Managed Services

By Counse Broders
Internet/Managed Services
November 2004

Market Definition

Security plays a factor in protecting corporate information. With companies increasingly reliant on interconnected machines that span communication networks across geographies, risks increase for data to be vulnerable to espionage, corporate spies, and hackers. This market assessment on managed security examines managed outsourced services and technologies, such as intrusion detection services, authentication services, hosted application security, and other managed security offerings. These can be offered by a variety of companies, ranging from small niche players to national and global providers. Focus is on managed security offerings as a service, not as custom-managed products that cannot be replicated for other firms. Managed security services reduce the cost and labor of security for enterprises and networks and improve the efficacy of network security.

While network security has been a primary concern of the telecom market since the first circuit-switched networks began to take shape, with the IP evolution, managed security has developed significant traction. In particular, online strategies have expanded beyond the capabilities and capacities of the in-house IT staffs. In addition, the growing number of small and medium-sized enterprises (SMEs) tackling online strategies is providing a rapidly growing market for managed security providers.

Market Review

• Merger Mania: The consolidation effort continues, as more companies look to grab share, reach, and more by combining efforts and bringing it all under one roof. In September, Symantec acquired several UK-based companies, including @stake and LIRIC Associates, to expand its security consulting business. TruSecure, Betrusted, and Ubizen in September announced their merger and rebranding under the Cybertrust name, providing a new threat on the global security stage; the new company will have 1,000 employees, 4,000 global clients, and $160,000,000 in annual revenue. In October 2004, Computer Associates acquired Netegrity, which makes access control and identity management products.

• VoIP Emerges in the Security Market: As competitors jockey for positions in the managed security space, some are looking in new directions for revenues and opportunities to expand their business. In October, RedSiren introduced its managed service for voice over IP (VoIP), designed to secure voice services that are converging within IT infrastructures. It also signed its first VoIP client. ISS also supports VoIP security with its Proventia appliances, which parse and analyze VoIP protocols for anomalous traffic.

• Partnerships and More: Efforts are underway to provide better synchronization among security players to ensure stronger client protections. IBM and Cisco Systems are working together on security measures. IBM's Tivoli software will enable products to work with Cisco network gear and Cisco's Network Admission Control program to scan devices that are attempting to connect to a network to ensure compliance with network security policies. The move will help better secure customer networks from worms and viruses. Finally, in August WilTel announced it was partnering with VeriSign to bring a suite of preconfigured managed security services to market.

• Moving Security Upstream: Carriers are looking to their networks to provide a measure of differentiation in the security wars. Sprint in October announced two new Internet protection and mitigation additions to its security services portfolio for companies, and will address threats to business, including denial of service, malicious code, e-mail-borne viruses, and unauthorized access. AT&T already has its Internet Protect service, which it has been heavily advertising with its “Trojan Horse” campaign in media and print. Both are efforts to move security monitoring and prevention upstream into the network, and away from the customer premise, making it easier to stop security issues from reaching clients.

• E-mail Targets: Service providers have heard the hue and cry among clients over e-mail security issues, and several have looked at solutions to ease the burdens of IT staffs. In September, McAfee extended its online managed services portfolio with McAfee Managed Mail Protection to provide a secure content management offering to allow for integrated anti-spam and anti-virus capabilities in an automated e-mail managed service for SME clients. Also in September, Equant rolled out a managed e-mail archiving solution, hoping to match AT&T vendor for vendor with its own EMC partnership and up the ante with its global support. It could be an interesting play, given complex country regulations on communication archiving.

• Addressing Security Awareness: Businesses continue to need educational efforts to ensure that all employees are trained in matters of security. Symantec announced in September availability of the Symantec Security Awareness Program, providing a new set of training and communication tools to companies. Its program is designed to help companies meet regulatory requirements for employee security awareness training, reduce vulnerabilities, and create a more security-conscious workforce.

Near-Term Market Drivers

• Organic Growth and More: Major security players are looking to gain size with added services and clients. Some are using acquisitions to gain scale quickly. This will also mean that players will see new expectations from clients as competition continues to percolate. Other players are also looking to gain better market reach, customer bases, and opportunity to reach users.

• Client Resource Constraints: End users are facing tight budgets, which in turn is pushing some companies toward outsourced security solutions that can deliver the necessary data protection without the heavy cost of doing it themselves. This may also drive the integrated security application, as vendors and service providers look to bundle more into their solution. It can also offer better cost management and the ability to “rent” some aspects of managed security solutions, which reduces capital requirements for end users.

• Training to Understand: Clients continue to require better understanding of the dangers of lax security. Providers can deliver this with training, information resources, and support. Clients have an innate sense that in this new world, security is critical, but sales reps and others must be able to communicate to a client what is important in a security risk assessment. Those that can do this well will be able to grab market share.

• Security Planning: One of the biggest near-term drivers for end-users is understanding security risks. Client security planning has to start by looking at vulnerability assessments, security need consulting, and

ongoing environment assessments. In some cases, this is becoming necessary to fulfill legislative requirements.

• Legal Issues: Government legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, are driving the health care and financial sectors to protect crucial data. In order to meet government standards, users often turn to outside companies for this security. The California Database Security Act is also fueling challenges for companies doing business in that state, which often means stepping up security efforts nationally as a result. Furthermore, corporate liabilities and penalties are boosters to get executive attention and action to meet SBO, SEC, and FDIC guidelines.

• Proactive to Preventative: From proactive SLAs that leave the onus on the service provider to understanding what is happening to a user in real time and comparing that against other users, the industry is shifting from reactive services to those that can ensure a greater level of prevention for clients.

Long-Term Market Drivers

• Cost and Complexity for Security Rise: As Web business models become increasingly complex, the security solutions grow more tangled for users. Businesses building online strategies from scratch can be overwhelmed by the initial investment of security solutions, while those trying to adapt existing solutions to evolving security concerns are besieged by maintenance costs. Like the classic Gordian knot, managed security providers can cut through the complexity to make things easy for clients.

• Device and Security Integration: While security used to be thought of as an "add-on" or an extraneous component of infrastructure, equipment makers are paying much closer attention to imbedded security functionality in devices and are actively attempting to integrate security as a value-added service. Furthermore, vendors are looking to unite service providers with standards programs that simplify client understanding and reduce the complexity of product buying.

• Knowledge Database Resources: One of the key resources for security analysts and those actively monitoring security is a knowledge database of attack patterns and other descriptions of the enemy. It saves reinventing the wheel and provides a faster response to known threats. Service providers can provide significant value from the spectrum of clients they support, gaining synergy from the shared information tracked in these databases.

• Trust Issues: End-users — whether they are corporate users putting a business plan on a server or a consumer buying a CD — have ingrained habits that they are not necessarily willing to give up. For example, no matter how good an online bank's security system is, a consumer will have to be convinced that its services are not only as good as a brick and mortar bank's services, but better. Security providers that can ensure a consistent message that they can be trusted can help win accounts.

• Addressing Social Engineering: Clients still face the security risk that employees represent just through the human desire to be helpful, and hackers exploit this through “social engineering.” A component of managed security will need elements of employee training to build awareness of outside threats.