eBook

EDR v XDR v MDR:

The Cybersecurity ABCs Explained

N-ABLE™

Table of Contents

Executive Summary

Cyber risks and attacks continue to mount, reflective regulatory responses impose additional operational responsibilities, yet budgets do not increase in parallel, and resources are all but exhausted. The need for a comprehensive and consolidated cybersecurity solution has become more prominent in recent years. At the core of cybersecurity solutions are detection and response capabilities that illuminate threats, facilitate investigations, and contain threats before they become business or operationally disruptive.

As the victims of cybercrime mount, so do the security offerings that promise holistic protection. The security industry continues to invent new acronyms creating self-inflicted market confusion for buyers who struggle to understand the growing alphabet soup of solutions, distinguish their differences, and determine which solution is right for their organization.

Most organizations are turning to some form of threat detection and response service[1], and the broad category is growing by almost 20 percent per year and is estimated to reach 22 billion USD in revenue. The majority of small to medium organizations prefer to outsource complex security operations and services such as Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), or Extended Detection and Response (XDR). At the 50,000-foot view, these solutions seem remarkably similar and proport interchangeable business benefits like greater protection, lowered operating costs, and simplified operations.

Yet behind the homogenous marketing lurk specific differences that can critically impact your organization in terms of operational cost and complexity and the ability to protect against cyberattacks. Much of this confusion stems from an expanding list of acronyms with aspirational definitions. Without a clear understanding of how vendors apply these terms and a clear understanding of their business benefits, organizations struggle to make informed decisions about which service will best protect them from cyber risks.

This provides an overview and comparison 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, we provide insights to assist you in making the right choice when investing your limited budget and maximizing your cyberprotection.

Learning the Alphabet

The most popular threat management services are **Endpoint Detection and Response (EDR)**, **Endpoint Protection Platform (EPP)**, **Managed Detection and Response (MDR)**, or **Extended Detection and Response (XDR)**. For this paper's purposes, we also include security information and event management (SIEM), and security orchestration automation and response (SOAR), as this is offered in some managed capacity.

Endpoint Security

Endpoint security solutions include Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP). Some vendors offer a managed version of their endpoint solutions. Endpoint is a popular entry vector or transit point during an intrusion, making endpoint detection critical in early detection and containment. Pandemic-driven work-from-home shifted the "perimeter" from the traditional premises to the remote devices (endpoints) connected to centralized workloads and databases. Endpoint security is growing 25 percent annually, reaching a market value of over 18 billion USD by 2031[2].

Endpoint Protection Platform (EPP)

According to Gartner, an endpoint protection platform is a solution to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to security alerts and events EPP is often referred to as a next-generation anti-virus. Definitions of malware and Indicators of Compromise (IoCs), the precursors to attacks, are stored in the cloud, with a device-side agent connected to the cloud database.

Endpoint Detection and Response (EDR)

Closely related to EPP, Endpoint Detection and Response (EDR) continually monitors an endpoint (laptop, tablet or mobile phone, server, or internet-of-things device) to identify threats through data analytics and prevent malicious activity with rules-based automated response capabilities.[3]

Common Vendors

Bitdefender, Cisco AMP, CrowdStrike, Cylance, Huntress, Malwarebytes, Microsoft Defender, Palo Alto Networks, Sentinel One, Sophos, and VMware CarbonBlack.

Managed SIEM

Security Information and Event Management (SIEM) systems are a staple of larger security programs and provide centralized logging of siloed security system alerts and events. Originally designed for compliance reporting, SIEM services support threat detection, compliance, and security incident management by collecting and analyzing security events, network logs, and other data sources.[4] SIEM systems vary in collection and analysis capabilities and require significant customization and configuration to build detection policies and alerts. They are often expensive and require investment in outsourced configuration services.

In response to competition and the recognized complexity, many SIEM vendors provide turnkey operations that provide monitoring and alerting services.

Common Vendors

ConnectWise, LogRhythm, Securonix, Splunk, and Sumo Logic.

Managed Detection and Response (MDR)

In response to a growing portfolio of security products, organizations turned to Managed security Service Providers (MSSP) to manage these devices, update and patch systems, aggregate information, and provide frequent reporting. MSSPs manage devices, whereas customers also needed a service to manage alerts, investigate threats, and contain attacks. MDR provides a turnkey combination of tools and security expertise to protect clients from cyberthreats.

MDR vendors also vary in their detection capabilities and response services. Detection is limited to the specific set of sources from which they pull security data. Response services range from simple alert notification to containment at the network traffic (TCP/IP or DNS) level, endpoint (in conjunction with an EDR/EPP), or cloud gateway (as available with their cloud access service).

There are two broad classes of MDR vendors: Pure-play MDR and managed endpoint or SIEM.

Pure-play MDR

This category of MDR service providers relies on a proprietary mix of third-party security tools and solutions, such as endpoint, SIEM, cloud access, or others, to collect logs and alerts. These vendors use a customized technology stack, which their 24/7 Security Operations Center (SOC) monitors. Most pure-play MDR vendors cannot decouple their technology stack from their SOC service offerings. While effective at detecting and responding to threats, this closed-loop approach often limits their ability to offer comanagement, work effectively with partners and customer vendors, and leaves customers reliant on their SOC to provide reports.

Common Vendors

Arctic Wolf, Cybereason, CyNet, eSentire, Fidelis, Rapid7, Securework.

Extended Detection and Response (XDR)

First coined by Palo Alto Networks, Extended Detection and Response (XDR) collects security data from network points, operating systems logs, application logs, cloud services, endpoints, and other logging systems, to correlate information and apply threat detection analytics to this data lake of information.[6] An evolution of MDR, XDR service providers claim the ability to identify threats and streamline response proactively. Security teams use XDR cloud-based platforms to automate or accelerate detection, enhance investigation capabilities, and respond using Security Orchestration and Automated Response (SOAR) services. Gartner predicts XDR adoption will grow from less than 5 percent today to 50 percent by 2027.[7]

Note: Many MDR and managed endpoint vendors claim XDR services since XDR is seen as the evolution of managed detection and response services.

Common Vendors

Cisco, Fidelis, Fortinet, Palo Alto Networks, Rapid7, Sophos and Trellix.

Security Orchestration, Automation, and Response (SOAR)

Security Orchestration, Automation, and Response (SOAR) is a stack of compatible software programs that enables an organization to collect data about security threats and respond to security events with little or no human assistance. Security Orchestration, Automation, and Response (SOAR) combine incident response, orchestration, and automation of investigation and response capabilities in a single platform.[8] Integrated workflows include initial triage, case management, containment orchestration, and forensic reporting. SOAR is often a collection of other capabilities in MDR or XDR services.

Common Vendors

Anomali, Cyware, Fortinet, Palo Alto Networks, Rapid7, Splunk, Sumo Logic and Trellix.

Selecting the Best Solution for My Organization

Most organizations face increasing cyberthreats 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.

	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

	EDR	MDR	XDR	Adlumin
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
	Endpoint isolation and blocking.	Endpoint isolation and blocking	Endpoint isolation and blocking	Endpoint isolation and blocking
		Traffic blocking (source IP/DNS)	Traffic blocking (source IP/DNS)	Traffic blocking (source IP/DNS)
		Cloud access reset or disabling	Account/Group reset or disabling	Account/Group reset or disabling
			Cloud access reset or disabling	Cloud access reset or disabling
Remediation	Endpoint only	Recommendations only if managed	Recommendations only if managed	Adlumin platform includes SOAR capabilities and automatically updates perimeter rules, and policy
	Recommendations only if managed	Customer must conduct remediation (system updates, account or device rebuilds)	Customer must conduct remediation (system updates, account or device rebuilds)	
	Customer must conduct remediation (system updates, account or device rebuilds)			
Reporting	Endpoint forensics	Based on SOC capability	Requires managed SOC serviceNetwork Traffic Co-managed reporting	Detections Investigations Custom reports Compliance insights Compliance examiner reports Executive sumamries

	EDR	MDR	XDR	Adlumin
Threat Intelligence	Not included	Included	Included	Dedicated Threat Intelligence team and researchers Threat intelligence feed Darknet 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	Multiple licenses for specific devices and services managed	One license for all services
		Log storage fees based on volume and retention	Log storage fees based on volume and retention	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

	EDR	MDR	XDR	Adlumin
Vulnerability Management	No	Yes	No	Integrated service Fully available in the Adlumin platform
Penetration Testing	No	Varies	No	Integrated service Fully available in the Adlumin platform
Awareness Training	No	Varies	No	Integrated service Fully available in the Adlumin platform
Ransomware Prevention	No	No	No	Kills process at the start of encryption Integrated service Fully available in the Adlumin platform

Which Solution is Right for Your Organization?

Endpoint and Managed Endpoint

All organizations should be using endpoint protection as a core defense against cyberattacks. All devices connected to your systems and applications (like email and databases) require endpoint protection.

Is endpoint right for you?

Endpoint security is foundational in any program. However, endpoint provides a limited view and requires expert ability to analyze alerts and take containmentactions. A managed endpoint option is more suitable for organizations that lack internal expertise.

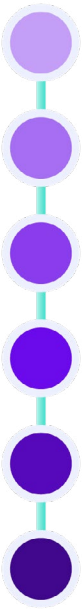
Coverage	Limited to endpoints running the EDR/EPP agent
Detection	Based on detection rules and device analytics to identify malware, zero-days, and some fileless attacks
Investigation	Deep device-level forensics, including process manipulation, registry changes, file access, and network connections
Response	Limited to endpoint: device isolation, power reset or poison-pill
Remediation	Specific file recover
Reporting	Provides deep device-level analytics

Managed SIEM

Managed SIEM offerings remove the complexity of SIEM operations but are limited by the sources of security data in your environment and deliver varying levels of investigation and response. In many cases, alerts are presented and passed to the customer, who is responsible for validating the threat and taking containment action.

Is managed SIEM right for you?

SIEM operation requires sophisticated security expertise and constant updates to address emerging threats. Managed SIEM offerings reduce this complexity but leave investigation and response activities to the customer. If you adopt a managed SIEM rather than MDR or XDR, be prepared to clear alerts and know how to contain threats across multiple systems once discovered.



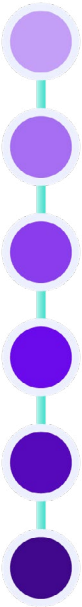
Coverage	Limited by customer security data sources
Detection	Based on rules and policies in operation
Investigation	Requires security expertise or managed service to validate alerts
Response	Limited to no response capabilities
Remediation	Analysis of logs provides some guidance
Reporting	Sophisticated reporting capabilities for both security operations and compliance reporting

Pure-play MDR

Managed Detection and Response (MDR) offerings provide a turnkey threat management service appropriate for customers who lack the internal expertise or resources to manage alerts and detections or the ability to contain threats. Some MDR offerings include access to threat intelligence teams (with varying cost models) or for-fee risk management and attack surface management services. These services are not integrated and are provided as professional service one-off projects.

Is MDR right for you?

Managed Detection and Response (MDR) service is appropriate for customers experiencing alert fatigue with their existing security operations team, looking to augment their internal operations, or cannot afford an internal security operations center (SOC).



Coverage	Specific to the MDR service provider technology stack
Detection	Specific to the MDR service provider technology stack
Investigation	Provides security expertise validate alerts and detections
Response	Specific to the MDR service provider technology stack
Remediation	Generally, provide guidance and recommendations
Reporting	Reporting is limited to the service offered through their SOC services

Extended Detection and Response (XDR)

Extended Detection and Response (XDR) offerings provide comprehensive coverage and deep machine learning analytics but are expensive and complex to operate. They require complementary capabilities from a Security Orchestration, Automation, and Response (SOAR) offering or a sophisticated internal Security Operations Center (SOC). Most small to medium organizations lack the budget and resources for XDR services.

Is XDR right for you?

Extended Detection and Response (XDR) service is appropriate for customers with a sophisticated internal Security Operations Center (SOC) or similar resources.

Coverage	Comprehensive monitoring of network, cloud, devices, etc.
Detection	Specific to the XDR service provider
Investigation	Deep analytics requiring security expertise validate alerts and detection
Response	Specific to the customer technology stack
Remediation	Generally, provide guidance and recommendations
Reporting	Comprehensive reporting based on the XDR SOC services

Additional Considerations

When it comes to selecting a managed security service, there are additional considerations that set service providers apart. The following capabilities are key considerations:

Threat Intelligence

More sophisticated service providers offer access to a threat intelligence research and hunting team. Threat intelligence collects information from public feeds (government and law enforcement agencies), aggregates this data on the latest Tactics, Techniques, and Procedures (TTPs) used by criminals, and follows the activity of known advanced persistent Advanced Persistent Threat (APT) actors, including statesponsored groups and ransomware gangs.

Moreover, threat researchers actively mine SOC data to identify patterns and attack trends to augment detection algorithms and predict new vectors of attack, potential vulnerabilities or exposures, or industry-centric campaigns that can easily migrate to new business segments.

Threat intelligence teams also offer regular briefings and industry reports. They provide briefings on active threat actors, new systemic vulnerabilities, or legal actions.

User and Entity Behavior Analytics (UEBA)

User and entity behavior analytics (UEBA) examines the relationships and privileges that connect different systems, including endpoints, applications, business services, and network devices. UEBA maps and monitors the connections and relationships between these systems. It connects users and accounts, associated privileges, and common activity patterns to baseline your organization's operations. UEBA detects anomalous behavior as an early warning to common attack patterns such as account hijacking, privilege escalation, uncorrelated account creation, and lateral movement. UEBA often catches events before endpoint, network perimeter defenses, or SIEM log events.

Access to Customer Data

Outsourcing security operations to a managed service provider can reduce cost and complexity, but it also limits visibility and access to your data and security records. This is particularly true for MDR/XDR vendors who cannot decouple their technology from their SOC services. They are often remiss in exposing SOC dashboards and their spartan orchestration platform, which is optimized for expert security analysts, but lacks the ease-of-use or navigation capabilities expected by non-practitioners. This leaves customers reliant on SOC requests and ticketing to produce reports or address ad-hoc queries. It can also create blind spots when it comes to compliance reporting.

Compliance Reporting

Organizations that are heavily regulated and must meet specific security and privacy requirements often struggle with MDR/XDR vendors who cannot decouple their technology from their SOC services. The reliance on SOC ticketing to provide specific operational details and performance metrics complicates the ability to generate comprehensive reports for regulators and inspectors. It also makes it challenging for customers to identify compliance insights and make remediations before a violation occurs. In the case of regulated entities, it is important to select a vendor who is experienced operating in regulated environments, familiar with specific compliance standards, and can provide regulator-approved reports and artifacts.

Attack Surface Management

Growing cyberattacks and increasing regulatory requirements expand the portfolio of security tools and services managed by customers. Yet, many organizations desire a consolidated approach to security. As cybersecurity standards improve, common services are required to establish compliance or reduce business and operational risk, including vulnerability assessments, automated patch management, deception technology, and employee awareness training and testing. Organizations should select service providers that offer core managed threat services and integrated attack surface management.

The Adlumin Advantage

Adlumin delivers Managed Detection and Response services through a unified platform for mid-market organizations that lack the resources to manage multiple tools from competing vendors to address security threats and meet their compliance requirements. With Adlumin, you have comprehensive visibility into the security posture in a oneplatform-one-license model that scales to ensure customers' security needs are met, regardless of their size or operating environment.

Speed

Adlumin's platform is cloudnative and serverless and takes less than 90 minutes to deploy.

Visibility

You see what we see. All your security data is in one location, from on-premises to the cloud.

Context

Insights into the user or system in question, a timeline of activity, and details of SOC actions.

Robert Johnston
Co-founder and CEO

Timothy Evans
Co-founder

Adlumin was founded in 2016 by two NSA veterans who bring the unique counterpoints of a cyberattack.

One an attack squadron commander and one a national cyberdefense leader. They are building on their expertise and continuing their tradition to support and serve. The Adlumin platform consolidates critical security tools and automates remediation for mid-market.

Adlumin Extended Detection and Response

Command more visibility to your security, compliance, and cyber risk

Get all the capabilities of enterprisegrade SOC built into one platform. You have everything you need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support, and much more.

Adlumin Managed Detection and Response

Let us manage your detection, response, and compliance

Our experienced analysts enhance your current team's capabilities and help you reduce threat detection and response times while gaining complete visibility. You get more time back in your day and peace of mind knowing you are covered.

Security Operations Platform Modules

Adlumin offers a growing portfolio of fully integrated, consolidated risk management and attack surface management services to reduce risk and meet regulatory compliance.

Vulnerability Management	Comprehensive monitoring of network, cloud, devices, etc.
Penetration Testing	Specific to the XDR service provider
Security Awareness Training	Deep analytics requiring security expertise validate alerts and detections
Total Ransomware Defense	Eliminate the success of a ransomware attack at every layer
Incident Response (IR)	Contain, eradicate, and recovery from an incident

adlumin™
An N-ABLE Company

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; contact us today or schedule a demo at www.adlumin.com.

Adlumin is the security operations command center that simplifies complexity and keeps organizations of all sizes secure. Its innovative technology and seamless integrations create a feature-rich platform that includes everything a sophisticated security team needs, while empowering channel resellers, service providers and organizations of any size with the collaboration and transparency required to establish a coordinated and mature defense.

With a vendor-agnostic approach and preexisting integrations, Adlumin's Security Operations Platform obtains security telemetry from across an organization to provide greater insights into security alerts and streamline workflows. Organizations can use Adlumin's Security Operations Platform on their own or get full transparency and visibility while utilizing the 24/7 monitoring and response services provided by the Adlumin Managed Detection and Response (MDR) team. Whether organizations manage the platform on their own or with MDR, Adlumin consolidates all security needs for a unified experience.

---

1. https://www.prnewswire.com/news-releases/managed-detection-and-response-mdr-market-size-to-reach-usd-21-93-billion-in-2030-emergen-research-301718957.html#:~:text=The%20Managed%20Detection%20and%20Response%20(MDR)%20market%20is%20expected%20to,USD%2021.93%20Billion%20in%202030.

2. https://www.gartner.com/en/information-technology/glossary/endpoint-protection-platform-epp

3. https://www.alliedmarketresearch.com/endpoint-detection-and-response-market-A16635#:~:text=Endpoint%20Detection%20And%20Response%20Market%20Research%2C%202031,25.3%25%20from%202022%20to%202031

4. https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

5. https://www.stratospherenetworks.com/blog/what-is-xdr-your-guide-to-extended-detection-and-response/

6. https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

7. https://www.gartner.com/document/4007995?ref=algorightrec&refval=4008795

8. https://www.gartner.com/document/4015541?ref=solrAll&refval=362368735

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com

---