IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2016 Vendor Assessment

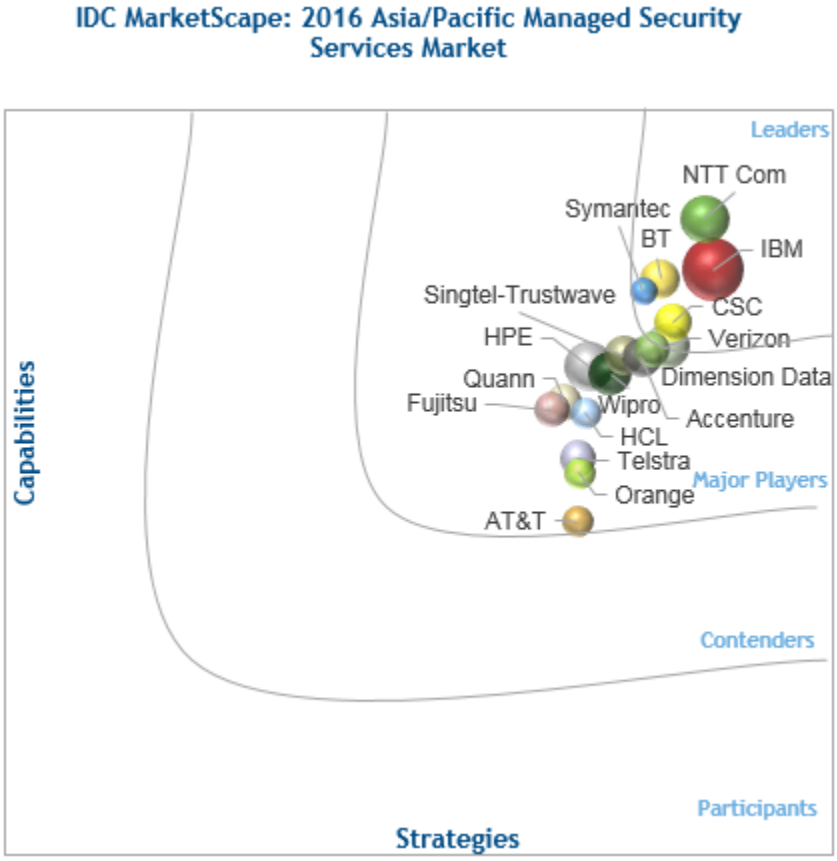
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES: IBM

IDC MARKETSCAPE FIGURE

FIGURE 1

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



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

Source: IDC, 2016

October 2016, IDC #AP40939616e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Asia/Pacific Managed Security Services 2016 Vendor Assessment (Doc # AP40939616). 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

Competition in the Asia/Pacific (AP) managed security services (MSS) market has intensified over the past 12 months in the wake of ongoing industry consolidation. Global MSS providers (MSSPs) that have invested in the region have beefed up their portfolio in a bid to vie for tech buyers' attention.

Using the IDC MarketScape model, IDC studied 17 organizations in 2016 that offer MSS in AP, although the majority of the participating companies deliver services worldwide. This study excludes the niche or country-specific MSS providers (MSSPs), which may also be considered to form the wide range of contenders in the AP MSS market.

Through a granular evaluation that involves more than 45 in-depth interviews with MSSPs and their customers, IDC found that each provider possesses some unique strengths and weaknesses when compared with those in their peer groups. As a result of IDC's evaluation, IDC found six leaders: NTT Communications (NTT Com), IBM, BT, Symantec, CSC, and Verizon. The second group of major players consists of Dimension Data, Singtel, Accenture, Hewlett Packard Enterprise (HPE), Wipro, Quann (formerly known as e-Cop), Fujitsu, HCL, Telstra, Orange, and AT&T.

Through this study, IDC found that almost all the providers have enhanced the breadth of their MSS portfolio in the past 12 months. However, advanced MSS capabilities vary among the providers. At the same time, the delivery and onboarding flexibility, for instance, the degree of leveraging cloud platform to offer MSS, vastly differentiate the providers. Other factors that differ from one provider to the other include the following: price competitiveness, security operations center (SOC) staffing, capabilities, and location; complementary services (including forensics or training services such as cyber-range); service-level agreements (SLAs); and customer portal capabilities.

Over the past 12 months, the AP MSS market has seen substantial change because of a number of factors, including market adoption of digital technologies, which resulted in a change in perception of risk and desire to revisit sourcing strategies.

In the early days, MSS providers focused on the management of security products. This remains a significant portion of the current market. However, there are increasingly new and emerging functions that are delivered as a managed service option and that extend beyond straightforward product-based services to include security operations, staff augmentation, and so forth, which are elementary and advanced in nature. A basic service includes, for example, management of policies and rule sets across the entire security product estate, ensuring consistency and availability of a security function. More advanced services include a managed SOC, managed encryption and key management, and compliance management.

In addition, the security as a service (SaaS) model is gaining momentum, particularly for the messaging and web security segments, such as web application firewall (WAF) SaaS or email SaaS. Moreover, the self-service setup is often used for the SaaS services. IDC believes this SaaS model is going to be an increasingly critical option for enterprises to source their security needs.

The adoption of threat intelligence is at an early stage in AP. Many MSSPs currently bundle their threat intelligence capabilities into their MSS offerings, not monetize it as a stand-alone offering. Although IDC predicts that threat intelligence will be one of the fastest-growing data-as-a-service (DaaS) offerings built on the 3rd Platform, the majority of AP clients' willingness to have the threat intelligence delivered "as a service" is weak at this stage.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 17 MSSPs within the 2016 IDC MarketScape Asia/Pacific Managed Security Services market assessment. Although there are many more suppliers that offer managed security services with varying degrees of portfolio and delivery capabilities, IDC narrowed down the field of players that participate in the AP 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 a 2015 MSS revenue in excess of US$20 million that was attained in AP.
- **SOC.** Each service provider is required to have a minimum of two SOCs in AP.

The following vendors are notable players in the region but were not included in this IDC MarketScape due to the defined vendor inclusion criteria:

- Dell SecureWorks
- Atos
- Ernst & Young

ESSENTIAL BUYER GUIDANCE

The AP MSS marketplace is competitive, with many MSSPs vying for customers. More importantly, with the industry seeing lots of consolidation, buyers face challenges and complexities in selecting the right MSSP. IDC encourages buyers to reference multiple sources for their evaluation process, including use cases, proofs of concept, pricing benchmarks, MSSP's customer satisfaction surveys, and a third-party vendor assessment study such as this MarketScape.

In addition, IDC recommends the following to tech buyers:

- **Focus on outcome**. For a long time, enterprises tended to address security challenges by simply investing in new security technologies, such as evolving generations of firewalls and threat management tools. However, this is a misconception in the industry because a sound security program needs a comprehensive approach that encompasses mindset, process, technology, and people. One of the Singapore-based CIOs puts it interestingly, "We do not invest in top-notch security technology but good enough technology because we understand security is more than just adopting good technology." Once the outcome is clear and defined, it is much easier to seek for related funding. IDC observes mature organizations tie the security

objective very closely to the business objective. As a result, some security investments are actually coming from the lines of business as part of the business transformation or innovation initiatives.

- **Creative security work sourcing enables agility**. Be creative when it comes to identifying, acquiring, and retaining security talent. The people behind the technology matter a lot to the overall cybersecurity proficiency. Conduct a regular comprehensive evaluation on the security work sourcing arrangement, which involves full-time staffing, contractors, and outsourcing options in order to meet security needs in a most optimized, agile, and cost-effective manner. Creative work sourcing requires investment in training and retaining people as well as a good understanding of the sourcing options in the market. IDC believes that it is critical to examine market offerings and prepare to take advantage of new sourcing models, such as crowdsourcing or cloud-based security functions. It is important to constantly monitor the cost-effectiveness of security functions and allocate resources accordingly.
- **Leverage cloud to deliver better security outcomes more efficiently**. As organizations continue to demand a wider range of options for on-premise and cloud-based solutions as well as a hybrid of both, many MSSPs have expanded their MSS portfolios to include the cloud security portion, embracing the management of security for cloud and hybrid environments. IDC believes a sound cloud security governance framework enables IT organizations to have better control and deliver services more effectively and efficiently. It will be beneficial to the organization overall, particularly in this digital era, which focuses more on agility and customer experience.
- **Threat intelligence adds a layer of richness on top of threat management**. Security threat intelligence allows organizations to be proactive in predicting various potential attacks instead of reacting after the fact. Although almost all MSSPs stress on expanding their threat intelligence capability, few of them are rolling out tailored threat intelligence, which is adaptive to the customer's industry, is risk-based, is business-focused, and enables effective threat detection and response. In addition, the capability to amalgamate external threat data, internal security log data, system vulnerabilities, and functional IT activities would require more than a security information and event management (SIEM) platform for full visibility and integration of data. IDC believes capability in threat intelligence can be used as a key evaluation criterion when buyers select an MSSP.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. Although 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.

IBM

According to IDC's analysis and customer feedback, IBM is positioned as one of the leaders in the 2016 Asia/Pacific Managed Security Services MarketScape study.

As a global leader in security products and services, IBM offers world-class expertise to the region. The goal of IBM Managed Security Services (MSS) is to maximize the effectiveness of the client's security operations, enabling the client's resources to outperform their own. More importantly, IBM's substantial local presence and regional partnerships enable the vendor to adapt its offerings to specific client needs. For example, IBM has a new National Cyber Security Center in Australia, and the center

connects Australian MSS customers to IBM's extensive global network of security research, including threat intelligence.

Automation has been a significant area of focus for the vendor over the past 12 months and is likely to be so in the near future as well. Specifically, IBM has been working on building cognitive capabilities into its MSS portfolio. For example, IBM plans to expose clients to the action of the "virtual engineer" in a more natural and digital way by leveraging natural language processing skills and other cognitive capabilities that it has built.

In late 2014, IBM introduced its cloud security portfolio, which focuses on authenticating access, improving visibility, and optimizing security operations for the cloud. The portfolio uses proven analytics capabilities (e.g., IBM QRadar) to give companies a clear line of sight into the security status of their entire business.

Strengths

IBM possesses arguably one of the strongest and most complete portfolios among all the MSS providers. Within AP, IBM is a brand reputed for MSS. The vendor has a long history as a leading technology vendor and is often the preferred choice for customers seeking security services. Leveraging on the global scale of IBM, extensive intelligence everywhere, and state-of-the-art security technology, IBM helps organizations transform and optimize their security operations.

Innovation and research and development (R&D) commitments have long been hallmarks of IBM. IBM maintains an active status in security research, including efforts in the areas of automation, machine learning, and AI. Some items, such as big data analytics and threat intelligence security services are included or embedded into MSS by design. Clients get to consume and benefit from these capabilities without the extra purchase.

In addition, IBM uses a variety of tools to help customers understand and justify their security investments. For example, the total cost ownership tool provides an illustration of the cost savings associated with each solution in its portfolio as against delivering these capabilities in-house. Similarly, its periodic business reviews identify key aspects of the customers' security strategy in order to enable them to refocus strategic priorities on areas in which their investments can yield the greatest benefit.

Challenges

IBM underwent an internal restructuring focused on integrating security products and security services teams earlier this year, with the intention of transforming into a well-rounded security services provider. However, it often takes time for the changes to materialize and for customers to recognize the new positioning.

In addition, IBM Security still takes a broad-based approach when it comes to positioning despite the overall new IBM having done much more on the industry alignment front. The result is that it is hard to elevate the security conversation from the usual technical conversation to the level of a more business-/industry-centric discussion.

Lastly, the distributed denial-of-service (DDoS) attack that took the Australian Bureau of Statistics (a client of IBM) offline for 36 hours in August 2016 brought some negative press for IBM. Though there was no data or security breach, the incident was an unwelcome blemish on IBM's historically strong security credentials.

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/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. The vendor market share is reflected in the MSS revenue, which is attained only in AP, and the information was primarily 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

For the purpose of this study, IDC defines managed security services as the round-the-clock management and monitoring of security solutions and activities delivered from a security operation center (SOC). We include all MSS, whether these involve the management of security solutions deployed on a customer's premises or solutions hosted in a datacenter external to a customer's premises.

There is a steady stream of new services offered by MSS providers that extend beyond traditional managed security solutions. The primary reason for many of these services is essentially to manage the security operation as a whole, including integration across various security technology domains, such as managed SOCs and different phases, such as managed response services. For additional information on MSS taxonomy, please see *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016).

LEARN MORE

Related Research

- *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016)
- *A Singapore-Based Homegrown Managed Security Services Provider Has Relaunched as Quann* (IDC #IcAP41139916, March 2016)
- *The Singtel Acquisition of Trustwave: Greater than the Sum of Its Parts* (IDC #AP40352015, December 2015)
- *IDC MarketScape: Asia/Pacific Managed Security Services 2015 Vendor Assessment* (IDC #AP251064, May 2015)

Synopsis

This IDC MarketScape presents a vendor assessment of 17 managed security services providers in the context of the Asia/Pacific region. 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 by technology buyers when selecting a managed security services (MSS) partner.

This IDC research has identified six market leaders, including NTT Com, IBM, CSC, BT, Symantec, and Verizon. Eleven MSSPs have been categorized under major players, including Dimension Data, Singtel, Accenture, HP, Wipro, Quann (formerly known as e-Cop), Fujitsu, HCL, Telstra, Orange, and AT &T.

"We have found that all the participating MSSPs have enhanced the breadth of their MSS portfolios in the past 12 months. However, the depth of advanced MSS capabilities and flexibility to deliver MSS vastly differentiated the vendors from one another," says Cathy Huang, the lead analyst for security services, IDC Asia/Pacific.

Huang adds "Also, with cybersecurity becoming more tied to enterprises' business objectives, buyers have begun to seek vendors that demonstrate an intimate understanding of their business objectives and operations."

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-community.com
www.idc.com