Advisory Report

Managed Security Services Update: It Just Got Better

January 11, 2012

Amy DeCarlo
Current Analysis
Principal Analyst, Security and Data Center Services

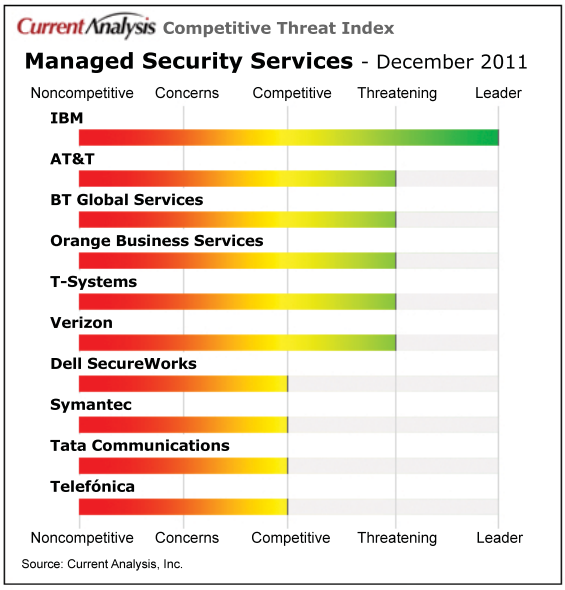
Bernt Ostergaard
Current Analysis
Research Director, IT Services

Issue

In 2011, to have a spot at the top in the managed security services (MSS) sector, providers needed to deliver the full scope of security services from the assessment and design phases through device management and governance, risk and compliance (GRC) management. They also need the capacity and the resources to support enterprise clients virtually anywhere in the world. MSSPs with the portfolio, scope and scale to meet these requirements have been richly rewarded in one of the prime growth sectors in IT services. After all, demand for advanced security capabilities is all the more urgent as effective risk management has become a boardroom priority and businesses struggle with their own internal security skill deficits.

The H2 2011 Current Analysis Managed Security Services review compares top telcos (AT&T, Verizon, BT Global Services, Orange Business Services, T-Systems, Telefonica and Tata Communications), alongside leading IT service providers (IBM and Dell SecureWorks) and a Tier 1 pure-play security provider (Symantec) in the global MSSP market. The study focuses on five aspects of MSSP offerings: service scope and availability; service packages/support guarantees; authentication and monitoring services; and Intrusion prevention and threat management. Discussions around cloud security expanded in 2011 with customers looking for common standards that would reassure them about cloud security (for details please see *Cloud Security Round-up Q4 2011: Cloud Security Complexity Still Confuses*, October 24, 2011).

Anxiety about the increasing fragmentation, consumerization and mobilization of the employees' devices accessing corporate IT resources are also pushing organizations to reexamine basic IT security and control postures. So how are the MSSPs repositioning their security capabilities? What are the H2 2011 security trend implications for 2012? And how are the MSSPs addressing overall corporate GRC issues?



Report:

Managed Security Services Update: It Just Got Better

Business Network and IT Services

Current Perspective

Market Trends

Managed security service providers (MSSPs) are concentrating on providing better security for mobile users, better protection of virtual computing environments and better management of large volumes of network data – known as big data analytics. Driven by the transformative nature of technology infrastructures and the fast evolving threat environment, global MSSP leaders are stepping up to the plate with more sophisticated solutions that address these threat landscapes and support compliance requirements, associated corporate policies, industry mandates and government regulations.

The overall 2011 vulnerability severity trend has actually been a positive one, according to Microsoft's Security Intelligence Report. Using the Common Vulnerability Scoring System (CVSS) that assigns a numeric value between zero and ten to vulnerabilities according to severity, disclosed medium and high severity vulnerabilities in H1 2011 were down respectively 6.8 percent and 4.4 percent from the same period in 2010. In H1 2011, high severity vulnerabilities that scored 9.9 or greater represented 10.5 percent of all disclosed vulnerabilities.

High severity vulnerabilities as well as low and medium severity DDoS attacks require better visibility into what is actually happening on the network based on a much broader set of data using deep packet inspection (DPI), correlated at high speeds with application and user activity. Present day SIEM tools still provide only very limited real-time insight into events taking place on the network. Log files and security events provide glimpses on activity, but the event data lacks context. MSSPs are actively improving their monitoring and analysis capabilities as demonstrated by wider adoption of Arbor Networks' intelligence gathering technologies, and major acquisitions by HP of SIEM market leader ArcSight, McAfee's NitroSecurity purchase and IBM's Q1 Labs buy. The aim is to provide better and faster network forensics and network behavior anomaly detection. Not only does SIEM analysis necessitate a lot of data power and wide access to traffic flows for analysis, but the ability to assess the information accurately requires significant expertise, which makes this particular discipline an MSSP sweet spot.

Security attacks expanded to include assaults on the IP infrastructure itself (DNS and VoIP) as well as widespread apps layer hits against ancillary supporting devices like web portals and servers, and attacks against protocols (SIP, IPv6). As worrying as these infrastructure attacks are, 2011 also saw hackers stealing digital certificates from certificate providers, and hackers also made off with key SecurID security technology from RSA, and promptly launched APT attacks on major U.S. military and high-tech companies. While still a rarity, these acts of aggression introduce uncertainty at a very uncomfortable level, namely the https: domains or the token-based access that you trust.

MSSP services are making significant changes to their services, not only increasing their abilities to analyze and advise their customers, but also aligning their services more closely with vertical industry needs and specific customer profiles.

Security Service Scope & Availability

MSSPs differ widely with respect to how many countries their services cover and how many security specialists they employ. Typically, their services are 'globally available', but often with a much smaller number of 'core' countries. At the top BT, Orange Business Services, AT&T and IBM lead the market with presence in more than 100 countries. Verizon's services are "available globally and with specific national government clearance in 35 countries". Symantec manages security devices for customers in "more than 70 countries worldwide and has 40,000 sensors in more than 200 countries". The rising importance of security experts to assist customers' GRC processes is reflected in the increasing number of specialists employed by MSSPs. Security operations centers (SOCs) supporting MSSPs' global operations have also been steadily increasing in numbers and geographic

spread, varying from three to 12 in our study, with leaders BT, IBM and Orange with 12, nine and eight SOCs respectively. At the other end, outliers Symantec with four SOCs and Telefonica and Tata Communications rely on just three centres.

Service Packages/Support Guarantees

Response SLAs come in many varieties and can also be customized to reflect specific user profiles. All providers except Symantec and Dell SecureWorks offer tiered service levels from standard services to dedicated service levels. Dell SecureWorks offers one standard SLA for each managed security service, and customers pay per monitored/managed device.

All MSSPs provide customer portals allowing customers self-service configuration options, trouble ticketing etc. However, they differ on how these portals are aligned with other managed services. The telcos integrate their security portals with their managed communication services. IBM's Virtual-SOC Portal provides the end-to-end interface for customers to interact with IBM's Managed and Cloud Security Services, whereas Symantec's and Dell SecureWorks portals are purpose-built for security only. The Dell SecureWorks portal additionally provides business intelligence features customers can use to customize dashboard experience. AT&T's Center Portal, which users can launch from the company's Business Direct, provides customers with a SOC-like interface into all of their security services.

Security Assessment Services

Compliance remains one of the biggest drivers of enterprise security expenditures. All MSSPs except Tata Communications provide extensive GRC and security audit support. Verizon offers an extensive set of GRC solutions, which include the ability for one company to compare compliance and security postures with other organizations in its industry. Verizon leverages proprietary sources for threat intelligence including reputational data, geo-spatial data, network intelligence, watch lists and updated threat and vulnerability databases integrated with its State and Event Analysis Machine (SEAM) correlation engine.

AT&T's Security Event and Threat Analysis service provides alerting based on an Incident Response Plan developed with the individual customer. The BT TrustCheck Solution uses several evaluation techniques in combination with a capability maturity measurement method to provide an in-depth review of people, processes and technology to define the customer's current security posture. IBM's Vulnerability Management Services (VMS) are turnkey solutions that combine managed scanning services with workflow and case management.

Authentication and Monitoring Services

All MSSPs provide authentication management services encompassing soft and hard two-factor token authentication, albeit each with a different emphasis, and likewise all except Tata Communications provide identity management. IBM provides a service-level identity lifecycle management solution that covers assessment, architecture and selection of best-of-breed security technologies. T-Systems provides Identity-as-a-Service for midsized companies, and end-to-end ID management solutions for MNCs based on its high security Trust Center and high availability directory services. BT has focused its portfolio on identity and fraud management services. Symantec monitors several VPN authentication services for customers to support a client's security needs and controls.

Authentication and access management services are continuously evolving as more organizations operate with a bring your own device (BYOD) policy that allows employee-owned devices access to corporate resources. Verizon's Secure Access Services, which offer cloud-based Web Access Management, single-sign-on, federation and SSL VPN service components as standard offerings. Orange Business Services incorporates SAML v2 technology to provide secure authentication also to cloud services, linked with customers' corporate directories to reflect any change in user account status in real time.

Report:

Managed Security Services Update: It Just Got Better

Business Network and IT Services

BT and IBM's scanning and alerting services stand out both in terms of the depth of their offerings and the range of package options available to customers. For example, IBM offers a vulnerability management service that blends scanning with workflow and case management. IBM's scanning service provides attestation, authorized to be used by acquiring banks and to comply with other regulatory requirements. BT supplies customers with a number of scanning and vulnerability assessment options including packages for specific verticals such as the Cyber Defense Quickstart, which ties into the Cyber Defense Managed Service to capture an end to end security perspective on the enterprise for decision support and risk management against cyber threats.

SIEM analysis is crucial to identify and mitigate malicious or accidental anomalies in network behavior – preferably before customer data is compromised. This is the prime role of big data analytics. The Dell SecureWorks' SIEM platform processes 15 billion security events per day to provide integrated vulnerability and threat intelligence analysis linked to workflow management and ticketing with change validation and management (for managed devices), as well as security and compliance reporting. Most of the MSSPs reviewed here have developed their own engines such as AT&T's SETA, BT's Socrates and Tata's Shiva, while a few, notably Verizon and Telefonica give their customers the choice of a variety of third party SIEM solutions (RSA EnVision, Juniper STRM, HP ArcSight, IBM Q1 Labs Radar, LogLogic and Huntsman).

Intrusion Prevention and Threat Management

Clean pipes, managed firewalls, fixed and mobile endpoint protection, IDS/IPS, UTM, DLP and DDoS mitigation services are arguably at the heart of any MSSP service package, and in this category BT Global Services, Tata Communications and Verizon lead the way. Verizon especially differentiates its capabilities by its wide-ranging multi-platform capabilities to accommodate different user environments.

Network- and premises-based firewalls can be beefed up with Web apps and proxy-based firewalls. AT&T Web Application Firewall Service is a fully managed security service that combines Web Application Firewall technology with expert management and monitoring to help protect Web applications and their underlying systems for customers with an Internet connection to an e-commerce or e-tail Web application that need to meet PCI specifications. Each of the providers covered in this report offers primary elements of scanning and alerting: intrusion detection/intrusion prevention, vulnerability assessments, monitoring and alerting services, and data loss prevention (DLP). Providers distinguish their services not just on their ability to scan multiple applications for viruses, malware and, in the case of DLP, sensitive or confidential information but also the accuracy of detecting malicious code or a possible leak. MSSPs use a variety of techniques including heuristics, signature recognition and reputational data to identify potential problems. Providers such as AT&T, IBM and Verizon can scan code before the application is put into production to identify potential vulnerabilities that are open to known exploits. Not only does this help businesses fix a flaw before a breach can occur, but it also helps customers meet a requirement of PCI compliance.

The ability to identify and thwart malware and DDoS attacks while maintaining accessibility for legitimate traffic to customer sites is now table stakes, but served up in different ways. A few MSSPs (AT&T, Verizon and Tata) provide low-latency data-scrubbing server farms to filter out attack traffic. These MSSPs will also provide some SLAs for DDoS mitigation in specific regions and within certain attack levels, making them attractive to e-commerce companies and online services like casinos. The Tata Communications' DDoS detection service is deployed globally with regional scrubbing facilities for on and off-net customers. SLAs are provided for detection notification and mitigation commencement. Other MSSPs including Orange Business Services, BT and Telefonica use network-based technology from Arbor Networks to identify and filter out DDoS packets. A few MSSPs, notably Symantec and Dell SecureWorks do not currently offer a standard DDoS service, but will work with customers and partners like VeriSign to combat the attacks. Besides providing UK customers with a cloud-based DDoS solution from Arbor Networks, BT Global Services

provides MNCs with Prolexic's full suite of service options, which include dynamic bandwidth adjustments, clean-pipe assurance services and automatic router reconfigurations in response to DDoS traffic patterns.

Conclusions

2011 has shown significant shifts in the security landscape, and corresponding swift changes and improvements in MSSP services as the security market continues to expand to embrace the increasing corporate reliance on mobile, networked and cloud-based resources. The keener corporate assessments of risk is leading to MSSP stratification with expensive, professional services-led MSSPs at the top, more specialized MSSPs addressing specific verticals or regions in the middle, and the no frills, self-service MSSPs offering cheaper global services available for price-sensitive customers. The result is a rich mix of options that are helping resource-constrained organizations close gaps in their defenses as they continue to push forward with new technology consumption models like cloud.

Recommended Actions

Recommended Vendor Actions

• Security concerns are top of mind for corporate executives, so this is one of the few IT disciplines that has not been cut during the financial downturn. MSSPs should document the overall and customer-specific reduction of severe security incidents in 2011, as proof of the ROI clients are getting from their MSS engagement. Given the expansion of the security market, such proof can only lead to more business.

• Customer security expectations are rising, and MSSPs must manage them, being very careful not to oversell their real-time capabilities. As yet, very few MSSPs can provide mobile traffic transparency, or a single sign-on that identifies the user, the user's location and access device, as well as the application's location, and provide conditional access in accordance with corporate security policies.

• The poisonous cocktail of exploding mobile data usage, smarter mobile devices and device consumerization constitutes a growing security hazard. MSSPs need to integrate their security approach with mobile device management (MDM) and mobile security systems such as Sybase Afaria. T-Systems, Verizon, Orange Business Services and Telefonica have all standardized on the Sybase MDM platform, so linking it tighter with their MSSP solutions should be straightforward.

• Virtualization from the desktop to the cloud creates a new threat landscape where corporate users and service providers are still developing best practices. MSSPs should not wait for standards to emerge, but rather engage in the best-practice dialogues underway in NIST, ENISA, the Jericho Forum, the Cloud Security Alliance and similar initiatives. This builds the confidence of customers and prospects looking to virtualize their infrastructures.

• Service scalability is of growing importance for customers. With the increasing frequency of DDoS attacks and the explosive growth in bandwidth availability and usage, MSSPs need to develop the computing muscle to handle much bigger volumes of data faster, and more accurately identify and thwart security threats. This is beyond even the biggest corporate capabilities today and is a great lead-in to managed services.

• MSSPs should expand their Security-as-a-Service offerings for SME customers and consider integrating them with other SaaS offers. The need for cheaper, flexible, standardized security services will become more critical as the business world emerges from the current downturn.

Recommended User Actions

• Optimized security deployments rest on credible risk assessments and the ability to implement and monitor compliance (e.g., ensuring that data storage policies are aligned with data management

capabilities). Large corporate clients can assess MSSPs' professional services capabilities individually in relation to the applications and locations they need to have protected, whereas SME customers should look for the security packages, notably UTM that provide 'good enough' security for their particular industry vertical.

• An MSSP's customer portal determines how transparent its services are to the customer. These portals should preferably be well integrated with other managed services and be open for third-party solutions rather than being proprietary, stand-alone solutions. As we expect fast paced developments in MSSP services, the portal capabilities will become crucial to security management.

• Service providers, telcos, vendors and ITSPs are baking security into all the services they provide – often acquiring pure-play security players to gain credibility. The next step is to link acknowledged security capabilities with apps hosting capabilities. Customers should investigate the level of integration and openness demonstrated by MSSPs notably in relation to supporting secure virtualization.

• Ease-of-use and good MSSP customer support is still critical, as many studies indicate that employees themselves are the major security problem - spending little time acquainting themselves with security procedures, and demonstrating very low tolerance for delays caused by complicated or disruptive security procedures. The many successful social engineering security exploits emphasize the need for involving employees in security practices, and to work with MSSP that have tiger teams and crystal box capabilities to evaluate the combined efficiency and user friendliness of corporate security.