IDC MarketScape

IDC MarketScape: Worldwide MDR/MXDR for the Enterprise 2026 Vendor Assessment

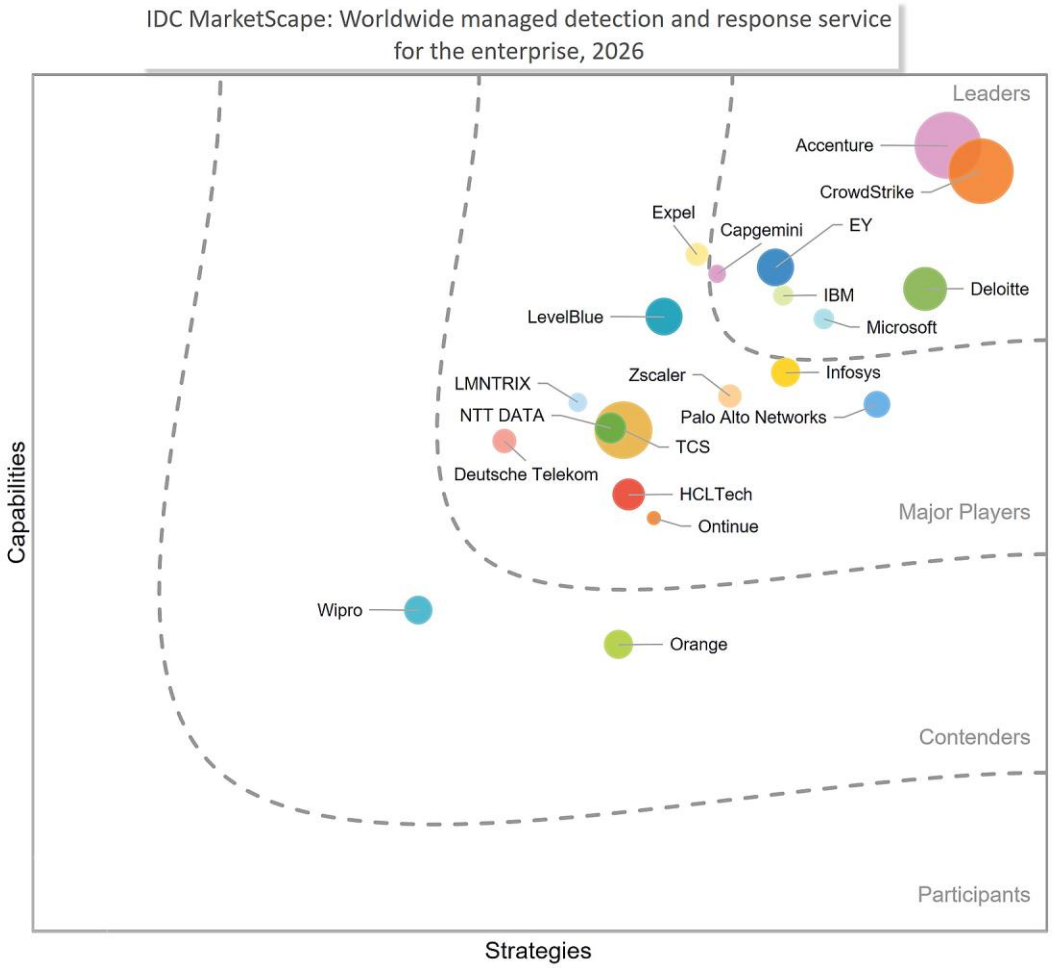
Craig Robinson

THIS EXCERPT FEATURES ACCENTURE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide MDR/MXDR for the enterprise, 2026



Source: IDC, 2026

August 2026, IDC #US54792426e

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

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: IDC MarketScape: Worldwide MDR/MXDR for the Enterprise 2026 Vendor Assessment (Doc # US54792426).

IDC OPINION

This IDC MarketScape assesses vendors delivering managed detection and response (MDR) and managed extended detection and response (MXDR) services to enterprise buyers worldwide, drawn from several structurally distinct provider categories, each approaching the market from a different starting point. Platform-native MDR providers built their practice around a proprietary detection stack and expanded to services. Global systems integrators and MSSPs bring large delivery organizations, broad telemetry integration, and bundled adjacencies such as identity and vulnerability management. Carriers and infrastructure operators layer MDR onto their existing network visibility. A newer cohort of GenAI-forward entrants is racing to differentiate on automated triage and agentic investigation. What unites them is a buyer base that has grown considerably more demanding about what “managed” means in practice, not only in the sales deck.

IDC observes that the enterprise MDR market has entered a phase where raw detection coverage is table stakes and the competitive battleground has shifted to consistency of execution, the quality of human judgment behind automated findings, and whether a provider’s output genuinely closes the loop between “we stopped this attack” and “here is how you should change your posture so it does not happen again.” Buyers are no longer satisfied with dashboards full of alerts and a monthly report. They are asking harder questions about analyst quality, SLA reliability under real stress, and whether GenAI investment inside the security operations center (SOC) is translating into better outcomes or simply faster-looking ones.

Analyst quality remains the market’s most persistent credibility gap

Despite years of provider investment in automation, ML, and now GenAI-assisted triage, buyers remain unconvinced that the human layer behind MDR services is consistently strong. In IDC’s *WW MDR and Managed Security Services Survey 2026*, only 37% of respondents said their provider’s analysts consistently deliver high-quality analysis with clear, accurate findings. Another 38% said the analysis is generally reliable but occasionally misses context or depth, and nearly 22% said it is adequate at best and often requires follow-up or clarification before it is usable. That leaves a majority of the enterprise base receiving something short of confidently reliable analytical output.

This finding carries more weight given how aggressively providers have marketed GenAI capabilities inside their SOCs over the past two years. The promise of GenAI-assisted investigation was supposed to compress the distance between raw telemetry and an analyst's finished conclusion, freeing human analysts to focus on judgment rather than data assembly. What buyers report instead is a persistent disconnect between the mechanics of stopping an active threat and the strategic value of turning that incident into an improved defensive posture. A provider can contain a ransomware attempt cleanly and still fail to tell the client which control gap allowed initial access, which segmentation change would prevent recurrence, or how the finding should reshape the client's broader risk program. Containment is being delivered. Connective insight is not, at least not consistently. This is precisely the gap that separates a commodity detection and response service from a genuine security partner, and it is the dimension IDC expects to separate Leaders from Major Players over the next several IDC MarketScape cycles. Providers investing in GenAI purely to accelerate ticket closure are optimizing the wrong variable. The buyers who rated their provider highest on analyst quality consistently described a specific behavior, which is the analyst who not only closes the case but explains the "so what" in language the client's own security team can act on without a follow-up call.

SLA performance shows wide variance, and the Middle East was a genuine stress test

The second signal buyers are increasingly scrutinizing is whether providers meet the SLAs they sold. Across the total enterprise sample, only 15% of respondents said their MDR provider always meets applicable SLAs, defined as better than 95% of the time. Another 44% said their provider usually meets SLAs, in the 80–95% range, while a third of the market reported SLA performance somewhere between sometimes and rarely. That is a wide spread for a service category whose entire commercial premise rests on guaranteed response times.

The regional breakdown is where this finding becomes operationally significant rather than merely a satisfaction metric. North American respondents reported considerably stronger SLA adherence, with 62% saying their provider always or usually met SLAs. Middle East respondents reported a starkly different experience, with only about 32% reporting the same level of consistency, more than half describing SLA adherence as merely sometimes achieved, and a rarely category running more than double the global average. This survey was fielded in April and May of 2026, a window that coincided with active kinetic conflict across parts of the Middle East. Regional MDR operations were, in effect, stress tested in real time against exactly the kind of elevated threat activity that MDR contracts are meant to withstand. The results suggest that a meaningful share of providers serving the region were not staffed, resourced, or architected to sustain committed response times once genuine wartime-adjacent threat volume and complexity arrived. Buyers evaluating a provider's Middle East delivery model should treat this period as a live reference case rather than a

hypothetical, and should ask pointed questions about surge staffing, follow-the-sun coverage depth in the region, and whether SLA credits or remediation commitments were actually honored during the stress window rather than only during calmer baseline conditions.

Taken together, these two findings point to the same underlying theme. The enterprise MDR market has largely solved the problem of technical detection breadth. It has not yet solved the harder problem of consistent human judgment and operational resilience under real pressure. Buyers should treat analyst quality and SLA performance during adverse conditions as core diligence items rather than assumed capabilities, and should ask providers for evidence, not assurances, of both.

The future direction of the MDR/MXDR market

The clearest trajectory is toward genuinely agentic security operations, where AI does not just accelerate triage but takes on structured investigation work under governed autonomy. Providers describe evolving from disparate, single-purpose agents toward interoperable, multiagent ecosystems that can hand off work between specialized functions, hypothesis generation, evidence gathering, correlation, and response recommendation, without losing context along the way. The direction is also toward reshaping the human side of delivery in parallel, with senior analysts increasingly repositioned toward threat hunting, forensics, and validating AI output rather than manually triaging volume. Enterprise buyers should expect this to translate into faster mean time to decision on routine incidents within the next two years, but the more important shift will be governance maturity keeping pace with autonomy, since a large enterprise environment cannot tolerate automated response actions without a clear, auditable escalation path. The providers building explainability and human-in-the-loop (HITL) checkpoints into their road map now, rather than treating them as an afterthought, are the ones likely to be trusted with expanded autonomous scope first.

Detection engineering is heading toward a similar inflection point. The stated direction across the road maps is continued growth of proprietary, behavior-based detection content, deeper multi-domain correlation spanning identity, cloud, SaaS, and OT, and a deliberate reduction in dependence on OEM-native detection logic. Over the next two years, this should translate into meaningfully better coverage for the kind of heterogeneous, multicloud, multi-acquisition environments that large enterprises run, rather than detection tuned primarily for a single vendor’s reference architecture. Buyers should also expect detection engineering to become increasingly AI-assisted, with GenAI accelerating rule creation, gap analysis, and tuning cycles that previously required large dedicated engineering teams. The practical benefit for enterprise buyers is a shorter lag between a new attacker technique emerging and a corresponding detection reaching production, which has historically been one of the weaker points in managed detection economics.

On triage quality specifically, the road maps point toward layered automation architectures that route alerts through a decision hierarchy, with high-confidence, low-risk determinations handled autonomously and novel or ambiguous cases escalated to human judgment while preserving full context. This is where the most enterprise-relevant improvement is likely to land over the next 18 months, since large organizations generate alert volumes that already exceed what human-only triage can sustain. The direction of travel suggests noise reduction and false-positive suppression will continue to improve despite recent increases in false positives due to conservative AI agent tuning. These investments will free analyst capacity for the harder investigative work, but buyers should watch closely to ensure autonomy expands in step with demonstrated accuracy rather than ahead of it.

Perhaps the most consequential shift for enterprise buyers is in outcome measurement and commercial accountability. The road maps consistently describe moving beyond time-based metrics such as mean time to detect (MTTD) and mean time to respond (MTTR) toward outcome-oriented measures such as containment precision, decision quality, and measurable risk reduction, metrics that map far more directly onto what a board or risk committee wants to hear. Alongside this, financially backed guarantees and service credit models tied to these outcomes are expected to become more common and standardized over the next two years, moving from a differentiator offered by a handful of providers toward something closer to a baseline expectation across the market.

Taken together, the direction for enterprise buyers is encouraging but not yet fully realized. IDC recognized that the gap between an autonomous, outcome-accountable MDR service and today's still-maturing capability is closing, and buyers negotiating multiyear contracts now should build in checkpoints, whether through contract renewal terms, capability audits, or advisory board participation, that let them capture these improvements as they land rather than locking into today's baseline for the life of the agreement.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the 2026 worldwide MDR service provider for the enterprise IDC MarketScape, providers had to meet the following criteria:

- Portfolio of MDR services: The security service provider must offer managed service for threat detection and response (TDR). These could include any or all of the following:
  - Pure-play MDR/MxDR
  - Managed EDR
  - Managed threat hunting
  - Managed SIEM
- At least US$45 million in global MDR revenue must be generated in 2025.

- At least 50% of total MDR revenue is derived from enterprise customers. For the purpose of this study, IDC defines an enterprise-sized organization as one with more than 2000 full-time employees.
- MDR service must have been generally available to customers in 2024 or earlier.
- Active MDR customers must be present in at least two of the four global regions (North America, EMEA, APAC, LATAM).

ADVICE FOR TECHNOLOGY BUYERS

Assessing the current capabilities and strategic alignment of an MDR service provider with your IT and business needs can be a lengthy process, and the calculus for a large or enterprise organization differs meaningfully from what a smaller buyer should weigh. IDC advises enterprise organizations that want to buy MDR or MXDR services to consider the following factors:

- **Understand where each provider sits on the spectrum between agentic autonomy and HITL control, and match that posture to your risk tolerance.** Providers in this market range from those pushing toward highly autonomous investigation and response, where AI agents independently gather evidence, form hypotheses, and in some cases execute containment actions such as endpoint isolation or credential revocation, to those that maintain a deliberate human checkpoint before any response action touches a production system. Heavy agentic reliance can meaningfully compress response times and absorb alert volume that would otherwise overwhelm human analysts, which matters at enterprise scale. It also introduces a different risk profile, since an autonomous action taken incorrectly across a large, interconnected enterprise environment can cause operational disruption well beyond the scope of the original alert. Enterprise buyers should ask each provider exactly which response actions are fully autonomous today, which require human sign-off, and how that boundary is governed and audited, rather than accepting a general claim of agentic capability. Organizations with complex, safety-sensitive, or highly interdependent environments should weigh demonstrated human validation discipline as heavily as automation speed, while organizations most constrained by analyst bandwidth may reasonably accept a higher degree of autonomy in exchange for faster containment.
- **Separate what your organization needs today from what a global, multiyear contract will require in 24 months.** Enterprise contracts run longer and involve more stakeholders than midmarket agreements, which makes road map durability a bigger risk factor. Ask each shortlisted provider precisely which agentic AI, exposure management, and detection engineering enhancements are contractually committed for your environment versus aspirational, and whether capability upgrades roll out automatically to existing enterprise accounts or require a renegotiation. A provider

whose road map depends heavily on features still in design risks leaving a multiyear enterprise commitment underwhelming well before renewal.

- **Treat regional and sovereign delivery consistency as a first-order evaluation criterion.** Enterprise buyers with multinational operations should not assume that service quality, staffing depth, or SLA attainment is uniform across every region a provider claims to cover. Providers vary in how far along they are in building genuine in-region SOC capacity, sovereign data processing, and local-language analyst coverage versus operating a thin regional presence layered on a centralized delivery model. Ask for region-specific SLA attainment data, not global averages, and pressure test how each provider's delivery model performed during a recent period of regional stress.
- **Demand specificity on detection and response metrics, including how automation is measured.** Enterprise buyers should push past MTTD and MTTR and ask how each provider defines newer outcome metrics such as containment precision, automated disposition accuracy, and the proportion of alerts resolved without human intervention. Confirm whether these figures are measured consistently across the provider's full global operation or only in reference accounts. Before comparing metrics across providers, require each vendor to define their measurement methodology precisely. Providers with mature metrics programs should be able to explain their measurement methodology, including where automation begins and where human validation resumes, without hesitation.
- **Evaluate financial accountability mechanisms at the scale your organization operates.** Enterprise buyers should examine whether financially backed guarantees, service credits, and breach warranties are structured to scale with enterprise-sized environments and multiyear total contract value, not capped at levels designed for smaller customers. Ask whether guarantees are standardized globally or vary by region, how incident response costs interact with warranty caps, and request evidence of compensation actually paid to comparable enterprise customers in prior periods. Clarifying these measures is best done prior to seeking compensation when needed.
- **Assess the customer portal as an integration layer into your existing security operations, not a standalone dashboard.** For enterprise buyers who typically maintain an internal SOC, security engineering function, or global risk team, the portal needs to function as an extension of existing tooling rather than another isolated system that analysts must check separately. Look for API-first architectures, support for natural language investigation queries, and the ability to feed provider findings directly into your own SIEM, SOAR, and case management systems, along with governance controls that support multiple business units and regional entities operating under one master agreement. Portals should be able to display views based on the persona interacting with it.

- **Insist on a genuine co-management and federation model rather than a binary fully managed relationship.** Nearly every enterprise organization retains some internal security capability, whether a regional SOC, a threat-hunting team, or an internal incident response function. The right provider should offer a formal RACI structure that precisely defines which actions it takes autonomously, which require your authorization, and which your internal teams retain, along with shared investigation workbenches that let your analysts and the providers' work the same case simultaneously rather than through a one-way reporting relationship.
- **Evaluate whether the provider can sustain your organization's scale and complexity as a durable strategic priority, not a stretch engagement.** Enterprise buyers should look past current capability claims and assess whether the provider is investing in detection engineering head count, sovereign delivery expansion, and vertical-specific content needed to remain credible at enterprise scale over a multiyear term. A provider whose enterprise business represents a small fraction of its overall book, or whose investment road map is oriented primarily toward smaller customers, carries higher execution risk for a large, complex account.
- **Plan implementation around organizational complexity, not just technical integration.** Enterprise onboarding typically spans multiple business units, legal entities, and regulatory jurisdictions, each with its own data residency and change management requirements. Develop a phased onboarding plan, confirm the provider's experience with staged, multi-entity rollouts rather than single-environment activations, and request reference customers with comparable organizational complexity and global footprint, not simply comparable size.

VENDOR SUMMARY PROFILES

This section briefly 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 opportunities.

Accenture

Accenture is positioned in the Leaders category in the IDC MarketScape: Worldwide MDR/MXDR Services for the Enterprise 2026 Vendor Assessment.

Accenture Adaptive MxDR framework delivers flexible, outcome-based security operations meeting clients at their maturity level while building road maps for continuous improvement. This positions MxDR as a core component within an integrated cybersecurity portfolio orchestrated through the Cyber.AI platform, unifying operational intelligence, automation, and AI across detection and response. 22 Cyber Fusion Centers service more than 120 countries. Accenture brings enterprise scale with deep industry specialization across aviation, healthcare, critical infrastructure, and financial services, reinforced by strategic partnerships with Google, Microsoft, and CrowdStrike.

Core MDR capabilities

- **Adaptive MxDR: Technology-agnostic platform integration.** At the heart of Accenture's offering lies a dual-model architecture. Full-stack MxDR provides a complete managed platform (Accenture-owned SIEM, SOAR detection content) for turnkey operations. Hybrid MxDR supports customer-owned infrastructure across Google SecOps, Microsoft Sentinel, CrowdStrike, Splunk, and other platforms. Both services leverage MxDR-Play, a proprietary integration layer orchestrating case management, automation, threat intelligence, and AI enrichment. This ensures clients retain platform ownership while accessing the Industry Content Library (hundreds of prebuilt use cases, playbooks, detection rules by industry and vendor) and Content Factory (over 100 engineers delivering rapid customization).
- **AI-augmented operations with layered intelligence.** Accenture's AI strategy prioritizes amplifying analyst talent over wholesale replacement, integrating ML (Arcanna for alert scoring), GenAI assistants, and agentic AI with human oversight. This multi-layered approach powers incident reporting, malware explainability, detection testing, and real-time translation across eight languages. The MxDR Threat Intelligence Bundle combines action-driven IOC feeds, risk-based engineering, SIEM/SOAR integration, and continuous updates. Proactive hunting incorporates AI-refined queries, with findings fed back into detection engineering.

- **Unified portal with transparent SLAs.** Client visibility is a key principle that drives their portal strategy. The Cyber Provisioning Portal and MxDR Portal deliver unified views into security posture, case management, real-time analytics, MITRE ATT&CK coverage, and data optimization. Features include role-based pages, 24 x 7 chat, live MTTX metrics, query builder, multi-language reporting, and ITSM integration. Granular SLAs extend beyond typical commitments: immediate triage for critical alerts, sub-10-minute detection, defined containment windows, and 99.9% availability.
- **Global delivery with local presence.** Accenture's "Glocal" model resolves the tension between standardization and localization. Twenty-two Cyber Fusion Centers (expanded to 30 locations through March 2026 CyberCX acquisition) deliver 24 x 7 coverage addressing sovereignty, compliance, and language needs across more than 11 spoken languages. This footprint spans Malaga, Chennai, Stockholm, Herndon, Paris, Cheltenham, Naples, Tokyo, Mexico City, San Antonio, Bangalore, Manila, and Sydney. The model combines standardized quality frameworks with localized proximity, supported by over 4,000 detection and response professionals.
- **Industry specialization and transformation outcomes.** Vertical depth distinguishes Accenture's approach. MxDR for Aviation (launched 2025) addresses ecosystem complexity spanning airport operations, aircraft maintenance, and air traffic management across IT, OT, 5G, and legacy stacks. Client outcomes validate this model: a Middle East country cybersecurity agency SOC (65 entities, 58% automation, 72–86% MTTR reduction), a global oil and gas company Autonomous SOC (20–86% automation across IT+OT+5G), and an aviation industry supplier ($1 million annual savings, enabling resale to ~50 airlines) were noted examples in a briefing to IDC. These reflect Accenture's focus on tailored 6-12-18-month transformation road map journeys.

Strengths

- **Technology partnership depth and operational AI maturity.** Accenture's partnerships run deeper than typical vendor alliances. With more than 8,000 Google Cloud professionals, over 37,000 Microsoft Azure certifications, and more than 3,300 Splunk practitioners, the company operationalizes platforms at architectural depth. This enables the Operational AI model to augment client platforms regardless of technology, while MxDR-Play permits seamless migration. Proprietary AI assets that are named after prominent Accenture associates, such as Sossio-Agent, (providing 24 x 7 KPI optimization) and detection coach, showcase their agentic AI technology capabilities.
- **Sovereign and critical infrastructure delivery at scale.** Federated sovereign cybersecurity capabilities are increasingly important. Two examples highlight their capabilities:

- A Middle East country cybersecurity agency SOC protects organizations while executing a five-year localization to 50% nationals.
- A global oil and gas company's autonomous SOC spans IT, OT, and 5G environments.

Both required in-country residency, defense clearances, consortium models, and multiyear commitments beyond typical MDR. Resilience was proven when one of the clients sustained 58% automation processing 16,606 incidents monthly during the Iran tensions.

- **Industry content engineering as intellectual property (IP).** The Industry Content Library and Content Factory represent IP differentiation beyond consultant expertise. Organized by industry, vendor platform, and threat category, this repository, maintained by over 2,000 cyber SMEs and more than 100 engineers, enables faster onboarding and vertical-aligned protection that reflects industry-specific threat patterns. MxDR for Aviation exemplifies this depth, addressing supply chain and airport operations challenges that horizontal MDR cannot replicate.
- **Outcome-based commercial flexibility.** Commercial relationships focus on maturity and transformation outcomes. This manifests in outcome-based SLAs (90% threat reduction for a multinational beverage company), flexible pricing (ingestion-based, outcome-based, chargebacks), and systematic improvement via the Sossio-Agent. Cost transparency tools position Accenture as a partner evolving pricing with client needs.

Challenges

- **Consultative complexity for midmarket buyers.** The transformation orientation and flexibility that benefit large enterprises can extend sales cycles for midmarket organizations seeking standardized procurement. Accenture's approach is to tailor scope, SLAs, delivery models, and resources rather than offer packaged tiers. While suiting complex enterprises, buyers seeking faster contracting may encounter longer evaluations. A heavy emphasis on road mapping and transformation can position MDR as a managed service wrapped in advisory. Accenture recently announced Accenture Edge to serve the midmarket, reflecting a more targeted approach and right-sized solutions for these buyers. Accenture does not provide financial loss guarantees.
- **Governance challenges with the Glocal delivery model.** Accenture's larger clients have appreciated the Glocal model for its flexibility and reduced friction across time zones, among other strengths. IDC notes that this creates for delivery consistency challenges, particularly for clients requiring uniform SLA enforcement, standardized detection engineering, and consistent analyst quality across multiple geographies simultaneously.

Accenture's continued success with the Glocal delivery model will require them to invest in significant governance overhead to maintain quality parity across centers that may vary in maturity, language capability, or technology specialization.

Consider Accenture when

Clients operate heterogeneous multivendor environments and prioritize platform-agnostic delivery with deep vendor partnerships, including flexibility to migrate platforms mid-contract via MxDR-Play.

Sovereignty mandates, defense clearances, or critical infrastructure sensitivity demand flexible delivery with global, regional, and national SOC options, in-country residency, and local language support across EMEA, APAC, and the Middle East.

Organizations value outcome-based commercial models with transparent metrics tied to operational penalties and optimization tooling, seeking partners who design pricing and service levels around maturity stages and transformation 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 go-to-market (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 in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behaviors, and capabilities.

Market definition

Managed detection and response (MDR), as a subset of managed security services (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.

LEARN MORE

Related research

- *Digital Sovereignty: Ramifications for Cybersecurity Capabilities and Practices in a Hostile World* (IDC #US54542526, May 2026)
- *The Essence of the RSAC Conference 2026 for the MDR Market* (IDC #IcUS54480326, April 2026)
- *IDC's Worldwide Security Services Taxonomy, 2026* (IDC #US53982726, March 2026)
- *Market Analysis Perspective: Worldwide MDR and Managed Security Services, 2025* (IDC #US53101725, November 2025)
- *Worldwide Managed Security Services Forecast, 2025–2029* (IDC #US53101826, September 2025)
- *Worldwide Managed Security Services Market Shares, 2024: Opportunity for All, in All Managed Security Areas* (IDC #US53101625, September 2025)

Synopsis

This IDC MarketScape presents a vendor assessment of managed detection and response (MDR) and managed extended detection and response (MXDR) service providers worldwide through the IDC MarketScape model. For this study, IDC evaluated a group of 20 MDR/MXDR service providers with operations and customers worldwide, with a deliberate focus on the needs of enterprise organizations. All providers evaluated in this study participated through a structured request for information process, including provider briefings and customer references. Providers were measured in terms of current capabilities

and future strategies for delivering MDR/MXDR services to enterprise customers worldwide. As noted in the inclusion criteria, all providers evaluated in this study have the organizational scale, technical depth, and service breadth to serve large, complex, and often multinational enterprise environments.

Craig Robinson, Research vice president, Security Services, says, “The enterprise MDR/MXDR market has entered a new phase of maturity, one defined less by whether providers can deliver effective detection and more by how they govern the AI doing the detecting and where they can deliver it from. This study reveals a market where agentic AI architecture, human governance discipline, and sovereign delivery footprint have become the primary axes of differentiation. MDR/MXDR remains one of the most compelling security investments available to enterprise organizations, offering access to SOC capabilities, threat intelligence programs, and incident response expertise operating at a scale most enterprises cannot replicate internally. But the gap between leaders and the broader field is widening, and buyers who treat MDR/MXDR as a commodity purchase will increasingly find that the details of how a service is automated, governed, and delivered determine whether it meets their risk tolerance.”

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider 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 and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com