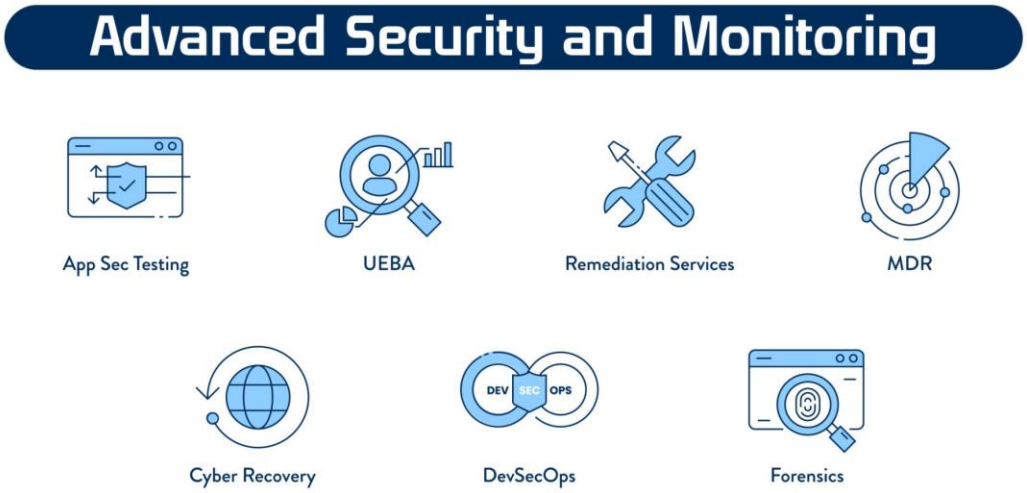
Quest Technologies Ltd
Smart Technology. Trusted Solutions.

**CYBER SECURITY 101**

# EDR vs. MDR vs. XDR: Choosing the Best Option




Cyber threats are getting smarter and traditional security tools are no longer enough to keep your organization safe. EDR, MDR, and XDR are three distinct technologies that play a vital role in safeguarding your users and assets. Cyber security can be confusing and data volumes are growing as we speak.

77% of security experts say that data leaks will occur more with the increasing use of Generative AI tools across industries. If you worry about your company's future, then enhancing cyber resilience is a high priority. Slow detection and response can cost you.

Over 50% of security leaders will invest in EDR, MDR, and XDR solutions. It's important to note that these three solutions are similar but work differently.

Don't wait around for your threats, because they won't wait for you to act.

Explore EDR vs. MDR. XDR solutions with us, compare their differences, and find out which ones are right for you.

## What is Endpoint Detection and Response (EDR)?

Endpoint Detection and Response captures all endpoint activities and uses advanced analytics to pinpoint anomalous behaviors across them. Security teams learn about the visibility of their endpoints and receive alerts regarding malicious events through EDR tools.

### Key Features of EDR

EDR offers the following key features to enterprises:

- Triages alerts and validates suspicious endpoint activities.
- Analyzes large data stores.
- Detects security events.
- Generates actionable threat intelligence.
- Generates appropriate and context-based threat mitigation responses.
- Gives deep visibility into multiple endpoints, including IoT devices, laptops, desktops, and others.

## What is Managed Detection and Response (MDR)?

Managed Detection and Response (MDR) is a special type of Security-as-a-Service (SaaS) offering where you employ dedicated security professionals to monitor and mitigate threats. Unlike other security automation tools in your arsenal, MDR adds a human element.

These experts review and take instant action on security events that are normally not caught by your existing stack. For threats that are evolving or if your tools are not accustomed or aware of the latest development, MDR can identify and eliminate them. MDR is a great way to boost your overall security maturity levels across the enterprise.

### Key Features of MDR

MDR brings security teams the following key features:

- MDR detects false positives and investigates alerts after it detects an incident. It provides proactive threat-hunting capabilities.
- It organizes security events, categorizes and prioritizes them, and lists them according to their risk levels. This helps security teams take action on the most critical ones first.
- MDR provides instant remediation and response to security events within a customer's network.

## What is Extended Detection and Response (XDR)?

XDR provides threat detection and response for cloud security tools, services, endpoints, and networks. It is an extension of traditional EDR solutions. XDR works best in complex and hybrid cloud environments and many companies request it as a software-as-a-service (SasS) offering.

### Key Features of XDR

Modern XDR solutions should offer security teams the following features:

- XDR solutions combine endpoint telemetry with data from logs and information security platforms. It detects a large number of threats, including evasive maneuvers which are normally invisible to other investigation methods.
- XDR applies context-based machine-driven analytics, reduces noise, and identifies the root causes of threats.
- XDR solutions also make smart recommendations and provide guidelines for queries and other response actions.
- XDR should be able to prioritize risks, guide responses, and generate multiple alerts.

## Critical Differences Between EDR, MDR, and XDR

The following are the critical differences between EDR vs MDR vs XDR solutions:

### 1. In-house Expertise vs. Security Automation

There is no need to hire security experts from outside your organization when you use MDR. It consolidates the use of both XDR and EDR tools, plus adds human expertise on top. MDR accelerates multi-domain threat analysis and can help secure firewalls, cloud security posture, sensors, networks, and any other elements of the company's IT Infrastructure.

### 2. Data Ingestion and Threat Visibility

XDR generates multi-domain security telemetry and streamlines security data ingestion, analysis, and workflows. It provides unified response capabilities and enables access to top-tier threat intelligence. XDR can enhance visibility across entire enterprises and provide detailed network traffic security analysis. Another key benefit of XDR over MDR and EDR is that it accelerates security operations and unifies organizations' cyber security strategies.

### 3. EDR vs MDR vs XDR: Integrations

EDR, MDR, and XDR solutions can integrate seamlessly with firewalls, VPNs, and intrusion detection systems. They minimize the impact of security data breaches and deliver comprehensive protection.

## EDR vs. MDR vs XDR: An Analysis of Key Differences

We've made a comparison table below to perform an EDR vs MDR vs XDR analysis:

| Parameter | EDR (Endpoint Detection and Response) | MDR (Managed Detection and Response) | XDR (Extended Detection and Response) |
|---|---|---|---|
| Focus | EDR detects and responds to threats across all endpoints, such as laptops, servers, BYOD devices, and desktops. | MDR focuses on detecting and responding to threats across multiple layers, including the network, endpoint, and cloud security. | XDR detects and responds to threats across all layers, including networks, endpoints, clouds, and apps. |
| Scope | EDR covers a limited scope, it focuses on individual endpoints. | MDR covers a broader scope, including multiple layers. | XDR covers broader scopes that range from networks to apps. |
| Detection | EDR detects and alerts about endpoint-level threats. | MDR detects and alerts threats across multiple layers. | XDR detects and alerts on threats across all layers, and it provides a more comprehensive view of enterprise security posture. |
| Response | EDR gives automated response capabilities. | MDR delivers automated response capabilities, as well as human-led incident response. | XDR provides automated response capabilities, as well as human-led incident response and remediation. |
| Threat Intelligence | EDR includes basic threat intelligence feeds. | MDR provides advanced threat intelligence feeds and analysis. | XDR offers advanced threat intelligence feeds, analysis, and contextualization. |
| Integration | EDR integrates with your existing security tools. | MDR gives you centralized dashboards and security tool integrations. | XDR offers a unified security posture view and integrates with existing security tools; it also provides centralized dashboards. |
| Cost | EDR tools are more affordable, with lower costs per endpoint. | MDR solutions can be more expensive, with higher costs per endpoint. | XDR solutions are the most expensive; their fees depend on their coverage limits. |
| Complexity | EDR is simple to implement and manage. | MDR requires more expertise and resources. | XDR is the most complex option; it needs great skills and planning to execute and oversee. |

## EDR, MDR, and XDR Use Cases

Here is a list of the most popular EDR, MDR, and XDR use cases:

### EDR vs MDR vs. XDR: Threat Remediation and Analysis

EDR solutions prevent phishing, malware attacks, ransomware, and provide advanced threat detection and response abilities. They detect malicious and unusual behaviors across all endpoints and secure sensitive data from cybercriminals. MDR provides 24/7 managed services for threat detection and response, security monitoring, threat hunting, and incident response. It provides access to the latest threat intelligence and gives deep visibility into the cloud and cyber security posture of organizations.

XDR incorporates threat analysis from multiple data sources, including cloud services, networks, and endpoints. It uses advanced analytics and automation to discover threats that are undetectable by siloed security tools.

## *1. Coverage Areas and Environments*

EDR is great if you have limited network visibility; you can employ MDR for larger and more complex environments that are situated in faraway locations. XDR covers environments that use cloud-based platforms and services. It detects and responds to multi-vector attacks and tactics. XDR responds to advanced threats too like APTs and nation-state attacks.

## *2. Compliance*

EDR meets HIPAA, PCI-DSS, and GDPR compliance policies easily. MDR assists with SOC 2 compliance, ISO 27001 framework, and maintains NIST standards. XDR deals with CMMC standards and matures cyber security. It complies with CSF standards and satisfies regulations like AWS Well-Architected Framework and Azure Security Center.

### Consolidating EDR, MDR, and XDR for Better Security

You can proactively consolidate EDR, MDR, and XDR features and get complete cloud and endpoint protection including the ability to secure your entitlements, identities, devices, and more.

This consolidation offers unprecedented speed, infinite scalability, and advanced threat response capabilities. It maximizes visibility across your entire cloud estate and resolves critical issues associated with connected security ecosystems.

### Conclusion

We’ve explored the top EDR vs MDR vs XDR use cases and compared their critical differences. Whether you use EDR, MDR, or XDR, or a combination of all three, will depend on your

business security requirements. Threats are evolving so your cyber and cloud security strategies will change too. If you're too worried and want to future-proof your endpoint and cyber security, we can help you to align your posture well to fit into your threat environment.

**FINAL THOUGHT**

Attackers are patient. They plan, they study and execute with precision.
Organizations must do the same.
PLAN | STUDY | UNDERSTAND | IMPLEMENT & REMEDIATE.

Contact us and Learn more about proactive detection, response & remediation. Let us discuss how you security posture must be done right.

info@questtechltd.com

https://questtechltd.com/cybersecurity/incident-response/

https://questtechltd.com/cybersecurity/assessment/

https://questtechltd.com/insights-advisory/ask-a-tech-question.html

https://questtechltd.com/insights-advisory/cybersecurity-posture-toolkit.html