AN INTRODUCTION TO
NEXT-GENERATION MDR

KUDELSKI
SECURITY

Navigating XDR: How to Close the Cyber Maturity Gap With Next-Gen MDR

Content

Executive Summary

If your're anything like most organizations with a large cybersecurity program, you'll know that not all cybersecurity solutions are created equal.

In an evolving security technology environment, a solution has evolved that has the potential to drive a new level of value: extended threat detection and response (XDR).

This guide takes a deep dive into XDR, and looks at what makes this solution one of the best ways to effectively defend against a wide range of cyber-attacks.

What is Extended Detection and Response (XDR)?

Extended Detection and Response (XDR) solutions connect to every element of your IT infrastructure, bringing together the data from across your different systems to correlate and enrich it. From there, your XDR solution works to automatically detect threats, prioritize them by severity, and alert IT security teams to take action. It can even trigger automated workflows—a series of preset actions, including alerts and task setting—to automate standard response procedures and minimize manual intervention.

XDR offers real-time monitoring of every IT system or endpoint used in your business. It is a 'single source of truth' for the security health of an organization's entire network that can be viewed through a central portal.

Open vs Native XDR Solutions

There are two primary types of XDR solutions: open and native. While they offer the same level of cybersecurity coverage, there are some key differences between how the two are delivered and integrated.

Native

Native XDR solutions are built on a centralized platform and offer a unified suite of security tools. Native XDR is typically delivered by a single XDR vendor, and they provide all necessary hardware and software.

The main benefit of a native approach to XDR is that there will be tight integrations between the various tools as they're all provided by the same vendor. This means internal IT teams won't have to worry about spending time configuring and integrating those technologies. It also simplifies the process of adding additional security tools to a native XDR platform (assuming they're from the same vendor).

The risk here is that you can become locked into a specific vendor if the cost of migrating the entire cybersecurity system to a new provider becomes too high and difficult to justify. This could also result in gaps in your cybersecurity if that particular vendor doesn't offer a particular solution and the native XDR platform can't integrate with solutions delivered by a different vendor.

Open XDR

In contrast, open XDR solutions integrate security tools from various vendors into a unified XDR platform.

The drawback of open XDR is that these integrations are complex and time-consuming to put into place. What's more, because solutions from different vendors won't necessarily offer 'out of the box' integrations, there may be issues with vendor support if they haven't been configured properly.

What's the Difference Between XDR and EDR Solutions?

Unlike Endpoint Detection and Response (EDR) which—as you may have guessed from the name—focuses on securing endpoints, XDR goes further. It provides holistic protection against cyber threats and attacks by expanding its scope beyond monitoring endpoints to include other aspects of your organization's IT infrastructure, like cloud environments and email systems.

EDR is one of the key elements of an XDR solution, and many organizations rely on EDR alone for their cybersecurity. An endpoint is defined as any physical device connected to your network, such as a desktop computer or a mobile device. Successful attacks on endpoints have been increasing in recent years. According to IBM 84% of security professionals believe the majority of attacks originate from the endpoint. For this reason, EDR is often considered the core of an effective cybersecurity strategy.

While monitoring endpoints provides a solid foundation for an organization's cybersecurity, it doesn't put endpoint activities into a broader context. This is where an XDR solution comes into play, offering comprehensive coverage across your entire IT infrastructure. XDR solutions encompass endpoints network, servers, cloud applications, emails, and more. Whether open or native, XDR also brings all of that data into one place, making it much easier for security teams to correlate and quickly identify and resolve threats.

How do EDR and XDR Solutions Differ From MDR?

If Endpoint Detection and Response (EDR) focuses on monitoring, detecting, and responding to threats specifically on endpoint and if Extended Detection and Response (XDR) provides a broader scope by integrating and correlating data from multiple security layers, then what is Managed Detection and Response, or “MDR”?

MDR is an outsourced service that provides specialized monitoring, threat hunting, and incident response to detect and address security threats across an organization’s IT infrastructure. MDR providers often use XDR, which integrates data from various sources like endpoints, networks, servers, cloud applications, and emails into a unified view. This integration enables MDR to offer comprehensive threat detection and response, leveraging advanced analytics and automation for more effective threat management.

MDR provides a broader, more coordinated approach by covering multiple security layers across the entire IT environment. This makes MDR a more holistic solution that takes into account an organization's individual context, offering more accurate detections and more efficient responses to security incidents, ultimately enhancing an organization's overall security posture.

MDR allows an organization to benefit from the monitoring of an EDR or XDR solution, while reducing the cost and complexity of building out an in-house security operations centre (SOC). It’s an approach that might be preferential for organizations without the requisite in-house skills or expertise to start from scratch.

The Benefits of XDR in Modern Cyber Defence Strategies

XDR is the cybersecurity solution of choice for modern cyber defence strategies because of the comprehensive visibility it provides, and there are several key benefits when implemented correctly.

Identify known and unknown threats

Threats target every part of your network, not just endpoints. XDR uses AI and machine learning to understand what normal behavior looks like across your environment. This enables it to effectively identify known threats, like malware with known signatures or attack patterns, and unknown threats, such as new or emerging tactics. By detecting behavioral anomalies whether it's unusual user activity, suspicious data movement, or abnormal network traffic, XDR flags both familiar and novel threats. This makes XDR highly effective at identifying and responding to attacks, whether the threat is known or not.

Respond automatically to threats

Automatic responses can be set up to swiftly and programmatically react to certain threats, ensuring standard procedures are adhered to. Your IT team is freed up to spend their time on more significant issues that most benefit from human attention.

Fewer false positives

XDR can automatically filter for potential threats so that your IT team is distracted by fewer false positives and can focus effort where it really counts. Having to review every minor potential threat indicator risks alert fatigue, which in turn, creates the potential for serious issues to slip through the cracks.

XDR improves over time

Thanks to machine learning, XDR can improve its detection and response capability over time as it's provided with more data about what's normal and abnormal across your network. The more data you provide your XDR solution with, the more protection and actionable insights you get out of it.

Lighter on your systems

XDR can be managed from a single dashboard, reducing the total number of software tools required and speeding up processes.

Supports regulatory compliance

Organizations face increasingly stringent compliance obligations around cyberattacks and data breaches. For example:

- Health Insurance Portability and Accountability Act (HIPAA) in the US
- Financial Industry Regulatory Authority (FINRA), a self-regulatory organization, also operating in the US
- General Data Protection Regulations (GDPR) in the EU and UK

Being able to demonstrate that your organization has taken all necessary steps to protect personal data and sensitive information, can help with compliance as well as avoiding the financial penalties that come with data breaches. XDR supports this by highlighting those attacks at the earliest opportunity, while significantly reducing the chances of those attacks being successful.

XDR integrates data from multiple security layers (e.g. endpoint, network, cloud, etc.). In addition to automated correlation, it uses machine learning and AI as well as anomaly detection, to identify threats more comprehensively and across the entire IT ecosystem.

MDR relies on expert human analysis aided by contextual awareness, signature-based detection, threat intelligence, and behavioral analysis to identify known threats and spot anomalies indicating unknown threats.

The result: more accurate threat detection and faster response.

Customization and scalability

Because the solutions leveraged within XDR are cloud-based it is simple to scale the system as required. You can add new data sources, ingest increasingly large volumes of data generated by diverse security tools, and devise custom rulesets designed to suit the organization.

Capable XDR platforms also include or benefit from integrations with various security tools across different categories, not just endpoints, which provide a comprehensive and unified threat detection and response solution:

- **Network Security:** Integrations with network security tools such as firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Network Access Control (NAC) solutions help monitor network traffic, detect suspicious activities, and enforce security policies across the network, broadening the scope of threat detection beyond just endpoints.

- **Cloud Security:** Integrating with Cloud Access Security Brokers (CASB) and Cloud Workload Protection Platforms (CWPP) secures cloud environments, allowing for monitoring cloud applications, data, and workloads, ensuring threats within cloud infrastructures are identified and mitigated.

- **Security Information and Event Management (SIEM):** Integrations with SIEM systems allow for the ingestion and correlation of logs and events from various sources, helping to identify complex threats that span across multiple security domains and providing a centralized view of security incidents.

- **Threat Intelligence:** Integrations with threat intelligence platforms leverage global threat data and insights, enhancing the ability to identify emerging threats and correlate them with internal data to detect potential risks.

- **Application Security:** Integrations with tools like Web Application Firewalls (WAF) and application security testing solutions monitor and protect applications from vulnerabilities and attacks, providing security coverage for web applications and services.

- **Identity and Access Management (IAM):** Integrating with IAM solutions such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) allows for monitoring and securing user access and identity management, helping to detect and prevent unauthorized access.

- **Data Security:** Integrations with Data Loss Prevention (DLP) tools allow for monitoring and protecting sensitive data, ensuring that data breaches or leaks are quickly detected and mitigated.

- **Vulnerability Management:** The possibility to continuously monitor and assess vulnerabilities within an organization's infrastructure is possible through integration with vulnerability management tools. Prioritization and response to threats, based on the criticality of identified vulnerabilities, is then possible.

- **Email Security:** Integrations with email security tools help monitor and protect against phishing attacks, malware, and other email-based threats, ensuring secure communication channels.

- **Mobile Security:** Integrating with mobile security solutions extends protection to mobile devices, monitoring and securing mobile endpoints against potential threats.

This flexibility means a well-configured XDR solution is ideally placed to adapt to new types of threats and attack vectors.

Is Your Organization Ready for XDR?

Although XDR offers a wide range of benefits, it only does so if it's been implemented correctly. The integration process can be complex, and can leave your organization vulnerable to cybersecurity attacks if not done right.

How should you prepare for effective XDR implementation?

Ahead of deploying an XDR solution, there are several steps your organization should take to prepare the team to ensure the platform is integrated effectively.

- **Establish a company-wide data handling policy:** One of the key goals of an XDR solution is to protect a company's sensitive data, and its configuration should be informed by your data handling policy. This policy should identify the most sensitive data to ensure it can be effectively secured, while the process will also identify the key assets that require protection.

- **Put together an XDR Implementation Team:** Whether it's led by your Chief Information Security Officer, Chief Technology Officer, Head of IT or simply an individual with the best knowledge of the IT infrastructure and its components, an XDR Implementation Team will be tasked with effectively implementing the XDR solution. By creating a dedicated team, you also ensure each of the key stakeholders has visibility into the implementation process.

- **Identify who will 'own' the XDR system:** Will you need to dedicate in-house resources to to maintain, monitor, and operate the XDR solution, or will you leverage a Managed Detection and Response (MDR) approach?

- **Identify required features:** XDR offers a wide breadth of cybersecurity tools, but you won't necessarily require every potential feature. The organization needs to be aware of how each feature helps achieve its business objectives. If you're working with a managed vendor, they will be able to support this process to make sure you're not investing in features you don't need.

Best practices for smooth XDR deployment

In order to smoothly and successfully deploy an XDR solution, follow these best practices:

- **Communication is key:** Maintain regular communication with key stakeholders to ensure they fully understand the benefits of XDR, and how its implementation will impact their role.

- **Identify all data sources:** All of your organization's data sources should be inventoried so you're clear on the location of all sensitive information, including cloud and on-premises endpoints. This is an essential step in order to identify the assets that need to be configured.

- **Deliver a phased rollout:** The integration of existing cybersecurity solutions with the XDR solution can be complex, so it's best to use a phased rollout. This not only allows users to gain experience of using the platform, but also makes sure everything is working correctly with the integrations before you add another data source.

- **Response playbooks:** Define your response processes while integrating new data sources with the XDR platform. What's automated and what needs to be actioned by the security team? The playbooks should be documented and made available to the key stakeholders, and training should be given for each use case.

Implementation mistakes to avoid

There are a few common issues that can arise while implementing an XDR platform.

- **Lack of integrations:** Some XDR platforms may not integrate with one or more of your existing security tools, which means the XDR solution won't be able to provide threat detection for a particular part of your network. For example, it's unlikely XDR will cover Operational Threat Intelligence (OTI), so you'll need to determine if this data can be collected through integrations with other platforms. This issue will arise if you haven't done the initial preparatory work of identifying exactly what you need from your XDR solution, or you've neglected a specific requirement during your vendor selection process.

- **Poor vendor selection:** Even if a vendor claims to offer full coverage, this doesn't necessarily mean it's done effectively. For example, if XDR components were acquired as part of a large acquisition by the vendor, resources may not necessarily have been invested to integrate them properly. Make sure you are thorough and diligent during the vendor evaluation and selection process to develop a clear understanding of how a specific vendor's solution meets each of your requirements.

- **Not prioritizing team buy-in:** Remember that the new XDR solution will be at the heart of your cybersecurity efforts. If you've not spent the time securing the buy-in of all key stakeholders, there might be issues with the implementation or use of the system once it's in place.

What's the Future of XDR?

Like any solution, XDR is expected to continue to evolve alongside the broader cybersecurity sector itself, and be impacted by similar trends.

Vendor consolidation

It's likely we'll see increased vendor consolidation by organizations looking to reduce costs and simplify vendor management. This trend will benefit experienced and specialist cybersecurity vendors that offer comprehensive solutions.

Increased dominance of cloud-native solutions

As an organization grows, its XDR solutions need to be able to scale with it. This can present challenges which are helped by cloud-native solutions that are designed to be more scalable, while enabling customers to purchase only what they need.

Using AI and machine learning to cut through the noise

AI and machine learning in XDR platforms reduce noise by filtering and prioritizing security alerts, minimizing false positives and focusing on real threats. They analyze and correlate data from multiple sources, understand normal behavior patterns to detect anomalies, and automatically triage alerts based on severity. Continuous learning and contextual awareness further enhance accuracy, allowing security teams to efficiently respond to genuine threats without being overwhelmed by excessive noise.

Why Kudelski Security?

Kudelski Security's MDR services are powered by our FusionDetect™ XDR Platform, which is operated by our 24/7 Cyber Fusion Center (CFC) team. This powerful technology takes a five-step approach to your cybersecurity:

1. **Collect Data**
   FusionDetect™ aggregates, normalizes and enriches security-relevant data across your entire network environment, ensuring a comprehensive view for threat detection.

2. **Enrich and Correlate**
   The system cross-correlates and maps attacker behaviors to MITRE ATT&CK® techniques. Combined with AI and machine learning this supports pattern recognition for faster, more accurate threat identification.

3. **Detect and Investigate**
   Our CFC analysts and threat hunters, supported by AI-enhanced tools, triage, investigate, and validate threats. The focus is on high-risk incidents, ensuring precise detection and minimizing false positives.

4. **Respond**
   FusionDetect™ automates initial responses and accelerates escalation with clear remediation guidance and hands-on expert support to minimize impact and speed recovery.

5. **Build Resilience**
   FusionDetect™ offers actionable insights and continuous learning to strengthen your cybersecurity posture amd help you move to a proactive security stance.

Kudelski Security offers flexibility in our **cybersecurity solutions:** you can opt for our standalone FusionDetect™ tools, or combine them with our managed services. Many clients prefer this integrated approach, as it allows our skilled professionals to collaborate seamlessly with your security teams, without the need for you to manage platform licensing or maintenance of the tools. Kudelski Security's MDR solution offers integrations with over 140 tools, so it provides comprehensive visibility across your IT environment.

Ready to find out how Kudelski Security can manage your threat detection and response with our dedicated MDR services? **Get in touch** with our cybersecurity experts today.

About the Author

Zrinka Maslic

Solution Architect at Kudelski Security

Zrinka is a Solution Architect and has worked since 2019 with Kudelski Security. She is based in the Zurich office, where she collaborates with Product Management and Go-to-Market teams to launch new products and services.

Her career in IT security and perimeter protection spans 20+ years, and she has held consultant, CTO, and CISO positions for a number of Swiss companies, building out managed security, technology, and operations services.

If you'd like to speak to Zrinka or need more information about XDR, **get in touch**

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

info@kudelskisecurity.com
www.kudelskisecurity.com
www.modernCISO.com

Contact Us

To learn more about our MDR services download our **factsheet.**

Disclaimer

The information in this document provides guidance on relevant technologies serving a specific enterprise security challenge. As each client environment and business need is unique, we do not warrant that these recommendations are appropriate in every instance. To clarify the appropriateness of a strategy or test the impact of a specific vendor, we recommend clients engage our presales solutions team for a more detailed analysis.