IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2015 Vendor Assessment

Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES: CSC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Asia/Pacific Managed Security Services Market Vendor Assessment

Source: IDC, 2015

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: Asia/Pacific Managed Security Services 2015 Vendor Assessment (Doc #AP251064). 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 16 organizations that offer managed security services (MSS) in Asia/Pacific. Through in-depth interviews with MSS providers (MSSPs) and more than 20 interviews with providers' customers, IDC learned that major differentiation among the 16 identified MSSPs centered on their go-to-market (GTM) capabilities in Asia/Pacific, such as customer services, sales or distribution structure, pricing alignment, partnership, and marketing. This is in line with the rapid maturing status of the MSS market in the region where many MSSPs can offer one form or another managed security services. A fast-growing number of enterprises and government organizations in the region are looking for an MSSP with global capabilities and strong local delivery capacities. The reasons behind this are the following:

- A global/regional MSSP tends to have stronger partnerships with global security technology vendors compared with a local MSSP (i.e., focused on one country). The strong partnership with technology vendors is not only important in terms of ensuring the MSSP can support and manage the latest models or features for the security solutions, but also critical to enable the customers to have the most up-to-date and comprehensive security intelligence and protection they can get from their MSSPs.

- More importantly, many of the global and regional MSSPs have their own security research lab and resources to have the first-hand security intelligence in real time. This is particularly true for the MSSPs that have security products or in-house security technologies, such as IBM, HP, Symantec, or e-Cop.

- The organizations in Asia/Pacific highly appreciate the interaction with qualified security professionals from their MSSPs that have strong knowledge of their industry and good understanding of their business pain points, preferably in a location with minimal time difference. Strong local presence and delivery are especially important when it comes to incident response.

Through more granular evaluation, IDC found that each provider possesses some unique strengths and weaknesses when compared with their peer group. As a result of the IDC MarketScape Managed Security Services research process, IDC found five "Leaders" in NTT Com, IBM, Computer Sciences Corporation (CSC), Verizon, and HP. A second group of "Major Players" consists of Symantec, BT, Wipro, Dimension Data, HCL, e-Cop, Singtel, Orange Business Services, and AT&T. Atos and Telstra are currently being positioned as strong "Contenders" in the marketplace. It is worth mentioning that IDC found that all the identified providers have necessary capabilities to deliver a fairly comprehensive portfolio of MSS offerings.
IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 16 MSSPs within the 2015 IDC MarketScape Asia/Pacific 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 the Asia/Pacific MSS market based on the following criteria:

- **Service capability across the MSS life cycle.** Each service provider is required to possess full-service MSS delivery capabilities.
- **Revenue.** Each service provider is required to have total MSS revenue in excess of US$10 million that was attained in Asia/Pacific in 2014.
- **Geographic presence.** Each vendor is required to have MSS delivery capability in minimum of two sub-regions: Greater China (i.e., the People's Republic of China [PRC], Hong Kong, and Taiwan), South Korea, India, Australia and New Zealand [ANZ]), and Southeast Asia (i.e., Singapore, Malaysia, Thailand, the Philippines, Indonesia, and Vietnam).

Vendors included in this IDC MarketScape are:

- Atos
- AT&T
- BT
- CSC
- Dimension Data
- E-Cop
- HCL
- HP
- IBM
- NTT Com
- Orange Business Services
- Singtel
- Symantec
- Telstra
- Verizon
- Wipro

The following vendors are considered but not included in this IDC MarketScape because they did not fully meet the criteria as defined previously:

- Dell SecureWorks
- Tata Communications
- T-Systems
ESSENTIAL BUYER GUIDANCE

Companies understand that their systems, storage operations, network connectivity, and endpoints need to be inherently secure. That is why customers demand security management that is effective, usable, affordable, and well integrated with the IT infrastructure. IDC suggests that buyer organizations to:

- **Develop a security framework that determines the best mix of models of offerings.** In Asia/Pacific, demand for security professionals far exceeds the supply. Therefore, it will be very challenging to deliver all of the security- or risk-related services required by the business using in-house staff. Enterprises need to assess the overall security architecture and determine which capabilities would best fit a software as a service (SaaS), managed services, or hybrid model.

- **Understand the evolution within MSS.** Traditionally, enterprises that adopt MSS are primarily driven by cost and security operations benefits that they can gain. A typical MSS is very much network-centric and devices focused and usually leverages on a security incident and events management (SIEM) platform to correlate logs or security events from various security devices and generate alerts for security incidents.

  With the rapidly increasing sophistication of threats and technological changes such as cloud and mobility brought to today's organizations, it is no longer sufficient to focus only on the network and be reactive. The new generation of MSS, advanced MSS (or known as "MSS 2.0"), is largely characterized by usage of big data and analytics (BDA) and is data and access centric. (See more details from *IDC's Asia/Pacific (Excluding Japan) IT Services Market 2015 Top 10 Predictions: Transforming IT Service Delivery in the 3rd Platform Era*, IDC #AP250906, January 2015.)

- **Identify the right MSSP.** The market is abundant of security vendors, and many of them claim to have end-to-end security offerings. Despite the identified 16 key players in the space, buyers purchasing MSS have plenty of options, especially those buyers that do not have a regional presence. There is a handful local MSSPs for them to choose from, such as Infosec and Samsung SDS in Korea, NSFOCUS and Topsec in China, i-Secure and CAT Telecom in Thailand, and ISSDU and Chunghwa Telecom in Taiwan.

  It is important to select a security provider that does not only have a compelling security technology, but also delivers offerings that suit your business needs and even help to optimize your existing investment. The measurement framework used in this study (see Tables 1–3) can be referenced when you investigate and assess MSSP capabilities.

  More importantly, it is critical to evaluate current and future MSSP offerings, along with the investment road map. It is important to assess things like whether this MSSP will expand its portfolio to include bring-your-own-device (BYOD)/mobile solutions and services to assist customers in their evolution toward cloud, or this MSSP has plans or in the process of updating its existing MSS platform to monitor and track both structured and unstructured data.

  In addition, it has always been a challenge for organizations to establish a business case for their security investment. Nonetheless, a growing number of MSSPs now have capabilities, such as models that will determine the financial impact of breaches and tools that will gauge and benchmark the IT security risks of an enterprise against its peers in the same industry.
VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations, resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

CSC

According to IDC's analysis and customer feedback, CSC is positioned as one of the Leaders in the IDC MarketScape Asia/Pacific Managed Security Services.

CSC is one of the largest IT services company in the world. The company has approximately 76,000 employees across 70 markets around the globe.

CSC has long been focused on security. Its cybersecurity portfolio includes comprehensive offerings across MSS, security consulting, business continuity, incident response services, and so forth. Some of the cybersecurity capabilities are rooted in the company's history with the United States government.

CSC also has solid professional security services capabilities on the assessment, threat intelligence, and compliance services fronts, which are complementary to the MSS offerings. For many of CSC's MSS engagements, the first step is to assess existing architecture and technology. This ensures that at service inception, the technologies are not only deployed correctly but also capitalize on the full value of the technology and architecture.

CSC Pulse Portal, its security management tool or customer portal provides immediate and clear insights into a client's IT risk and compliance posture with information and data. It is now integrated with HP Arcsight SIEM, which facilitates a single portal interface for client ticketing, reporting, and providing near-real-time configurable views and dashboards. The portal has a rich set of features, providing a simple streamlined navigation menu, detailed querying of live data, security feed, and real-time chat with SOC personnel.

In Asia/Pacific, CSC has one global SOC in Australia and three regional SOCs in two different time zones to support the regional customers. The company plans to expand two new SOCs in the region in the next 24-36 months.

From marketing standpoint, the company has initiated the messaging of "SOCs as Risk Management Centers (RMC)," integrating cybersecurity services with its Cyber Assurance program to create "chief information security officer (CISO)-in-a-box" to ensure risk is managed across all parts of the organization. This is a powerful messaging that is in line with the trend in the security market, that customers are advised to take a risk-based approach for its security investment.

Though CSC predominately leverages a direct sales model, the company has done joint messaging and marketing activities with its key strategic alliance partners, such as HP for application security (HP Fortify), SIEM (HP Arcsight) services, and with Trend Micro for cloud security services. On top of the joint GTM activities, CSC can also leverage these strategic alliance partners' sales operations across the globe for its MSS.

Over the past 18 months, CSC has added three acquisitions of value to its cybersecurity portfolio. Two of the acquisitions are in the big data space (i.e., 42Six Solutions and Infochimps) and have tangential impact on its cybersecurity vision through increased analytics capabilities. For instance, CSC Cyber
team is currently working on its security BDA offerings by working closely with its BDA team. The third and most recent acquisition (i.e., ServiceMesh) is in the cloud orchestration space and has a direct impact on the security policy of virtualized workloads. It is expected to see the vendor strengthen and broaden its MSS in the marketplace.

**Strengths**

CSC has a mature practice when it comes to the service-level agreements (SLAs) design and adherence. The company takes a customer-focused approach to its MSS SLA as many SLAs are defined by clients, along with remedies that come with expected targets and risk amounts.

As for the customer support, CSC ensures best possible support by assigning two dedicated resources for each client. While the assigned account security manager (ASM) acts as the single operational interface, provides governance, and manages the delivery of all cyberservices and reporting, the cyber assurance lead (CAL) is responsible for risk and compliance reporting and vertically aligned innovation advice. As a result, the existing CSC customers rated very high for the customer satisfaction level.

**Challenges**

CSC primarily focuses on a direct sales model. The company has not engaged any channel partners other than its technology partners.

As the company is in the midst of transitioning, the execution issues at a high level may affect the acquisition and retention of security professionals, which can potentially pose a challenge for its cybersecurity growth plan in the region.

**APPENDIX**

**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 will look at how well a vendor is building or 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 GTM 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. The vendor market share for this study represented by the MSS revenue is attained only in Asia/Pacific, and the information was from the data collected during the IDC MarketScape process.

**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 capability.

Market Definition

The definition and scope of MSS vary greatly. For the purposes of this IDC MarketScape, IDC defines "managed security services" as the round-the-clock management and monitoring of security solutions and activities delivered from a vendor's SOCs or a third-party service provider's datacenter.

Some examples of MSS include customer premises equipment-based (CPE-based) managed and monitored firewall services, intrusion prevention and detection services, security event and incident management, vulnerability management services, patch management and upgrades, and identity and access management services.

Synopsis

This IDC study uses a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, IDC found five vendors – NTT Com, IBM, Computer Sciences Corporation (CSC), Verizon, and HP – in the "Leaders" category in the Asia/Pacific managed security services (MSS) market. A group of "Major Players" consists of Symantec, BT, Wipro, Dimension Data, HCL, e-Cop, Singtel, Orange Business Services, and AT&T. Atos and Telstra are currently being positioned as strong "Contenders" in the marketplace. IDC found that all the identified providers have a fairly comprehensive portfolio of MSS offerings.
"Through in-depth interviews with MSS providers (MSSPs) and more than 20 interviews with providers' customers, IDC learned that major differentiation among the 16 identified MSSPs centered on their go-to-market (GTM) capabilities in Asia/Pacific, such as customer services, sales/distribution structure, pricing alignment, partnership, and marketing," says Cathy Huang, the lead analyst for this study.

Huang continues, "While we have seen the growing frequency of cybersecurity being featured in conversation nowadays, be it business transformation or digitalization, we also acknowledge that CIOs demand security management that is effective, usable, affordable, and more importantly well integrated with the changing IT infrastructure. That is why we believe that the introduction of advanced MSS (also known as "MSS 2.0"), which is often characterized by the use of big data analytics (BDA) and automation technologies, is very important to meeting the proactive, dynamic requirement of risk and security management goals."
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.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
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 2015 IDC. Reproduction is forbidden unless authorized. All rights reserved.