IDC MarketScape

IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment

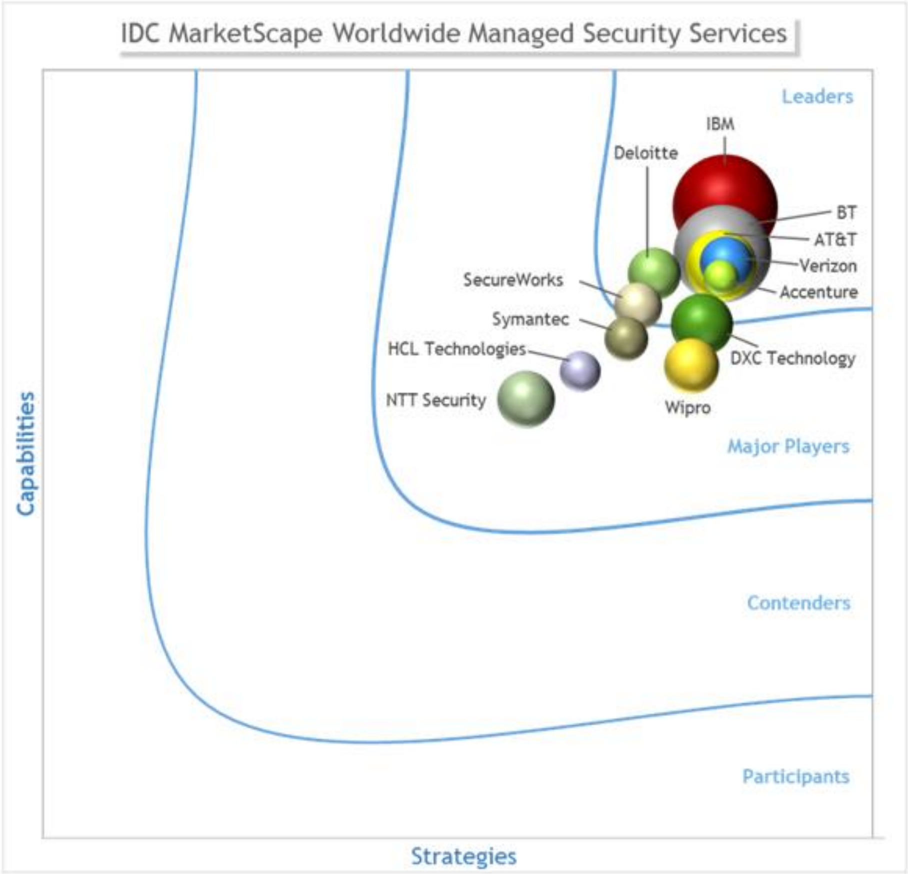
Martha Vazquez

THIS IDC MARKETSCAPE EXCERPT FEATURES: DXC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Security Services Vendor Assessment



Source: IDC, 2017

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment (Doc # US41320917). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The managed security services (MSS) market continues to evolve rapidly. Within just the past few years, even the past 18 months, managed security services providers (MSSPs) have added more capabilities and advanced security services to assist organizations in defending against and responding to today's attacks. Using the IDC MarketScape model, IDC has compared 12 organizations that offer MSS worldwide. Through in-depth MSSP interviews and more than 20 interviews with providers' customers, IDC learned that all the providers included in this study have the necessary capabilities to deliver traditional worldwide MSS. However, most are now able to go beyond the traditional services areas, incorporating advanced services such as distributed denial of service (DDoS), web application security, identity access management (IAM), managed security and information event management (SIEM), and managed security operation center (SOC) (see Appendix for further details) into their propositions. By its very nature, inclusion in this rating study indicates that participants are top-rated global providers and should be considered for managed security services. Furthermore, as a result of this IDC MarketScape evaluation, IDC identified the following eight companies as Leaders: IBM, BT, Verizon, AT&T, Accenture, Deloitte, DXC Technology, and SecureWorks. The group of Major Players consists of Symantec, Wipro, HCL, and NTT Security. Given the rapid pace of development within the MSS market, it is important that all providers continue to develop upon MSS capabilities and go beyond the traditional offerings. This is essential to keep pace with the development of the market, let alone remaining ahead of the chasing pack. Through more granular evaluation, IDC found that each provider possesses some unique strengths and weaknesses when compared with its peer group. At a high level, the major differences centered on their strategies for the next 12 months. Many of the providers now offer a breadth of complementary security transformation services to assist customers with digital transformation. Other factors that were looked at include pricing, marketing, security operation centers staffing, and customer portal capabilities. IDC believes that the following areas will drive the MSS market forward while providing vendors with the opportunity to hone a differentiated proposition:

- Complementary services that provide customizable opportunities for assistance in security transformation and maturity; these can include enabling security within a customer's journey to the cloud
- Cloud monitoring, visibility, and management capabilities that seamlessly enable hybrid implementations
- Flexible consumption models that match customers' preferences for integrating MSSP expertise, processes, and technology
- Pricing models that support the end customer's buying preference
- Mobility and IoT solutions
- Advanced detection methods 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
- Customer portal and reporting capabilities
- Security orchestration and automation technologies to provide more efficient incident response workflow
- Security operations centers
- Advanced methods of acquiring and retaining security talent

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 12 MSSPs within the 2016 IDC MarketScape worldwide 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:

- **Service capability across the MSS life cycle.** Each service provider was required to possess full-service MSS delivery capabilities (see the Appendix section for an explanation of MSS).
- **Revenue.** Each service provider was required to have 2015 total MSS global revenue in excess of $180 million and a SOC presence in each of three regions – the Americas, EMEA, and APAC – in addition to having a minimum of five SOCs.
- **Geographic presence.** Each vendor was required to have MSS delivery capability in each of three regions: the Americas, EMEA, and APAC.

ADVICE FOR TECHNOLOGY BUYERS

Buyers face complex choices in selecting an MSSP because of 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. This is important 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.

To enhance the decision-making process in vendor selection, IDC recommends that buyers bear in mind the following considerations:

- **Evaluate the MSS research and development (R&D) road map.** Many organizations are embarking on a digital transformation journey and are changing the way they operate, deliver services, and interact with their customers. It is imperative that an MSSP supports these organizations by providing trusted relationships and the security services needed to achieve their goals. Forward-looking MSSPs are paying attention to these changes and are enhancing their proposition around themes such as cloud evolution, incident response, forensics, advanced detection techniques, threat intelligence, artificial intelligence, machine learning, and big data analytics. Organizations need to evaluate an MSSP's future road map strategies and determine whether the MSSP will be able to provide the security support necessitated by digital transformation. For example, cloud monitoring services are becoming more important as organizations adopt cloud. A knock-on effect of this change is that identity access management will be a critical factor as more applications move to the cloud and users move to hybrid clouds. A further example is provided by the trend of MSSPs seeking to implement software-defined networking (SDN) and network function virtualization (NFV) technologies as a means to create internal cost efficiencies and provide more nimble and flexible services.

- **Review cloud adoption strategy and future security strategy.** Workloads are shifting to multiple cloud platforms. This makes it important to select an MSSP that can deliver the offerings that best fit your business needs and can be flexible to meet future changes occurring within your infrastructure. Many MSSPs are working with customers to help them move to the cloud securely and successfully, perhaps as part of broader IT services engagements. In fact, for some enterprises and public entities, this has become a top priority. MSSPs are working with customers to expand the delivery of cloud offerings, and they are helping organizations with management and monitoring using on-premises equipment for log collection. Organizations are looking for ways to monitor their infrastructures as well as applications when delivered through public cloud platforms such as AWS and Azure. While on-premises has been a stable delivery model for MSSPs, ongoing cloud migrations are driving the demand for MSSPS to offer hosted and even cloud-based delivery models.
- **Leverage threat intelligence and big data analytics.** 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. A commonsense best practice in retaliation to mitigate against these advanced attacks 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, user behavior- and heuristic-based detection (versus signature-based detection), anomaly detection, machine learning, emulation/sandboxing, virtual containerization, forensics, detection, and response tools. Buyers should look at how threat intelligence is being analyzed and distributed and whether MSSPs are using big data platforms such as Hadoop or Elastic Stack. Many MSSPs are investing in decreasing the human impact by automating data-related processes and analysis, which in turn will lead to faster decisions and response times. Buyers should look at how these MSSPS are investing in big data analytics, in growing their specialized skilled pool of researchers, adding dark web analytics, and cognitive and artificial intelligence.
- **Review 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. Many providers are revamping their MSSP portals to make them user friendly and easy to navigate with visualization tools and customizable reporting capabilities. In addition, portals typically include real-time data analysis and advanced analytic capabilities to improve investigation workflow for purposes of enhancing detection and response times. Increasingly, portals include role-based access, querying of security and information event management data with broad correlation capabilities, and real-time chat or instant messaging. MSSPs are expanding search and communication, self-service capabilities, and in-depth reporting and enhancing visibility for customers. 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).

- **Consider security expertise and customer engagement.** Buyers should consider how the engagement will occur between them and an MSSP once the services are established. It is important that the MSSP acts as a trusted advisor and as an extension to the customer's IT team. Buyers may want to review whether staff augmentation is needed to support their initiatives and bring on staff to work with them on-premises or evaluate the expertise of the analysts being provided to them. MSSPs should be investing in cybersecurity proficiency and acquiring and retaining security talent. Investments in training and retention methods are important differentiation in a competitive marketplace.
- **Evaluate 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 services such as security transformation, IoT, adversary simulation, security awareness training, and cloud security. Buyers should consider an MSSP that can help develop, strengthen, and continue to evaluate their security programs. 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 resources based on a current-state/future-state risk analysis.
- **Review package security solutions.** Security is becoming important not only in large enterprises but also in small to midsize organizations that are looking for lower cost, bundled security solutions. Services such as DDoS protection can be bundled with internet services and so forth. Small to midsize organizations should evaluate providers that will be able to provide these bundled services and products at a reasonable cost.
- **Investigate flexible pricing methods.** MSSPs typically offer their customers a number of pricing models. Ordinarily, a customer will choose to pay per device, by consumption of data (utility price option), or per IP pricing options. As MSS starts to downstream into midsize and smaller businesses, pricing models are becoming more flexible to accommodate the differences in scale and prioritization of smaller enterprises in comparison with larger ones. For example, some MSSPs are looking at newer and more innovative approaches. These include pricing per change request, logs/events collected, device-volume basis for which different tiers are offered, or pay-as-you-go pricing. Further, some MSSPs are investigating prepaid concepts, which hold some similarities in comparison with incident response "retainer" contracts. For example, customers can pay for a certain number of credits in advance using a standard rate. They allocate those credits against the activities they want at different times throughout the contract. With the introduction of new technologies, buyers need to be aware of the new pricing models and evaluate what will work best for their organizations.
- **Review security orchestration and automation technologies.** Providers are investing in automation and orchestration of technologies. The new techniques have a variety of benefits that can help customers order new services on demand and provide a more efficient workflow for analyzing threats. Buyers should be aware of what the MSSP road map looks like in implementing these new efficient technologies.
- **Determine which SOC implementation matches business requirements.** The types of SOC implementations are:
  - In-region: A standalone SOC in a country or region
  - Follow the sun (FTS): A type of global workflow in which tasks are passed around daily at the end of work shifts among work sites that may be in different time zones
  - Global: Workflow that occurs in one global location in a 24 x 7 and multishift arrangement
  - Some combination of in-region, FTS, and global SOC

More advanced MSSPs are able to offer a combination of SOC service delivery models in order to create a smooth handoff of change orders, tickets, and implementation as well as to create monitoring redundancy. In-region SOCs allow customer data to be retained in that region or country, which satisfies data privacy concerns and, in some cases, data sovereignty laws. To stay at the forefront of threat intelligence, however, MSSPs need to provide for anonymized meta-level data to leave the region or country for correlation purposes.

FTS creates an advantage for MSSPs with international or multinational clients (MNCs) that require around-the-clock monitoring and management. The single-shift nature often associated with FTS allows employees to live their lives without working a nighttime shift and can create a cost benefit for the customer. The disadvantage of FTS can be a lack of consistency in support around handoff processes, installations, and incidents as well as in a possible lack of monitoring redundancy. Finally, FTS allows for localization of talent, which satisfies clients that prefer in-region language support and cultural perspective. However, there can be disconnects between each SOC in the rotation, and these cultural/language barriers can become an obstacle.

IDC believes the highest tier of MSSPs, which are on the cutting edge of a truly global MSS delivery (versus international — see the Terminology section), can satisfy regional data privacy concerns and the facilitation of an MNC security strategy with a combination of in-region, FTS, and global SOC structure.

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.

IDC reviewed 12 MSSPs against current capabilities and future strategy criteria as part of its IDC MarketScape on the worldwide MSS market. IDC also conducted customer interviews of more than 20 vendor customers to obtain feedback on how the vendors performed in delivering MSS. Vendors participating in the analysis are Accenture, AT&T, BT, DXC Technology, Deloitte, HCL Technologies, IBM, NTT Security, SecureWorks, Symantec, Wipro, and Verizon.

DXC Technology

According to IDC analysis and buyer perception, DXC Technology is considered an IDC MarketScape Leader worldwide.

In early 2017, CSC and Hewlett Packard Enterprise (HPE) combined to create a service provider named DXC Technology. CSC is a multinational corporation based in the state of Virginia that provides IT services and professional services. Hewlett Packard Enterprise is located in Palo Alto, California. For this research, IDC has analyzed DXC Technology as HPE's capabilities and then combined CSC's capabilities into its future strategy. As of today, both offerings are still separate but will be consolidating their offerings starting in 2Q17. These two companies together bring significant mass and expertise to the MSSP landscape. Both companies bring capabilities to the other to strengthen and fill gaps in the overall offering. For example, HPE has nine SOCs globally, with two in EMEA, four in the Americas, and three in the APJ region. All of the SOCs function on a 24 x 7 x 365 model, with in-region pairing for support of regional clients in a model that ensures client familiarity and failover in case of disaster. The support model is used by some providers where the support for customers includes level one SOC analysts along with higher senior level SOC analysts. They are all grouped around a small number of clients within the same industry and can also be assigned to just one large enterprise client.

CSC brings six global SOCs all managed under a 24 x 7 x 365 workflow model. The SOC locations include three in APJ, two in the United Kingdom, and one in the United States — many supporting both public sector and commercial clients.

HPE describes one of its key differentiators as the combination of its security advisory, threat intelligence, and managed security services capabilities. This is particularly beneficial to organizations that are looking for an end-to-end, advisory-led approach, especially in meeting country-specific data privacy requirements. HPE is focused on helping organizations through security transformation, security maturity improvement, and managed services for those clients that require hybrid or ongoing comanaged services. These capabilities are supported by a full portfolio of MSS services that provide clients device and operational management of their security infrastructure, monitoring, and incident response. HPE believes that the combination in the MSS business of one player that can offer an integrated proposition between advisory, security management, security monitoring, and incident response is offering significant value to its customers from both a detection and a response perspective.

CSC differentiates itself in the market by being a vendor independent end-to-end IT services company. CSC has developed cloud partnerships to offer cloud security services. CSC is creating cloud security solutions that can be deployed in virtual, public, and private cloud environments. In addition, CSC has also invested in a similar security monitoring offering to HPE called Integrated Security Operations (ISecOps) that will further integrate with client's workflow and the remediation processes. This new capability provides a set of cybersecurity operational processes and advanced workflows built on top of the ServiceNow platform. As DXC Technology consolidates its offerings and platforms for MSS, IDC expects a blend of detection and response capabilities from HPE and workflow, orchestration, and response capabilities from CSC.

Strengths

Both companies have a stable reputation and brand name. The combination of CSC and HPE will result in a span of new capabilities and complement some service gaps lacking in each. HPE's advisory and consulting services and CSC's strong partnerships will also enable DXC Technology to make a leap in creating new cloud security services as well as improve automation and orchestration techniques.

Challenges

DXC Technology could further enhance its advanced detection and analytic technologies such as behavioral and heuristic-based detection techniques and big data analytics, which we understand has been in progress on the HPE side. IDC anticipates that the new company may run into challenges related to retaining employees and transitioning customers to new processes.

APPENDIX

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 and 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). They are also investing in mobile/IoT, cloud, threat intelligence/big data analytics, incident response/forensics, and advanced detection techniques. Cloud, mobile/IoT, 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.

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

LEARN MORE

Related Research

- *IDC MarketScape: Western Europe Managed Security Services 2017 Vendor Assessment* (forthcoming)
- *Worldwide DDoS Prevention Products and Services Forecast, 2017-2021* (IDC #US42570517, May 2017)
- *IDC MarketScape: U.S. Emerging Managed Security Services 2016 Vendor Assessment* (IDC #US41320816, August 2016)

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.

"The security landscape is changing rapidly, and organizations continue to struggle to maintain their own in-house security solutions and staff. As a result, organizations are turning to managed security service providers (MSSPs) to deliver a wide span of security capabilities and consulting services, which include predicative threat intelligence and advanced detection and analysis expertise that are necessary to overcome the security challenges happening today as well as prepare organizations against future attacks. The MSSP market is highly competitive, and many MSSPs have a breadth of security services in their MSS portfolio. The differentiation among these MSSPs will be tied around their flexibility in delivering security services and advanced MSS capabilities and how these MSSPs can continue to assist organizations with their security needs today and in the future." – Martha Vazquez, senior research analyst, Infrastructure 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