IDC MarketScape

IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment

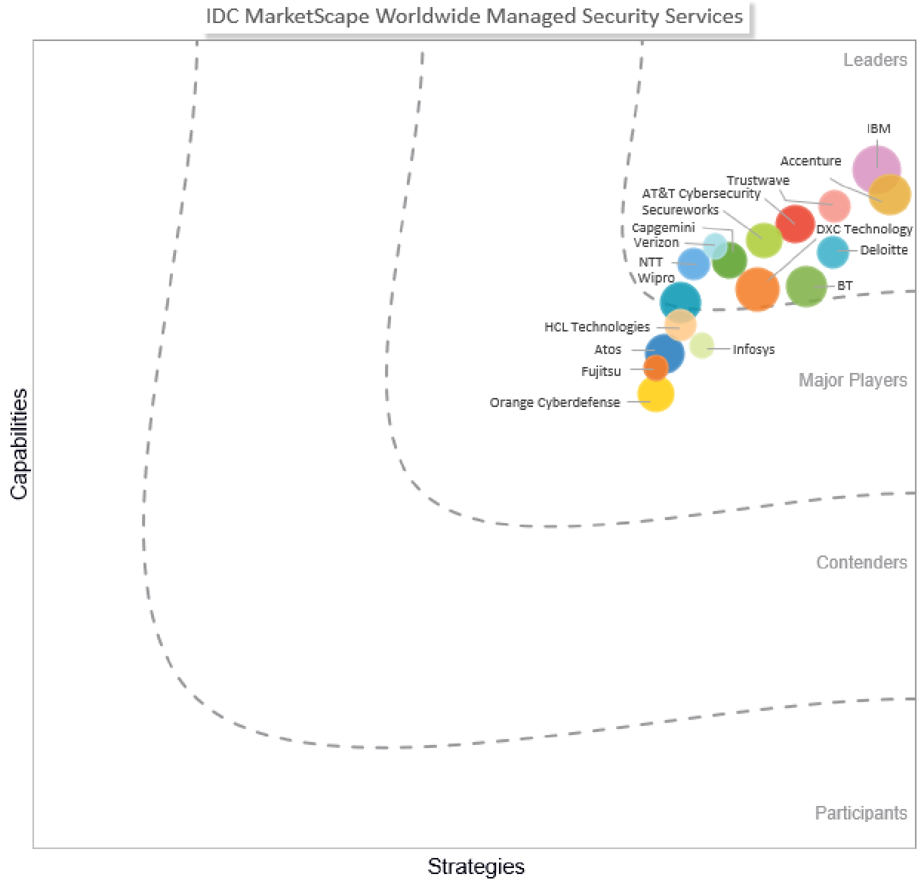
Martha Vazquez

THIS IDC MARKETSCAPE EXCERPT FEATURES NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Security Services Vendor Assessment



Source: IDC, 2020

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

September 2020, IDC #US46235320e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment (Doc # US46235320). 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. Especially over the past year, MSS service providers (SPs) have continued to flourish even during these turbulent times. In 2020, IDC has studied how service providers are shifting their offerings, technology, methods, and processes to assist organizations in defending and responding against modern attacks. The year of 2020 has been quite interesting because of the COVID-19 pandemic, and while IDC did not rate any providers on their responses to the current pandemic, we did see a shift in focus because of the rapidly changing needs of worldwide organizations. The pandemic pushed organizations to take a step back and review their security functions that they had in place and those that were needed to support the new remote workforce.

Even before the pandemic, service providers had already been experiencing a pivotal change in how they view security and they needed to notch up their detection and response capabilities. No longer are organizations only looking for management of security products and management of policies and rule sets or looking to just maintain compliance regulations, although that is not to say that these functions are not important. Instead, organizations are asking their service providers to assist them in quicker response times and to provide remediation against current attacks. In addition, organizations are struggling with understanding their security maturity and risk. As organizations struggle with elevating their cybersecurity maturity, they also look at security from a business and strategic viewpoint to know how they can be prepared against an attack when it occurs.

The shortage of cybersecurity experts, who could make sense of the data coming in from different environments (e.g., multiple clouds, edge, and on premises), motivated security service providers to invest more in areas such as threat intelligence, machine learning (ML)/artificial intelligence (AI), automation, and analytics. The combination of these new investments also provided the scalability for organizations to do things faster and with fewer errors than humans. In fact, according to *Key Findings: 2019 U.S. Managed Security Services Survey Results* (IDC #US45632819, November 2019), the top demand for outsourcing security services was driven by the need to protect against advanced security threats, 24 x 7 support, and security expertise to improve availability and performance and for access to new emerging security technologies.

IDC believes that the following areas will drive the MSS market forward while providing vendors with the opportunity to hone a differentiated proposition:

- The breadth and scope of MSS offerings for complex IT environments
- The use of advanced and emerging technologies that will provide greater visibility against sophisticated threats and provide enhanced use of automated processes
- Flexible and satisfactory onboarding time frames, methods, and procedures
- The ability to deliver higher level of orchestration, automation, and openness in the core platform

- Global delivery and support of security services such as security operations centers (SOCs) distributed evenly across various geographies and with follow-the-sun (FTS), 24 x 7 capabilities
- Cloud monitoring, visibility, and management capabilities that seamlessly enable multiple cloud implementations
- High level of customer support, expertise, and satisfaction
- Flexible deployment models that match the customer's preferences for adopting and consuming services
- Pricing models that support the customer's buying preference
- Customer portal enhancements such as a mobile app and reporting templates to present to C-suite and board executives
- Acquiring and retaining top-notch security talent

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied 17 organizations that offer MSS across the globe and surveyed over 20 customers using their services in 2020. Evaluated vendors provide global capabilities, and while there are many service providers providing MSS globally, specific services and criteria must be met to have qualified for this vendor assessment:

- **Service capability across the MSS life cycle.** Each service provider was required to possess full-service MSS delivery capabilities (see the Appendix for an explanation of MSS).
- **Revenue.** Each service provider was required to have 2019 total MSS global revenue in excess of $170 million and minimum of five SOCs located globally.
- **Geographic presence.** Each vendor was required to have the MSS delivery capability in each of the three regions: the Americas, EMEA, and APAC.

ADVICE FOR TECHNOLOGY BUYERS

Organizations that are considering purchasing managed security services realize that their IT environment is in a state of flux, constantly changing especially during the recent pandemic, which created some unique challenges in how organizations are conducting business. As organizations evaluate the type of providers to outsource their security controls to, they should be mindful in understanding the wide scope of security service providers that can handle their unique IT requirements.

A plethora of variables are looked at when selecting a third-party service provider, which includes the portfolio of security service capabilities, expertise and service support, onboarding processes, portal functionality, partnerships, platform openness, deployment options, and flexible pricing options.

With the ongoing changes occurring today in the security landscape, along with the rapidly evolving pace of technology, organizations must evaluate offerings for today and for the future. This is important to be sure that future offerings align with anticipated business changes 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. A provider that can offer customer satisfaction surveys, pricing benchmarks, use cases, proofs of concept, and/or best practices can also aid the decision process.

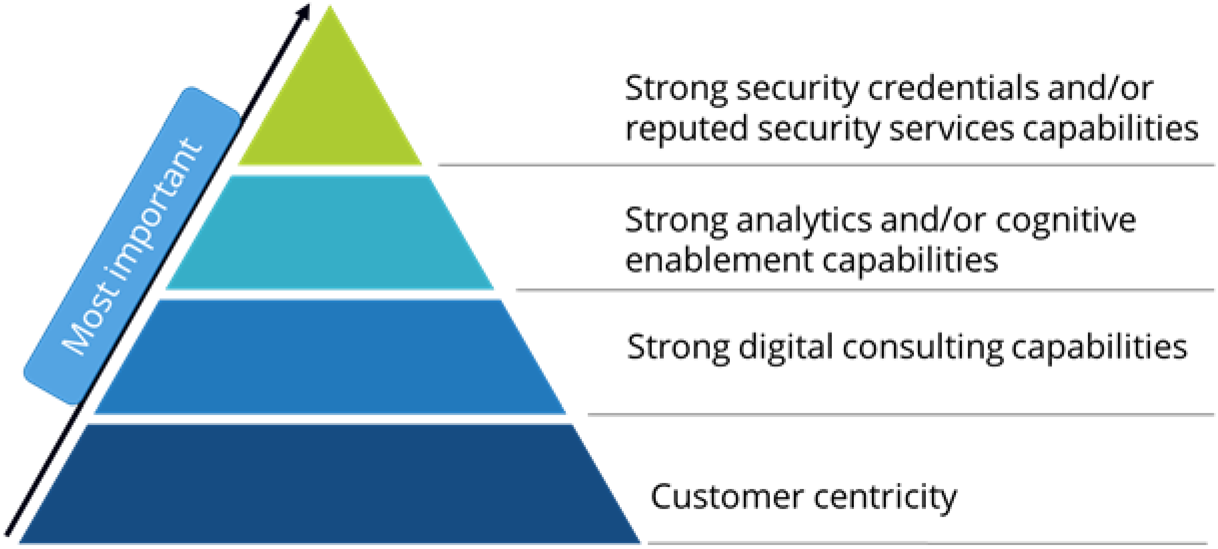
In 2020, IDC continued to see more security service providers, such as telecoms, cloud providers, systems integrators, value-added resellers (VARs), boutique providers, security product suppliers, and consulting companies, entering the MSS market as a MSS service provider or as a managed detection and response (MDR) provider. All these providers offer a differentiated value, service, and support to their offerings. As organizations start evaluating providers for their outsourcing needs, the breadth of options can only exacerbate the evaluation process in choosing the right service provider. In addition, the expanding attack surface, the remote workforce, and the complexity in the IT infrastructure are a lot to take in and understand. Buyers of these security services need to be selective in trusting and picking a partner that can help them make strategic security decisions and maintain a healthy security posture.

According to IDC's 2019 *Managed Security Services Survey,* when organizations were asked what are the requirements when looking for a MSS service provider, they said the following four requirements are of upmost importance for forward-thinking MSS service providers to be able to respond quickly to advanced threats: strong security credentials and/or reputed security service capabilities, strong analytics and/or cognitive enablement capabilities, strong digital consulting capabilities, and customer centricity (see Figure 2).

FIGURE 2

Top Requirements for the Next-Generation MSS Service Providers

Q. What requirements should a future-thinking MSSP should have?


Most important
Strong security credentials and/or reputed security services capabilities
Strong analytics and/or cognitive enablement capabilities
Strong digital consulting capabilities
Customer centricity

n = 402

Source: IDC's *Managed Security Services Survey,* January 2019

Choosing the right provider is critical, and buyers of MSS should consider their organization's IT requirements, geographies, verticals, and overall strategic business goals when choosing a provider. IDC advises organizations to keep the following things in mind when selecting the partner provider:

- **The breadth of the MSS portfolio.** There are a breadth of providers that offer low-end services to customization type of managed security services. Therefore, it is important for an organization to evaluate all various types of offerings that will meet their IT requirements. The buyer in this market could be looking for traditional security controls such as firewalls, IDS/IPS, security information and event management (SIEM), vulnerability scanning, and secure messaging. All providers in this document provide these offerings, but these offerings have also expanded to include advanced services such as identity and access management, threat intelligence, web application scanning, managed detection and response, managed SOC, and vulnerability management/risk monitoring. MSS service providers have also started to offer complementary services such as incident response (IR), forensics, and other digital consulting capabilities. Depending on the buyer's security posture, one may choose to go with a provider that can help the organization move up its security curve (see Figure 4).
- **Digital consulting capabilities.** When planning on adopting and/or addressing security challenges, organizations should not just implement the "newest" and "shiniest" technology. A sound security program needs a comprehensive approach, which includes evaluating the people, process, and technology. Many of the providers listed in this document can assist organizations to access their inventory, assets, data, and security program, but it's important for an organization to understand what they have today and what they may need in the future. Many service providers offer digital consulting capabilities as complementary services, which can assist an organization in how to utilize security within digital (3rd Platform technologies) and achieve their strategic objectives. According to IDC's *Managed Security Services Survey* (refer back to Figure 2), organizations believe that a forward-thinking MSS service provider should offer strong digital consulting capabilities. Organizations should choose a provider vendor that can partner with them as they assess where they are today, what gaps they have in these security programs, and how they will work together to continue to build upon their security journey.
- **Managed detection and response.** According to IDC's 2020 *MSSP and MDR Survey,* respondents noted that one of the five drivers for partnering with a service provider is the ability to access emerging security tools and technologies. Therefore, organizations looking for a MSS service provider should consider what security type of advanced tools are being used to enhance their security position. For example, MDR has become the next advancement of MSS, which includes an integration of capabilities such as threat detection (TD) tools for endpoint detection and response (EDR/cloud network), SIEM, threat intelligence, threat hunting, automated response and orchestration, big data and analytics, ML/AI, incident analysis, and remote incident response (see the Market Definition section). The response capabilities will be a differentiator for many service providers. High-performing incident response takes time and skill, which many organizations just don't have. Therefore, looking for a provider that can provide various levels of support for deeper investigation analysis along with enhanced guidance on containment, remediation, and future mitigation should be a crucial area during the evaluation.
- **Threat intelligence, threat hunting, and other advanced capabilities.** Service providers are going beyond the normal abilities and deepening into areas such as threat intelligence. Threat intelligence has become such an important component to advanced services such as MDR and is being integrated into MSS and MDR offerings. Threat intelligence is one offering that can vary depending on the expertise and global network of the provider. Many providers continue to enhance in this area by providing deeper sharing abilities (across network, endpoints, and other telemetry), going beyond just indicators of compromise (IoCs) by making the intelligence more insightful in verticals, geographies, and adversary tools, tactics, and procedures. Service providers are also finding ways to extend their data set to improve the

analysis and create better ways to identify modern threats and understand the various of known campaigns. Threat intelligence is fed into the other importance aspect, which is threat hunting. Some service providers are providing regular usage of human-led or automated threat hunting from the integrated threat intelligence feeds and creating processes and playbooks from its discoveries.

- **Platform that provides visibility across endpoints, network, and cloud.** A security partner should be able to demonstrate innovation capabilities in its core platform as well as its use of emerging technologies. A true value to the organization is the ability to choose a vendor that can provide complete visibility of a detection and response management life cycle. Service providers continue to add to their core platform more abilities to take in various types of data into a single platform. While the cloud aspect has brought in several complexities, other technologies such as Internet of Things (IoT) and operational technology (OT) are also being added and need to be considered. The introduction of IoT and OT infrastructures is bringing a new set of threats, and CISOs need to be prepared to face these challenges, as the response and mitigation techniques vary wildly between IT and IoT/OT devices. As the data coming in now increases in volume, service providers are embedding enhanced AI/ML technologies and leveraging cognitive support systems to advance detection and response capabilities.
- **Integrations of orchestration and automation processes.** Service providers are focusing more on orchestration and automation tools and integrating these technologies into their core delivery platforms. Along with advanced ML and AI, technologies such as orchestration and automation are assisting service providers to enhance SOC efficiency and help analysts prioritize, analyze, and respond to threats faster. Automation and orchestration tools are assisting organizations to evolve and utilize analytics in much greater capacity and delivering reduced mean time to detect and mean time to respond (MTTR). The use of these areas in automation is also assisting in delivery mechanisms, reducing onboarding time frames and standardizing processes in implementing new services.
- **Global SOC requirements.** Global organizations should consider security providers' methodologies and SOC operations that will fulfill their direct requirements. Service providers like to demonstrate their multiregional and/or global capabilities by listing the number and locations of each of their SOCs that provide MSS capabilities. Having the first shift for each SOC being able to respond to any IoC for another region that is outside of their first shift rather than relying on an overnight (graveyard) shift to analyze and potentially respond to incidents will provide better outcomes. This is a key offering of delivering a 24 x 7 x 365, follow-the-sun capability.
- **Research and development (R&D) investments.** As previously mentioned, emerging technologies and advancements are crucial areas to evaluate when selecting a partner. Future-thinking security providers not only need to be investing in their offerings, but they should have a sizable R&D budget to look out over the horizon at what is required to keep their clients safe in the outlying years. Are they investing in key technologies like cloud security, IoT/OT infrastructures, and the IR playbooks that are so crucial in automating and reducing the mean-time-to-respond KPI? The need for monitoring and responding for OT and IoT is becoming more crucial along with the cloud security requirements. Organizations should evaluate what the provider's current and future investments are in these areas.
- **Security expertise and support.** Ask about the provider's customer engagement program. A good security service provider will agree that the teams of cybersecurity practitioners that power their services are often thought of as remote members of their clients' cybersecurity team. The tenure of the cybersecurity team is increasingly becoming a differentiator. Key components of talent retention and training are critical to be a reliable security provider. Buyers must select a provider that will act as a trusted partner and as an extension to the IT

team. Knowing that the provider understands the organization's IT environment and challenges will simplify the ability to continue to make recommendations and tweaks and provide ongoing guidance along their security journey.

- **Cloud security strategy.** One of the areas that continues to be developed and enhanced includes cloud security. Organizations are moving to the cloud faster than ever before and therefore should look at the provider's current integration of cloud security and how it is integrated across the life cycle from strategy to implementation to run operations. The ability to deliver flexible cloud models across multiclouds and work in environments for providers such as Amazon Web Services (AWS), Microsoft, and Google is important based on the organization's needs. It is important to evaluate a service provider that will assist and provide recommendations for the organization moving and utilizing these diverse IT environments.
- **Portal reporting and capabilities.** Portals are still used to enhance the customer experience and support mechanisms. Organizations should review portals and demo the various differentiators between each provider. Forward-thinking service providers either have a mobile app or are investing in one that can benefit end users by providing real-time access and availability to ticketing and workflow analysis. In addition to providing solid visualization and analytic tools, enhanced reporting capabilities, risk metrics, self-service, live support, and authentication are all the areas that can help drive a better customer experience.

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.

NTT

NTT is positioned as a Leader in the IDC MarketScape for worldwide managed security services 2020 vendor assessment.

After integrating all the MSS-specific resources and delivery platforms of NTT Group companies in 2016, NTT carried out another reorganization exercise in 2019, consolidating 28 of its brands under one new entity called NTT Ltd. The integration, finalized in July 2019, made NTT Ltd. an $11 billion company with over 40,000 employees.

NTT has 12 SOCs: 6 in APAC, 3 in Europe, and 3 in the United States. Although these SOCs are 24 x 7, not all are for the same services. Workflow models are determined primarily by the functionality delivered rather than by location. Some SOCs specialize in delivering the threat detection service and have 24 x 7 capability for this service. Other SOCs may have clients in region that require threat detection, which the SOC can support only during regular business hours before a handoff to one of the 24 x 7 threat detection SOCs. Some SOCs may have no TD capability and clients are served by the next appropriate SOC. The approach is applied for other services such as security device management, enterprise security monitoring, and vulnerability management. Some SOCs specialize in these services and can deliver 24 x 7, while other SOCs only have the regular business hours capability and then handoff to one of the 24 x 7 SOCs.

NTT has acquired many companies in the past several few years but has now combined these resources and platform into one. Its MSS offerings are aligned to business-specific objectives and cornerstone in the full life cycle of services. Through a common delivery model and structure, NTT offers all services in a centralized manner where possible and localized when required. NTT offers modular managed security services components within threat detection, vulnerability management, enterprise security monitoring, and device management. This modular approach allows NTT to tailor to client requirements and ultimately deliver value to customers. NTT's MSS support hybrid IT and OT environments. Its advanced analytics detects the proverbial "needle in the haystack," and NTT achieves this by reducing focus on "blocked alerts" and shifting focus to "suspicious allow-events." Its advanced analytics engine is made up of components such as threat intelligence correlation, threat hunting, and the machine learning framework.

According to NTT, the scale and innovation of the threat detection service has the visibility and ability to uncover threats and confirmed incidents. TD underpins NTT's value proposition to stay one step ahead of threat actors and to proactively manage client's security posture and risk profile. NTT's threat detection differentiates from the company's MSS offerings because it creates efficiencies that improve clients' cyber-resilience, operational maturity, and response capabilities.

The scale of NTT's threat intelligence capabilities is based on internal and external sources, which NTT believes is difficult to build in-house. One example of this innovation is that a TD analysis engine relies on proprietary custom IoCs for detection of threats. Developed specifically to enhance endpoint detection and response technologies, incidents are detected ~70% of the time by the custom IoCs rather than by the native technology alone. Often, these IoCs are developed because of advanced correlation of network and endpoint log events. Depending on the devices under management, NTT can conduct additional activities for greater visibility into the incident such as endpoint forensics as well as contain or isolate problem areas for customers.

NTT engages over 200 technology partners and works very closely with its strategic partners to co-innovate or jointly develop new offerings. Further, NTT acquired WhiteHat Security and made strategic investments with innovative companies such as ShieldX to enhance its capabilities and push new offerings such as DevSecOps services.

Strengths

According to customer feedback, NTT has been one of the most straight-forward, easiest companies to work with. From a customer perspective, NTT was notable for having the expertise and strong knowledge in threat intelligence and accurate detection capabilities.

NTT works in global operating model and local presence when needed. NTT delivers a wide range of MSS that address the full life cycle of security services. NTT offers modular components of MSS to help customers in building their security posture. NTT today offers service packaging for existing services to target specific needs such as threat detection and OT to cover both IT and OT into a single service. In addition, service packaging is offered for specific verticals such as vehicle SOC for automotive. Pricing models are flexible and offer different service levels, devices type, metrics, and discounts. From a road map perspective, NTT is looking at streamlining pricing models and simplifying them for customers.

NTT continuously invests in R&D and develops its proprietary tools and platforms. The company plans to continue to invest in the platform and address additional levels of automation, orchestration, and openness by introducing emerging technologies and offering an open API concept for multivendor integration into the platform.

Challenges

While the portal has some very good features, it does lack enhanced analytics and visualization tools. Specific compliance reporting is also not available, but it is on the road map to provide to customers in the next 12–18 months. In addition, NTT has alluded to adding portal enhancements to the analytics and visualization capabilities.

Consider NTT When

Midsize to large multinational organizations that are looking for a global telco provider with good local support should consider NTT for their MSS needs.

APPENDIX

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 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

For the purposes of this research, IDC defines managed security services (MSS) as "round-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs)." We include all MSS, whether these involve the management of security solutions deployed on a customer's premises or solutions hosted in a datacenter external to a customer's premises. There is a steady stream of new services offered by MSS providers that extend beyond traditional managed security solutions. The primary reason for many of these services is essentially to manage the security operation, including integration across various security technology domains, such as managed SOCs and different phases, such as managed response services.

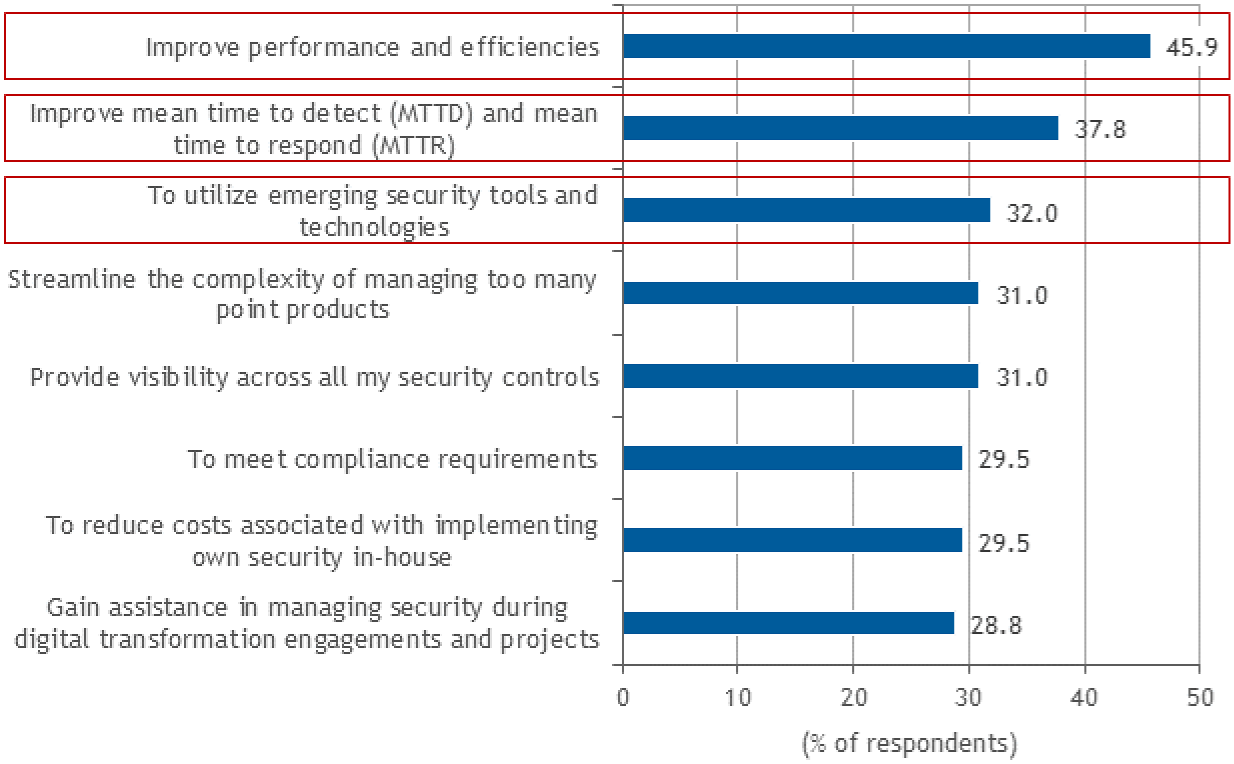
Figure 3 lists the top reasons that are most important when using a service provider. According to IDC's 2020 *MSSP and MDR Survey,* customers are turning to security service providers for various needs — but the top drivers include improving performance and efficiencies, improving mean time to detection and respond, utilizing emerging security tools/ technologies, providing visibility across all security controls, and meeting compliance requirements.

IDC defines managed security services as the around-the-clock remote administration and/or monitoring of IT security functions delivered by remote personnel at security operations centers operated by a third party. Activities such as patch management, managed endpoint/antivirus, managed firewall/unified threat management (UTM), and managed security information and event management (SIEM) are performed on cloud and managed on-premises devices.

FIGURE 3

Top Reasons to Use Security Services Provider

Q. Please select the top 5 reasons that are most important when using a security services provider.



n = 410

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *MSSP and MDR Survey,* May 2020

To fully understand why so many providers are seeking to provide managed detection and response (MDR) to aid firms in upping their cybersecurity programs, it is essential to know how the vendors that provide managed security services have evolved their functionalities over the years. Grouping together the different capabilities into different classifications, IDC currently recognizes three distinct levels of MSS, which are discussed in the sections that follow (see *MDR: The Next Generation of Managed Security Services,* IDC #US46427920, June 2020).

MSS 1.0

The first rollout of MSS represented the initial mindset of organizations that were seeking to stop attacks at the perimeter or the endpoint level. Managing the configuration of firewalls and collecting logs from various devices marked some of the initial offerings that MSS service providers and managed SPs performed. As firewalls morphed into unified threat management appliances, service providers also took on the role of managing the antivirus, intrusion detection and prevention, content filtering, and other capabilities that these devices were able to provide. Other services offered include traditional MSS functions like patch management, device health checks, and vulnerability scanning.

MSS 2.0

As organizations started undergoing digital transformation (DX) and shifting to hybrid (cloud and on-premises) IT environments, the need for more advanced cybersecurity capabilities became more apparent. Security service providers were forced to evolve and accelerate their adoption of new security technologies to meet the cybermiscreant on the battlefield. Advanced technologies such as machine learning/artificial intelligence, big data and analytics, automation, and orchestration provided the technical foundation to assist customers in combating advanced threats.

As some MSS service providers moved deeper into MSS 2.0, consultative or complementary security services such as breach management, assessments of architecture and design, forensics, and incident response became part of the service offering. In this world of increased privacy and security regulations, compliance services that are needed for government and third-party compliance tracking have been added to the menu of services that service providers now offer.

MDR Services Creates the Next Generation of MSS 3.0

Now more than ever, service providers are racing to offer in-depth advanced detection and response capabilities to compete in the ever-evolving cybersecurity market. As competition stiffens, IDC is seeing the market brings in a breadth of different competitors such as consultants, integrators, pure-play security vendors, telecoms, and cloud/hosting companies. These different providers are all partnering and developing their own proprietary technology to stay ahead of the curve. Since the market has evolved, the role of a traditional MSS service provider has matured and expanded in which IDC acknowledges the expansion of managed detection and response providers and services, which we could consider the next generation of MSS, or MSS 3.0. MDR, as a subset of MSS, combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity life-cycle capabilities for an organization. Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities, along with cybersecurity partners' supplied tools or services and private intellectual property. MDR services are supplied by a provider's well-trained cybersecurity staff in a 24 x 7 x 365 remote SOC. IDC will publish a follow-up document to this IDC MarketScape and review those providers offering managed detection and response capabilities. IDC MarketScape for MDR will be published in 2Q21.

LEARN MORE

Related Research

- *Data Security and Threat Detection/Response Top of Mind in Both MSSP and MDR Evaluation* (IDC #US46762320, August 2020)
- *COVID-19 Implications for Security Services* (IDC #US46192319, April 2020)
- *Key Findings: 2019 U.S. Managed Security Services Survey Results* (IDC #US45632819, November 2019)

Synopsis

This IDC study presents a vendor assessment of worldwide 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.

"Organizations are struggling to acquire the security expertise to assist in managing and monitoring the constant flow of security threats and to fully implement and integrate the growing number of tools that their security teams have acquired. As a result, organizations are turning to MSS service providers to deliver the security expertise, spanning managed security and complementary services to assist in preparing, detecting, and responding against future attacks. These service providers are racing to offer in-depth advanced detection and response capabilities to compete in the ever-evolving cybersecurity market. The various providers are all partnering and developing their own proprietary technology to stay ahead of the curve. Since the market has evolved, the role of a traditional MSS service providers has matured and expanded in which IDC acknowledges the expansion of MSS, termed *MSS 3.0,* which entailed managed detection and response. It will be interesting to see how these competitors continue to stay ahead of the curve and display continued differentiation within the security landscape." – Martha Vazquez, senior research analyst, Infrastructure Services at IDC

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