



IDC MarketScape

IDC MarketScape Excerpt: Worldwide Managed Security Services 2014 Vendor Assessment

Christina Richmond

THIS IDC MARKETSCAPE EXCERPT FEATURES: IBM

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Security Services Vendor Assessment



Source: IDC, 2014

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Managed Security Services 2014 Vendor Assessment (Doc # 248646). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Using the IDC MarketScape model, IDC compared 11 organizations that offer managed security services (MSS) worldwide. Through in-depth managed security services provider (MSSP) interviews and more than 20 surveys with providers' customers, IDC learned that all providers have the necessary capabilities to deliver traditional worldwide MSS. Through more granular evaluation, IDC found that each provider possesses some unique strengths and weaknesses when compared with its peer group. At a high level, the major differences centered on their strategies for the next 12 months. IDC believes the following areas will drive the MSS market forward and differentiate the providers:

- Security services to assist customers in their evolution toward cloud and cloud security enablement
- BYOD/mobile solutions
- Abilities to thwart the increasingly impervious adversaries with threat intelligence and analysis via big data capabilities
- Supporting customers after the inevitable breach with incident response and forensic capabilities
- Security operations center (SOC) operating model
- Security talent

As a result of IDC's evaluation, IDC found six Leaders in AT&T, Computer Sciences Corporation (CSC), Dell SecureWorks, HP, IBM, and Verizon. A second group of Major Players consists of Atos, BT, Orange Business Services, Symantec, and T-Systems. With the maturation of MSS upon us, it is incumbent upon these top 11 worldwide MSSPs to lead the next generation of MSS, which IDC is calling MSS 2.0. Buyers certainly face complex choices in selecting a vendor with which to partner. However, despite these complexities in vendor selection, buyers purchasing MSS have plenty of options.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 11 MSSPs within the 2014 IDC MarketScape worldwide managed security services market assessment. While the market arena for MSS is very broad and there are many suppliers that offer these services, IDC narrowed down the field of players that participate in worldwide MSS based on the following criteria:

- **Service capability across the MSS life cycle.** Each service provider was required to possess full-service MSS delivery capabilities (see the Situation Overview section for an explanation of traditional MSS).
- **Revenue.** Each service provider was required to either have 2012 total MSS revenue in excess of \$120 million or demonstrate that at least 10% of its MSS revenue was attained in each of three regions – the Americas, EMEA, and APAC – in addition to having a minimum of five SOCs.
- **Geographic presence.** Each vendor was required to have MSS delivery capability in each of three regions: the Americas, EMEA, and APAC.

ESSENTIAL BUYER GUIDANCE

Because of the number of providers and a multitude of variables, buyers face complex choices in selecting an MSSP: breadth and depth of offerings; SOC staffing, capabilities, and locations; data privacy requirements; complementary services; onboarding options; service-level agreements (SLAs); payment options; customer portal capabilities; customer service delivery methods; and more. Given the pace of technology change, current and future MSSP offerings should be evaluated, along with the investment road map, to be sure that future offerings align with anticipated business and cost projections. It can be expensive and disruptive to change providers, so it is worthwhile to take the time to find the right fit, no matter how many security services are being outsourced. Customer satisfaction surveys and pricing benchmarks may be helpful to the decision process.

VENDOR SUMMARY PROFILE

IBM

According to IDC analysis and buyer perception, IBM is an IDC MarketScape Leader worldwide.

IBM, a New York-based multinational technology and consulting business, began offering MSS in 1995. IBM is one of a few study participants whose MSS delivery can be considered truly global, in part because of its ability to integrate MSS and security services globally.

IBM operates its SOCs in a modified follow-the-sun model that is designed to have senior staff available at all times. A majority of the SOCs operate 24 x 7, with live 24 x 7 customer support and language support. In 2013, IBM staffed three new global SOC delivery locations.

The X-Force Protection System (XPS) platform performs data collection and aggregation for customers' devices. On-premise appliances stream data to IBM to facilitate threat correlation and analysis. IBM's MSS offerings are available bundled and à la carte.

The company has one of the world's largest threat and vulnerability databases, and it is the foundation of its threat intelligence activities. The X-Force Threat Analysis Service is available for non-MSS clients if they want a standalone subscription, and it is provided to MSS clients at no extra charge. IBM reported growth in 2013 in managed SIEM, managed DDoS, and its "technology bundle" – a model for

customers to buy both technology and security services for a predictable monthly fee. Also in 2013, IBM completed two notable acquisitions: SoftLayer, which brings a private, global cloud infrastructure, and Trusteer, a premier vendor in fraud and malware defense.

In February 2014, IBM and AT&T announced a new service that combines security network infrastructure with advanced threat monitoring and analytics. AT&T provides network-based firewall, IDS/IPS, Web filtering, secure email gateway, and DDoS protection services for security devices managed on-premise or in the AT&T cloud. IBM capabilities include IBM Network Security Consulting to assess and transform network security, IBM Security Monitoring and Threat Intelligence for faster threat detection and response, and IBM Emergency Response Services for around-the-clock security expert support.

Strengths

IBM has strengths in advanced threat intelligence, big data analysis of threat intelligence, cloud security, complementary services, and customer portal. Further, it's a dominant player in managed SIEM. It has developed the Security Operations Optimization practice to help customers identify ways to improve results from their SIEM solutions and assist customers that want to build their own SOCs.

The IBM and AT&T joint venture meets a real market need with an end-to-end security solution that provides enterprise customers with both integration and simplicity.

Customers report high marks for SLA performance, daily threat assessment reports, and monthly review meetings.

Challenges

Areas of opportunity include flexibility in pricing and payment structures, managed BYOD/mobile security, and additional routes to purchase.

APPENDIX

Situation Overview

The security landscape is complex and challenging for businesses globally, and IDC recommends a holistic, enterprisewide security posture that is proactive and predictive versus reactive. In-house 24 x 7 security solutions are expensive, however, and expertise is scarce. It's a daunting task to sustain the necessary level of threat intelligence and advanced analytics capabilities, along with the skills to interpret and act on findings.

The current state of security creates budgetary pressures that lead organizations to have "build versus buy" discussions. Engaging a security services provider can allow organizations to transfer the cost of ownership, thereby reducing capex and transferring the budget line item to opex. This step creates a predictable expense with a regular cadence in the budget cycle. And, managed security services providers are focused solely on the rapidly changing threat landscape and the protection of their customers' businesses.

The rise in frequency and complexity of attacks and the need for increasingly sophisticated security solutions have led to a new echelon of MSS that IDC is calling MSS 2.0. A MSSP 2.0 is further "up the stack" than traditional MSSPs which are offering MSS 1.0 services such as basic managed and monitored services (firewalls, intrusion detection services [IDS]/intrusion prevention services [IPS], unified threat management [UTM], IAM, log monitoring, vulnerability scanning, etc.). Traditional MSSPs may also offer advanced services such as DDoS, Web application security, managed SIEM, and managed SOC. MSSPs that are focused on MSS 2.0 deliver basic and advanced traditional MSS plus professional/complementary services (see the Market Definition section). And, they are investing in mobile/BYOD, cloud, threat intelligence/big data, and incident response/forensics. Cloud, mobile/BYOD, and big data are three of four pillars that IDC has identified as top trends in 2014. The fourth pillar, which doesn't factor into this IDC MarketScape, is social media. Social media, however, does impact security, and advanced MSSP capabilities, in our analysis, can help detect, analyze, and protect against threats in the social media arena.

A complication in the security landscape is the shortage of security talent. As a result, employee acquisition, training, and retention are top priorities. Trail-blazing MSSPs are going far beyond traditional hiring practices to ensure near- and long-term access to a security talent pool. Some of their tactics include creating their own universities, developing lab partnerships with universities, sponsoring cyber-competitions, establishing scholarships, and partnering with schools to develop curriculum.

Further, regulatory requirements continue to evolve, and MSSPs can provide the expertise and evidence needed for oversight and compliance based on industry-standard certifications. Data privacy laws, which are yet to be formalized, are expected to vary from country to country. To date, MSSPs are meeting customer data privacy requirements on a case-by-case basis. IDC believes that data privacy laws will greatly influence SOC strategy and implementation.

Businesses are increasingly turning to MSSPs to monitor and manage some or all of their security needs. Based on IDC market sizing, the MSS market is expected to continue to see growth in double digits in coming years.

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capabilities.

Service Provider Customer Interviews

As part of this IDC MarketScape, IDC conducted interviews with vendor-provided client references. IDC utilized these customer interviews to learn about the customers' project backgrounds, how customers selected the service provider and what critical criteria they used to select their vendor, what sort of results customers were able to generate from their MSS engagement, what lay ahead, key lessons learned, and what customers felt were the differentiating and key strengths their chosen managed security service provider possesses.

Weightings

This MSSP assessment is designed to evaluate the characteristics of each firm and each firm's global presence. Many types of firms compete in the MSS market. As such, this evaluation is not an exhaustive list of the players to consider for an engagement. Instead, this evaluation reviews the primary players that offer capabilities spanning the MSS landscape. Factors like business and information technology (IT) objectives, business and IT requirements, and the business and IT culture of an organization play integral roles in determining which firms should be considered as potential candidates for an MSS engagement.

Market Definition

Managed Security Services

For the purposes of this research, IDC defines managed security services as "the around-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs), not through personnel onsite."

Exceptions and Inclusions

Managed security services can include complementary consulting and advisory activities that are typically defined under professional security services. The study did seek to understand whether the MSSPs offer complementary services as IDC believes these are critical to the evolution and maturity of MSS. The MSSPs in this study do provide complementary services although there is no standard

approach for how they are offered. Commonly, an initial assessment is bundled with MSS. Some MSSPs bundle other services. Most, however, offer complementary services as optional add-ons and charge separately for them.

Complementary services surveyed in the study include breach management, incident response, forensics, compliance services, and assessment of architecture and design. Not all MSSPs provide all of these services. Some MSSPs provide all of the listed complementary services and many others.

Terminology

- **Global versus international.** Global business and international business are often used interchangeably in casual conversation. When these ideas are looked at specifically in the ways companies operate as they move beyond domestic borders, they are quite distinct. The term global has a more broad and universal concept of the global marketplace, while international business refers to the application of a business model to various markets. In this study, most of the MSSPs analyzed are not truly global entities, at least not in reference to their MSS business. A truly global MSSP has a global 24 x 7 fully redundant SOC, localizes its marketing, sells through regional channels in addition to local direct sales, and conducts customer satisfaction studies and pricing evaluations with regional methods.
- **Managed security and information event management (SIEM).** This managed on-premise event collector transmits the raw log data to the MSSP's SOC for analysis, reporting, and archiving. This is an advanced and niche offering that only a handful of MSSPs offer.
- **Managed SOC.** A security operations center includes the people, processes, and technologies involved in detecting, containing, and remediating security threats. Some MSSPs take over the operation of SOCs that their customers have built and no longer want to manage. This is an advanced and niche offering that only a handful of MSSPs offer.

LEARN MORE

Related Research

- *Worldwide Threat Intelligence Security Services 2014-2018 Forecast: "Iterative Intelligence" – Threat Intelligence Comes of Age* (IDC #246977, March 2014)
- *IBM MSS: Vendor Agnostic, Custom, and Off the Shelf* (IDC #246858, February 2014)
- *AT&T Managed Security Services Offers "Defense in Depth"* (IDC #246446, January 2014)
- *Market Analysis Perspective: 3rd Platform Drives Growth and Disaggregation in Security Services* (IDC #244989, December 2013)
- *Trustwave: Solutions and Services for Security and Compliance* (IDC #244994, December 2013)
- *Trustwave Announces Enhancements and New Managed Secure Web Gateway* (IDC #1cUS24456813, November 2013)
- *Dell SecureWorks: An Integrated Approach to Security* (IDC #242998, September 2013)

- *IBM Launches Managed Cloud-Based DDoS Mitigation With Akamai* (IDC #243284, September 2013)
- *Solutionary: Building Situational Awareness into Managed Security Services* (IDC #242468, August 2013)
- *Another Security Services Acquisition: NTT to Acquire Solutionary, a North American Managed Security Services Provider* (IDC #IcUS24187113, June 2013)

Synopsis

This IDC study represents a vendor assessment of providers offering managed security services (MSS) through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for MSS. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the MSS market over the short term and the long term.

"The high profile of security incidents and the costs associated with protecting the enterprise from them are driving executives and the boardroom to increasingly consider managed security services. No longer are the traditional managed security services enough, however, as greater predictive insights and advanced tools are required to win the battle against alarmingly skilled adversaries. Add to this challenge that there is not enough trained and 'battle-ready' security talent available. This coalescence has created 'MSS 2.0,' which raises the requirement for MSSPs to add iterative threat intelligence and advanced threat detection and analysis capabilities. It requires the proactive development of a new breed of security employees and demands cost-effective protection all while providing comprehensive visibility to customer security executives." – Christina Richmond, program director, Security Services

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2014 IDC. Reproduction is forbidden unless authorized. All rights reserved.

