IDC MarketScape

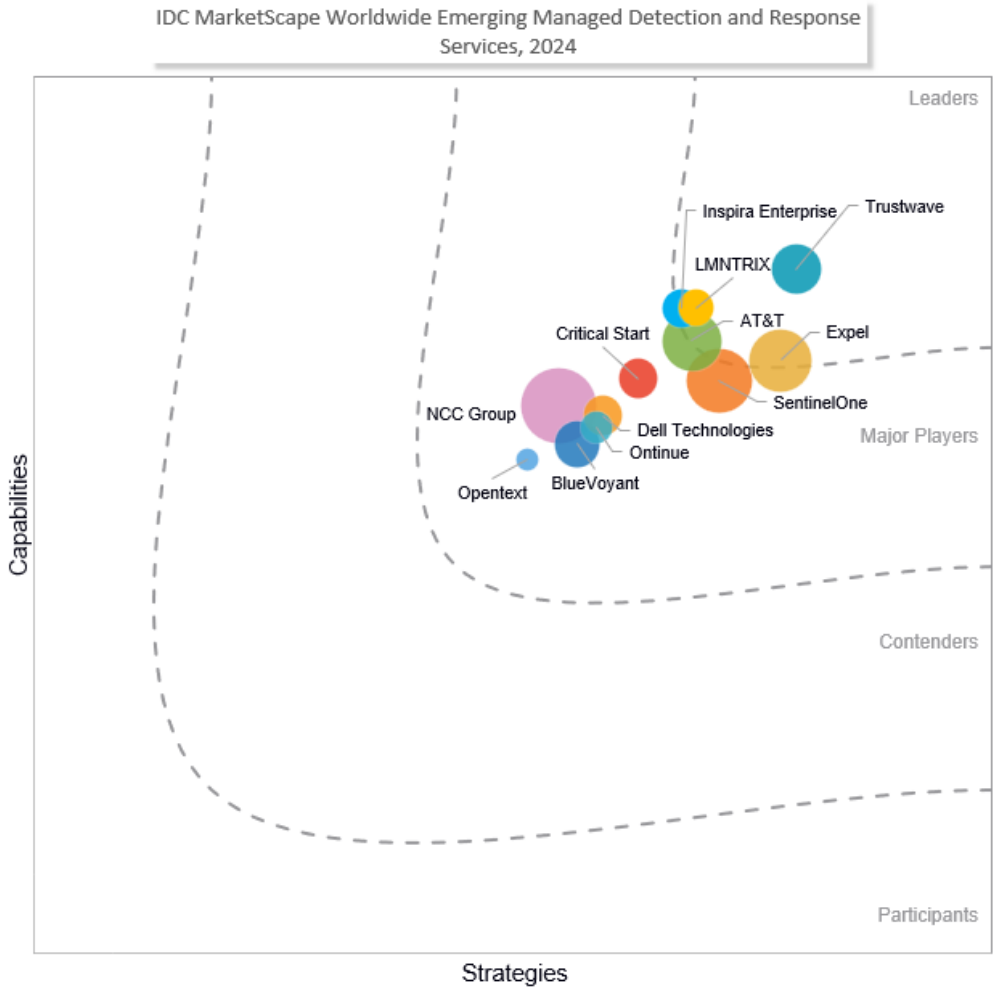
IDC MarketScape: Worldwide Emerging Managed Detection and Response Services 2024 Vendor Assessment

Yogesh Shivhare

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Emerging Managed Detection and Response Services Vendor Assessment



Source: IDC, 2024

April 2024, IDC #US50101523

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

IDC OPINION

Managed detection and response (MDR) services have experienced significant growth, fueled by the escalating sophistication and frequency of cyberthreats. Organizations are increasingly turning to MDR services to enhance their cybersecurity posture and effectively combat evolving cyber-risks.

One of the primary drivers behind the increasing adoption of managed detection and response services is their significantly shorter time to value compared with establishing an in-house security operations center (SOC). Setting up a SOC involves procuring underlying security technologies, hiring and training a specialized security team, and then gradually improving the SOC's efficiency over the years. However, this process is time-consuming and resource intensive. Security leaders are often faced with the pressing need for protection from advanced threats and require immediate solutions. MDR services offer a rapid and effective alternative, either as a dedicated cyberdefense capability or as an augmentation of existing SOC efforts, providing organizations with access to advanced threat detection and response capabilities without the need for extensive setup and investment. This enables security leaders to quickly enhance their cybersecurity postures and protect their organizations from evolving threats.

Other key drivers behind the rise of MDR services is their ability to leverage threat intelligence, artificial intelligence (AI), and machine learning (ML) technologies for threat hunting, anomaly detection, incident validation, and triage. Threat intelligence provides MDR services with valuable insights into the latest cyberthreats, enabling them to proactively detect and respond to emerging threats. By incorporating threat intelligence and proactive threat hunting into their operations, MDR providers can stay ahead of cybercriminals and better protect their clients' networks and data. AI and ML play a crucial role in enhancing the effectiveness of MDR services. These technologies enable MDR providers to analyze vast amounts of security data rapidly, identify patterns indicative of malicious activity, and respond to threats in real time and at scale. By automating routine tasks and augmenting human analysts' capabilities, AI/ML help MDR services improve detection accuracy and reduce response times.

Furthermore, MDR services help organizations address the challenges posed by the cybersecurity skills gap. By outsourcing threat detection and response to MDR providers, organizations can access a team of cybersecurity experts with specialized skills and knowledge. This allows organizations to enhance their security operations (SecOps) without the need to recruit and retain expensive cybersecurity talent in-house.

The differentiating factors for MDR service providers (SPs) can vary based on their specific offerings and focus areas. However, IDC believes some factors that will continue to differentiate MDR service providers are:

- **Advanced threat detection capabilities:** MDR providers differentiate themselves by offering advanced threat detection capabilities, such as behavior analytics, threat intelligence integration, and machine learning algorithms, to identify advanced and novel threats.

- **Proactive threat hunting:** MDR providers that excel in proactive threat hunting differentiate themselves by actively searching for and mitigating potential threats before they can cause damage, offering a higher level of protection to their clients.
- **Incident response (IR) and remediation:** The effectiveness and speed of incident response and remediation are key differentiators for MDR service providers. Providers that offer rapid and orchestrated cross-technology response and comprehensive remediation plans can better mitigate the impact of cyberattacks.
- **Integration and compatibility:** MDR providers that offer seamless integration with existing security infrastructure and compatibility with a wide range of security tools and platforms can provide a more holistic and effective security solution.
- **Threat intelligence and research:** MDR providers that invest in threat intelligence and conduct ongoing research to stay ahead of emerging threats can offer more proactive and effective threat detection and response services.
- **Scalability and flexibility:** MDR providers that offer scalable and flexible solutions, allowing organizations to easily adapt to changing security needs and requirements, are more attractive to organizations of all sizes.
- **Compliance and regulatory expertise:** MDR providers that have expertise in compliance and regulatory requirements, such as GDPR, HIPAA, and PCI DSS, can help organizations meet their compliance obligations.
- **Customer support and service-level agreements (SLAs):** MDR providers that offer responsive customer support and clearly defined SLAs for incident response and resolution differentiate themselves by providing a higher level of service and accountability.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this 2024 IDC MarketScape for worldwide emerging MDR services, providers had to meet the following criteria:

- **Portfolio of MDR services:** The security service provider must offer managed service for threat detection and response. These could include any or all the following:
  - Pure-play MDR/managed extended detection and response (MXDR)
  - Managed endpoint detection and response (EDR)
  - Managed threat hunting
  - Managed security information and event management (SIEM)
- **Revenue:** The worldwide MDR revenue of the service provider should be from $20 million to $60 million for the year 2021.
- **Multiregion footprint:** The MDR service provider should have customers in more than one region out of North America, LATAM, EMEA, and APAC.

ADVICE FOR TECHNOLOGY BUYERS

Assessing the many current capabilities and strategic alignment of a 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:

- **Define your requirements:** Clearly define your cybersecurity needs, including the level of threat detection and response capabilities required, compliance requirements, budget constraints, and scalability needs. Understand that MDR is not an all-or-nothing solution. Many organizations adopt a hybrid approach, integrating their in-house security operations team with an MDR partner, leverage MDR services for critical IT assets only, or use two different MDR providers for IT and operational technology (OT).
- **Evaluate provider capabilities:** When evaluating MDR providers, ensure they offer essential capabilities, including 24 x 7 threat detection and remote response beyond simple alerting. Look for a security platform operated by the provider, integrating the latest threat intelligence and enabling automated indicators of compromise (IoC)–based threat hunts. Ensure the provider offers tuning for threat detection content, playbooks, and integrations with third-party solutions, along with unlimited triage, investigations, and response. In addition, consider advanced capabilities such as enrichment with vulnerability or attack surface data, digital forensics and incident response (DFIR) for comprehensive IR life-cycle support, resiliency guidance for IT environment hardening, and hypothesis-driven proactive threat hunting for detecting unknown threats. These capabilities should be either included or available as add-ons.
- **Consider industry expertise:** Look for MDR providers with expertise in your industry, as they will be better equipped to understand your specific cybersecurity challenges and compliance requirements.
- **Review customer feedback:** Check customer reviews and references to gauge the MDR provider's reputation for service quality, responsiveness, and customer support.
- **Assess threat intelligence and research:** Evaluate the MDR provider's capabilities in threat intelligence and research to ensure they can stay ahead of emerging threats and provide timely protection.
- **Understand service-level agreements:** Review SLAs carefully to understand the provider's commitments regarding threat detection and response times, incident resolution, and service availability.
- **Consider customer service portals:** These portals offer more than just operational reporting, with features like interactive visuals, customizable dashboards, and audit report generation. They enhance transparency in MDR services, which can otherwise seem opaque. Leading providers are adding GenAI use cases to their portals, empowering customers to query their security data effectively. Buyers should consider the portal's capabilities when selecting an MDR service, as it greatly impacts the user experience and service effectiveness.
- **Evaluate cost and value:** Compare costs and value propositions of different MDR providers, considering factors such as pricing models, included services, and additional features. MDR is not a standard offering, and vendors have varying opinions on what should be a base offering and what should be an add-on.
- **Plan for implementation and integration:** Develop a plan for implementing MDR services, including integration with existing security tools and platforms, and ensure that the provider can support your implementation timeline.
- **Consider long-term partnerships:** MDR services are advancing beyond traditional threat detection and response, expanding to include broader aspects of threat prevention, risk management, and recovery. Some providers are integrating risk management services such as vulnerability management, breach attack simulation, and attack surface management to transform MDR into a comprehensive risk management offering. Others are moving toward post-incident recovery, providing a holistic managed detection, response, and recovery (MDRR) service. It's crucial for buyers to consider the long-term road map of the service when selecting an MDR provider.

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.

AT&T

AT&T is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Headquartered in Texas, United States, AT&T announced the general availability of its managed threat detection and response (MTDR) services in 2019. The company extends its services to both local and global clients, operating from 10 security operations centers/network operations centers (NOC) located worldwide. In a strategic move, in late 2023, AT&T disclosed plans to spin off its managed security business into a standalone entity, securing investment from WillJam Ventures.

AT&T's MTDR service is built on the foundation of its Unified Security Management (USM) platform. The USM platform consolidates essential security functionalities into a unified console, enabling early threat detection, reducing false positives, and facilitating rapid response times.

The MTDR service ensures continuous data collection across diverse environments, encompassing both cloud and on-premises assets. Offering centralized security monitoring for critical assets, the USM platform provides a comprehensive view of the security landscape, covering threat monitoring, cloud and network asset discovery, vulnerability assessment, user and asset configuration, and dark web monitoring. The platform's extensible architecture supports the integration of modular software components, known as AlienApps, enhancing security orchestration and automation capabilities. Currently, there are over 450 prebuilt AlienApps, offering out-of-the-box integration and enabling cross-technology automated responses across the network and endpoint.

Backing the MTDR service is AT&T Alien Labs, comprising a global team of threat researchers and data scientists. Their expertise, combined with proprietary technology in analytics and ML, analyzes vast collections of threat data from diverse open source and commercial threat intelligence (TI) feeds. Alien Labs also collects threat data from its Alien Labs Open Threat Exchange (OTX) platform, which supports an open threat intelligence sharing community of more than 450,000 members. Curated threat intelligence from AT&T Alien Labs is directly integrated into the USM Anywhere platform, enhancing threat detection and response for all MTDR clients. A dedicated proactive threat hunting team engages in hypothesis-based hunting across the entire customer base, with automated threat hunts sweeping customer environments as new threats are discovered.

AT&T's focus for future investment is on enhancing the capabilities of the USM platform and the MTDR service. This involves adding more integrations, particularly in cloud, identity, and mobile domains. Investments are also directed toward improving threat hunting capabilities with automation, aiming to enhance fidelity and accuracy. In addition, AT&T is exploring integrations across services, with a focus on its managed network security services, and AI/ML use cases to streamline onboarding processes, reducing the overall time to value for its clients.

Strengths

AT&T Cybersecurity has built a cybersecurity ecosystem of systems integrators and top security solutions vendors whose technology they integrate with USM Anywhere platform that benefits their customers through technology advancement and innovation, service delivery, and collaboration.

Furthermore, AT&T Alien Labs collaborates closely with the AT&T chief security office, providing it with visibility into threats observed on the AT&T IP network. This partnership enables the Alien Labs research team to gain valuable insights into emerging global threats, enhancing their ability to proactively address new and evolving cybersecurity challenges.

Challenges

AT&T has a strong presence in the United States but has limited reach in other regions.

The company's MDR service is tiered and priced based on ingest volume. However, customers have noted that the service tiers are significantly spaced apart, potentially leading to their usage falling between tiers. AT&T is actively working to introduce more service tiers soon to better accommodate varying customer needs and usage patterns.

Consider AT&T When

Midmarket organizations in North America across industry verticals should consider AT&T's managed threat detection and response services as their dedicated cyberdefense capability or as an add-on to their existing SOC efforts.

BlueVoyant

BlueVoyant is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

IDC notes that BlueVoyant did not actively participate in this IDC MarketScape, and its evaluation is based on IDC's knowledge of its MDR practice.

BlueVoyant, headquartered in New York, United States, has been offering MDR services globally since its establishment in 2017. The company operates with a team of analysts spread across different time zones to cater to clients worldwide.

BlueVoyant's comprehensive portfolio includes MDR, supply chain defense (SCD), and digital risk protection (DRP) services, complemented by a broad suite of professional security advisory and assessment services. Notably, the company's MDR services have been a core offering since the company's inception.

A distinctive feature of BlueVoyant's MDR is its strategic focus on Microsoft and Splunk environments. For Microsoft environments, the MDR service provides an integrated security solution that seamlessly works with Microsoft's suite of security tools, such as Azure Sentinel and Microsoft's Defender suite. This integration facilitates efficient threat detection and response within the Microsoft security ecosystem.

Similarly, for Splunk environments, BlueVoyant's MDR service ensures a high level of security coverage. Integrating with Splunk's security suite, including Splunk Enterprise Security and Splunk User Behavior Analytics, the MDR service enables effective detection and response to threats within the Splunk environment.

BlueVoyant's MDR services are designed to maximize the utility of clients' security stack. While clients retain ownership of licenses and host security solutions, BlueVoyant contributes its SOC capabilities for 24 x 7 monitoring, proactive threat hunting, and ongoing SIEM management and detection engineering. Notably, for clients utilizing MDR for Microsoft Defender and MDR for endpoint solutions, BlueVoyant offers full incident response through its integrated DFIR services.

The MDR platform from BlueVoyant integrates threat content management; security orchestration, automation, and response (SOAR); threat intelligence platform (TIP) capabilities; and automation. This combination drives risk-based analytics, incident enrichment, and streamlined investigation processes.

In terms of future investments, BlueVoyant is actively exploring AI/ML use cases to enhance decision-making capabilities, empowering analysts to validate incidents swiftly and provide remediation guidance based on insights from previous investigations. In addition, the company has outlined plans to introduce services aimed at bolstering cloud security. A short-term goal involves integrating (SCD and DRP services into the MDR offering, thereby effectively managing cyber-risks both internal and external to clients' IT environments.

Strengths

BlueVoyant's MDR service is aimed at enhancing, not replacing, the threat detection and response capabilities of its customer's security technologies. The customers retain the licensing of their technology stack and host the solution, thereby minimizing security data leaving their environment.

BlueVoyant's vison of its MDR service to go beyond threats and reduce organizations cyber-risk resonates with many end-user organizations.

Challenges

BlueVoyant has showcased extensive capabilities for detecting and responding to security alerts within a short period of time. However, BlueVoyant is yet to offer SLAs around mean time to detection and mean time to response to its MDR clients.

Consider BlueVoyant When

Midsize to large businesses looking to outsource SOC operations with investments in Microsoft or Splunk security stack should consider BlueVoyant's MDR service.

Critical Start

Critical Start is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Headquartered in Texas, United States, Critical Start has been delivering MDR services since its establishment in 2012. The company serves both local and global clients, with a particular focus on the United States, where it operates through two risk and security operations centers (RSOCs).

Critical Start's MDR service empowers clients to maximize their current security investments by seamlessly integrating with EDR and extended detection response (XDR) solutions providers, such as Microsoft Defender XDR suite, Crowdstrike Falcon, and SentinelOne, and can be based on the customers' platform of choice, for example, Microsoft Sentinel or Splunk — fully managed by Critical Start. Notably, the company's MDR offering tailored for the Microsoft security stack is Microsoft certified. Critical Start's MDR services are built on its proprietary Cyber Operations Risk and Response

platform, providing security posture monitoring, management, and response orchestration for security analytics and cross-technology response. The platform seamlessly integrates with supported technologies through API integrations for event ingestion, status syncing, and event enrichment. Telemetry and security logs are collected comprehensively from various sources, including networks, endpoints, cloud platforms, SaaS applications, SIEM, email, and identity providers. The collected data undergoes processing through Critical Start's Trusted Behavior Registry (TBR) to filter out false positives. Remaining alerts are scrutinized by the company's RSOC analysts and escalated to clients as necessary. The company's web platform and mobile application make it rather simple to work with its team and the alerts that automation have not been able to clear. The company collaborates closely with clients to establish rules of engagement for automated response and remediation based on the criticality of assets, users, and other parameters.

The Cyber Research Unit (CRU) at Critical Start is responsible for detection engineering, threat research, and the curation of TI. This intelligence is integrated into the service for correlation and enrichment of alerts. While the RSOC is responsible for performing reactive threat hunts across customer environments based on detections, the CRU conducts periodic proactive threat hunts based on threat intelligence and trends. MDR customers can engage the CRU for deeper proactive threat hunting service through Critical Start's Managed Threat Intelligence offering.

Critical Start's in-house DFIR capabilities support the entire life cycle of incident response, covering digital forensic investigations, evidence seizure, chain of custody, and secure storage. When customers include the asset visibility and risk assessment essentials add-ons with the MDR service, they gain added value through the cyber-risk dashboard and risk-ranked recommendations. Critical Start is actively investing in enhancing its security platform and plans to launch new MDR offerings designed specifically for OT environments.

Strengths

Critical Start's MDR customers highly appreciate the user-friendly nature and reporting capabilities of its customer portal. A key feature is the API access, which allows users to extract security data for peer benchmarking, productivity analysis, and visualization of security posture trends over time.

Moreover, Critical Start's MDR services are supported by a 60-minute or less median time to respond (MTTR) service-level agreement for all alert priorities, enhancing customer confidence in the effectiveness of its MDR offering.

Challenges

Critical Start specializes exclusively in MDR services and offers a limited range of additional managed or professional security services. Customers seeking to consolidate their security services may need to engage with multiple vendors.

The company's primary focus is currently on North America, and the company has a limited presence in other regions.

Consider Critical Start When

Midsize to large organizations across industries in North America with current or planned investments in the Microsoft security stack should consider Critical Start's MDR service.

Dell Technologies

Dell Technologies is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Headquartered in Texas, United States, Dell Technologies unveiled its managed detection and response services in 2021, extending its reach to both local and global clients worldwide through a global delivery SOC with "follow the sun" coverage.

Dell Technologies has developed its MDR services to align with customer preferences for security solutions, offering options such as Secureworks Taegis XDR, CrowdStrike Falcon XDR, and Microsoft Defender XDR (positioning itself as a certified Microsoft managed extended detection and response provider). The service is designed to ingest telemetry from customers' diverse security technologies through API integration, ensuring a comprehensive and unified approach to threat detection.

Telemetry and security log data from both on-premises and cloud solutions undergo processing through Dell's security platform. An automation layer, integrated over the XDR platform, correlates alerts with the latest threat intelligence and enriches them with asset and vulnerability data. These refined alerts are then reviewed by Dell's security analysts. In case of security incidents, Dell, if allowed by clients, can initiate automated incident containment and response actions.

Dell's MDR service is offered in three tiers: MDR, MDR Pro, and MDR Pro Plus. This tiering strategy elevates the baseline MDR offering to an overall managed risk solution. The MDR Pro Plus tier provides a 360-degree security operations solution, encompassing vulnerability management, annual penetration testing, continuous attack simulation management, year-round managed security awareness training, and incident recovery.

All MDR service tiers include incident response and recovery hours to facilitate incident response life-cycle management and proactive threat hunting to uncover unknown threats. For customers with Dell's Cyber vault, the Cyber Recovery Solution, there is an entitlement to a Cyber Recovery Guarantee, ensuring a robust approach to cyber-resilience.

Dell Technologies has made significant investments to offer clients an integrated security solution. This solution will combine unified risk management, proactive security operations, and devices and infrastructure. The innovative approach brings deep orchestration and automation capabilities, fostering faster detection, cross-technology response, and an enhanced customer experience through a new Dell client portal that will enable a "single pane of glass" view into subscribed security services. In addition to technology improvements, Dell is building partnerships with cyberinsurance and legal firms to assist customers in meeting coverage requirements and streamline cyberincident management.

Strengths

Customers leverage Dell's extensive global presence to meet their security service needs across 75 countries. This includes access to a global SOC team, offering advantages such as continuous 24 x 7 x 365 coverage, global threat intelligence sharing between regional SOCs, scalability across time zones, diverse expertise, and enhanced incident response capabilities.

Furthermore, Dell can provide localized expertise when necessary to meet regulatory compliance requirements, offer faster onsite response times, ensure language and cultural alignment, reduce communication latency, and foster stronger relationships with local client teams.

Challenges

Dell Technologies' strong reputation in the infrastructure market often eclipses its brand awareness in security services. To address this, Dell Technologies should make strategic investments to highlight the unique features of its MDR services and position itself as a leader in this field.

Some Dell MDR customers have indicated the need for further support from Dell to maximize the benefits of their MDR service. In response to this feedback, Dell has reaffirmed its dedication to customer experience by increasing investment in a customer success function. This investment aims to automate processes and provide better assistance to its customers.

Consider Dell Technologies When

Small to enterprise customers worldwide looking for fully managed 360-degree SecOps solution should consider Dell Technologies' MDR Pro Plus offering.

Expel

Expel is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Headquartered in Virginia, United States, Expel has positioned itself as a significant player in the cybersecurity landscape since its establishment in 2016. Launching its MDR services in 2018, the company initially served clients in North America and has since expanded its reach with the addition of vulnerability prioritization and phishing and is now serving clients across EMEA, APAC, and LATAM.

As a pure-play MDR services provider, Expel distinguishes itself with its commitment to delivering comprehensive cybersecurity solutions. At the heart of its services is the Expel Workbench, a patented security operations platform that not only serves as an internal tool but is also part of the Expel MDR customer experience. Complementing its core MDR offering, Expel provides additional services such as threat hunting, vulnerability prioritization, and phishing investigation and response, strategically aimed at reducing organizations' overall risk and upleveling their security talent.

Expel's MDR service is characterized by its technology-agnostic approach, boasting over 120+ native integrations for monitoring diverse environments, including endpoint detection response, identity and access, cloud control plane, cloud workload (K8), network, SaaS, and more across the technology landscape. The service ingests data directly from clients' security technologies via RESTful API calls or by querying the customer's SIEM if available.

Automation lies at the core of Expel's MDR service, with an automated tier 0 SOC handling data normalization and rule application and a tier 1 SOC automation (Ruxie) responsible for alert enrichment, triage, and automated responses. This multilayered automation ensures efficient processing and response to security events with resiliency recommendations and root cause analysis. Beyond threat management, automation also extends into onboarding and service provisioning. Clients benefit from self-service features for onboarding a vast majority of their tech stack, both on premises and in the cloud. Cloud authorization templates are automatically generated, and clients can define response actions for individual assets/users or asset/user groups, significantly reducing onboarding time and accelerating time to value.

The service is fortified by the latest threat intelligence, curated from commercial and open source sources and Expel's own investigations. Continuous indicators of compromise-based threat hunts are standard for all clients, while hypothesis-based threat hunting across multiple attack surfaces can be purchased as an add-on.

Expel's Workbench extends an API-based customer portal for reporting and visualizations, providing clients with the flexibility to connect to the company's IT service management (ITSM) platforms or pull data for customized analytics. Clients gain real-time visibility into analysts' actions and workflows, fostering transparency and collaboration. This collaboration also enables customers to provide suggestions for the overall service through the portal, ensuring their input influences the service's evolution over time.

Expel, having completed its Series E funding in 2021 and experiencing rapid growth, is directing investments toward global expansion and enhancing its MDR service. Future investment themes include core platform enhancements, expanded coverage for Kubernetes and cloud provider ecosystems such as Wiz and Google (Mandiant), automated response and remediation actions, and innovative reporting features.

Strengths

Expel's AI-based tiers 1 and 2 SOC-automated enrichment, correlation, and investigative activities, integrated within its proprietary security platform Workbench and machine learning analysis, allow for rapid alert triage at scale. Customers benefit from complete visibility into Expel Workbench, providing them with the same view as Expel's SOC analysts. This transparency ensures that customers can track the progress of investigations in real time, from the actions being taken to address valid alerts all the way through resilience recommendations and remediation actions.

Challenges

Expel has proven its ability to achieve rapid detection and response times and give customers the ability to view specific metrics as needed. Expel offers SLAs for solution availability and incident notification time but does not currently extend SLAs to cover incident response times.

In addition, as a pure-play MDR service provider, Expel's portfolio focuses on MDR threat detection and hunting and does extend its security expertise to help customer tackle the security challenges associated with phishing/email security and vulnerability prioritization but does not offer traditional managed security SPs services like compliance and security solutions management. Customers seeking to consolidate their managed and professional security services may need to engage with multiple vendors. Expel does collaborate with some managed service providers and security consulting firms to address these gaps and offer a more comprehensive security solution.

Consider Expel When

Organizations of all sizes, with or without established SOC operations, looking to outsource threat management should consider Expel's MDR offering.

Inspira Enterprise

Inspira Enterprise is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Headquartered in Mumbai, India, with its U.S. headquarters in Texas, Inspira Enterprise has been a significant player in cybersecurity and data analytics services since its establishment in 2008. In 2017, the company broadened its services with the introduction of MDR offerings. Presently, Inspira operates globally across more than 10 countries and maintains five strategically positioned cyber fusion centers (CFC) worldwide. With nearshore capabilities serving across a diverse clientele in North America, ASEAN, the Middle East, Africa, and India, Inspira Enterprise is steadily gaining recognition in other regions as well.

As a provider specializing in cybersecurity strategic advisory, consulting, and managed security services, Inspira Enterprise offers extensive range of services, including proactive detection and closed-loop remediation, as part of its Intelligence-Driven Cyber Defense (ICD) practice. The company's MDR service adopts a platform-agnostic approach, meeting clients where they are in terms of security technology investments. Whether clients prefer to leverage their own SIEM or opt for an outcome-based model, Inspira Enterprise tailors its services to the business context. The MDR service integrates SIEM, UEBA, SOAR, and TIP capabilities while also delivering a unified cyber-risk dashboard to provide visibility into threat detection coverage and maturity. Telemetry and logs data from cloud infrastructure, SaaS applications, and on-premises solutions are collected through over 135+ data connectors and is processed by MDR platform's native detections, enhanced with Inspira's investments of over 700 in-house developed use cases.

Automation and orchestration are foundational to Inspira's MDR service, with over 130+ playbooks facilitating a15-minute detection, 30-minute containment, and 4-hour remediation SLA for highest severity incidents. Proactive threat hunts, driven by intelligence from commercial, open source, and government sources, are included as Inspira's standard offering, with clients having the option to enhance threat hunting capabilities as an add-on.

Inspira Enterprise has invested significantly in developing its native MDR platform, (iMDR), expected to be available to clients in 2024. This platform will bring advanced detection and hunting capabilities along with GenAI-enabled dashboard embedded in its iSMART2 customer portal. This new unified offering will integrate offensive strategies such as integrated attack simulations and ongoing validation of defensive measures by incorporating continuous security attestation.

Inspira Enterprise is also diversifying its services with offerings like deception as a service, IT-OT converged SOC and continues to invest in service offerings and automation to improve SOC Program Governance through measurable and actionable KPIs. Inspira Enterprise's proactive stance and ongoing investments position it as a forward-thinking partner in the dynamic field of managed detection and response services.

Strengths

Inspira Enterprise's MDR offering extends beyond threat containment to include a closed-loop remediation process after containment that ensures that enterprisewide policies and configurations are updated, effectively preventing future attacks using similar methods. This process enables Inspira's service to improve analyst interaction and develop a deeper understanding of the client's context.

Furthermore, Inspira Enterprise brings wealth of experience in providing threat detection and response services in complex environments, particularly for midmarket and enterprise customers in the banking and financial services (BFSI), healthcare and life sciences (HCLS), and public sector, with steady adoption of its services within organizations in other industry verticals.

Inspira Enterprise's comprehensive set of accelerators forms the foundation for assisting its clientele transition from their existing security information and event management solutions to Inspira MDR platform.

Challenges

Inspira Enterprises' MDR services, highly respected in Asia/Pacific, are now gaining clients in North America and other regions. To grow globally, Inspira Enterprise should strategize to highlight its offerings and enhance the visibility of its future strategy. This will help the company gain a stronger presence in underserved industry sectors and international markets, appealing to a wider range of clients seeking comprehensive security solutions.

Consider Inspira Enterprise When

Midsize to large customers with complex IT environments looking to completely outsource cyberdefense or augment their existing SOC efforts should consider Inspira Enterprise's MDR service offering.

LMNTRIX

LMNTRIX is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

LMNTRIX, headquartered in California, United States, has been a prominent player in the cybersecurity landscape since its establishment in 2015. Serving a global clientele, the company employs security analysts strategically across the world, ensuring a comprehensive "follow the sun" support model.

Specializing in MDR, LMNTRIX is renowned for its "active defense" service, complemented by an array of security testing and assessment services. This service is modularized into three tiers — foundation, enhanced, and premium — each offering distinct features tailored to varying security needs.

The foundation subscription provides essential services like continuous monitoring, exploit prevention, and automated threat containment across the network, endpoints, mobile, and cloud. The enhanced tier introduces intelligence, deception, and identity protection for enhanced detection against human attackers that have established point of breach looking to move laterally.

Tailored for large organizations with a low risk tolerance, the premium subscription is focused on post-breach forensic strategies and offers advanced services, including packet capture and proactive threat hunting, external deep and dark web monitoring, and actionable insights through technology and subject matter expertise fusion.

LMNTRIX has invested significantly in its proprietary XDR platform, seamlessly integrating threat intelligence, EDR, NDR, network forensics, SIEM, SOAR, UEBA, and mobile and cloud security together with deceptions everywhere. The platform's flexibility allows integration with various third-party security solutions and cloud providers for streamlined data ingestion, analysis, and containment.

Within its "active defense" service, LMNTRIX provides unlimited hours of digital forensics and incident response, guiding clients through the entire incident response life cycle.

LMNTRIX is committed to enhancing its services with self-service capabilities, providing clients with control over policy management across their entire security technology stack without formal ticket processes. Ongoing investments focus on expanding the portfolio of third-party integrations for enriched data ingestion, containment, and remediation capabilities.

Strengths

LMNTRIX's homegrown XDR platform brings in cross-technology detection and response by design along with AI-based automation for tiers 1 and 2 SOC workflows like incident validation, investigation, and client notification, which is foundational to the company's quick threat detection and response.

The hyperconverged cyberdefense SaaS platform approach means clients can leverage the benefits of 12 detection technologies cost effectively through a single interface while the entire tech stack is operationalized by LMNTRIX.

Unlimited containment, remediation, DFIR hours, and proactive threat hunting included within the subscription are important to clients, especially SMBs that require full incident response life-cycle support.

Challenges

For LMNTRIX, the absence of a portfolio of managed security and professional services presents a notable challenge. Its focus on MDR and XDR solutions means that clients seeking a comprehensive security approach may need to engage with multiple vendors. This limitation could potentially restrict its ability to cater to clients looking for a one-stop solution for their security needs. In a market where integrated security services are increasingly valued, this aspect could pose a challenge to its competitiveness and growth.

Consider LMNTRIX When

Small to midsize organizations across industries seeking to outsource threat management should consider LMNTRIX's MDR offering as a dedicated cyberdefense capability while enterprise clients can look to LMNTRIX to augment their existing SOC efforts by taking advantage of the advanced detection and response capabilities offered by the LMNTRIX Managed XDR.

NCC Group

NCC Group is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

NCC Group, headquartered in Manchester, United Kingdom, has been operating in the MDR sector since the launch of its MXDR services in 2018. The company primarily serves clients in the EMEA region and the United Kingdom, expanding its global presence through four strategically positioned global SOCs and recently acquiring key clients in North America and APAC.

As a cybersecurity services provider, NCC Group offers a suite of services categorized into four pillars: Technical Assurance Services, Consulting and Implementation, Managed Services, and DFIR Services. The core of its MDR service is a managed SIEM solution, incorporating threat intelligence-driven detection logic mapped to MITRE ATT&CK framework, a detection engine, related SOC services, and threat hunting and incident response capabilities.

NCC Group's MXDR services are based on Microsoft Sentinel, verified by Microsoft, and other prominent technologies like Splunk. Their flexibility is demonstrated through seamless integration capabilities with leading EDR, network security, and cloud providers. Telemetry and security logs collected from networks, endpoints, cloud platforms, and SaaS applications are processed for automated detection using both signature and ML-based methodologies. An ML-based automation engine enriches alerts with threat intelligence and asset data before human intervention is sought for further investigation. The MDR offering includes intelligence-based, hypothesis-based, and tactics, techniques, and procedures (TTPs)-based proactive threat hunting for all clients.

Collaborating closely with clients, NCC Group determines the extent of automated response within their environment. With client authorization, the company can trigger automated responses across endpoints, networks, and identity vectors as required within the scope of several automated playbooks. The company has in-house DFIR capabilities to support the entire life cycle of incident response.

NCC Group is investing strategically in expanding its MXDR offering. The company's focus includes enhancing coverage for OT and mobile security while concurrently advancing ongoing automation efforts. The company has also made significant investments in global service delivery to extend its presence beyond EMEA into key markets in North America and APAC, aiming for broader geographical reach and market penetration.

Strengths

NCC Group possesses extensive security consulting expertise and the ability to coordinate various security solutions in intricate environments. This allows the company to provide clients with tailored and comprehensive security solutions that effectively address their specific security needs.

The company's emphasis on AI/ML-driven detection and triaging has been instrumental in achieving a low mean time to detect and respond (MTTD&R), a key component of its MDR service. This is supported by a SLA of 15 minutes to triage the most critical alerts, demonstrating NCC Group's commitment to rapid and effective incident response.

Challenges

While NCC Group has achieved notable success in the European market, its presence in other regions remains limited. To expand its global footprint, the company should consider strategic investments in marketing initiatives aimed at building brand awareness and capturing new business opportunities in these regions. By establishing a stronger presence and showcasing its expertise and capabilities, NCC Group can position itself as a key player in the international market for MDR services.

The organization's customer portal offers valuable insights into service operations and provides basic reporting functionality. However, it lacks user-friendly features and advanced capabilities, which may impact its usability for customers seeking more sophisticated tools.

Consider NCC Group When

Midsize to large organizations with complex security landscape should consider NCC Group's MDR offering to improve their SOC outcomes.

Ontinue

Ontinue is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Ontinue, a global company with North American headquarter based in Redwood City, California, and European headquarter based in Zurich, Switzerland, launched its managed extended detection and response offering in 2020 while it was still part of Open Systems. In 2023, the MXDR business of Open Systems transitioned into Ontinue, which currently serves clients across EMEA and North America from its global CDCs strategically positioned in Europe, the United Kingdom, the United States, and India.

Ontinue's ION MXDR service caters to customers utilizing or planning to implement the Microsoft Security Stack, with a strong focus on operationalizing Microsoft Defender 365, Microsoft Defender for Cloud, Microsoft Defender for IoT, and Microsoft Sentinel, in addition to existing non-Microsoft legacy controls. Ontinue's specialized Microsoft expertise allows it to offer additional value beyond managed detection and response, including helping clients harden their environment with best practice configuration and deployments, achieve their tool consolidation goals, reduce data ingestion costs, and accelerate time to value. As an early member of the Microsoft Intelligent Security Association (MISA) program, Ontinue's MXDR offering is Microsoft certified.

At the core of Ontinue's MXDR capabilities lies the ION platform, a homegrown AI and automation solution. ION automates tier 1 SOC activities from data filtering to enrichment with threat intelligence for triage, investigation, and response. The ION platform also incorporates the ION IQ AI engine, developed internally and through the acquisition of Skooba, an AI/data science start-up based in Bern, Switzerland. ION IQ models client environments, supports threat investigation and response through a variety of AI models (semi-supervised learning, boosted trees, graph neural networks, large language models, and so forth), pattern matching and behavior analytics, and guides defenders through investigations based on learned behavior.

Ontinue's MXDR service includes threat intelligence integration and proactive threat hunts based on IoC and behavioral hunts mapped to the MITRE ATT&CK framework. Notably, Ontinue has integrated its entire interaction model within Microsoft Teams, eliminating the need for additional management consoles and facilitating real-time collaboration between clients, cyber defense centers, and designated cyber advisors through Teams' native chat capabilities, including voice, text, and video on any device. Cyber advisors provide customers with regular guidance and recommendations for environment hardening to continuously improve the customer's security posture over time. In addition, Ontinue has built an AI-driven chatbot directly into Teams to provide customers with insights and recommendations related to a variety of topics including incident trends, cost optimization, posture improvements, and MITRE techniques.

Ontinue is committed to ongoing investments in AI, focusing on expanding ION IQ Chatbot capabilities, AI-based automation of triage and investigations, and launching a security score to help clients improve resiliency. These investments underscore Ontinue's dedication to enhancing its MXDR service and providing clients with advanced, collaborative, and efficient cybersecurity solutions.

Strengths

Ontinue's MDR service is underpinned by advanced analytics, AI, and ML technologies. These technologies drive innovation in their ability to analyze and model a customer's environment and security operations workflows, and then use that model to tailor incident response and remediation efforts to each customer's existing operational processes.

In addition, Ontinue's MDR service places significant emphasis on attack surface management. This includes a risk-prioritized vulnerability management service, security posture monitoring and hardening recommendations, and security cost management. This approach aims to not only manage threats but also reduce overall cyber-risk for clients.

Challenges

Ontinue focuses exclusively on MDR services, distinguishing itself as a pure-play provider in this field. This specialization allows Ontinue to concentrate its expertise solely on MDR, potentially leading to deeper specialization and innovation. However, this focus may limit Ontinue's ability to offer a comprehensive suite of security solutions, which may include compliance and security solution deployment and management, requiring clients to engage with multiple vendors for diverse security needs.

Some customers suggest that Ontinue could enhance customer relationship management by providing more frequent updates on the latest threat landscape. In response, Ontinue has recently released its inaugural Threat Intelligence Report for 2023. The first edition of this report, compiled by Ontinue's advanced threat operations team, provides insights and trends related to threats, attack techniques, and attacker groups, including industry-specific breakdowns of what to look out for in 2024.

Consider Ontinue When

Midsize to large organizations that prioritize Microsoft's security stack and aim to optimize their investments while enhancing their security outcomes should evaluate Ontinue's MDR service.

OpenText

OpenText is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

OpenText, headquartered in Ontario, Canada, launched its MDR services in 2021, catering to local and global clients, primarily in North America and EMEA. The company's global virtual SOC, supported by security analysts spread across continents, ensures "follow the sun" coverage for clients.

OpenText has developed its MXDR service internally and through strategic acquisitions. Notably, the 2023 acquisition of Micro Focus enhanced OpenText's threat hunting capabilities, now available as an add-on to the MXDR service.

At the core of OpenText's MXDR offering is the Devo SIEM, featuring out-of-the-box integrations with leading security technologies for endpoint protection, on-premises infrastructure, cloud services, and cloud applications. The service leverages OpenText's BrightCloud threat intelligence for alert validation, enrichment, and proactive threat hunting.

For response capabilities, OpenText employs a rule-based approach to trigger automated responses, utilizing EDR agents deployed by clients. The service also supports third-party EDR solutions such as CrowdStrike and Microsoft Defender. In addition, the service provides guided remediation for response coordination across various security technologies. OpenText actively conducts threat hunting, focusing on both known threats and behaviors based on TTP, offering clients the option to subscribe to standalone threat hunting services using ArcSight intelligence and CrowdStrike EDR.

OpenText's MXDR service integrates proprietary AI/ML models, particularly in user and entity behavior analytics (UEBA), forming the foundation for high-fidelity detections of unknown threats. The service also features inbuilt incident response hours, which can also be purchased as add-on over and above what is included. OpenText also offers in-house forensic investigation support to help clients with full IR life-cycle management.

In terms of future investments, OpenText is dedicated to integrating the advanced capabilities gained through the Micro Focus acquisition, incorporating ArcSight and OpenText cybersecurity solutions and services into the MXDR offering. The company plans to expand the service's capabilities, starting with identity management and privacy features. OpenText also aims to integrate dark web monitoring and establish new industry partnerships to broaden the scope of its MXDR service.

Strengths

OpenText's managed extended detection and response service comprises an accessible SIEM system, an EDR agent, managed threat hunting, custom detections tailored to specific needs, and an IR retainer. This standardized offering enables clients to quickly realize value and simplifies pricing, addressing key considerations for its clients. With a global presence, OpenText is well suited for large clients with operations spanning multiple regions.

Challenges

OpenText's managed extended detection and response offering is a relatively recent addition; however, it holds strategic importance for OpenText, evident from the company's significant investments in the service and acquisitions such as that of Micro Focus. While these acquisitions have brought new capabilities, they also pose integration and redundancy challenges. OpenText is working to integrate these new capabilities into a cohesive offering to enhance its MDR service.

Consider OpenText When

Midsize to large organizations across industries should consider OpenText's MXDR offering.

SentinelOne

SentinelOne is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

SentinelOne is a California-based cybersecurity provider that launched its MDR services in 2019, catering to both local and global clients through a network of SOCs strategically located around the world, operating in a "follow the sun" model.

SentinelOne's portfolio of threat services includes the MDR and DFIR service, Vigilance, and threat hunting and intelligence service, WatchTower. Vigilance Respond, the base tier, offers 24 x 7 x 365 threat detection and response, while the advanced tier, Vigilance Respond Pro, adds DFIR capabilities, providing end-to-end IR life-cycle management. WatchTower services are available as an add-on to deliver proactive threat hunting and threat intelligence reporting.

A significant feature of SentinelOne's MDR services is its advanced automated response capabilities driven by AI. The AI is trained on past analyst investigations, improving the accuracy of incident validation and reducing false positives. This capability is fundamental to achieving the company's impressive 60-minute MTTR service-level agreement.

Originally designed to complement its endpoint protection platform, SentinelOne has expanded its MDR services with the introduction of the Singularity platform. This allows clients to integrate various technologies such as network, identity, cloud protection, and email with the MDR service. These integrations provide contextual data and enrichment beyond the endpoint, enabling comprehensive incident analysis and reporting. Customers can also define policies for automated response across these technologies.

SentinelOne's future investments focus on expanding third-party coverage for its MDR offering through continuous enhancements to the Singularity platform. The company is investing in its proprietary Purple AI, a GenAI model, to enhance threat hunting and analysis capabilities. Furthermore, SentinelOne is revamping its portal experience to offer improved visualizations, comprehensive operational reporting and dashboarding, and executive reporting for a more enriched user experience. Customers and prospects can expect these developments as part of SentinelOne's commitment to providing cutting-edge and efficient cybersecurity solutions.

Strengths

SentinelOne's focus on AI has significantly improved the speed of threat response. The company's AI security analyst and threat hunting tools, such as Purple AI and generative AI, allow for faster threat detection and response by automating operations across various devices and environments and is foundational to its 60-minute mean time to respond service-level agreement.

SentinelOne's global presence strengthens its position within the MDR market. This reach allows the company to offer its services worldwide, ensuring comprehensive security coverage for organizations regardless of location. It also enables SentinelOne to support clients with operations in multiple regions, providing consistent and effective security solutions globally. In addition, this global reach enhances SentinelOne's ability to detect and respond to emerging threats by accessing diverse threat intelligence sources.

Challenges

SentinelOne's Vigilance MDR service is tailored to maximize the effectiveness of its EDR agent. However, a challenge arises from the fact that this service does not encompass other telemetry sources or third-party integrations. SentinelOne intends to address this issue with support for identity, threat intelligence, and other attack surfaces in 2024.

SentinelOne does not directly provide traditional managed services for compliance and security solutions management. Instead, the company collaborates with a worldwide network of partners that offer services that complement its MDR offerings. This approach might pose a challenge for clients seeking a comprehensive security suite from a single vendor. However, the launch of PinnacleOne Strategic Advisory Group in November 2023 enhances SentinelOne's consulting services. This new group provides customers with intelligence, insights, and risk management capabilities, further strengthening SentinelOne's offerings.

Consider SentinelOne When

Organizations of any size and industry worldwide looking to maximize the value of their SentinelOne investment should consider the company's MDR offering.

Trustwave

Trustwave is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide emerging managed detection and response services.

Trustwave, headquartered in Illinois, United States, has been a prominent player in the managed security service provider space. Launching its MDR services in 2018, Trustwave operates globally, with SOCs distributed worldwide, employing a "follow the sun" model.

As a pure-play managed security SP, Trustwave offers an extensive suite of managed security services alongside security advisory and assessment services. Within its service portfolio, the MDR services, integrated with the managed SOC/SIEM offerings, deliver comprehensive 24 x 7 x 365 security monitoring, threat detection, response, and security tuning.

Central to Trustwave's MDR offering is the Fusion platform, a real-time analytics and ML engine equipped with security orchestration and automation capabilities. The Fusion platform collects logs and alerts from various security technologies across on-premises and cloud environments through bidirectional APIs or through Trustwave Connect, a physical or virtual device, that facilitates the connection of security technologies to the Fusion platform, supporting data filtering, compression, and encryption.

The Fusion platform processes security telemetry and logs, leveraging threat intelligence from SpiderLabs, Trustwave's in-house threat intelligence unit. Employing ML and AI modules, the platform contrasts data against known threat indicators, applies relevant use cases, and automates response actions based on the client's predefined traffic light protocol (TLP) configuration. This protocol delineates the level of authorization required for various response actions.

Trustwave's MDR services come in two tiers: a base offering focused on deeper detection and response using endpoint telemetry and an elite tier expanding the scope with additional SpiderLabs services, custom MTTR service-level agreements, and high-touch engagements. Both tiers include SpiderLabs threat intelligence integration, IoC-based proactive threat hunts, and the option to upgrade to advanced continual threat hunting among other available add-ons. The Fusion portal, complemented by a custom mobile app, provides clients with a real-time view into threat investigations, one-click resolution actions, and advanced visualization and reporting.

In 2023, Trustwave expanded its MDR services to include offerings tailored for Microsoft Sentinel and MDR based on the Microsoft Defender and related technology stack. As an early member of the Microsoft Intelligent Security Association (MISA), Trustwave brings deep Microsoft expertise to help clients make the most of their Microsoft security investments.

A unique offering from Trustwave is the Security Colony, accessible to all MDR clients. This platform, designed for CISOs, provides a wealth of toolkits, guidelines, playbooks, and assessment capabilities derived from global cybersecurity consulting engagements.

Trustwave has heavily invested in AI to propel its security operations toward an "autonomous SOC." This includes an AI-driven "tier 0" SOC analyst for real-time incident detection and resolution, assisting human analysts with guided investigations and reporting. Additional investments are directed toward a proprietary threat investigation platform to expedite investigations and further enhance MTTR service-level objectives.

Strengths

SpiderLabs, a division of Trustwave, serves as a core strength for Trustwave's Managed Detection and Response service. SpiderLabs provides Trustwave with access to cutting-edge threat intelligence and research capabilities. This allows Trustwave to stay ahead of emerging threats and provide proactive threat detection and response for its MDR clients. In addition, SpiderLabs' expertise in threat hunting and malware analysis enhances Trustwave's ability to identify and mitigate complex threats.

Trustwave clients indicate that Security Colony is a valuable resource that has helped them improve their overall security maturity.

Challenges

While Trustwave has successfully achieved low mean time to detect and respond to security alerts through automation, a key challenge is the absence of a standard service-level agreement around detection and response times.

Consider Trustwave When

Organizations of all sizes and industries that prioritize proactive threat detection and response should consider Trustwave's MDR services.

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.

Strategies and Capabilities Criteria

This section includes an introduction to market-specific weighting definitions and weighting values (see Tables 1 and 2).

TABLE 1

Key Strategy Measures for Success: Worldwide Emerging Managed Detection and Response Services

Strategies Criteria	Definition	Weight (%)
Functionality or offering strategy	The criteria for rating a vendor's future MDR offering strategy include expanding essential capabilities, enhancing threat detection and response across security domains, improving threat intelligence integration and threat hunting, introducing new use cases for advanced security analytics and AI/ML, driving R&D, and reducing time to value.	48.00
Go-to-market strategy	The criteria for rating a vendor's go-to-market strategy include evaluating their sales and marketing efforts, channel management strategies, and customer relationship management initiatives.	14.00
Customer portal strategy	The criteria for rating a vendor's customer portal strategy include their focus on improving ease of use, operational and executive reporting, and other use cases aimed at enhancing transparency and engagement with the service.	8.00
Talent management strategy	The criteria for rating a vendor's talent management strategy include their efforts to secure their talent pipeline and improve the quality of their security talent.	8.00
Range of services strategy	The criteria for rating a vendor's range of services strategy include their road map to expand the portfolio of managed and professional security services other than MDR.	6.00
Future outlook	The criteria for rating a vendor's future outlook strategy include their focus on revenue, profitability, and customer growth, aiming for overall financial stability in the future.	6.00
Security outcome strategy	The criteria for rating a vendor's future strategy for security outcomes include their plans to introduce SLAs and efforts to improve mean time to detect (MTTD) and mean time to respond (MTTR) and introduce key performance indicators (KPIs) to enhance overall service.	5.00
Cost normalization strategy	The criteria for rating a vendor's cost normalization strategy include their strategy to standardize service delivery, implement service tiering, and leverage automation to normalize costs in the future.	5.00
Total		100.00

Source: IDC, 2024

TABLE 2

Key Capability Measures for Success: Worldwide Emerging Managed Detection and Response Services

Capabilities Criteria	Definition	Weight (%)
Functionality or offering	The functionality or offering of the vendor is evaluated based on its demonstrated essential capabilities, breadth and depth of security data sources for threat detection and analysis, response capabilities across security domains, extensive proactive and reactive threat hunting capabilities, aggregation and utilization of threat intelligence, use of advanced security analytics including AI/ML, and ability to ease and accelerate client onboarding to reduce time to value.	42.00
Security outcomes	The criteria for security outcomes evaluate the vendor based on its service-level agreements (SLAs) across various metrics such as mean time to detect (MTTD) and mean time to respond (MTTR), improvements in MTTD and MTTR over time, and the competitiveness of its 2023 MTTD and MTTR compared with other vendors.	14.00
Range of services	The range of services is evaluated based on the vendor's managed security services portfolio complementing its MDR, breadth of professional services including consulting and assessments, and capabilities in digital forensics and incident response.	12.00
Go to market	The go-to-market criterion evaluates the vendor's marketing capabilities, including digital marketing and regional campaigns, and its channel management, focusing on partnerships to drive indirect sales. It also considers the vendor's sales capabilities, such as size and distribution of sales team, and its customer management, including relationship management initiatives for customer delight.	12.00
Customer portal	The customer portal criterion evaluates the vendor based on the ease of use of its service portal, which includes an intuitive user interface (UI) and well-organized information tailored for different user personas. It also assesses the portal's reporting capabilities, including predefined, persona-based, and customizable reporting options, covering operational, executive, and compliance reporting needs.	8.00
Service tiers	The service tiers criterion evaluates the vendor based on its tiered managed detection and response (MDR) offering, catering to customers with varying needs, and its pricing model, which includes flexible pricing options to accommodate different budgets and requirements.	6.00
Talent management	The talent management criterion assesses the vendor based on the experience and training of its security full-time equivalents (FTEs), including its tenure and training programs, as well as its talent pipeline, which includes talent attainment and retention strategies.	6.00
Total		100.00

Source: IDC, 2024

LEARN MORE

Related Research

- *Worldwide and U.S. Comprehensive Security Services Forecast, 2024-2028* (IDC #US50635924, April 2024)
- *Abundance in Tools, Shortages in Talent – Security Service Providers Addressing Feast and Famine in 2023* (IDC #US51842423, February 2024)
- *Market Analysis Perspective: Worldwide Security Services, 2023 and Beyond* (IDC #US51228723, September 2023)
- *IDC's Worldwide Security Services Taxonomy, 2023* (IDC #US50332523, March 2023)

Synopsis

This IDC study presents a vendor assessment of emerging MDR service providers worldwide through the IDC MarketScape model. Using the IDC MarketScape model, 12 emerging MDR service providers with operations and customers worldwide were evaluated. This process included interviewing 11 providers and two or more customers from each provider, while for one that did not actively participate in this study, the evaluation was based on IDC's knowledge of its security services offerings and capabilities. Providers were measured in terms of current capabilities and future strategies for delivering MDR services to customers worldwide.

Yogesh Shivhare, research manager, Cybersecurity, says, "The managed detection and response services market is indeed a diverse landscape, teeming with a variety of service providers. It encompasses pure-play MDR providers, traditional managed security SPs that have evolved their managed security information and event management (SIEM) offerings into MDR, and security technology vendors that offer MDR services as part of their comprehensive security stack. Each of these vendors brings unique capabilities to the market, enabling them to meet the specific and unique needs of organizations across various sizes and industries. This diversity, while challenging for buyers due to the complexity of the market, ultimately leads to a more robust and tailored cybersecurity posture for the organizations that utilize these services."

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.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com