opentext™

Managed XDR: Attainable extended detection and response (XDR) for forward-thinking security teams

Contents

Executive summary

Securing enterprise technology environments to protect high-value information assets has never been easy, but it continues to grow more challenging. IT ecosystems are becoming more dynamic, distributed and complex. It is increasingly difficult for security practitioners to maintain visibility across them. As core business processes become more and more dependent upon digital technologies, it is increasingly important to protect corporate technology assets from sophisticated cyber threats.

Cybersecurity vendors have put forth a multitude of tools and products in their efforts to address the increasing complexity of IT environments. Among these, extended detection and response (XDR) is one of the most promising, largely because it ties all of the others together into a comprehensive solution that is greater than the sum of its parts.

XDR is still emerging as a market category, and confusion about how it should be defined and what capabilities it should encompass remains prevalent. With these uncertainties, security operations center (SOC) leaders are struggling to identify the right technology investments. Meeting their requirements without sacrificing detection accuracy or rapid response capabilities is critical. Unfortunately, they sometimes end up chasing the latest and greatest technologies that may dilute, rather than enhance, the efficacy of their SOC. Improvements in efficiency and cost reductions are often what their systems need instead.

XDR can deliver the efficiency and productivity gains that security leaders are hoping for. However, it can only do so if they follow the right strategy, one that manages the inherent complexity of this new approach.

Managing XDR's inherent complexity requires the right expertise and skills to oversee its successful execution. Unfortunately, many organizations don't have the necessary resources, knowledge or technology budgets. As a result, Managed Extended Detection and Response (MxDR) services are quickly gaining traction as an attractive approach to XDR. MxDR provides the expertise and capabilities organizations need, making XDR's benefits accessible to a far larger audience.

This paper will explain the rise of MxDR. Drawing upon original research on the state of the XDR market. It will also offer recommendations on what to look for in a best-in-class MxDR solution.

Introducing XDR

The cybersecurity marketplace has never been more crowded or confusing. The total number of companies in the market is estimated to be more than 39,000.[1] Given the plethora of available products and services, one might think that organizations would be better able to defend their technology assets than they were in the past.

Recent data breach numbers tell a different story. According to Forrester Research, 63 percent of surveyed organizations were breached within the last 12 months, a four percent increase from the previous year.[2] The victim enterprises spent an average of $2.4 million investigating and recovering from each of these incidents. The number of successful ransomware attacks also continues to grow. IDC Research estimates that approximately 37 percent of global organizations were the victim of some form of ransomware in 2021.[3]

The damage caused by these cybercriminal activities is extensive and familiar, encompassing:

- Financial harm, including lost business and customers, ransomware payments and costs associated with incident response and recovery.
- Lost data, including intellectual property and its associated competitive advantage.
- Lost productivity.
- Compliance penalties.

Enterprise leaders understand the financial risks posed by cybercrime are severe. As a result, they continue to invest heavily in cybersecurity products and services, with the average business spending between six and 14 percent of its total technology budget on cybersecurity.[4]

However, are these companies realizing the value they sought from these investments? Does the real-work risk reduction measure up? These remain open questions.

Certainly, enterprise technology ecosystems have grown more complex, compounding the challenges involved in monitoring and maintaining visibility across them. Cloud adoption, the hybrid workforce and core business processes becoming more dependent on digital technologies have created more distributed, complex and highly dynamic environments. It is more difficult to detect and respond to threats rapidly and effectively.

CISOs and decision makers continue to look for technological solutions to this problem. Given the talent shortages that have long troubled the cybersecurity field, there is great interest in tools and solutions that can add efficiency to operational workflows, making it easier for small security teams to defend diverse and ever-changing IT ecosystems.

An emerging technology category that's quickly gaining traction in the marketplace, Extended Detection and Response (XDR), promises to resolve at least some of these challenges.

[1] Ciso Portal, How Many Cybersecurity Companies We Have? (2021)

[2] Forrester Research, 2021 State of Enterprise Breaches Report. (2022)

[3] IDC Research, IDC's 2021 Ransomware Study: Where You Are Matters! (2021)

[4] Deloitte Insights, Reshaping the cybersecurity landscape: How digitization and the COVID-19 pandemic are accelerating cybersecurity needs. (2020)

To realize its full promise, organizations need to understand exactly what XDR is—and what it isn't. This isn't a simple proposition, given the amount of noise within the marketplace, where vendors and analysts continue to debate the relative merits of their favorite products with increasing fervor. Organizations also need access to the necessary resources, capabilities and budget to manage, integrate and maintain this complex technology—a tall order for resource-strapped security operations centers. Increasingly, they are turning to Managed Extended Detection and Response (MxDR) service providers as a viable means of realizing the full benefits of XDR, especially for small and mid-sized organizations with lean security teams.

XDR challenges and stumbling blocks

To better understand the state of the market for this emerging technology and how its adoption is progressing, OpenText partnered with CyberEdge Group to conduct a global survey of security leaders and practitioners. People involved in security technology selection and procurement decisions, as well as those who work with these tools daily, were interviewed. Respondents included qualified information security operations executives, managers, directors, analysts and engineers, as well as incident responders and compliance auditors.

While enthusiasm for XDR is running high, information security staff don't have consistent expectations of what this technology should include—or which tools and telemetries should be integrated with it. XDR is perceived to be complex to implement and manage, and many organizations feel they will need expert assistance managing their XDR deployments as this technology moves into the mainstream. Thus, services and solutions that make its benefits more accessible are in demand.

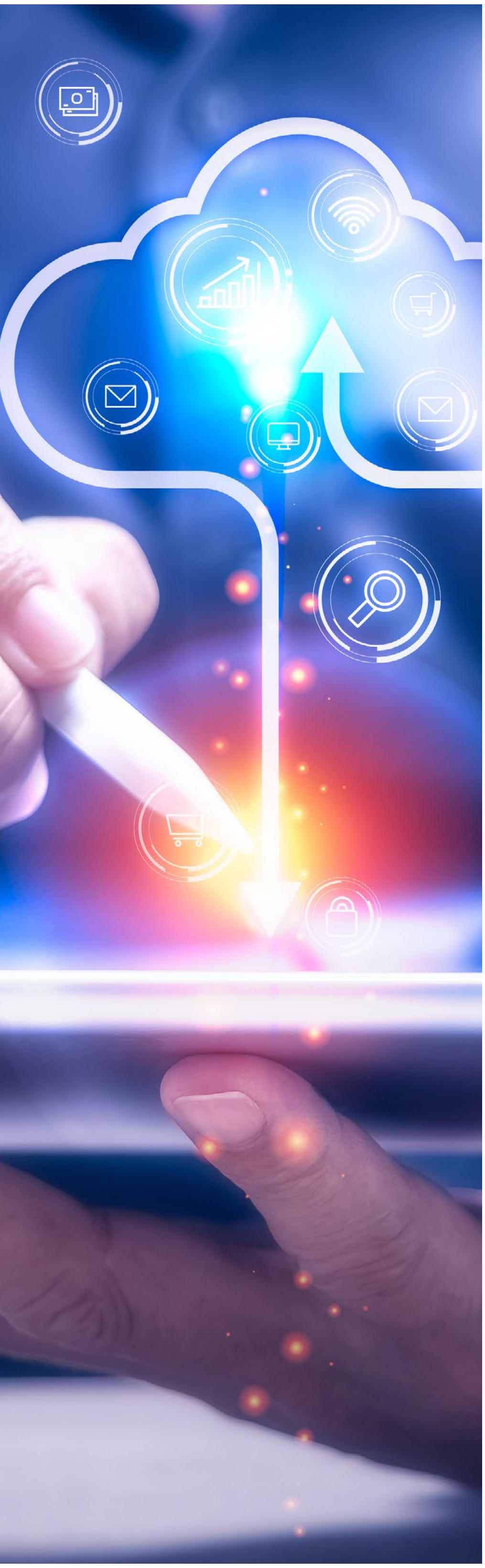
Organizations are unsure of what to expect from XDR

In recent years, XDR has received a great deal of analyst and media attention. It promises to improve efficiency in security operations, as well as enhance visibility and response capabilities. Resource-constrained security programs are sorely in need of greater proficiency in these areas, so it is unsurprising that XDR is generating so much buzz.

Survey respondents appeared to be aware of XDR's potential benefits. More than 98 percent reported that their organization either already had an XDR solution in production or was planning to acquire or implement one. This is a higher market penetration rate than analyst firms are observing but may reflect the relatively high levels of sophistication within the survey audience, nearly half of whom (49 percent) are working in organizations with more than 5,000 employees.

However, such high adoption rates also invite the question: what is it, exactly, that these security teams are interested in deploying? The term "extended detection and response" is said to have been coined in 2018,[5] but definitions of the concept still vary. Some market analysts describe it as an iteration upon endpoint detection and response (EDR), which extends EDR's threat detection and response capabilities to the network layer, as well as across other signal sources (such as email and the cloud). Others emphasize its status as an alternative to traditional security information and event management (SIEM) platforms, while others suggest that XDR can complement and enhance a SIEM's capabilities.

[5] Forrester Research, XDR Defined: Giving Meaning to Extended Detection and Response. (2021)



What is XDR? Analyst firms weigh in:

Gartner: “Extended detection and response is a platform that integrates, correlates and contextualizes data from multiple security prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple point solutions and advanced analytics to correlate alerts from multiple sources into incidents.”[6]

Forrester: “[XDR is…] the evolution of EDR, which optimized threat detection, investigation, response and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.”[7]

IDC Research: “The extended detection and response (XDR) cybersecurity software stack… brings in telemetry from the endpoint, logs, web/email, and threat intelligence on one dashboard. Open questions remain about what else should go onto the stack, if best-of-breed point products can be integrated successfully, and what else can be done within compliance frameworks.”[8]

These varied and competing definitions reflect the fact that there is no single, clear industry standard for which capabilities and telemetries must be included in an XDR solution. This uncertainty was reflected in survey participants’ responses as well. When asked about the capabilities of 18 different security tools, almost every one was seen as important to include in an XDR solution by about one-third of the respondents.

The most often-cited capabilities were those of endpoint detection and response (EDR) products (mentioned by 43 percent of participants), data loss prevention (DLP) tools (40 percent) and network detection and response (NDR) (also 40 percent). However, more than 33 percent of respondents said that as many as 10 different capabilities were important to include.

[6] Gartner, Market Guide for Extended Detection and Response. (2021)

[7] Forrester Research, XDR Defined: Giving Meaning to Extended Detection and Response. (2021)

[8] IDC Research, Extended Detection and Response – The Must-Have Security Tool in a Digital-First World. (2022)

Which of the following security tools should be provided by every best-of-breed XDR vendor as part of a cohesive, unified security incident detection and response solution? (Select all that apply.)

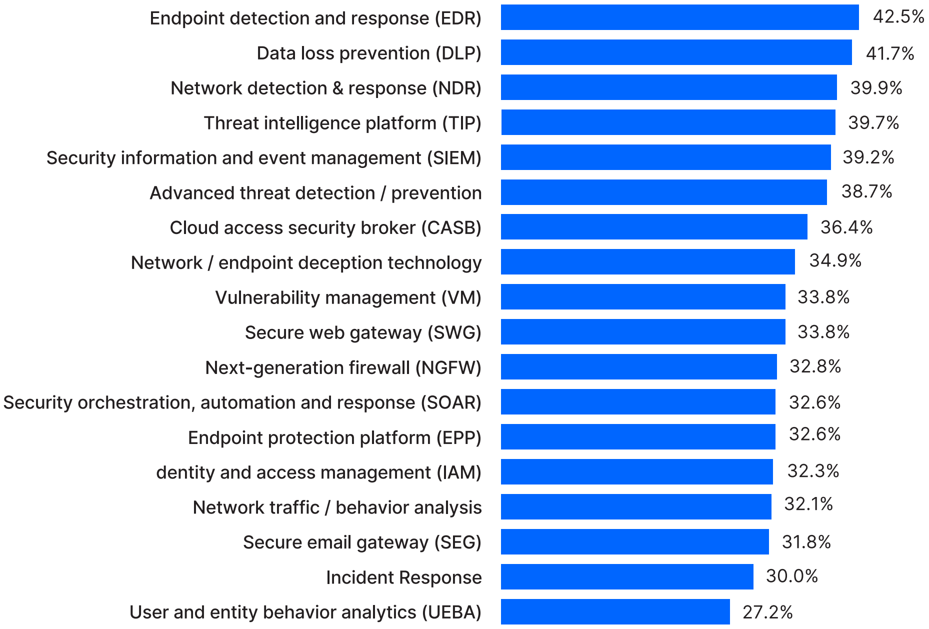


Figure 1: Tools that should be provided as part of comprehensive XDR.

The struggle to find expertise

The survey revealed that concerns about XDR's perceived complexity are widespread. This comes as no surprise. After all, it has been reported that there is an estimated global shortage of 2.72 million cybersecurity professionals, and expertise managing security analytics in the cloud is particularly difficult to come by.[9] Even among survey respondents, who tended to be employed by larger and relatively well-resourced security programs, more than 73 percent reported that their organization was struggling to fill at least some information security positions.

To ease the burden posed by the cybersecurity skills shortage, organizations are looking for XDR solutions that are simple to operate and well supported. When asked what was most important to them in an XDR solution, more than half of respondents cited ease of use. The second-most-common choice was excellent customer support from the solution's vendor.

Which of the following factors are most important when evaluating XDR vendors?

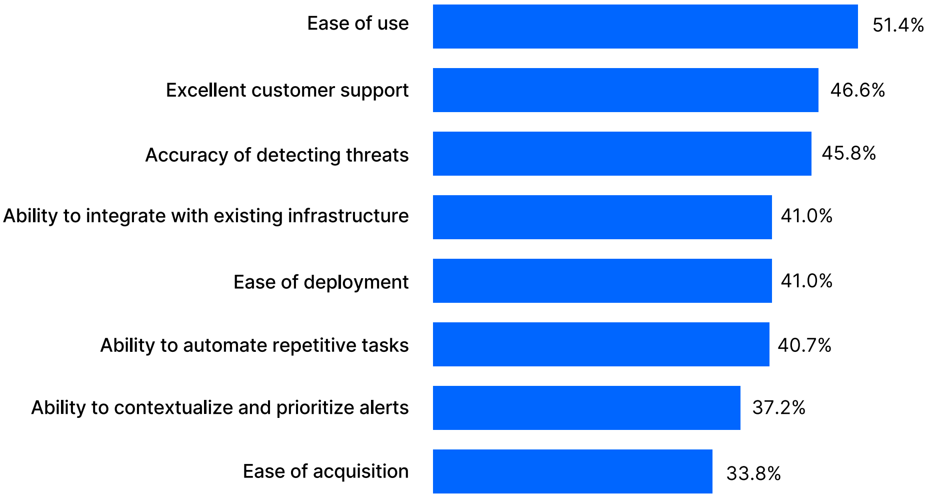


Figure 2: Most important factors when evaluating XDR vendors.

Organizations are not necessarily wrong to have worries about the complexity of XDR. Bringing in an unlimited number of additional telemetry sources can be a problem - particularly if they are not being ingested into a properly-tuned SIEM or if analyst teams aren't leveraging analytics to assist in triage - can quickly lead to overwhelming false-positive alert volumes. To some extent, this is again a question of definitions: without consensus in the market on exactly what is and is not part of XDR, it is impossible to measure how complicated the solution would be to manage.

The reality is that deploying, implementing, tuning and managing an XDR solution can in fact be complex. There's a need not only for security analyst expertise for round-the-clock monitoring, but also for content creation skills (in writing detection rules) and expertise in operating the analytics and integrating various components of the security technology stack.

[9] (ISC)2, Cybersecurity Workforce Study. (2021)

Building the right XDR strategy

While multiple vendors are promoting XDR as a one-size-fits-all, single-vendor solution set, the reality is that none yet offer best-of-breed capabilities across the entire security incident lifecycle. Although a single-vendor strategy might simplify the process of building integrations, it is also likely to be expensive depending on how much of the existing security stack would need to be replaced. Unfortunately, integrating multiple components from different vendors adds yet more complexity.

This tradeoff is likely to be a familiar one for security staff. Additional coverage, such as adding network detection and response (NDR) to an EDR solution, for instance, improves visibility and control. Unfortunately, it can also raise costs and increase the false positive rate. XDR's greatest promise is that it may make it so that security leaders no longer need to choose between coverage and cost. However, that is only possible if the solution is simple enough to manage and monitor, or if the right third-party assistance is available to help.

Ninety-three percent of survey participants voiced a strong belief that XDR could help their organizations mitigate the risks of advanced cyber threats while 99 percent expected XDR would lower security operations costs.

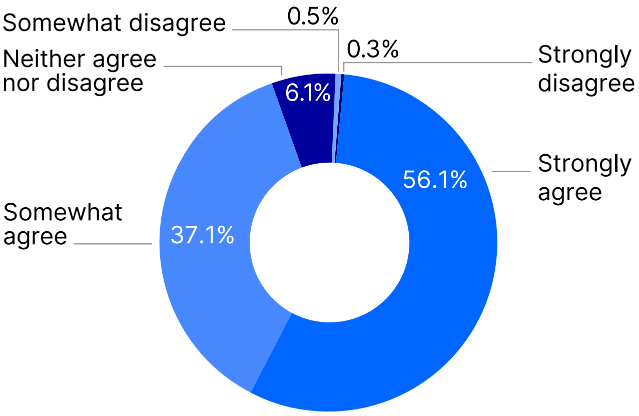


Figure 3: Percentage of organizations who agree or disagree that XDR can improve their organization's ability to mitigate risks while lowering costs.

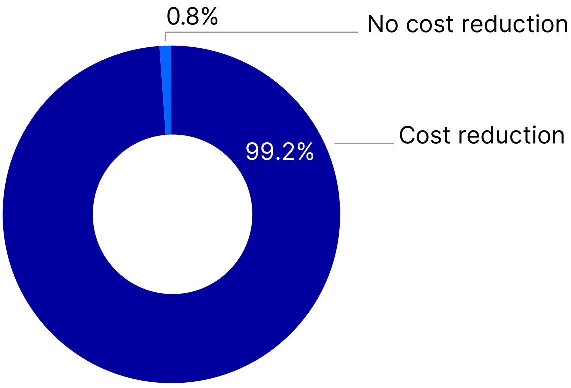


Figure 4: Percentage of organizations expecting to see a cost reduction from XDR's adoption.

This optimism isn't misplaced. XDR can generate large downstream efficiencies that lead to cost savings while improving coverage, detection accuracy and the ability to respond to threats. However, achieving this result requires the right XDR strategy. For success, organizations will need a roadmap: they need to understand which XDR use cases are most important for their unique threat profile, how they'll integrate the necessary telemetries and how they'll monitor the XDR platform.

Key questions to ask when considering an XDR solution:

- How many XDR components or integrated security tools can be monitored from within a single dashboard?
- How readily can our existing security operations team orchestrate response actions within the platform?
- Do we need help building playbooks?
- How many known attack tactics, techniques and procedures (TTP), including those mapped in a standard reference framework like MITRE ATT&CK®, can that XDR platform identify?

Realizing XDR's promise in the real world with MxDR

Among survey participants, outsourcing the management and monitoring of an XDR solution is becoming an increasingly attractive proposition. More than 94 percent said they outsource the monitoring and management of their XDR solution to a managed extended detection and response (MxDR) provider or are planning to do so in the future. When coupled with the high XDR adoption rates and planned adoption rates among the survey participant sample, these numbers are particularly striking.

Of course, outsourcing is frequently leveraged to address the cybersecurity skills shortage. There continue to be large numbers of unfilled positions in the field all around the world, experienced analysts remain hard to come by and professionals with skills in detection engineering and security tool integration—which are needed to implement and manage an XDR solution—are scarcer still.[10]

Leveraging MxDR gives an organization access to expertise, knowledge of best practices and shared efficiencies—capabilities that are challenging to hire for, but relatively easy to access through a leading provider. Especially for small and mid-sized organizations with less mature security programs, this represents an efficient way to overcome the major roadblocks associated with XDR adoption. Even for organizations with limited budgets, MxDR can increase efficiencies so much that they'll quickly see value.

Not only can an MxDR provider supply 24×7 monitoring capabilities, they can also bring expertise in managing incidents all the way through resolution. This means they will be able to shore up existing security programs in the areas where aid is most needed. It also means that they will provide the skills needed to take full advantage of the visibility and detection accuracy that XDR can provide.

[10] ISACA, State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations.

"XDR can equate to better visibility and better detection," says Marc St-Pierre, global head of cybersecurity services at OpenText. "It can also reduce false positive rates, because if you're pulling in telemetry from the endpoint and XDR allows you to cross-check your findings against multiple other sources that you're correlating, you can have much greater confidence that something did or did not happen. It gives you that validation, which adds up to fewer false positives."

Biggest benefits of MxDR:

- Enhanced visibility from endpoint to network to proxies, email and Software-as-a-Service (SaaS) application logs
- Efficiencies of scale across the entirety of security stacks
- Augmentation of capabilities with top-notch expertise, including in areas like incident response and threat hunting
- Economies of scale make advanced capabilities affordable
- Access to cutting-edge technologies such as artificial intelligence (AI)-driven analytic workflows that would otherwise be within reach of only the most mature (and best-funded) security operations programs

What to look for in an MxDR provider

As XDR grows in popularity, it is likely that the number of vendors tailoring their managed service offerings to support XDR platforms will increase as well. After all, the market for managed security services continues to experience what Forrester Research calls "hypergrowth" even as companies seek out more specialized detection and response capabilities to help them bridge the talent gap.[11]

Deep bench of expertise in multiple tools, platforms and multi-vendor integrations

Not all managed security service offerings are created equal. MxDR requires extensive knowledge of multiple tools, platforms and multi-vendor integrations. This means it demands a deep bench of expertise in a broad array of areas—expertise that a newer market entrant may not have in house. This expertise should include proficiency in security monitoring, but should also span threat hunting, detection engineering, incident response and forensics. The key is to be able to not only identify and remediate risks, but also rapidly respond to threats all the way through the incident lifecycle to full resolution and restoration of operations.

Ability to leverage security tools already in place

Not every MxDR vendor supports all vendors' technologies. Look for one that can leverage the security tools already in place, rather than forcing the organization to spend more by taking a rip-and-replace approach. Those that have experience tuning and managing an extensive array of commercial security solutions from different vendors enable a best-of-breed approach. Organizations can leverage their custom-built capabilities or evolve the security stack over time—whatever approach best supports the organization's XDR strategy and budget.

[11] Forrester Research Understanding Today's Security Services: MSS, MDR and SOCaaS. (2021)

Reduction in false positives to focus on hunting for and investigating threats

In addition, look for an MxDR provider whose security operations team will spend most of its time on high-value activities such as hunting for and investigating real-world threats, not one who will get bogged down with false positives. False positive alerts are all too common in security operations. An MxDR provider with a platform that leverages behavioral analytics to detect the attack tactics, techniques and procedures (TTP) outlined in the MITRE ATT&CK framework and that uses advanced machine learning to reduce the noise will see far fewer of them. When a security operations team can spend more of its time identifying and remediating real risks, the time-to-value for MxDR will shrink dramatically.

Optimization of log collection, monitoring and retention

The promise of XDR is that a security program can extend the visibility and response capabilities that EDR offers far beyond the endpoint. This means collecting and monitoring more logs, of course. A top-notch MxDR vendor will have the necessary expertise to tell organizations exactly which logs they should collect and monitor, and how long the retention periods should be. This is a complex problem, especially extended across the diverse attributes that logs from various cybersecurity vendors, cloud platforms and SaaS products have. Optimizing log collection and retention helps ensure maximum value from XDR investments.

MITRE ATT&CK Evaluations

The MITRE Engenuity ATT&CK® Evaluations program provides transparent and impartial insights into how well managed detection and response providers' capabilities perform and how well they are able to analyze adversary behavior. During the 2022 ATT&CK® Evaluation, MITRE Engenuity recognized the high quality of OpenText™ Managed Extended Detection and Response (MxDR), noting quick detection of real incidents and recording a 100-percent detection rate for all attack tactics. Throughout the evaluation, OpenText MxDR did not generate any false positive alerts and did not incorrectly report any threat behavior, showcasing its ability to minimize noise for overwhelmed and understaffed security teams. OpenText demonstrated its capabilities against threat actors known for evasive techniques, complexity and persistence.

The MITRE Engenuity 2022 ATT&CK® Evaluation recognized OpenText MxDR for quick detection of real incidents and a 100-percent detection rate for all attack tactics.

Managed Extended Detection and Response | OpenText

Conclusion

Detecting and responding rapidly to cyberthreats in enterprise IT environments will likely always pose challenges. Implementing the right security technologies can help minimize them so that security operations teams can finally begin spending most of their time on high-value activities—instead of being trapped with too many false positive alerts and too little time. In this sense, XDR does indeed have the potential to be a game changer for the efficiency of security operations, and MxDR can supply the expertise needed to transform this potential into reality.

OpenText Managed Extended Detection and Response (MxDR) reduces noise by 97 percent and detects 99 percent of threats.[12] As a fully outsourced service, OpenText MxDR integrates with leading vendors' technologies to secure more than 137 million endpoints around the world. OpenText MxDR security professionals have decades of expertise in threat hunting, breach response investigation, malware analysis, digital forensics and incident response. This deep expertise provides security teams with a unique understanding of threat actors' behavior, enabling them to custom-build tactics, techniques and procedures (TTPs) that are used in advanced threat modeling algorithms. With this foundation of experience and technical proficiency, OpenText continuously improves its detection and response capabilities to accelerate time-to-value.

Interested in digging deeper into our research? Download the full survey report to learn more.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

[12] ATT&CK Evaluations for Managed Services, November 2022, https://attackevals.mitre-engenuity.org/managed-services/oilrig/

opentext.com/contact