Magic Quadrant for Managed Security Services, Worldwide

23 December 2015 | ID:G00273932

Analyst(s): Kelly M. Kavanagh, Toby Bussa

Summary

Security managers should evaluate MSSPs for enterprise scale operations, multinational and local presence, and effective threat management and compliance capabilities. Use this Magic Quadrant to evaluate MSSPs to support global service requirements, regional presence and leading-edge services.

Market Definition/Description

For the purposes of this research, Gartner defines managed security services (MSSs) as "the remote monitoring or management of IT security functions delivered via shared services from remote security operations centers (SOCs), not through personnel on-site." Therefore, MSSs do not include staff augmentation, or any consulting or development and integration services.

MSSs broadly include:

- Monitored or managed firewalls or intrusion prevention systems (IPSs)
- Monitored or managed intrusion detection systems (IDSs)
- Monitored or managed multifunction firewalls, or unified threat management (UTM) technology
- Managed or monitored security gateways for messaging or Web traffic
- Security analysis and reporting of events collected from IT infrastructure logs
- Reporting associated with monitored/managed devices and incident response
- Managed vulnerability scanning of networks, servers, databases or applications
- Distributed denial of service (DDoS) protection
- Monitoring or management of customer-deployed security information and event management (SIEM) technologies
- Monitoring and/or management of advanced threat defense technologies, or the provision of those capabilities as a service

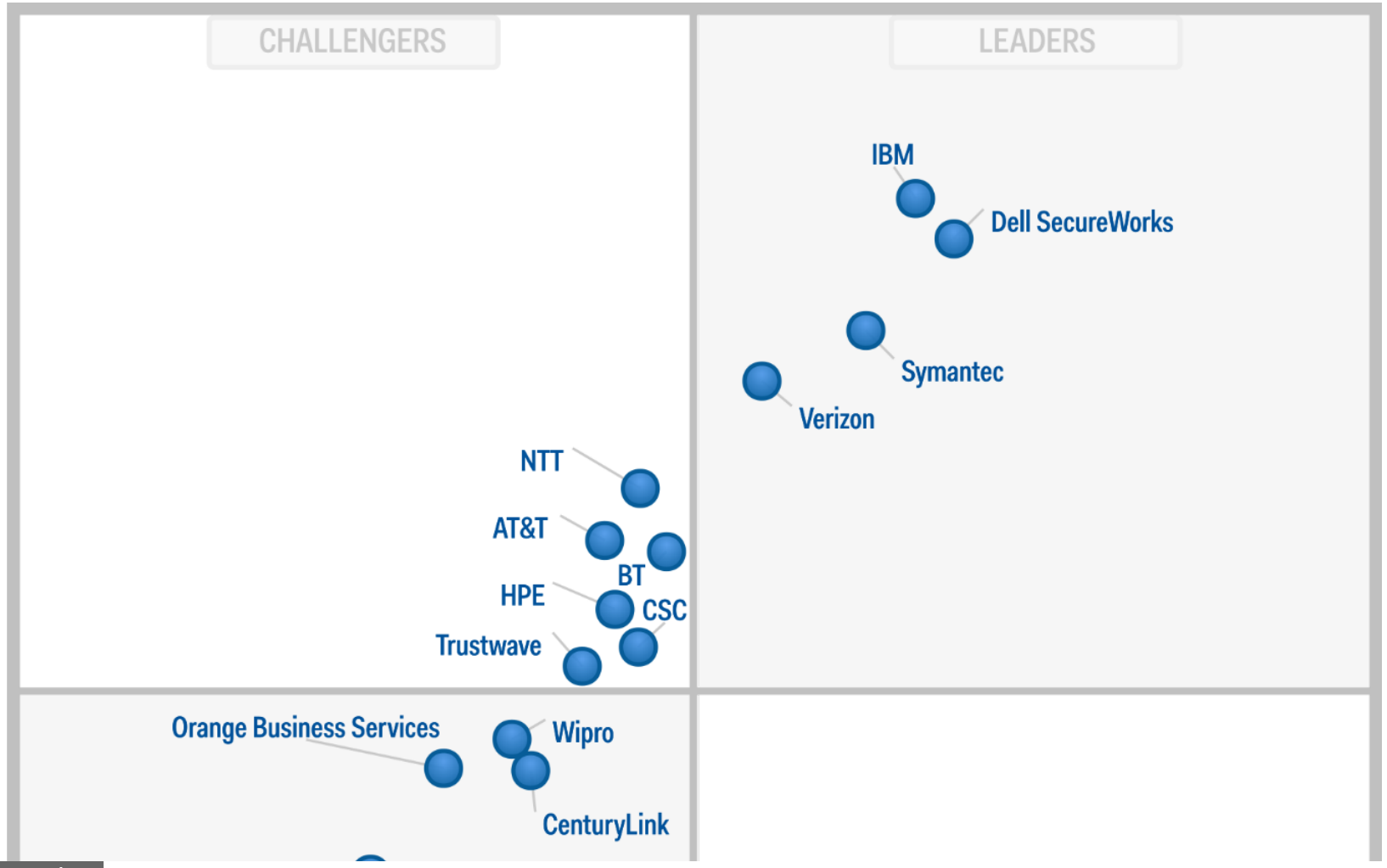
This Magic Quadrant evaluates services for monitored/managed firewall and intrusion detection and prevention functions, as well as log analysis and reporting services. These functions make up the core of MSS procurements. Chief information security officers (CISOs) and security directors seeking MSS providers (MSSPs) able to support global service delivery should use this Magic Quadrant to identify providers positioned to meet their requirements.

There are no vendors appearing in the Visionaries quadrant of this Magic Quadrant. MSS is a mature market with a core set of services that appear in most MSS engagements. As described in the Vendor Strengths and Cautions section, several MSSPs have introduced, or will introduce shortly, services to detect advanced targeted

attacks, using commercial technologies or their own. These are advanced services, but the vendors that are introducing them have strong capabilities reflected in the Ability to Execute criteria, and thus do not appear in the Visionaries quadrant. In addition, there are other service firms that have introduced similar capabilities, but do not yet have the scale to be included in this Magic Quadrant.

Magic Quadrant

Figure 1. Magic Quadrant for Managed Security Services, Worldwide



Source: Gartner (December 2015)

Vendor Strengths and Cautions

AT&T

AT&T offers a range of security monitoring and management services, in addition to other telecommunications (wired and wireless) and IT services, for business customers ranging from large enterprises to small or midsize businesses (SMBs) to governments. Headquartered in the U.S. (Dallas), and with regional offices in the U.K. (London) and Hong Kong, AT&T delivers services from eight SOCs — including three U.S.-based operating 24/7, and two in the Asia/Pacific region, one in Brazil and one in Europe operating on local business hours. Customers served by a SOC operating local business hours and seeking support after hours are routed to a 24/7 location with full language support. AT&T's enterprise-grade threat offering is the Security and Threat Analysis (SETA) service, which includes correlation and analysis of network flow data from customers' devices and the AT&T network, with customer-specific configuration and response templates. For other customers,

AT&T provides 24/7 security event monitoring and alerting via AT&T Threat Manager with Advanced Log Management, delivered by Security On-Demand (SOD). Device management is via the AT&T Security Device Management offering (part of the Security Analysis and Consulting Solution). Firewall Security Services, Intrusion Detection and Prevention Services, and Proxy Services are all offered as discrete managed services. Device management and workflow is handled through the AT&T BusinessDirect portal. Security-related monitoring and incident management is handled through the AT&T Security Portal. AT&T offers threat intelligence via the AT&T Internet Protect service, which monitors its Internet Protocol (IP) backbone for attacks. AT&T leverages big data analytics and behavioral analytics in its other offerings, and has plans to integrate these offerings for threat analytics. Where necessary, AT&T supports in-country data management and can use local partners for device management to meet data residency requirements. AT&T should be considered by organizations where global services need to be sourced from a single supplier, especially network services where network security controls need to be deployed, managed and monitored both on the customer's and provider's premises. Existing AT&T customers should also consider AT&T's portfolio of MSS offerings.

AT&T moves from the Leaders quadrant to the Challengers quadrant in 2015 due to continued use of partners to deliver threat management and advanced log management, while competitors improved their internal capabilities to deliver these functions.

STRENGTHS

- AT&T's network-based security offers mature security management and monitoring that are attractive to MSS customers with remote and branch office coverage requirements, and security service requirements for email, mobile, Web application and DDoS protection.
- AT&T is a mature and stable service provider, with delivery capabilities in multiple geographic regions.
- The vendor centralized all security-focused teams supporting its Network Security offering, which should improve service coordination and delivery for customers of MSSs.

CAUTIONS

- Potential MSS customers should validate that AT&T's use of service delivery partners for log management and for security event and threat monitoring will meet their requirements for vendor management, service levels and service continuity.
- AT&T MSS customers using both device management and security monitoring services are required to use separate portals for related activities. AT&T plans to unify these in early 2016, initially focusing on an integration of all Network Security offerings into a single portal.
- The vendor provides 24/7 support for threat monitoring/management, but this service is available only from U.S.-based SOCs.
- AT&T is only occasionally mentioned by Gartner clients for consideration as an MSSP.

BAE Systems

BAE Systems, headquartered in Farnborough, U.K., offers national defense products and services to industry and governments. The MSS group is headquartered in Guildford, U.K., with offices in Boston, Sydney, Dubai and Singapore. In December 2014, BAE Systems acquired U.S.-based SilverSky, a provider of MSS and email security services. In addition to the SMB-oriented services acquired via SilverSky, MSS offerings are delivered using four 24/7 SOCs — one in the U.K., two U.S.-based and one in the Philippines. BAE Systems delivers its MSS offering using a mixture of proprietary and commercial solutions, depending on the customer's region. The vendor offers advanced threat detection services to large enterprise customers. The majority of its MSS customers are in the U.S., and their large enterprise customers in Europe utilize the company's advanced threat detection services in addition to network monitoring, and most of its advanced threat defense customers are in the U.K. BAE Systems can meet buyer requirements for data residency with in-region/in-country data collection and retention options. Companies in the financial services, retail, healthcare, energy and defense markets that need a mix of UTM device management and monitoring, with the potential for increased protection via

advanced threat detection and analytics, should consider BAE Systems.

BAE Systems is in the Niche Players quadrant based on its continuing work to complete the integration of the SilverSky acquisition into its managed security service portfolio and on the limited scope of its MSS footprint, notably in the Asia/Pacific region.

STRENGTHS

- BAE Systems has the security intelligence technology infrastructure to support targeted advanced threat detection services based on advanced analytics.
- The large MSS customer base acquired via SilverSky should benefit from operational integration of BAE System's threat intelligence research.
- BAE Systems is an experienced defense contractor that has developed tradecraft for addressing advanced targeted attacks, which influences its advanced threat detection and threat intelligence offerings. Customers indicate that detection of advanced targeted attacks was a primary consideration for selecting BAE Systems.

CAUTIONS

- BAE Systems' Advanced Threat Detection services and MSS services are distinct offerings with different buyers. The vendor has not integrated these two offerings, and they are each mostly present in distinct regions.
- The BAE MSS portal lacks the mature customization, presentation and reporting capabilities found in competitors' portals. There is no support for advanced threat detection services in the MSS portal. The vendor has a roadmap to address portal enhancements.
- BAE MSS customers span very large enterprises with advanced requirements and very small businesses with very basic requirements. The vendor will be challenged to develop MSS offerings and the associated sales and delivery mechanisms that can scale to both types of buyers.

- BAE Systems is not mentioned in MSS vendor shortlist discussions with Gartner clients.

BT

BT is headquartered in London, with offices around the world, including a regional presence for MSS in London, Hong Kong and Irving, Texas. BT's MSS offerings are composed of monitoring and management of customer-premises-deployed devices and network-based security controls as part of its larger portfolio of telecommunications and IT services. BT has three European SOCs, one North American SOC and three Asia/Pacific SOCs staffed 24/7, with an additional eight SOCs worldwide. The vendor uses a proprietary platform to deliver network-focused security monitoring (Assure Threat Monitoring). Other commercial tools are used to deliver workflow and device management. BT's Assure Analytics capability offers advanced threat analytics and visualization. Assure Threat Defence and Assure Threat Intelligence are global offerings that focus on detecting advanced targeted and persistent threats. Additional big-data-based analytics support the Assure Threat Monitoring service. BT offers managed firewalls and network intrusion detection/prevention, in addition to vulnerability scanning, DDoS and cloud-based security for Web traffic. A single MSS portal is used by customers and BT staff. BT can meet requirements for data residency with in-region/in-country service provision and citizenship requirements for SOC staff. Customers of other BT services, and enterprises seeking global MSS delivery as well as additional threat intelligence, analytics and visualization capabilities, should consider BT.

BT's placement in the Challengers quadrant reflects both the strength of its global capabilities and the lack of visibility for MSS among buyers, especially in North America.

STRENGTHS

- All MSS and security services are integrated under the BT Assure business, providing a single source for managed security and other security service offerings for enterprises seeking broad capabilities in a single provider.

- BT has numerous partnerships with security technology vendors to deliver its device management, security monitoring and threat intelligence offerings.
- The vendor has developed a strong threat intelligence capability, and provides threat hunting as a component of its MSS.
- BT customers give good marks for its understanding of their security requirements and for the security expertise of BT's MSS operations staff.

CAUTIONS

- BT's portal is focused on features for technical security staff. Customized dashboards and content are only available to customers of the Assure Cyber services.
- BT's offerings for monitoring hosts and the application layer have a strong bias toward network security controls. Buyers that require host-level security monitoring are limited to Web traffic monitoring, as there is currently no endpoint detection and response (EDR)-based service offering.
- BT has lower visibility among MSS buyers in North America and the Asia/Pacific region than in Europe.

CenturyLink

CenturyLink is based in Monroe, Louisiana, and has offices in Hong Kong, London and North America. It provides managed security services as well as telecommunications, public and private cloud services, and colocation to small, midsize and enterprise-level customers. MSS customers have primarily been customers of CenturyLink's infrastructure services. MSS is delivered through a combination of commercial and proprietary technologies. The vendor has four 24/7 SOCs operating in North America, and one in Europe and one in the Asia/Pacific region that operate on a "follow the sun" model, with plans to expand to 24/7 in 2016. There are dedicated North American SOCs to support U.S. government contracts. Support for targeted attack detection via network forensics, payload analysis, and endpoint behavior and forensics is available through CenturyLink

Professional Security Consulting Services. CenturyLink acquired Cognilytics in December 2014, which provides big data and predictive analytics that will be adapted to enhance CenturyLink's advanced threat detection capabilities. CenturyLink can limit access to customer systems based on the location of SOC staff, and can store data in-region to support some residency requirements. The vendor's network services, infrastructure as a service (IaaS) and cloud service customers should consider the CenturyLink for MSSs.

CenturyLink delivers most of its MSS capabilities to customers of its other services, and has very limited visibility for MSS in North America and less outside that region; thus, it appears in the Niche Players quadrant.

STRENGTHS

- CenturyLink's enterprise and SMB customers for network, cloud and platform services can augment their relationships with CenturyLink via MSSs.
- CenturyLink's rationalization of security services across its lines of business has enabled a more focused and consistent delivery of MSSs.
- Customers give good marks for CenturyLink's delivery of MSSs.

CAUTIONS

- CenturyLink trails competitors in support for advanced threat detection and threat intelligence capabilities. Offerings to support these are planned, but not yet available.
- CenturyLink's MSS portal lags behind those of other MSS providers. A major update is planned for release in 1Q16.
- The vendor's 24/7 SOC services are only available from a U.S.-based SOC. Customers in other regions with requirements for local 24/7 SOC support must request custom services until CenturyLink upgrades availability in 2016.

- CenturyLink rarely appears on Gartner clients' shortlists for MSSs.

CSC

CSC has its headquarters in Falls Church, Virginia, with regional offices in Aldershot, U.K., Singapore and Sydney. MSS is part of CSC's cybersecurity services, which complement CSC's IT services aimed at enterprise and government customers. CSC uses commercial SIEM technology for security event collection and correlation, real-time alert generation, and log management. Customers can opt for dedicated SIEM instances to meet various regulatory or client concerns. Services are delivered from nine 24/7 SOCs, with four located in the U.S., two located in the U.K., and three located across the Asia/Pacific region. CSC's Pulse Portal is leveraged across all SOCs to provide customers access to MSS alerts, reports and tickets using a common workflow. Advanced threat detection services are delivered using Trend Micro's Deep Discovery suite to support payload and network analysis, and network and endpoint forensics, supported by CSC's Global Threat Intelligence. CSC plans to expand its big data analytics, advanced threat detection and global threat intelligence offerings in 2016. Data residency and privacy concerns are addressed through local log collection, reporting options and SOC staffing. CSC outsourcing customers, hybrid cloud customers, cloud IaaS customers and enterprises — especially those in the international public sector, healthcare and financial services industries — should consider CSC for MSSs.

CSC is in the Challengers quadrant due to the strength of its security services in specific verticals and the challenges it faces in selling managed security services as a stand-alone offering beyond its existing IT services customer base.

STRENGTHS

- CSC offers extensive MSSs for its cloud IaaS offerings and security monitoring options, with flexible pricing models for most offerings.
- Customers give generally good marks to the security expertise of CSC's MSS staff.

- CSC's security expertise supports its strong presence in the international public sector, in financial services, and in critical infrastructure markets. Government clients are serviced by the Computer Sciences Government Services (CSGov) group, and security capabilities among commercial and government groups are expected to be shared for the near term.

CAUTIONS

- CSC's Network Defense Analysis service, a correlation/alerting/visualization capability based on big data analytics, is available only to customers that share their security data among a consortium of other customers.
- CSC is rarely included on Gartner commercial clients' shortlists for stand-alone MSS deals.

Dell SecureWorks

Dell is headquartered in Round Rock, Texas, and Dell SecureWorks is headquartered in Atlanta, with five offices in the U.S., plus Edinburgh, Scotland, London and Tokyo, and with additional offices in the Asia/Pacific region and Europe. In November 2015, Dell announced its intention to acquire EMC. Dell SecureWorks offers a full suite of MSSs as well as security consulting, incident response and threat intelligence services. MSS delivery is based largely on its self-developed Counter Threat Platform technology, with commercial products used for endpoint monitoring and log retention services on the customer's premises. The Dell SecureWorks Counter Threat Unit research team provides threat intelligence, malware analysis and analytics support for MSS operations, in collaboration with incident response and risk consulting teams. Three SOCs are located in the U.S., with additional SOCs in the U.K. and Japan and a "Center of Excellence" based in Romania. Access to customer data can be restricted to Dell SecureWorks employees in specific regions to support data privacy requirements. Network advanced attack detection and protection services are offered in the Advanced Threat Services portfolio. Advanced endpoint threat detection and forensic services using Bit9 + Carbon Black are available globally. Small and midsize organizations that want to meet compliance requirements, and

enterprises looking for full-featured MSSs, should consider Dell SecureWorks.

Dell SecureWorks is in the Leaders quadrant due to the strength of its MSS offerings, the quality of its service delivery and its high visibility among MSS buyers.

STRENGTHS

- Dell SecureWorks is almost always included in competitive MSS deals by customers ranging in size from small to large enterprise and global buyers based in North America, and has good visibility with European customers.
- Gartner customers regularly offer positive feedback for Dell SecureWorks' MSS delivery, security expertise and relationship management.
- Customers report that Dell's sales efforts result in responsive, comprehensive and easy-to-assess proposals for services.
- The SecureWorks MSS portal offers extensive access to event data, supporting context, threat intelligence and reporting.

CAUTIONS

- Dell SecureWorks continues to mature in Asia/Pacific markets, but is challenged due to less visibility than in other geographies, reports of inconsistent service delivery, and limited sales and presales expertise outside of Japan.
- Gartner clients have increasingly reported that Dell SecureWorks' pricing is more expensive relative to other MSSPs.
- Gartner clients have expressed concerns regarding a planned Dell SecureWorks initial public offering (IPO) and the potential for distraction or issues with account management responsiveness.

HPE

Hewlett Packard Enterprise (HPE) Managed Security Services is part of the recently formed HPE organization in the Enterprise Security Services business. HPE is headquartered in Palo Alto, California, with global MSS operations in Sydney, Australia, Manchester, U.K. and Plano, Texas. HPE has a number of security solutions in its portfolio supported by professional services and MSSs; technologies for SIEM, application and data security; and services and solutions focused on enterprise customers. HPEs MSS leverages the HPE Security ArcSight SIEM platform, the Vertica platform and related event-collection components. Log management is delivered via HPE Security ArcSight Enterprise Security Manager (ESM) and HPE Security ArcSight Logger in SaaS, hosted or on-premises deployments. HPE provides managed advanced threat detection and incident response services through a strategic partnership with FireEye. HPE has two SOCs in the U.S., one in Canada, one in Latin America, three in Europe and three in the Asia/Pacific region. HPE offers a portal for its MSS customers and uses the HPE Security ArcSight Logger technology for log management. Log management features are available via the HPE Security ArcSight Logger portal. HPE offers an MSS portal for separate governance, risk and compliance-oriented activities for executive dashboards. The MSS portal provides role-based access, ticketing and security reporting features. Large and midsize companies requiring a global presence, especially those using HPE IT services and solutions, should consider HPE for MSSs.

HPE is in the Challengers quadrant based on the relative lack of maturity of its MSS portal, and the challenges HPE faces in gaining share beyond its IT outsourcing customers.

STRENGTHS

- HPE has multiregional security delivery resources and support capabilities for large service engagements.
- HPE's broad technology and service delivery options enable extensively customized MSS engagements, including technology bundling and hybrid delivery options. HPE has made specific investments in its MSS capabilities for security monitoring.

- HPE's standardization on the HPE Security ArcSight platform for global MSSs brings consistency to its delivery capabilities. Its partnership with FireEye for incident response services brings recognized advanced threat detection and incident response capabilities to HPE's existing MSSs.

CAUTIONS

- The HPE MSS portal lacks several features that are available in competitors' portals, especially in asset and vulnerability details, self-service reporting capabilities, and integration with customer ticketing systems. Potential customers should validate that HPE's current capabilities and future enhancements will meet their deployment and operations requirements.
- Gartner clients report that the presales engagement with HPE can be challenging, and requires persistence to engage with the desired resources for MSS. HPE SIEM products and MSS services compete for the same customer budget.
- As HPE shifts MSS to pricing based on data volume, prospective MSS customers should validate assumptions about security data volume in the anticipated scope of services, and understand the impact of higher- or lower-than-planned-for volume on service delivery and pricing.

IBM

IBM is headquartered in Armonk, New York, with primary MSS offices in Atlanta, and regional offices in Singapore and Belgium. IBM offers a broad range of MSSs, security consulting, incident response and integration services, either as stand-alone offerings or as part of larger multiservice or solution contracts. MSSs are delivered from six 24/7 SOCs: two in the U.S., one in Costa Rica, one in Brazil, one in Tokyo and one in Wroclaw, Poland. IBM has three additional non-24/7 SOCs around the world. IBM uses its QRadar SIEM to deliver MSS, as well as monitoring in cloud-based, as-a-service, on-premises managed or co-managed monitoring. IBM's advanced analytics and targeted attack detection capabilities for the network and hosts include third-party vendors with an emphasis on IBM solutions and customer-deployed products. Threat

intelligence is delivered via the IBM X-Force threat research team and the X-Force Exchange portal. Support for data residency requirements is available through managed SIEM deployment on the customer's premises or using SIEM as a service hosted within IBM's SoftLayer. Enterprises with global service delivery requirements and those with strategic relationships with IBM should consider IBM for MSSs.

IBM's placement in the Leaders quadrant reflects its strong MSS delivery capability and ability to compete with other vendors on a global basis.

STRENGTHS

- Gartner clients very often include IBM in competitive MSS evaluations, and the vendor has high visibility for MSS in all geographic regions.
- IBM has a full-featured portal that leverages elements of the QRadar management console for log management. The vendor also plans to release enhancements for additional intelligence and dashboard capabilities based on BigInsights and Cognos.
- IBM is a large, mature provider of security and IT services and products, with global delivery capabilities.
- Customers generally give good marks for IBM's ability to deliver core MSS capabilities.

CAUTIONS

- Gartner clients report challenges engaging with the IBM sales processes, and obtaining timely and responsive MSS bids.
- IBM's advanced threat protection for network analysis and forensics uses IBM's QRadar SIEM components and other service offerings, such as managed FireEye or Carbon Black. Prospective customers with other network behavioral analytics or forensics products may require custom services, although IBM plans to support more-advanced threat solutions in the future.

- Although IBM's MSS supports multiple security vendors and their technologies — including many from its competitors in the IPS and SIEM markets — MSS customers should monitor planned and actual MSS support for the security technologies deployed in their environments.

NTT

NTT is based in Tokyo, with London and New York offices. MSS is delivered by three brands, representing companies acquired over the past several years: NTT Com Security, with a focus on Europe; Dimension Data, with a focus on the Asia/Pacific region and Solutionary, with a focus on North America. Each organization can deliver MSS to customers in multiple regions. NTT is included in this Magic Quadrant on the basis of its combined offerings and the scale of its MSS entities. NTT has multiple SOCs in the Asia/Pacific region, Europe and North America. Targeted attack protection is embedded in the MSS offering of each delivery group, and it differs among the groups, although the groups share threat information. NTT customers and enterprises seeking a large global service provider with specific regional strengths should consider NTT for MSSs. Specifically, buyers seeking North America-centric services should consider Solutionary; those requiring Europe- or Japan-centric services should consider NTT Com Security; and those seeking broader Asia/Pacific-centric services should consider Dimension Data.

NTT's position in the Challengers quadrant reflects the strong service record of its several MSS delivery organizations in specific geographies, and the lack of overall unified sales and delivery capability for MSS.

STRENGTHS

- NTT Com Security, Solutionary and Dimension Data are well-known in Europe, North America, the Middle East/Africa and the Asia/Pacific region, respectively, and they appear in MSS deals in those regions. These MSSs get generally positive reviews from Gartner clients.
- NTT has a global presence, as well as a wide range of security service offerings and delivery options, in addition to broader telecommunications and IT infrastructure service offerings.

CAUTIONS

- Gartner reviewed the Solutionary MSS portal, but did not validate the MSS portal capabilities of Dimension Data and NTT Com Security. Due to distinct delivery platforms and portals, the features and functions available in the NTT Solutionary portal may not be available to MSS customers with service that is not delivered by Solutionary.
- MSS operations are not integrated across business units. Prospective global customers with delivery requirements that include region-specific requirements should verify that NTT will ensure best-of-breed capabilities in each region, with the required level of global service coordination.
- Customers should continue to closely monitor MSS delivery for quality and meeting roadmap commitments. Gartner clients have reported service issues with NTT.

Orange Business Services

Orange Business Services, headquartered in Paris and with regional offices in Atlanta and Singapore, offers a broad range of telecommunications and cloud-based IT infrastructure services, security consulting services, and MSSs. Orange's MSSs are based on commercial technologies for log management, event correlation and advanced threat detection. Threat intelligence is gathered using proprietary tools monitoring Orange's IP networks. Services are delivered from five 24/7 SOCs, with three located in Europe, one in North America and one in the Asia/Pacific region. Data residency requirements are addressed on a case-by-case basis, with European data storage available for non-European clients, if needed. Orange's network and infrastructure service customers, and organizations seeking a large, global and stable Europe- and Asia/Pacific-focused MSS provider, should consider Orange Business Services.

Orange Business Services appears in the Niche Players quadrant due to a relative lack of comprehensive security monitoring and mature portal compared with its competitors, and the vendor's lack of visibility among MSS buyers.

STRENGTHS

- Orange is a large, stable service provider offering a broad range of network and IT services that can be bundled with MSSs.
- The vendor can deliver services to customers seeking MSSs with data storage and analysis based outside of North America.
- Customers give good marks for Orange's MSSs, especially for network device management.

CAUTIONS

- The Orange MSS portal (there is a separate IT service management portal) lags behind those of competitors in supporting day-to-day investigation of security events. There is limited context and navigation capability, and customers seeking to investigate log data directly must be granted access to the console of SIEM platforms (HPE Security ArcSight or IBM Security QRadar) to do so.
- Orange lags behind many MSS competitors in providing advanced attack analytics as part of its MSS.
- Orange rarely appears on Gartner clients' shortlists for MSS procurement, and it has very limited MSS market visibility.

Symantec

In October 2014, Symantec announced the sale of the Veritas information management business, effective 1 January 2016. The security business, including MSS delivery, will retain the Symantec name and be part of the Cyber Security Services portfolio. Symantec's Cyber Security Services offerings include security monitoring, security intelligence, incident response services, and security training and awareness services. The vendor also has a broad portfolio of security solutions. Symantec's MSS architecture is based on self-developed technology. Symantec is headquartered in Mountain View, California, and the vendor has six SOCs: one each in the U.S., the U.K., and Japan, and three in the Asia/Pacific region, with two more EMEA SOCs planned for 2016.

The SOCs operate on a follow-the-sun model, and customers are assigned a primary SOC in their regions and a designated team of analysts. Customer event and log data are analyzed and retained in the North American SOC. Customers that require other data storage options can use an on-premises-deployed commercial log storage solution. Symantec supports endpoint behavioral and forensics services based on its Advanced Threat Protection product. Symantec also announced its Cyber One pricing, which provides security monitoring, intelligence and incident response services in one agreement. Enterprises seeking an established MSSP with a global presence should consider using Symantec.

Symantec is in the Leaders Quadrant due to the strength of its security monitoring service delivery and ability to compete globally with leading competitors.

STRENGTHS

- Symantec collects logs from a broad range of security and IT sources, and offers full MSS portal-based query capabilities for retained log data.
- MSS customers indicate that the DeepSight Intelligence threat feeds and intelligence reports are differentiators of Symantec's services.
- The vendor's MSS portal provides comprehensive features for alerts, log search, reporting and workflow.
- Gartner customers very often consider Symantec's MSS offerings in competitive evaluations.

CAUTIONS

- Symantec's services for endpoint threat detection and response are built around monitoring its own endpoint products. Those using EDR products from competitors must validate whether Symantec will support them.
- Unlike most MSSPs, Symantec offers only very limited device management services. It offers device management for IDS/IPS, not for other security controls. Prospective customers seeking those services in addition to monitoring must anticipate working with Symantec partners.

Trustwave

In August 2015, Singtel completed the acquisition of Trustwave, which is now a stand-alone business within Singtel Group Enterprise. Trustwave will continue to operate under the Trustwave brand and remains headquartered in Chicago, with regional headquarters in London, Sao Paulo and Sydney, and offices in 26 countries. Trustwave has several security technologies — including SIEM, UTM, network access control, application security, Web application firewall (WAF) and anti-malware — and builds MSSs around those as well as third-party products. Security intelligence capabilities are provided by the Trustwave SpiderLabs group, and augmented through Singtel's network monitoring capabilities. Trustwave has three U.S.-based SOCs, one in Europe and one in the Asia/Pacific region. Targeted attack detection and advanced analytics capabilities are standard components of Trustwave MSSs, and are delivered via services such as Managed Anti-Malware and Managed SIEM. Singtel customers, as well as companies in the retail, hospitality, healthcare and banking vertical industries, should consider Trustwave for MSSs.

Trustwave moved from the Niche Players quadrant to the Challengers quadrant in 2015 due to the access it gained to greater resources and new markets resulting from the acquisition by Singtel, and its increasing investments in competing for enterprise customers.

STRENGTHS

- Trustwave provides managed services with its broad, growing portfolio of security products. These can be packaged and sold as subscription services with no capital expenditures. Trustwave continues to expand its relationships with third-party technology providers and offers monitoring and management services for third-party technologies.
- The Trustwave portal supports over 20 languages for localization.
- Trustwave SpiderLabs' threat intelligence is used to provide protective and detective capabilities to the Trustwave products used in MSS, and to SOC analysts monitoring customer devices.

- The vendor remains a well-recognized provider of services and technologies to support PCI Data Security Standard (DSS) compliance. Compliance customers can leverage Trustwave services to extend security monitoring beyond the scope required for PCI compliance to address threat management use cases.

CAUTIONS

- Trustwave lags behind other MSSPs in employing advanced analytics technologies and methods to help SOC analysts and customers to identify unusual behaviors among users and other entities.
- As Trustwave continues to add support for third-party security technologies, customers should validate when and to what extent the security products they have deployed will be fully supported by Trustwave MSSs.
- Trustwave's TrustKeeper MSS portal currently lags behind those of its competitors. The compliance view portal offers very basic dashboards showing event counts and trends, but does not support drill-down, pivot and navigation through event data. A separate Enterprise View portal offers hierarchical views of activity, including agents deployed, logs collected and scans executed. Extensive portal changes are planned for 2016.
- Trustwave rarely appears in MSS inquiries among Gartner clients.

Verizon

Verizon is headquartered in Basking Ridge, New Jersey, with offices throughout the U.S., Europe, Latin America and the Asia/Pacific region. Verizon offers MSSs and security consulting, as well as a broad range of telecommunications and infrastructure services. The vendor is in the process of migrating its legacy MSS delivery technology to one based primarily on Splunk and open-source technologies for event correlation, analysis and storage. Three SOCs are located in the U.S. (one serving only government customers), two in Europe and four in the Asia/Pacific region. Verizon's Research, Investigations, Solutions, Knowledge (RISK) team provides threat intelligence and malware detection signatures that support MSSs, and the vendor's breach

response services inform MSS monitoring efforts. Verizon uses regional SOCs and data retention to meet requirements for local data storage and analysis. Network traffic analysis and payload analysis are available via third-party technologies to customers worldwide. Network and endpoint forensics are available on retainer as consulting services, and endpoint behavior analysis services are available via integration with third-party technologies. Enterprises should consider Verizon if they are looking for an established service provider that is capable of delivering a broad range of security services in multiple regions.

Verizon appears in the Leaders quadrant because it is highly visible to MSS buyers, competes with other leaders globally and has a strong track record for delivering MSS.

STRENGTHS

- As a telecommunications provider, Verizon offers MSS offerings including network-based and premises-based controls, and security data acquisition and analysis of customer network traffic and premises-based logs.
- The vendor's MSS receives positive marks from Gartner clients. They also cite Verizon's security expertise as a differentiator for MSSs.
- Verizon is very visible as an MSS provider among Gartner clients, and is often included in competitive MSS evaluations.

CAUTIONS

- Verizon is presently developing a new unified MSS portal. Today, depending on the features selected, MSS customers might have to use two portals. Verizon plans general availability of the new portal in 2Q16.
- The vendor is in transition with its MSS delivery platform. Current MSS customers should monitor service delivery and be prepared to assess changes in service quality during and after the transition. Prospective MSS customers should validate the capabilities that will be available on the date they plan to initiate

services.

- Verizon has been slow to introduce targeted attack detection features to all regions. MSS customers who anticipate introducing new advanced threat defense capabilities should validate the scope of MSS support available worldwide.

Wipro

Wipro is headquartered in Bangalore, India, with offices around the world. Wipro provides security event monitoring and incident response, infrastructure security operations, threat and vulnerability management, and other security services under the ServiceNxt MSS brand. Services are delivered from six SOCs in the Asia/Pacific region, two in Europe and one in North America. The India-based SOCs are ISO 27001-compliant. Wipro uses shared SOC staff and customer-dedicated commercial SIEM products to deliver security monitoring and compliance reporting. The vendor offers managed network security analytics and threat detection services using commercial solutions deployed on the customers' premises. Flexible options are available to meet data residency requirements and regulations. Service reporting is delivered via a security intelligence portal. Wipro outsourcing customers, and enterprises seeking MSS based primarily on dedicated SIEM instances that can be customized, should consider Wipro.

Wipro's relative lack of visibility for MSS outside its existing customer base, and its emphasis on packaging multiple management services and customized managed SIEM for MSS deals, is reflected in its placement in the Niche Players quadrant.

STRENGTHS

- Wipro's MSS delivery scheme is highly customizable to customers' requirements for scope, alerting and response support.
- Customers of Wipro's IT infrastructure services can add security monitoring delivered by a dedicated monitoring group, rather than the infrastructure management team.

CAUTIONS

- Customer access to log data is available only by specific customization to allow access to the SIEM log management and query capabilities, and these capabilities differ among the SIEMs supported by Wipro.
- The Wipro MSS portal provides basic summary data of security event activity and tickets, including drill-down into ticket history. However, operational views into events, compliance reports and user-created reports are accessible only when the SOC grants customers secure access to the SIEM portal.
- Wipro very rarely appears on Gartner clients' shortlists for MSS outside of the subcontinent.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

BAE Systems is included in this Magic Quadrant based on the addition of MSS capabilities gained through the acquisition of SilverSky.

Wipro is included based on its development and expansion of MSS delivery capabilities and offerings consistent with the MQ inclusion criteria.

Dropped

No vendors were dropped.

Inclusion and Exclusion Criteria

As a remote service, MSS can be delivered to and from any locations with sufficient connectivity. MSSPs that have operations in one geographic region can support customers in other regions. Gartner sees a distinct preference among customers seeking MSSs to first consider MSSPs with a presence in their region. For global enterprises, that includes a presence in multiple regions where the enterprises operate, in order to provide more local support. Local presence enables the MSSP's ability to keep some data in specific regions, as well as to provide local business hours, access to advanced support, staffing requirements (such as specific citizenship) and local language support, among other capabilities. In addition, compliance with data residency and privacy regulations can be addressed in many cases with local operations centers.

This Magic Quadrant includes MSSPs that have met thresholds for scale (expressed as devices supported and customers) and presence (SOCs) in multiple regions, as well as a threshold for MSS revenue.

The criteria include a threshold for the number of firewalls or IDP devices under monitoring or management, and a threshold for the number of MSS customers — both distributed across multiple regions. MSSs refer to remote management and monitoring of security technologies. We note that several large infrastructure outsourcing vendors offer other service delivery options (such as staff augmentation) in addition to MSSs, but we don't evaluate these other delivery options. Also excluded from this analysis are service providers that offer MSSs only as a component of another service offering (such as bandwidth or hosting), and vendors that provide MSSs only for their own technologies, not for third-party technologies.

Inclusion Criteria

Vendors must have:

- Services to remotely monitor and/or manage firewalls, IDP devices from multiple vendors via discrete service offerings and shared-service delivery resources.

- Firewalls/IDP devices under remote management or monitoring for external customers.
- Reference accounts that are relevant to Gartner clients in the appropriate geographic regions.
- A threshold of the number of customers as well as the number of firewalls and IDS/IPS devices in multiple geographies. The thresholds for customers and devices have increased from the prior Magic Quadrant to reflect market growth.
- A threshold for MSS revenue of $40 million in 2014. The threshold for revenue has increased from the prior Magic Quadrant.
- A SOC presence in multiple geographic regions.
- Service providers that Gartner determines to be significant vendors in the market because of their market presence or service innovation.

Inclusion thresholds for firewalls/IDP devices under MSSs are 315 in Asia/Pacific, 2,090 in Europe, 3,135 in North America and 35 in the rest of the world (ROW). MSSPs must meet the thresholds in one of the following combinations:

- Asia/Pacific and Europe
- North America and ROW
- Asia/Pacific and North America
- Europe and North America

Inclusion thresholds for MSS clients are 60 in Asia/Pacific, 100 in Europe, 300 in North America and 15 in ROW. MSSPs must meet the thresholds in one of the following combinations:

- Asia/Pacific and Europe

- North America and ROW
- Asia/Pacific and North America
- Europe and North America

Exclusion Criteria

Vendors have:

- Service offerings that are available only to end users that buy other non-MSS services
- Services that monitor or manage only the service provider's own technology
- Services delivered by service provider resources dedicated to a single customer
- Services that fail to meet the inclusion criteria

Evaluation Criteria

Ability to Execute

Product or service refers to the service capabilities in areas such as event management and alerting, information and log management, incident management, workflow, reporting, and service levels.

Overall viability includes the organization's financial health, the financial and practical success of the overall company, and the likelihood that the business unit will continue to invest in the MSS offering.

Sales execution/pricing includes the service provider's success in the MSSP market and its capabilities in presales activities. This also includes MSS revenue, pricing and the overall effectiveness of the sales channel. The level of interest from Gartner clients is also considered.

Market responsiveness/record evaluates the match of the MSS offering to the functional requirements stated by buyers at acquisition time. It also evaluates the MSSP's track record in delivering new functions when the market needs them.

Marketing execution is an evaluation of the service provider's ability to effectively communicate the value and competitive differentiation of its MSS offering to its target buyer.

Customer experience is an evaluation of the service delivery to customers. The evaluation includes ease of deployment, the quality and effectiveness of monitoring and alerting, and reporting and problem resolution. This criterion is assessed by surveys of vendor-provided reference customers, as well as by feedback from Gartner clients that are using the MSSP's services, or have completed competitive evaluations of the MSSP's offerings.

Operations includes the MSSP's service delivery resources, such as infrastructure, staffing and operations reviews or certifications.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium

Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (December 2015)

Completeness of Vision

Market understanding involves the MSSP's ability to understand buyers' needs and to translate them into services. MSSPs that show the highest degree of market understanding are adapting to customer requirements for specific functional areas and service delivery options. MSSPs with market-leading vision are investing in expertise and technology to monitor and analyze the external threat environment to better understand the sources, motives, targets and methods of attackers. They are using that insight to improve the effectiveness of their MSS. They are also developing and introducing services that support large-scale data collection; advanced analytics, including statistical and behavioral functions; and monitoring of new data sources, such as endpoint and network, to include in analysis. The goal of these capabilities is to more effectively find and respond to advanced targeted attacks.

Marketing strategy refers to a clear, differentiated set of messages that is consistently communicated throughout the organization; is externalized through the website, advertising, customer programs and positioning statements; and is tailored to the specific client drivers and market conditions in the MSS market.

Sales strategy relates to the vendor's use of direct and indirect sales, marketing, service, and communications affiliates to extend the scope and depth of market reach.

Offering (product) strategy is the vendor's approach to product development and delivery that emphasizes functionality and delivery options as they map to current and emerging requirements for MSSs. Development plans are also evaluated.

Vertical/industry strategy and **geographic strategy** include the ability and commitment to service geographies and vertical markets.

Innovation refers to the service provider's strategy and ability to develop new MSS capabilities and delivery models to uniquely meet critical customer requirements. Examples include the capabilities described in market understanding.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Medium

Innovation	High
Geographic Strategy	Medium

Source: Gartner (December 2015)

Quadrant Descriptions

Leaders

Each of the service providers in the Leaders quadrant has significant mind share among enterprises looking to buy an MSS as a discrete offering. These providers typically receive very positive reports on service and performance from Gartner clients. MSSPs in the Leaders quadrant are typically appropriate options for enterprises requiring frequent interaction with the MSSP for analyst expertise and advice, for portal-based correlation and workflow support, and for flexible reporting options.

Challengers

In the Challengers quadrant, Gartner customers are more likely to encounter MSSs that are offered as components of an IT or network service provider's other telecommunications, outsourcing or consulting services. Although an MSS is not a leading service offering for this type of vendor, it offers a "path of least resistance" to enterprises that need an MSSP and use the vendor's main services.

Visionaries

Companies in the Visionaries quadrant have demonstrated the ability to turn a strong focus on managed security into high-quality service offerings for the MSS market. These service providers are often strong

contenders for enterprises that require frequent interaction with MSS analysts, flexible service delivery options and strong customer service. MSSPs in the Visionaries quadrant have less market coverage and fewer resources or service options compared with vendors in the Leaders quadrant.

Niche Players

Niche Players are characterized by service offerings that are available primarily in specific market segments, or primarily as part of other service offerings. These service providers often tailor MSS offerings to specific requirements of the markets they serve.

Context

Prospective MSS buyers with threat management use cases should highly weight MSSPs' threat research and security intelligence capabilities.

Current and prospective MSS users should require a proof of concept (POC), or a demonstration of MSS offerings for advanced analytics and big data, to validate ease of use, effectiveness and value.

Current and prospective MSS users should validate MSSPs' services to address advanced attacks via network behavior, network forensics, payload analysis, endpoint behavior and endpoint forensics.

Market Overview

The market for MSS offers prospective customers numerous options among providers of several types, including outsourcers, telecommunications providers and pure-play MSSPs. Threat management and meeting compliance requirements via 24/7 security monitoring remain the primary drivers for considering an MSS. These may be complemented by related drivers, such as the access to deeper or broader security expertise than is available in-house, or the need to redirect existing internal resources to other security areas. An important

emerging driver related to threat management is service provider support for the protection from, early detection of and response to targeted attacks. MSSPs seek to address that need by developing capabilities to:

- Understand the external threat environment through the collection and analysis of information on attackers, methods and motives
- Leverage insight gained from monitoring a large number of security events from a global customer base
- Use advanced analytics to identify threats through behavioral or statistical anomalies in security events, IT logs, network traffic or endpoint activity
- Provide incident response capabilities that include attack mitigation and forensic investigation services

Requirements to monitor mobile devices and assets in public cloud services (PCSs) are additional areas of concern for some MSSP customers. Several MSSPs directly partner, or can integrate via custom services, with cloud access security brokers (CASBs) and cloud-based security-as-a-service providers. Several MSSPs have provisions for monitoring assets located in public cloud services, such as Amazon Web Services (AWS), Microsoft Azure and IBM SoftLayer, or their own cloud service offerings. However, there is variation across the offerings, and custom services for monitoring is likely required.

The 2015 Magic Quadrant for MSSPs, Worldwide reflects the requirements of customers with service needs in multiple geographic regions. MSSPs included in the evaluation meet the minimum thresholds for MSS delivery in two or more regions. MSSPs with multiregional business typically have a sufficient understanding of region-specific customer requirements, as well as sufficient service delivery capabilities that can scale to support global service delivery. Customers with a mix of global delivery requirements and local regulatory requirements related to, for example, data privacy, may require customized services.

MSSPs that do not meet the criteria for inclusion in this Magic Quadrant may still deliver high-quality services within a region, and typically deliver in multiple regions. When considering MSSs, Gartner customers should

develop evaluation criteria that meet their specific requirements.

In 2014, the global market for security outsourcing was $13.8 billion, with a forecast compound annual growth rate of 15.4% through 2019. In 2014, the global market for managed security services was $7.9 billion.

Growth in enterprise demand for MSSs is driven primarily by four factors:

- **Security staffing and budget priorities:** Gartner sees continued expectations to reduce operational costs and capital expenditures, and to avoid staffing increases related to the monitoring and management of mature security technologies, such as IDSs and firewalls, and the collection and reporting of logs for compliance purposes. MSSPs can provide these services on a 24/7 basis, allowing customers to devote internal security resources to higher-value activities.
- **Increased emphasis on monitoring and breach detection:** Efforts to provide earlier detection of and response to security breaches or compliance lapses through monitoring and analysis of user, system and network event information require tool and analytical expertise that will be difficult for many organizations to supply in-house. An MSSP's understanding of the external threat environment and indicators of compromise can provide expertise that many organizations cannot afford to develop and maintain. This includes expertise in the deployment, configuration and ongoing operation of advanced detection technologies.
- **Evolving compliance reporting requirements:** The evolution of existing compliance requirements and the development of new requirements — industry-specific, country-specific and region-specific — and of corporate governance policies directly or indirectly create stronger requirements for incident monitoring, identification, and response internally and among business partners. As formal compliance regimes become more stringent or more pervasive, or as audit/enforcement activity increases, organizations will consider external service providers to reduce the costs of meeting compliance requirements.

MSS growth can also be constrained by a few factors:

- **Enterprise deployment of SIEM technology to provide in-house alerting and log analysis:** MSSPs typically lack deep insight into the customer IT and business environment; thus, they are less able to determine the degree of risk associated with events involving users, administrators, internal applications and data. Wherever enterprises want close monitoring of internal activities, they may opt to do it themselves. Some organizations monitor internal activities and also use an MSSP for external/perimeter monitoring. Such an arrangement still constrains the growth of MSSs in those organizations.
- **Data residency and other privacy requirements:** Regulatory requirements regarding movement of and access to specific types of data may limit the scope of monitoring enterprises entrust to MSSPs.
- **Alternative security service providers:** Other service delivery options are available for security monitoring and management. These include IT infrastructure outsourcers who offer customer-specific device management and monitoring with dedicated staffing on-site or remote; technology vendors that offer services for their own technologies, and specialist providers that offer advanced threat detection services that focus on discrete detection capabilities (often network and endpoint behavior) without offering other device monitoring or management services.
- **Change in strategy to reduce outsourcing:** At the enterprise level or within the security organization, a change in strategy regarding the use of external services can mean that MSSs are not considered effective options.

MSS Portfolio

The services that are core to MSS offerings involve the monitoring of perimeter network security technologies. They are:

- Firewalls and next-generation firewalls (NGFs)
- IDSs/IPSs and next-generation IDS/IPS

- Multifunction firewalls/UTM services
- Secure Web gateways (SWGs)
- WAFs

MSSPs have begun to introduce services to manage and monitor both proprietary and commercial technologies designed to detect protect against advanced threats. These services analyze payloads to detect malicious software and monitor activity and behavior of network traffic and endpoints.

In addition to monitoring, many MSSPs have management services for those technologies. It is now common for MSSPs to also provide monitoring and log collection from IT infrastructure such as servers, user directories and applications. Recent advances in the use of big data repositories have enabled MSSPs to introduce services that provide for the collection, search, analysis, reporting and retention of a much larger scope of security events, IT logs and network data than was previously available.

Among organizations that have deployed SIEM technology, Gartner sees increasing interest for services to monitor or run the SIEM. Several MSSPs have offerings to support customer-deployed SIEM.

MSSPs may also provide cloud or SaaS-based services, including:

- DDoS protection
- Email security
- Web filtering/SWG
- Vulnerability scanning
- Network-based firewall/IDP

MSSPs offer cloud services directly or via partnerships with other service providers. The degree of integration of

partner-delivered services with MSSP services varies from little more than purchasing convenience to integration of partner data and management functionality into the MSSP's portal. Deeper integration can provide operational and vendor management advantages, but may reduce the ability to "swap out" one cloud-based service for another.

Buyers should take into consideration the degree of integration of any partner-delivered services with the MSSP's offering. SLAs should ensure that service upgrades occur in a coordinated manner that does not adversely affect service outcomes. Potential customers should also evaluate whether the delivery of services from multiple providers will affect training, operational efficiency and end-of-contract switching costs.

Threat Intelligence and Advanced Analytics

Most MSSPs have created research groups to improve their understanding of the threat landscape — that is, the identities, motives, targets and techniques of attackers. Those that do not have their own threat research groups often partner or license threat information from one or more providers. MSSPs use threat intelligence to support their security operations analysts; they may also provide customers with subscription-based access to this research, or offer customers project-based access to the group for analysis/reverse engineering of malware and other incident response activities. Potential customers of threat intelligence feeds from MSSPs should require proof-of-concept access to evaluate the relevance of the information, as well as their ability to consume and act on it. Several MSSPs now support, or will in the next 12 months, common threat intelligence description and sharing formats, such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII).

Many MSSPs claim capabilities to assist their customers in addressing advanced targeted attacks. These capabilities may be visible as discrete service offerings or options, or as features embedded in existing offerings. They may include, for example:

- Correlation of events with object reputation, such as known bad IP or email addresses or URLs

- Comparison of alerts, activity patterns or state (such as device configuration, registry settings, running process and so on) to those of known indicators of compromise
- Analysis of activity patterns (across an MSS customer base as well as within the customer environment) to identify outliers, exceptions or deviations from baselines in security events, network traffic, or the activity of users or entities on the network

These offerings are now primarily based on the security events monitored by the MSSPs; nearly every MSSP has introduced, or will in the next 12 months, distinct service offerings to acquire, retain and analyze large volumes of customer data — so called "security big data" — from other sources such as network traffic, hosts and applications. The immediate benefit to most MSSPs customers will be an increase in log retention times and faster searches for incident investigation. Several MSSPs currently have large data analytic capabilities, but these are utilized on the back end to complement traditional security event correlation and monitoring. Some vendors plan to expose more of these capabilities directly to the customer in the next year. Gartner recommends that customers require a limited pilot or proof of concept to identify specific areas where relevant, actionable intelligence results from the collection and analysis of the data, and to identify the service levels required. Based on feedback from Gartner clients, early adopters should plan for the inclusion of relevant domain experts — who are typically outside the security group, such as IT operations, application owners, and line-of-business owners — in the evaluation of these capabilities. Successful use of these advanced capabilities is likely to require establishing processes to support the ongoing involvement of relevant domain experts in investigations and response activities.

Most MSSPs also offer incident response capabilities to assist customers with investigation and remediation activities in the event of a breach. Gartner clients are increasingly asking about these services and looking to source them in conjunction with MSSP deals. These services are typically available on a consulting basis, and can be purchased as needed, or via a retainer for a set number of hours, with service-level commitments for response time. Prospective customers should confirm with MSSP candidates how much response support is

available within the context of the standard monitoring services, and when a consulting engagement is required. If the MSSP offers packaged or prepaid retainer hours for incident response activities, then customers should ensure that those hours are available for other security services if they are not needed for incident response.

Pricing Models

Pricing models for MSS are becoming more diverse. Most MSSPs offer a pricing model based on the type and size of the security technology to be monitored for customer-premises equipment-based devices, or on the bandwidth or number of users/endpoints for network-based controls. Log collection is typically priced by the number and types of sources, or on number of events per time period (device count pricing includes implicit expectations of event volumes). There is often a clear distinction between technology that is monitored in real time and subject to alerting SLAs, and technology that is not — that is, where logs are collected and subject to reporting or querying, but not to real-time correlation and analyst review. Device management pricing is typically based on the number of configuration changes to be performed within a period of time. This model offers a fairly straightforward means for potential customers to determine the cost of a service and compare among alternative providers. Customers can opt to include more or fewer devices in the scope of service in order to balance coverage and budget requirements. A potential issue with this model is that where customers have high-capacity event sources that are underutilized, they pay for the potential capacity, rather than actual usage of those devices.

An alternative model is emerging based on the average volume of data collected over a time period. This model allows customer to pay based on the actual volume of data provided to the service provider for analysis, rather than the number or type of data sources. This is not the dominant model in the market, and in some cases is an optional model (based on the costing model of the underlying SIEM technology used to provide services). A potential issue with this model is that customers may have little or no control over the volume of data generated. A second issue is that not all data provides equal benefit for threat detection, but customers pay the

same rate for high-value and low-value data collection.

Other possible pricing models include those based on the number of security incidents raised by the detection technologies (typically a SIEM), or models based on analytic activities (such as running specific algorithms against a volume of data). In for former case, customers have no control over the events raised, thus have no control over cost increases.

Gartner expects the trend for common services, such as firewall and IDP monitoring and management, to decline 5% during 2016. Downward price pressure comes from new sources for these services, such as from the technology providers themselves, from other MSSPs and from continued corporate efforts to reduce IT budgets. As MSSPs continue to introduce new services to monitor and manage advanced threats, including the collection of more data and new types of data, we expect an increasing number of engagements with pricing models based on data volumes and types of analytics. SLAs (with the exception of data retention, which is well-established) will also be introduced that are based on the types of analyses run and the volume of data in scope.

MSSP Landscape

The basic makeup of the MSSP vendor space has not changed fundamentally. There are three major types of MSSPs:

- **System integrators/business process outsourcers:** These are broad IT service providers that typically manage security devices as part of larger outsourcing deals. Where the integrator or outsourcer acquired a pure-play MSSP and maintained a discrete MSS delivery capability, these providers often compete for MSS-only deals.
- **Carriers and network service providers:** These are bandwidth and connectivity providers that manage network security products. They often provide remote monitoring, premises-based technologies and cloud-

based services through their Internet connections.

- **Pure plays:** These are generally smaller, privately held MSSPs that are completely focused on security services. Pure-play MSSPs will continue to be acquired by larger service or IT infrastructure firms that seek to provide MSSs. New pure-play security service providers often focus on specific vertical markets or regulatory requirements, or on specific analytic services (such as user activity) or advanced threat detection technologies. We expect existing MSSPs to acquire pure-play service providers that have developed advanced analytics capabilities, especially those related to user activity monitoring and to network and endpoint monitoring.

This Magic Quadrant reflects the requirements of customers that seek MSSPs with a global presence and global delivery capabilities. The vendors that meet those requirements fall into the first two categories of MSSPs.

In general, the MSS portfolios of these providers look broadly similar. Customer satisfaction with services can be strongly related to customer expectations. Customers occasionally report dissatisfaction related to objectively poor performance, including missed SLAs. However, it is more common for dissatisfied customers to express disappointment related to subjective criteria that may never have been made explicit to prospective providers, or to the MSSP selected.

Gartner customers using MSSPs express differing expectations regarding their relationships with MSSPs. Expectations may range from frequent interactions and knowledge sharing among the customer security staff and MSSP staff, to almost no interactions beyond the provision of periodic reports of monitoring activity. Gartner recommends that prospective MSS buyers develop explicit requirements for service delivery. MSSPs' responses to these requirements (including via demonstrations, proofs of concept and the like) will enable customers to discern distinct differences among the MSSPs.

Buyers should define expectations for:

- The degree and quality of interaction with the MSSP's SOC analysts
- The features of the MSSP's portal that will support the customer's use cases
- Reporting for operational and management reporting
- The depth of threat and security intelligence offerings
- Support for specific compliance requirements
- The MSSP's professional services capabilities

Prospective buyers that evaluate MSSPs within the context of specific requirements will find that the providers that best fit those requirements may come from any segment of the Magic Quadrant.

Prospective customers seeking more advanced offerings, such as threat intelligence, or monitoring of network or endpoint behaviors or forensics services, should engage MSSPs to provide a thorough POC. Buyers should use the POC to validate the utility of these services in meeting specific use cases, as well as the resources needed to address the results of the analysis provided by the MSSP.

MSSP Mergers and Acquisitions in 2015

The MSSP market has been more dynamic in the past 12 months due to an increase in acquisition activity. For example, BAE Systems acquired Silversky, Singtel acquired Trustwave, and Raytheon acquired Foreground Security. In each case, a larger service provider acquired an MSS capabilities via a smaller provider. There have been other changes in business structure for several vendors on the Magic Quadrant, including the splitting of HP into two businesses, Symantec doing the same and Dell announcing its intention to acquire EMC. Gartner expects additional activity in 2016, as MSSPs seek to add capabilities to support advanced threat detection services via technology acquisitions, analytics expertise and threat intelligence operations.

Growth Areas for Managed Security Service

Several areas represent potential growth opportunities for MSSPs — and opportunities for disruption by alternative providers and delivery models. These are:

- **Mobility:** MSSPs have been generally slow to extend monitoring and management to mobile technologies, even central points like enterprise mobility management (EMM) and mobile device management (MDM). Service providers of unified communications platforms have an advantage in having access to mobile infrastructure in order to deliver security controls and monitoring for mobile, but may not be able to address broader monitoring requirements. Enterprises may be required facilitate cooperation between MSSPs and mobile providers.
- **Cloud environments:** Expanded enterprise use of cloud-based IT and services presents challenges to MSS. Access to those environments may be limited, as may be the security logs or events available for monitoring. MSSP support for public cloud environments is inconsistent and evolving.

Enterprises seeking unified security monitoring across their network, data center, mobile and cloud infrastructure may need to work with MSSPs to develop custom service approaches to achieve the desired scope and depth of monitoring.

MSSPs Not Evaluated in the Magic Quadrant

Not included in this Magic Quadrant analysis are smaller, regional or subregional providers, which can include small pure plays and larger providers that do not have enough MSS business in multiple regions to meet the inclusion criteria. Example vendors include Masergy, Clone Systems, Nuspire Networks, Optiv (formerly Accuvant and FishNet Security) and Alert Logic. Also excluded from this analysis are service providers that provide MSSs only for their own technologies, and that do not deliver services for third-party commercial technology. Service providers whose security services are sold and delivered primarily with infrastructure outsourcing, staff-augmentation or account-dedicated resources are also not included in this Magic Quadrant. Vendors such as Capgemini, CGI, HCL and Leidos have MSS delivery capabilities, although Gartner customers

and reference contacts often report that services are delivered via other means.

Because this Magic Quadrant focuses on the remote monitoring of customer controls, it does not include security monitoring services that focus only on threat detection and response services using data analytics, such as Alert Logic, eSentire, Datashield, FireEye, Lockheed Martin, LightCyber, and Rapid7. Gartner is monitoring the deployment and use of these services by enterprise customers. Customer inquiries for MSSPs are still significantly higher compared to managed threat detection and response services.

Gartner notes the entry into the managed services market of technology vendors that provide management and or monitoring services for their own technologies, or provide threat detection as a service, based on their own technology stack. Although these vendors do not meet the MSSP criteria established for this Magic Quadrant, they may at times compete against global or regional MSSPs. Gartner continues to monitor these vendors and their presence in the market.

?

Asia-Pacific Context

Market Differentiators

This document was revised on 16 February 2016. For more information, see the Corrections page .

The managed security service provider (MSSP) service offering is one of the most heavily contested areas of the IT market in the Asia/Pacific (APAC) region. The depth and breadth of services available, as well as country and language support, vary greatly in the enormous APAC region, providing clients with a wide range of services and prices from which to choose.

The APAC region is highly diverse in geography, culture, regulatory frameworks and economics. This diversity has created considerable opportunities for regional MSSPs that have invested in coverage and geographically

relevant offerings to differentiate their services. Global MSSPs based outside the APAC region are using their scale and brand awareness to compete in this market off the back of existing global clients with an APAC presence. As a result, an increasing number of regional and global providers are continuing to develop and invest in the MSSP market in the APAC region.

Some APAC countries (e.g., India, Thailand, Vietnam and Malaysia) have been relatively slow to embrace MSSPs for their networks, because of a preference for do-it-yourself (DIY) projects, lower labor costs and, in some cases, Internet bandwidth constraints that impede remote monitoring. Continuing breaches, regional security operations centers (SOCs) and improved networks have led organizations in the region to consider assistance from MSSPs.

Organizations in this region are in an early adoption phase of advanced network security technologies that include Web application firewalls (WAFs), next-generation firewalls (NGFWs), distributed denial of service (DDoS) and security information and event management (SIEM). Clients are facing service and support issues with some international vendors. Hence, many organizations are now seeking MSSPs to manage these technologies, as well as to deliver 24/7 management and monitoring. The MSSP market is gradually growing in this region.

Due to the increasing importance of enterprise information security to businesses, Gartner anticipates a steady growth and continuing maturity of the MSS market in the APAC region. At a high level, there are two "classes" of MSSPs in the context of this research:

- MSSPs with a primarily APAC-focused staff and client base
- Global MSSPs that also address the APAC market, but with a smaller base of existing local customers, compared with their number of worldwide clients

Clients in the APAC region continue to prefer providers with a security operations center (SOC) and "feet on the street" in the region. This preference has aided the growth of local providers with a more-tailored approach that

takes into account regional nuances. In response, multinational providers have invested in the region — building SOCs and acquiring personnel — which is diluting geography as a competitive differentiator. In addition, a small, but growing number of APAC clients are seeking "hybrid" security operations services that may include managed security services (delivered remotely), as well as on-premises service and/or staffing components.

The blurring lines between managed security services and other security services, such as implementation and consulting, mean that pure-play MSSPs in the region are at a disadvantage when competing with MSSPs that have a broader portfolio of offerings. There is also a small, but statistically notable, increase in clients that want their own SOCs, but need assistance to build, run and then transition ownership and staffing back to the end-user organization.

Considerations for Technology and Service Selection

Migrating from the internal management of security infrastructures to an MSSP model is a complex process. The hurdles encountered often have nothing to do with technology, but involve industry vertical considerations (for example, data sovereignty preferences and legislative mandates); IT organization preferences; and internal social or political issues.

Gartner clients indicate that they choose MSSPs based on a combination of general requirements and are influenced by local presence. In particular, APAC clients are focusing on the following:

- SOC location in the APAC region
- SOC staffing levels with in-region availability
- Vendor market perception and sales visibility in the APAC region
- Existing relationship with vendors
- Customer service within local time zones

- Ability to deliver ancillary services with qualified local personnel

Notable Vendors

Vendors included in this Magic Quadrant Perspective have customers that are successfully using their products and services. Selections are based on analyst opinion and references that validate IT provider claims; however, this is not an exhaustive list or analysis of vendors in this market. Use this perspective as a resource for evaluations, but explore the market further to gauge the ability of each vendor to address your unique business problems and technical concerns. Consider this research as part of your due diligence and in conjunction with discussions with Gartner analysts and other resources.

AT&T

AT&T has a smaller MSSP presence in the APAC region, compared with its market share in the U.S.; however, a growing portion of its portfolio involves in-region teams trained on the security service portfolio. Most of AT&T's devices under management are with multinational corporations (MNCs) headquartered outside the region, which require consistent MSSP delivery and a single vendor relationship.

AT&T can be considered by clients that are already using its carrier and other services, or have a large, distributed office network globally or in the APAC region. AT&T has eight SOCs. In the APAC region, they are located in Malaysia, India and Australia. AT&T has 2,000 employees in SOC engineering, sales and other related roles worldwide.

BT

BT takes its managed security services to market under the name "BT Assure." It has an APAC footprint via its three dedicated SOCs, two customer-specific SOCs and its regionally focused specialist sales staff. BT's local offerings include a wide range of managed security services focused on network protection, threat intelligence, identity and access management (IAM), data protection, cloud and mobile security services, and compliance

and incident management consulting as part of its larger telecommunications and service offerings. BT is increasing its security business unit sales and presales teams to provide better coverage in the region, which has increased the number of clients it served in 2015. BT's APAC footprint lags behind that of EMEA and the U.S.

BT Assure has three APAC SOCs: one in Australia, one in Singapore and one in India. In total, BT has 235 employees in SOC engineering, sales and other security roles in the APAC region.

Dell SecureWorks

Since its acquisition of SecureWorks in 2011, Dell SecureWorks has continued to grow its global MSSP business and the services it has offered. SecureWorks provides a range of MSSP and complementary specialist security services centered on threat intelligence, consulting, compliance and incident response.

Dell SecureWorks should be considered by global organizations with a footprint in the APAC region and by organizations that value expertise in security research and threat intelligence.

Dell SecureWorks has five SOCs worldwide. Japan is its only APAC-based SOC. In total, Dell SecureWorks has approximately 100 employees in SOC engineering, sales and other roles in the APAC region.

e-Cop

Headquartered in Singapore, e-Cop also has other regional offices. It has a leading number of SOC locations and other processing facilities in the APAC region, which gives it a larger presence than most of the global MSSPs that operate in the APAC region. e-Cop's ability to deliver SOCs in multiple countries has made it an attractive alternative for clients such as Singapore government agencies and finance and health verticals, where local staff and data sovereignty are both perceived and legislative imperatives for clients. Its clients have historically been loyal and consistently rate e-Cop's services as good to excellent.

Due to its extensive geographical coverage, range of security services and competitive pricing, e-Cop should be

considered for any APAC-centered midsize organization or government agency.

There are 10 e-Cop SOCs worldwide, including in Singapore, Malaysia, Hong Kong, Thailand, Indonesia, India and Japan, some of which are operated by partners. In total, e-Cop has more than 300 employees in SOC engineering, sales and other roles in the APAC region.

HCL

Headquartered in India, HCL offers a wide range of managed security service offerings and a broad range of IT consulting, system integration (SI) and outsourcing services. HCL has expanded its customer portfolio outside its historical client base in India. However, based on recent inquiries, few end-user organizations in Southeast Asia or Australia indicate they include HCL on their shortlists for managed security services. The company has sales personnel throughout the APAC region and is now in 31 countries, with more than 90,000 employees. Previous client reviews of HCL are generally good.

HCL can be considered by APAC-centric businesses that require a broad range of consulting and infrastructure management requirements, including risk and security management, and by organizations seeking end-to-end IT outsourcing services that have a security component.

HCL has three SOCs in the APAC region, but did not provide details on SOC locations and staffing.

HPE

Hewlett Packard Enterprise (HPE) is a large provider of a broad range of security consulting and traditional and on-premises-based managed security service offerings. HPE continues to build out pure-play managed security services, as well as a large-enterprise outsourcing business that can offer services to manage and monitor security technology in the APAC region. HPE's managed security services are growing in the APAC region, but should not be confused with the outsourcing arm of its business, which also offers security services. HPE managed security service is part of the HPE Enterprise Security practice and leverages specialized security

personnel for regional go-to-market execution.

HPE should be considered by large organizations that need a mix of infrastructure, outsourcing and software, and require a sizable strategic IT partner.

HPE has 10 SOCs globally, and has three APAC locations in Australia, Malaysia and India. HPE did not disclose its managed security service APAC staffing levels.

IBM

IBM has a long-established MSSP business. Building on this, it offers a full range of MSSP services, along with extensive consulting and integration services that can be consumed as stand-alone or as part of a larger outsourcing arrangement in the APAC region.

IBM should be considered for its MSSP services, when an enterprise has global service delivery requirements, large outsourcing deals, strategic relationships with IBM and a preference for APAC-located SOC delivery capabilities.

IBM has three SOCs in Australia, Japan and India, and did not disclose its managed security service staffing levels.

NEC

NEC's MSSP business is new and is primarily successful in the APAC and "rest of the world" markets today. NEC is building out this service by having support for the standard range of services, such as firewall/unified threat management (UTM), intrusion prevention system (IPS), Web and email security, and vulnerability assessment.

NEC should be considered for MSSP by existing NEC clients, clients with large investments in NEC operational technology systems, and smaller organizations that are headquartered in Japan and other locations supported by regional SOCs.

NEC has four SOCs in the APAC region, located in Japan, Australia and Singapore.

NTT

NTT has acquired three MSSP businesses servicing the APAC region: NTT Com Security, Solutionary and Dimension Data. All three were well-regarded and competitive in their own right in different locations. NTT now has three MSSP "brands," all offering the same "service" in the APAC market. Individually, all three have sizable numbers of clients and devices under management. At this time, they are separate MSS offerings that will be merged partially (managed security service back-end processing, for example) or fully at some point in the future.

Clients that have most of their offices in the U.S. looking for APAC-managed security service coverage should consider NTT's U.S. offering (Solutionary). Clients that are based primarily in Europe with APAC branches or have a Japan-specific footprint should consider NTT Com Security (formerly Integralis).

All other APAC-centric clients should focus on Dimension Data, because this is the largest of NTT's security practices in the region. Dimension Data's client portal is a leader in the APAC market. It also has a significant SI business covering consulting, cloud, integration, outsourcing and maintenance that is leveraged to cross-sell its well-regarded MSSP service.

NTT has nine SOCs in the APAC region — in Australia, New Zealand, Singapore, Malaysia, India and Japan — and seven unstaffed processing locations in Japan, Hong Kong, Singapore, Thailand, Malaysia and Australia. In total, NTT has 420 employees in SOC engineering, sales and other roles in the APAC region.

Paladion

Paladion is a pure-play service provider in the APAC region, headquartered from India, with footprints in the APAC region, the U.S., Europe and the Middle East. Paladion offers a wide range of IT governance, analytics, fraud management, security and compliance assessment, data protection, identity and access management

(IAM), and cloud and mobile security services, in addition to its MSSP offering. With four SOCs in the APAC region, it also offers the ability to build SOCs for clients, as well as deliver traditional MSSP offerings. Paladion is frequently seen in customer shortlists in India and also the Middle East. Historically, Paladion customers have rated its services as good to excellent, and it is a steadily growing business unit within Paladion.

For organizations with a large footprint in India that stretch into the APAC region, Paladion can offer a range of services at competitive prices.

Paladion has nine SOCs: two in India and one each in Malaysia, Vietnam, Doha, Dubai, Kuala Lumpur, Riyadh, Toronto and the U.S. It also has two unstaffed processing locations in the U.S. and the United Arab Emirates. In total, Paladion has 400 employees in SOC engineering, sales and other roles in the APAC region.

Symantec

Symantec has a long security heritage in both products and managed security services, with local APAC language availability, an attractive client portal, mature staffing and training models, and a global reach. Symantec was also listed most often by other vendors as their No. 1 competitor in the APAC region.

Some APAC clients may find this offering suboptimal, because all data resides in the U.S., and some technology management capabilities, such as firewalls, are being deprecated in favor of analytics and threat intelligence offerings. Although its APAC business is growing, there is a delta in the size of Symantec's devices under management in North America versus the APAC region that is behind the market average. Symantec has been in the APAC region for a long time, with a significant installed base of security product customers into which its MSSP sells. Symantec's renewed focus on security services is leading to managed security services becoming a more prominent part of its go-to-market strategy in the region.

Symantec appears regularly on Gartner client shortlists and can be considered by large APAC organizations or global organizations with a footprint in the APAC region. Symantec has three SOCs in India, Australia and Japan and a newly opened SOC in Singapore. In total, Symantec has 395 employees in SOC engineering, sales

and other roles in the APAC region.

Tata Communications

Tata Communications is a large telecommunications provider that is headquartered in India, has a worldwide presence and offers a good range of services in the market. These include a number of on-premises technologies — for example, firewall, UTM, IPS and WAF, as well as cloud coverage for virtual firewalls. Although its managed security service is a direct offering, it is also taken to market as an adjunct to its primary offerings around network services, hosting and colocation services across its data centers.

Tata is rarely seen on Gartner shortlists outside India, and competitors seldom list Tata as a competitor. At this time, its primary client base is predominantly in the APAC region, with 50% of its revenue coming from this region. It offers a competitive range of services and a useful client access portal. Its managed security service is also supplemented by professional security services.

Tata should be considered by clients that have an existing relationship with Tata, are headquartered in India with an APAC focus or have price sensitivity as a primary driver in their managed security service requirements.

Tata has two staffed SOCs: India and Singapore. In total, it has 140 employees in engineering and operations in the APAC region.

Telstra

Telstra is Australia's largest telecommunications provider. It offers a large number of adjacent services to its core offerings, including managed security services. It previously had a partnership with IBM to deliver some managed security services and is still transitioning these clients to its MSSP business unit. It also offers consulting services to complement its offerings. Telstra has embarked on a push to expand throughout APAC both organically and via recent acquisitions such as Pacnet. It has also created a joint venture with Telkom Indonesia called Telkom Telstra to offer data center services in Indonesia that will include managed security

services.

Being the largest telecommunications provider in Australia, it also has a strong DDoS offering, which complements its strength as an Internet service provider (ISP). Compared with other APAC-centric MSSPs, Telstra has a credible number of clients and devices under management; however, its clients are almost exclusively in the Australian market. Telstra has also announced its intention to expand throughout the APAC region, which will include its security practice, of which managed security service is a part.

Telstra should primarily be considered for Australia-centric businesses that are already using Telstra's services, or for businesses that are primarily based in Australia.

Telstra does not regularly appear on the shortlists of Gartner's APAC clients. Telstra has two SOCs in Australia. In total, the company has 395 employees in SOC engineering, sales and other roles in the APAC region.

Trustwave

Trustwave is a sizable North American MSSP that was acquired in April 2015 by Singtel, a large APAC-anchored telecommunications provider. Trustwave has a range of security products that are also leveraged throughout its managed security service offering, in addition to supporting a range of third-party providers' products. Trustwave has a large client base in North America and is expanding its client base into the APAC region. The acquisition by Singtel is interesting, in that most telcos have entered the managed security service business via acquisitions of credible MSSPs. (Singtel is the latest example.)

Singtel's footprint in the APAC region as a telco is promising for Trustwave's regional business; however, there will be a transition period for existing Singtel managed security service clients onto the Trustwave service. It will take some time for Singtel's business to become capable of taking this new offering to market, without disturbing the existing Trustwave operation.

In APAC, Trustwave should be considered by midmarket companies, organizations with a large network of

branches and those that can get value from additional services, such as PCI compliance.

Although Trustwave does not regularly appear on the shortlists of Gartner's APAC clients, Trustwave has three SOCs in the APAC region, located in Manila, Singapore and Australia.

Verizon

Verizon's APAC business does not have the same level of customer penetration as its U.S. and EMEA operations have achieved. It offers security consulting and the capability to support the management of on-premises SIEM, as well as traditional MSSP off-premises management via a very functional client Web portal. Verizon has a respected research and investigation team that complements its MSSP operation. Clients benefit from this by receiving Verizon threat intelligence data. In addition, Verizon can offer DDoS services to its ISP clients.

Organizations that require global coverage, a range of managed security service offerings and strong specialist security services (e.g., incident response) should consider Verizon.

Verizon has four SOCs in the APAC region, with two each in Australia and India. Verizon did not disclose its APAC managed security service staffing numbers.

Wipro

Wipro delivers a broad range of IT services worldwide. Its APAC MSSP client base and the number of devices under management, while substantial, are smaller than its client bases in the U.S. and EMEA, respectively. Customers have rated Wipro's services between good and fair. Wipro appears on shortlists throughout the region, especially on the subcontinent. Wipro's strengths in SI and consulting have produced a sound project-managed onboarding process.

An ideal APAC MSSP customer for Wipro is an organization that requires a broad range of consulting, SI and project management services, either in a single country or throughout larger areas.

Wipro has eight SOCs: Two are in the U.S., one each is in Europe and Malaysia, and four are in India. One has been in the build phase in Australia. It also has five unstaffed processing locations in Germany, and two each in the U.S. and India. In total, Wipro has 500 employees in SOC engineering, sales and other roles in the APAC region.

Evidence

- Gartner customer inquiries and information sharing related to MSSPs
- Analyst interactions with Gartner customers via inquiries and meetings
- Survey of MSSPs
- Survey of MSS reference customers

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports

them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the

organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.
