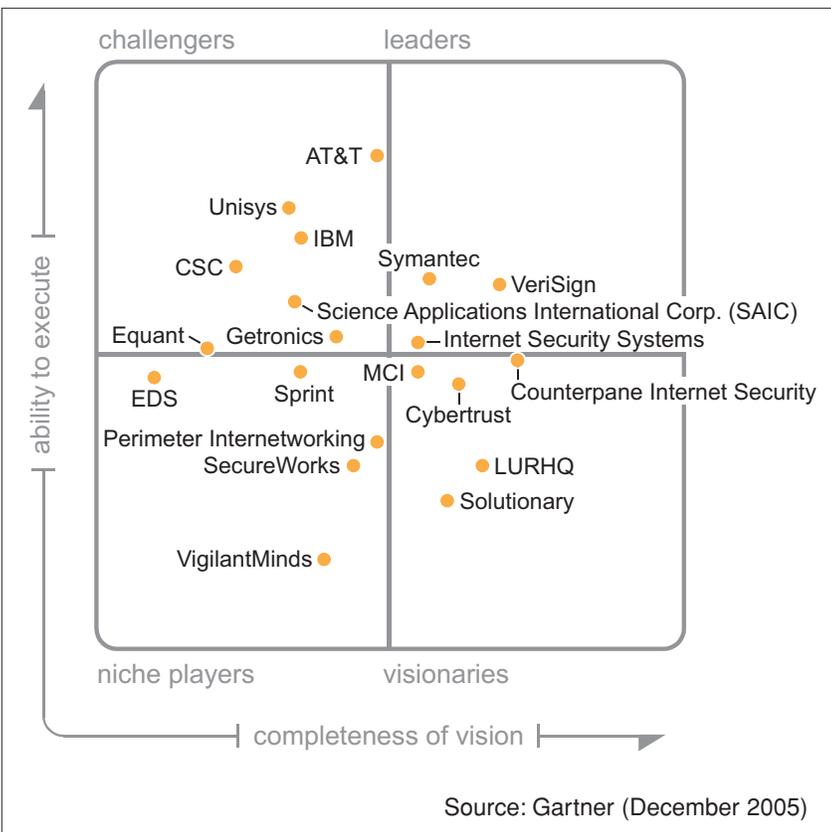# Magic Quadrant for MSSPs, North America, 2H05

The 2H05 Magic Quadrant for managed security service providers in North America shows the effects of continued market maturation. Merger and acquisition activity, as well as the expansion or contraction of service offerings, has changed the ratings of several vendors.

Market Overview

The managed security service (MSS) market in North America generated revenue of $936 million in 2004, and Gartner estimates revenue will reach $1 billion in 2005. Market growth has been accompanied by two waves of consolidation since 2001. In the first wave, smaller companies merged to increase devices under management or to gain customers. More recently, the trend is for larger

> **WHAT YOU NEED TO KNOW**
> When evaluating managed security service providers (MSSPs), begin with a clear set of requirements for device monitoring and management, vulnerability assessments, scanning, and incident management and reporting. Compare your requirements with customer premises equipment (CPE) product-based services and in-the-cloud (ITC) services. Consider current or pending IT or network outsourcing arrangements, and evaluate MSSPs from all quadrants against your requirements.

solution providers to acquire security service "pure plays," such as MCI buying NetSec and Getronics obtaining RedSiren's assets. Larger vendors buy pure plays to gain the security expertise (personnel and infrastructure) and to use the "specialist" pedigree of the smaller players.

The acquisitions are one indication of the continuing maturation of the MSS market, in which growth is driven increasingly by the following:

- More activity in outsourcing basic security operations, with a strong focus on firewall management and intrusion detection system (IDS) monitoring and with an interest in intrusion prevention system (IPS) functions in the future

- Compliance concerns because government regulations, as well as payment card requirements, are driving interest in MSS that can provide documented processes and in reporting that spans vulnerability management cycle activities

- An increasing requirement for more-frequent vulnerability scanning delivered as a subscription service and as part of a larger monitoring effort,

MAGIC QUADRANT
Figure 1. Magic Quadrant for MSSPs, North America, 2H05

Source: Gartner (December 2005)

rather than as a one-time professional services engagement, and as an alternative to maintaining tools and expertise in-house

Several vendors are actively developing (and LURHQ has announced) security information and event management functionality through their portal technology that will allow customers to use the service providers' data aggregation, normalization and categorization capabilities for reporting only. This allows customers to address specific reporting needs for devices or systems that don't require 24x7 monitoring. This approach allows MSSPs to extend existing infrastructure into new revenue lines and reach deeper into existing accounts to devices that support compliance reporting rather than active monitoring. It also gives them a "walk away" offering for prospects that will not outsource security monitoring.

In addition, several pure-play providers are piloting efforts to offer monitoring services based on ITC security devices hosted by telecommunications providers. These services could be offered as a "powered by" solution that exposes the MSSP to the ISP customers, or as an original equipment manufacturer solution in which the ISP handles customer interface. ITC services will allow telecom players to provide more-potent competition to established MSSP pure plays, but the telecom players have been slow to make the required business investments and market education efforts to move forward.

Gartner also sees increasing competition for MSS renewal deals. A growing number of clients we've spoken with are approaching the end of their MSS outsourcing contract and want renewal bids from competing MSSPs. They are, typically, satisfied with the service received. Their interest in competitive bids is driven by a requirement to maintain their service levels but reduce their MSS costs, or by a desire to increase their service levels and maintain their spending levels. Smaller stand-alone MSSPs continue to face challenges in acquiring large contracts from large companies that are looking for transparent financials and global support presence.

Market Definition/Description

An MSS includes remote, subscription-based monitoring and/or management of firewalls, intrusion detection and prevention functions via customer-premises-based or network-based devices.

Inclusion and Exclusion Criteria

To be included in this Magic Quadrant, an MSSP must have:

- More than 200 customer devices under management or monitoring
- The ability to organically monitor and/or manage firewalls
- IDS and IPS devices via a discrete service offering
- Reference accounts relevant to Gartner customers in North America

Vendors that have MSS offerings, such as distributed denial-of-service protection (Prolexic Technologies) or vulnerability scanning (Qualys), but not device monitoring and management are not included in this Magic Quadrant. Others, such as Savvis, offer MSS primarily to hosting customers, with limited offerings to others. As these providers expand the scope of

their MSS offerings, they may be included in future Magic Quadrants. NetSolve was removed from the Magic Quadrant after it was acquired by Cisco Systems. MSS is not a focus for Cisco Managed Services.

Added

We have added Perimeter Internetworking and VigilantMinds to the 2H05 Magic Quadrant.

Dropped

We have dropped Cisco (NetSolve) from the 2H05 Magic Quadrant.

Evaluation Criteria
Ability to Execute

Completeness of Vision

Criteria weights for completeness of vision are shown in the table below.

Leaders

Each of the service providers in the Leaders quadrant have significant "mind share" among enterprises looking to buy an MSS from pure-play security vendors, and they generally receive positive reports on service and performance from Gartner clients.

Challengers

Gartner customers are far more likely to encounter an MSS offered by a service provider in the Challengers quadrant as a component of that vendor's other telecom, outsourcing or consulting services. While 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 MSS and use the vendor's main services. It also represents the largest portion of overall MSSP revenue.

Table 1. Ability to Execute Evaluation Criteria

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

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	standard
Sales Strategy	standard
Offering (Product) Strategy	high
Business Model	standard
Vertical/Industry Strategy	standard
Innovation	high
Geographic Strategy	low

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.

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.

Vendor Comments

AT&T

AT&T continues to focus on security services, with the result that the company is often in the mix of vendors mentioned by Gartner customers as shortlist providers. AT&T's ITC offering complements the more-traditional CPE-based offerings. The company has taken aggressive steps to demonstrate a distinct MSS offering that takes advantage of AT&T's visibility into Internet backbone traffic and advanced intrusion prevention capabilities. AT&T is being acquired by SBC. As with any acquisition, customers should be vigilant that they continue to receive acceptable service levels during and after the acquisition.

Counterpane Internet Security

Counterpane has improved mind share among enterprise security managers and once again winds up on shortlists for MSSP buys. By adding professional services, device management and additional device monitoring capabilities, Counterpane has demonstrated that it is listening to market demands for broader offerings and flexible buying options. The company has stepped up its direct sales approach, which is key to winning larger-enterprise deals. Counterpane's challenge is to find a European partner channel and delivery partner to replace Getronics.

CSC

CSC has announced that Symantec will take over much of the security device monitoring that CSC had been performing. CSC will continue to deliver other security services. Partnering with a pure-play MSSP is not an unusual arrangement for a larger service provider, but it does introduce an additional responsibility to ensure that the arrangement is transparent to customers and results in better service delivery or lower cost. CSC's organic MSS efforts are largely oriented toward government contracts.

Cybertrust

Cybertrust was created from acquisitions and mergers between TruSecure, Ubizen and Betrusted. Ubizen's MSS architecture will deliver the MSS. Gartner has seen no evidence of customer defections or decline in service levels following the merger, although Gartner has seen greatly reduced feedback from the marketplace about Cybertrust. This demonstrates the challenge Cybertrust faces in staying focused on MSS (other than managed public-key infrastructure services), given the need to integrate several businesses, in several markets, that have a very broad range of product and service offerings.

EDS

EDS offers managed firewall and IDS services primarily to customers of its other infrastructure outsourcing services, with limited capabilities to deliver discrete MSS offerings. To be considered a top-tier MSSP, EDS must find a way to use the relatively large number of devices it manages to develop a discrete, visible and credible security service.

Equant

Equant has broadened its MSS offerings, but this has mostly helped the company reach parity with its competitors. Equant does have strong global reach, however, and it generally receives high marks for support.

Getronics

Getronics acquired the assets of RedSiren. Prior to the acquisition, RedSiren had been largely absent from MSS deals involving Gartner customers. Its acquisition by Getronics gives current and prospective customers greater assurance of financial stability. Getronics faces challenges in establishing a security brand for MSS that is distinct from its other IT outsourcing business, yet builds on Getronics' global service delivery capability.

IBM

IBM sells MSS as a component of its strategic outsourcing offering and as a stand-alone offering. Over the past year, IBM has only slightly improved the visibility of its MSS in the marketplace, in which it typically does not compete with smaller pure-play vendors. Feedback from current and prospective customers indicates IBM needs to address the "stovepiping" of security data and provide a more-integrated view of this data by improving its portal and reporting tools.

Internet Security Systems

Internet Security Systems (ISS) has begun to officially support non-ISS monitoring products as part of its MSS offering. The company has also improved its portal functions and reporting capabilities, and it has begun integrating its X-Force intelligence and improved scanning capabilities into its MSS offering. ISS has been working on its operational systems, which has resulted in additional service delivery capabilities. However, as a major IDS and IPS product vendor, ISS faces the same channel conflict that Symantec does. ISS needs to reinforce its messaging to potential customers to distinguish its service capability from its competitors' products.

LURHQ

LURHQ continues to improve its portal and back-end reporting capabilities to address security operations, management and reporting. The company has added in-the-cloud Security Information and Event Management (SIEM) managed service, and it has begun to build a professional service capability and improve its sales presence.

MCI

MCI completed its acquisition of NetSec in February 2005. NetSec remains the security brand for MCI security services. NetSec's capabilities for CPE-enabled services, including an improved portal capability, give MCI a better story for security services and complement MCI's ITC. MCI must ensure it maintains service levels as it aligns operations from its original MCI customers, those from its VeriSign partnership and those from NetSec. MCI must also demonstrate that it can focus on security services as a customer-facing business that is distinct from internal security operations. MCI is being acquired by Verizon. As with any acquisition, customers should be vigilant that they continue to receive acceptable service levels during and after the acquisition.

Perimeter Internetworking

Perimeter Internetworking offers ITC services to the midsize financial service provider market, as well as CPE-based services to small-and-midsize-business (SMB) buyers through ISP channels. Perimeter has had success gaining customers in vertical SMB markets in which reference accounts are important. The company is expanding beyond those vertical markets via partners and acquisition.

Science Applications International Corp. (SAIC)

SAIC has consolidated several security service operations into a more-unified MSS offering. This should make it somewhat easier for enterprises to engage with SAIC for security services, although commercial prospects perceive SAIC as being government-focused. SAIC must continue to refine its offerings and messaging to ensure that its MSS offerings address the security requirements of the commercial marketplace.

SecureWorks

SecureWorks focuses on the financial service provider market with an all-in-one CPE appliance-based model. SecureWorks has gained customers primarily via direct sales to a close-knit market in which "reference-ability" counts, and the company is expanding its partner focus to expand beyond those markets to those in which it has not yet established a reference base.

Solutionary

Solutionary has a well-rounded MSS offering that augments device monitoring and management with scanning, database and application monitoring, and professional services. Solutionary's focus on the midmarket and nonpublic ownership put it at the periphery of vendors that Gartner customers focus on for MSS. Solutionary needs to continue to align itself with national (and global) integrators and solution providers as service partners.

Sprint

Sprint, like its telephone company competitors, offers CPE-based services, as well as ITC services. Sprint has not advanced its service offerings or portal capabilities at the pace its competitors have, and as a result the company has struggled to get mind share for MSS beyond its government customers and bandwidth customers.

Symantec

Symantec has kept the core service capabilities it acquired with Riptech and augmented them with the consulting services it acquired through the @stake deal. CSC announced in February 2005 that it will use Symantec for security device monitoring for CSC MSS customers; we expect that Symantec will pursue and find success with more of these types of opportunities. While Symantec continues to maintain vendor neutrality for its MSS offering, and feedback from Gartner customers for the most part backs this up, inherent channel conflicts continue to be a negative for Symantec when competing with VeriSign and other MSSPs that do not sell competing products.

Acronym Key and Glossary Terms	
CPE	customer premises equipment
IDS	intrusion detection system
IPS	intrusion prevention system
ISS	Internet Security Systems
ITC	in-the-cloud
MSS	managed security service
MSSP	managed security service provider
SAIC	Science Applications International Corp.
SMB	small and midsize business

Unisys

Unisys has moved beyond its initial government contract focus for its MSS business. The company has experienced some success with midsize financial service companies and where it can sell MSS into an existing customer base.

VeriSign

VeriSign has successfully integrated Guardent from the 2004 acquisition, keeping a product-neutral approach and expanding the device-management and monitoring options. In addition to direct sales to large accounts, VeriSign has had some success developing a "powered by" strategy serving other service providers. VeriSign's acquisition of iDefense gives the company competitive security intelligence offerings similar to Symantec's Threat Management System.

VigilantMinds

VigilantMinds offers ITC as well as CPE-based services, and it has developed offerings that target the hospital market. VigilantMinds must address the dual nature of its efforts to offer premium CPE-based services to midsize and large customers while using its ITC solution to reach a broader segment of the market.

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, and so on, 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, 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 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 Web site, 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.
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.