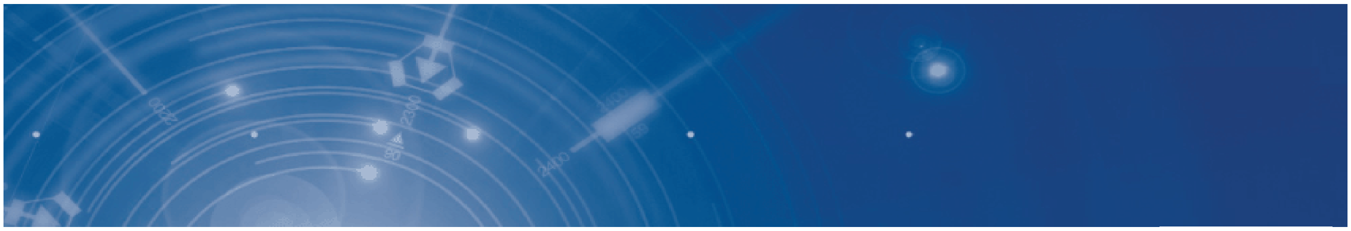


Magic Quadrant for MSSPs, North America

29 November 2010

Kelly M. Kavanagh, John Pescatore

Gartner RAS Core Research Note G00208473

Enterprises face a wide range of options when selecting a managed security service provider for security monitoring and management. This Magic Quadrant provides our analysis of which MSSPs and which security services can meet enterprise requirements.

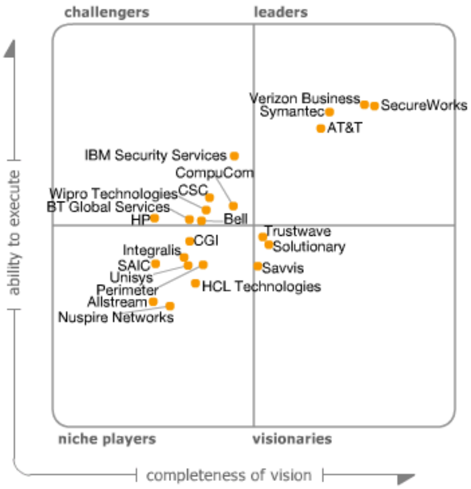
What You Need to Know

The number and types of managed security service providers (MSSPs) are growing, and enterprises are faced with more choices of managed security services (MSSs). Enterprises must define the scope of security activities and their level-of-service expectations before evaluating prospective MSSPs. MSSPs differ on the emphasis of their offerings and geographic delivery capabilities, from staff augmentation of traditional outsourcing, to device management, to real-time monitoring and security response expertise. Selecting an MSSP with service delivery capabilities and security expertise that are best aligned with enterprise requirements and expectations increases the chance of a successfully managed security engagement.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for MSSPs, North America



As of November 2010

Source: Gartner (November 2010)

Return to Top

Market Overview

Gartner projects continued growth for MSSs in North America, but with a shift to midsize (or smaller) buyers driving price erosion for core services, and the introduction of lower-price, multifunction firewall, log management, and other new offerings. Areas of growth include monitoring and management for network-based services or smaller unified threat management (UTM) devices (to address remote office/branch office requirements), or log management services related to compliance requirements.

Acronym Key and Glossary Terms

CICA	Canadian Institute of Chartered Accountants
CPE	customer premises equipment
DDoS	distributed denial of service
DLP	data loss prevention
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act
IDP	intrusion detection and prevention
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IPS	intrusion prevention system
ISO	International Organization for Standardization
MSS	managed security service
MSSP	managed security service provider
PCI	Payment Card Industry
SMB	small and midsize business
SAS 70	Statement on Auditing Standards No. 70
SIEM	security information and event management
SIM	security information management
SLA	service-level agreement
SOC	security operations center
UTM	unified threat management
WAF	Web application firewall

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of

Increased enterprise use of software as a service and the "consumerization of IT" will lead to more cloud-based security-as-a-service offerings, which will grow faster than the customer-premises-equipment- (CPE-) focused MSSP market in 2H10 and 2011. Gartner expects that there will be new security-as-a-service-based offerings addressing specific security controls and market segments, such as small and midsize businesses (SMBs), over the next two years. All these factors will combine to increase pressure on marginal service providers, leading us to predict additional consolidation in the market, and lower overall revenue growth in 2011.

In 2009, MSSPs in North America generated revenue of $1.8 billion, representing growth of 24% over 2008, while the number of firewalls and intrusion detection and prevention (IDP) devices under monitoring/management grew more than 20%. We are predicting that revenue will have grown to $2.3 billion for 2010. Growth in enterprise demand for MSS is driven primarily by four factors:

- **Staffing and budget constraints:** Gartner's forecast for IT spending indicates a 3.2% growth rate in 2010. Gartner sees continued corporate pressure to reduce operational costs, capital expenditures and staffing, while maintaining a sufficient security posture and meeting compliance mandates.

- **Evolving compliance reporting requirements:** Gartner customers report continued efforts to stabilize and reduce the cost of meeting compliance requirements as they evolve, or as enforcement activities increase, such as Payment Card Industry (PCI) standards, Federal Information Security Management Act (FISMA) requirements for U.S. government agencies, Federal Financial Institutions Examination Council (FFIEC) requirements for banking, and for related activities such as privileged user monitoring or data protection. Gartner believes that increased federal efforts to drive suppliers to demonstrate compliance with FISMA, as well as increased Critical Infrastructure Protection (CIP) compliance (e.g., with the North American Electric Reliability Corporation — NERC), will add to this. In addition, there is a trickle-down compliance effect, in which companies are requested by their customers and business partners to have processes in place to monitor, identify and respond to security incidents.

- **Expansion of Internet connection points:** Enterprises are adding firewalls and UTM devices to remote locations as they move toward distributed Internet connections. In addition, the deployment of network intrusion prevention devices and the increased demand for remote security monitoring of servers have led to increased device count and contract value when renewing managed service agreements.

- **Growing experience with remote services for IT:** As enterprises gain experience consuming IT functions, such as applications, storage and processing as services, security outsourcing will become more routine. Gartner sees significant growth in security outsourcing in areas adjacent to MSS, such as secure Web gateways, e-mail security, and identity and access management. Related to this is the increase in the number of IT services organizations that are adding managed security to their offerings, thus giving their customers options to outsource security functions to vendors with which they already have trusted relationships.

Constraints to adding internal IT resources and regulatory compliance requirements can have more acute effects on smaller businesses, where security resources are often limited. Smaller firms outsource security activities to increase their security levels and to meet regulatory demands, and the most direct way of doing so is by extending their relationships with existing IT services providers that offer security services, and by bypassing a competitive selection process.

Return to Top

Supply of MSSPs Increases

The number of IT services firms offering managed security is growing. This is evidenced by the types of firms seeking to brief Gartner on their security service offerings, and by Gartner customers, who increasingly mention previously unknown MSSPs in discussions about prospective service providers. The range of security services of these newer entrants typically includes real-time monitoring and security information management and log management.

The growing availability of security information and event management (SIEM) products with features designed to support multitenant service delivery has lowered the barrier to entry for potential MSSPs. Every major SIEM product vendor is actively courting service providers as distribution channels for enterprise product buyers, and as MSSPs for businesses that prefer managed services over product deployment. However, there is more to being an MSSP than running a multitenancy SIEM deployment — enterprises should fully evaluate the MSSP's reporting, alerting and security intelligence feeds.

Security managers considering MSSs will improve their chances of a successful MSS engagement if they are explicit about their expectations of the quality and degree of interaction expected from an MSSP, and if they are diligent in investigating the service delivery capability of MSSPs. Prospective MSSPs should demonstrate the ability to deliver scalable, reliable, continuous services, and add value through security expertise related to the customer's security infrastructure and the threat environment.

For mainstream technology adopters or risk-averse organizations, security managers may need to balance the benefits of focused security expertise, service innovation, and the delivery processes of MSSP specialists with the established relationship and the leverage it may offer with an incumbent IT services provider that offers MSSs as well.

Return to Top

Pricing

Gartner expects that, during 2010-2011, pricing for common services, such as firewall and IDP monitoring and management, will continue to decline slightly. The more widespread availability of these services from IT

that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track 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 in order 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, 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, etc.

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 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 product 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 set as they map to current and future requirements.

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

outsourcing providers will drive price pressure, reflecting corporate budget pressure on IT spending. As the number of devices under management by MSSPs expands, per-unit pricing should decline as some of the economies of scale are passed on to customers. Pricing remains a strong vendor selection criterion for Type B (mainstream IT users) and Type C (risk-averse) customers, and Gartner sees Type A (technically aggressive) customers increasingly factoring in pricing for MSS vendor selection or renewal negotiations. Although per-device and per-user pricing will continue to decline, MSSPs can increase their average deal sizes as enterprises add additional devices under management and consume new service offerings.

There are several service trends related to pricing:

- **Compliance-specific offerings:** MSSPs are proposing services designed to meet compliance requirements — for example, monitoring server logs or payment systems, or providing Web application firewall services. These offerings are designed to obtain customers that are looking to meet those specific requirements at a low price (especially where PCI is the driving requirement), with the MSSP anticipating expanding the scope of services as customers gain familiarity and see value.
- **Virtualization:** MSSPs have ended their early experiments for virtualized device management and monitoring. Pricing for virtualized devices has largely stabilized at similar price points for CPE devices, with discounting for volume. Gartner believes that, over the long term, however, virtualization will drive per-node pricing down, but also present enormous opportunities for increased total "device" count.
- **"On demand" services:** This option is most often available for log management services (described in greater detail below), and allows the MSSP to omit real-time analysis (and analyst involvement) from the collection and storage of log data. Customers view data or run reports as needed. These services are priced much lower per data source than those that are subject to include real-time analysis.

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

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.

Return to Top

MSS Portfolio

In addition to the core services of monitoring and managing firewall and intrusion detection systems/intrusion prevention systems (IDSs/IPSs), MSSPs now offer a range of additional managed services:

Return to Top

Multifunction Firewall/UTM Services

MSSPs typically offer monitoring and management for UTM products that incorporate firewall, IPS, e-mail antivirus and anti-spam, and URL filtering capabilities in one device. These services typically target midsize customers seeking to address several security controls in a single device, managed by a single service provider. Monitoring and management services for these devices typically involve minimal security analyst interaction, and limited configuration changes and reporting, because the target market has limited internal resources to interact with the security operations center (SOC), and typically has a stable network environment. Some services will incorporate the cost of the multifunction firewall in the service subscription fee, allowing customers to use operating budgets, rather than capital budgets. Services often include packaging or reports and features to meet specific compliance requirements, and prospective customers for multifunction firewall services to meet compliance requirements should assess the ability of MSSPs to deploy and update devices with standard configurations that address those requirements.

Enterprises also take advantage of managed services for UTM devices to provide monitoring or management to remote-office or branch-office locations. These deployments are also characterized by a limited need for analyst interaction, and can be served by a limited number of standard configurations that the enterprise customer deploys to branch offices. Enterprises looking to use MSSPs for remote-office/branch-office device management and monitoring should assess the ability of MSSPs to provide alerting reporting that yields sufficient detail by location to the corporate security team.

In the SMB and enterprise remote-office scenarios, service providers may deploy their own technology, rather than a commercial multifunction firewall, to deliver the security functionality. This can result in cost savings compared with using commercial technology. Where the MSSP is able to quickly develop and deploy detection and protection capabilities to its own technology, this option can result in a stronger security posture. Customers evaluating MSSP-owned technology should ensure that the capabilities meet functional requirements, and that content updates by the MSSP are covered by service-level agreements (SLAs).

Return to Top

Web Application Firewall

Attacks against Web-based applications, as well as PCI requirements to address Web application security, have driven demand for MSSPs to add managed and monitoring Web application firewall (WAF) services. Typically, these include configuration and tuning, real-time monitoring of alerts, and reporting. Full life cycle support, including selection and deployment, availability management, maintenance and backup may be available as well. Gartner believes that WAF-as-a-service offerings from ISPs and others will compete effectively with CPE-based managed WAF.

Return to Top

Data Loss Prevention Services

The majority of MSSPs offer services for data loss prevention (DLP) technologies. Most service delivery for DLP is focused on product assessment, product selection and deployment, not on remote monitoring and management. Gartner expects that initial managed services for DLP will focus on limited-scope deployments in which the rate of false-positive alerts will be acceptable to the MSSP and the customer.

Return to Top

Security Information Management Services

It is now standard for MSSPs to offer security information management (SIM — or sometimes simply called "log management") as a service. Enterprises and smaller organizations, in many cases driven by compliance or internal audit requirements, have expanded the scope of security monitoring of their IT environments. MSSPs include the acquisition, storage and archiving of security logs from network devices, servers and applications. These services may be accompanied by differing degrees of device management, content analysis, reporting and workflow support from the service provider. These services represent an evolution in the MSS market, with important implications for MSS buyers, including:

- **Log management is not real-time monitoring:** SIM services typically offer limited or no MSSP analyst review of logs under the scope of SIM services. Customers run reports, identify potential issues, and initiate investigations and eventual remediation.

- **MSSPs can add more value to real-time monitoring than to SIM:** MSSP analysts can leverage their knowledge of the external threat environment, and the activities they see across the devices they monitor for all their customers, to provide expertise that warns or protects multiple customers. Because the internal activities of any one customer — i.e., system or application access, privileged user actions — are unique to that customer, the MSSP can't easily use information about those activities to help other customers.

Return to Top

MSSs and Security as a Service

Gartner defines "security as a service" as "security controls that are owned, delivered and managed remotely by one or more providers. The provider delivers the security function based on a shared set of security technology and data definitions that are consumed in a one-to-many model by all contracted customers anytime on a pay-for-use basis, or as a subscription based on use metrics." MSSs can be defined as "security as a service where an MSSP selects, owns and manages the technology that delivers the security function." This definition holds true whether the controls are based in the cloud, in the service provider's network, or on the customer's premises.

Gartner continues to see demand for services based on this delivery model, such as managed firewall services and distributed denial of service (DDoS) offerings from ISPs and telephone companies (telcos). Several MSSPs offer security as a service for firewall or IDP controls, vulnerability scanning, and, in a few cases, log management services. Security buyers considering security-as-a-service delivery options should, of course, assess functional capabilities, but must also address these other questions:

- **Customization:** Is the degree of customization offered sufficient to meet current and anticipated requirements?

- **Switching costs:** Does implementation of the controls increase "lock-in" with the provider, and result in higher costs to switch the function to another provider?

- **Availability and continuity:** What alternatives exist in case of service delay or interruption?

The trend toward competition for MSS renewal deals continues as buyers seek better pricing or better service delivery. Gartner expects a continuation of customers renewing or recompeting for MSS deals to try to keep costs from rising, even as they look at possibly expanding the services already under contract.

Return to Top

Offshore MSSs

As a remotely delivered service, the MSS can be delivered globally from SOCs located far from the security devices being monitored or managed. MSSPs with SOCs in multiple geographic regions worldwide have the option to deliver services to local customers from SOCs within a local region, or to move analysis and management workloads to other SOCs. Multiregion MSSPs approach this in one of two ways:

- **Division of labor:** MSSPs may staff SOCs 24/7, but segment specific types of tasks (such as monitoring activity and management activity) to different locations based on available skill sets, workloads and labor costs.

- **Follow the sun:** In this approach, the majority of monitoring and management work will be performed in SOCs during local business hours for those SOCs, and then be shifted to other SOCs as they enter their own "local business hours." This involves coordinating the transition of ongoing work, including open tickets and customers with active incidents.

Several large, global MSSPs have employed these approaches with mixed results (as validated by the service providers and by Gartner customers). The primary issues identified with *division of labor* include communication difficulties when offshore SOC staffs interact with North-America-based customers. These are addressed through hiring and training improvements, as well as by keeping customer-facing SOC activities in local regions, and by moving, for example, device management to offshore SOCs. The *follow-the-sun* model can be subject to transition difficulties that are especially notable when the SOC going off-shift is handling a critical customer incident.

For some organizations — especially those with multiregional operations, and those that already have relationships with service providers that have remote services based on offshore staffs — the location of SOC resources is a secondary consideration. For others, it is important to understand the remedies available from the MSSP, if they encounter communication or coordination difficulties based on the location of SOC personnel.

For most Gartner customers, the locations of the MSSP SOCs, support staff, management and sales force remain important because MSSs are a relationship sale, and local sales teams, presales support, consulting resources, location of sensitive data, and management availability carry weight in the selection process. Where the prospective customer is turning over control of the security technology from internal resources to the MSSP, the perception of loss of control can be mitigated by the ability to see the MSSP's facilities, meet the SOC staff, and engage in face-to-face account support. There are also geopolitical issues, where businesses realize that MSSPs with operations in certain countries may be forced to cooperate with government requests for surveillance of their customers. The USA Patriot Act and similar laws in other countries are inhibitors to location-independent outsourcing in general, and are even bigger issues in security outsourcing.

Gartner expects to see a continuation of the slow erosion of preference toward in-region SOC presence as customers become more familiar with security outsourcing, as MSSs are delivered by offshore service providers with which the customer already has a trusted relationship, and as MSSPs offer lower pricing based on offshore labor. However, MSSPs must address other potential concerns by providing more visible, documented and auditable evidence of service delivery to customers.

Return to Top

MSSP Landscape

The basic makeup of MSSPs has not changed fundamentally. Basically, there are three major types of MSSPs:

- **Pure plays:** Generally smaller, privately held MSSPs that are completely focused on security services.
- **System integrators/business process outsourcers:** Broad IT services providers that typically manage security devices as part of larger outsourcing deals.
- **Carriers and network service providers:** Bandwidth and connectivity providers that manage network security products and often provide cloud-based services on their end of the Internet connection.

In general, the MSS portfolios of these providers look similar, although there may be delivery options that are available to some providers, but not others (such as DDoS protection or carrier-network-based firewall services), and some MSSPs provide greater flexibility or customization of their offerings. However, not all customers have the same requirements or expectations of MSSs, and Gartner recommends that prospective MSS buyers develop explicit requirements for service delivery. These should include the degree and quality of interaction with the MSSP's SOC analysts, the usefulness of the MSSP's portal and reporting, the depth of threat and security intelligence offerings, support for specific compliance requirements, and the MSSP's professional service capabilities. Prospective buyers with multiregional deployment requirements, or those that require additional IT support from their security service provider, should evaluate MSSPs against those requirements as well. When prospective buyers evaluate MSSPs in the context of specific requirements, the providers that best fit those requirements will come from any segment of the Magic Quadrant: Leaders, Visionaries, Niche Players and Challengers.

Not included in this analysis are smaller, subregional providers, which can include small pure plays as well as larger providers that do not have enough MSS business to meet the criteria for inclusion. Excluded from this analysis are service providers that offer MSSs only for their own technology, and do not offer services for commercial technology.

Return to Top

Market Definition/Description

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

MSSs do include:

- Monitored or managed firewalls or IPSs
- Monitoring or managed IDSs
- DDoS protection
- Managed secure messaging gateways
- Managed secure Web gateways

- SIM
- Security event management
- Managed vulnerability scanning of networks, servers, databases or applications
- Security vulnerability or threat notification services
- Log management and analysis
- Reporting associated with monitored/managed devices and incident response

This research evaluates service providers that offer monitored/managed firewall and IDP functions, rather than those whose main focus is on other elements of the services listed above.

Return to Top

Inclusion and Exclusion Criteria

We have changed our inclusion criteria for this iteration of the Magic Quadrant for MSSPs, North America. The criteria now include a threshold for the number of firewall or IDP devices under monitoring or management, and a threshold for the number of North American customers. MSSs refer to remote management and monitoring of security technologies. Several large infrastructure outsourcing vendors offer other service delivery options, such as staff augmentation, in addition to MSSs. We don't evaluate those other delivery options, but we do note when the providers deliver the majority of their security monitoring or management services by those means. 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 technology.

Return to Top

Inclusion

- The ability to remotely monitor and/or manage firewalls and IDP devices from multiple vendors via discrete service offerings
- At least 1,000 firewall/IDP devices under remote management or monitoring for external customers
- At least 100 external customers with those devices under management or monitoring

Return to Top

Exclusion

- MSS offerings that are available only to end users that buy other non-MSSs
- Service providers that monitor or manage only their own technology

Return to Top

Added

The following vendors have been added to our evaluation:

- Nuspire Networks
- Allstream
- CSC
- HCL Technologies

Return to Top

Dropped

The following vendors were dropped from the Magic Quadrant:

- **Orange Business Services:** Orange offers a full range of MSSs, but did not meet the inclusion criteria for the number of customers and devices in North America.
- **Sprint:** Sprint offers in-the-cloud MSSs to its telecommunications customers and partners with CompuCom for CPE-based MSSs.

- **Tata Communications:** Tata Communications offers a full range of MSSs, but did not meet the inclusion criteria for the number of North American customers and devices.

Return to Top

Evaluation Criteria

Ability to Execute

- **Product / 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 includes MSS revenue, pricing, and the overall effectiveness of the sales channel. The level of interest from Gartner clients is also considered.
- **Market responsiveness and track record** evaluates the match of the MSS offering to the functional requirements stated by buyers at acquisition time, and evaluates the MSSP's track record in delivering new functions when they are needed by the market.
- **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 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 conducting qualitative interviews of vendor-provided reference customers, as well as feedback from Gartner customers 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.

Criteria weights for ability to execute are shown in Table 1.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	High

Source: Gartner (November 2010)

Return to Top

Completeness of Vision

- **Market understanding** involves the ability of the MSSP to understand buyers' needs and to translate those needs into services. MSSPs that show the highest degree of market understanding are adapting to customer requirements for specific functional areas and service delivery options.
- **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 MSS. Development plans are also evaluated.
- **Business model** includes the process and success rate for developing features and innovation and service delivery capabilities.
- **Vertical, industry 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.

Criteria weights for completeness of vision are shown in Table 2.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Low

Source: Gartner (November 2010)

Return to Top

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 generally 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, portal-based correlation and workflow support, and flexible reporting options.

Return to Top

Challengers

Gartner customers are more likely to encounter MSSs offered by an IT or network service provider in the Challengers quadrant as a component of that 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. These service providers also represent the largest portion of overall MSSP revenue.

Return to Top

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 requiring frequent interaction with MSS analysts, flexible service delivery options and strong customer service. Visionaries quadrant MSSPs have less market coverage and fewer resources or service options compared with Leaders quadrant firms.

Return to Top

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.

Return to Top

Vendor Strengths and Cautions

Allstream

Allstream provides telecommunications services to Canadian businesses. Security services offered include security architecture and technology deployment, in addition to MSSs. Allstream's service delivery is heavily weighted to multifunction firewall monitoring and management services, with some network-based firewalls. Like other telco MSSPs, Allstream is investing in the delivery of MSSs as a component of its networking services. Allstream partners with SecureWorks for the delivery of advanced security management, monitoring and SIM services.

Canadian firms seeking MSSs for multifunction firewalls or network-based firewalls, or those seeking to use an incumbent service provider for MSSs, should evaluate Allstream.

Return to Top

Strengths

- Allstream provides stand-alone and multifunction firewall capabilities that are positioned to address the needs of small to midsize buyers and large enterprises.
- Allstream customers can add MSS with a trusted incumbent service provider.
- Allstream undergoes annual SAS 70 Type II/CICA 5970 audits of its MSS operations.

Return to Top

Cautions

- Allstream's security portal provides limited functionality. Prospective customers with requirements for advanced security management/monitoring, reporting and SIM functionality should consider the services and portal capabilities that Allstream provides through SecureWorks.
- Allstream must continue to develop network-based security service delivery capabilities and focus on new client acquisitions for those services.

Return to Top

AT&T

AT&T offers a full range of MSS monitoring and device management services, including CPE and security-as-a-service offerings, in addition to other IT and telecommunications services. AT&T's acquisition of VeriSign's security consulting business has bolstered the suite of services available for its customers. AT&T continues to focus on establishing more security controls in its network, including wireless. Enterprises requiring a global service provider with a broad range of service offerings and deployment capabilities that include CPE and network-based options, or customers of other AT&T services seeking MSSs from a trusted and established provider, should consider AT&T.

Return to Top

Strengths

- AT&T's service portfolio includes network-based and CPE delivery options, and encompasses a broad range of services.
- The service capabilities acquired via VeriSign's consulting group should enable additional compliance-oriented MSS offerings.
- AT&T continues to leverage the capabilities of a global network provider in its MSS development and delivery, and maintains delivery leadership in security controls as a service.
- AT&T is a stable service provider vendor with a presence and delivery capabilities in multiple geographies.

Return to Top

Cautions

- AT&T's portal lacks features for asset reporting, log browsing and SLA reporting capabilities that are found among some competitors' offerings.
- While AT&T has worked on simplifying the pricing of network-based MSSs, there is an opportunity for improvement to give prospective customers greater ability to compare AT&T with CPE-based alternatives.
- AT&T's focus on cloud-based security services has affected its visibility to organizations seeking more traditional CPE MSSs. AT&T must do a more effective job of exposing CPE management and monitoring capabilities to MSS buyers.

Return to Top

Bell

Bell provides telecommunications services and a broad range of professional, hosted and managed services in the areas of network, video, contact center, customer experience and unified communications solutions, in addition to professional services and MSSs. Bell's security management services are weighted toward more-traditional account-based outsourcing delivery, rather than shared remote security monitoring, although Bell is increasing its capability for MSSs. Enterprises seeking an established vendor for MSS delivery in the Canadian market should consider Bell.

Return to Top

Strengths

- Bell is starting to improve its stand-alone MSS delivery capability, which should help address the needs of customers for which account-based outsourcing is not a good fit.
- Bell has strong delivery experience with the Canadian government.

Return to Top

Cautions

- Bell has not been as fast to introduce and establish remote MSSs as some of its competitors.
- Bell has not established itself in cloud services delivery as quickly as many of its telco competitors.

Return to Top

BT Global Services

BT's MSSs in North America have roots in the acquisition of Counterpane, an early MSSP pure-play vendor, as well as other MSSs that BT had offered before then. BT's MSS delivery capability across multiple regions is still fragmented into different groups within BT. Since the acquisition, BT has expanded the former Counterpane's SOC facilities in North America, but BT's appearances on Gartner enterprise customers' shortlists for MSSP deals have fallen off. BT has stated its intention to renew its efforts in the MSS market. Enterprise customers of BT's telecommunications and IT services should consider BT for MSSs.

Return to Top

Strengths

- BT has multiregion delivery capabilities and a broad range of security and IT services.
- BT SOCs undergo SAS 70 Type II audits and are ISO/IEC-27001-compliant.

Return to Top

Cautions

- BT MSS offerings need greater visibility to prospective enterprise security buyers (and to BT customers) to be considered for MSS-specific deals.
- Compared with other telecommunications provider competitors with MSSs, BT's in-the-cloud MSS offerings are less standardized and defined.

Return to Top

CGI

CGI provides MSSs as well as IT and business outsourcing, consulting, and system integration. More than 90% of CGI's business is in North America, and is split nearly evenly between Canada and the U.S. CGI focuses on government, financial services and insurance markets. Enterprises seeking MSS delivery capabilities in these vertical markets, and CGI IT services customers looking to add MSSs, should consider CGI.

Return to Top

Strengths

- CGI is well-established in the Canadian market, and has a growing presence in the U.S. market.
- CGI gets good marks for security expertise and for good security service delivery in the context of overall IT outsourcing.

Return to Top

Cautions

- CGI's current MSS portal is not as feature-rich as its competitors' portals, and its log management compliance reporting is not as comprehensive as many of its competitors'. CGI is in the process of upgrading its portal and regulatory reporting capabilities.
- CGI has not established itself as a visible contender in MSS-specific deals, outside of its base of IT outsourcing customers.

Return to Top

CompuCom

CompuCom offers the full range of IT outsourcing and other services, in addition to MSSs. CompuCom's MSS business is focused on compliance-driven financial services and retail vertical industries, but also includes customers in all major industry segments. Core MSS monitoring and management services are augmented by IP telephony security services. Customers of CompuCom's IT services that are seeking to add security services, and enterprises looking to meet PCI or financial compliance requirements, should evaluate CompuCom.

Return to Top

Strengths

- Customers give CompuCom good marks for security device management services.
- CompuCom delivery centers are ISO/IEC-27001-compliant.
- CompuCom has integrated its security portal into its IT service delivery portal, and provides extensive compliance reporting.
- CompuCom has several large channel partners providing SMB market access to managed security and compliance services.

Return to Top

Cautions

- CompuCom's focus on specific markets and its core IT services business makes it less visible to enterprise buyers looking for MSS-specific capabilities.

Return to Top

CSC

CSC provides a broad range of IT outsourcing and consulting services to enterprises and government agencies. CSC has offered security outsourcing and staff augmentation services for some time, and recently increased its efforts to grow its managed security business in the private and public sectors. CSC initially focused on the financial services and critical infrastructure markets.

Return to Top

Strengths

- CSC has extensive delivery resources for multiregional coverage for security services, as well as a wide array of other IT services.
- CSC's IT services customers can add MSSs with multiple service delivery options.
- CSC has a strong presence in the U.S. federal government and critical infrastructure markets.

Return to Top

Cautions

- CSC's focus on its core IT outsourcing and consulting businesses resulted in MSSs primarily focused on existing CSC customers. CSC is working on expanding its MSS-specific business.
- CSC's account-focused outsourcing heritage may impede the sharing of monitoring and response best practices across the MSS customer base.
- To reach a broader market, CSC must ensure that its MSS offerings and messaging resonate with the broader enterprise market beyond critical infrastructure and defense industrial base customers.

Return to Top

HCL Technologies

HCL is a large, India-based service provider with a small MSS business in North America. HCL provides a wide range of IT consulting, system integration and outsourcing services. HCL delivers MSSs from its U.S.-based SOC as well as its India-based SOCs. Enterprises that use HCL for IT services, and are seeking MSSs from an incumbent partner, should consider HCL.

Return to Top

Strengths

- Customers of HCL's broad range of IT services can add MSSs from a provider with which they already have a relationship.
- HCL's log management capabilities are a strong component of the overall MSS portfolio.

Return to Top

Cautions

- HCL customers report mixed results for MSS service delivery. HCL must leverage its security expertise and best practices across all its MSS accounts to improve its service delivery.
- Prospective customers should establish MSS-specific service-level requirements, reporting and remedies.

Return to Top

HP

HP's managed security capabilities have been augmented by acquisitions (e.g., EDS in North America and Vistorm in Europe), and delivery of MSSs is still segmented among various organizations within HP. In North America, most MSS customers are also customers of HP's IT outsourcing services. HP offers a broad range of professional and managed services for security. Recent technology acquisitions include TippingPoint in 2009 (network IDS/network IPS), Fortify Software in 2010 (application security) and ArcSight in 2010 (SIEM). Enterprise and midsize companies with HP IT services should consider HP for managed security.

Return to Top

Strengths

- As a large IT services provider, HP offers a wide range of managed security functions, as well as consulting and system integration services in multiple regions.
- Major data centers undergo a SAS 70 Type II audit.

Return to Top

Cautions

- Compared with competitors, the HP MSS portal lacks many correlation and reporting features (or has those features available only in Europe).
- HP must avoid service disruptions as it rationalizes its various MSS delivery organizations and service offerings across multiple regions.

Return to Top

IBM Security Services

IBM offers MSSs to customers of its infrastructure outsourcing services, and as a discrete offering. IBM has SOCs distributed worldwide, and offers extensive language support via portal and telephone. IBM's typical MSS deal includes device monitoring and device management, and IBM offers a broad range of security services beyond the core firewall and IDP devices, including Web gateway and e-mail managed services. IBM offers a cloud-based SIEM solution and supports customer premises technology from Tivoli. IBM Global Services includes extensive security consulting and integration services. IBM recently introduced an enhanced vulnerability assessment service that supports PCI reporting requirements. Enterprises with global service delivery requirements, and those with strategic relationships with IBM, should consider IBM for MSSs.

Return to Top

Strengths

- IBM has global delivery capabilities with a broad portfolio of MSSs, security consulting services and other IT services.
- The X-Force threat intelligence capability provides expertise to support MSSs, and is also available as a service offering to customers.
- New managed vulnerability assessment services bring IBM's managed vulnerability assessment offering on par with competitors' offerings, and includes Web application assessment.

Return to Top

Cautions

- Customers report uneven service delivery for MSSs. IBM must ensure that its extensive customer support resources are engaged across the breadth of the MSS customer base, and it must improve communication between customer support and operations.
- CPE log management technology support is currently confined to Tivoli, so customers seeking an MSSP to manage other CPE SIEM technology should validate that IBM's SIEM support road map meets their requirements.

Return to Top

Integralis

Integralis, based in Germany and with a strong U.K. presence, has had a relatively small MSS business in North America for several years. In 3Q09, NTT Communications announced its intention to acquire control of Integralis in 2010. Early indications are that Integralis will provide MSSs to NTT customers, in addition to Integralis' existing MSS customer base. Enterprises looking for MSS capabilities to augment infrastructure management services from a provider with service presence in multiple regions should consider Integralis.

Return to Top

Strengths

- Integralis has service presence in multiple regions, including two U.S. SOCs.
- Integralis gets good marks from customers for responsiveness and security expertise.
- Integralis exhibits flexibility in meeting customer requirements for MSSs.

Return to Top

Cautions

- The Integralis portal displays normalized incident data, but does not provide browsing display of raw log messages.
- The log management services offered by Integralis are not as rich as those from competitors, and, by comparison, they lack compliance reporting capabilities.
- Integralis must work to maintain MSS delivery quality during the NTT acquisition process. NTT also acquired Dimension Data and Nordic provider Secode, so customers should request updates to understand the plans for MSSs and IT outsourcing activities among these various entities.

Return to Top

Nuspire Networks

Nuspire offers managed security, network gateway and help desk services. Although Nuspire's primary delivery model is the monitoring and management of its own technology, it also provides MSSs to customer-owned technologies. Nuspire's services are composed mainly of multifunction appliance monitoring and management. Other services include endpoint security, log management services and help desk. Vulnerability scanning services are available via professional services. Nuspire has tapped a niche of automotive retail customers. MSS prospects looking for services that can be quickly deployed at multiple locations, such as branch offices or retail, and can be bundled with help desk and network services, should consider Nuspire.

Return to Top

Strengths

- The delivery model and pricing of Nuspire's MSS is well-suited for SMB customers looking for multiple security controls in a fully managed offering.
- Nuspire has established several distribution partners that provide access to an existing market of

potential customers with similar requirements.

- Nuspire gets good marks for meeting service commitments and flexibility in implementing delivery.

Return to Top

Cautions

- Nuspire's current direct sales approach provides limited access to the enterprise market, and to SMB markets outside the automotive retail channel.
- Nuspire's security portal lacks features related to managing and correlating vulnerability assessment results that are available from competitors' portals.

Return to Top

Perimeter

Perimeter's primary market for its MSS is small and midsize banks. Perimeter recently experienced top management changes, and consequently added technology development resources to expand its offerings, delivery options and target markets. Perimeter offers a wide variety of MSSs and related security services via several delivery modes, including hosted, as-a-service and CPE monitoring/management. Current customers are typically compliance-focused and have very limited internal security resources. SMBs looking for MSSs with a wide range of security services to assist with meeting compliance requirements, and SMBs requiring easy deployment options and a relatively low-touch relationship with the service provider, should consider Perimeter.

Return to Top

Strengths

- Perimeter gets good marks for device management and for customer care, and has shown consistency in upgrading services.
- Perimeter offers a broad suite of compliance-oriented services for customers subject to banking regulations.

Return to Top

Cautions

- Compared with its competitors' portals, Perimeter's portal lacks the capability to present correlated data and SLA performance.
- Perimeter will need to improve its marketing and sales efforts to gain visibility and traction in the broader midsize enterprise market.

Return to Top

Savvis

Savvis sells MSSs primarily to its base of network, hosting and cloud services customers, although it also provides MSSs for CPE, and for customers that do not have its other IT services. MSS offerings include log management, network-based firewall and DDoS protection, in addition to core firewall and IDP services. Customers of Savvis' hosting or network services should consider Savvis for MSSs.

Return to Top

Strengths

- Savvis is able to credibly position security services alongside its other IT virtualization and cloud services that are focused on cost reduction.
- As a network service provider, Savvis is able to offer security controls embedded in the network, including DDoS protection as a service.
- Savvis' security expertise is enhanced by its Arca Common Criteria Testing Laboratory.

Return to Top

Cautions

- Savvis' security portal lacks some correlation capabilities and SLA reporting compared with competitors' portals.

- Because most of its MSS business is delivered to its existing IT and network service customers, Savvis' security offerings are targeted to the requirements of those customers, rather than enterprises seeking MSSs as a discrete service offering.

- Savvis' focus on delivering MSSs to hosting and cloud infrastructure customers via direct sales means it is less visible to prospective customers that are only looking for MSSs.

Return to Top

SAIC

SAIC offers IT outsourcing, integration and consulting services in addition to security services. Enterprises with MSS deployments that will involve significant implementation and integration work should consider SAIC's strengths in delivering those services, as well as its ongoing monitoring and log management capabilities.

Return to Top

Strengths

- SAIC's security service capabilities are well-known in the U.S. federal government market, as well as in commercial markets concerned with critical infrastructure security.

- SAIC's security expertise is augmented by a strong professional service capability and by its Common Criteria Testing Laboratory.

Return to Top

Cautions

- SAIC's MSS capabilities have a low level of visibility to Gartner clients outside of government and selected large enterprises.

Return to Top

SecureWorks

SecureWorks offers security monitoring, device management, scanning, and log management for third-party technologies and its own appliances, and targets enterprise as well as midsize organizations. Delivery models include CPE-based services and "as a service" delivery for monitoring and log management. In December 2009, SecureWorks acquired dns, a U.K.-based provider of managed security and consulting services, which adds a U.K. presence to SecureWorks' operations. SMBs seeking to meet compliance requirements, and enterprises looking for full-featured MSSs, should consider SecureWorks.

Return to Top

Strengths

- SecureWorks continues to get high marks from Gartner customers for maintaining high standards of service delivery and security expertise, while integrating acquired firms and customers into ongoing operations.

- SecureWorks has established very good visibility in the MSS market, and is included in a large number of MSS evaluations, with larger and smaller competitors, by Gartner customers.

- SecureWorks offers services based on customer-owned technology or its own technology, which provides flexibility for pricing and delivery models.

Return to Top

Cautions

- SecureWorks must continue to align and rationalize service delivery among its MSS customers, and among those acquired from VeriSign and dns.

- SecureWorks needs to improve its ability to provide services in the Asia/Pacific region to support North-America-based enterprise customers with a presence in Asia/Pacific.

Return to Top

Solutionary

As a pure-play MSSP, Solutionary offerings focus on security monitoring, information management, compliance and vulnerability assessment. Solutionary also offers security consulting services. Solutionary has two SOCs in the U.S. and partners with e-Cop to support local MSS delivery in the Asia/Pacific region. Enterprises and midsize businesses that need customizable MSS delivery for firewall, IDS, IPS, WAF, next-generation firewall, scanning and log management services should consider Solutionary.

Return to Top

Strengths

- Solutionary gets good marks from customers for service quality and for flexibility in its service design, delivery and SLAs.
- Solutionary has made progress in developing channel sales capabilities to augment its direct sales.
- Solutionary's main SOC undergoes SAS 70 Type II audits, as well as additional security audits.

Return to Top

Cautions

- Solutionary must continue to grow its channels to reach the midsize market.
- Solutionary must continue to sharpen its efforts to gain the awareness and attention of enterprise MSS buyers.

Return to Top

Symantec

Symantec provides security monitoring and security intelligence services, messaging security services, and a range of security software products. In addition, log management services are available through a customer-premises deployment of Symantec Security Information Manager as a hosted service. Symantec's traditional focus on the enterprise full-service MSS market has expanded to include midsize buyers with more compliance-oriented requirements. Symantec has decided to rely increasingly on channel partners for a consulting capability, rather than increasing its own capabilities. Enterprises seeking an established MSSP should evaluate Symantec.

Return to Top

Strengths

- Symantec gets high marks from Gartner customers for service delivery and the security expertise of its SOC staff.
- Symantec very often appears among the finalists in MSS evaluations by Gartner customers, and has become more competitive and flexible on pricing and service packaging.

Return to Top

Cautions

- Notwithstanding its recent moves to better integrate MSS procurement within broader Symantec licensing programs, Symantec must continue to streamline its sales/procurement processes to make it easier for customers to acquire products and services.
- Symantec's decision to rely increasingly on partners for consulting services may provide leverage to competitors that offer MSSs and security consulting services.

Return to Top

Trustwave

Trustwave's MSS has been largely focused on PCI compliance requirements, and the typical customer for Trustwave MSS is a midsize or smaller merchant, or a larger enterprise with retail locations. Trustwave has acquired several technology vendors offering products for encryption, network access control, WAF, DLP and SIEM, and is bringing these technologies to its MSS offerings. Trustwave has also acquired an enterprise SIEM product and intends to integrate it into its MSS, as well as support enterprise product sales. Companies with PCI compliance requirements should consider Trustwave for MSSs.

Return to Top

Strengths

- Trustwave has a variety of MSS offerings based on its own technology, brought in via acquisitions over the past several years.

- The addition of the Intellitactics SIEM has provided Trustwave with an opportunity to address a market organization with security operations requirements for real-time monitoring and log management via MSSs or product offerings.
- Trustwave's business relationships with credit card payment processing channels, and its aggressive pricing, give it broad reach across the lucrative PCI service market.

Return to Top

Cautions

- Trustwave's various technology acquisitions must be integrated into its MSS delivery capabilities without resulting in negative effects on its existing service levels.
- Providing managed services and providing product are two distinct businesses. Trustwave must balance resource allocation to maintain MSS and product development activities for its SIEM product.

Return to Top

Unisys

Unisys delivers MSSs and IT infrastructure outsourcing, system integration and consulting services to commercial and government organizations. Unisys' monitoring and log management services are delivered via a "follow the sun" model that engages SOC staff worldwide during local first-shift hours. Enterprises or government agencies seeking to add MSSs to infrastructure outsourcing should consider Unisys.

Return to Top

Strengths

- Unisys offers MSSs in concert with IT outsourcing and consulting capabilities.
- Unisys maintains SAS 70 Type II and ISO/IEC 270001 certifications at its operations centers.

Return to Top

Cautions

- Unisys must better differentiate its MSS offerings for commercial customers from its services directed at governments and critical infrastructure industries.

Return to Top

Verizon Business

Verizon Business offers a full suite of MSSs, including denial-of-service protection and compliance services, as well as a strong consulting practice. Verizon has leveraged its position as a major telecommunications provider to augment MSSs with services based in the network cloud, as well as services supported by its core network management and monitoring activities. Enterprises looking for an established service provider capable of delivering a broad range of security services in multiple regions should consider Verizon Business.

Return to Top

Strengths

- Verizon is leveraging its position as a large ISP to augment its MSSs with security-as-a-service offerings, in addition to more traditional CPE-based offerings.
- Verizon has been successful in competing for discrete MSS deals against pure-play MSSPs.
- Verizon gets high marks from Gartner customers for service delivery and security expertise.

Return to Top

Cautions

- Verizon must balance its approach to MSS packaging and pricing to meet the needs of its large enterprise customers, and of midsize buyers seeking stand-alone MSS engagements.

Return to Top

Wipro Technologies

Wipro is an India-based service firm with four SOCs in the U.S. and additional service delivery from India. Wipro offers a wide range of IT services in addition to security services; it also offers more traditional outsourcing and staff augmentation for security, in addition to a growing MSS business. Wipro is most visible in financial services and telecommunications markets. Enterprises looking to augment IT services with MSSs from a trusted incumbent provider should consider Wipro.

Return to Top

Strengths

- Wipro gets good marks from customers for device management, and for going above and beyond contractual minimums for service delivery.
- Wipro customers of other IT services can leverage their existing Wipro relationship to add MSSs or other security services.

Return to Top

Cautions

- Wipro's security management and monitoring services are still heavily account-based, and customers should request service commitments for MSS delivery that reflect cross-customer security intelligence and insights.

Return to Top

The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.