans to grow its capability through organic development, acquisition, and partnering. In 2015, Level 3 launched its DDoS Mitigation service and will offer more complementary services in the future.

Challenges

Level 3 is lacking in providing more advanced MSS capabilities such as identity and access management and BYOD/mobility today. The company has moved at a slower pace, but with new leadership in the security program, new and innovative capabilities are under way. In addition, Level 3 could enhance its offering through providing specific marketing programs for retaining and upselling its customers and developing more complementary services such as breach management, forensics, and incident response.

Optiv

According to IDC analysis and buyer perception, Optiv is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Optiv, a pure-play security company in North America, was created in 2015 as a result of the Accuvant and FishNet Security merger. Optiv's focus is not to offer only separate point security products but to help organizations plan, build, and run successful cybersecurity programs. Optiv intends to provide strategic and tactical consulting and security programs to its customers.

Three SOCs are located in the United States, with approximately 150 SOC analysts providing on-demand 24 x 7 x 365 support. The SOCs are delivering a breadth of services across 16 different security platforms, which include solutions such as firewalls, IDS/IPS, unified threat management (UTM), NextGen firewalls, SSL VPN, web application firewall, firewall management, load balancing, and SIEM.

Optiv offers a comprehensive portfolio of basic and advanced MSS, along with complementary services that include breach management, incident response, forensics, compliance services, and assessment of architecture and design. Optiv's basic MSS includes platform management that provides firewall, UTM, network IDS/IPS, vulnerability management, and security event monitoring. The advanced services include a comanaged SIEM, managed next-generation endpoint, threat analysts, and threat intelligence and advanced reporting.

Optiv's advanced services are not only reflected in the blend of service offerings currently offered but also include a proven process of personnel delivering these services. Optiv helps companies that are in different phases of their security program, and its advanced services assist customers to determine their security posture and risk. Optiv plans to continue to focus on bringing flexible technology-based solutions to its customers to help them mature their security program. Optiv will continue to create services geared toward providing traditional managed services that fit and align with its client's adoption of cloud services and that are hosted or enabled to support an organization's business objectives.

Enterprise organizations that are looking to partner with an MSS provider that can assist in developing and managing their security program should consider Optiv.

Strengths

Optiv is a blend of two different companies, and the integration of these companies has brought in a variety of MSS capabilities as well as complementary services. To help expand its MSS capabilities, Optiv plans to move forward in launching advanced threat analysis, which will include threat reporting, hunting, and reverse engineering.

Optiv offers flexible pricing options, which include à la carte, bundled, and single-priced services. In addition, Optiv provides flexible payment options for its clients. Optiv has many methods of marketing for targeting its market. For retaining existing customers, Optiv has an ongoing effort that includes "client first" services delivery and personal communication with its customers. Customers reported that Optiv has been very receptive to their needs, and when there is a question or concern, it is easy to get senior-level management involved. Optiv has also done a good job at going above and beyond to address its customer's needs, which has not been typical with other providers.

Challenges

Optiv has a few hurdles to face because of the combination of FishNet Security and Accuvant. As of 2015, the portal had not been integrated and only had basic portal functionality plus real-time updating. The company is updating its portal to incorporate new features in 2016.

Optiv provides only one method for the setup of services that includes using an engagement manager. Optiv partners with the top security product vendors to sell product and service (e.g., SIEM + Co-Managed MSS) in a teaming approach where Optiv sells the product as a channel for its partner and the service directly from Optiv. No channel sales of services is offered today, so Optiv should look at expanding other methods in this area. Customers reported that some changes for their setup were not as smooth and that they would have liked to have had a simpler, easier, and more organized implementation process to speed up the onboarding process.

Solutionary

According to IDC analysis and buyer perception, Solutionary is an IDC MarketScape Major Player in the U.S. Emerging Managed Security Services market.

Solutionary is an MSSP that was acquired by NTT Group three years ago. The NTT Group, based in Japan, also has other subsidiaries such as NTT Communications and Dimension Data. As part of this umbrella, Solutionary delivers MSS capabilities to the North America region for NTT. The company's focus is to provide a full life cycle of security services based on intelligence technology and security experts that exceed the evolving threat landscape and contribute to cyberdefense to protect social and economic activities globally. Solutionary itself provides local expertise and a breadth of security services to midsize and large global enterprises across various verticals.

With the joining with NTT, much transformation has happened, bringing major changes to large customers as part of NTT's family. As a result of NTT's overall growth in the market, Solutionary has grown as well as many of the customer demographics have changed. Solutionary finds itself embedded in more outsourcing deals, automating and providing customers with components of a security program or the security program itself.

With the power of NTT, Solutionary can deliver global security services with local delivery, including security consulting services, cloud-based and managed security services, threat intelligence, security integration, and risk management solutions around the world.

For Solutionary, the goal is to provide the life cycle of security solutions across the full stack. With the acquisition, Solutionary can provide everything from design, any hardware acquisition, and deployment globally to the traditional Solutionary component of monitoring management to product replacement. The list of basic and advanced managed security services offered includes threat intelligence, log monitoring, log management, vulnerability management, web application scanning, web application firewall, file integrity, managed SIEM, penetration testing, and advanced detection methods. The list of complementary services includes breach management, incident response, forensics, compliance services, and assessment of architecture and design.

As of August 1, 2016; Solutionary, NTT Com Security, and the managed security services of Dimension Data have been combined by NTT into a new global security services company called NTT Security. The company's stated mission is to bring cyber resilience to the global digital economy using the Full Security Life Cycle approach.

Organizations in the financial, healthcare, and critical infrastructure that need in-depth log monitoring capabilities and have compliance restrictions should look at partnering with a company such as Solutionary.

Strengths

Solutionary is moving from a basic MSS portfolio to offering a full life cycle of security services that brings in complementary services to complete the security cycle. The company is also addressing key technology trends such as cloud evolution, threat intelligence, IR/forensics, big data analytics, and advanced detection and analytics methods. Solutionary, with NTT capabilities, will be able to build in netflow data and utilize each other's datacenters. In the past, Solutionary had developed its threat intelligence and partnered with other vendors, but with NTT, Solutionary will be expanding and developing more of its footprint and intelligence capabilities.

Customer feedback was very positive, where one customer stated that doing business with Solutionary was incredibly easy and the company provides sufficient support. Another customer said that Solutionary offers a powerful tool and provides a lot of capabilities and flexibility. The service behind the SIEM and analytics is very powerful; therefore, Solutionary remains an essential part of its customers' security program. Solutionary was praised for its customer-facing portal. The customer believes Solutionary provides an exceptionally strong tool that is relatively easy to use when collecting data.

Challenges

Solutionary has a good future road map and offers a breadth of complementary services, such as forensics, incident response, and compliance services, but it could look at offering more advanced services like BYOD/mobility and providing management of other SIEM providers. Programs for retaining and acquiring employees could be revamped to make it more attractive for analysts. Integration within the NTT Group may experience some crossover issues as other companies such as Dimension Data sell to similar prospects.

According to customer feedback, continual responsiveness is important, so providing more feedback in regard to offering the customer new services could be improved.

Trustwave

According to IDC analysis and buyer perception, Trustwave is an IDC MarketScape Leader in the U.S. Emerging Managed Security Services market.

Trustwave is a security-based company that has a strong history and foothold in the compliance market. Trustwave operates eight SOCs globally. SOC locations are the United States (Chicago, Denver, and Minneapolis), Philippines (Manila), Poland (Warsaw), Canada (Kitchener-Waterloo Region), Singapore, and Australia. In 2016, Trustwave opened a new SOC in Sydney, Australia, along with its sister company Optus, a leading telecommunications provider in Australia. In 2015, Trustwave opened a new SOC in Canada and expanded into Singtel's Singapore SOC.

Trustwave serves more than 3 million subscribers on the Trustwave TrustKeeper MSS portal and platform. Customers range from small to midsize companies as well as distributed enterprises that need to be in compliance with various regulations. In 2015, Trustwave announced a major enhancement to its TrustKeeper portal called Enterprise View, which gives distributed enterprises more actionable threat intelligence. It provides customers customized views designed specifically for each role in their organization.

Trustwave offers managed security services in three different categories: threat management, vulnerability management, and compliance management. Trustwave's roots are in compliance, and that business continues to grow. Trustwave partners with banks, credit card processors, and small businesses through alliance partnerships. While Trustwave does have a partner channel, most of its business comes through the direct sales channel. Recently, the company began partnering with various telcos in different international markets, opening up new managed security services opportunities and new markets, and expanding its global capability. Examples include Rogers Communications in Canada, Optus in Australia, Singtel in Singapore, and Globe in the Philippines. Trustwave will continue to work with other telcos to expand its MSS offering and footprint.

Trustwave has a comprehensive portfolio, both developed by its engineering team and through acquisition. The compliance management section is more of the risk management compliance services. More developments and work are expected to occur in the compliance portfolio. The other buckets of services include vulnerability management and threat management. Under the vulnerability management is Trustwave's core offering called Managed Security Testing. This service offers automated security scanning with in-depth human-driven penetration testing across applications, databases, and networks. On the threat management side, Trustwave provides managed security services such as managed SIEM, managed antimalware, managed secure web and email solutions, and UTM. For all of these categories, Trustwave utilizes both its own technology products and other third-party security vendors, which allow the company to be flexible with the customers' needs and price point.

Small to midsize companies and distributed enterprises that have tight compliance restrictions should look at partnering with a company such as Trustwave.

Strengths

Trustwave's strengths include the company's breadth of basic and advanced services, which include managed encryption, DDoS, managed SIEM, web application scanning, web application firewall, identity and access management services, managed SOC, mobile services, and penetration testing. Trustwave's strengths also include the breadth of complementary services, delivery models, and payment options. Singtel's recent acquisition of Trustwave will help Trustwave to build on its global presence and provide an increase in enterprise customers. Trustwave developed and launched a new Managed SIEM Enterprise solution coupling its onsite SIEM Enterprise solution with remote management powered by Trustwave MSS/SOC expertise. With the addition of Managed SIEM

Enterprise, its entire SIEM portfolio is available as a self-managed, Trustwave managed, or hybrid MSS solution.

Trustwave will continue to add more strategic security partnerships to leverage multiple technologies. In 2015, new strategic alliances were developed, which include Akamai, Palo Alto Networks, and Carbon Black (formerly Bit9). Trustwave will enable more flexibility and offer more advanced security service offerings for customers by managing Palo Alto Networks' firewalls and added managed DDoS protection services, which are based on Akamai's cloud-based technology.

According to a customer's feedback, Trustwave did a great job when implementing over 8,000 UTMs for the customer. The customer acknowledged that for such a large deployment, Trustwave made it very easy to work with the company. Customers also praised Trustwave for having customized solutions that meet their needs and for being able to give them the level of support they need to be successful.

Challenges

The feedback of customers stated that reporting from the portal could be more dynamic and that they would like to have the capability to run reporting by themselves rather than having to ask Trustwave for more detailed reports. The customer believes that with the ability to enhance this reporting feature, the team could be more efficient. The portal still keeps MSS and compliance separate, but Trustwave is under development to enhance its MSS platform that will create a new portal experience for its users.

APPENDIX

Situation Overview

The security landscape is complex and challenging — an understatement given the number of moving parts that are involved in defending an enterprise from cyberattacks. IDC recommends that companies undertake a holistic, enterprisewide security posture that is proactive and predictive.

It's a daunting effort, however, to sustain the necessary level of threat intelligence and advanced analytics capabilities, along with the skills to interpret and act on findings. In-house 24 x 7 security solutions are expensive, and security talent is scarce. As a result, organizations debate "build versus buy," and many are turning to MSSPs. A security services provider can allow organizations to meet several objectives:

- Transfer the cost of ownership, thereby reducing capex and transferring the budget to opex.
- Create a predictable expense with a regular cadence in the budget cycle.
- Enable a dedicated application of technology, processes, and people to the rapidly changing threat landscape.
- Implement best practices that are evolving with a rapidly changing threat landscape.
- Benefit from "strength in numbers" from an intelligence perspective.

The rise in frequency and complexity of attacks and the need for increasingly sophisticated security solutions have led to a new echelon of MSS that IDC is calling MSS 2.0. An MSSP 2.0 is further "up the stack" than MSSPs that are offering MSS 1.0 services, which include the following:

- Log monitoring

- Basic managed and monitored services (firewalls, intrusion detection services/intrusion prevention services)
- Unified threat management
- Identity and access management
- Vulnerability scanning

MSSPs 1.0 may also offer advanced services such as DDoS, managed SIEM, and managed SOC.

MSSPs 2.0 deliver basic and advanced MSS plus professional/complementary services (for more details, see the Market Definition section). And they are investing in mobile/BYOD, cloud, threat intelligence/big data analytics, incident response/forensics, and advanced detection techniques. Cloud, mobile/BYOD, and big data are three of four pillars that IDC has identified as top trends. The fourth pillar, social media, doesn't factor into this IDC MarketScape; however, advanced MSSP capabilities can help detect, analyze, and protect against security threats in the social media arena.

Security, in general, is complicated by the shortage of security talent. Innovative MSSPs focus on short- and long-term employee acquisition, training, and retention using both traditional and progressive practices. Some of their tactics are apprentice programs, scholarships, in-house universities, university partnerships, and flexible career paths.

Further, regulatory requirements continue to evolve, and MSSPs can provide the expertise and evidence needed for oversight and compliance based on industry-standard certifications.

Businesses increasingly are turning to MSSPs to monitor and manage some or all of their security needs. Based on IDC market sizing, the MSS market is expected to continue to see growth in double digits in coming years.

Essential Service Provider Guidance

Organizations turn to MSSPs for the top 3 reasons:

- The challenges and costs associated with maintaining in-house solutions and expertise
- The opportunity to move from a capex to an opex expense model
- The need of assistance to combat adversaries that are increasingly "one step ahead"

The vendor selection process typically involves multiple decision makers, including C-level executives and even board members, who are well aware of the consequences of a breach. Enterprise priorities include risk reduction and compliance with applicable existing and emerging regulations and laws. Cost is always a factor, of course, but it is weighed in the context of what an MSSP can provide: overall breadth and depth of protection for an enterprise, threat detection/containment, brand and reputation preservation, perceived peace of mind, and even competitive differentiation.

Buyers can choose from pure-play MSSPs, systems integrators, consultancies, value-added resellers, and telcos — all of which can make a case for outsourcing some or all security functions.

For MSSPs that aspire to lead the U.S. MSS marketplace, IDC recommends:

- Determine how to define, package, and deliver cutting-edge services to targeted customer segments. Forward-thinking MSSPs have a vision, can articulate their approach, and demonstrate discipline and consistency from R&D through customer support.

- Understand that MSSPs without MSS 2.0 capabilities are likely to be at a competitive disadvantage. The future of MSS is cloud, mobile/BYOD, threat intelligence/big data, advanced detection techniques, and incident response/forensics. Marshaling the investment dollars, IP, technology, people, partnerships, and delivery/support mechanisms is advisable and necessary.
- Develop different versions of go-to-market messaging that highlight strengths and differentiation. Savvy MSSPs are prepared to speak to all levels of an enterprise (from workers to board members) with appropriate language, examples, demonstrations, and benefits. Other useful tools may include ROI scenarios and industry benchmarks. Furthermore, ongoing education is a value-added service that goes a long way toward establishing credibility and loyalty.
- Map out each customer's security journey that includes current and future states. Develop a living document that is the basis for ongoing conversations about strategy, technology, staffing, certifications, SLAs, and so on. Demonstrate thought leadership and mastery of the big picture and the details.
- Stay on top of target customers' security requirements, and implement the appropriate SOC model(s). SOCs and portals must provide a seamless user experience, which includes the desired visibility and control. Make it a priority to inform customers of new or improved services, and assist them with adoption. Send the right message about customer service and value.
- Be creative when it comes to identifying, acquiring, and retaining security talent. The people behind the technology matter a lot to customer satisfaction and growth.

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Managed Security Services

For the purposes of this research, IDC defines managed security services as "the around-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs), not through personnel onsite."

Exceptions and Inclusions

Managed security services can include complementary consulting and advisory activities that are typically defined under professional security services. The study did seek to understand whether the MSSPs offer complementary services as IDC believes these services are critical to the evolution and maturity of MSS. The MSSPs in this study do provide complementary services, although there is no standard approach for how they are offered. Commonly, an initial assessment is bundled with the onboarding fees, and some may bundle other services. Most, however, offer complementary services as optional add-ons and may charge separately for them.

Complementary services surveyed in the study include breach management, incident response, forensics, compliance services, and assessment of architecture and design. Not all MSSPs provide all of these services. Some MSSPs provide all of the listed complementary services and others such as managed security testing, application security testing, advisory services, integration services, and data privacy assessment.

Terminology

- **Managed security and information event management (managed SIEM).** This managed on-premises event collector transmits the raw log data to an MSSP's SOC for analysis, reporting, and archiving. This is an advanced, niche capability that is offered currently by half of the participants in this study.
- **Managed SOC.** A security operations center includes the people, processes, and technologies involved in detecting, containing, and remediating security threats. Some MSSPs take over the operation of SOCs that their customers have built and no longer want to manage. This is an advanced, niche offering that is offered currently by a majority of the participants in this study.
- **Security operations center types:**
  - **In-region.** A standalone SOC in a country or region
  - **Follow the sun.** A type of global workflow in which tasks are passed around daily at the end of work shifts among sites that may be in different time zones
  - **Global.** Workflow that occurs in one global location in a 24 x 7 multishift arrangement

Strategies and Capabilities Criteria

This section includes an introduction of market-specific weighting definitions and weighting values (see Tables 1 and 2).

TABLE 1

Key Strategy Measures for Success: U.S. Emerging Managed Security Services

Strategies Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weights
Offering strategy		
Functionality or offering road map	Excellence is marked by plans to offer core MSS with a road map for advanced MSS functionality including threat intelligence and complementary security services.	3.75
Delivery model	Excellence is marked by meeting customers' shifting preference for adoption and consumption.	2.50
Cost management strategy	Superior service includes vendor use of research, benchmarks, and other tools to ensure competitive cost and pricing and help clients justify expenditures for MSS.	1.50
Portfolio strategy	Excellence is marked by a portfolio of advanced and/or complementary services such as assessment and design that enable the client to make the most of the MSS engagement; in addition, greater weight is given to either proprietary technology or partner-licensed technology that is enhanced with proprietary capabilities and support/integration.	2.25
Subtotal		10.00
Go-to-market strategy		
Pricing model	Excellence is marked by comprehensive planning to align pricing options with customer and market preferences.	3.00
Sales/distribution strategy	Excellence is demonstrated by plans to offer various routes of purchase (e.g., online, direct, and indirect).	2.00
Marketing strategy	There is a well-articulated marketing plan associated with major initiatives or strategies.	2.75
Customer service strategy	There is continuous focus on ways to improve customer retention and satisfaction as they relate to service and support over the next three years.	2.25
Subtotal		10.00
Business strategy		
Growth strategy	Firms poised for growth focus on R&D/innovation and provide relevant offerings that address specific needs, particularly for industries or the size of the client.	4.00

TABLE 1

Key Strategy Measures for Success: U.S. Emerging Managed Security Services

Strategies Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weights
Innovation/R&D pace and productivity	Firms have plans to expand R&D activities and innovation initiatives for purposes of refreshing offerings and adding value for customers.	3.00
Employee strategy	There are clearly articulated plans for attracting and cultivating talent, including customized career paths and programs to develop future skills.	3.00
Subtotal		10.00

Source: IDC, 2016

TABLE 2

Key Capability Measures for Success: U.S. Emerging Managed Security Services

Capabilities Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weights
Offering capabilities		
Functionality/offering delivered	Excellence is marked by providing core MSS with some advanced MSS functionality including threat intelligence and complementary security services.	3.75
Delivery model appropriateness and execution	The vendor's current delivery model meets end-user preferences for MSS adoption and consumption.	2.50
Cost competitiveness	Pricing is competitive with market pricing as well as modular and scalable to meet customer requirements.	1.50
Portfolio benefits delivered	Excellence is marked by a portfolio of advanced and/or complementary services such as assessment and design that enable the client to make the most of the MSS engagement; in addition, greater weight is given to either proprietary technology or partner-licensed technology that is enhanced with proprietary capabilities and support/integration.	2.25
Subtotal		10.00

TABLE 2

Key Capability Measures for Success: U.S. Emerging Managed Security Services

Capabilities Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weights
Go-to-market capabilities		
Pricing model options and alignment	Flexible arrangements are available so that the client can choose to be billed as the budget allows (utility, capex/opex, with migration, quarterly/annual, etc.).	3.00
Sales/distribution structure, capabilities	Excellence is marked by the strength of the vendor's distribution model for the industries, geographies, and target companies the vendor serves.	2.00
Marketing	Target markets are well defined, and marketing messages are consistent and appropriate for each of the target markets.	2.75
Customer service	Customer service excellence is marked by the breadth of customer service and support offerings and by results.	2.25
Subtotal		10.00
Business capabilities		
Growth strategy execution	The company has a well-articulated growth strategy supported by examples of milestones achieved, acquisition of new capabilities, and organic growth.	4.00
Innovation/R&D pace and productivity	Firms are engaged in R&D activities and innovation initiatives.	3.00
Employee management	The vendor uses traditional and innovative methods of attracting and cultivating talent.	3.00
Subtotal		10.00

Source: IDC, 2016

LEARN MORE

Related Research

- *BrightPoint Security: Increasing the Relevance of Threat Intelligence with Trusted Circles* (IDC #US41151515, April 2016)
- *Worldwide Threat Intelligence Security Services Forecast, 2016-2020: Strength in Numbers* (IDC #US41053415, March 2016)
- *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016)

- *Vendor Profile: HackerOne — Bringing Hackers and Companies Together* (IDC #US40751416, February 2016)
- *Market Analysis Perspective: Worldwide Security Services, 2015 — Breach Is a Foregone Conclusion* (IDC #259239, September 2015)
- *Worldwide Cloud Hosted Enterprise Security Services (Security as a Service) Forecast, 2015-2019* (IDC #257959, July 2015)
- *Market Analysis Perspective: Worldwide Security Services, 2014* (IDC #253061, December 2014)
- *IDC FutureScape: Worldwide IT Security Products and Security Services 2015 Predictions — Moving Toward Security Integration* (IDC #253026, December 2014)
- *IDC MarketScape: Worldwide Managed Security Services 2014 Vendor Assessment* (IDC #248646, June 2014)

Synopsis

This IDC study presents a vendor assessment of providers offering managed security services (MSS) through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for MSS. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the MSS market over the short term and the long term.

"In-house security solutions are expensive and challenging to maintain in the face of a rapidly evolving threat landscape and formidable adversaries. As a result, enterprises increasingly are considering managed security services providers (MSSPs). MSSPs that offer MSS 2.0 services provide a plethora of security and consulting services along with the predictive threat intelligence and advanced detection and analysis expertise that are necessary to thwart attacks and protect assets. In the highly competitive security services marketplace, enterprise leaders need to be discerning buyers that understand their requirements and evaluate MSSP capabilities accordingly, regardless of how many security services are being outsourced." — Christina Richmond, program director, Security Services

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.