Cumberland Managed Services
3301 Eighth Street
Cumberland, BC, V0R 1S0

(250) 336-0463
www.cumberlandmsp.ca

EDR vs MDR: A Strategic Comparison

Definitions

EDR (Endpoint Detection and Response)

EDR is a security solution deployed on endpoints (like computers and servers) that monitors, detects, investigates, and responds to cyber threats in real time. It provides visibility into endpoint activity and enables IT teams to take automated or manual action against malicious behavior. Best suited for organizations with in-house security expertise, EDR offers control and customization but requires skilled personnel and ongoing oversight.

MDR (Managed Detection and Response)

MDR is a fully managed cybersecurity service that combines EDR tools with 24/7 monitoring, threat hunting, and incident response by a team of external experts. It's ideal for organizations lacking internal security resources, providing rapid response and continuous protection without the overhead of managing tools or hiring staff. MDR reduces the operational burden while enhancing threat detection and compliance support.

EDR/MDR Breakdown

Category	**EDR (Endpoint Detection & Response)**	**MDR (Managed Detection & Response)**
Definition	Software solution focused on detecting and responding to threats at endpoint level	Outsourced service that includes EDR capabilities along with human expertise and 24/7 monitoring
Core Features	- Endpoint activity monitoring - Threat detection - Forensics - Automated response actions	- 24/7 monitoring - Threat hunting - Incident response - Expert analysis - Reporting
Who Manages It	Internal IT/Security team	Third-party security provider (SOC team)

Cumberland Managed Services
3301 Eighth Street
Cumberland, BC, V0R 1S0

(250) 336-0463
www.cumberlandmsp.ca

Category	EDR (Endpoint Detection & Response)	MDR (Managed Detection & Response)
Expertise Needed	High – Requires skilled security analysts to interpret and act on alerts	Low – Expertise provided by MDR vendor
Implementation	Installed on endpoints and integrated into internal security stack	EDR component included, deployed and managed by the MDR provider
Scalability	Moderate – Limited by internal team resources	High – Scales with the provider's infrastructure and resources
Response Time	Fast if internal team is responsive	24/7 response capability from MDR team
Cost	Lower upfront cost but higher internal resource demand	Higher subscription-based cost but includes labor and expertise
Pros	- Full control over data and processes - Deep customization possible	- 24/7 monitoring and response - Less burden on internal team - Faster deployment of expertise
Cons	- Requires internal resources and expertise - Risk of alert fatigue	- Less control over internal data - Dependency on third party
Use Case	Suitable for organizations with in-house security operations	Ideal for SMBs or understaffed IT teams lacking in-house SOC capabilities
Compliance Support	Depends on internal implementation and policies	Often includes reporting and support for compliance frameworks (e.g. PCI, HIPAA)
Integration	May require effort to integrate with other tools	Often comes pre-integrated or with professional support

Category	EDR (Endpoint Detection & Response)	MDR (Managed Detection & Response)
Future Trends	- Moving toward AI-enhanced autonomous response - Greater integration with XDR	- Increasing use of AI/ML for threat analysis - Growth in hybrid MDR + XDR offerings