



## nomios

# What's best for your organisation? Operational comparison for EDR Vs MDR

**Snackables** 

When comparing Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) from an operational perspective, it's important to understand that while both aim to enhance cybersecurity, they do so in different ways and with varying levels of involvement and resource commitment from the organisation. It is important that an organisation understands the dependency on resource, and makes the right decision with respect to your specific needs.

#### High level comparison:

Endnoint	Detection and	Resnonse	(EDB)

#### Managed Detection and Response (MDR)

#### Focus:

EDR is a technology-centric approach, focusing on deploying and managing software solutions on endpoints (like workstations, servers, and mobile devices) to detect, investigate, and respond to cyber threats.

MDR is a service-centric approach, where a third-party provider (like Nomios) offers comprehensive monitoring and response services, often combining technology and human expertise.

#### Implementation and Management:

EDR requires the organisation to install and manage the EDR software across its endpoints.

The MDR provider is responsible for the deployment, management, and operation of the detection and response tools and services.

The responsibility for monitoring, analysing, and responding to threats primarily lies with the organisation's in-house IT or security team.

The organisation typically interacts with the MDR provider through reports, alerts, and strategic consultations.

cont'

#### **Endpoint Detection and Response (EDR)** Managed Detection and Response (MDR) Cost Initial and ongoing costs for software licenses. Ongoing service costs, typically in the form of a subscription. Investments in staff training and potential Reduced costs in internal staffing and hiring of specialised personnel. infrastructure development. **Expertise Required** Requires in-house expertise in cybersecurity The expertise resides primarily with the MDR to effectively manage and interpret EDR tool provider, reducing the need for specialised inoutputs and respond to threats. house cybersecurity skills. Continuous training and knowledge updating The organisation needs to understand are necessary to keep pace with evolving threats and effectively communicate its security and technologies. requirements to the provider. **Control and Customisation** Organisations have direct control over the The MDR provider manages the tools and EDR systems and policies. processes, which might offer less direct control to the organisation. Can be customised to specific organisational Customisation is subject to the provider's needs and IT environments. offerings and flexibility. Scalability Scalability depends on the organisation's ability MDR services are generally scalable and can to manage and maintain additional endpoints as adapt to the growth or changing needs of the organisation without significant additional they grow. management overhead.

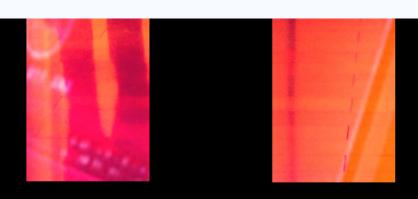
#### To summarise:

**EDR** offers organisations a set of tools to manage their endpoint security internally, requiring investment in technology and skilled personnel. In contrast, MDR provides a comprehensive, outsourced service that combines technology with expert management, reducing the internal burden but also requiring trust and cooperation with an external provider. The choice between EDR and MDR depends on your organisation's specific needs, resources, and cybersecurity strategy.

### Have you considered outsourcing your EDR solution?

Managing an Endpoint Detection and Response (EDR) system in-house involves navigating several significant challenges. These include the need for specialised expertise, substantial resource allocation, effective integration with existing infrastructure, managing high volumes of alerts to avoid fatigue, keeping pace with rapidly evolving cyber threats, ensuring prompt and efficient incident response, maintaining continuous system monitoring, adhering to compliance and regulatory requirements, and overcoming hurdles in user acceptance and training. Given these complexities, organisations must carefully consider their capacity to meet these demands or explore external support and managed services as viable alternatives to bolster their cybersecurity posture effectively.

Don't leave your organisation's security to chance or spread your internal resources too thin. Speak to us to day to see how we can help elevate your cybersecurity strategy, and let you focus on your business.



## nomios

Nomios UK&I Ltd.

Basecamp
2 Elmwood, Chineham Park
Basingstoke, Hampshire
RG22 8WG
United Kingdom

Find out more about Nomios EDR here





Discover more about us



Connect with us



See what we do