Market Guide for Managed Security Services

Published 7 December 2020 - ID G00716393 - 24 min read

By Analysts Pete Shoard, Kelly Kavanagh, Mitchell Schneider, John Collins

Initiatives: Security Operations

Managed security services (MSSs) provide organizations with remote 24/7 monitoring of security technologies and response to security events across a range of environments. Security and risk management leaders use MSSs to identify, advise and, where appropriate, respond to threats on their behalf.

Additional Perspectives

- Summary Translation: Market Guide for Managed Security Services
  (25 December 2020)

Overview

Key Findings

- MSS providers offer an array of standardized and customized security services for the purposes of threat awareness and defense, and this breadth of service offerings provides wide choice but overlaps with capabilities offered by other market segments.

- Differentiation among MSS providers can be hard for buyers to quantify, as service capabilities and delivery models are not always directly comparable with one another.

- The security technology management services that were traditionally offered only by the MSS market are now seen offered by nonsecurity-specific vendors in the ITO and NSP markets as well as directly by technology vendors themselves.

- Consultancy-driven engagements are often confused with services engagements, making it hard to predict cost and value for money in provider offerings.

Recommendations

Security and risk management leaders responsible for security operations should:

- Prepare adequately before engaging MSS providers by having well-defined, risk-based security requirements and use cases.

- Focus on outcomes and deliverables and, where possible, avoid being prescriptive around the delivery model or technologies used to deliver against requirements.
Assess if existing managed service providers (MSPs) and IT outsourcing partners meet security technology management requirements before approaching dedicated security service providers.

Prepare the internal processes that will be used to consume and respond to the outcomes and deliverables that an MSS provider will deliver.

Ensure that constraints on technology choices or deployment restrictions (such as compliance, regulatory or legal needs) are well-communicated to potential providers early in the stages of engagement.

Strategic Planning Assumption
By 2025, 50% of organizations will allow third parties to go beyond pure monitoring for security breaches but also provide mitigation using remotely accessible security technologies, up from 15% today.

Market Definition
MSSs primarily provide organizations with remote 24/7 monitoring of security technologies and security-related events across a wide range of platforms for the purposes of identifying, advising on remedial action, and (where appropriate) responding to threat exposure and security incidents on behalf of clients.

In addition to threat detection and response services, MSS portfolios usually include one or more of the following managed services, often delivered in addition to other services that may be specific to the provider’s core market (for example, IT outsourcing or telecommunications):

- Incident response services
- Vulnerability assessment and managed vulnerability services
- Threat intelligence services

MSS providers offer a variety of different engagement models. These include heavily customized and consultancy-led models and commoditized technology management-driven experiences. Each engagement considers the customer’s individual use-case-driven requirements, current technologies and risks. Each then aligns repeatable services where possible and design and build elements where necessary.

Delivered as human-performed, technology-supported services, managed security must deliver more than the findings of a technology. It must combine human expertise and analysis, with efficient processes to deliver actionable outcomes that the buyer can consume.

Market Description
The MSS market is composed of security pure-play vendors, network services or telecommunications providers, and system integration (SI), IT outsource (ITO) and consultancy firms, which offer managed security independently of, and in addition to, connectivity and enablement technology. There are also consultancy-driven organizations that often provide services as a logical offshoot of an assessment and have standardized their offerings to deliver them repeatedly as a service.

Services offered are commonly delivered on a 24/7 basis, although there is often flexibility in MSS models to offer off-hour capabilities and staff augmentation. At the center of such services are threat detection and response capabilities, usually delivered through leveraging a multitenant security information and event monitoring (SIEM) platform. They can also include or run these services directly on endpoint detection and response (EDR) platforms and network detection and response (NDR) platforms without the need for a central log management platform such as SIEM. More traditionally, MSS services are passive and informational, not providing containment or response to incidents outside of call-off incident retainer-style services. However, as advancements in security technologies have enabled remote containment and MSS organizations have begun to offer managed detection and response (MDR) services (see Market Guide for Managed Detection and Response Services), MSS providers are more commonly containing issues remotely on behalf of buyers. This is also an increasing trend that is available outside of MDR services. Alongside these services, there are often a wide array of nonrepeatable security assessments and security technology implementation offerings that are delivered in a complementary or supporting way to enable or enhance the services. Although these are common, they cannot be effectively compared due to their individuality on a client-by-client basis and variance across the providers.

The MSS market has shifted away from providers that had expertise in delivering and maintaining security technologies or simply detect and alert customers about threats (“throwing alerts over the wall”) with little or no context. Now, the market features a set of providers that deliver security insights and interpret security requirements so as to prioritize and focus a buyer on security issues that have direct risk impacts to that organization (see The Managed Security Services Landscape Is Changing). This is delivered across detection of threats and exposures, response to mitigate those threats in-flight and technology enablers to provide adequate visibility and reach to prevent the escalation of security threats and issues and reduce risk for that buyer organization.

MSS providers that have a wide portfolio of services (see Figure 1) often target larger enterprises that have an accumulation of requirements, both customized and standard, and require significant implementation efforts and sometimes dedicated technology. These wider, more complex engagement types make MSS services hard to compare, as no two are identical (see Toolkit: RFP for Managed Security Services).

The main advantage of utilizing MSS for many buyers is the flexibility to utilize existing security technology investments and accelerate the operational effectiveness of those technologies. Where technology is a focus, providers are often more engaged in onboarding those technology types, and this can extend the cycle time for deploying a service and getting it to its full operational capability. When this is compared with curated or proprietary technologies used to deliver MDR services, for instance, this
can be significant. However, the compatibility with a wide range of technologies can be seen as advantageous to organizations that cannot or will not introduce or change their existing security technology stack.

Figure 1: Managed Security Portfolio of Services

Managed Security Portfolio of Services

Managed security services are characterized by the following attributes:

- Remote 24/7 monitoring of security events and security-related data sources through:
  - Providing and operating technologies to detect, identify, investigate and respond to threats and threat exposure, delivered from a centrally managed platform and in a globally consistent format.
  - Offering remote response options that may include guidance around proactive containment and the reduction of risks associated with active threats.
  - Retaining expertise in the analysis and resolution of threats as well as specific technology focused knowledge for the configuration and customization of security technologies being managed.
Consultative engagements that:

- Complement or inform the delivery of a subscription-based security service. Such engagements are sometimes delivered as a preassessment for gathering service requirements or as part of technology implementation to enable services.
- Deliver call-off consultancy to assist with complex incident response functions to deliver forensic detail following a severe security incident.
- Design and build SOC processes and tooling against customized requirements that cannot be delivered remotely or in line with industry standards.
- Provide named resources, remote or on-site, to act as an extension of the internal team.
- Address security technology changes and design/management security configuration and integrations.

Maintain security technologies in the form of:

- SaaS and/or cloud-based security technologies, such as SIEM platforms.
- On-premises security technologies and services that offer shared responsibility for operational delivery of an SOC capability, such as co-managed SIEM (see Toolkit: Managed SIEM RFP).
- Management of response-enabling technologies directly in support of monitoring services such as EDR, managed firewalls or intrusion prevention systems (IPS).

Market Direction

The MSS market revenue continued to grow year over year and reached 7.5% in 2019 (see Market Share: Managed Security Services, Worldwide, 2019).

Choosing an MSS provider is difficult for end users because many providers offer a large and disparate array of services. This is often coupled with network services and security consultancy, for example. Some of the most prevalent providers in this market have dominant shares in other markets, such as network connectivity, ITO, consulting and system integration. There is considerable crossover with areas such as MDR with MSS providers shifting or adding to their offerings to better align with the characteristics of MDR in order to compete within this high-growth part of the marketplace.

There are key commonalities within modern MSS portfolios. These are manifesting as a split between technology-driven and operational service. At the center of the MSS market are threat detection and response services. These identify, explain and react to security incidents through the detection and investigation process, providing mitigation through recommendations and sometimes remote response actions. Linking security exposure in the form of vulnerability identification is becoming a more common accompanying service and helps to contextualize, provide prioritization and make recommendations more preventative. Threat detection and response services are delivered in various different formats.
These include the provider hosting, managing and configuring the technology; offering a SaaS platform on which the client can operate their own operations; and a fully managed combination of integrated platforms aligning with a buyer’s need for outcome-driven visibility and risk-driven threat response.

MSS buyers must focus on the deliverables and outcomes rather than the delivery mechanism, and they are risk-driven rather than technology-driven in their requirement setting.

MSS providers are increasingly competing with more turnkey offerings from pure-play MDR providers that are widening their capability to include and capitalize on some of the traditional MSS market in areas such as vulnerability management (VM) and log management. In response, MSS providers have been adding MDR services to their already extensive portfolios, often through acquisition of other service providers or technologies in adjacent or overlapping markets (see Protect Yourself as Your MDR Is Merged or Acquired).

ITOs, SIs, network service providers and a wider range of consultancy firms now widely offer what would have traditionally been called managed security but is now simply defined as managing security technologies. These services offer a form of security technology implementation and technology maintenance-wrapped professional services. Because of the accessibility of security technology and the growth in providers able to facilitate the delivery of services wrapped over such technology, there has been a shift in what represents an MSS.

MSS is 60% process, 30% people and 10% technology. Engaging an MSSP will require the right internal staffing levels and additional processes to account for the security operations and life cycle.

Market Analysis
Buyer Focus on Threat Detection and Response
Central to all MSS portfolios are threat detection and response services. This is because most buyers focus on the awareness and resolution of threats following investment in preventative technologies such as IDS, firewalls or endpoint protection solutions. Detection and response services are delivered in several different formats, utilizing a variety of different technologies as their central capability:

- Centrally delivered technology, curated by the provider — This is a collection of third-party and proprietary tech integrated together to deliver a service. The focus is sometimes on consuming the
outcomes from as much of the existing technology that the buyer has presently to create a more complex but integrated solution. The focus could also be on introducing new technologies to collect data and enable remote response actions in areas such as endpoints or through CASB on cloud platforms. In this format, the service is delivered centrally, often within the provider’s own data center infrastructure, and is often a shared platform that services a large number of customers. This requires it to have large capacity for data ingestion and a wide array of compatibility with other security technology solutions. The benefit to the buyer in this method is that content and processes are already established and, therefore, the services can be quicker to deploy and deliver. Centrally shared platforms also mean that buyers benefit from the learnings of the providers, other customers and a continuous development model that can be widely tested in a multitude of scenarios. As with all centrally delivered, multitenant services, the limitations mean that the development of the service is focused on a crowd approach, meaning much fewer custom functions for individual businesses.

- **Proprietary technologies developed by the provider** — A few providers have invested in the development of or purchased a single detection technology to operate a core service on. These services are often known as MDR (see *Midsize Enterprises Should Embrace MDR Providers*), but they are still delivered by MSS providers. Services of this type use a limited set of technologies to deliver fixed format services and often involve the buyer having to introduce new technologies such as EDR to their environments. With a focus on delivered outcomes, these proprietary technology-driven services offer little or no customization, but they do support incident response functions that allow providers to mitigate threats easily on behalf of the buyer.

- **Managed detection technology** — Deployed and operated for the benefit of a single customer, managed detection technologies such as SIEM or EDR provide an overlay, often simply maintaining the health and well-being of the chosen platform. Buyers that focus on these types of services have adequate internal staff with the correct levels of skills to operate these technologies and interpret the outcomes they deliver. Sometimes these services can be delivered in a co-managed capacity, whereby a provider and the internal staff share responsibility for the content development and the operation of such platforms, often on an off-hour basis. This also happens across separate analyst tiers where initial triage is carried out by the provider and more in-depth investigation is handled internally.

- **Cloud-based detection technology** — Services such as SaaS/cloud-based SIEM are gaining traction in the market as they remove the burden of maintaining a security technology and provide a flexible scaling capability. However, such services are more SaaS than managed security, providing a capability much like those outlined in the bullet above on “managed detection technology” (see *Questions to Answer Before Adopting Cloud SIEM Solutions*).

- **On-site staff augmentation functions** — Less and less like a managed service, some providers offer an “SOC in a box” or a “buy and build” capability where they will bring tried and tested procedures and technologies, implement them in line with a buyer’s needs, and then staff them for a number of years until the buyer can self-sustain a capability internally. These types of services are more aligned to consultancy and, while they are seen regularly, especially in the Middle East, they frequently do not fit the managed service definition, as they are individual in each engagement.
MSSPs focus on three areas that allow them to deliver their services to customers:

- **Delivery platform** — Providers offer a curated and preconfigured security toolset or platform in a centralized location for use by the buyer (rented to the buyer). It often includes the development of content for that platform either at the initial stages of the engagement or as part of regular upgrades. Services that center around this core delivery platform can be considered SaaS services or co-managed services, depending on the level of operations that the provider is offering.

- **Technology management and maintenance** — While not a dominant function for MSS consumers, the management and maintenance of security technology enables providers to carry out response actions across a wide variety of technologies on behalf of the buyer. It is a hidden but key feature of delivering a security service on a dedicated technology or providing visibility in areas where a buyer has no existing technologies.

- **Security operations** — Arguably the centerpiece of security services, security operations is the combination of people and processes that layer over the provider’s and the buyer’s technology stack to deliver the outcomes they require to reduce risk and increase threat awareness. The operations function identifies, investigates, validates, advises on remedial action and, where possible, responds to high-fidelity security detections and incidents on behalf of buyers.

No two managed security services are identical, but there are areas and functions that are delivered consistently. The volume and combinations of the functions these services offer is dictated by drivers in the buyer organization, such as:

- Lack of staff or expertise in areas of security technology implementation, configuration and operations. MSS exists primarily to connect buyers with skilled individuals who can interpret operational security information and provide advice or reaction. By grafting this capability into their own organization through a managed service, a buyer can increase their security maturity quickly, with a relatively small investment. Staffing a security function requires experience in areas most organizations are not primarily focused on. Retaining security staff is also difficult, as engagement and security activity is scarce in a single business environment. MSS organizations provide a much wider variety of security issues and incidents for individuals to maintain their interest.

- Lack of time to deliver a capability or a need against a risk-based requirement. For most organizations, security is an afterthought, but in today’s climate it’s something that needs a swift resolution. The goal of MSS is to provide fast and effective deployment of technologies, processes, and specific skill sets without the need for a lengthy development process. While more complex MSS engagements can take a number of months to get established, more turnkey approaches such as MDR have begun to dominate the market and can be part of a wider set of requirements with the intent of delivering a limited capability in very short order.

While combating issues such as time to value and gaps in skill sets, these services do require investment from the buyer. Providers focus on the security problem, and buyers then must bring the risk-based
requirements and priority needs of the organization. They must prepare to consume the output of services and not simply attempt to shift responsibility to the service providers, expecting them to know what is the right resolution for their organization. They must also recognize that services must evolve over time to stay current with the organization's up-to-date risks (see Get the Foundational Elements Right When Selecting a Detection and Response Service Provider).

MSSs attract different buyer types. The wide range of services, delivery models and other affiliated core market services can contribute to this, but buyers typically align with the functional areas already outlined:

- Buyers that purchase security alongside other services such as network services or as a result of a consultative engagement.
- Buyers looking to outsource the management of security technologies and capabilities because they don't fit with the company's architectural plans (such as cloud migration).
- Security greenfield organizations looking to achieve a capability in security to satisfy a compliance requirement or as a result of a serious breach.
- Buyers who are looking to reduce their cost burden by outsourcing security rather than hiring staff and buying technology.
- Buyers that have an established security operations capability but are looking to outsource the more generic security issues and problems as well as the volume of work that comes with these.
- Buyers looking to learn from or take over from a security services company in the long term but need to establish a capability quickly and see MSS and the quickest and most efficient way of gaining capability and processes.
- Buyers that have invested in security technology and realize staffing and operating it is harder than they first thought.

**Diversity of MSS Portfolios and the Commoditization of Security Technology Management**

As security technology vendors have begun to offer their technologies “as a service” and as they have generally become easier to operate and maintain, there has been a commoditization of some of the key functions Gartner previously associated with MSS providers. These predominantly exist in the security technology management space.

While many of the largest and most prevalent security services firms still offer the specialist management of security technologies, it is true that these capabilities have also, at a large scale, bled into other areas of the IT market. This is especially true regarding nonsecurity specialist network service providers, telecommunications firms and IT outsourcing. Terms such as “managed firewall” and “managed endpoint” are commonplace in the portfolios of nonsecurity specialist companies.
Furthermore, the diversification and increase in volume of both technology types and new technology vendors has complexified security service vendor portfolios with an array of “managed <insert security vendor name here>.”

Some security technologies have survived this commoditization and are still far too complex for nonsecurity service providers to offer competent services for, typically in areas such as application security container security and cloud workload protection. As predominantly preventative technologies, the services in this area survive not only because of the understanding required to implement and run them correctly, but also because of the fast pace of technological change. This means that services wrapped over these technologies require regular manual analysis and complex changes to be carried out in line with what is often a business-critical operational need.

Left- and right-of-center capabilities in areas such as vulnerability management can also be delivered by nonsecurity specialist companies, often those focused on patch management. When delivered in isolation like this, such services do not represent a great deal of directional operational security value. Many MSS providers are choosing to bolt such functions around a central threat detection and response capability, making them more able to prioritize and manage risk for the buyer. Some of the more proactive service providers in the MSS market are beginning to offer a combination of vulnerability identification with threat identification and provide a more prioritized vulnerability assessment while being more preventative with their advice following an active threat identification.

Incident response is another area of security services that provide organizations with skill sets that they can graft directly into their organizations. As legal and compliance requirements grow and place more responsibility with your organization, it is more critical than ever that there is some facility to provide deep understanding of the circumstances or the technical impact of a security incident. These services are traditionally offered alongside threat detection and response-driven functions but are also regularly offered by independent consultancy firms and through relationships with cyber insurers. There are benefits from having incident response embedded with your current MSS provider. These include the speed of identification and the prework that can be done to contextualize an incident (see Market Guide for Digital Forensics and Incident Response Services). There are also benefits to independent contractors who should be considered on the basis of cost or the relationship they have with accreditable standards in the industry, such as CREST.

Security Services Are Consumable

For most buyers, security services represent a part of their requirements that they either have a low level of understanding of or have a lack of time to achieve. They then forget that security services are a consumable and approach them more like a solution or an implementation. The value of an MSS is directly aligned to the buying organization’s ability to consume what it delivers, and the value gained from that consumption is related to how relevant the outcome is for the risk reduction of the organization.
The MSS market has been adjusting over the past few years to be more driven by customer engagement. We have seen this through the gradual evolution of dashboarding and customer portals as well as wider traction with chat functions and technologies that engage the end user directly with the team providing the service. MSS is often referred to as an “extension of your security team.” As security services become more integrated with organizations, there is more demand for response actions to be carried out remotely for tying integrations directly into workflows already in use by teams across our businesses.

A modern MSS provider communicates in ways that help organizations understand how they can consume the service provided. The benefits rarely include more security or more technology, but they create efficiency and speed within our ability to deal with security issues that arise.

The MSS Market Saw Minor Acquisition Activity

During the past 12 months, there have been few major acquisitions in this market:

- January 2020 — Accenture acquires Symantec
- March 2020 — Accenture acquires Context
- April 2020 — Accenture acquires Revolutionary Security
- June 2020 — Atos acquires Paladion
- July 2020 — Herjavec Group acquires Securience
- September 2020 — Secureworks acquires Delve

Representative Vendors

Market Introduction

A list of representative vendors is provided in Tables 1, 2 and 3. These lists are grouped by security pure-play vendors, network services or telecommunications providers, and system integration (SI), IT outsource (ITO) and consultancy firms. While all types of MSS providers offer services in line with the market description, associated offerings, such as network connectivity, technology provisioning or consultative functions, can vary between providers. Buyers should consider secondary projects and requirements and select an appropriate type of provider based on a range of criteria.
## Table 1: Representative Security Pure-Play Vendors

Viewing partial table. Click here to view full table

<table>
<thead>
<tr>
<th>Provider</th>
<th>Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ackcent</td>
<td>Barcelona, Spain</td>
</tr>
<tr>
<td>Alert Logic</td>
<td>Houston, Texas, U.S.</td>
</tr>
<tr>
<td>Arctic Wolf</td>
<td>Eden Prairie, Minnesota, U.S.</td>
</tr>
<tr>
<td>BlueVoyant</td>
<td>New York, New York, U.S.</td>
</tr>
<tr>
<td>Cysiv</td>
<td>Dallas, Texas, U.S.</td>
</tr>
<tr>
<td>eSentire</td>
<td>Cambridge, Ontario</td>
</tr>
<tr>
<td>F-Secure</td>
<td>Helsinki, Finland</td>
</tr>
<tr>
<td>Herjavec Group</td>
<td>Toronto, Canada</td>
</tr>
<tr>
<td>IBM Security</td>
<td>Cambridge, Massachusetts, U.S.</td>
</tr>
<tr>
<td>Integrity360</td>
<td>Dublin, Ireland</td>
</tr>
</tbody>
</table>

Source: Gartner (December 2020)
Table 2: Representative Network Services/Telecommunications Vendors
Viewing partial table. Click here to view full table

<table>
<thead>
<tr>
<th>Provider</th>
<th>Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T Cybersecurity</td>
<td>San Mateo, California, U.S.</td>
</tr>
<tr>
<td>BT Security</td>
<td>London, U.K.</td>
</tr>
<tr>
<td>Etisalat</td>
<td>Abu Dhabi, United Arab Emirates</td>
</tr>
<tr>
<td>Lumen (Formerly CenturyLink)</td>
<td>Monroe, Louisiana, U.S.</td>
</tr>
<tr>
<td>Masergy</td>
<td>Plano, Texas, U.S.</td>
</tr>
<tr>
<td>NTT Security</td>
<td>Ismaning, Germany</td>
</tr>
<tr>
<td>Orange Cyberdefense</td>
<td>Paris, France</td>
</tr>
<tr>
<td>T-Systems</td>
<td>Frankfurt, Germany</td>
</tr>
<tr>
<td>Telefonica</td>
<td>Madrid, Spain</td>
</tr>
<tr>
<td>Telstra Enterprise</td>
<td>Melbourne, Australia</td>
</tr>
</tbody>
</table>

Source: Gartner (December 2020)
Table 3: Representative SI, ITO and Consultancy Firm Vendors

<table>
<thead>
<tr>
<th>Provider</th>
<th>Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atos</td>
<td>Bezons, France</td>
</tr>
<tr>
<td>Capgemini</td>
<td>Paris, France</td>
</tr>
<tr>
<td>Deloitte</td>
<td>London, U.K.</td>
</tr>
<tr>
<td>DXC Technology</td>
<td>Tysons, Virginia, U.S.</td>
</tr>
<tr>
<td>EY</td>
<td>London, U.K.</td>
</tr>
<tr>
<td>Fujitsu</td>
<td>Tokyo, Japan</td>
</tr>
<tr>
<td>Infosys</td>
<td>Bengaluru, India</td>
</tr>
<tr>
<td>TCS</td>
<td>Mumbai, India</td>
</tr>
<tr>
<td>Wipro</td>
<td>Bengaluru, India</td>
</tr>
</tbody>
</table>

Source: Gartner (December 2020)

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Recommendations

Security and risk management leaders responsible for security operations should:

- Clearly understand what MSS providers require, for what purpose and how they will effectively consume the outcomes of these services before embarking on a procurement journey. MSS providers offer a broad range of services, which are often presented in an overly complex manner.

- Separate preservice assessment and consultancy from service delivery to ensure the organization can effectively control cost. While there is no conflict in using the same provider for both, the process by which they are acquired and requirements aligned with service scope must be separated.
Plan how they will respond to significant issues in a business-focused way. Effective security incident response planning is still required should an organization choose to procure a managed security service, and while providers can offer valuable context in regard to security issues, there is not commonly a solution or service that crosses between security and business risk.

Separate architectural requirements and compliance requirements from risk-based requirements for security. Buyers must be focused on what is being delivered, not how it is being delivered. Prefilter potential providers based on their ability to meet architectural- and compliance-based constraints prior to analysis for capability and scoped security requirements.

Utilize and integrate existing engagements with partners in the network or IT outsourcing space, where available, to ensure a fluid resolution to issues identified by a security service. While they don’t necessarily have to be the same partner, it is helpful to understand how they can work together directly to provide a more comprehensive and efficient service.

Note 1: Representative Vendor Selection
Gartner has included a range of providers in this research to ensure coverage from a geographical, vertical and capabilities perspective. Gartner estimates that more than 500 providers in this market claim to offer MSS services. Listed here are those that are visible to Gartner clients based on inquiries, have core capabilities that represent the central requirements seen from buyers in the MSS market, and represent variety in both global distribution and size.

Document Revision History
Magic Quadrant for Managed Security Services, Worldwide - 2 May 2019
Magic Quadrant for Managed Security Services, Worldwide - 27 February 2018
Magic Quadrant for Managed Security Services, Worldwide - 26 January 2017
Magic Quadrant for Managed Security Services, Worldwide - 23 December 2015
Magic Quadrant for Managed Security Services, Worldwide - 30 December 2014
Magic Quadrant for Global MSSPs - 26 February 2014
Magic Quadrant for MSSPs, North America - 15 November 2012
Magic Quadrant for MSSPs, North America - 28 November 2011
Magic Quadrant for MSSPs, North America - 29 November 2010
Magic Quadrant for MSSPs, North America - 16 April 2009
Magic Quadrant for MSSPs, North America, 1H07 - 1 August 2007
Magic Quadrant for MSSPs, North America, 2H05 - 30 December 2005

Recommended by the Authors
Toolkit: RFP for Managed Security Services
Market Guide for Managed Detection and Response Services
Toolkit: Managed SIEM RFP
Market Share: Managed Security Services, Worldwide, 2019
Protect Yourself as Your MDR Is Merged or Acquired
The Managed Security Services Landscape Is Changing
Get the Foundational Elements Right When Selecting a Detection and Response Service Provider
Midsize Enterprises Should Embrace MDR Providers
Questions to Answer Before Adopting Cloud SIEM Solutions
Market Guide for Digital Forensics and Incident Response Services

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. It consists of the opinions of Gartner’s research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."