IDC MarketScape

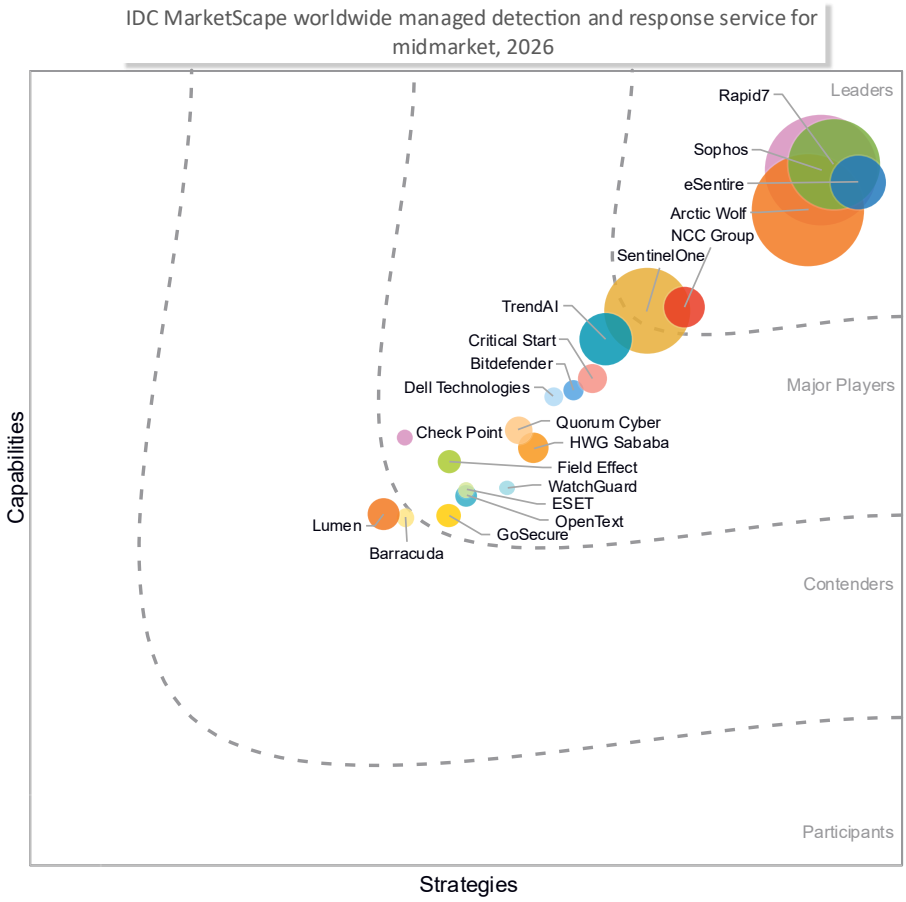
IDC MarketScape: Worldwide Managed Detection and Response Service for Midmarket 2026 Vendor Assessment

Yogesh Shivhare

THIS EXCERPT FEATURED HWG SABABA AS A MAJOR PLAYER IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape worldwide managed detection and response service for midmarket vendor assessment



Source: IDC, 2026

July 2026, IDC #US52992326e

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: Worldwide Managed Detection and Response Service for Midmarket 2026 Vendor Assessment (Doc # US52992326).

IDC OPINION

The managed detection and response (MDR) market is undergoing a structural transformation that goes well beyond incremental capability improvements. IDC's evaluation of MDR vendors for this study, conducted with a deliberate focus on the needs of midmarket organizations, reveals a market at an inflection point: one where the architectural decisions vendors are making today about artificial intelligence (AI) will define competitive positions for the next several years. The question is no longer whether AI belongs in a SOC. It is whether AI is bolted on to an existing service model or built into its foundation.

IDC observes a clear divergence in how vendors are approaching AI integration. A leading group of providers has moved beyond using AI for alert triage and noise reduction, which has become table stakes, and has deployed agentic AI architectures in which purpose-built AI agents autonomously conduct investigation, evidence collection, and response orchestration, with human analysts validating outcomes rather than performing them from scratch. These architectures are not experimental. Several providers evaluated in this study have agentic AI operating in production across their full customer base, completing end-to-end investigations at machine speed and generating complete audit trails of every action taken. Providers that remain in an AI-augmented human model, where analysts drive investigation with AI-generated suggestions, are already operating at a structural efficiency disadvantage relative to this leading group. IDC expects the gap to widen materially over the next 18 to 24 months as agentic capabilities mature and scale.

The midmarket, in particular, stands to benefit from this shift. Organizations in the 1- to 2,000-employee range typically lack the internal security head count to absorb meaningful analyst workloads, making the efficiency gains from agentic AI directly translatable into faster response, broader coverage, and lower effective cost per protected asset. MDR providers that can demonstrate measurable outcomes at scale, not just describe their AI architecture in marketing terms, will find strong receptivity among midmarket buyers that have budget constraints but with no tolerance for slow response to confirmed threats. IDC encourages midmarket organizations to ask vendors for specific AI outcome metrics rather than capability descriptions, a distinction that this study found to be a meaningful signal of operational maturity.

Financial accountability has emerged as a second major differentiator, and its evolution has been rapid. The market has shifted from a posture of contractual service-level agreements (SLAs) with response time commitments to one where leading vendors now back outcomes with financial breach warranties of up to $3 million. This warranty arms race reflects growing vendor confidence in their detection and response capabilities, but it also reflects pressure from the cyberinsurance ecosystem, where insurers and insureds alike are looking for managed security service providers that can translate service commitments into quantified risk reduction. IDC found meaningful variation in how vendors structure these commitments: the stronger providers tie warranty coverage to specific coverage requirements, include incident response costs outside of the warranty cap, and back obligations from their own corporate balance sheet rather than through third-party underwriters alone. Buyers should treat the structure of warranty commitments as a window into how a vendor thinks about accountability, not just as a marketing differentiator.

A third force reshaping the MDR market is the convergence of continuous threat exposure management with detection and response operations. Historically, MDR was a reactive service augmented by proactive threat hunting. IDC now observes leading providers integrating vulnerability intelligence, attack surface data, and asset criticality context directly into the investigation workflow, so that when a threat is detected, the SOC analyst already understands the exposure context around the affected asset before the first keystroke. This integration produces faster and more accurate severity assessments, reduces unnecessary escalations, and enables providers to offer something closer to continuous risk reduction rather than incident response. For midmarket organizations that often lack dedicated vulnerability management programs, providers that embed this capability within MDR are effectively delivering two programs in one.

Threat intelligence (TI) remains a foundational differentiator, but IDC's evaluation reveals a widening gap between vendors that produce genuinely proprietary intelligence and those that aggregate commercial feeds. Vendors with the most defensible intelligence positions in this study share three characteristics: large dedicated in-house research teams, active relationships with law enforcement and national cyberagencies, and unique collection infrastructure, such as honeypot networks, backbone-level network telemetry, or vulnerability disclosure programs, that generate intelligence unavailable through any commercial subscription. For midmarket buyers, the practical implication is that the richness of a provider's threat intelligence directly affects the quality of the detections that protect them. Intelligence sourced exclusively from third-party platforms is available to every provider and to their adversaries. Intelligence sourced from unique collection infrastructure is structurally differentiated.

Finally, IDC notes that service structure and financial accountability mechanisms have become as analytically important as technical capabilities in evaluating MDR providers. The vendors that performed most strongly in this study are not uniformly those with the largest

research organizations or the most advanced AI. They are the ones that have thought carefully about how their service model maps to customer outcomes: clear tier differentiation that explains what changes between levels of service rather than just what is named, response authority frameworks that give the SOC the latitude to act without requiring customer approval at every step, and transparent metrics that allow buyers to hold providers accountable for the outcomes they promise. As the MDR market continues to mature, IDC expects buyer sophistication to accelerate alongside it, and providers that have built accountability into their operational model will be structurally better positioned than those that have treated it as a sales conversation.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

- The security service provider (SP) must offer managed service for threat detection and response; these could include any or all the following:
  - Pure-play MDR/MxDR
  - Managed EDR
  - Managed threat hunting
  - Managed SIEM
- At least $5 million in global MDR revenue in 2024 from midmarket customers (For the purpose of this study, IDC defines a midmarket organization as one with fewer than 2,000 full-time employees.)
- Minimum of 200 active midmarket MDR customers by the end of 2024
- At least 50% of total MDR revenue derived from midmarket customers
- MDR service must have been generally available to customers in 2024 or earlier
- Active MDR customers in at least two of the four global regions (North America, EMEA, APAC, LATAM)

The revenue threshold used for inclusion in this study was finalized in 4Q25, at which point full-year 2025 revenue figures were not yet available for the majority of participants. As a result, 2024 reported revenue was used as the basis for applying the inclusion criteria. It is important to note that the evaluation of vendor capabilities and strategies, as well as the bubble sizes reflected in the MarketScape graphic, are based on 2025 figures and information gathered through the study's active research period. The use of 2024 revenue was strictly limited to determining eligibility for inclusion in the study and had no bearing on any vendor's scoring, positioning, or bubble size representation within the IDC MarketScape.

While this study was conducted with a deliberate focus on the needs of midmarket organizations, IDC recognizes that every provider evaluated in this IDC MarketScape has the organizational scale, technical depth, and service breadth to serve large enterprise customers. The midmarket lens reflects the study's evaluative emphasis, not a ceiling on any participant's capabilities or addressable market. Several providers in this study count among their customers some of the largest and most security-mature organizations in the world, and a number of these providers operate global SOCs, maintain extensive compliance and regulatory certifications, and offer service tiers, comanagement models, and contractual frameworks specifically designed for enterprise-scale deployments. Buyers from larger organizations reading this document should feel confident that the providers evaluated here are well equipped to meet enterprise requirements and are encouraged to engage directly with vendors to understand how their offerings scale to their specific environment and organizational complexity.

ADVICE FOR TECHNOLOGY BUYERS

Assessing the current capabilities and strategic alignment of an MDR service provider to your IT and business needs can be a lengthy process. IDC advises organizations that want to buy MDR services to consider the following factors:

- **Understand the architectural trade-off before you short list.** Platform-native providers, those that deliver MDR through a platform you are already running or will adopt, offer faster activation, tighter telemetry integration, and lower initial complexity. Open architecture providers ingest from your existing security stack regardless of vendor, preserving prior investments and providing broader coverage potential, but require an integration and baselining period before the service reaches full effectiveness. Neither model is universally superior. The right answer depends on how homogeneous your environment is, how quickly you need protection in place, and whether your environment is likely to change significantly over the contract term.
- **Separate what you need now from what you will need in 24 months.** MDR providers vary enormously in how their service evolves over the contract life cycle. Some offer a largely static service with incremental improvements; others are actively integrating exposure management, agentic AI investigation, and proactive risk quantification into the base MDR offering on a rolling basis. Ask providers specifically what capabilities are on the road map, which capabilities are contractually committed versus aspirational, and how capability improvements are delivered to existing customers versus new ones. A provider with strong current capability but a weak strategic road map may look attractive at signing and underwhelming at renewal.
- **Treat threat intelligence as a first-order evaluation criterion, not a background capability.** There is a significant gap between providers that generate genuinely proprietary threat intelligence through dedicated research teams, unique collection

infrastructure, and active law enforcement partnerships, and those that aggregate commercial threat feeds. Intelligence sourced exclusively from commercial platforms is available to every provider simultaneously and offers no detection advantage. Intelligence produced from proprietary sources, including backbone-level network telemetry, global honeypot networks, or large-scale vulnerability research programs, provides pre-commercial visibility into attacker infrastructure and emerging tradecraft. Midmarket organizations are frequently targeted precisely because adversaries perceive them as less defended and benefit disproportionately from providers with strong proprietary TI depth.

- **Demand specificity on detection and response metrics, and on how those metrics are defined.** There is wide variation not just in the numbers vendors report but in how they define the underlying measurements. Mean time to detect means different things depending on whether the clock starts at event occurrence, at log ingestion, or at the first analyst action. Mean time to contain means different things depending on whether it measures the first response action taken or confirmed containment on the first affected host. Before comparing metrics across providers, require each vendor to define its measurement methodology precisely. Providers with mature metrics programs will answer this without hesitation.
- **Evaluate financial accountability mechanisms as seriously as technical capabilities.** The MDR market has moved toward financial warranties and penalty-backed service-level agreements, and the structure of these commitments varies significantly across providers. The most accountable frameworks combine contractual response time SLAs with financial penalties for nonperformance and breach warranties that compensate customers for losses arising from incidents occurring under the provider's watch. Examine whether incident response costs are included within or separate from warranty caps, whether coverage requires specific configuration prerequisites that may be difficult to maintain, and how claims are actually processed and paid. Transparency around compensation paid to customers in prior periods is a meaningful signal of operational accountability.
- **Assess the customer portal as a strategic asset, not a reporting dashboard.** MDR can be an opaque service: activity happens in a provider's SOC, and customers often have limited visibility into what is being done on their behalf and why. There is a clear divide between providers whose portals deliver genuine investigative capability, including natural language query against security data, AI-generated investigation summaries, shared forensic tooling, and exposure-aware risk context, and those whose portals remain primarily alert notification interfaces. For midmarket organizations where security staff may double as IT generalists, a portal that translates SOC findings into plain language, actionable outputs is a practical prerequisite for deriving full value from the service.

- **Consider comanagement maturity if your organization has any internal security capability.** Many organizations with up to 2,000 employees have at least some internal security practitioners, whether a dedicated analyst, a security-aware IT manager, or a virtual CISO. For these organizations, a fully managed model that treats the customer as a passive recipient may not be the right fit. The most mature comanagement offerings include shared investigation workbenches, role-based response authority frameworks, and formal RACI structures that define precisely which actions the provider takes autonomously, which actions require customer authorization, and which action the customer handles independently.
- **Evaluate the provider's commitment to MDR as a primary business.** This study includes providers ranging from pure-play MDR companies for whom MDR is the only business to large, diversified technology vendors for whom MDR is one service line among many. A provider for whom MDR represents the majority of revenue has structural incentives to invest in detection engineering, threat intelligence, and SOC capability that a provider treating MDR as a portfolio add-on does not. Midmarket buyers entering multiyear contracts should satisfy themselves that the provider's organizational commitment to MDR is durable, not contingent on portfolio priorities that may shift.
- **Plan carefully for implementation and integration.** Develop a clear plan for onboarding MDR services, including integration with existing security tools and platforms, and ensure the provider can support your specific implementation timeline and environment. Time to value varies significantly across providers and is directly influenced by architectural model, onboarding automation maturity, and the complexity of your existing environment. Ask providers for reference customers with similar environment profiles to your own.

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 challenges.

HWG Sababa

HWG Sababa is positioned in the Major Players category in the 2026 IDC MarketScape for worldwide managed detection and response service for midmarket.

HWG Sababa is a privately held cybersecurity company headquartered in Verona, Italy, and backed by Investcorp Technology Partners. The company was formed through the merger of HWG and Sababa Security and has grown through four acquisitions since 2022, including the acquisition of Akito in February 2025, with further Southern European expansion in

progress. HWG Sababa operates as a pure-play cybersecurity services company across more than 20 countries, with its portfolio organized around managed security services; cyberthreat intelligence; governance, risk, and compliance advisory; and professional security services. MDR is delivered as the company's primary managed service and sits at the center of its service portfolio. Security operations are delivered through a multiregional SOC model supporting customers primarily across Europe, the Middle East, and Central Asia, with service delivery in Italian, English, and Arabic, and Spanish and Portuguese language capability in development as the company expands its Southern European footprint.

HWG Sababa's MDR service — HyperSOC — is built on the PULSE platform, a proprietary security operations platform developed over 15 years of SOC operations that embeds a validated knowledge base of playbooks, use cases, detection rules, and technology integrations. The PULSE platform is technology agnostic, supporting coexistence with customers' existing security investments without requiring technology replacement while also enabling delivery of a full-stack security architecture for organizations that prefer a more comprehensively managed approach. The platform hosts more than 250 use cases and playbooks developed from the company's accumulated operational experience across critical infrastructure, banking, energy, defense, and industrial environments. Hyperautomation is integrated into the platform through a dedicated automation framework that orchestrates detection, investigation, and response workflows across the customer's IT and security stack, enabling rapid containment actions and consistent process execution across heterogeneous technology environments.

HWG Sababa structures its MDR offering into four tiers — Essential, Advanced, Advanced+, and Ultimate — while also providing customized service bundles tailored to specific customer requirements. Tier differentiation is driven by the depth of proactive services, threat intelligence integration, and comanagement engagement included at each level, with higher tiers providing access to dedicated threat intelligence operations, more granular SLA commitments, and deeper comanagement arrangements. A RACI-based comanagement model is available for organizations seeking to retain active internal SOC involvement alongside HWG Sababa's managed operations, providing a structured framework for shared responsibility. The company's SLA framework includes financial penalty provisions, with commitments covering time to acknowledge and investigation timelines segmented by alert priority level.

A defining characteristic of HWG Sababa's service model is its depth of operational technology and industrial control systems security capability. The company has invested in specialized OT and ICS monitoring capabilities, including support for industrial communication protocols, OT-aware detection logic and playbooks, and integrated IT-OT threat correlation. This positions HWG Sababa as a provider capable of managing security across converged IT and OT environments, a requirement that is increasingly prevalent in

energy, utilities, manufacturing, and critical infrastructure sectors where IT-OT convergence has expanded the attack surface beyond what traditional MDR services address. A dedicated OT HyperSOC capability is on the company's road map, designed to provide a purpose-built MDR environment for industrial and critical infrastructure customers with specialized telemetry ingestion and OT-specific response actions.

HWG Sababa's threat intelligence operations are conducted by a dedicated cyberthreat intelligence function staffed by specialists with backgrounds in defense, critical infrastructure protection, and advanced threat actor tracking. CTI is operationalized directly into MDR detection engineering, hunting hypothesis development, and customer advisory outputs. The company's Enforcement Measures heatmap is a customer-facing reporting construct that visualizes security posture improvement against a baseline of best practices accumulated over more than 15 years of SOC operations, providing customers with a longitudinal view of their security program's maturity progression.

AI investment within HWG Sababa is currently centered on the systematic adoption of AI to augment detection engineering, alert triage, investigation workflows, and response decision support, under the company's Applied AI for MDR initiative. The intent is to improve detection scalability, reduce false positive rates, and accelerate analyst workflows while maintaining human-validated detection outcomes. The hyperautomation framework already in production provides the orchestration foundation on which AI augmentation is being layered.

IDC sees HWG Sababa's investment priorities center on three areas. The OT HyperSOC expansion will formalize and scale its industrial security MDR capabilities into a dedicated service offering with specialized infrastructure, staffing, and go-to-market focus for critical infrastructure and industrial sectors. A dedicated defense, space and cyberthreat intelligence business unit is being developed to provide advanced threat actor tracking, early warning intelligence, and sector-specific detections for defense and space sector customers, reflecting the company's established relationships within these verticals. The third investment area is the continued development of applied AI capabilities across the MDR delivery pipeline, with a focus on detection automation and analyst augmentation that maintains accountability through human-validated outcomes.

Strengths

HWG Sababa's operational technology and ICS security capabilities, supported by specialized industrial protocol coverage and integrated IT-OT threat correlation, provide depth in converged industrial environments that extends beyond what most MDR providers can deliver through standard endpoint and network telemetry. For organizations in critical infrastructure, energy, manufacturing, and defense sectors, this represents a structurally relevant capability advantage.

HyperSOC leverages the PULSE platform's accumulated knowledge base of playbooks and use cases, built from 15 years of operational experience across complex and regulated environments, combined with a hyperautomation framework for orchestrated response execution, and provides a service delivery foundation that reflects operational maturity in sectors where standard MDR approaches are frequently insufficient.

Challenges

HWG Sababa's primary operational footprint is concentrated in Europe, the Middle East, and Central Asia, and the company's geographic coverage, language support, and regulatory compliance capabilities are most fully developed within these regions. Organizations with significant operational requirements outside EMEA, particularly in North American or Asia/Pacific markets, should assess current regional delivery capabilities against their specific coverage and data residency requirements.

HWG Sababa does not currently offer a financial breach warranty, and the company has not indicated plans to introduce insurance channel partnerships or warranty-backed outcome commitments in the near term. For organizations where warranty-backed managed security is a procurement consideration, this represents a gap relative to providers that have formalized financial guarantee frameworks.

Consider HWG Sababa when

Organizations in critical infrastructure, energy, defense, or industrial sectors, particularly those operating across converged IT and OT environments in European or Middle Eastern markets, seeking a managed security partner with deep sectoral expertise and specialized OT detection and response capabilities should evaluate HWG Sababa's HyperSOC MDR offering.

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 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, behavior, and capability.

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 Market Shares, 2024: Opportunity for All, in All Managed Security Areas* (IDC #US53101625, September 2025)

- *Worldwide Managed Security Services Forecast, 2025–2029* (IDC #US53101826, September 2025)

Synopsis

This IDC study presents a vendor assessment of MDR service providers worldwide through the IDC MarketScape model. For this study, IDC evaluated a group of MDR service providers with operations and customers worldwide, with a deliberate focus on the needs of midmarket organizations, which IDC defines for this study as organizations with up to 2,000 employees. Of the group of providers evaluated, the majority actively participated through a structured request for information process, with provider briefings and customer references, while two providers were assessed based on IDC's knowledge of their security services offerings and secondary research. Providers were measured in terms of current capabilities and future strategies for delivering MDR services to midmarket and 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 customers well beyond the midmarket segment.

Yogesh Shivhare, senior research manager, Security and Trust at IDC, says, "The managed detection and response market has entered a new phase of maturity, one defined less by whether providers can deliver effective threat detection and more by how they do it and what they stand behind. This study reveals a market where artificial intelligence architecture, financial accountability, and the depth of proprietary threat intelligence have become the primary axes of differentiation. MDR remains one of the most compelling security investments available to midmarket organizations, offering access to SOC capabilities, threat intelligence programs, and incident response expertise that would be prohibitively expensive to build internally. But the gap between leaders and the broader field is widening, and buyers that treat MDR as a commodity purchase will increasingly find that the details of how a service is structured, measured, and backed determine whether it delivers on its promise."

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

Copyright and trademark notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit idc.com/about/offices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.