IDC Spotlight sponsored by NCC Group
June 2024

How Managed XDR Bolsters Businesses' Cybersecurity Posture

Richard Thurston
Research Manager
European Security Services, IDC

How Managed XDR Bolsters Businesses' Cybersecurity Posture

Introduction

Cybersecurity continues to ascend the enterprise agenda as the threat landscape becomes ever more complex and organizations battle to mitigate risk and meet extensive compliance requirements. Cybersecurity posture is now a common board-level discussion, with cybersecurity leaders now readily able to communicate cybersecurity issues in business terms.

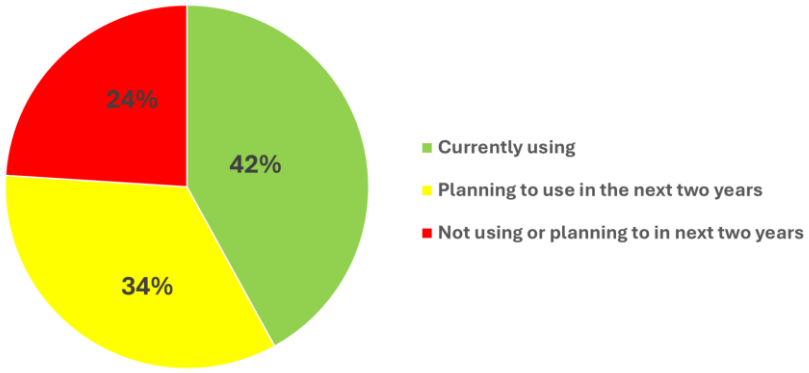
Due to a lack of in-house capabilities and skills — and thanks to the economies of scale and capabilities available from service providers — many organizations are looking to partly or fully outsource cybersecurity services. They are choosing from a range of services providers, from cybersecurity specialists to systems integrators, telco and network providers, and general IT services players.

A broad array of managed security services (MSS) is available to organizations. IDC groups these in three categories:

- Managed detection and response (MDR)
- Managed infrastructure aimed at protecting cloud workloads, endpoints, or email, or providing a specific function like a managed firewall or gateway, or managing vulnerabilities
- Other MSS (e.g., managed identity, privacy, or application security)

Managed extended detection and response (MXDR), a key MSS that is growing in popularity, sits within IDC's MDR grouping. Two-fifths (42%) of businesses were using MDR services at the end of 2023, according to IDC's *EMEA Security Services Survey*, while 34% expected to start using MDR within two years.

Figure 1: Adoption of Managed Detection and Response (MDR) — Currently and in 2 Years



Source: IDC's *EMEA Security Services Survey 2024*; (N = 804)

IDC forecasts that worldwide MDR spending will post a compound annual growth rate of 26.1% from 2023 to 2028, making MDR one of the fastest growing IT services markets.

Benefits

MXDR Evolves to Address Organizations' Cyber-Risk Objectives

MXDR has evolved continually as the needs of enterprises and the threat landscape have changed, from simple offerings initially into the current range of highly advanced, time-critical services.

The lines blur between an MXDR platform-based service and a managed service like MDR, though both can deliver successfully on cyber-risk mitigation. Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities and cybersecurity partners' tools or services and intellectual property.

Some MSS providers utilize an XDR platform for the technical portion of the MDR service (hence MXDR), then wrap that with services delivered by their own cybersecurity practitioners to fulfill the "hands on" part of the service. The additional services capabilities are critical to ensure client objectives are met. These are supplied by a provider's highly-trained cybersecurity staff in a 24 x 7 x 365 SOC (physical or remote).

MXDR is now offered by a wide range of providers, including broad IT services companies, network providers including telcos, and security providers that specialize entirely in managed and professional security services.

Many related security services can complement MXDR in mitigating cybersecurity risk and improving organizational resilience, including attack surface management, vulnerability services/penetration testing, incident management, managed cyber-recovery, and managed application security. Previous textbook concepts around disaster recovery and business continuity have evolved markedly as business leaders' understanding of risk, and their risk appetite, has evolved.

Resilience and risk mitigation is now one of the highest priorities for organizations, with 59% of cybersecurity professionals in EMEA describing it as a main business priority. This is driving interest in multiple MSS.

Trends

Key MXDR Purchase Drivers

For most IT services, price tops the list of organizations' buying criteria. However, this is not the case for cybersecurity services. IDC's *EMEA Security Services Survey 2024* found that for cybersecurity services, trust and assistance with extensive compliance requirements are the top 2 requirements for buyers in EMEA (Europe, the Middle East, and Africa). Price comes well down the list at number five (length of tenure in the market and skills and certifications rate higher).

These findings show that service providers have a clear opportunity to help organizations mitigate risk. Accordingly, buyers require a high level of confidence in service provider credibility — that is, they must trust that the provider will help the organization deliver business outcomes.

The importance of trust as a factor is likely to remain significant for buyers in the coming years due to the substantial amount of change organizations are facing and a raft of new technologies at their disposal, including generative AI, new machine learning techniques and LLMs, and the greater use of cloud resources and operational technology (OT) within IT environments. Any of a number of process or technological failures with these technologies could have adverse consequences for an organization.

There are differences in purchasing criteria between sectors and sizes of businesses. For example, financial services organizations are more likely to seek case studies from other financial services organizations before buying cybersecurity services. They are also slightly more likely to value speed of response due to the critical impact of downtime in this sector.

In terms of organization size, MXDR services are widely available to large organizations but are not always tailored to smaller organizations, which expect a simpler offering as they tend to have smaller in-house technology teams. This can act as an inhibitor to effective use of MXDR.

Across all segments, buyers are more confident in organizations with whom they have a track record, personal reference, or that can otherwise prove their technical abilities. The quality of threat intelligence, threat hunting, and automation/AI tools will increase confidence among technical buyers and can make the difference in purchasing decisions (though these are usually not the answers first sought in the procurement process).

Innovation is often desired by buyers — and as an issue, this requires some unpacking. Most providers have some level of innovation that supports their MXDR services. But due to hugely varying R&D budgets and different rates of change, some providers innovate faster than others. Most have created a customer advisory board to enable the innovation of multiple products and enhance the customer journey. One thing is certain: Organizations expect their service provider to keep pace with the threat landscape and proactively advise them when a significant new risk or vulnerability is identified.

Technology is a key factor in the successful realization of business outcomes — but some essential human skills remain required, including hunting for and understanding, prioritizing, and articulating risks. These human skills, supported by technical certifications, form an important part of a successful MXDR service.

Important Customer Portal Factors and Considerations

The most common contact some organizations have with security service providers is through a customer portal. The portals of most providers offer a broad range of metrics on the customer's security posture and the threats their organization is facing or has faced, as well as on service provider actions to address security events.

Provider portals can vary significantly. Some deliver a far broader range of reports than others, with some offering reports tailored for multiple audience types (e.g., security teams, CFOs).

Portals have a large effect on customer satisfaction and, accordingly, many providers are investing in improvements to their portal capabilities. This can involve adding reports, improving

visualization and accessibility, improving the ability and speed of interrogating data, or integrating multiple portals into a single interface (multiple portals often arise among IT service providers due to mergers and acquisitions).

Transparency of service provider actions is essential, as is the ability of the service provider to cut through the huge security volumes they are seeing to provide strong clear actions and advice to the customer. Security professionals expect unified and insightful reporting that enables them to proactively address their organization's cyber-risk objectives and compliance requirements.

MXDR to Become Leading Service Worldwide to Counter Rapidly Evolving Threats

Cybersecurity services have evolved faster than IT services markets as a whole due to rapid changes in the threat landscape. MDR as a service, for example, has already been through three key iterations.

IDC's analysis of the future of security services has identified three key issues that will shape the MDR market:

- **AI/ML:** The adoption of generative AI and other advanced AI/ML tools will enable threat actors to cause harm faster and with greater effect. However, advancements in these tools will also help defenders. Service providers must tell a story around the development of their proprietary and nonproprietary AI/ML capabilities — but human skills will continue to play a critical role in MSS provision.
- **OT:** The risks surrounding OT (e.g., connected manufacturing equipment or energy networks) have long been neglected. But as these assets become networked and therefore more vulnerable to threats, this situation is not sustainable. MXDR solutions must protect all valuable enterprise assets — IT, OT, and IoT — and this can require new skills and solutions. MXDR for OT remains in its infancy.
- **Inhibitors:** There will be winners and losers in the MXDR services realm. Some organizations will successfully mitigate cyber-risk while some will not move quickly or comprehensively enough. Inhibitors to the successful use of MXDR services include a lack of resources and knowledge and skills gaps (these can drive the outsourcing of detection and response), as well as a lack of alignment between business and cyber-risk and an increasingly complex marketplace with many types of providers that can make decision-making more difficult.

The need for third-party cybersecurity service expertise will grow for at least the next five years, according to IDC's cybersecurity services forecasts. The blend of managed and professional services purchased by organizations will continue to evolve. Threat hunting, in particular, is becoming a specialized science. An effective service wrap with the right SLA will be essential for organizations.

Vendor Profile

NCC Group, an MSS provider with footprints in North America, Europe, the Middle East, and Asia/Pacific, was created when the U.K.'s National Computing Centre sold its commercial divisions to its then management team. It has offered cybersecurity services for over 25 years,

growing via acquisitions including consultancy Fox-IT (which brought threat intelligence capabilities and a skill set from its Netherlands headquarters) and a number of cybersecurity service and solution providers.

NCC Group provides a range of managed services (including MXDR for Microsoft and Splunk and vulnerability management), digital forensics and incident response, consulting and implementation, technical assurance, and regulatory compliance services.

NCC Group focuses on providing targeted alerts to clients using automation and its enrichment engine that minimize the volume of false positives, increase speed of response, and enable clients to focus on priority events. NCC Group creates detection logic using insights from its threat intelligence team, incident response cases, red/purple team engagements, and external feeds. It implements these insights in its proprietary detection platform to keep pace with the threat landscape.

These technical capabilities are complemented by advisory services to help clients understand the threat, prioritize the response, and, in the longer term, work to improve and benchmark their cybersecurity posture.

NCC Group's services are intended to work with organizations' existing security environments, reducing requirements for new investments. Customers have a choice of platforms and can create unified visibility across endpoints, networks, and cloud. NCC Group leverages the detection platforms of its partners and its proprietary network sensor technology, integrating information from those platforms into its Unified Cyber Platform to create a broad view of the customer's IT environment and a single source of truth. Data ingestion and enrichment have been identified by NCC Group as a priority intellectual property investment for the company.

NCC Group has recently built a new customer portal based on ServiceNow, which will shortly become the single platform for all of its managed services customers. Service provider portals vary significantly by the data available, how data is reported, and how it can be analyzed. In our opinion, a demonstration of NCC Group's portal showed a clean appearance and was understandable and easy to query/navigate, with the aim of providing a fast, high-level view of the risk in question (which is important due the vast quantity of information available to defenders on the threat landscape and the time-critical nature of response).

The portal provides a single view of the MXDR and other services from NCC Group like attack surface management, managed vulnerability scanning services, threat intelligence, and online exposure management.

NCC Group is part of the Microsoft Intelligent Security Association and is recognized by Microsoft as a Managed Security Solutions Provider. Microsoft has recognized NCC Group with its verified MXDR solution status. NCC Group is also a Splunk top-tier Elite Partner.

In terms of external relations, the company focuses heavily on engaging with governments, regulators, and international organizations (including the UN, OECD, and World Economic Forum) — holding 30 parliamentary meetings in its 2023 FY — which has brought an opportunity for high profile recognition and influence on cybersecurity regulations and policy.

NCC Group is named as a Major Player in the IDC MarketScape: Worldwide Emerging Managed Detection and Response Services 2024 Vendor Assessment. It is growing quickly in MXDR, with a notable increase in its customer base.

Challenges

The MSS and MXDR markets are highly competitive, with a broad range of supplier types. Organizations must clearly articulate their differentiating strengths to grow share in these expanding markets. Many players are stronger in particular geographic regions and find that scale can provide increasing returns.

NCC Group has a strong customer base in the U.K. and Benelux, where it will find brand awareness to be high. IDC would expect lower levels of brand awareness in other countries and regions. The company has recently opened an office in the Philippines, increasing its Asia/Pacific presence.

Another challenge for cybersecurity specialists like NCC Group is in winning business where the customer's objectives are wider and dependent on services or assets outside of its portfolio. These could include some professional cybersecurity services, services around business risk, or services that benefit from ownership of network and cloud assets.

Conclusion

Increasing numbers of organizations are adopting MXDR services to harness the skills and capabilities of service providers and mitigate risk for their organization, helping them to achieve their resilience goals.

Two-fifths (42%) of businesses in EMEA were using MDR services at the end of 2023, according to IDC's *EMEA Security Services Survey*, with a further 34% saying they will start using MDR within two years. Worldwide spending on MDR will increase by a compound annual growth rate of 26.1% from 2023 to 2028.

In choosing an MXDR service, buyers are primarily motivated by trust in a supplier and the goal of meeting compliance requirements. Trust is a complex science that IDC has studied in depth. Heritage in the industry and strong customer references help build it. Service providers that offer a broad range of MSS based on human strengths, augmented by AI/ML and a customer portal with clear data visualization and tailored recommended threat resolutions, will be well-positioned with cybersecurity buyers.

The pace of change in the threat landscape is rapid and MXDR Services must continue to evolve to keep organizations secure. New advancements in AI/ML, as well as in cloud services and OT, provide both new challenges and new opportunities for organizations.

NCC Group is an MSS provider with over 25 years of experience providing security services to businesses. Its customers have a choice of platforms and can create unified visibility across endpoints, networks, and cloud. NCC Group leverages the detection platforms of its partners and its proprietary network sensor technology. It integrates the information from those platforms

into its Unified Cyber Platform to create a broad view of the customer's IT environment — and a single source of truth.

It has just built and released its new customer portal. The portal provides clear and immediate access to a wide variety of threat information relevant to the customer, enabling them to act promptly to security events. NCC Group stresses how its services are intended to work with organizations' existing security environments, reducing requirements for new investments.

NCC Group is named as a Major Player in the IDC's MarketScape: Worldwide Emerging Managed Detection and Response Services 2024 Vendor Assessment.

MESSAGE FROM THE SPONSOR

NCC Group's Unified Cyber Platform (UCP) … Your Cybersecurity Streamlined in One Place

NCC Group's UCP is a vulnerability and threat management platform powered by human expertise and AI. The UCP underpins our MXDR solutions to provide faster time to value and better detection, all with a cost-effective approach. It enables unified visibility across endpoints, networks, operations, and cloud environments by integrating partner detection platforms with our proprietary network sensor technology. It can be tailored to your requirements, as it supports multiple solutions and log sources.

We start with native capabilities and enrich these with our own intellectual property. We leverage the resulting insights, intelligence, and innovation across all of NCC Group's capabilities, from threat intelligence to incident response, penetration testing, and vulnerability management.

Benefits of the UCP:

- Gain threat protection quickly from data discovery through to real-time protection from day one
- Ability to integrate new technologies and leverage current technology investments
- Reduce time to detect, isolate, and remediate
- Save time and resources to maximize productivity
- Customize your implementation, delivery model, and portal presentation

About the Analyst

Richard Thurston, Research Manager, European Security Services

Richard Thurston leads IDC's European Security Services program. He has 20+ years of experience in the technology sector, working as a journalist and analyst (including in IDC's Infrastructure and Telecoms team), working for U.K. regulator Ofcom, and serving in a number of research, insight, and thought leadership roles in cybersecurity and communications service providers. Richard is based in the U.K. and holds a degree in Mathematical Statistics and Operational Research and a diploma in Economics and Econometrics from the University of Exeter.

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 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.), the world's leading tech media, data and marketing services company.

IDC U.K.

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.