IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2020 Vendor Assessment

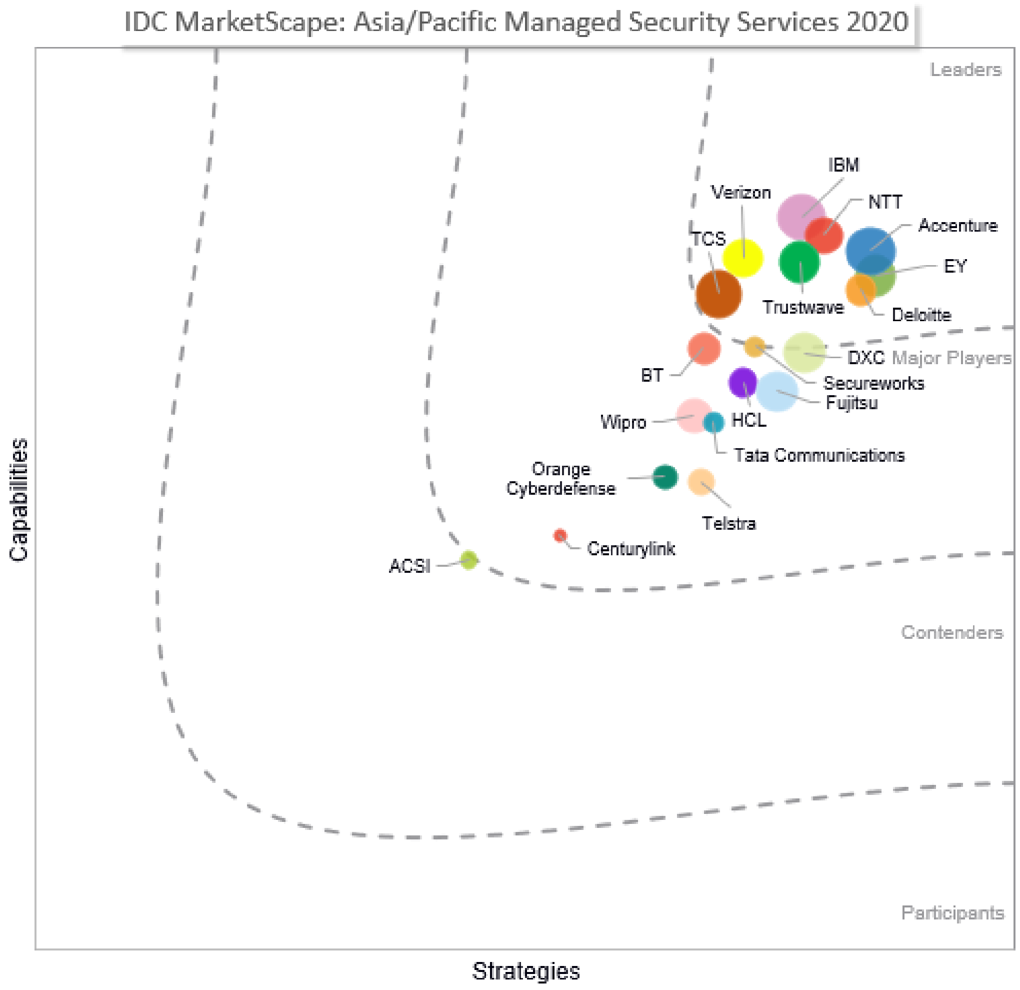
Cathy Huang James Sivalingam

THIS IDC MARKETSCAPE EXCERPT FEATURES: ACCENTURE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Asia/Pacific Managed Security Services Vendor Assessment



Source: IDC, 2020

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

IDC OPINION

As industries make rapid progress in their digital transformation journey on the back of growing regulatory pressure and an increasingly sophisticated threat landscape, many organizations are facing difficulties in maintaining a robust security posture. Perhaps more importantly, with the rising significance and impact of cybersecurity, it is no longer viewed as an exclusively technical or compliance issue, but a business and strategic issue that deserves deliberations in the boardroom. Insufficient awareness about the organization's response plan or lack of preparedness could severely impact business operations and the organization's reputation.

Accordingly, more and more CISOs or heads of IT security are now summoned to boardroom meetings to present the company's security strategy, communicate the value of security investment, and provide cyber risk updates, and so forth. The elevation of security from an add-on element to the strategic imperative status in many organizations have also increased the demand for security services such as managed detection and response, and managed threat intelligence. This increase in demand, in turn, helps drive the growth and evolution of the regional security market, where newer players seek to expand in the area, while traditional market leaders continue to enhance their offerings. Against the backdrop of these new developments, the Asia/Pacific managed security services (MSS) market is shaping up to be highly competitive and vibrant, from which organizations in the region could benefit immensely.

Using the IDC MarketScape model, IDC evaluated 19 organizations between 2019 and 2020 that offer MSS in the region. The assessment reviews the organizations against a broad set of parameters that define current market demand and expectation of MSS buyers. These include breadth of MSS offerings, portfolio benefits, threat life-cycle capabilities, cloud security, delivery model, cost management, market execution, geographic presence, thought leadership, innovation, customer satisfaction, and customer advocacy. Through primary research, in-depth interviews of vendors, and their customer references, IDC evaluated the service providers (SPs) to identify their strengths, and their challenges in the market. Some of the notable themes found in the study are:

- **Varying maturity, varying objectives.** The Asia/Pacific market is arguably the most heterogenous in nature, and as such, there is a high degree of variation in digital maturity among different organization and industries within the region. The objectives and motivations in engaging with an MSS provider also vastly differ according to the maturity levels across the market. IDC found that more mature customers, mainly those belonging in the highly regulated industries, look to vendors to augment their in-house security teams with the provider's expertise, IP, frameworks, or processes that are contextualized to the organization, or industries. In contrast, the less mature customers prefer to outsource most, if not all, of the security and compliance responsibilities to these MSS providers. Thus, vendors with end-to-end, comprehensive portfolio and vertical expertise would have an upper hand in winning accounts from both categories of customers.
- **Customer centricity, the common denominator.** Despite the differences in motivation and objectives, one thing in common between these two customer groups is the need to be customer-centric when it comes to services design, onboarding, and delivery. Customer centricity is reflected by managed security SPs' flexible delivery models, such as MSS-as-a-service option. Having this adaptive and cloudified option is especially important for clients when a growing number of workloads are moving to multiple public and private cloud. Complexity has never been greater as organizations often find themselves with unused, partially installed, and poorly configured security tools that they have accumulated over time.

There is a need for managed security SPs to address complexities, de-risk the cloud migration process, and, more importantly, optimize the cloud investment, including those embedded security tools as part of an infrastructure-as-a-service (IaaS) subscription and/or leveraged cloud security tools from security vendors. IDC observes that a vast number of participating firms could leverage on-premise security information and event management (SIEM), cloud SIEM, and a hybrid of these to offer flexibility and customer-oriented value propositions.

- **Cloud takes center stage.** Many organizations have, at this point, adopted cloud-based security services, and also progressed on the cloud security front, which is an indication of the improving proficiency of managed security SPs' cloud security capabilities. For instance, cloud monitoring, cloud access security brokers (CASB) support (mainly for protection of software as a service, or SaaS) are experiencing growing momentum in the region. Some of the managed security SPs with telecommunication providers offer their own security embedded cloud offerings that automate and orchestrate many security functions for threat detection and reporting. Furthermore, many of the participating firms in the study have enhanced their native cloud security capabilities and push offerings such as DevSecOps services.
- **Innovative user interface (UI), enhanced user experience (UX).** Customer centricity also underlies innovation at the interface level. Some of the identified leaders clearly lead the way in terms of user experience features that closely mirror social media, where app-like and Uber-style mechanisms assign available analysts to incidents and shows a stream of threat investigations, alerts, and updates. Moreover, the interface will be enabled with potential voice-controlled digital assistants.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Many service providers compete in various aspects of managed security services and other capacities. This evaluation is not an exhaustive list of all the players to consider for MSS. Instead, this evaluation reviews the primary players that offer capabilities spanning the entire life cycle of threat management from identify to protect to detect to respond to recover. IDC has collected and analyzed data on 19 managed security SPs for this IDC MarketScape. IDC narrowed down the field of players based on the following criteria:

- **MSS portfolio.** Each service provider is required to possess a fairly comprehensive MSS portfolio, with at least 50% or more matching to IDC's scope of MSS taxonomy, including managed threat intelligence services, managed detection and response services, managed network security services, managed endpoint security services, managed secure web gateway services, cloud posture and compliance monitoring, and OT/IoT monitoring.
- **Geographic presence**. Each vendor is required to have in-country MSS delivery capability (or presence of a security operations center, or SOC) in a minimum of two Asia/Pacific subregions: North Asia (Japan, Korea), Greater China (China, Hong Kong, and Taiwan), Southeast Asia (Singapore, Malaysia, Thailand, Indonesia, Vietnam, and the Philippines), South Asia (India, Pakistan, Sri Lanka, Bangladesh), and ANZ (Australia and New Zealand).
- **Revenue.** Each participating company is required to have a total revenue in excess of US$10 million that was attained in Asia/Pacific in 2018.
- **Multipoint assessment completion**. Each participating company is required to complete a multipoint assessment covering a total of 29 capabilities and strategy criteria defined by IDC to be most conducive to success in delivering managed security services in the region.

ADVICE FOR TECHNOLOGY BUYERS

As picking the right security vendor is a critical business and strategic decision that should ideally align with their overall business goals, here is IDC's advice that organizations should keep in mind when choosing their vendor-partner:

- **Embrace security by design.** For tech buyers that have just started their digital transformation journey (of which cloud is a key enabler), it is critical to make security foundational or to embrace "security by design" when adopting any new technology or deploying into the cloud to ensure maximum but affordable security and visibility.
- **Incorporate and integrate cyber risk monitoring**. If the organization has an existing managed security SP, review the service-level agreement (SLA) and add metrics regarding cyber risks. In the latest *IDC FutureScape: Worldwide Security and Trust 2020 Predictions*, IDC predicts that, by 2021, 80% of publicly traded companies will embed cyber-risk monitoring into their business planning and quarterly reporting. Continuous cyber-risk monitoring will become table stakes and foundational in business-to-business (B2B) relationships and instrumental in attracting investors and building trust. Building such a process will help drive a more secure and correspondingly trustworthy organization. This will also lead to a tighter integration of an organization's IT and business strategies so technology risk can be translated to business risk.
- **Augment technical capabilities with vertical expertise.** What does it mean for managed security SPs? Your managed security SPs should not only have excellent technical expertise, but also vast experience in business risk or offer cyber risk strategy services. To build effective cyber risk strategies and align them with business goals require deep industry expertise and ability to develop industry-specific threat models that go beyond conventional infrastructure layer monitoring. Based on IDC's evaluation of participating vendors, the majority of the vendors servicing the region are to a degree differentiated by their track record and vertical competencies.
- **Continually review and assess.** For tech buyers that are not in a regulated industry and have a record of limited security investment, it is important to review your organization's current security needs and evaluate if the current setup or vendors are sufficiently equipped with the capabilities to meet both current and future needs. For instance, does the current workflow of the SIEM systems generate too many alerts? What is the rate of false positives? Can new sources, such as IoT connected devices, be added to SIEM? What is the automation rate of Level 1 tasks (e.g., log assembly and triage)? What is the productivity level of SOC analysts? In the near term, evaluate the efficacy of the current SOC setup with key metrics such as time to qualify (an incident), mean time to detect, mean time to mitigate, mean time to recover, rate of automated responses, and alert accuracy. Further, buyers from the critical infrastructure sector stand to benefit from engaging a managed security SP to operationalize the IT-OT convergence and particularly address the rising cyber risks on industrial systems and OT/IoT environment.
- **Deploy emerging technology, consume flexibly**. Leverage artificial intelligence (AI)/machine learning (ML), automation, and threat intelligence analytics to scale and improve current SOC operations. Many of the participating firms in the study have shown significant improvement in their SOC/SIEM capabilities, specifically in analytics, automation, and contextualization. The managed security SP can leverage and incorporate various analytics and AI/ML tools to its SIEM platform to reduce false positives and enhance orchestration and automation. Moreover, the managed security SP should provide flexible options, including cloud SIEM, to its customers. As IT environments' requirements evolve and cloud companies such as Amazon Web Services (AWS), Google, Microsoft, and AliCloud begin to enhance their security

offerings, security as a service will have a greater influence for those organizations with limited IT resources, smaller budgets, and escalating awareness of their security shortcomings. As such, managed security SPs should be flexible with their delivery options, including cloud-based security as a service, as we expect to witness increased market demand.

VENDOR SUMMARY PROFILE

This section explains IDC's key observations resulting in Accenture's position in the IDC MarketScape and provides a summary of the vendor's strengths and opportunities.

Accenture

According to IDC's analysis and customer feedback, Accenture is positioned as one of the Leaders in the 2020 Asia/Pacific managed security services IDC MarketScape

Accenture provides a comprehensive managed security services portfolio in the Asia/Pacific region, including Threat Operations, XDR (Expanded Detection and Response), Managed Digital Identity, and Managed Application Security. On the threat life cycle front, Accenture's in-house solution, iDefense, which includes threat sensing, prediction, detection, defense, and repulsion, adds significant differentiation to its MSS portfolio. On top of it, Accenture is scheduled to release a new AI/cognitive platform coded "Emily" to drive better operational and strategic risks, which allows customers' CISOs to operate at a higher level in their organization.

Accenture Security will acquire Symantec's Cyber Security Services business from Broadcom, which includes global threat monitoring and analysis through a network of SOCs, real-time adversary and industry-specific threat intelligence, and incident response services. Enterprises will benefit from Accenture's and Symantec's combined expertise fine-tuned to their industry with tailored global threat intelligence powered by advanced analytics, machine learning, orchestration and automation capabilities. Four of its six SOCs are in Asia/Pacific: Australia, India, Japan, and Singapore. Once completed, this acquisition will give Accenture Security's managed security services unprecedented scale globally.

Accenture Security is continually investing and enhancing its existing services by acquiring new companies and working closely with its partners to create differentiated solutions, and address critical business challenges. For instance, Accenture has established multiyear-long, multimillion-level co-development partnerships with Splunk and Palo Alto Networks, respectively, to develop a capability for continuous cloud compliance management, secure software-delivered networking solutions, and managed threat operation centers for app-based delivery.

In addition, its blockchain-based digital identity services use core technologies of distributed ledger technology and biometrics such as facial recognition and fingerprints. Besides technology partnerships, Accenture is developing joint relationships with complementary industries such as insurance companies to support its customers. For example, Accenture has teamed up with AXA XL to provide global cybersecurity services to AXA XL's underwriters, brokers, and clients while enhancing Accenture's overall experience with distributed customer segments and markets. Maintaining deep relationships with more than 25 strategic partners, Accenture constantly evolves its MSS capabilities and portfolio.

Accenture develops new offerings that can accelerate and secure clients' digital transformation initiatives. Such is seen with the development of new offerings such as trusted AI, blockchain, and IoT security (by leveraging its recent Deja vu acquisition).

From a go-to-market perspective, Accenture leverages its broad portfolio across consulting, strategy, digital, operations and its deep industry-specific expertise to embed its security capabilities. In the case of cloud security, global cloud providers such as AWS, Google Cloud Platform and Microsoft Azure along with Palo Alto Networks, have all partnered with Accenture as anchor partners for full life-cycle services around secure migrating, maintaining, and operationalizing workload to cloud. At the moment, a considerable percentage of global MSS customers use Accenture's cloud security capabilities, and Asia/Pacific region is registering a fast-growing momentum.

Strengths

Accenture continues its industry-driven approach to security, which significantly helps its resources to deepen their understanding of the respective operating models and value chains, including sector-specific regulatory needs. Within the Cyber Fusion Center, Accenture builds different pods catering to different industries. For example, a life science pod comprises a pool of security professionals who only support life science organizations. This allows Accenture to contextualize threats to business risks and provide customized, fit-for purpose solutions. In its overall strategy, it aims to raise the relevancy of MSS in organizations to a strategic business function and desirably as a market differentiator.

Accenture's global model ensures the delivery of efforts and benefits from its global resources combined with their local delivery capability. Its Form methodology used for co-creation with clients is another key differentiator. This methodology unleashes innovation by discovering true client needs and creating ways to quickly map the right solutions for various or unique needs. Examples are an attack surface management of SCADA/OT systems for a client in Malaysia and a secure 5G solution for a client in Japan.

Accenture invests a significant amount of resources in research and development (R&D) for innovation. Its Cyber Applied Innovation Fusion Centers in Asia/Pacific employ multidisciplinary approaches including R&D, artificial intelligence (AI), and co-development with clients. In addition, it has invested in people development, training, skills, diversity, and certifications. In 2019, Accenture Security doubled the number of custom security classes and significantly increased its security training budget, helping with the skill enhancement and retention of its employees.

Challenges

According to customers' feedback, despite Accenture's use of automation and emerging technologies to drive efficiency, the vendor can still improve how it demonstrates the business value of its services. To this end, Accenture has rolled out "Measurements of Value Excellence (MOVE)" which helps to enhance and provide transparency to its MSS customers.

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, the 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 represent 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 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, or MSS, as the round-the-clock management and monitoring of security solutions and activities delivered from a security operations center, or 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 or cloud external to a customer's premises.

There is a steady stream of new services offered by MSS providers that extend beyond traditional MSS solutions such as managed threat intelligence and managed detection and response, which directly link to an outcome.

LEARN MORE

Related Research

- *IDC FutureScape: Worldwide Security and Trust 2020 Predictions — APEJ Implications* (forthcoming)
- *Acceleration of Outcome-Driven Managed Security Services in the Asia/Pacific Region* (IDC #AP45395519, January 2020)
- *Security Investment Priorities and Requirements by Verticals: BFSI, Manufacturing, and Retail in Asia/Pacific* (IDC #AP44700819, December 2019)
- *IDC FutureScape: Worldwide Security and Trust 2020 Predictions* (IDC #US45582219, October 2019)

- *Distributed Denial-Of-Services Attacks Are Increasingly Used to Negatively Impact Business in Asia* (IDC #AP44718419, July 2019)
- *Lessons Learnt from the SingHealth Case – Effective Incident Response Strategy and Consideration of Zero Trust Security Framework* (IDC #AP43913219, February 2019)
- *IDC MarketScape: Asia/Pacific Managed Security Services 2018 Vendor Assessment* (IDC #AP42609818, June 2018)

Synopsis

The IDC MarketScape: Asia/Pacific Managed Security Services 2020 Vendor Assessment study evaluates 19 vendors providing managed security services within Asia/Pacific. Participating vendors were assessed against 29 different market determining criteria, which include breadth of service offerings, portfolio benefit, services delivery model, market execution, cost management, customer satisfaction, and business performance. IDC conducted a series of interviews and multipoint assessments with vendors and their clients, to comprehensively capture the differentiating factors, strengths, and challenges of each vendor. Following comprehensive and exhaustive analysis, the results were deliberated with IDC's internal panel of expert analysts, resulting in a positioning within the IDC MarketScape figure.

"The top managed security SPs not only have excellent technical expertise and threat life-cycle management capabilities, but also vast experience in cyber risk strategy and services," said Cathy Huang, associate research director, IDC Asia/Pacific Services and Security. "To build effective cyber risk strategies, a managed security SP has to align with business goals, which requires deep industry expertise and capability to develop industry-specific threat models that go beyond conventional infrastructure layer monitoring," she advises.

"The threat landscape continues to evolve at a breakneck speed, and security providers have to consistently be one to two steps ahead of the bad actors," warned James Sivalingam, research manager, IDC Asia/Pacific Services and Security. He added, "The situation is made more challenging in a rapidly digitalizing region such as Asia/Pacific, where organizations have varying levels of maturity across different countries and verticals. However, the study has found that all the major security vendors servicing the region are more than prepared for the challenges for now. In addition to robust capabilities, technologies, and bandwidth to mitigate the prevailing risk factors, security services providers should position themselves as strategic partners to their respective clients and help them achieve security by design to deliver true value to the customer in the region,"

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

Copyright and Trademark 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. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2020 IDC. Reproduction is forbidden unless authorized. All rights reserved.