IDC MarketScape

IDC MarketScape: Asia/Pacific Cloud Security Services 2021 Vendor Assessment Study

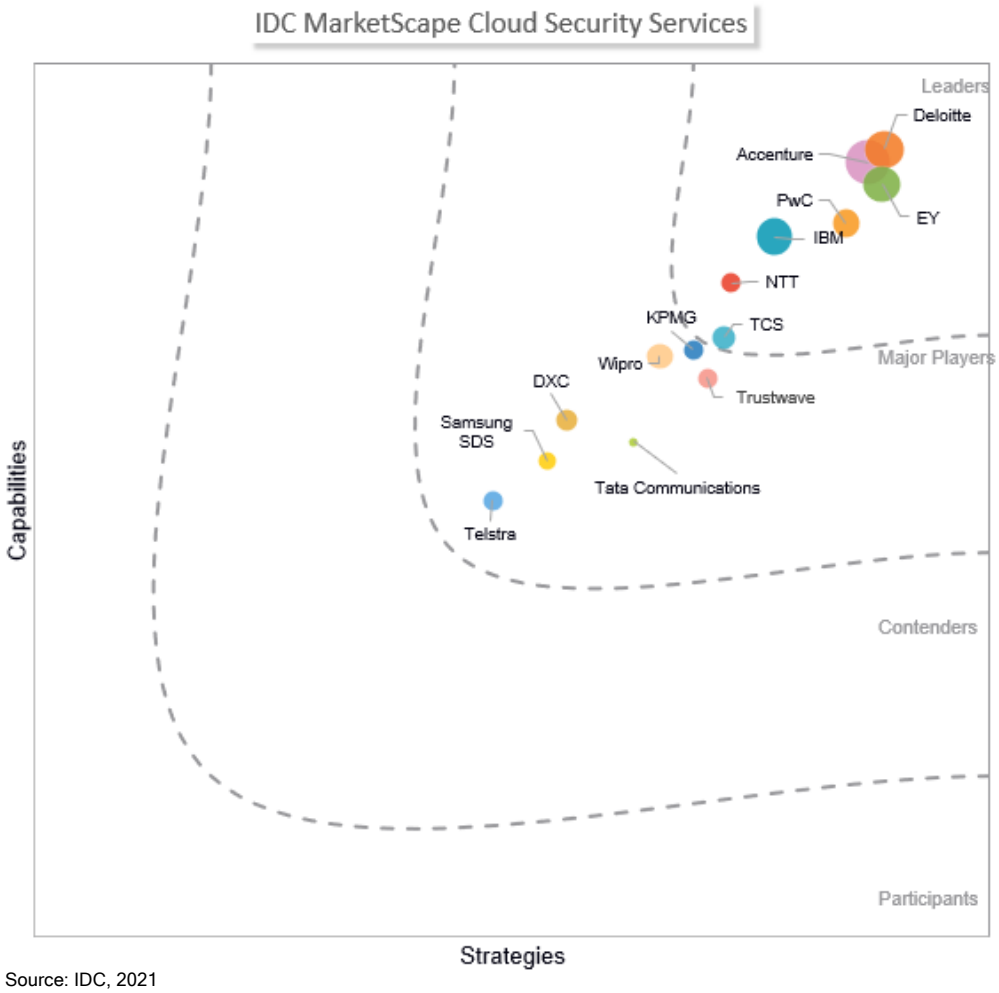
Cathy Huang James Sivalingam

THIS IDC MARKETSCAPE EXCERPT FEATURES: NTT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Cloud Security Services



Source: IDC, 2021

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

June 2021, IDC #AP47097721

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Asia/Pacific Cloud Security Services 2021 Vendor Assessment (IDC Doc # AP47097721). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The cloud-first approach took the Asia/Pacific market by storm in 2020. Fast-growing organizations in Asia/Pacific tend to adopt a cloud-first or cloud-only approach when digitizing their business to take advantage of the agility, efficiency, and resilience that cloud technology promises. According to data from IDC's *2020 COVID-19 Impact Survey*, investments in cloud technology have often been identified as a top priority among businesses in the region. For instance, about 42% of organizations in the Asia/Pacific region indicated that they use cloud as a platform for digital innovation. Similarly, 42% of enterprises also indicated they would move more applications to cloud because of its enhanced security and availability. Despite the varying degree of maturity levels in the cloud transformation journey among businesses in Asia/Pacific today, security continues to be critical in enabling customer trust and building confidence in cloud-based platform and services as the technology steadily progresses at all levels.

This IDC study assesses cloud security services vendors in the Asia/Pacific region on their strength of their current capabilities, portfolio, delivery, and go-to-market (GTM) activities and how well placed they are to grow within the space in the region. Key findings of this research include:

- **Comprehensive breadth of cloud security offerings.** A majority of the cloud security services vendors assessed demonstrated formidable breadth and depth in terms of service offerings from assessment, advisory, and implementation to management and optimization. The wide range of offerings is reflective of the growing customer demand and indicative of vendors' abilities to address broader customers' concerns on cloud migration, securing cloud infrastructure and cloud workloads, and security transformation. Offerings such as security posture assessment across cloud and hybrid environments, cloud risk framework and architecture design, cloud platform engineering and integration, and managed cloud operation services are in high demand. Mature clients that have adopted cloud for several years are now focusing on adopting security at greater scale and speed. Therefore, pattern development, SecDevOps, and continuous security monitoring service remain imperative in the region.
- **Services aligned to cloud-native solutions/platforms**. A sizable proportion of all the available cloud security services offerings are closely aligned to major cloud hyperscalers' solutions, indicating that many of the offerings are also ecosystem-driven. These include secure Amazon Web Services (AWS) Landing Zone and Azure Sentinel Implementation, Managed Services and Support. These tightly knit service offerings and ecosystem support indicate strong partnerships among hyperscalers and the service provider community, particularly around security competency and hands-on experiences in working with cloud-native solutions. As some of the cloud-native platforms have a much faster innovation cycle, clients should also be able to depend on their security partner for strategic advice when it comes to picking the different features applicable to their respective environments. Additionally, the clients and end users interviewed for the study appreciated vendors that were proactive in recommending new approaches, methodologies, and emerging technologies to be part of their cloud security strategy services engagement.

- **Localization and market penetration**. Customers in the region expect their cloud security services vendor to possess a deep roster of local resources and a sizable presence to understand the market's specific needs, nuances, and challenges. Although a majority of the participating firms have demonstrated a deep understanding of market dynamics, only 40% have a local presence in more than 10 Asia/Pacific markets. The rest still have obvious gaps from a geographic coverage standpoint, and the majority of their cloud security service businesses come from fewer than three Asia/Pacific markets. To a large extent, this porous market dynamics provides tremendous opportunities for country-specific vendors serving in their home market to thrive while playing the role of GTM ecosystem partners for some of the big global cloud security services vendors.
- **Pricing mechanism under microscope**. Several customers interviewed for the study raised some concerns of the black-box approach to pricing and expressed their increased expectation for a flexible and an outcome-based pricing model in this new as-a-service era. About 28% of the participating firms' pricing models were lauded by their clients, particularly because of the vendors' practice of transparency and communicating value realization in their security engagement. Some customers also applauded the effective use of automation and offshore resources to keep the engagement cost competitive yet seamless and disruption-free.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This evaluation does not offer an exhaustive list of all the players in the Asia/Pacific cloud security services market. IDC narrowed down the field of players based on the following criteria and subsequently collected and analyzed data on these 14 cloud security services providers with relevant portfolios and regional scale in this IDC MarketScape study:

- **Revenue.** Each participating company is required to have a total revenue in excess of US$10 million and attained in Asia/Pacific in 2020.
- **Geographic presence.** Each participating firm is required to have services delivery capabilities in at least one of the following subregions: Australia and New Zealand (ANZ), the Greater China region, South Korea and Japan (North Asia), Southeast Asia, and India.
- **Partnership and certifications.** Each participating firm is required to possess partnerships with at least two hyperscale cloud providers and related security certifications, such as AWS, Azure, Google Cloud Platform (GCP), or Alibaba Cloud.
- **Cloud security strategy and offerings.** Each participating vendor should show a clear cloud security services strategy and offer a set of cloud security services that can map to IDC's cloud security services definition.

ADVICE FOR TECHNOLOGY BUYERS

This IDC study represents a vendor analysis and assessment of the 2021 Asia/Pacific Cloud Security services market through the IDC MarketScape model. Based on this study, IDC recommends that buyers consider the following pieces of advice:

- **Design and deploy base security controls to create secure landing zone on the cloud solution provider platform**. Landing zones pre-provisioned through secure coding ensure that security is foundational, and the migration and deployment satisfy the necessary security, governance, and compliance requirements.

- **Design reusable cloud solutions to secure platform-as-a-service templates with integrated security controls**. Adopting a "build once, deploy many" approach with security-integrated platform-as-a-service (PaaS) templates ensures the efficient use of resources, quick scaling of operations, and speed to market without compromising security.
- **Spell out the authorized roles to operate in the environment and what they can do**. With access management being critical, IT leaders are encouraged to use cloud infrastructure entitlements management (CIEM) solutions to manage identities and access privileges in their cloud and multicloud environments that apply the principle of least privilege.
- **Secure connectivity to on-premises datacenters and use a hub-and-spoke network security model**. Adopting a hub (central network zone) and spoke (internet, on-premises, hosted private cloud) model enables efficient security policy management and enforcement in a central location and allows for the separation of concerns.
- **Select vendors with robust growth and partnership strategies to access the latest technologies and platforms**. A robust security partner does not only address the current security challenges but also foresees future problems and proactively suggests relevant upgrades and security optimization. Thus selecting vendors that are progressive and routinely involved in co-innovation exercises with hyperscalers and solution providers will bode well for long-term transformation goals.
- **Regularly engage independent or third-party security assessments to ensure security systems are in check**. Although it is easy to transfer the risk to the security partner, clients should also routinely audit and assess their security systems even when not required by regulatory compliance to ensure continuous improvement and assurance.

VENDOR SUMMARY PROFILE

This section 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 areas for improvement.

NTT

According to IDC's analysis and customer feedback, NTT is positioned as a leader in the IDC MarketScape: Asia/Pacific Cloud Security Services 2021 vendor assessment study.

NTT is a global technology services firm that operates a global network of SOCs and Global Threat Intelligence Centers with direct presence in 17 countries in Asia/Pacific. NTT's primary cloud security strategy revolves around supporting its clients' DX journey with service offerings from consulting and managed services to technology support services. Its cloud security operations in the region are supported by around 1,000 cloud professionals who work closely with 800 security professionals.

NTT's professional security service is anchored around its consulting digital platform SecureInsight, which ensures a globally consistent service delivery while supporting clients' needs in a modular fashion. A typical consulting engagement of this nature starts with a capability maturity review, which provides clients with a bird's-eye view of their security controls, maturity, and capabilities. The findings could then be augmented further with NTT's cloud security posture assessment, which delivers a snapshot of the actual cloud tenancy configurations, and with a quantitative risk analysis capability, which produces greater visibility of the risks and impacts to the organization. This integrated platform also features "control validation" capabilities, which enable NTT to validate critical security controls continuously.

Meanwhile, NTT's managed security service practice is also rather comprehensive, offering a slew of cloud-focused services, such as enterprise security monitoring, cloud security posture management, threat detection for public cloud, and IaaS gateways, including attacks on web applications. To help clients streamline and simplify the daunting process of technology selection, NTT continually assesses, selects, and pre-integrates a partner technology into its managed security services platform.

NTT engages with more than 200 technology partners and leverages strategic partnerships to drive innovation within the cybersecurity space and deliver scalable security to its clients. It has formed a multiyear strategic alliance with Microsoft with the goal of delivering best-of-breed solutions to clients by combining the strengths of the two companies. As a result, NTT is currently developing purpose-built advanced threat detection (ATD) for Microsoft Azure assets, especially servers, firewalls, and application gateways. Further, NTT Security Unit also collaborates and co-innovates with its cloud infrastructure unit to build solutions on Azure, creating tools, such as cloud threat detection and AI-/ML-based threat detection services for its cloud clients on Azure.

Strengths

The tight integration of security with other practices within the wider NTT Group is a deliberate approach to help clients achieve its secure by design ambitions. NTT's cloud security services strategy is client-centric and globally aligned to reflect the macromarket drivers. From a portfolio perspective, in 2020, NTT launched its Global Portfolio Review Board, which ensures the global and regional plans align to meet the needs of its clients. Although it is a global strategy, it allows regions to create adapted versions of the strategy for execution based on local client priorities.

NTT has invested a sizable number of well-trained resources dedicated to the Asia/Pacific region, and the return is evident. Its customers reflected positively on the technical expertise, knowledge, and capabilities of NTT's cloud and security professionals. Besides that, NTT's customer experience strategy is also well developed, with technical account managers (TAMs) always on call to support and provide clients with actionable insights and technical recommendations. At the onset of the COVID-19 pandemic, NTT worked with several of its clients to advise them on how they can efficiently use its services and provided incident response remediation services at no cost to clients in the healthcare sector, which was crucial to delivering care at the height of the pandemic.

NTT's broad portfolio, especially the fact it owns the global network, makes it an attractive option in the market. Apart from extensive offerings, NTT also has a slew of proprietary tools, such as the Cyber Threat Sensor (which assists clients in detecting potential threats in their cloud environments) and web application firewall-as-a-service offerings (which protect enterprise web applications deployed in the cloud). By integrating emerging technologies, such as AI and ML, that power enhanced levels of automation, NTT can also achieve service consistency across different markets. In addition, the acquisition of WhiteHat Security has further matured its DevSecOps capability in terms of application development.

Challenges

As discussed, NTT is a proven security provider, possessing several characteristics that make it stand out in the region. However, there are areas that the vendor can further improve. For instance, organizationally, NTT is still fragmented, which, at times, results in inconsistent service quality as it is operated by different units. Although it is a good move to establish a strategic alliance with Microsoft, it is equally important to provide options to clients, especially those that prefer to engage multiple cloud hyperscalers.

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 the customer's 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 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.

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 to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

IDC defines a set of security services whose primary focus is to provide security management capabilities to ensure 24 x 7 operations of cloud technologies and architectures as well as "embedded" professional security services in which security consulting, assessment, and advisory services are incorporated into a cloud engagement, such as cloud security assessments, cloud-driven policies and architecture reviews, cloud security strategies, and so forth. The ultimate objective of these services is to ensure secure cloud migration and continuous assurance in monitoring and protecting the hybrid multicloud environment. For more details, please refer to *IDC Market Perspective Cloud Security Services — Accelerating Migration to Cloud and Assuring the Client Value Continuously* (IDC #AP46319221, March 2021).

Security management capabilities include the management of both threats and risks, often including monitoring, threat detection and response services, and security management pertaining to managing identities, cloud-native applications, workloads, containers, and data in the multicloud/hybrid cloud environment.

LEARN MORE

Related Research

- *IDC's Worldwide Security Services Taxonomy, 2021* (IDC #US47681721, May 2021)
- *Cloud Security Services – Accelerating Migration to Cloud and Assuring the Client Value Continuously* (IDC #AP46319221, April 2021)

Synopsis

This IDC study represents a vendor assessment of the Asia/Pacific cloud security services market through the IDC MarketScape model. The evaluation is based on a comprehensive and rigorous framework that assesses vendors relative to one another against the criteria which are the factors expected to be the most influential for success in both the short term and the long term.

"Over the course of the study, it is amazing to learn how some of the Asia/Pacific organizations which have adopted cloud for several years are now focusing on adopting security at greater scale and speed. The value of engaging a cloud security services vendor really provides the continuous assurance and operational excellence to these mature organizations. At the same time, for organizations just starting on their cloud transformation journey, it is very important to have an expert view to assess, design and implement the relevant security frameworks at the early stage, and adopt the applicable cloud-native controls accordingly," says Cathy Huang, Associate Research Director for Services and Security at IDC Asia/Pacific.

"Moving to the cloud provides organizations in the region a chance to rethink their infrastructure, business applications, and overall digital transformation strategy," says James Sivalingam, research manager, IDC Asia/Pacific Services and Security Research. "However, cloud migration is not as simple as the strategy lift and shift implies, and there are several layers of complexities involved in secure migration to the cloud. In addition to modernizing application, adhering to 'secure-by-design' principles, and managing workload and data across different environment, businesses continue to face run-of-the-mill security challenges now with an added layer of cloud complexity. Thus, finding the right security partner is imperative to ensure the security is foundational to the cloud journey," adds Sivalingam.

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
blogs.idc.com
www.idc.com