IDC MarketScape

IDC MarketScape: Asia/Pacific (Excluding Japan) Managed Detection and Response Services 2025 Vendor Assessment

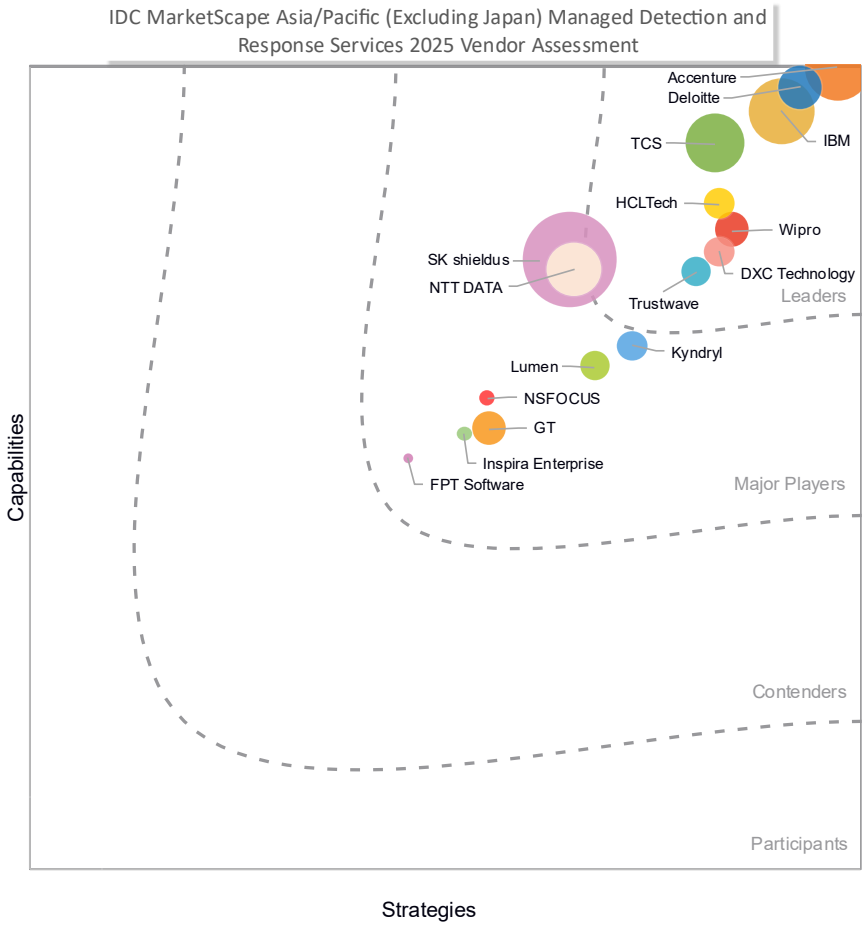
Sakshi Grover Yih Khai Wong

THIS EXCERPT FEATURES ACCENTURE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Asia/Pacific (Excluding Japan) Managed Detection and Response Services 2025 Vendor Assessment



Source: IDC, 2025

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

September 2025, IDC #AP52998725e

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Asia/Pacific (Excluding Japan) Managed Detection and Response Services 2025 Vendor Assessment (Doc #AP52998725e).

IDC OPINION

The managed detection and response (MDR) market in the Asia/Pacific (excluding Japan) (APEJ) region has grown rapidly as enterprises face an evolving and complex threat landscape. According to IDC's *Future Enterprise Resiliency and Spending Survey* (Wave 5, June 2025, n = 250, APEJ), 77% of enterprises in the region experienced ransomware attacks in the past 12 months, with 48% paying ransoms of up to US$1 million. This underscores the scale of the problem and highlights the urgent need for advanced detection and response capabilities.

When asked which technologies were effective in preventing attacks, enterprises in APEJ highlighted a mix of endpoint, network, and analytics-driven tools. Network detection and response (NDR) emerged as the most effective technology, with 47% of enterprises indicating it successfully prevented attacks. This was followed by identity analytics and user and entity behavior analytics (UEBA) at 37% and endpoint detection and response (EDR) at 35%. Security information and event management (SIEM) was cited by 31% of organizations, while packet capture and network packet monitoring (PCAP/NPM) ranked at 28%.

While traditional managed security services (MSS) focused primarily on monitoring and compliance, MDR has emerged as a distinct category centered on proactive detection, intelligence-led hunting, and rapid response. Organizations in financial services, government, manufacturing, healthcare, and critical infrastructure are increasingly viewing MDR as essential to business resilience rather than an operational add-on. The rise of sophisticated adversaries, accelerated cloud adoption, hybrid workforces, and growing regulatory requirements has elevated MDR to a board-level priority across the region.

In this evolving landscape, IDC notes several trends shaping MDR adoption in APEJ:

From monitoring to response. Enterprises now demand measurable outcomes such as reduced mean time to detect (MTTD) and mean time to respond (MTTR). MDR providers are differentiating by embedding response orchestration, threat hunting, and adversary emulation into their offerings, moving well beyond alert management. Despite advances in automation, enterprises continue to value the role of human-led threat hunting and contextual analysis to uncover stealthy threats and validate AI-generated insights.

AI and autonomous operations. Generative AI (GenAI) and agentic AI capabilities are being integrated across MDR platforms. Providers are using AI for enrichment,

summarization, and workflow acceleration, while also piloting autonomous threat hunting and automated playbooks that allow up to 80–90% of incidents to be triaged without analyst intervention. This is particularly relevant in Asia/Pacific, where the cybersecurity talent shortage remains acute. This talent scarcity is one of the key drivers of MDR adoption in the region, as enterprises look to providers with access to specialized expertise that they cannot easily build in-house.

In particular, organizations cite shortages of talent in advanced threat hunting, malware reverse engineering, cloud and application programming interface (API) security analytics, and incident response/forensics. Skills in automation engineering and AI/ML-driven security analytics are also in short supply, underscoring why MDR providers that combine domain expertise with automation are becoming critical partners for enterprises. At the same time, traditional L1 and L2 security operations center (SOC) roles are diminishing, with repetitive triage and enrichment tasks increasingly being taken over by agentic AI tools, allowing scarce human expertise to be redirected toward higher-order investigations and proactive threat hunting. Some providers are also piloting AI assistants to copilot analysts, reconstruct multistage attacks, and fuse telemetry across endpoints, identity, and cloud. This signals a shift toward collaborative, agentic AI models embedded in MDR workflows.

MDR and incident response convergence. IDC notes a growing convergence between MDR and incident response (IR) capabilities. Leading providers are embedding IR readiness elements such as tabletop exercises, adversary emulation, and sector-specific response playbooks into their MDR offerings. This ensures that enterprises not only detect and contain threats quickly but are also prepared to recover effectively when incidents occur. In parallel, AI/GenAI is being applied to accelerate incident triage, forensic analysis, and automated reporting, further strengthening the overall response capability within MDR engagements.

Verticalized use cases and compliance. MDR delivery is increasingly tailored to regulated sectors such as banking, financial services, and insurance (BFSI); healthcare; telecom; and critical infrastructure. Providers are building sector-specific playbooks, aligning with compliance frameworks and incorporating industry threat intelligence to improve contextual detection and meet regulatory mandates around sovereignty and data residency.

Customized threat intelligence. IDC also observes that MDR providers in APEJ are still evolving in how they deliver threat intelligence. Increasingly, firms are moving beyond generic feeds to develop industry-aligned content libraries, custom detection engineering (e.g., sector-specific MITRE-aligned use cases), and regional threat profiles that reflect localized attack patterns. Providers are also embedding this contextualized intelligence directly into MDR platforms and analyst workflows, making it actionable at scale. The ability to personalize intelligence, whether for BFSI facing fraud campaigns or retail and hospitality exposed to supply chain risks, is emerging as a key differentiator. Some enterprises now expect intelligence mapped to their own asset inventories and attacker exposure, ensuring correlation rules and

detections are highly relevant. This personalization not only reduces noise and increases detection fidelity but also helps improve MDR outcomes such as lower false positives, faster investigations, and shorter response times. Providers are beginning to leverage AI to enrich and tailor intelligence, but human validation remains critical to ensure accuracy and applicability.

Cloud, operational technology, and API coverage. With enterprises accelerating migration to multicloud and software as a service (SaaS), MDR providers are extending detection to APIs, SaaS platforms, and operational technology/Internet of Things (OT/IoT) telemetry. MDR offerings are also expanding toward OpenXDR-driven models that consolidate telemetry across IT, OT, IoT, and cloud, reducing integration challenges and providing unified visibility across attack surfaces. This marks a shift from endpoint-only monitoring to truly holistic coverage across enterprise technology landscapes. MDR providers are also increasingly acting as integrators across heterogeneous multivendor environments, ensuring telemetry from diverse EDR, SIEM, and cloud security platforms can be unified into a single, effective MDR workflow.

Regional delivery and sovereignty. Enterprises in APEJ often require in-country MDR delivery or sovereign SOC capabilities to comply with local regulations. Providers with regional SOC footprints, hybrid delivery models, and strong ecosystem partnerships are best positioned to address these needs. A defining feature in the region is the emphasis on "glocal" delivery, that is, standardized global methodologies adapted through sovereign SOCs to align with country-specific sovereignty and compliance requirements. Looking ahead, as AI-enabled MDR becomes mainstream, regulatory frameworks around AI sovereignty, data residency, and explainability are expected to further shape how providers design and deliver services in APEJ.

Client experience and co-innovation. Enterprises increasingly view MDR vendors as long-term partners. Continuous feedback loops, customized reporting, outcome-based service-level agreements (SLAs), and co-innovation pods are becoming central to provider differentiation. Customers are looking for transparency and measurable improvement in security posture, rather than generic service outputs. IDC notes that enterprises increasingly expect MDR providers to demonstrate quantifiable outcomes, such as improvements in MTTD, MTTR, mean time to contain (MTTC) and false positive reduction, as proof of value.

Pricing models and outcome orientation. MDR pricing in APEJ is evolving from device- or volume-based models toward more flexible, consumption-driven, and outcome-based approaches. Enterprises increasingly expect transparency, with pricing aligned with measurable metrics such as reduction in false positives, MTTR improvements, or incident containment levels. Some providers are also piloting playbook-based pricing, in which costs are tied to the execution of specific detection and response workflows. Although still nascent, this model reflects a shift toward

valuing response actions rather than raw monitoring volume, and IDC will be watching closely to see how adoption develops in the region.

Overall, the APEJ MDR market is maturing toward integrated, AI-enabled, and outcome-driven services that combine global delivery standards with regional nuance. The shift is from "monitor and notify" models to proactive, resilient, and business-aligned MDR strategies. Providers that can scale AI-led automation, localize delivery, and demonstrate measurable risk reduction will be best positioned to succeed in this market. Future differentiation in APEJ will depend on MDR providers' ability to combine AI-driven automation with customized threat intelligence, incident readiness, and localized delivery models that align with both regulatory expectations and industry-specific needs.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

MDR offerings. The participating company is required to have a portfolio that matches at least 50% of IDC's scope of MDR for this study. This encompasses, but not limited to, pure-play MDR, managed EDR, managed SIEM, and managed threat hunting.

Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities and cybersecurity partners' supplied tools or services and private intellectual property. Some managed security SPs will utilize a third-party extended detection and response (XDR) platform for the technical portion of the MDR service, then wrap that with their own cybersecurity practitioners to fulfil the "hands on" service part of the service. MDR services are supplied by a provider's well-trained cybersecurity staff in a 24 x 7 x 365 remote SOC.

Geography presence. Each vendor is required to have in-country MDR delivery capability (or SOC presence) in a minimum of two subregions of Asia/Pacific — North Asia (Japan, Korea), Greater China (China, Hong Kong, and Taiwan), Association of Southeast Asian Nations (ASEAN) (Singapore, Malaysia, Thailand, Indonesia, Vietnam, and the Philippines), South Asia (India, Pakistan, Sri Lanka, Bangladesh), and Australia and New Zealand (ANZ). The in-country security services delivery capabilities can be leveraged through local partnerships if applicable.

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 managed detection and response services in Asia/Pacific (excluding Japan).

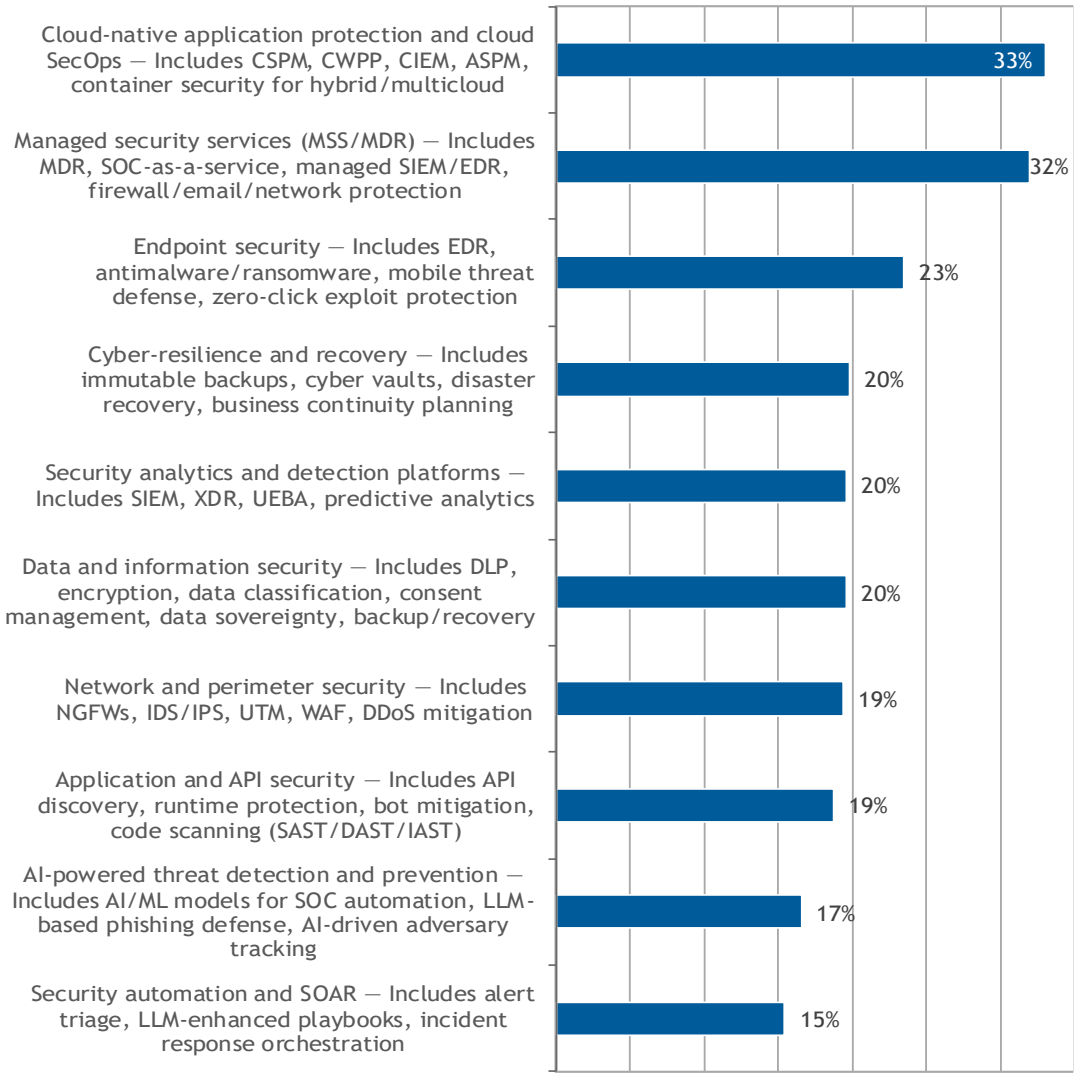
ADVICE FOR TECHNOLOGY BUYERS

Chief information officers (CISOs) across Asia/Pacific have made their priorities clear. According to IDC's *Asia/Pacific Security Survey*, August 2025 (see Figure 2), MSS/MDR ranks as the second-highest spending priority for the next 12–18 months, identified by nearly one-third of enterprises. This growing emphasis reflects the urgency to strengthen detection and response as organizations face rising ransomware, regulatory mandates, and increasingly complex hybrid environments.

FIGURE 2

CISO Priorities: Security Investments Over the Next 12–18 Months

Q. Which of the following areas will be the top 3 priorities for security spending in your organization in the next 12–18 months?



Note: n = 460 for APEJ

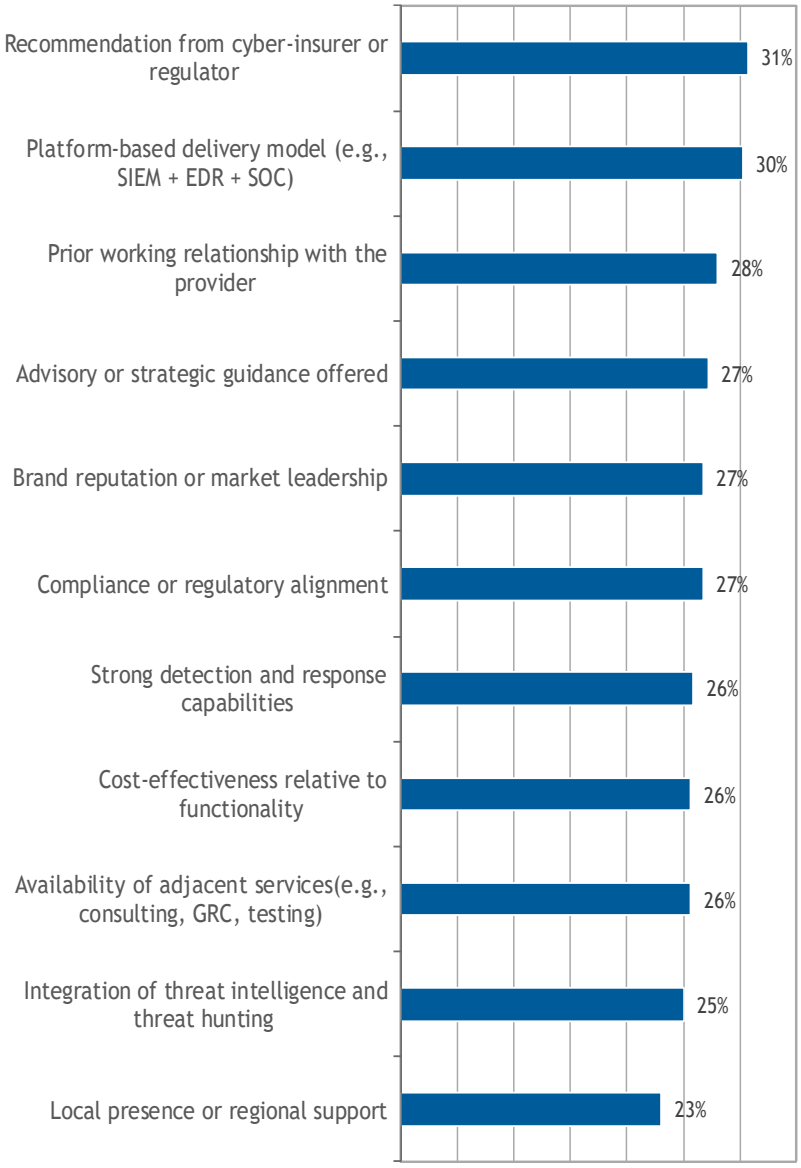
Source: IDC's Asia/Pacific Security Survey, August 2025

Building on these priorities, IDC's research also sheds light on the factors that influence how enterprises actually select MDR providers (see Figure 3). While recommendations from insurers or regulators, platform-based models, and established relationships often guide initial decisions, buyers must increasingly look beyond familiarity and reputation. To maximize value, enterprises should evaluate MDR providers based on measurable outcomes, integration capabilities, and alignment with regional compliance and sovereignty requirements.

FIGURE 3

Top Drivers for Selecting an MDR Provider in APEJ

Q. What were the top 3 reasons your organization chose its current MDR provider?



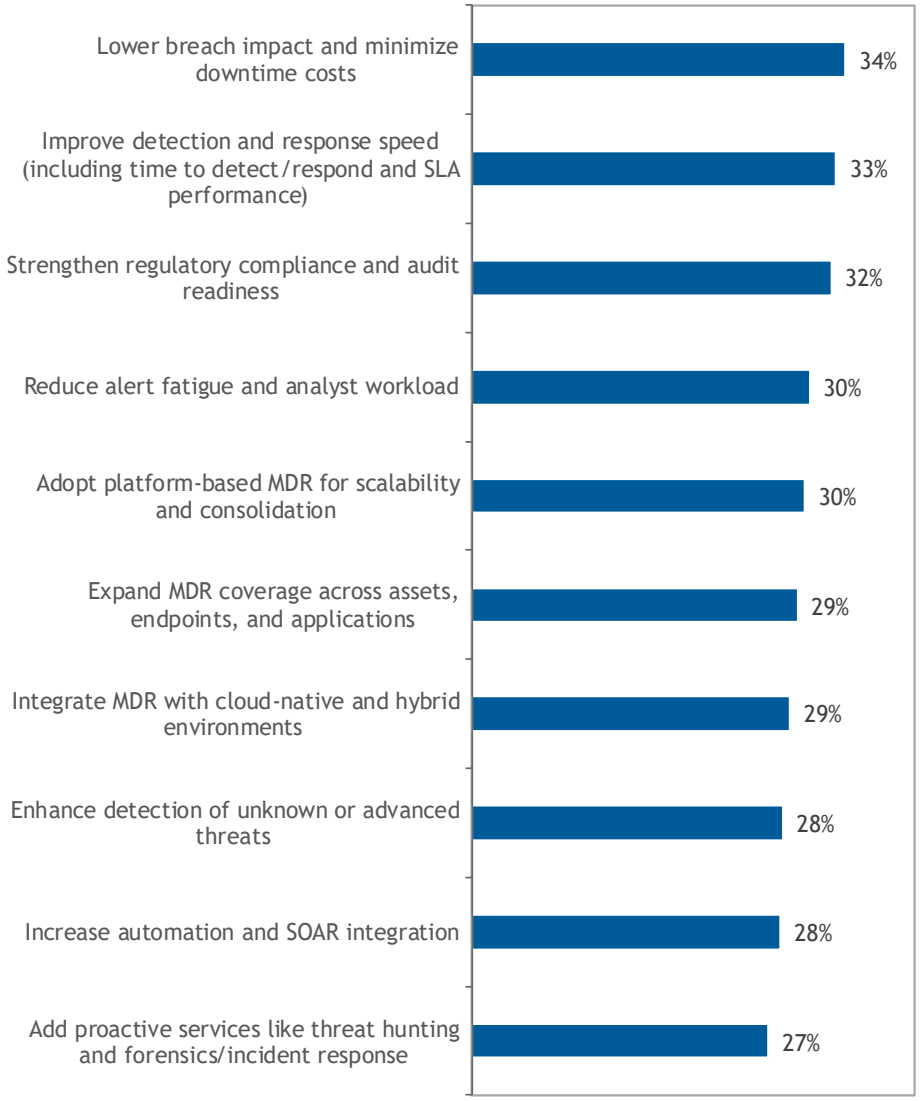
Note: n = 460 for APEJ

Source: IDC's Asia/Pacific Security Survey, August 2025

Looking ahead, enterprises in Asia/Pacific are not only investing more in MDR but also reshaping their expectations from providers. According to IDC's research (see Figure 4), the top priorities for evolving MDR engagements over the next 12–18 months include lowering breach impact and downtime costs, improving detection and response speed, and strengthening regulatory compliance. CISOs are moving beyond basic monitoring to demand outcome-focused MDR partnerships that reduce business risk, ensure audit readiness, and deliver faster, more effective response.

FIGURE 4

How APeJ Enterprises Plan to Advance MDR in the Coming Year



Note: n = 460 for APeJ

Source: IDC Asia/Pacific Security Survey, August 2025

IDC offers a practical checklist for enterprises in APEJ evaluating MDR services. Rather than focusing on features or brand familiarity, buyers should anchor their selection process on outcomes, resilience, and regional fit. The following considerations provide a structured guide to help CISOs assess MDR partners that can deliver measurable improvements, balance automation with expertise, and align with the unique compliance and operational realities of Asia/Pacific.

IDC's Checklist for Technology Buyers:

- Enterprises in APEJ evaluating MDR services should approach vendor selection with a focus on outcomes rather than features. The ability of a provider to demonstrate measurable improvements in MTTD, MTTR, MTTC, and false positive reduction should be a key evaluation criterion. Buyers should ask for outcome-based SLAs, client references, or case studies that show quantifiable improvements.
- Given the acute talent shortage in the region, organizations should also assess how MDR providers balance automation with human expertise. Although GenAI and agentic AI are increasingly embedded into MDR workflows, human-led threat hunting, contextual analysis, and incident response expertise remain critical. Buyers should evaluate the maturity of a provider's AI capabilities, the scope of automation in their SOC processes, and how scarce analyst resources are redirected toward higher-order investigations. In parallel, they should recognize that traditional L1/L2 roles are diminishing as repetitive triage and enrichment tasks are increasingly handled by AI, freeing up experts for proactive threat hunting and forensic work.
- Industry alignment is another critical factor in APEJ. MDR providers that deliver vertical-specific playbooks, regulatory alignment, and customized threat intelligence can better support enterprises operating in regulated industries such as BFSI, healthcare, telecom, and critical infrastructure. Buyers should ensure providers not only bring global best practices but can also adapt to local compliance, sovereignty, and operational requirements, especially as data protection, digital sovereignty, and AI governance laws continue to tighten across the region.
- Geographic presence and localization matter more in APEJ than in many other markets. The region is both linguistically and operationally diverse, making local-language SOC support, in-country analyst presence, and regional threat intelligence teams essential to ensuring detection and response are timely, relevant, and compliant with local requirements.
- Integration and ecosystem fit should not be overlooked. Many enterprises in APEJ operate hybrid and multivendor environments across endpoint, network, cloud, and identity solutions. Buyers should evaluate whether MDR providers

can seamlessly integrate telemetry from their existing stack into unified MDR workflows, or whether they are tied to a single-vendor ecosystem. Providers with strong OpenXDR capabilities, open APIs, and an ecosystem approach will offer greater flexibility and resilience. OT monitoring capabilities are also another area of integration that needs to be considered, especially for enterprises that deal with critical information infrastructure.

- Enterprises should also consider whether a provider can support adjacent or converging services. MDR is increasingly bundled with managed vulnerability management, threat intelligence, and incident readiness. Consolidating these capabilities with one partner can improve efficiency, while certain services, such as offensive testing and compliance audits, may still be better sourced independently to preserve objectivity.
- Pricing transparency and flexibility are especially critical in a cost-sensitive region like APEJ. Traditional device- or volume-based models may not always align with enterprise needs. Consumption-driven, outcome-based, or even playbook-based models are emerging. Although still nascent, playbook-based pricing, in which costs are tied to the execution of specific response workflows, reflects a shift toward valuing outcomes rather than raw monitoring volume. Buyers should evaluate which models provide the right balance of predictability, scalability, and value.
- Finally, enterprises should assess how MDR providers manage incident response and historical data. Some vendors include IR hours or unlimited support in MDR contracts, while others offer financial credits or compensation. Buyers should ensure these align with cyber-insurance policies and internal risk appetites. Providers that can ingest historical data to baseline "normal" behaviors will also deliver stronger detection fidelity over time and help reduce alert fatigue in resource-constrained teams.

Overall, enterprises in APEJ should prioritize MDR providers that combine automation and human expertise, deliver measurable outcomes, embed localized delivery and intelligence, integrate with diverse ecosystems, extend into adjacent services, and offer transparent, flexible pricing models. Providers that align with these criteria will be best positioned to help enterprises transition from reactive monitoring to proactive, resilient, and business-aligned security.

FEATURED VENDOR SUMMARY PROFILE

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

Accenture

According to IDC's analysis and customer feedback, Accenture is positioned in the Leaders category in the 2025 IDC MarketScape for Asia/Pacific (excluding Japan) managed detection and response services.

Accenture is a global professional services firm providing consulting, technology, and outsourcing services, with a focus on digital, cloud, and security solutions. Accenture delivers MDR services across the Asia/Pacific region through its globally integrated Cyber Fusion Centers and its modular, intelligence-driven MxDR platform. The MxDR solution is designed for flexibility and integration, supporting hybrid environments across IT, OT, and IoT. It leverages a proprietary layer called MxDR-Play, which provides unified visibility, enriched analysis via automation and GenAI, and seamless integration with SIEM, security orchestration, automation, and response (SOAR), and IT service management (ITSM) platforms to accelerate incident response and reduce human error. MxDR is further differentiated by its ingestion-based pricing model, modular deployment options (including bring-your-own-platform and platform-as-a-service), and integration with clients' existing investments. The platform supports integration with over 50+ security technologies, including SIEM, EDR, NDR, SOAR, and ITSM/ticketing systems, allowing clients to retain their existing toolsets or adopt a fully managed platform model for faster time-to-value.

Accenture has embedded GenAI across the MDR life cycle through its proprietary operational GenAI layer, which enhances decision making and analyst confidence during critical incidents. This layer powers use cases such as real-time incident report generation, malware explainability, multilingual translation (supporting six languages), automated malware classification, and SOC assistant support. Designed to be platform-agnostic, these capabilities operate alongside native GenAI tools within client environments to deliver greater speed and precision in threat response. Accenture also offers a continuously updated Industry Content Library and a dedicated Content Factory with over 100 engineers delivering detection-as-code, SOAR playbooks, dashboards, and emergency content mapped to the MITRE ATT&CK framework.

The company's MDR approach is heavily intelligence-led, supported by a 300+ strong global threat intelligence team operating across 11 countries and 22 languages, with curated industry-specific threat feeds, and integration with partners such as Mandiant and CrowdStrike. Accenture's intelligence operations are further enhanced by insights from 1,000+ clients, national Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs), and regular threat briefings.

Accenture delivers vertical-specific SOC capabilities and modular MDR offerings tailored to the operational and compliance needs of sectors such as manufacturing, energy, aviation, healthcare, and financial services. The MxDR platform provides

role-based self-service dashboards that deliver real-time visibility into KPIs such as MTTR, false positive rates, and attack types, helping improve SOC transparency and executive reporting. Its hybrid architecture supports integration with widely used platforms including Google Chronicle, Microsoft Sentinel, and CrowdStrike Falcon, allowing organizations to retain existing tools or transition to a managed model. With MDR services operating across 67 countries in Asia/Pacific, Europe, the Middle East, and Africa (EMEA), and the Americas, Accenture offers consistent delivery and localized support at global scale.

Service delivery is enabled through sovereign and delivery centers in India, the Philippines, Malaysia, Australia, and Singapore. Accenture continues to scale its talent through local hiring and structured training via its Security Academy, which offers role-based upskilling paths for SOC personnel, including GenAI-specific modules to ensure readiness for AI-augmented operations. The firm maintains a partner-agnostic stance and actively co-engineers MDR capabilities with ecosystem partners and hyperscalers to drive innovation, including initiatives such as the Microsoft Copilot integration with MxDR workflows and GenAI integrations with Google.

Accenture's strategy focuses on furthering the use of agentic AI, expanding its sovereign delivery footprint, accelerating SOC transformation from legacy to modernized architectures, and reducing MDR onboarding time. The company also facilitates ongoing knowledge exchange with security leaders across regions through dedicated forums and community engagement initiatives.

Accenture is deepening its MDR strategy by embedding agentic AI, GenAI, and detection-as-code across its MxDR platform to enhance analyst efficiency, threat response speed, and platform adaptability. Over the next 12–18 months, the company plans to expand GenAI capabilities for incident summarization, malware explainability, SOC assistants, and multilingual support, while enriching its Content Factory with industry-specific detection logic and dynamic threat modeling. To meet growing regulatory demands, Accenture is scaling sovereign delivery in Asia/Pacific with expanded operations in Singapore, India, and Australia, and aligning its MDR services to the needs of regulated industries such as manufacturing, energy, healthcare, and aviation. It continues to codevelop GenAI-led threat response use cases with hyperscalers and ecosystem start-ups and is investing in GenAI-powered onboarding accelerators and integration toolkits to reduce time-to-value. With governance guardrails and explainability embedded into its operational design,

Accenture is positioning itself to deliver measurable outcomes through AI-augmented detection, modular platform innovation, and localized compliance-driven service delivery across Asia/Pacific. As part of its broader transformation agenda, Accenture also assists clients in optimizing and consolidating security toolsets, supporting both improved operational efficiency and reduced environmental impact.

Strengths

Clients value Accenture's ability to provide 24 x 7 managed SOC operations and incident response, supporting consistent security monitoring and faster containment. The firm's breadth of experience across managed EDR, SIEM, and threat hunting services was cited as a key factor in reducing reliance on internal resources and improving the organization's cyber-risk posture. Accenture's MDR offering, which includes telemetry ingestion, analytics-driven detection, and remote incident response, aligning it with client expectations for integrated threat management. Clients have reported reduced monthly threat incidents up to 90%, improved compliance postures, and enhanced executive visibility through real-time dashboards. Accenture's MDR services benefit from the firm's broader experience in delivering large-scale IT transformation programs, enabling it to support centralized cybersecurity operations with consistent delivery, integration depth, and global scalability.

Challenges

As Accenture continues to expand the use of AI to improve efficiency and accelerate response times across its MDR services, the MxDR platform is also evolving with ongoing enhancements. There are opportunities to further strengthen investigative depth and deliver even more proactive security recommendations. Similarly, continued refinements to the user interface and analyst experience are expected to improve overall usability and engagement. Investments in contextual response capabilities and analyst workflows reflect Accenture's focus on advancing the platform's end-to-end effectiveness.

Consider Accenture When

Consider Accenture when you need an MDR provider with global delivery scale, deep domain experience in securing critical infrastructure, and the ability to localize services for regulatory and operational needs. Accenture's modular MxDR platform supports diverse environments and integrates with a wide range of existing security investments, making it suitable for both large enterprises and midmarket organizations undergoing security modernization. Organizations seeking a centralized security partner that can align cybersecurity operations with broader IT transformation agendas may also benefit from Accenture's integrated service approach and cross-functional delivery capabilities.

Please Note: *At the time of this evaluation, Accenture's acquisition of CyberCX had not been completed. This transaction represents a significant step in Accenture's growth strategy to expand its cybersecurity capabilities across the Asia/Pacific region. CyberCX brings approximately 1,400 skilled professionals, AI-powered security platforms, and a broad portfolio of managed detection, incident response, and offensive security services,*

along with operations in Australia, New Zealand, London, and New York. As this assessment was developed prior to the completion of the acquisition, it reflects Accenture's standalone capabilities and does not yet incorporate CyberCX's

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.

This IDC study evaluates MDR service providers in the Asia/Pacific (excluding Japan) region based on their breadth of detection and response offerings, threat hunting and incident response capabilities, platform integration, cloud and endpoint coverage, and use of AI/automation. The assessment also considers their go-to-market approaches, regional delivery models, and ability to address diverse

customer segments. In addition, the study examines each vendor's growth trajectory in the region, their investments in innovation, and strategies for expanding MDR capabilities in the future.

Market Definition

Managed Detection and Response

IDC recognizes that the managed security services (MSS) market has seen three distinct evolutionary points. The first offerings were designed to protect the perimeter of the organization by providing the management and support of security devices and software such as antivirus, firewalls, and log management. The second generation saw evolutions such as comanaged or outsourced security information and event management (SIEM) and the use of AI/ML technologies to help speed up the detection of indicators of compromise (IoCs) as organizations were launching their DX efforts.

In the third generation, managed detection and response (MDR) services offerings have come about to provide a unified service to protect organizations from the advanced velocity and quality of cyberattacks that are now the norm. Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities and cybersecurity partners' supplied tools or services and private intellectual property. Some managed security SPs will utilize a third-party extended detection and response (XDR) platform for the technical portion of the MDR service, then wrap that with their own cybersecurity practitioners to fulfil the "hands on" service part of the service. MDR services are supplied by a provider's well-trained cybersecurity staff in a 24 x 7 x 365 remote SOC.

MDR can be categorized into four main areas:

Pure-Play MDR

MDR, as a subset of MSS, combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity detection and response capabilities for an organization. Service providers can deploy MDR services utilizing a mixture of customers' existing capabilities and partner-supplied tools or services and private intellectual property. MDR services are typically supplied by a provider's well-trained cybersecurity staff that works in one or more 24 x 7 x 365 remote SOCs.

IDC recognizes the following capabilities as a minimum set of pure-play MDR capabilities:

- Endpoint protection capabilities are utilized as an embodiment of an endpoint detection and response (EDR) system. The greying of lines between EDR and XDR is resulting in the recognition that an XDR platform with EDR functionality can take the place of a traditional EDR system.

- Multiple telemetry sources are ingested into a common data lake or similar system. A back-end SIEM or XDR platform may take the place of a data lake. Telemetry beyond the endpoint that can be ingested includes:
  - Identity
  - IoT
  - OT
  - Email/messaging
  - Cloud
  - Mobile
  - SIEM
  - Network
  - UBA/UEBA
- MDR systems must ingest telemetry from endpoint, identity, cloud, network, UBA and/or UEBA, and SIEM data to be considered a complete MDR service. IoT, OT, email/messaging, and mobile telemetry feeds are beneficial but not always captured.
- Big data and analytics and ML algorithms are used to correlate and then detect likely attacks that require further investigation and a possible response action.
- The integration of multiple threat intelligence feeds provides timely information into the MDR service. The objective is to enable organizations to understand what systems are being targeted, who is doing the targeting, and the tactics, techniques, and procedures that are vital in moving cybersecurity from a reactive stance to a proactive stance.
- Human-led threat hunting is regularly used to supplement threats uncovered by IoCs to be based on risk analysis and/or integrated threat intelligence feeds. The processes and playbooks that are created in human-led threat hunting activities should be included in the equally important automated threat hunting activity.
- Remote incident response (little R) services include containment and removal of adversaries, incidents, or breaches in which data is suspected or known to have been exfiltrated, destroyed, or manipulated. IDC believes that a core part of the MDR service must go beyond offering guidance and recommendations and should include a component that can automate a response for a customer when malware is downloaded but no other collateral damage occurs.
- Comprehensive remote incident response (big R) services (at an additional charge) are for the serious breaches that require a coordinated response, remediation, and forensic capability. Some firms will choose to utilize a partner for the actual incident response work. In addition, some MDR providers might choose to utilize a partner for any required forensics.

- Web-based dashboards allow for the monitoring, updating, and reporting of all IoCs and/or tickets that are created from the service.

An important difference to note in the post-pandemic world is that the remote capabilities that MDR providers offer do not necessarily have to be done from an actual SOC. The continued cybersecurity talent shortage and proven ability of work-from-home cybersecurity practitioners have shown that a physical SOC, while beneficial for collaborative teamwork, is not a requirement for MDR.

The evolution of the extended detection and response market has provided new opportunities for enhanced detection and response. Building upon its roots as an extension of EDR, XDR is now the platform for which detection and response actions can occur beyond the endpoint. Initial iterations of XDR added additional telemetry that traditional EDR did not provide, such as cloud, messaging, and application telemetry ingestion and correlation. More recent iterations of XDR are more cognizant of the value of network telemetry and usually provide internal network detection and response (NDR) capabilities, or they work with third-party NDR providers to provide this capability. Like other known security tools, XDR is often offered as a managed service by managed security SPs or systems integrators and consultancies as an MXDR service.

The lines blur when trying to differentiate between an MXDR platform–based service and a managed service such as MDR. Generally speaking, an MDR service wraps services around the customer's current cybersecurity tooling stack. Tools such as endpoint detection and response (EDR) and security information and event management (SIEM) were the workhorses of early MDR services. As MDR matured, security orchestration, automation, and response (SOAR) capabilities were add-on options, usually at an extra cost, for their customers. Today, SOAR capabilities are a given, and the capabilities that these tools provide are almost always embedded into the MDR service.

Managed EDR

Managed EDR is a service that actively manages EDR systems as they preemptively detect malicious activity and respond to threats before endpoint compromise occurs. It can also be configured to automatically remediate a host that is compromised. EDR uses multiple monitoring points to detect attempts to compromise the system. EDR scans memory, running processes, network activity, and common attack rule sets to preemptively stop threats before they can change files or exfiltrate data. EDR can be complex and generate large amounts of data that may need large data storage requirements for an enterprise.

Managed SIEM

A managed SIEM service is an alternative to the on-premises deployment, setup, and monitoring of a SIEM software solution. An enterprise may choose this managed service to monitor the organization's network for potential security threats. Ideally,

this service will provide real-time analysis of security alerts that are generated by other security tools, network feeds, and applications and that recognize potential security threats before they have a chance to impact and disrupt the enterprise. A managed SIEM can benefit an enterprise with faster deployment; reduced setup, tuning, and training costs; and access to wider expertise of security specialists.

Managed Threat Hunting

This managed service delivers proactive, human-led, and machine-aided threat hunting to detect suspicious activity and cyberthreats. This can be done through manual and automated techniques such as analyzing log data, conducting network scans, and using threat intelligence feeds. Managed threat hunting aims to identify potential threats that may have evaded traditional security controls such as firewalls or intrusion detection systems (IDSs). By detecting and responding to these threats early, organizations can reduce their risk of being impacted by an attack.

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide Incident Response 2025 Vendor Assessment* (IDC #US52036825, August 2025)
- *Regulatory Turning Point: How Data Privacy, Cybersecurity, and AI Laws Are Reshaping Enterprise Strategy in Asia/Pacific* (IDC #AP52287825, June 2025)
- *Securing the Cloud: Key Priorities Driving Security Investments in Asia/Pacific* (IDC #AP52287725, June 2025)
- *The Critical Control Points for Security* (IDC #AP52287525, May 2025)
- *IDC's Worldwide Security Services Taxonomy, 2025* (IDC #US53294625, April 2025)
- *Disruptive Cybersecurity Solutions Shaping the China Market: How Emerging Security Innovations and Local Vendors Are Transforming Cyberdefense in China* (IDC #AP52287425, March 2025)
- *The Digital Operational Resilience Act: What Does It Mean for Asia/Pacific Financial Institutions?* (IDC #AP52898425, March 2025)
- *IDC ProductScape: Worldwide Managed Detection and Response, 2024–2025: Technology Supplier Solution Functionality* (IDC #US53104825, January 2025)
- *AI-Powered Cybersecurity: Navigating the Expanding Attack Landscape, Asia/Pacific CISO's Concerns, Priorities and Investment Areas, and Strategic Vendor Support* (IDC #AP52591824, September 2024)

Synopsis

This IDC MarketScape evaluates 16 vendors that provide managed detection and response (MDR) services within the Asia/Pacific (excluding Japan) market, a segment that is expanding rapidly as enterprises shift from traditional monitoring to outcome-driven detection and response. The participating firms were rigorously assessed using the IDC MarketScape methodology, which reviews each vendor's current capabilities and future strategies against a comprehensive set of criteria. The assessment framework encompassed over 20 market-defining factors, including breadth and depth of MDR offerings, platform integration, response orchestration, cloud and endpoint coverage, vertical-specific use cases, delivery models, regional presence, partner ecosystem, innovation, pricing, marketing and thought leadership, and customer experience.

IDC conducted extensive primary research, including structured request for information (RFI) submissions, detailed briefings, and multipoint interviews with both vendors and their clients to capture differentiating factors, customer perceptions, and service outcomes. This was complemented by IDC's in-depth industry expertise and regional insights. Following comprehensive analysis and deliberation with IDC's internal panel of experts, the findings informed the positioning of vendors in the IDC MarketScape figure. The resulting vendor positioning offers enterprises in APEJ a practical barometer for identifying and evaluating MDR partners capable of delivering measurable detection and response outcomes, improving security resilience, and aligning with the unique regulatory and operational needs of the region.

"Enterprises in Asia/Pacific are redefining MDR as more than a security operations extension; it is becoming the digital control plane for resilience. The next wave of MDR in this region will fuse telemetry across IT, operational technology, cloud, and application programming interfaces (APIs) while embedding agentic AI assistants that copilot analysts, automate cross-domain correlation, and continuously validate posture against regulatory and sovereign mandates. Early signals point to MDR platforms capable of reconstructing multistage kill chains, simulating adversary behavior, and executing preapproved response playbooks in milliseconds. In a region marked by talent scarcity, ransomware scale, and diverse compliance regimes, providers that position MDR as an adaptive, AI-infused risk platform, rather than a static service, will define the future of trusted digital ecosystems in APEJ," says Sakshi Grover, senior research manager, Cybersecurity Products and Services, IDC Asia/Pacific.

"The MDR market is undergoing an evolution, shifting from detection and monitoring to a proactive and outcome-driven platform. The rapid adoption of AI/GenAI solutions has raised the bar in terms of threat detection and response expectations from organizations. Security SPs can no longer rely on monitoring and reporting threats, but are expected to integrate AI, automation, and threat intelligence analytics into a unified MDR platform to deliver outcome-based business

resilience. As the threat landscape expands and becomes even more complex, service providers will need to demonstrate strong MDR platform delivery capabilities with cutting edge in-house AI-driven tools to deliver strategic business outcomes," adds Yih Khai Wong, senior research manager for Cybersecurity Services and Products, 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