IDC MarketScape

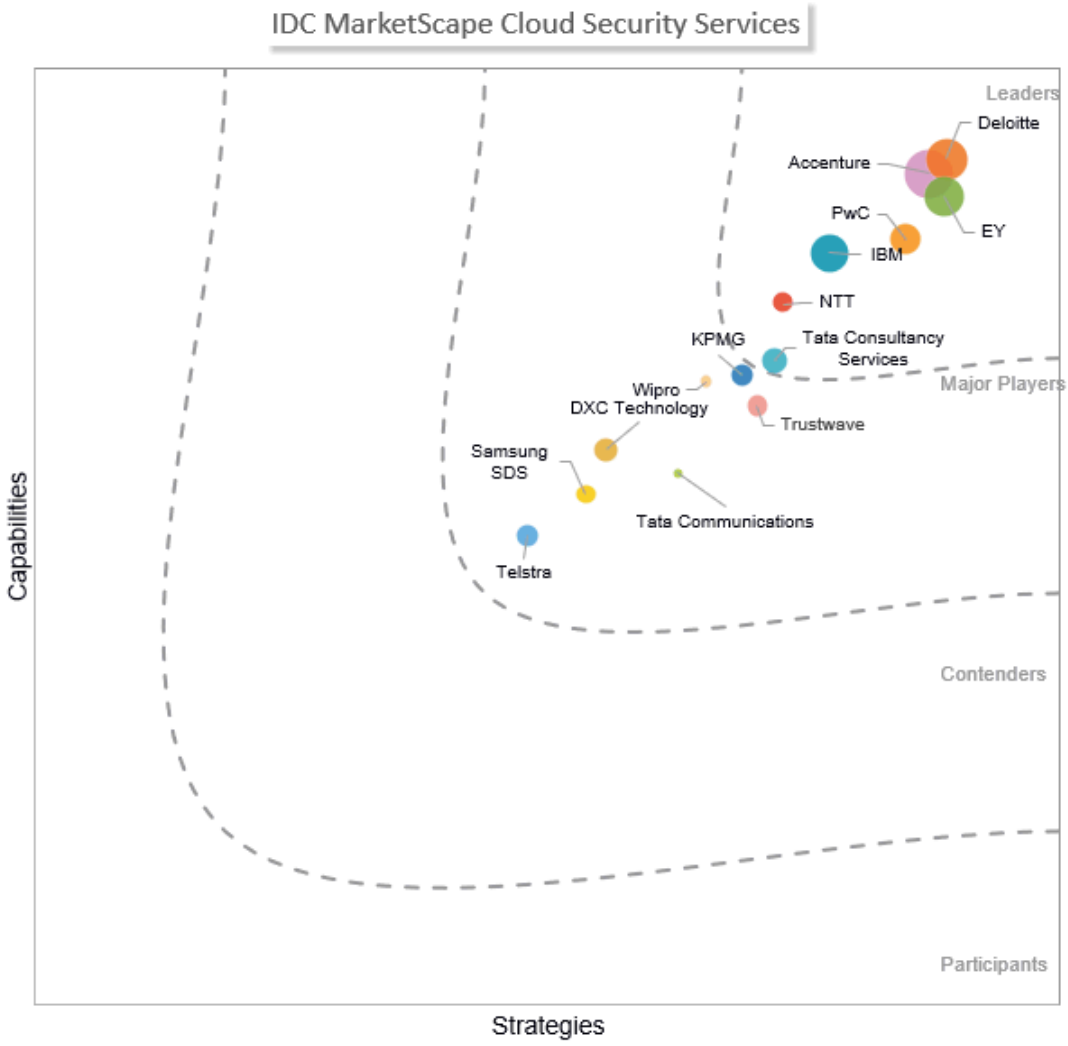
IDC MarketScape: Asia/Pacific Cloud Security Services 2021 Vendor Assessment Study

Cathy Huang James Sivalingam

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Cloud Security Services



Source: IDC, 2021

June 2021, IDC #AP47097721

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

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.** Majority of the cloud security services vendors assessed demonstrated formidable breadth and depth in terms of service of 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 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 majority of their cloud security services 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 expresses 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 vendor's 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 easy to transfer the risk to the security partner, clients should also routinely audit and assess their security systems even when not required by the regulatory compliance to ensure continuous improvement and assurance.

VENDOR SUMMARY PROFILES

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.

Accenture

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

Accenture's cloud security strategy is deliberately integrated into all of its transformation and cloud adoption engagements with the intention to embed security early to drive optimal outcomes. Its multilevel customer governance structure plays a primary role in ensuring cross-functional integration and timely decision making. Being part of Accenture's recently announced US$3 billion Cloud First initiative, its cloud security services business is expected to increase exponentially.

Accenture has put concerted efforts in driving its cloud security business to be asset-based rather than people-based, which drives the firm to invest in machine learning (ML), artificial intelligence (AI), and automation. Accenture has developed hundreds of assets, templates, and prebuilt accelerators for the deployment of cloud-native security controls and security management for cloud environments. The proven assets improve the time to value and cost effectiveness of its offerings.

Standardization templates and automation are critical for Accenture to achieve delivery consistency, with fewer full-time employees required to support daily operations. For instance, Accenture's function as a service removes the need for infrastructure deployment and management and creates a proactive, self-healing environment with little to no human interaction required. The focus and investment in AI/ML and automation are strategic to Accenture; those areas have been identified as key differentiators and growth drivers for its cloud security services.

Accenture has strategic relationships and a deep experience with a vast partner network. Besides formalizing specific business units with various hyperscalers, Accenture has partnerships across all major security domains, namely governance and compliance, identity, application security, data privacy and protection, and cyberdefense.

Accenture has global security operation center (SOC) delivery teams across seven locations in Asia/Pacific. Its strategic investments in InCountry and TripleBlind also enable Accenture to support clients' data residency concerns. In addition, Accenture has rigorous customer satisfaction and quality assurance reviews, with continuous closed-feedback processes to ensure value creation and an outcome-based delivery. Relating to this, Accenture has many commercial models that tie to value (e.g., level of fraud/incidents reduction) and ensure it has some skin in the game, in which Accenture acts as a true partner with its client. Its recent casualty transformation program is an interesting initiative that correlates upstream issues (e.g., basic security hygiene) to overall managed security services cost reduction.

During the pandemic, Accenture initiated numerous programs to better support its customers without imposing additional charges, including a round-the-clock enablement of its client resources to work remotely and extended security support for cloud environments to minimize the impacts to the service levels provided.

Strengths

Accenture has demonstrated strong automation capabilities across the life cycle of client engagements, not only in the mentioned delivery stage but also in the initial stage in which Accenture's Cloud Security Quick Start tool can autodiscover all assets and services the client is using across various hyperscaler providers and rapidly identify and establish a risk-aligned architecture for baseline cloud security and overall security investment optimization. One example is called the "no regrets" configurations, which leverage the use of functions to automatically maintain the risk posture of a client's cloud environment.

Accenture's end-to-end security capabilities and much broader services portfolio attract many clients that deeply value the breadth of its offerings. Accenture's operation expertise and large-scale complexity management make it an attractive option in the market. Moreover, for heavily regulated industries, such as the financial services, critical infrastructure, healthcare, and public sectors, Accenture has a strong focus and expertise on proactive compliance and security assurance.

Accenture has deep engineering capabilities and strong, long-standing research and development (R&D) relationships with AWS, Azure, GCP, Alibaba Cloud, and IBM. For instance, it is the strategic launch partner of many hyperscalers, such as AWS, Azure, and GCP. Accenture works with hyperscalers' product and engineering teams in advance of the release of cloud-native security solutions.

According to client feedback, Accenture manages staff turnover well. It can retain knowledge and quickly staff projects with the right people. This reflects well on "One Accenture" in which all teams and people are incentivized based on shared goals. It also shows the depth of talent and agility the firm has when it comes to staffing. It is effective in managing knowledge sharing and enablement across Accenture and the client team, enabling the resources to quickly adapt to the constant changes brought by cloud.

Challenges

Given that the nature of many cloud security operations is cosourcing, Accenture could do better in motivating security engineers/analysts at the client side or giving them sufficient time to achieve each project milestone. In addition, the cost of Accenture's offering, if it adopts discreetly, is significantly higher than competitors', especially in markets such as Japan, which requires local language support.

Deloitte

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

Deloitte is a premier brand with a broad portfolio and commands a large number of competent professionals to ensure quality service delivery. Deloitte's cloud security offering is split into two buckets — direct and integrated — which are incorporated into a broader set of products and cloud platform services. These integrated services include cloud-native development, secure app migration, and business transformation services. The firm, whose security portfolio is one of the most extensive in the market, offers end-to-end, full life-cycle security services, from assessment, advisory, and implementation to operation/managed and optimization.

By positioning itself at the intersection of business transformation, security, and compliance, Deloitte brings business- and industry-focused risk insights to clients across various verticals. Deloitte's cloud governance and compliance offerings enable the firm to address the critical client requirement for the continuous assessment of its cloud security posture, whereas its cloud threat monitoring offering provides 24 x 7 detection and response services for clients' cloud and hybrid cloud platforms. The monitoring services are done using cloud-native security information and event management (SIEM) and SOC services optimized for a cloud environment. At the start of 2021, Deloitte acquired root9B, a cloud-native network security platform provider, to further enhance Deloitte's capabilities within the space.

As an early adopter of cloud, many of Deloitte's Cyber Intelligence Centers (CICs) in Asia/Pacific are entirely hosted on the cloud. Deloitte has been delivering SOC services with Azure Sentinel since the platform's genesis in 2019, further contributing to cloud-native SIEM adoption in the region. Deloitte also helps its clients integrate security controls within the software development life cycle and cloud-based tool and build a secure DevOps continuous integration and continuous delivery (CI/CD) pipeline via robust professional services practices.

In addition to its extensive portfolio, Deloitte also developed a slew of cloud security accelerators, frameworks, and methodologies to ensure quality service delivery at scale without compromising speed and client outcome. These frameworks include Deloitte's Cyber Strategy Framework (CSF), which outlines a tried and tested methodology to evaluate clients' cybermaturity based on their organizations, specific business model, and corresponding risk factors.

As part of a six-phase Cloud CSF methodology, leveraging several international standards and its own Cloud Computing Risk Intelligence Map, Deloitte developed the Cloud Security Content Pack, which is a customizable platform with 21 capabilities, 62 subcapabilities, and several integrated, exportable dashboards that help clients build a robust cloud security strategy. In addition, Deloitte Fortress is a service that enables clients to implement and manage security guardrails and automated remediation in the event of a deviation from cloud compliance standards across multicloud environments.

Strengths

Deloitte is a household name within the security services space in the Asia/Pacific region, consistently finishing among the top service providers in any vendor assessment. Its strong position within the relatively nascent cloud security services space in the greater Asia/Pacific region is not merely an accident but a result of its "Tilt to Asia" global initiative and implementation of several deliberate business strategies and innovative organizational culture, backed and sponsored by exemplary leadership.

In line with the firm's forward-looking and innovative culture, Deloitte was one of the early enablers of cloud technology and has been integral in driving cloud adoption among key verticals in the Asia/Pacific region. The provider boasts a strong cloud platform engineering business aligned with all the major hyperscalers (AWS, Azure, GCP, Alibaba) that serve the Asia/Pacific market. Its security team works closely with its cloud engineering team to ensure security is embedded at the core of its client's cloud transformation journey. Moreover, Deloitte has created learning programs with cloud hyperscaler platforms (AWS, Azure, GCP and others) so its staff can be certified. Aside from learning programs from cloud vendors and Deloitte's Cloud Institute training platform, Deloitte's staff also have access to independent training and certifications from the SANS Institute, the Cloud Security Alliance (CSA), the Cloud Academy platform, or Udemy.

Understanding that investing in people and competencies is one of the most efficient differentiators in the fast-growing cloud security services market segment, Deloitte has focused on developing and investing in its people to produce the top-tier talent required to serve its clients better. It boasts one of the largest security workforces in the region and is clustered based on various domain expertise and capabilities.

Challenges

Deloitte can co-innovate and co-create solutions with clients on Microsoft platforms and is actively managing Azure Sentinel deployments for clients across the Asia/Pacific region. However, as the auditor for Microsoft globally, it is not permitted to co-innovate and run joint GTM initiatives with Microsoft.

DXC Technology

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

DXC Technology's cloud security services, as part of its broader cloud and platform services offerings, focus on securing data, identities, and access across various cloud environments, including public, hybrid, and multicloud environments and cloud platforms. As part of DXC Offerings, chief technologists help drive and oversee the development of the DXC Technology's cloud security strategy, offerings, and partnerships. This group operates globally, with local representation and engagement.

DXC Technology, very often, is engaged by clients to assess their infrastructure and security landscape as part of clients' cloud transformation journey. This could include business case development, cloud security strategy development, cloud security design, regulatory requirement assessment, and technical and organizational measures recommendations. DXC Technology has templates or accelerators for developing a cloud security framework or any phase of the cloud journey. Its Cyber Reference Architecture (CRA) is a vendor-agnostic, granular, and versatile approach to enable cyber-resilience so organizations can minimize the operational impact of the inevitable breach.

The CRA is often used as a framework, allowing DXC Technology to co-create with its clients and includes 12 domains that are categorized into three levels, with 55 subdomains and 347 capabilities. It is supported by 10 blueprints. Globally, DXC Technology has over 3,000 security professionals.

In 2020, DXC Technology announced its plan to merge operations in Asia with Australia and New Zealand, forming a combined business entity across Asia/Pacific. From a cloud security services perspective, the move is promising, with a plan to leverage the strengths and scale of both employees and technology capabilities across the region and better meet customer demand. On the training front, DXC Technology has the OneCloud Guild in the region in which all DXC Technology personnel have been required to complete introductory cloud training, with additional trainings designed across personas, such as executives, sales, solution architects, engineers, marketing, and so forth.

Strategic acquisitions are another important element of DXC Technology's security offerings and capability enhancement. These acquisitions include the acquisition of Luxoft in 2019, a 13,000-person workforce that provides digital strategy consulting and software engineering services, Syscom, a ServiceNow partner with security operations and IT service management expertise, and Virtual Clarity, a leading consulting and advisory firm that focuses on IT transformation and application migration, which includes apps and security consulting and transformation.

Strengths

The cybersecurity and analytics teams of DXC Technology are structured together and report to a single leader in the Asia/Pacific region. It has been helpful when two teams work in tandem, especially when it comes to creating and training new data models using ML algorithms that enhance threat detection, threat intelligence, or threat hunting capabilities. Being a strategic partner of Microsoft, DXC Technology has adopted Azure Sentinel internally and many other AI-/ML-based threat detection and threat hunting capabilities.

Since the creation of DXC Technology, the previous CEO, Mike Lawrie, decided that automation must be applied at scale across the company's managed service client operations and offerings. The investment in DXC Bionix is the largest the company has made in internal technology enablement to date. DXC Bionix leverages analytics, AI, lean principles, and automation to modernize traditional delivery environments. It is underpinned by Platform X, which is designed for managed services delivery with zero ops and day-one engineering and positioned as the new digital generation delivery platform for DXC Technology. DXC Technology is already well underway in developing its next-generation Platform X, which will build upon Bionix and Platform DXC as the single managed services platform foundation on which all services, including cloud and security, are delivered.

From a GTM strategy perspective, DXC Technology has scaled back and focused on fewer key verticals (e.g., financial services, automobile, and public sectors) for cloud security services in the Asia/Pacific region. After sharpening its focus, it witnessed a strong year-over-year (YoY) growth in the Asia/Pacific region for its cloud security services business and achieved better customer satisfaction and profitability.

Challenges

DXC's cloud security capabilities are often packaged with its application modernization and managed cloud infrastructure engagements. The service delivery consistency across Asia needs some work with different levels of capabilities across the region, but with the new integration between Australia and Asia operations, we expect that things will be delivered in a more consistent fashion, with automation

and AI/ML capabilities built in Platform DXC to meet the demands of global customers. DXC Technology should also accelerate the transition of its pricing strategy to meet the growing customer demand of flexible and outcome-based pricing. Fortunately, DXC Technology is looking at some niche emerging vendors to better align its pricing scheme with this demand.

Ernst & Young

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

EY's approach to cloud security services is operated on a continuous basis of an "infusion" strategy, meaning EY's cloud security capabilities are infused with EY's other competencies, service lines, and solution offerings. It also offers technology and services in one bundle by leveraging EY's ecosystem partners and hyperscalers.

EY's Trusted Cloud services address four critical pillars associated with a cloud transformation program: assessment, design, development, and migration. EY has developed a number of fit-for-purpose tools and methodologies that help deliver its cloud security services. To name a few:

- EY Cloud Governance Tool is a multicloud monitoring solution that evaluates enterprise compliance against leading risk, security, compliance, data and architecture standards.
- EY Cloud Migration Factory is a cloud-agnostic platform that is deployable on containers and built on open standards. It acts as a control center and provides visibility of the entire migration process: discovery, assessment, migration planning, migration execution, and hypercare.
- EY Dash is a multicloud management platform that includes EY's proprietary DevSecOps dashboard, which provides a view for security in the DevOps pipeline.
- EY Cloud Security Framework is a methodology that includes both a top–down and bottom–up view of a company's cloud environment.

In addition, the expertise in the critical power and utilities or critical infrastructure sector vertical allows EY to see the evolving need to modernize legacy operational technology (OT) systems while implementing security by design principles and security controls from the onset in alignment with business and economic criticality. The EY Digital Energy Enablement (DEEP) and EY UtilityWave are good examples that EY has leveraged its intensive industry insights and technical know-how of cloud technologies to create industry-specific, cloud-based solutions. OT cloud is gradually becoming an important differentiator for EY's cloud security capabilities and GTM strategy.

On data residency/sovereign requirements, EY leverages its own proprietary EY Data Protection and Privacy Manager (EY DPPM) solution. The solution is portable and can be deployed on-premises or hosted within a given country. Moreover, there is an extensive network of centers of excellence (COEs), wavespace, and cybersecurity. COEs are made of near-shore, onshore, and offshore capabilities in the Asia/Pacific region, meeting clients' requirements and providing them with flexibility and option.

During the pandemic, in several instances, EY executed payment holidays and offered flexibility in contract amendments or renegotiations to support clients financially and operationally. EY also introduced its Enterprise Resilience framework, a proprietary methodology that examines nice key pillars for enterprise resilience in the context of the pandemic, which EY opened to the public for use.

Strengths

Being a long-term strategic alliance partner of Microsoft globally, EY has shown strong capabilities of implementing/managing customer solutions based on Microsoft platforms. For instance, several of EY's industry- or sector-specific solutions, such as the EY Global Tax Platform or EY Cybersecurity as a Service (CaaS), are based on Microsoft technologies and Azure platforms.

According to clients' feedback, EY's skills and support coverage around Microsoft Azure Sentinel, a cloud-based SIEM platform, in Southeast Asia was rare and excellent when the solution was very new in the market. Clients highlighted access to needed skills and sound talent retention as areas of EY Asia/Pacific's particular strengths.

On the skills front, EY has put significant efforts in training and reskilling its workforce to meet the growing demand and address skills shortages on cloud security. One significant initiative was introduced in July 2020 (i.e., start of EY's financial year) called EY Tech MBA, which is a fully accredited corporate master of business administration (MBA) degree, with the online qualification awarded by Hult International Business School. Broadly speaking, its Cybersecurity Career Framework, as part of its global Tech Careers Framework, offers technology professionals the ability to drive their careers at EY with greater transparency and clarity.

EY's cloud security offerings are price-competitive and available through several different pricing models. EY has developed a comprehensive approach, with supporting proprietary tools to enable customers to evaluate pricing models and build business cases. The success criteria developed and communicated for each engagement before contracts are signed give sufficient visibility and remove the black-box approach for the client, which clients highly appreciate.

Challenges

According to client feedback, EY could do better from a project management perspective during the onboarding process, especially with assisting clients in ironing out the internal processes for the cloud platform, which was new to the client. Fortunately, EY is very receptive to clients' feedback and shows improvement very quickly. EY could also build out better incentives to continuously drive the level of automation and resources optimization in engagements.

IBM

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

IBM, a multinational technology company based in the United States, has been a pivotal digital transformation (DX) partner among organizations worldwide in the last few decades. It employs over 10,000 employees across the globe – with about 700 dedicated to the Asia/Pacific region — to support its cloud security practice. The IBM Security business unit is part of the IBM Cloud and Cognitive divisions, and its cloud security strategy is rooted in its goal of giving clients the translation layer across hybrid multicloud environments. By providing the translation layer across hybrid multicloud environment and applications, IBM's approach has a differentiated value for its clients. Its comprehensive cloud security portfolio is underpinned by its overarching security brand strategies, which are:

- Align — aligning the client's security strategy to business needs across risk, compliance, and security management for multicloud and hybrid cloud

- Protect — protecting the client's valuable assets, which may include, among others, digital users, workload, and data
- Manage — managing growing digital threats by detecting, defending, and responding to and recovering form cyberincidents
- Modernize — modernizing security and compliance posture, leveraging best-of-breed, open, multicloud, and hybrid cloud capabilities

IBM Security defined a method for delivering its cloud security services, which is composed of six distinct phases that address every client's unique needs across assessing, reducing, and managing risks. This in-depth methodology allows IBM to work closely with the client's security, compliance, and architecture teams or leadership to design, implement, and manage a right-sized set of security projects based on the client's region and sector-specific context. Once improvement areas or gaps are thoroughly assessed and identified, IBM then deploys a combination of professional services and managed security services to properly mitigate the risks.

IBM delivers cloud security via one delivery unit — managed security services for cloud — to ensure a consistent delivery experience for clients. IBM's managed security services account for a significant share of its security business in the Asia/Pacific market, and, given the size and nature of typical IBM clients in the region, these engagements usually involve complex and diverse IT environments. IBM's comprehensive SOC capabilities, processes across multicloud hybrid environments, and ability to leverage robotic process automation (RPA) or other automation technologies for incident response resonate well with its clients in the region.

As for professional cloud security services, IBM can also easily leverage its library of use cases, which consists of a rich set of use cases for both cloud and on-premises scenarios. Its recent acquisitions of Spanugo and StackRox are expected to further enhance IBM's cloud security offerings, particularly around cloud security posture management and container security.

Strengths

Complementing its comprehensive portfolio, IBM has a plethora of proven technologies, platforms, tools, and methodologies at its disposal, which have augmented extensive ecosystem partnerships. Depending on client requirements and risk factors, IBM can seamlessly leverage one of its many pre-integrated technology platforms for cloud security services. These include IBM Multicloud Management Platform, IBM DevOps Commander for accelerated DevSecOps, and IBM Security X-Force threat management services.

With sizeable engineering possibly behind it, IBM is continually improving its existing platforms and developing newer methodologies. For example, it is currently incubating a capability to deliver DevSecOps across application, data, and infrastructure security controls. Furthermore, many of its offerings are AI-/ML-enabled, including threat management service platforms, Guardium Data Protection for hybrid cloud workloads, Trusteer MaaS360, and user and mobile security solutions. With the acquisition of Red Hat, IBM extends its portfolio of security services across advise, move, manage, and build to Red Hat OpenShift environments.

Apart from its technical capabilities, IBM also tends to possess a solid project governance model and ensure positive customer experience. Monthly executive meetings are conducted between IBM's global leadership and its client's chief information security officer (CISO) or leadership team to foster a greater relationship, build trust, and maintain a robust feedback loop. Furthermore, IBM's professional services team is almost always a combination of local, regional, and global practitioners, ensuring

globally consistent service quality without ignoring local nuances and challenges. IBM's methods and platforms are designed as global offerings and are engineered to be ran and managed by its global security operations and regional teams, tapping into the "glocal" approach.

Challenges

IBM had basked in the glory of being one the largest IT and security providers in the region in the last couple of decades. However, as of late, acquiring new customers and logos has been a bigger challenge because of the increased competition in the market. IBM's customer experience and customer centricity program could be further improved to reflect current market trends. This could include anything from pricing strategy to managing client relationships at the execution level.

Although its recent restructuring of its organization to focus its efforts and resources on growth areas is progressive and a positive step, the benefits and effects of the move are yet to be seen.

KPMG

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

KPMG's cloud security services form part of KPMG's broader cybersecurity services and strategic priorities that are aligned with the firm's broader cloud transformation capabilities. The cloud security services capabilities across the Asia/Pacific region vary based on the local market maturity, reflecting unique needs in specific markets. KPMG provides consistent services to its clients across the region through its global delivery network and capability centers using frameworks such as KPMG's Global Quality and Risk Management framework.

KPMG has approximately 450 cloud security professionals out of its total 1,200 cyberprofessionals in the Asia/Pacific region. These professionals are joined regionally and globally through its Global Cloud Nexus community. KPMG's cloud security delivery framework incorporates leading-practice models to help organizations assess, design, build, deploy, test, operate, and monitor secure workloads across multiple cloud environments. The percentage of leveraging offshore resources is quite low for KPMG, with the firm usually utilizing local resources and local expertise to support its clients. KPMG understands that in a heterogeneous market, such as Asia/Pacific, which is composed of organizations of varying degrees of cloud maturity, there are different sets of security needs and, as such, has made it a point to tailor its offerings and service delivery strategy to reflect this reality.

KPMG's Global Cloud Nexus is a network of specialists across the globe that is responsible for generating the latest thought leadership, providing deep technical expertise, and creating innovative, integrated client solutions inclusive of KPMG's cloud security professionals. The KPMG Global Cloud Nexus coordinates and governs its cloud cybersecurity development and reports directly to its Global Cloud steering committee. It also holds the repository for KPMG's best practice approaches, methodologies, and frameworks for the team to reference. A good example is KPMG's Powered Execution Suite (PES), which is an integrated, preconfigured platform supported by digital assets and methods that KPMG engagement teams use to better manage the delivery of business transformation with clients, accelerating their time to value.

KPMG's Powered Enterprise is another example of a preconfigured solution that can be technology-agnostic or delivered with a solution provided by one of KPMG's alliance partners, for instance:

- Powered Risk (governance, risk, and compliance solution) enabled by ServiceNow

- Powered SecOps also leverages ServiceNow
- Powered Enterprise Identity (identity and access management [IAM]) with SailPoint or Okta.

KPMG Threat Inspect is a CrowdStrike-enabled solution that automates the process to identify, investigate, and escalate potential security threats.

KPMG is one of the first global professional services companies that signed a letter of intent for a strategic alliance with Alibaba Cloud in 2018. KPMG and Alibaba Cloud went on to jointly announce the formation of a global alliance to provide DX to businesses of all sizes and across multiple industries.

Strengths

The KPMG assessment framework for infrastructure as a service (IaaS) and platform as a service (PaaS) combines critical domains of cloud security with pragmatic and operational expertise across cloud environments. According to clients' feedback, KPMG demonstrates a strong technical know-how when it is engaged by the client for assessment, especially around penetration testing, red teaming, and incident response. Moreover, KPMG provides important transparency and responsiveness that are highly praised by clients.

KPMG pays a lot of attention to its employee retention and reskilling. As part of the Global Cloud Nexus, training and certification support is also provided through a learning pathway developed by KPMG's Global Cyber Learning and Development team, which guides all cloud cyberprofessionals across all levels of the training and certification they aim to achieve. For instance, KPMG has over 500 personnel with AWS skills and over 135 formal certifications across the world in a joint program led from the United States and Australia. KPMG is one of only 11 service providers worldwide with an AWS Advanced Consulting Partner: Security Competency accreditation, which secures priority in-region support from AWS.

On the thought leadership front, KPMG is heavily involved in the Information Security Forum (ISF) community and the International Information Integrity Institute (i-4) (acquired by KPMG), the world's longest-running strategic cybersecurity think tank and peer-to-peer knowledge exchange for CISOs and cybersecurity leaders of global corporations, including multinationals based out of Asia/Pacific.

Challenges

KPMG is relatively late in investing in digital technology capabilities, including cloud and cybersecurity, especially when compared with its closest peers. For instance, when Microsoft just launched its Sentinel platform, KPMG's Microsoft certification status back then made it miss some opportunities. However, KPMG has identified Azure Sentinel Accelerator as a key area for the KPMG cloud cyberpractice to focus on, along with other solution areas, such as multicloud compliance, SecDevOps delivery toolchain, and data and identity governance.

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 services 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. During 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.

PricewaterhouseCoopers

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

PwC is a multinational professional services network of firms and has a strong presence in Asia/Pacific. It began investing in cloud business in 2007, which has since grown in both breadth and depth. Its Cybersecurity and Privacy (C&P) business is one of the firm's largest investment areas. At present, it operates five Cyberlabs in Asia/Pacific, two SOCs in India and Australia, and a growing number of Cyber Impact and Experience Centers across the region and around the world.

PwC's cloud security strategy revolves around four domains — transform security, secure cloud infrastructure and platforms, secure cloud workloads, and extend enterprise security services to the cloud — within which PwC's various services are populated. These domains span cloud security readiness and planning, securing cloud infrastructure and platforms and securing applications in the SDLC, as well as hybrid security services. By embedding security as a significant pillar across all its cloud transformation model, PwC ensures its clients adopt a holistic approach to security regardless of the maturity of the organization. For example, its Enterprise Cloud Strategy offering focuses on defining a cloud vision, strategy, road map, and business case for the enterprise. Meanwhile, its Cloud Engineering and Security offering helps to ensure security and resilience across various layers, such as cloud foundation, data engineering, integration layers, microservices and containerizations, platforms, and DevSecOps services, among others.

PwC has an extensive portfolio of integrated solutions and robust delivery accelerators. These solutions and frameworks are developed by PwC itself, as well as with its ecosystem partners, including all the major hyperscalers. One such example is Proactive Risk Intelligence Monitoring Solution (PRIMS), a forensic solution built on Microsoft platform for fraud and risk analytics for continual monitoring. Another would be Microsoft Insider Risk Management, which is a compliance solution built on Microsoft 365 that uses native and third-party signals to help organizations identify and investigate malicious and inadvertent activities within the organization.

In addition to engineering capabilities, PwC also leverages a slew of proprietary frameworks to ensure consistent service delivery. Its global delivery method, business, experience, and technology (BXT) aims to ensure clients predictable value, speed, focus, and agility. This strategy enables PwC to essentially position itself as a local firm grounded on providing services at a local level with higher

awareness of challenges while drawing from globally standardized capabilities, resources, and expertise as needed.

Strengths

PwC has a unified global strategy when it comes to portfolio development, which is shared by its territory practice around the world. The firm also has a products organization that owns, manages, and continues to develop the products and proprietary solutions related to cloud security and has built a series of enablers to support its execution strategy at scale. These include its network of global acceleration centers, consulting source, digital hub, digital lab, apps marketplace, BXT agile methodology, and other toolsets to help ensure consistent service delivery. Further, PwC also has established cloud security collaboration communities to promote sharing of expertise, experience, and resources from its acquisition of Eagle Dream Technologies, a U.S.-based cloud-native transformation company.

Innovation is another area that is quickly emerging as a strength of PwC, as many of its solutions and platforms are integrated with next-gen technologies, such as analytics and AI, which results in enhanced levels of automation. It assists organizations to build an orchestration platform that removes manual processes in security testing across various technology platforms and environments, such as within the CI/CD pipeline, trust and compliance management, and container security.

Apart from technology, PwC has invested significantly in building competencies, and the skills of its security professionals are a clear strength. Clients spoke highly of the firm's experts and practitioners' capabilities, and how the personnel and senior staff members have been a factor for their organizations' continuous engagements with PwC in Asia/Pacific. In addition, clients found PwC's pricing model more favorable compared with that of its competitors in the market. Being able to take on highly customized and at time small one-off engagements on short notice is another quality that resonated with the clients.

Challenges

Despite the approaches and templates in place to ensure consistent services delivery, PwC, much like any other "membership firm," does suffer from instances of inconsistent service delivery across the region. In addition, the composition of delivery teams, as well as the level of engagement by the vendors' senior staff members with clients.

Samsung SDS

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

Samsung SDS is a household name within the Asia/Pacific IT services market. Although it first existed primarily to support its Samsung affiliates, the vendor is now keen on branching out of its captive market and home base of South Korea to position itself as a leading IT services provider in Asia, especially with its vision to be a data-driven DX leader.

Samsung SDS' cloud security business is composed of managed security services, security solutions, and security consulting services. Samsung SDS has built its security practice and capabilities around three core principles — no way in, no way out, and useless once out — and it has doled out a considerable number of investments to do so. Its services portfolio runs the gamut from security policy

and plans development, architecture design, implementation and provisioning, operations, and management all the way to security optimization.

A key component of Samsung SDS' cloud security offering is its DX security consulting services, which help conduct security maturity assessments, vulnerability assessments, penetration testing, and benchmark client readiness against Samsung SDS' IT Security Index (ITSI). Samsung SDS' managed security services are largely centered around detecting threats via real-time log collections and a correlation analysis of threats. Samsung SDS CLOUDION is an integrated security platform for the admin to enforce security policies, detection rules, alert settings, and audit log settings to monitor assets in real time via a visualized dashboard.

Complementing its services portfolio, Samsung SDS boasts its own suite of network-, server-, and platform-level security solutions that are interoperable and optimized for unique vertical needs. The vendor operates a security R&D center that keeps it updated on the innovation front and develops proprietary security solutions and technology stacks. Through this innovation pipeline, Samsung SDS has developed its White-Box Cryptography (WBC) and homomorphic encryption for privacy-enhancing technologies (PET) to protect clients' diverse IT environments, including the cloud. Additionally, the R&D center is developing a natural language processing (NLP) threat intelligence model that automates context analyses and threat extraction from unstructured texts.

Although Samsung SDS has a strong R&D focus to drive product innovation in-house, it has an extensive partner and ecosystem, ranging from global major tech vendors to niche Internet of Things (IoT)/edge security vendors, such as Karamba Security. The expansive partnership ecosystem supports its multicloud vision.

Strengths

Samsung SDS is a primary security provider to its parent group, Samsung Group, a global brand with a direct presence across 63 countries, lending the provider a solid credibility within the cybersecurity space. The extensive experience of working with various subsidiaries and non-Samsung clients across different verticals proves Samsung SDS to be a reliable security partner, delivering quality services for businesses in Asia/Pacific, specifically in North Asia and Southeast Asia. In addition to two fully functioning SOCs in South Korea and the United States, Samsung SDS has implemented two new SOCs in China and Vietnam for its business partners and strategic IT service provider to continue expanding its global footprint and operations in Southeast Asia by leveraging the local capabilities from the SOCs.

Samsung SDS' security practice started in 1999 as a security consulting service before becoming a full-fledged security service provider by 2002. It has since developed a formidable cloud security capability as part of its portfolio. Having been the first vendor that could provide an entirely cloud-based managed security service in South Korea catering to clients' AWS environment, Samsung SDS further expanded its monitoring services to Azure and Oracle Cloud. Since 2018, Samsung SDS started supporting container security, serverless security, and DevSecOps and putting a tremendous focus on managing identities, cloud-native apps, and workloads and data in the cloud.

Samsung SDS boasts collecting upwards of 64TB of data per day from its very own extensive digital footprint across the globe and other sources, including from government agencies and global IT providers. The ubiquitous use of AI-powered automation in its operations helps enhance cost efficiencies, which is highly praised by its clients. According to client feedback, Samsung SDS has

been delivering contextualized guidance and reliable services through many years of engagement. It is also effective in optimizing clients' security investment with the rising adoption of cloud services.

Challenges

Although Samsung SDS has an ambitious plan to expand beyond its home base to tap into the regional market's opportunity, majority of its security resources and competencies are based in South Korea. This could hinder the vendor in delivering services to potential clients outside of North Asia, especially for its consulting and transformation services, which could lead to bigger opportunities.

Samsung SDS' continuous threat monitoring and detection responses services have yet to fully gain traction among its clients. However, the vendor is optimistic that the managed services category will emerge as a growth engine for the company, having only recently started its expansion of security orchestration, automation, and response (SOAR) platform–based services.

Tata Communications

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

Tata Communications is a leading communications, connectivity, and IT services provider, with its headquarters being in Mumbai, India. It boasts an extensive, end-to-end IT services portfolio and stellar track record in helping its clients in their respective transformation journeys, including secure cloud transformations. It does so by taking a holistic approach to design, migrate, and manage the right cloud model, with security embedded at each phase, helping clients stitch the cloud and cloud security decision in a single, results-oriented plan.

Understanding that the hybrid cloud model is emerging as the go-to method of organizations in the region, Tata Communications offers a cohesive security architecture across hybrid digital estates, with centralized governance utilizing management tools, processes, and frameworks. It is worth to note that Tata Communications has its own IZO private cloud offering, which is based on OpenStack and VMware. Having managed its own IZO Private Cloud offerings alongside customer infrastructure hosted at Azure, AWS, and GCP platforms gives Tata Communications solid credibility in multicloud security management.

The portfolio development at Tata Communications is based on the simple yet effective philosophy of securely enabling the customer's DX journey. To this end, all the new services in its security product road map are designed to be scalable, agile, cloud-delivered, and predictive. It continuously strives to enhance its deployment framework and intellectual properties (IPs) through its center of excellence (COE) operated by its dedicated security engineering team. This COE also consists of a cybersecurity data science and analytics team that works to develop a predictive model that performs deep analyses of network flow using AI/ML technology to provide early notifications and avoid potential network services disruptions.

Majority of Tata Communications' cloud security services are delivered and managed via its state-of-the-art cybersecurity response centers (CSRC) with optional onsite staffing to support customer-specific operational and regulatory requirements and more than 550 certified cloud and security staff in the Asia/Pacific.

On top of having deep relationships and joint GTM strategies with three major hyperscalers (Microsoft Azure, AWS, and GCP), Tata Communications has upwards of 10 technology partners for cloud

security services, including Zscaler, Trend Micro, McAfee, Recorded Future, Check Point Software Technologies' Dome9, LogRhythm, and Ping Identity.

Tata Communications has built several alliances within the cloud security space, including with Microsoft, AWS, and CSA, in which it is a corporate member.

Strengths

As critical enterprise applications are increasingly deployed on the cloud, Tata Communications provides enterprises the ability to better govern, monitor, and control these applications and mitigate the inevitable technology risks that come with cloud migrations. These include delivering more visibility, securing increasingly complex hybrid IT cloud environments and ensuring compliance with the relevant regulatory requirements.

According to clients' feedback, Tata Communications is very responsive, approachable, and generally good at executing and implementing solutions. Its consolidated and cloud-delivered SIEM with an optimized SOAR approach is very effective and brings cost benefits to the client directly. The great client feedback is an excellent reflection of its agile principles and agile new product introduction (NPI) process that Tata Communications follows internally to meet customer demands.

Tata Communications has a dedicated security platform and engineering team that focuses on innovating through service platform creation and integration with technology partners' solution, such as incorporating native cloud security components from AWS, Azure, and GCP as well as third-party security solutions to ensure enhanced control and effective risk mitigation.

Tata Communication's extensive portfolio (e.g., network, cloud, ISP, security) and ability to guide its clients through a secure cloud transformation journey has certainly won high praises and rave reviews from its customers. From a customer experience standpoint, Tata Communications' end-to-end life-cycle approach of engagement, consulting and architecture planning, technology implementation and provisions, and managed services have been winning factors. Its clients speak highly of the vendor's service delivery quality, technical capabilities, and flexibility to package its services to fit customers' needs.

Challenges

Having an end-to-end portfolio could, at times, be a double-edged sword for a service provider. This has been the case for Tata Communications. Similar to many other companies in this sector, Tata Communications will need to constantly scale up in competencies in fast-changing technology domains, including some of the rarer, niche segments. According to client feedback, Tata communications should be more proactive in recommending new approaches and emerging technologies into the engagement. The knowledge transfer could be further enhanced as well.

Tata Consultancy Services

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

TCS is one of the largest IT services, consulting, and business solutions providers globally by market capitalization, with presence across 46 countries around the world and 14 countries in Asia/Pacific. In its over five decades of existence in Asia/Pacific, it has a solid track record of being a business and IT

transformation partner, with many key organizations across the region from various verticals. TCS' list of clients includes some of the biggest names in their respective sectors and geographies and has long-term partnerships with clients in the banking, financial services, and insurance (BFSI), telecommunications critical infrastructure, transportation, and public and government sectors, highlighting the vendor's range of capabilities and expertise.

TCS has one of the most comprehensive cloud security portfolios in the market, addressing the entire life-cycle stages of cloud adoption. For instance, TCS Cloud Counsel provides discovery, cloud assessment, and recommendation offerings to select the right cloud model and provider and determines the migration road map, with necessary ROI and total cost of ownership (TCO) estimates. There are more than 11 distinct services offered by TCS. The comprehensive set of offerings enables TCS to fulfill client requirements for security endorsement in cloud adoption and tech modernization programs and enforce security controls for cloud with policy development, technology configuration integration, and security operation extension. On top of its standalone cybersecurity business unit that addresses clients' cloud security requirements, TCS has embedded security services into its five streamlined cloud services business units, which are aligned with their strategic partners, namely Azure, AWS, GCP, and Oracle. TCS also has alliance partnerships with more than 70 security technology partners.

TCS has made significant efforts in developing cloud as a specialization. It has invested in 12 cloud security COEs, 3 cloud security solution centers and 1 cloud security garage with each hyperscale cloud providers enabling co-innovation and co-creations activities, and over 120 cloud technology partners. TCS has clearly made its intent clear in achieving its mission to become the go-to cloud security partner in the region. TCS has developed an elaborate pricing structure for its security services in the region, providing its clients with options, such as consumption-based pricing and fixed prices.

Strengths

Being one the largest service providers in size in the region, TCS could dip into its extensive roster of talent pool and complement its services with enhanced automations powered by AI to ensure optimal services quality. This sizeable resource is a result of its strategic investments focused not only on expanding its talent pool but also equipping it with the necessary competencies and certifications. TCS has set its sights on becoming one of the top trusted enterprise cloud security services brands globally. To that end, the provider has deliberately invested in numerous key initiatives based on strategic principles, including continuous innovation and customer centricity.

As with most leading providers, TCS has also developed a plethora of platforms, accelerators, and proprietary assets as part of its arsenal to ensure optimal service delivery. These include, among others, TCS' Cyber Vigilance (a security-as-a-service-based solution that delivers the "single pane of glass" for real-time monitoring and advanced contextual analysis to proactively prevent, detect, and address security threats) and TCS IdentiFence (which provides digital identity as managed services). Some of these platforms are also available in localized versions. For example, TCS Havens is a Japanese version of the Cyber Vigilance platform and provides bilingual support to cater to regional-specific requirements.

Having worked with clients from various industries and sectors, TCS is able to bring what it considers "contextual knowledge" to develop product and service packages that fit clients' needs in the region. TCS' clients spoke very highly of its quality of service (QOS) and ability to source the right talent for the job at hand even in difficult and highly competitive markets. Moreover, the dedicated TCS staff, with

the offshore model, enables greater cost savings and faster project delivery that often exceeds clients' expectations. Majority of TCS' clients are very likely to recommend the vendor to their peers, which indicates a high level of trust.

Challenges

Despite having a strong brand presence across the globe, most of TCS' cloud security revenue in Asia/Pacific comes from Australia and India. The vendor could demonstrate a stronger integrated or security-embedded approach to further expand in the region, specifically in developing markets, such as Southeast Asia, where cloud adoption is taking place at an accelerated rate.

Telstra

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

Telstra's cloud security services have evolved from the previous security services practices that were delivered separately via its professional services, managed services, and security products to today's consolidated Telstra's Next-Generation Growth (NGG) program, which provides:

- Initial advisory and consulting services for cloud migration and transformation
- Professional services to execute the cloud transformation road map
- Managed services to manage cloud environments
- Security monitoring and response services to provide assurance based on Telstra's open managed security service (OpenMSS)

Telstra's multicloud strategy focuses on driving choices of cloud adoption (i.e., public, hybrid), coupled with Telstra's network and breadth of expertise, to assist customers in their journey with choice, control, security, and confidence.

The strategy of consolidating professional services, managed services, and products is executed under Telstra's NGG program, which sets out the growth strategy in areas outside of Telstra's heritage of network services. NGG has been seen internally as a big achievement, considering how fast the program has been put together and how quickly the program has been brought to the market. The NGG program's GTM stream covers an extensive sales and market enablement program. All NGG services will be part of the coordinated marketing campaigns. The consolidated and well-coordinated NGG approach responds well with the growing customer expectation of "secure by design," in which security controls are intrinsic to the service being provided.

The three guiding principles of the NGG program to develop and deliver cloud security services are using repeatable IP, more standardized and digitized ways of working, and high scale through automation. There are some good examples to illustrate these guiding principles for Telstra's cloud security services. For instance, Telstra Cloud Sight (TCS) is a powerful web-based platform that simplifies the way Telstra's customers buy, deploy, and manage multiple cloud services — public, private, or hybrid — and associated network connectivity all through a single portal.

Moreover, Telstra Purple has a dedicated automation team that actively identifies repeatable tasks to be automated and drive better efficiency for its customers. Telstra also leverages AI and ML with a heavy focus on Elastic and Databricks to deliver customer outcomes through advanced detection and analytics.

Strengths

Telstra Purple is the brand for Telstra's professional services and managed services team to consolidate all the services skills, expertise, and assets, including the likes of previously acquired firms Virtual Machine Technology (VMTech), MSC Mobility, Readify, Kloud, Bridge Point, O2 Networks, NSC, iVision, Company85, and most recently Epicon. These acquisitions are driving the services-led growth strategy of Telstra Enterprise. Telstra Purple is the largest Australia-owned technology services firm in the country, providing the largest pool of expertise in Australia across multiple domains, such as cloud architects, migration specialists, automation experts, threat analysts, security engineering, and others, as well as across a wide range of market-leading vendors and partners that Telstra has, such as AWS, Microsoft, VMware, Check Point Software Technologies, CrowdStrike, Palo Alto Networks, and many others.

Telstra understands the customer expectations for services to quickly react and scale. It operationalizes the customer expectation of agility into service definitions, service-level agreements (SLAs), commercial models, onboarding process, and so forth. A good example is when Telstra onboarded a customer to its security monitoring platform and commenced the incident response and remediation within 24 hours. Another recent example that shows how customer-centric Telstra is and how it effectively acts on client feedback is through the updates for its OpenMSS (i.e., for security monitoring) pricing strategy to have options to charge the client irrespective of log storage or log ingestion rates.

On the partnership front, Telstra has a long-standing relationship with Microsoft as a customer and GTM partner. To support the 360-degree relationship (i.e., across multiple business functions), there is a CEO peer relationship between Telstra CEO Andy Penn Microsoft CEO Satya Nadella. Similarly, Telstra has a strategic collaboration agreement with AWS, with a CEO and executive peer relationship across sales, engineering, and marketing to support the Telstra–AWS partnership.

Challenges

As Telstra is on track on its T22 strategy (i.e., a three-year plan focused on simplifying the business structure and product offerings a s well as boosting profits by the end of 2022), such a laser-focused strategy puts the primary focus of the Telstra Enterprise business on its home market and not so much on international markets. As an end-to-end transformation partner, Telstra could showcase more of its expertise and thought leadership around compliance, risk, and change management.

Trustwave

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

Trustwave sees itself as a cloud-first security services organization, meaning it always has the cloud in mind and prioritizes it when developing platforms and services. For example, the Trustwave Fusion platform is based on a hyperscaler cloud platform and can integrate with multiple cloud providers via a bidirectional application programming interface (API). Fusion is the core platform to deliver Trustwave's managed security services, managed detection response services, and even penetration testing services.

The broader vision that Trustwave has is to become the aggregator of cloud platforms from a security perspective, integrating "all of the relevant dots" and automating detection and response in the multicloud world. As of today, Trustwave has over 700 different integrators into its Fusion platform and

is able to work across heterogenous security technologies and vendors to effectively triage customer alerts and execute any containment actions.

Other Trustwave products, such as Trustwave's database security solution (i.e., DbProtect and AppDetectivePRO), provide extensive protection and support for databases in various types of cloud and are also able to run on the cloud. Similarly, its Secure Email Gateway solution — Trustwave MailMarshal — has multiple deployment options and, other than the on-premises version, can be deployed in Azure, AWS, or any other cloud infrastructure service. In fact, MailMarshal has a version that is significantly integrated with Microsoft Office 356 and 100% hosted in Azure.

From an organizational perspective, Trustwave continues to structure its teams through security disciplines and not by where the workloads run. Its Information Security Advisors (ISAs) work directly with clients, serving as a single point of contact to obtain analytical support, such as codeveloping or optimizing client-specific use cases, runbooks, and in-scope customized threat detection content as well as escalating security-related activities for the client. At the same time, client success managers who regularly interact with clients will identify both account-/client-specific and broader service delivery trends that may be impacting multiple clients.

On the consulting and professional services front, Trustwave offers a wide range of advisory-led diagnostic services, which include cloud security diagnostic services that examine the maturity of an organization's cloud security strategy as currently implemented as well as a review of cloud security policies, procedures, architecture, privileged access, data protection, and core security controls against best practices.

Trustwave's proprietary Security Colony platform (as part of the Hivint acquisition) is also a cloud-based security collaboration platform that includes cloud-based vendor risk assessments. In fact, Trustwave offered to complete a whole-of-government security assessment using the Security Colony Vendor Risk Assessment service (passive mode) to a regional government at no cost. It demonstrated a highly automated and anonymous process. Moreover, during the pandemic period, Trustwave has packaged a wide range of previously subscription-only security resources from the Security Colony platform into a "Remote Working Security Pack" and made them all available for free (i.e., a six-figure investment was made free to support the clients and the broader industry).

Strengths

Trustwave has recently revamped its pricing strategy for cloud security services, moving away from events-per-second-based pricing to one that is based on a combination of user and telemetry volume. It has also developed an innovative pricing model — "digital wallet" — in its Fusion platform for the SpiderLabs penetration testing services, in which customers can configure and schedule tests through the Fusion portal and deduct from the digital wallet in which customers can prepurchase a set number of services. It is a good example to give customers flexibility, transparency, and visibility through this pricing and consumption model.

Based on clients' feedback, Trustwave is able to bring a deep technical understanding to the projects. Trustwave's threat intelligence and hunting capabilities, together with knowledge transfer, are also well praised by clients. In Australia, the Trustwave SOC is colocated with the Optus Network Operations Centre and allows for unprecedented threat intelligence sharing, from distributed denial-of-service (DDoS) attacks observed through network traffic spikes to multivector threats from across the globe.

Moreover, Trustwave leveraged proprietary and third-party ML technologies in the Fusion platform to improve the detection of advanced/unknown threats and the reduction of false positives. A near-real-time streaming ML engine is part of Trustwave's security sauce, which is embedded in its Fusion platform. On top of that, it employs various DevOps automation tools to enable continuous integration (CI)/continuous delivery (CD) capabilities, cloud-native services, serverless technologies, and so forth. The focus on and investment in the Fusion platform are tremendous compared with that in other Trustwave products.

Challenges

Other than the internal use of DevOps automation tools, Trustwave could showcase more of its capabilities and expertise around DevSecOps, container security, and security automation and how it helps clients address these rising concerns and drive better outcomes when many organizations operate in a multicloud/hybrid cloud environment.

Wipro

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

With a new CEO, Wipro has done significant organizational restructuring, simplifying its operating model to organize the business into four strategic markets (e.g., Asia/Pacific, Middle East, Africa [APMEA], capturing local business trends, culture nuances, and regulatory requirements) and two global business lines. Wipro's Cybersecurity and Risk Services (CRS) has been moved under the global business line, and newly appointed CRS global head Tony Buffomante has seat representation in Wipro's executive committee. Wipro's cloud security has become an integral part of Wipro's overall cloud offerings, cutting across cloud infrastructure, applications, and the digital ecosystem. The creation of a cyberaccount leader is to effectively tap into Wipro's overall strategic accounts.

In the Asia/Pacific region, Wipro has about 225 professionals dedicated to deliver cloud security, with a blend of onshore and offshore. Aside from the nine offshore delivery centers in India, Wipro built a Cyber Defense Centre in Melbourne, Australia in 3Q19, providing onshore delivery support and addressing local data resilience concerns. In April 2021, Wipro announced its acquisition of Ampion, an Australia-based provider of cybersecurity, DevOps, and quality engineering services. Ampion's experience, talent, and proven client credentials in ANZ will greatly enhance Wipro's ANZ presence and, more importantly, deepen its technical know-how in the cybertransformation and DevSecOps domains.

Wipro's Cloud Application Risk Governance (CARG) solution is key in providing critical visibility and continuous security posture assessments across various cloud environments. It is a cloud-based platform that performs a comprehensive risk profiling of business applications and reports security risks of business applications spread across multicloud environments. Wipro is rolling out CARG to all of its managed services clients. It is also integrated into Wipro's unique Cloud Security Architecture Assessment Framework, which often acts as a starter kit to help customers in assessing their cloud security maturity and develop architectural blueprints for hybrid and multicloud environments.

On strategic partners, Wipro has a 360-degree relationship with four hyperscalers, namely AWS, Microsoft Azure, GCP, and IBM, for executive-level commitment, joint funding, and so forth. For instance, Wipro's CARG is a good example of a joint engineering effort between Wipro and AWS. Similarly, Wipro's Identity Management Center solution is built for Azure Active Directory (AD)

application acceleration and automated migration from other single sign-on (SSO) products. In September 2020, Wipro opened another Wipro–AWS Launchpad in Sydney, Australia. It is an immersive co-innovation center that focuses on helping customers fast-track their cloud transformations securely.

Strengths

Wipro's recent organization restructuring was well received by its customers. According to customer feedback, Wipro has improved in responding to clients' request and has become more agile and accessible. Based on clients' feedback, Wipro is very open-minded and willing to adapt to clients' feedback or suggestions. The commitment and camaraderie it has shown in engagements were highly appraised by its clients.

On the skills and culture perspective, Wipro has set a vision for its cyberbusiness organization to "be the most respected full-suite cloud security services organization in the world," which means it may not necessarily be the largest but aims to be a sought-out destination for cyberprofessionals. Wipro has built a cloud security academy that focuses on hyperscaler-based trainings, certification programs, and third-party security tools (e.g., Palo Alto's Prisma Cloud, Check Point Software Technologies' CloudGuard Dome 9, Qualys, Aqua Sec, Zscaler, etc.) that cut across identity, data, infrastructure, and security monitoring for cloud. On top of that, Wipro's Cloud Security Experience Center is a lab and a use case–driven cloud security skills enhancement program in which employees get real-time exposure on various practical cloud security challenges.

Wipro has a very mature investment arm that identifies and invests in innovative security specialist firms and is integrated into Wipro's portfolio. CloudKnox helps provide a continuous protection of critical cloud resources by enforcing least privilege policies, Immuta helps data engineers and DataOps teams automate data governance, CyCognito is a platform-based attack surface assessment and continuous threat surface management tool, and Vulcan Cyber helps orchestrate vulnerability remediation from start to finish and automate vulnerability prioritization processes. The integration of Vulcan Cyber significantly enhances the level of automation for Wipro's vulnerability and cyberdefense capabilities and speeds up remediation, which greatly benefits Wipro's cloud security clients.

Challenges

Wipro should accelerate its transition from traditional service levels to an outcome-driven approach. Based on clients' feedback, how partners stay updated is very critical to the client. The growing number of organizations in the midst of transforming their security operations requires a partner such as Wipro to equip them with deep technology know-how on cloud-native solutions and deliver value constantly.

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 the 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.

Strategies and Capabilities Criteria

This section includes an introduction of market-specific weighting definitions and weighting values. IDC believes that cloud security services vendors in Asia/Pacific must exhibit the characteristics shown in Tables 1 and 2 to be completely successful when crafting a future strategy and in leveraging existing capabilities to their advantage. The factors were weighted because IDC believes that some factors are more important than others are in maximizing market opportunity and realizing market success.

TABLE 1

Key Strategy Measures for Success: Asia/Pacific Cloud Security Services, 2021

Criteria	Definition	Weight (%)
Functionality or offering strategy	This refers to the vendor's capabilities and mechanism in understanding geo- and sector-specific challenges, demands, and processes to translate the insights into offerings and products.	8
Portfolio development	A strong portfolio strategy dictates that well-thought-out plans are in place to ensure the development of the portfolio meets current and future customer needs.	8
Partnership strategy	This refers to the competency level with hyperscalers and breadth for third-party security product vendors to support the vendor's cloud security services portfolio. A higher score is given to a vendor that has a partner strategy to penetrate smaller markets.	15
Track record	Excellence is marked by a vendor that has a strong track record and can articulate its own security strategy well in ensuring its security posture and cyberdefense effectiveness.	7
Pricing strategy	Excellence is marked by comprehensive planning to align pricing options and cost with customer and market preferences.	8
Delivery strategy	Excellence is marked by meeting customers' shifting preference for adoption and consumption.	10
Talent development	Vendor has clearly articulated plans for attracting and cultivating talent with global and regional sensibilities. A higher score is given for career customization programs that facilitate multiple paths to career success within the firm.	10
Innovation strategy	This refers to the vendor's strategy to incorporate and integrate next-generation technology to its service delivery methods and offering to enhance value to clients.	8
Growth strategy	This refers to the vendor's near- and long-term plan to expand within Asia/Pacific as well as specific plans to penetrate into subregions to tap into growing opportunities.	8
Marketing and branding strategy	This refers to the vendor's strategy to further enhance its brand, awareness, and mindshare within the cloud security space.	8
Customer experience strategy	This refers to the vendor's near- and long-term vision to ensure positive customer experience for increased customer stickiness and new logo wins.	10
Total		100

Source: IDC, 2021

TABLE 2

Key Capability Measures for Success: Asia/Pacific Cloud Security Services, 2021

Criteria	Definition	Weight (%)
Functionality or offering	This refers to a vendor whose portfolio and methodologies strongly demonstrate essential cloud security capabilities.	11
Portfolio benefits	This refers to the comprehensiveness of the vendor offering across the entire life cycle of cloud security services, including the assessment, design, implementation, transformation, and management of services. It should have a good combination of functional (domain) knowledge, industry insights, and technical capabilities to deliver the desired business outcomes for clients.	10
Partnerships	This is when the vendor's current partner ecosystem shows strong security competency of the major hyperscalers, especially on the understanding and experience in using cloud-native security tools.	15
Pricing model	The vendor's pricing model shows flexibility, especially when supporting the as-a-service model. A higher score is given to a vendor with an innovative pricing model and good customer feedback as a type of validation.	7
Delivery consistency	This refers to how well a vendor's current delivery model meets end-user preference for adoption and consumption. A higher score is given to vendors that demonstrate strong governance/project management capabilities and meet client requirements with regard to the ratio of onshore versus offshore resources and level of automation.	9
Innovation	This refers to how well a vendor leverages or incorporates emerging technologies, such as ML and AI, to deliver higher customer value.	7
Market penetration/execution	The vendor demonstrates a wide coverage of regions and verticals in the cloud security services.	9
Human resources and talent management	Success is measured, in part, by the headcount associated with the practice. It is also measured by how well a vendor manages its staff turnover during project delivery and resource quality for the project based on client feedback.	9
Marketing	The vendor demonstrates a concerted effort to enhance branding, reputation, and mindshare within the rapidly evolving cloud security space.	8

TABLE 2

Key Capability Measures for Success: Asia/Pacific Cloud Security Services, 2021

Criteria	Definition	Weight (%)
Customer experience	This refers to the vendor's existing programs and methodologies being implemented to ensure a satisfactory customer experience. This could include user portal, routine engagement, customer advisory council, and so forth.	6
Customer satisfaction	This refers to how well a vendor provides customer service and support. A higher score is given to a vendor that receives a high satisfaction score directly from its clients.	9
Total		100

Source: IDC, 2021

VENDORS TO WATCH

AWS

AWS has a dedicated security services team in Asia/Pacific made up of a team of industry experts, supporting the full life cycle of clients' cloud adoption, including assessment, business case development, cloud security strategy, governance and cloud security operating models, solution architecture services, implementation, and dedicated technical support. This is a combination of free presales support paid for Professional Services engagements and postsales technical support that varies based on the customer's required support level.

For many of its engagements, the AWS Professional Services team works closely with its customer's choice of partners. This approach reflects the philosophy of the AWS Professional Services team to help AWS customers and partners build their capability and confidence to move their most important workloads to the cloud by equipping and enabling its partners to perform the bulk of the service element in the engagement, whereas its own professional services team is focused on solving first-in world customer problems and building repeatable solutions that help customers achieve specific business outcomes related to enterprise cloud adoption.

AWS' Professional Services Security business is never meant to be a significant revenue generator for AWS. Instead, the team is often deployed strategically to enhance the adoption of AWS-native security technology and build trust with customers that AWS is fit for purpose for their most important workloads, information, and business processes.

IDC believes AWS Professional Services Security team's role in the ecosystem is critical in providing high-touch assistance and much needed guidance to its enterprise customers. This is especially true as organizations, including public sector customers and highly regulated industries, shift to a cloud-based operating model and incorporate AWS into their overall IT architecture.

Google

Google Cloud is a hyperscale cloud provider that offers IaaS, PaaS, and serverless computing environments. It has been expanding aggressively in the Asia/Pacific region and has launched its ninth cloud region in the market.

Google has continually developed a plethora of cloud-native tools and services, including security analytics and operations (Google Chronicle platform), web app and API protections, and data privacy and data loss protection. In addition, it offers highly automated and fine-grained permission management systems in the form of Cloud IAM, compliance and security controls for sensitive workload, as well as integrated secure access solution (i.e., BeyondCorp Enterprise).

It has a professional services organization composed of security specialists that provide assessments and customized enablement, proof-of-concept development, and implementation services to its key accounts in the region. Google also augments its delivery team with partner resources when the engagement calls for a larger team. To actively enable and guide its partners in the region to deliver its offerings, Google also runs formal trainings around GCP security and its best practices.

Google enjoys tremendous brand reputation as a leading technology company among end users and consumers and has successfully managed to develop enterprise strategies for business customers. Its app development platform, CI/CD functions, and AI-/ML-powered analytics tools backed by robust security have made it an attractive prospect for organizations in Asia/Pacific.

IDC expects Google to continue its investment in security- and compliance-focused tools and services and enjoy sustained growth in the region.

Microsoft

When Microsoft announced that its security business surpassed the US$10 billion mark in 2020, after experiencing a 40% YoY growth, the market started to pay closer attention to the global tech giant and its activities in cloud security.

In addition to baked-in security offerings tied closely to its other solutions or systems, Microsoft also boasts a list of security services offerings that contribute to its overall security business. For example, Microsoft Threat Modeling for security risk is a fixed-week engagement in which Microsoft Security consultants help the customer build a threat model based on systems and components in scope, identify threats, and develop a mitigations strategy. Its other software development life-cycle offerings and practices range from open source security to statistic/dynamic analysis security testing.

Further, Microsoft's services also offer consulting and dedicated technical support to help organizations adopt digital solutions and, more importantly, accelerate implementation and reduce risks. In particular, the security expertise and proven customer examples are often structured into three categories: identity modernization, intelligent security for the workplace, and cybersecurity essentials. These help organizations assess risks and implement capabilities to protect their environment against cybersecurity attacks, detect attacks, and respond to them as they happen.

IDC believes Microsoft's tactic of attaching Microsoft security and compliance offerings to its Office 365 and Azure workloads is actively contributing to the effective penetration of its cloud services. As its standalone security services practice gains more traction in the market, Microsoft's security business will continue to grow and develop into an important differentiator for Microsoft.

LG CNS

LG CNS is a global IT services, platform, and solutions provider headquartered in Seoul, South Korea. Backed by upwards of 6,000 employees, the vendor supports international companies, with over 14 overseas subsidiaries and numerous branches worldwide. LG CNS' security offerings are divided into four distinct buckets: security consulting, security implementation, security solutions, and managed security services. Its cloud security consulting offerings are established cloud security measures and geared toward clients looking to design, build, and operate on the cloud. Its security management shared service supports core security operations for clients seeking to outsource their security functions. LG CNS backs these offerings with its differentiated security solutions, namely cloud environment protection, which is developed to protect public, hybrid, or multicloud deployments.

LG CNS is one of the few Asia-headquartered vendors and the first South Korea provider to receive an AWS Security Competency certification, specifically in security engineering, which was one of the four areas for cloud security certifications at the time. In addition to cloud security, LG CNS has showcased formidable strength in providing security for other cloud-related and -enabled areas, such as smart factory, Smart City, and IoT security. However, despite possessing the qualities to be a formidable regional player, LG CNS still lacks meaningful mindshare among clients in the region.

IDC expects LG CNS to focus on making a more concerted effort to showcase its competencies in cloud security to position itself as a viable cloud security partner for organizations in the region.

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 have adopted cloud for several years are now focusing adopting security at greater scale and speed. The value of engaging a cloud security services vendor really provide the continuous assurance and operational excellence to these mature organizations. At the same time, for organizations just started 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