Excerpt

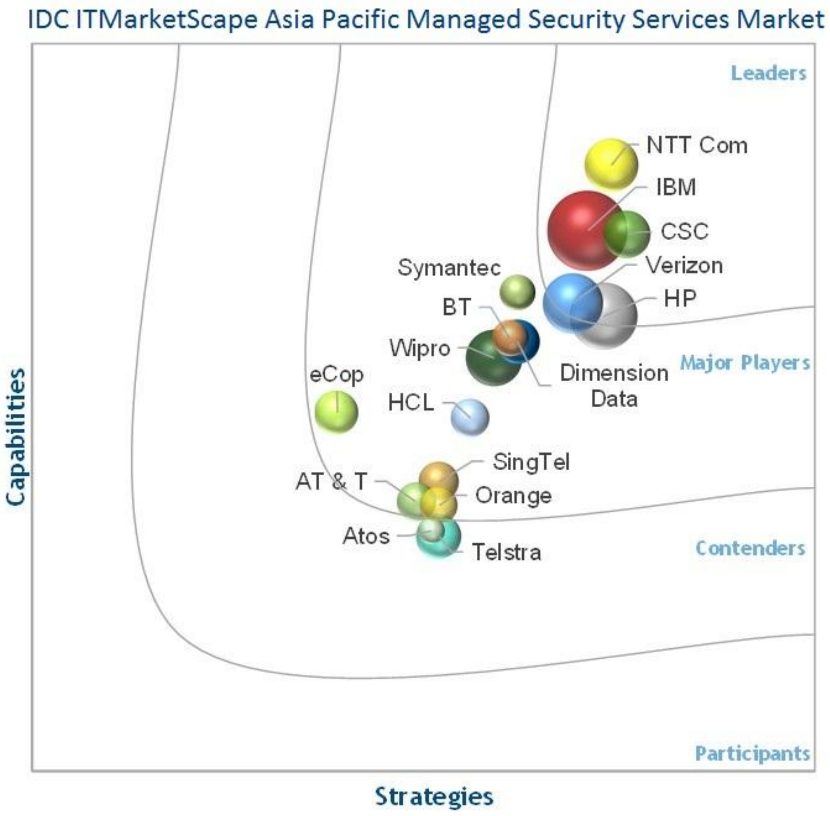
IDC ITMarketScape: Asia/Pacific Managed Security Services 2015 Vendor Assessment

Cathy Huang

IDC ITMARKETSCAPE FIGURE

FIGURE 1

IDC ITMarketScape 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 ITMarketScape: Asia/Pacific Managed Security Services 2015 Vendor Assessment* (IDC #AP251064_JP, May 2015). All or parts of the following sections are included in this excerpt: IDC ITMarketScape Figure, IDC Opinion, IDC ITMarketScape Vendor Inclusion Criteria, Essential Buyer Guidance, Vendor Summary Profiles, Appendix and Learn More.

IDC OPINION

Using the IDC ITMarketScape 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 ITMarketScape 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 ITMARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 16 MSSPs within the 2015 IDC ITMarketScape 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 ITMarketScape 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 ITMarketScape 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 ITMarketScape. 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.

NTT Communications

According to IDC's analysis and customer feedback, NTT Communications (NTT Com) is positioned as one of the Leaders in the IDC ITMarketScape Asia/Pacific Managed Security Services.

NTT Com is the ICT solutions and international communications business within the NTT Group, one of the largest ICT companies in the world. The company's security strategy is closely tied with its global cloud vision, which extends beyond cloud services to encompass the entire services vision for the NTT Group. The company's security strategy aims to offer total risk management to the entire ICT environment (including on-premises, cloud, and datacenters) in various forms, including professional services, solution implementation, and managed security services. It has a comprehensive services menu for different groups of customers, including global multinational companies, regional, and local companies. The company is moving lots of low-value or commoditized security services toward automated or self-service. More importantly, NTT Com plans to deliver or manage many of these services leveraging software-defined networking (SDN) or network function virtualization (NFV).

The go-to-market (GTM) model for NTT Com security is a combination of direct and indirect sales structure. For its domestic market, NTT Com usually employs the direct sales model to target the ICT and technology services needs of Japan organizations and more importantly, security services that are typically integrated with NTT Com's cloud or datacenter or network services.

For customers outside of Japan, NTT Com largely relies on its subsidiaries such as NTT Singapore, NTT Com Asia, NTT Com ICT Solutions (Australia), and Emerio, an NTT Communications company (via an acquisition in 2010) to co-sell its MSS in Asia/Pacific. Emerio, a Singapore-headquartered IT services and solution company, has more than 2,000 employees across 11 countries, with delivery centers in Singapore, Malaysia, Indonesia, India, the Philippines, and Thailand. NTT Com has successfully leveraged Emerio's relationship to rapidly expand its presence in Southeast Asia, and its MSS business also experienced more than 20% year-over-year (YoY) growth among the Southeast Asian markets in 2014. Similarly, NTT Com also experienced strong revenue growth in Australia because of its local investment and consolidated presence in the market. In late 2013, NTT Com has consolidated two acquisitions (i.e., Frontline Systems and Harbour MSP) in Australia with its local entity.

In addition to its GTM model, which effectively relies on its subsidiaries, sister companies, and channel partners in the region, the increased MSS revenue is also attributed to the greatly improved attack detection rate in 2013 (most likely due to the Secode acquisition by NTT Com and the Solutionary acquisition by NTT group). Since 2009, NTT Com has acquired a number of pure-play security services providers, including Integralis and Secode, which greatly enhance NTT Com's security capabilities.

Strengths

Unlike its peers that primarily focus on direct sales model, NTT Com has a great level of flexibility in terms of its GTM strategies, which helps the company to rapidly expand the client coverage in the region. Other than direct sales model, which is primarily used in its home market Japan, the company leverages its channel partners to penetrate the market. NTT Com has so far leveraged its Singapore subsidiaries (i.e., Emerio in Singapore and NTT Com ICT Solutions in Australia) to sell through or co-sell its managed security services in Asia Pacific. More importantly, its partnerships with consulting firms such as PwC, KPMG, and E&Y also help NTT Com to target business and senior executive members for its MSS because of the joint GTM programs.

On the customer support front, NTT Com was rated very high by its customers, particularly in the area of real-time notification of high-risk threats or security events. Other than the basic log monitoring services, its advanced detection (i.e., real-time malware detection services) and analytics services have seen growing traction in the region. NTT Com also offers highly flexible options, including self-service to get onboard the customers.

On the research and development (R&D) fronts, NTT Com also taps on the global resources of NTT Group companies, including Dimension Data and NTT DATA, which spends US$6.8 billion a year. NTT Com also continuously utilizes NTT Holdings R&D center's threat detection logics into its own developed SIEM engine. Its R&D budget on the MSS platform alone has been around US$15 million each year.

Challenges

Despite having four security operations centers (SOCs) across four different countries in Asia/Pacific, NTT Com has only one SOC in Japan, which operates 24 x 7 with a business continuity plan (BCP) SOC site located 400km from its primary site. The capacity for the other regional SOCs can be upgraded.

In addition, the market awareness for its security services can be further improved in regions outside Japan.

APPENDIX

Reading an IDC ITMarketScape 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 ITMarketScape 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 ITMarketScape process.

IDC ITMarketScape Methodology

IDC ITMarketScape 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 ITMarketScape, 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 ITMarketScape, 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.

LEARN MORE

Related Research

- *Market Analysis Perspective: Asia/Pacific Managed Security Services Market 2015 and Beyond* (Forthcoming)
- *Professional Services Market Opportunities for the 3rd Platform Technologies and Security* (Forthcoming)
- *Another Asian Acquisition of a North American MSSP: Singtel Acquires Trustwave* (IDC #lcUS25565015, April 2015)
- *IDC Asia/Pacific 2014 IT Services End-User Survey Results I: IT Services Spending Trends across Asia/Pacific (Excluding Japan)* (IDC #AP250967, March 2015)
- *IDC Asia/Pacific 2014 IT Services End-User Survey Results II: IT Services Engagement and Management Across Asia/Pacific (Excluding Japan)* (IDC #AP250986, March 2015)
- *Asia/Pacific (Excluding Japan) IT Services Market 2015 Top 10 Predictions: Transforming IT Service Delivery in the 3rd Platform Era* (IDC #AP250906, January 2015)
- *Resources Consolidation, Security Enhancement and Business Innovation Spur 2015 IT Services Spending in Asia Pacific: IDC* (IDC #prHK25334914, December 2014)
- *IDC MarketScape: Worldwide Managed Security Services 2014 Vendor Assessment* (IDC #248646, June 2014)

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 Japan

3rd Floor, Hulic Kudan Building, 1-13-5 Kudankita, Chiyoda-ku Tokyo 102-0073, Japan
81.3.3556.4760
Twitter: @IDC
idc-insights-community.com
www.idc.com