CLICK HERE TO READ THE eBOOK

adlumin™

EDR v XDR v MDR:

Selecting the best solution for your organization

Most organizations face increasing cyber threats and regulatory obligations, with exhausted resources and limited budgets. Moreover, organizations must leverage existing security investments to maximize the return from endpoint, cloud access, VPNs, perimeter security, and logging systems.

The comparison chart provides an overview of three primary threat management services: Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and Extended Detection and Response (XDR). For each service, insights are provided to assist you in making the right choice when investing your limited budget and maximizing your cyber protection.

	EDR	MDR	XDR	ADLUMIN
Investment (includes internal resources and expertise)	$$	$$$	$$$$$	$$
Who manages what?	Managed Service or Customer Manages	Managed Service	Managed Service or Customer Manages	Managed Service or Customer Manages
Data Sources	Endpoint	Endpoint Network Traffic Cloud services	Endpoint Network Traffic Perimeter Cloud services Active Directory Email	Endpoint Network Traffic Perimeter Cloud services Active Directory Email
Detections	Malware/IoCs Fileless attacks	Malware/IoCs Fileless attacks	Malware/IoCs Fileless attacks Behavioral anomalies Machine Learning	Malware/IoCs Fileless attacks Behavioral anomalies Machine Learning
Investigation	Requires managed SOC service Customer must investigate detections and determine if response is required	Included in SOC service (varies)	Requires managed SOC service SOC conducts investigations	Included in SOC service Included in SOC service
Response	Customer must investigate detections and determine if response is required.	MDR SOC Service: Manage Yourself	Requires managed SOC service	Adlumin SOC Service: Extended Security Team
Remediation	Endpoint isolation and blocking	Endpoint isolation and blocking Traffic blocking (source IP/DNS) Cloud access reset or disabling	Endpoint isolation and blocking Traffic blocking (source IP/DNS) Account/Group reset or disabling Cloud access reset or disabling	Endpoint isolation and blocking Traffic blocking (source IP/DNS) Account/Group reset or disabling Cloud access reset or disabling
Reporting	Endpoint forensics	Based on SOC capability	Requires managed SOC service Co-managed reporting	Detections Investigations Custom reports Compliance insights Compliance examiner reports Executive summaries
Threat Intelligence	Not included	Included	Included	Dedicated Threat Intelligence team and researchers Threat intelligence feed Dark web monitoring Managed deception technology
Deployment Speed	Days to configure and tune	Requires services licenses first Weeks to configure and tune	Requires services licenses first Weeks to configure and tune	90 minutes fully up and running Agent deploys via global policy object (GPO)
License Model	Multiple licenses for endpoint and SOC services	Multiple licenses for specific devices and services managed Log storage fees based on volume and retention	Multiple licenses for specific devices and services managed Log storage fees based on volume and retention	One license for all services No data upcharges
Visibility	Only one entity license holder can access the portal (not visible if managed by extended security team)	SOC requests for reports or investigation information	Co-management varies	100% fully visible to customer. The customer sees and has access to the same portal as the SOC Real-time customer reporting
Context	Provides endpoint only	SOC requests for reports or investigation information Limited compliance reporting	Co-management varies	A simplified view: The customer sees and has access to the same portal as the SOC Threats and detections At-risk programs Network Health Policy violations Compliance insights
Vulnerability Management	No	Yes	No	Integrated service Fully available in the Adlumin portal
Penetration Testing	No	Varies	No	Integrated service Fully available in the Adlumin portal
Awareness Training	No	Varies	No	Integrated service Fully available in the Adlumin portal

adlumin™

Illuminate Threats and Eliminate Risks

Learn more about how Adlumin's Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, eliminate cyber risk, and command authority.

Interested in diving deeper into the differences between EDR, XDR and MDR?

Read the eBook

Adlumin Inc. provides the enterprise-grade security operations platform and managed detection and response services that keep mid-market organizations secure. With one license and one platform, its patented technology gives organizations and solution providers everything they need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support and much more.