IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2018 Vendor Assessment

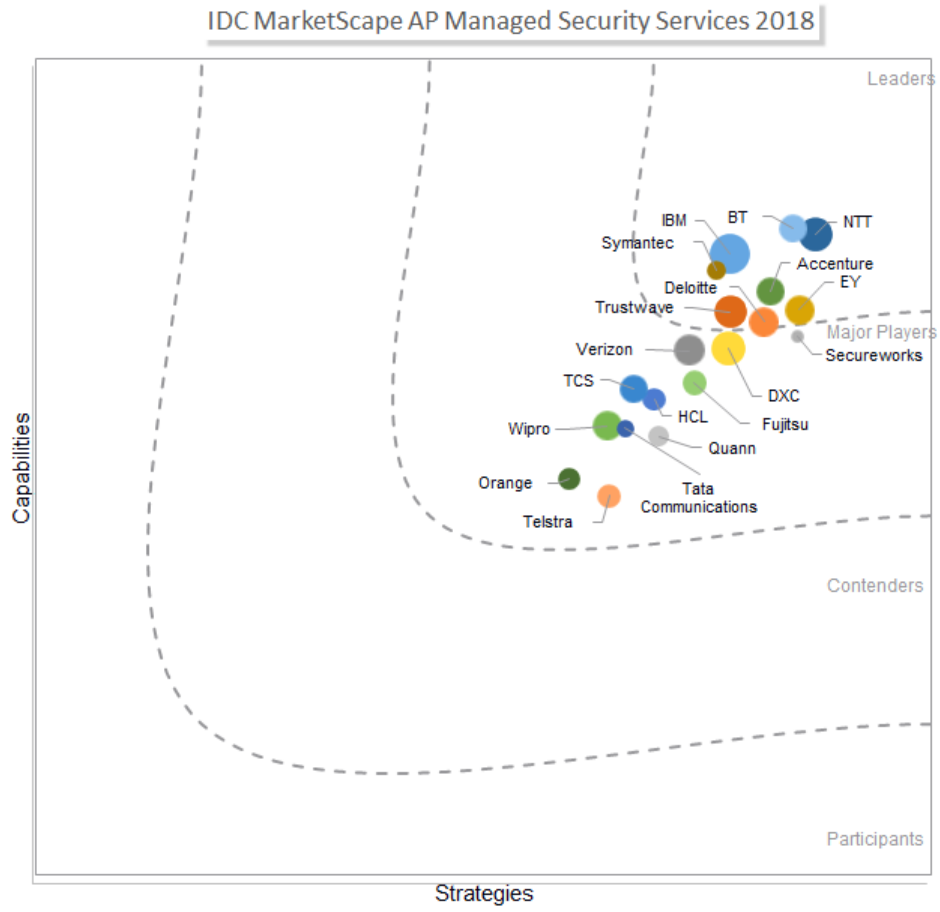
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES: NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Asia/Pacific Managed Security Services Vendor Assessment



Source: IDC, 2018

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

June 2018, IDC #AP42609818e

IN THIS EXCERPT

The content for this excerpt was taken directly from *IDC MarketScape: Asia/Pacific Managed Services 2018 Vendor Assessment* (IDC #AP42609818, June 2018). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Buyer Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Using the IDC MarketScape model, IDC studied 19 organizations in 2017–2018 that offer managed security services (MSS) in Asia/Pacific, although majority of the participating companies deliver services worldwide. The assessment reviews against a large set of parameters, such as comprehensiveness of service offerings, portfolio benefits, delivery model, market execution, cost competitiveness, platform capabilities, and customer services that define the current market demands and expected buyer needs for managed security services. Through in-depth interviews with the managed security service providers (MSSPs) and their customers, IDC evaluated the vendors in the study and found that each provider possesses certain strengths and weaknesses when compared with a peer group. All the participating companies in this study have been selected because they are strong providers and each firm differentiates itself uniquely. Besides unique differentiation, we observe several common trends among the providers in the market:

- **Platform innovation**. A substantial number of MSSPs have advanced the level of automation and orchestration in their core platforms by leveraging emerging technologies, such as artificial intelligence (AI) and machine learning, to achieve faster detection and response time. A couple of them have also elaborated the use of robotic process automation (RPA) and robotics to further streamline their security operations.
- **Flexibility and portability**. Besides automation and orchestration, flexibility and portability are also very important traits of the core platform. This enables MSSPs to seamlessly move customers through a continuum of security services as their security maturity and proficiency levels evolve and meet their specific requirements.
- **Integration**. Some MSSPs stand out as they have integrated their security information and event management (SIEM) platform with other important platforms, such as a threat management platform and/or incident response platform. As a result, it has greatly improved the security outcome and client experience.
- **Cloud security**. As part of portfolio enhancement, we see an increased number of MSSPs that have introduced a cloud security portfolio or expanded their cloud security portfolios this year. Some of the leading MSSPs stand out due to much earlier investment in the space or deeper partnership with some market-leading cloud security vendors. In addition, it is a compelling proposition when some MSSPs have moved the majority of their own core infrastructure to public cloud and have adopted their own cloud security architecture and offerings by themselves.
- **Internet of Things (IoT)/operational technology (OT) security**. Similar to cloud security, IoT/OT security has often been mentioned in the offerings road map of many MSSPs. A few of them have demonstrated pilot projects of their OT security monitoring capabilities.
- **Customer-centricity**. Customer-centricity is one of the most important factors differentiating MSSPs. This is reflected by a number of factors, including in-region local support, ease use of customer portal, reporting and service-level agreement (SLA) metrics customization, project management, onboarding process, and dedicated account/technical account management. In fact, many enterprises choose pure players despite their size over large MSSPs because of this factor.

- **Midmarket**. It's good to observe a growing number of MSSPs, especially those that have been traditionally focusing on the large enterprise market, starting to pay more attention to the midmarket. Some MSSPs have developed packaged solutions around compliance management aimed at midsize customers, which, in turn, provide a key differentiation.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC has collected and analyzed data on 19 managed security service providers within the 2018 IDC MarketScape assessment. Although there are many more MSSPs or services vendors that offer managed security services with varying degrees of portfolio and delivery capabilities, IDC narrowed down the field of players based on the following criteria:

- **Service capability across a broader MSS portfolio**. Each service provider is required to possess a fairly comprehensive MSS portfolio and delivery capabilities in the Asia/Pacific region. For instance, the vendor is required to offer a combination of security infrastructure management, security monitoring, security operation augmentation, compliance management, identity and access management, distributed denial-of-service (DDoS) mitigation, retainer-based incident response services, and threat intelligence services, among others.
- **Geographic presence**. Each vendor is required to have in-country MSS delivery capabilities in a minimum of two sub-Asia/Pacific regions: North Asia (Japan, Korea), Greater China (China, Hong Kong, and Taiwan), ASEAN (Singapore, Malaysia, Thailand, Indonesia, Vietnam, and the Philippines), South Asia (India, Pakistan), and Australia/New Zealand. The in-country security services delivery capabilities can be leveraged through local partnerships of the vendor.
- **Revenue**. Each participating company is required to have a total MSS revenue in excess of US$20 million that was attained in Asia/Pacific in 2016/2017. The MSS revenue excludes resale revenue of security products. The exception can be made to the MSSP that meets the two aforementioned criteria as well as demonstrates a strong market visibility and solid growth strategy for the region.

ESSENTIAL BUYER GUIDANCE

The Asia/Pacific 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, price benchmarks, MSSP's customer satisfaction surveys, and a third-party vendor assessment study, such as this IDC MarketScape and the upcoming threat life-cycle services IDC MarketScape study, which will place more focus on professional security services, such as security assessment, cyber range, incident response, and forensics services.

In addition, IDC recommends the following to tech buyers:

- **Shift of focus from system protection to cyber risk reduction**. As organizations progress on their proficiency and maturity levels on security, we see more mature organizations leveraging robust risk management capabilities to guide their IT security programs, representing a strong interplay of technology, process, and people. More importantly, these organizations can build a good alignment between their security programs (including the objective, security investment, adopted security controls, and so forth) and business strategies. This is particularly important in the digital age where lots of company assets become digital, in the form of data that gives greater incentives for cyber criminals and attackers to steal any form of digital assets. In addition, the crossover of cybersecurity incidents and fraudulent activities becomes more prominent because of the explosive growth of digital channels and online or mobile transactions, as organizations are leveraging these new avenues to reach out or interact with their customers. Thus, the need to protect critical assets and reduce cyber risks becomes a must to a digital enterprise.

- **Security management in hybrid environment**. As enterprises embark on their digital transformation journeys or acquire net-new IT services or replace their existing IT services, they would take a cloud-first approach. In a study when we were assessing "security through cloud," about 45% of the organizations in the region indicated that they foresee their on-premise security footprint dropping by 15% in the next three years as they move to cloud-based solutions. In our latest 2018 APEJ security services sourcing survey, *security management across hybrid environment* has been identified as the primary security challenge across markets. To tackle this challenge, IDC recommends tech buyers to consider the following:
  - **Apply "security by design"** to any new type of non-on-premise environment, including private, public cloud, managed public cloud, and multicloud. For any business/digital transformation initiatives, lines of business (LOBs) will need to work with IT organizations to include a security element in the design/proof-of-concept stage.
  - **Review the existing security solution** before investing in new security solutions. Conduct an assessment or rationalization process on the existing security solutions. Consider flexible consumption models, such as managed security services and a security-as-a-service option that can be particularly useful here when there is budget constraint.
  - **Consider disruptive/emerging solutions** that orchestrate and optimize the security functions across the physical, on-premise to the virtual/cloud/multicloud environment.
- **Service-level agreement metrics**. Traditional MSS SLAs are focused on efficiency in the contract, such as availability and response time (see Table 1 for the examples of commonly used SLA components). Although such metrics continue to be important, they fall significantly short of measuring the effectiveness of security services, and very often, IT or the security administrator is overwhelmed by a large number of alerts or false positives. IDC recommends that while it is critical to maintain the key SLA metrics focused on the availability and reliability of security infrastructure components, organizations should also develop a small number of intuitive SLA metrics, for example, risk reduced per unit (i.e., a normalized return ratio that describes the number of dollars that are purportedly "saved" in risk reduction for every dollar spent on security) that can be reported back to the lines of business which carry obvious impacts on business outcomes. This requires engaged MSSPs to have a deep industry understanding of and an industry benchmark capability for their serving clients.

TABLE 1

Service-Level Agreements

SLA Component	Widely Accepted Time Ranges Based on Aggregated Service Provider Responses
Security incident alert notification to the customer	15 minutes for a severity 1 incident
Mean time to resolution (MTTR) of an incident	3 hours for a severity 1 incident
Time to complete and report on forensic analysis after an incident	Within 1 hour of notification for a priority 1 incident
Mean time to response of a customer-generated service request	2 hours for an urgent request

Source: IDC, 2018

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 challenges.

NTT

According to IDC's analysis and customer feedback, NTT is positioned as one of the Leaders in the 2018 Asia/Pacific Managed Security Services study.

NTT represents a number of companies, such as NTT Security, Dimension Data, NTT Communications, and NTT DATA. In August 2016, NTT integrated all its MSS-specific resources and delivery platforms of NTT Group companies, including Solutionary, NTT Com Security, Dimension Data, NTT Communications, NTT DATA, and NTT Innovation Institute, to be one comprehensive "Global Managed Security Service Platform" (GMSSP).

The platform is based on its proprietary-developed security information and event management, which closely connects with its global threat intelligence platform and NTT Security threat intelligence database. It is a result of NTT Group's US$2 billion annual investment in security. The GMSSP, a critical component in ensuring service delivery consistency across multiple regions, is particularly important for enterprisewide security monitoring and management, vulnerability life-cycle management, and custom managed detection and response.

The formalization of this specialized security company aims to align investments and support its wide range of security portfolio — security consulting, systems integration, support services, and managed security services. The fronting group companies — Dimension Data, NTT Communications, and NTT DATA — will leverage their respective domain expertise to help clients support in-region or in-country requirements, for example, incident detection and response, risk management, security consulting, and solution support services, which require deep in-country understanding and in-region delivery capabilities.

Since 2017, NTT has specifically included and enhanced user and entity behavior analytics and dark web crawl into its real-time analysis. As a result, customers experience more accurate "critical alerts" with very low false positives or false negatives. The advanced analytics capabilities combining SIEM and machine learning technology with unrivalled threat intelligence, including 40% of the world's internet traffic (given the NTT telecommunications background and over 1,200 honey pots' deployment across 23 countries) and a team of quality analysts to real-time verify threat severity, have greatly improved the security outcome as well as client experience.

In 2018, NTT has also enriched security offerings for a number of use cases, including software-defined wide area network (SD-WAN) and OT/IoT environments. For example, the use of deception technology in defending Internet of Things and operating technology from cyberattacks is one of the latest innovations. Besides security for cloud (e.g., integrated cloud security services across various domains, including CASB, EDR, and threat intelligence), NTT has also effectively leveraged cloud, be it AWS or its own Enterprise Cloud 2.0, to deliver managed security services. Now, the customer can apply service order and change UTM configuration from the cloud-based control panel.

From a go-to-market perspective, NTT has a direct presence in more than 14 Asia/Pacific markets and 6 security operations centers (SOCs) in the region. At the beginning of 2018, NTT has refurbished its SOC in Singapore and often leveraged its SOC facilities (not just the Singapore SOC) to organize customer visits to educate them on advanced security analytics services and threat hunting, bringing a high level of automation and artificial intelligence to life.

Strengths

As the business grows, providing attentive service becomes a challenge. In comparison with other large MSSPs with which customers often experience long response cycles and multiple touch points for their requests, NTT customers appreciate the integrated yet effective touch point they have with NTT. This has often been cited as a key strength of NTT, from a customer experience point of view. In addition, excellent customer experience also includes a smooth setup process, dedicated delivery operation, providing industry benchmark, and so forth.

NTT's threat detection capabilities, especially around the accuracy level, are highly praised by its customers. In addition, the cloud-based, searchable raw data logs that can be used to assist with incident investigations and compliance queries are a highly regarded functionality that NTT has.

On the employee retention and management front, NTT has a very structured career rotation practice in place where three groups of analysts/researchers, including the vulnerability information research, real-time analyst, and threat information research teams, will rotate to gain wider and deeper intelligence and be continuously motivated.

In addition, NTT has continued its efforts in building thought leadership; the annual publication Global Threat Intelligence Report is gradually gaining traction in the market.

Challenges

Although customer experience is generally rated highly positive by NTT customers, there is still inconsistent customer experience and service delivery across the region. For example, in device management, the lengthy documentation required from the customer's end seems to cause a low satisfaction level.

Even as NTT's Global Managed Security Service Platform promises greater enhancement and rich functionalities, the platform migration has somewhat caused customer churn and temporary dissatisfaction. However, this does not seem to affect many loyal customers of NTT.

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 with 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 relative 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 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 operations center. We include all MSS, whether these involve the management of security solutions deployed on a customer's premises or solutions hosted in a datacenter or cloud 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 to assist clients to be more effective in managing the security element of their growing complex environment.

LEARN MORE

Related Research

- *Enhancing Security Proficiency and Addressing Challenges Brought by Cloud: A Perspective on Manufacturers and Retailers in Asia* (IDC #AP42610518, March 2018)
- *IDC's Worldwide Security Products Taxonomy, 2018* (IDC #US43535614, February 2018)
- *IDC FutureScape: Worldwide Security Products and Services 2018 Predictions* (IDC #US43286117, December 2017)

Synopsis

This IDC study presents through the IDC MarketScape model a vendor assessment of providers offering managed security services. The assessment reviews against a large set of parameters, such as comprehensiveness of service offerings, portfolio benefits, delivery model, market execution, cost competitiveness, platform capabilities, and customer services that define the current market demands and expected buyer needs for managed security services. Through in-depth interviews with the managed security service providers and their customers, IDC evaluated the vendors in the study and found that each provider possesses certain strengths and weaknesses when compared with a peer group.

"Given the wide range of maturity and heterogenous nature of the region, the Asia/Pacific managed security services market is abundant with different types of players. All the participating companies in this study have been selected because they are strong providers, and each firm differentiates itself uniquely. Although it takes time to conduct a thorough evaluation and selection process, it is important for a tech buyer organization to select the right security services provider that is trusted and provides high value. Tech buyers should leverage the right MSSPs to augment and optimize their security operations and, more importantly, transform their security programs to be more aligned with their business strategies. At the same time, this expectation, along with the vastly sophisticated threat landscape, drives security services providers to step up and accelerate their own security innovation and cyberdefense strategies to ensure themselves and their serving clients steps ahead of bad guys," says Cathy Huang, senior research manager, IDC Asia/Pacific 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.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-community.com
www.idc.com