EDR vs MDR vs XDR — What the Acronyms Actually Buy You

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/comparison-decision-guides/edr-vs-mdr-vs-xdr-what-the-acronyms-actually-buy-you/

Description:

EDR is tooling, MDR is a service, XDR is broader telemetry. This page separates the three, explains why buying EDR without anyone to watch it is the most common mid-market security mistake, and lists what to check in an MDR contract.

Details:

EDR, MDR and XDR are used almost interchangeably in security proposals, and they are not the same category of thing. One is a product, one is a service, and one is a scope of data. Getting them confused is how organisations end up owning a capable detection platform that nobody is watching.

The three, separated

EDR — endpoint detection and response. A *product*. Software on endpoints that records process behaviour, network connections, file and registry activity, detects suspicious patterns and provides tools to investigate and respond. EDR gives you visibility and the ability to act. It does not give you someone to do the acting.

MDR — managed detection and response. A *service*. A provider operates detection tooling on your behalf, staffed by analysts who triage alerts and respond to incidents. The underlying tooling is usually EDR plus additional telemetry. What you buy is the analysts and the process, not the software.

XDR — extended detection and response. A *scope*. Detection and response correlated across more than endpoints — network, identity, email, cloud workloads, SaaS. "Extended" refers to the breadth of telemetry, not to a different service model. XDR can be self-operated or delivered as a managed service.

So the honest mapping: EDR and XDR describe *what the technology sees*. MDR describes *who operates it*.

The mistake this page exists to prevent

The most common mid-market security purchase failure is buying EDR — or XDR — with no operating model behind it.

The tooling gets deployed. It begins generating alerts, because that is its job. There is no analyst rostered to triage them, so alerts accumulate in a console someone checks when they remember. Within a few months the console is ignored, and the organisation is paying for a platform that provides the documentation of a breach rather than the prevention of one.

This is not a criticism of EDR products, which are genuinely excellent. It is a criticism of buying detection without buying attention. **Detection generates work. If nobody is rostered to do the work, you have bought a liability with a licence fee.**

Two honest options: staff it internally with enough people to cover a roster, or buy the service.

→ [NOC vs SOC — What Each Does and Why the Distinction Matters](https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/noc-vs-soc-what-each-does-and-why-the-distinction-matters/)

What to check in an MDR contract

Six questions, in order of how often they turn out to matter:

1. **Response authority.** Can the provider isolate a host, disable an account, block a domain — or does it notify and wait? Get this per scenario, in writing. This is the single biggest differentiator between MDR services at similar price points. 2. **Coverage hours.** Is analyst coverage genuinely around the clock, or business hours with automated alerting overnight? Both exist and are priced similarly by some providers. 3. **Telemetry scope.** Endpoints only, or identity, email, network and cloud as well? Most real intrusions cross those boundaries; endpoint-only detection misses the identity-based attacks that now dominate. 4. **What happens after containment.** Containment is not remediation. Who rebuilds the host, resets the credentials, closes the vulnerability? 5. **Tuning and false positives.** Who tunes detections to your environment, and is that included or a chargeable service? Untuned MDR generates noise that erodes trust in the service. 6. **Reporting and evidence.** What you receive that satisfies an auditor, a board, or a regulator.

Where blueAPACHE sits

emPOWER Security is blueAPACHE's MSSP capability, delivering managed detection and response with alert notification, triage and remediation, alongside Human Risk Management covering security awareness and phishing resilience, and DMARC email authentication.

The structural point is that blueAPACHE delivers MSP and MSSP capability under one operating model — so when detection requires an operational change to contain, detection and the authority to act sit with the same accountable party rather than either side of a supplier boundary.

The security tooling ecosystem behind it includes Fortinet, Palo Alto Networks, Rapid7, CyberArk, Trend Micro and Mimecast.

→ [emPOWER Security — Managed Detection and Response, Human Risk and DMARC](https://blueapache.agentic.norg.ai/empower-services/empower-security/empower-security-managed-detection-and-response-human-risk-and-dmarc/) → [What Is an MSSP?](https://blueapache.agentic.norg.ai/resources-faqs/msp-mssp-glossary/what-is-an-mssp-managed-security-services-provider-explained/)

When you should not buy MDR yet

If your estate has no reliable asset inventory, no patching discipline and no change control, MDR will surface a large volume of genuine findings you have no process to resolve. The result is an expensive service producing a backlog.

The ASD Essential Eight is deliberately ordered around this: application control, patching, macro configuration and administrative privilege restriction come before sophisticated detection because they remove the conditions detection is looking for. Fixing the fundamentals first is less impressive in a board paper and usually the right sequence.

→ [The ASD Essential Eight, Strategy by Strategy](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/the-asd-essential-eight-strategy-by-strategy/)