IDC MarketScape

IDC MarketScape: Asia/Pacific Professional Security Services 2024 Vendor Assessment

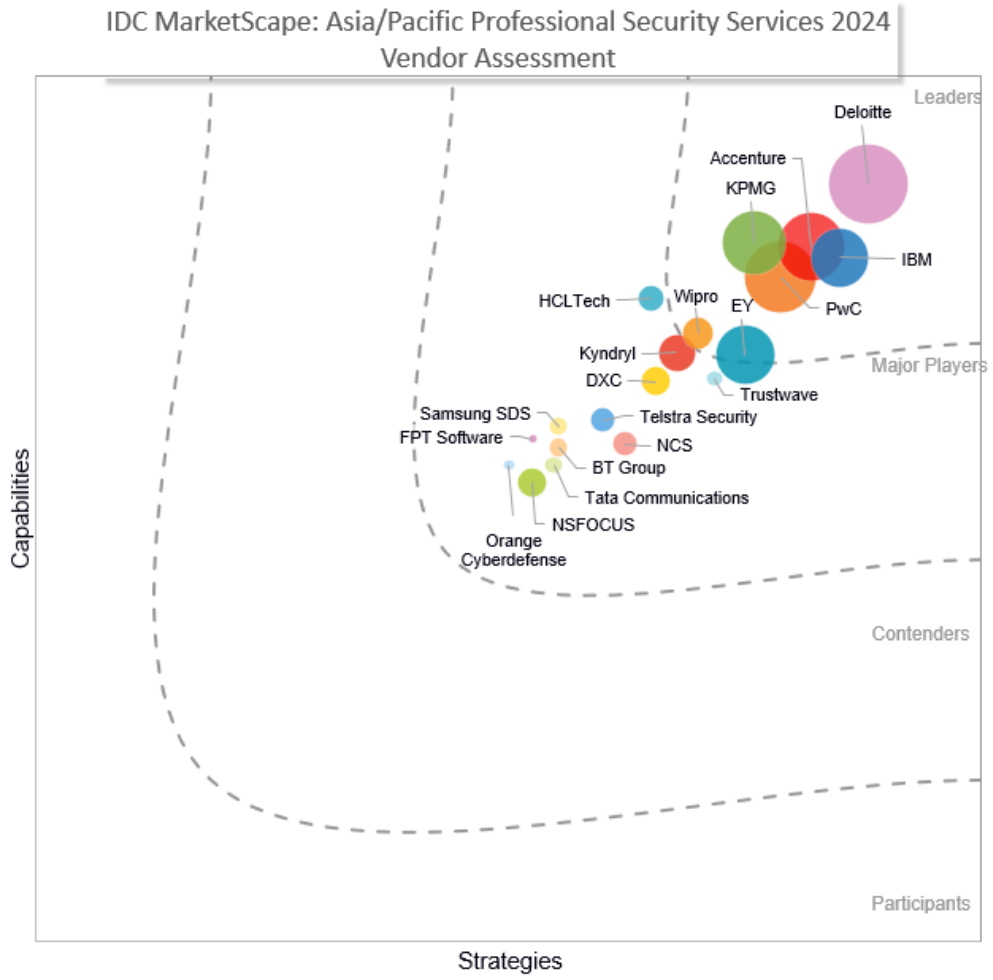
Sakshi Grover Christian Fam

THIS IDC MARKETSCAPE EXCERPT FEATURES KPMG

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Asia/Pacific Professional Security Services 2024 Vendor Assessment



Source: IDC, 2024

September 2024, IDC #AP51571324e

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Asia/Pacific Professional Security Services 2024 Vendor Assessment (Doc # AP51571324). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The professional security services (PSS) landscape in the Asia/Pacific region continues to evolve, driven by an increasing demand for advanced cybersecurity capabilities and the integration of emerging technologies such as AI, ML, and cloud security. Organizations across industries — ranging from finance and healthcare to manufacturing and government — are realizing that cybersecurity is no longer just a protective measure but a strategic enabler of growth, resilience, and competitive advantage.

In this IDC MarketScape study, IDC assesses the following cybersecurity professional service offerings closely, while most of the featured vendors in this study do have a broader portfolio that goes beyond cybersecurity professional services:

- Cybersecurity consulting services
- Governance, risk, and compliance (GRC) services
- Incident management services

Cybersecurity professional services can be tailored and delivered as standalone customized solutions based on specific needs, but they are frequently designed as part of, or integrated within, broader IT or business transformation initiatives.

In this landscape, IDC notes several trends shaping the market:

- **Evolving cyberthreats.** The rise of more sophisticated cyberattacks, including ransomware, supply chain vulnerabilities, and nation-state threats, is pushing companies to adopt a proactive stance on cybersecurity. Causing vendors to not just respond to threats but are taking a more predictive approach, using advanced threat intelligence, automation, and ML to anticipate and mitigate risks.
- **Cloud and hybrid work environments.** The shift to cloud computing and hybrid work models has transformed the security landscape. Companies are demanding end-to-end security services that protect cloud infrastructures, remote workforce, and distributed applications. Vendors that can offer

seamless security across cloud, on-premises, and hybrid environments, while ensuring compliance with regional regulations, are gaining a competitive edge.

- **Focus on cyber-resilience.** Cyber-resilience, which encompasses the ability to recover from and adapt to adverse cyber events, is becoming a key area of focus. IDC has observed that market leaders are increasingly integrating resilience measures such as disaster recovery, incident response, and business continuity planning into their service offerings.
- **Innovation in security.** Vendors at the forefront of the Asia/Pacific PSS market are heavily investing in cutting-edge technologies such as AI, ML, quantum computing, and blockchain to offer innovative security solutions. These innovations help automate security processes, improve threat detection, and address emerging challenges such as privacy-preserving technologies and quantum-safe cryptography.
- **Strategic partnerships.** A robust partnership ecosystem is crucial for delivering comprehensive cybersecurity solutions. Forward-thinking vendors have developed extensive collaborations with cloud providers (e.g., Amazon Web Services [AWS], Microsoft Azure), cybersecurity software providers (e.g., Palo Alto Networks, CrowdStrike), and even emerging tech firms to provide clients with state-of-the-art security services. These partnerships enable vendors to offer integrated, scalable solutions that can address both current and future cybersecurity needs.

IDC's analysis notes that vendors that excel in innovation, maintain strong global-local partnerships, and offer customer-centric service models, are better positioned to meet the complex security demands of organizations in the Asia/Pacific region. These vendors are not just SPs but strategic partners that play a key role in clients' broader digital transformation (DX) strategies.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

- **PSS offerings.** The participating company is required to have a portfolio that matches at least 50% of IDC's scope of PSS for this study. This encompasses, but is not limited to, consulting, GRC, and incident management services.
- **Geography presence.** Each vendor is required to have in-country PSS delivery capability in a minimum of two Asia/Pacific subregions — North Asia (Japan, Korea), Greater China (China, Hong Kong, and Taiwan), Singapore, Malaysia,

Thailand, Indonesia, Vietnam, and the Philippines (ASEAN), South Asia (India, Pakistan, Sri Lanka, Bangladesh), and Australia and New Zealand (ANZ).

- **Multipoint assessment.** Each vendor is participating in a multipoint assessment covering a number of capabilities and strategy criteria determined by IDC to be the most conducive to success in providing professional security services in Asia/Pacific.

ADVICE FOR TECHNOLOGY BUYERS

When considering a professional security services provider, organizations should take a strategic and long-term approach. Choosing the right vendor goes beyond solving immediate security issues; it is about selecting a partner that can help enhance your overall security posture while supporting your business' DX. Here are key areas to consider:

- Alignment with Business Needs and Industry Expertise
  - Tailored solutions. Different industries have distinct security needs — what works for a financial institution may not be suitable for a healthcare provider or a manufacturing company. Look for vendors that offer industry-specific solutions and have a deep understanding of your regulatory environment, business processes, and operational risks. A vendor with experience in your sector will be better equipped to anticipate potential vulnerabilities and align its security strategy with your business objectives.
  - Long-term value. Ensure that the vendor can provide both immediate value and long-term strategic support. This could include helping you evolve your cybersecurity practices as your organization scales, and as technology and regulatory landscapes change.
- Robust Partnership Ecosystem
  - Technology alliances. A vendor's partnerships with leading technology providers (AWS, Google Cloud, or Microsoft) can be a crucial differentiator. These partnerships give you access to integrated solutions that can enhance the security of cloud deployments, digital identities, and hybrid environments. Vendors with strong alliances can also offer seamless implementation and faster access to cutting-edge innovations.
  - Integration and co-innovation. Some vendors collaborate with customers to cocreate solutions that are uniquely suited to specific challenges. This co-innovation not only ensures better alignment with your needs but can also speed up the time to market for new security capabilities.
- Service Flexibility and Customization.
  - Scalable models. Given that every organization has different security requirements and budget constraints, it is important to work with a vendor that offers flexible engagement models. Whether you need onsite,

offshore, or hybrid delivery, ensure the provider can adjust to your operational demands without compromising quality. Flexibility in pricing models such as outcome-based pricing or subscription models can also make a significant difference, particularly for medium-sized enterprises with limited resources.

    - Global-local presence. Consider a vendor with a strong regional footprint but global capabilities. This combination can ensure that you receive localized expertise while benefiting from global best practices, advanced threat intelligence, and shared security services. Local presence is particularly important when it comes to navigating regional compliance requirements and regulatory landscapes.

- Commitment to Innovation
    - AI, automation, and advanced threat detection: As cyberthreats become more sophisticated, vendors that invest in AI, automation, and ML will be better positioned to provide predictive security and automated responses. These technologies can reduce response times, minimize manual intervention, and detect threats that might go unnoticed with traditional approaches.
    - Emerging technologies. It is important to partner with a vendor that is future-proofing its offerings by investing in areas such as quantum security, blockchain, and privacy-preserving technologies. These capabilities are not just a competitive advantage today — they will be essential in the future as threats continue to evolve.
- Customer-Centric Approach and Service Quality
    - Customer support and communication. Security is an ongoing process, and your vendor should provide regular updates, performance reviews, and be proactive in communicating potential risks or opportunities for improvement. Regular feedback loops and personalized account management can ensure that your security needs are consistently met and that the vendor remains a trusted partner over time.
    - Customized security strategies. Beyond technical expertise, vendors should demonstrate a deep commitment to understanding your organization's unique security challenges and business goals. Providers that take a consultative approach, offering customized security road maps, and being adaptable to changing business environments, can offer significant value in the long run.

By considering these factors, technology buyers can ensure they are choosing a vendor that not only addresses their current cybersecurity needs but also supports their broader digital transformation efforts. Security providers should be viewed as strategic partners that drive business resilience, foster innovation, and help navigate the complexities of today's regulatory and technological landscapes.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

KPMG

According to IDC's analysis and customer feedback, KPMG is positioned in the Leaders category in the 2024 IDC MarketScape for Asia/Pacific professional security services.

KPMG's cybersecurity services portfolio spans various industries, offering comprehensive, end-to-end solutions tailored to market sentiment, business drivers, and emerging cybersecurity trends. With a renewed focus on delivering measurable outcomes grounded in trust, resilience, and security, KPMG strives to navigate the constantly evolving cyberthreat landscape. Its aim is to not only address market opportunity but also to help its customers achieve sustainable cyber-resiliency, ensuring long-term security and business continuity. KPMG's professional security services can be delineated into its strategy and GRC services; assure security and privacy services; transformational security improvement programs; and threat management, response, and recovery services. Across its offerings, KPMG's government and national defense security services, IAM services, and GRC services are the main revenue contributors to its PSS portfolio in the region. However, the firm's cyber transformation, resilience, and data security and privacy services have achieved significant growth recently.

KPMG's established position as a global firm ensures seamless access to a vast pool of resources, enabling the delivery of comprehensive solutions from both technological and business perspectives. Their "cyber as a golden thread" strategy underscores the principle that cyber-risk is interconnected within product integrity, customer experience, and regulatory compliance. This holistic approach weaves cybersecurity into the fabric of business and technology operations. By considering a wide range of business, technology, and cyber use cases, KPMG aims to optimize and embed security throughout the entire business value chain, ensuring robust and resilient operations.

Of the firm's plethora of IPs, tools, and solutions, KPMG's flagship Powered Enterprise Cyber offering provides a unique approach to sustainable DX for its customers. This proposition employs an outcome-based methodology to drive business transformation, utilizing a systematic approach to enhance various business functions integrating Cyber throughout. It encompasses four distinct offerings: Powered Identity, Powered SecOps, Powered Privacy, and Powered Risk. These solutions are designed to be technology-agnostic, capable of being implemented across a variety of popular technology platforms. Another notable

mention is the firm's newly launched Cyber-Risk Insights (CRI) SaaS-based platform that employs a scenario-driven approach to assess the likelihood and impact of cyberattacks more accurately. This allows for cyber-risk to be expressed quantitatively allowing customers to justify business cases to the board and determine optimal strategic business portfolio management over cyber-related investments. In addition, KPMG's freshly developed Quantum Care Framework is designed to help organize and enhance an organization's cyber-resilience in preparation for the inevitable quantum era.

The partnership between KPMG and Microsoft enhances the delivery of comprehensive security solutions, leveraging KPMG's security expertise with Microsoft technologies to help clients achieve their business and security objectives. This collaboration spans multiple joint global propositions, including cloud cyberdefense, data governance, managed detection and response (MDR), and General Data Protection Regulation (GDPR) discovery and maturity, with plans to expand their identity offerings. In 2023, KPMG and Microsoft announced a significant expansion of their global relationship, aiming to reshape professional services in areas such as workforce modernization, secure development, and AI solutions. This includes a multibillion-dollar commitment from KPMG in Microsoft cloud and AI services over the next five years. Additionally, KPMG's strategic partnerships with identity vendors such as SailPoint, Okta, ForgeRock, and Saviynt play a crucial role in streamlining project delivery and minimizing risk for its clients. These collaborations are integral to the success of KPMG's Powered Identity solution, ensuring efficient and secure identity management.

Moving forward, KPMG has plans to establish an AI hub in Asia/Pacific alongside Cranium aimed at helping clients deploy and manage AI with a focus on safety, trust, and compliance. This will better equip customers with the ability to engage with regulators and stakeholders, ensuring their AI initiatives align with evolving legal and ethical standards. This initiative follows the recent launch of a similar hub in Europe, developed in collaboration with Cranium and Microsoft, focusing on the European Union (EU) AI Act. The Asia/Pacific AI Hub will leverage insights from the EU hub, combining KPMG's Trusted Responsible AI Framework, Cranium's enterprise software, and Microsoft's AI technology to provide a comprehensive global perspective on AI security.

Strengths

A standout feature of KPMG's portfolio is its innovative Powered Enterprise service, which emphasizes sustainable DX. This service adopts an outcome-driven methodology, systematically guiding clients in transforming their business functions to achieve desired results. In addition, KPMG's newly furnished Quantum Care and Cyber-Risk Insights services demonstrate a forward-looking approach with a strong emphasis on effectively addressing market needs.

Customers' feedback highlights KPMG's extensive portfolio of offerings and its exceptional ability to tailor services to enhance clients' overall cybersecurity posture. Customers have expressed high satisfaction with KPMG's collaborative approach, praising the firm's ability to work seamlessly with internal teams to achieve desired outcomes across various areas and engagements. This close cooperation has facilitated a smooth transition throughout the customers' DX journey.

Challenges

Customers' feedback suggests that KPMG could enhance its services by offering more industry-specific thought leadership on cyberthreats. By contextualizing insights and strategies to address the unique challenges faced by different sectors, KPMG can better support clients in navigating the evolving cybersecurity landscape. Additionally, customer's feedback indicates that KPMG could improve by deepening its expertise and knowledge of clients' existing platforms, solutions, and technologies. Nonetheless, KPMG continues to demonstrate its commitment to advancing and transforming its cybersecurity professionals by prioritizing cyber certifications and fostering a culture of continuous learning.

Consider KPMG When

With KPMG's extensive global presence, coupled with its suite of professional security services, KPMG is an ideal partner for enterprises that value innovation, foresight, and trust. KPMG's approach is not only cyber-focused but also business-focused, addressing risks from a holistic business perspective to ensure that clients achieve both security and strategic business objectives.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis or strategies axis indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and GTM plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represent the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior and capability.

Market Definition

IDC defines professional security services as specialized, short-term, project-based engagements designed to achieve specific outcomes or deliverables by the project's conclusion. These services can be categorized into three main areas: consulting services, GRC services, and incident management services.

- Consulting services encompass a wide array of professional activities, including security strategy development, transformation planning, cyber-resilience consulting, and architecture assessment and design. These services are designed to help organizations strengthen their overall security posture and align their cybersecurity strategies with broader business objectives.
- GRC services address the increasingly complex requirements organizations face in adhering to local and international cybersecurity frameworks. This includes compliance with privacy regulations, cyber governance standards, risk management practices, and conducting cyber audits to ensure robust security controls are in place.
- Incident management services focus on preparing organizations to effectively handle cyberincidents through comprehensive incident response planning. This includes developing detailed response plans and testing them in simulated scenarios to ensure readiness in the event of a breach or attack.

It is important to note that, for the purposes of this study, professional security services do not include implementation services, which typically involve the installation and configuration of security software or hardware products. The emphasis here is on strategic advisory and planning services rather than on technical product deployment.

LEARN MORE

Related Research

- *Cyber-Recovery as a Service: Enhancing Cyber-Resiliency in a Scalable Fashion* (IDC #AP50956624, June 2024)
- *The State of Ransomware in Asia/Pacific: A Comprehensive Analysis of Ransomware Trends, Payment Dynamics, Data Exfiltration, and Cybersecurity Solutions* (IDC #AP50956924, June 2024)
- *Augmenting Security with Artificial Intelligence* (IDC #AP50957024, June 2024)
- *Implications of the NIST Cybersecurity Framework 2.0 for Asia/Pacific Businesses* (IDC #AP50956724, June 2024)

Synopsis

This IDC MarketScape examined 19 different vendors that offer professional security services in the highly competitive and maturing Asia/Pacific market. The assessment focuses on key vendors providing short-term, project-based services that help organizations address their evolving cybersecurity needs. These vendors were evaluated across multiple criteria, including their ability to deliver consulting services; governance, risk, and compliance (GRC) support; and incident management solutions.

The study highlights how vendors are adapting to emerging threats, regulatory changes, and the increased demand for cloud and digital transformation (DX) security services. Many vendors are leveraging strategic global-local partnerships and innovative technologies, such as AI, ML, and automation, to stay ahead in this dynamic market. The report identifies the strengths of and challenges for the vendors, offering insights into their market positioning and the unique value they bring to clients.

Leaders in the IDC MarketScape are noted for their strong consulting capabilities, extensive service portfolios, and customer-centric approaches, while Major Players are recognized for their growing market presence and focus on regional or industry-specific solutions. With the combination of primary research, as well as IDC's own in-depth industry knowledge and insights, we were able to methodically assess the strength of each participating vendor and its challenges. The vendor's position on the IDC MarketScape figure will be a valuable indicator for enterprises and organizations in Asia/Pacific that are currently seeking a security provider and trusted partner to guide them on their digital transformation (DX) journey.

"Organizations in the Asia/Pacific region are increasingly looking for cybersecurity SPs that not only offer protection but also act as strategic partners in their DX journey. The ability to deliver tailored solutions, leverage cutting-edge technologies, and integrate cybersecurity into broader business strategies will distinguish the

leaders in this rapidly evolving market," says Christian Fam, senior research manager, IDC Asia/Pacific Security.

"The professional security services landscape in Asia/Pacific is witnessing a transformative shift, driven by the integration of emerging technologies such as AI, ML, and quantum-safe cryptography. What sets today's PSS market apart is the emphasis on customer co-innovation, in which vendors are not just service providers but strategic partners as well. By collaborating closely with clients, leading vendors are cocreating solutions tailored to industry-specific challenges, enhancing agility, and ensuring security strategies are aligned with broader DX goals. This co-innovation approach, coupled with advanced threat intelligence and seamless security across hybrid environments, is redefining the standards for cybersecurity resilience in the region," says Sakshi Grover, senior research manager, Cybersecurity Products and Services, IDC Asia/Pacific

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

IDC Asia/Pacific Headquarters (Singapore)

168 Robinson Road
Capital Tower, Level 20
Singapore 068912
65.6226.0330
Twitter: @IDC
blogs.idc.com
www.idc.com