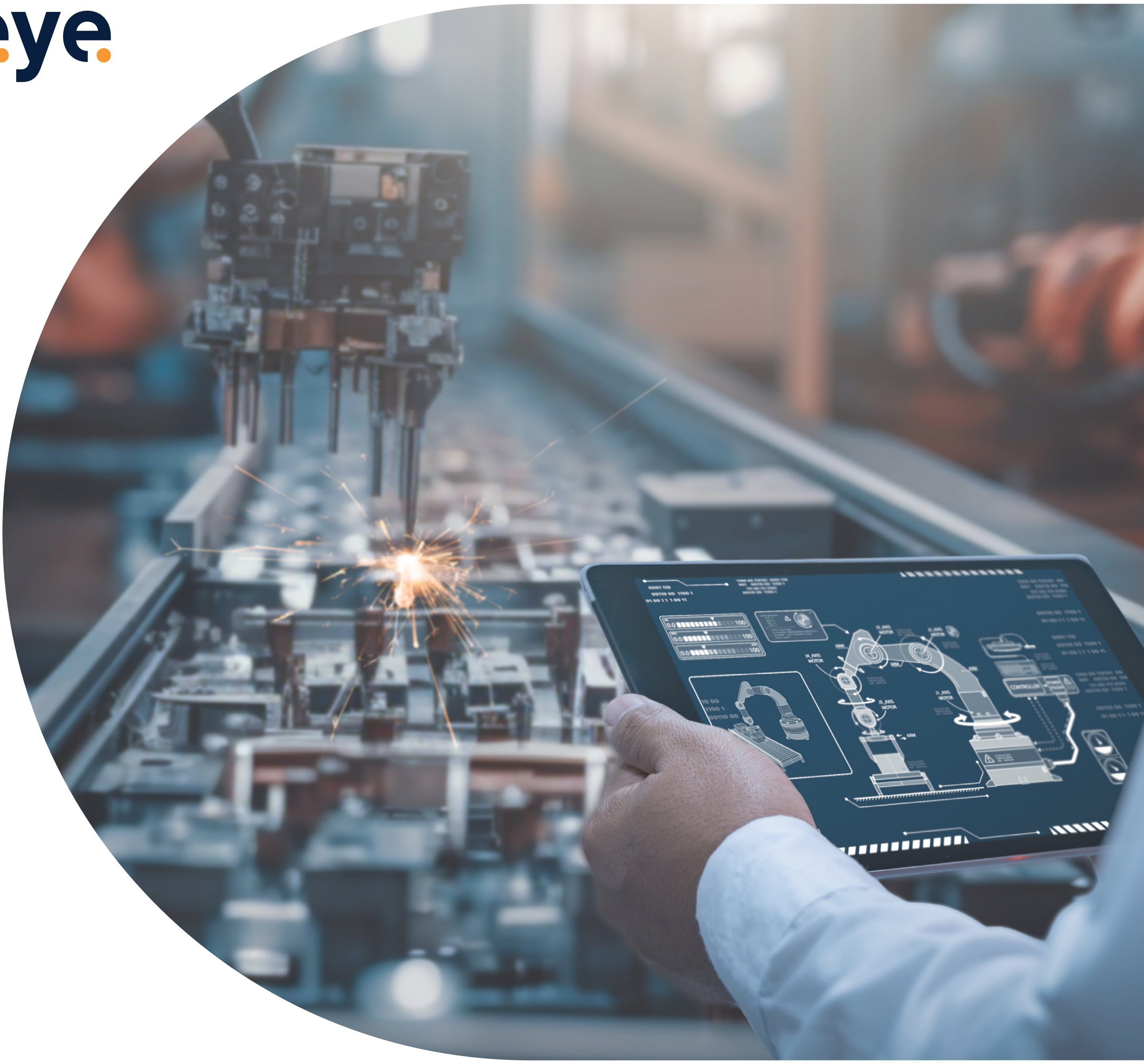
eye



MDR Technology Evaluation Guide

The Case for Using EDR

Table of contents

This guide is for technology evaluators of MDR solutions who have reached the stage where they must determine which security technology should serve as the foundation of the service: endpoint, network, or both.

MDR providers will fall into one of three categories:

- **Managed Endpoint Detection and Response (EDR)**
- **Managed Network Detection and Response (NDR)**
- **Managed Cloud Detection and Response (CDR)**

Most vendors offer an element of Extended Detection and Response (XDR), and many call their service Managed Extended Detection and Response (MXDR). They absorb signals from point security measures and correlate them with those from EDR or NDR. However, one of these two technologies will form the foundation of the service. It is your decision which one you should choose.

Core differences between EDR and NDR

EDR	NDR
Focuses on individual devices such as desktops, laptops, and servers. It monitors files, processes, users, and network activities at the endpoint level and detects threats where they often begin and pivot—on the endpoint itself.	Focuses on the flow of information across the network, detecting anomalies or potential threats within network traffic. NDR primarily monitors east-west (internal) or north-south (external) network activity.

This guide makes the case for EDR. Many vendors complement NDR with a lightweight endpoint agent that attempts to deliver EDR-like functionality. However, they do not match the capabilities provided by leading EDR vendors.

Why your choice of security product is important

You might assume that because you are outsourcing your detection and response, the underlying technology on which it is based is irrelevant to you, as it is the provider's responsibility to protect you. There are two reasons why you need to care.

Reduce the risk of a successful attack

The speed of the MDR provider's response can be the difference between a successful incursion being contained and a threat actor stealing and/or encrypting your sensitive and business-critical information. Their response time will be determined by several factors. This guide will help you answer the following:

- **Detection efficacy.** How many threats, at which stage of an attack, does it detect?
- **Detection speed.** Does it correlate signals quickly to determine whether a real attack is in progress?
- **Detection accuracy.** Does it create alerts for low-priority activities that result in false positives?
- **Threat visibility.** Does it provide context around the threat to enable rapid investigation?
- **Active response.** Does it enable a choice of response mechanisms to rapidly contain an attack with minimal business impact?
- **Investigation tools.** Does it provide the appropriate tools to help with the above and post-attack incident investigation and remediation?

Your team must be comfortable with the foundational products

You are not outsourcing your cyber security infrastructure and programme – just elements of detection and response. You will be involved in some activities yourself, the level of which will depend on your chosen provider and the foundational technology on which they are relying. It is imperative that you select a provider that uses products that you and your team are most comfortable with, based on your experience and skillsets. This guide will help you answer the following questions:

- How complex is the deployment of the detection and response products?
- Do I need to deploy additional agents, sensors, and probes?
- Do I need to configure integrations with other security tools and applications?
- How much effort do I need to expend, working with the provider during an ongoing attack, to provide information they cannot access?
- How much post-containment incident investigation and remediation do I need to do and what tools and information are made available?

Deployment steps and visibility

Without visibility into potential threats, it is extremely difficult to take protective action. EDR delivers deep visibility into host behaviour in Windows, Linux and MacOS systems. This includes (virtual) servers and laptops, independent of their location. NDR delivers broad visibility into network behaviour with a central appliance, which brings some trade-offs.

	EDR	NDR
Deployment methodology	The agent software deployment profile is configured in common Mobile Device Management (MDM) solutions like Intune, AD Group Policy or others.	Virtual or hardware appliance, central location in the network, passive Switched Port Analyser (SPAN) port or in-line (less common).
Phased deployment	Agents are commonly deployed in learning/ passive mode, creating a behaviour baseline while processes are not stopped/killed (and thus the business is less impacted).	The NDR implementation plan needs to be drafted based on the local network architecture. Multiple IT stakeholders need to adjust firewalls and embed hardware maintenance processes in the team.
Time to value (TTV)	Once the agent installation profile is deployed, all managed endpoints will be onboarded within minutes or hours.	An NDR implementation usually takes several weeks or months to complete.

Visibility (telemetry)	EDR monitors and collects processes, running applications, file changes, user activities, cloud connections, neighbouring devices and even network connections to and from the device. Best-of-breed EDR solutions combine the telemetry of all agents into one central IT asset overview.	Depending on the network architecture, NDR monitors and collects network metadata like source IP address, destination IP address and corresponding port numbers. With sNAT, the source IP address is not available. Any relevant data fields are often encrypted with TLS when SSL offloading is not implemented.
Caveats to proper deployments	EDR coverage is key to adequate visibility to minimise unmonitored endpoints (Shadow IT). Asset discovery telemetry, available in most best-of-breed EDR solutions, must be used to manage EDR coverage to near 100%. Do not forget to enable the EDR uninstall protection.	Enforce always-on VPN in hybrid environments. Otherwise, remote workers will not be seen. Consider decrypting traffic with SSL offloading, otherwise, detections will mostly be non-actionable without context. Avoid creating (insecure) routes between segmented networks to NDR as this potentially eliminates the value of this segmentation.

Detecting modern cyber threats

The annually updated ENISA Threat Landscape (ETL) highlights that ransomware, phishing, and supply chain attacks are among the most significant challenges facing organisations today. Detecting these threats requires a careful balance between maximising detection capabilities and minimising false positives to reduce response times. EDR and NDR offer a different value in detecting these modern threats.

	EDR	NDR
Lateral movement	Tracks unusual internal connections, privilege escalations, and process anomalies on endpoints. Can detect attackers trying to move between devices or escalate privileges.	Depending on network architecture, NDR monitors traffic between internal hosts for unusual connections or data flows. Detections are difficult to triage because of a lack of endpoint context.
Ransomware	Detects mass file encryption through file system monitoring and behavioural analysis. Isolates compromised endpoints and kills malicious processes.	Monitors unusual outbound traffic to C2 (Command-and-Control) servers but struggles to limit false positives because of TLS and because the lifetime of the C2 infra is short (minutes to days).
Phishing (attempts)	Monitors compromised applications for unusual behaviours and uses Indicators of Compromise (IOCs) to detect trusted software acting maliciously.	Detects unexpected communications from compromised software. Struggles to distinguish legitimate traffic from malicious traffic without endpoint context.

Supply-chain attacks	Monitors compromised applications for unusual behaviours and uses Indicators of Compromise (IOCs) to detect trusted software acting maliciously.	Detects unexpected communications from compromised software. Struggles to distinguish legitimate traffic from malicious traffic without endpoint context.
Exploitation (attempts)	Detects exploitation attempts using behavioural analysis and threat intelligence. Provides real-time alerts and can isolate the endpoint.	Monitors network anomalies indicating exploitation but struggles with attacks occurring purely at the host level.
Data (crown jewel)	Endpoints often contain/manage the crown jewels (like data) that attackers seek. Even if an earlier detection opportunity is missed, EDR ensures that there are multiple opportunities along the attack path to identify and halt an attacker before considerable damage occurs.	Monitors for suspicious data transfers and network communications potentially targeting sensitive assets. However, NDR lacks visibility into specific actions occurring at the endpoints, which could easily be mistaken for benign IT admin activity like backups. Once data exfiltration to external IP addresses is detected, it is often too late.

Response capabilities to mitigate active threats

Detection is only part of the equation within EDR and NDR. The ability to respond rapidly and effectively is what makes a solution powerful.

EDR offers advanced response capabilities that go beyond just notifying security teams. It provides direct interventions, including isolating an endpoint, terminating malicious processes, and rolling back changes made by malware. This allows organisations to contain and neutralise threats before they escalate into breaches.

NDR's response options are limited, typically to sending TCP reset packets to disrupt suspicious connections. This does not remove the underlying threat. The result is often a delay in remediation as the true cause of the threat remains active. Additionally, pinpointing which device is the source of malicious network activity can be challenging without the detailed visibility that EDR provides, especially in complex or poorly documented network environments.

In practical security workflows, analysts often pivot from NDR to EDR when they need to understand the depth and context of an alert. NDR might flag suspicious traffic. But without endpoint-level insight, it is difficult to determine the full story—such as which process initiated the behaviour or whether malicious changes have occurred. Leading EDRs fill this gap by offering the depth needed for effective, informed responses.

Addressing common misconceptions

NDR is tamper resistant; EDR is not

This is a common misconception. Being deployed out-of-band does not make NDR a safer option for network security. Attackers might find it harder to disable, since it operates separately from endpoints, but this does not make it invincible. Attackers can bypass NDR by using encrypted communications or trusted platforms like GitHub to spread malware—effectively rendering NDR unable to monitor their activities.

EDR kernel-level tamper protection will trigger a critical alert if a threat actor attempts to interfere with the agent. This is true even if they have local admin privileges. In this case, if they are also armed with “EDR killer” software that is new, unknown, and effective, they might be able to disable the EDR. However, EDR across the estate will have already detected the activity that resulted in the compromise of these local admin credentials.

NDR is essential for detecting attacks involving unmanaged devices

Another argument in favour of NDR is its value in monitoring environments where endpoint agents cannot be deployed, such as OT, IoT, and legacy systems. However, these systems typically represent a small portion of the overall infrastructure and often have limited network exposure. The more effective strategy is to isolate these legacy systems and protect the IT infrastructure surrounding them with EDR, ensuring that attackers cannot pivot to more critical systems.

While NDR might offer visibility into network-based attacks, most are endpoint-focused, often leveraging remote access methods to breach systems via the internet. Attacks such as ransomware have always involved remote compromise, with endpoints being the point of entry. EDR is ideally suited for these scenarios, providing comprehensive detection and response capabilities.

Conclusion: EDR as core, NDR as a supplement

After evaluating the capabilities and limitations of both EDR and NDR, it becomes evident why EDR is the foundation of any effective cybersecurity strategy. It provides real-time visibility, advanced response capabilities, and the context necessary for threat detection and mitigation—all of which are essential for today's rapidly evolving threat landscape.

While NDR can play a supporting role—offering additional anomaly detection for unmanaged devices or lateral movement within specific network architectures—it should not be considered the primary solution. NDR is most effective when it complements EDR, helping to cover blind spots that arise in complex environments. However, it falls short in detection, response, and overall operational effectiveness when compared to the endpoint-centric focus of EDR.

To achieve the best results, organisations should focus on implementing a best-of-breed, managed EDR solution, ensuring it is properly configured with effective tamper protections and incident response playbooks. NDR should be seen as an optional layer, deployed only when specific visibility requirements exist that EDR alone cannot fulfil.

Case Studies

KeyTec Netherlands

As reports of ransomware in their industry soared, manufacturing company KeyTec Netherlands decided to act. Find out how Eye Security helped them proactively bolster their defences and create a cyber-savvy work culture.

Signature Foods

As cybercrime becomes increasingly sophisticated, companies racing to keep up are turning to external suppliers. Find out how Eye Security helped Signature Foods get blanket cyber protection in just a few weeks.

At Eye Security, we advocate for a no-nonsense approach to cybersecurity—one that emphasises the fundamentals, prioritises endpoint defence, and uses network monitoring selectively to fill in the gaps. By doing so, we help build a resilient security posture that stays ahead of attackers and adapts to emerging threats.

Visit www.eye.security