

Enterprise-ready security with cloud-native Managed Extended Detection and Response (MxDR)

On-premises Endpoint Detection and Response (EDR)

- Alert fatigue
- Storage challenges
- Data disparity
- Lengthy time to detect and respond

Cloud-native MxDR

- Extended visibility
- Automation
- Data optimization
- Security-as-code

High context alerts through extended visibility

	EDR	MxDR extends to
Coverage	Emails, applications and devices	Identities and cloud environments
Visibility	On-premises	Multi-cloud and even multi-country
Alerts	Many false positives and negatives, and no prioritization	Machine learning proactively finds anomalies and exfiltration
Results	A siloed and limited view	Better decision making and resource allocation


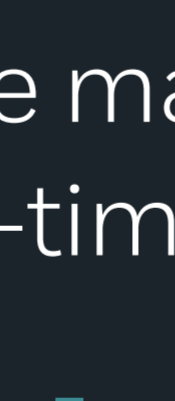

Reduced manual work for security teams with automation

	SOC analysts	MxDR automation
Tier One	Review daily alerts to verify genuine incidents	With a single security analytics platform working across a multi-cloud environment, automation can handle Tier One and Tier Two tasks, offering SOC analysts greater speed to insight. AI connects data streams, ingesting and verifying alerts across the enterprise. Actionable information is reported to security analysts.
Tier One	Configure monitoring tools	
Tier Two	Address security incidents and gauge threat level	
Tier Two	Pinpoint affected systems and run diagnostics	
Tier Two	Create strategy for containment and recovery	
Tier Three	Manage critical incidents	
Tier Three	Carry out vulnerability assessments and penetration tests	Cloud-native MxDR supports all Tier Three activities, hunting queries, running playbooks, and even deploying infrastructure as code.
Tier three	Assess organizational resilience to isolate weaknesses	

Data optimization for transformation and compliance

Traditional EDR environment	MxDR
Log collection bottlenecks	Enhanced log detection stores lower value data in a cloud data lake while routing high-value data into detection systems.
Limited search capacity	Parsing, tagging and filtering of security data helps speed up threat detection.
Federated organizational structures	A continuous process that prevents blind spots utilizes risk-driven, technology-agnostic use case management to adopt proven security models.

Security as code makes infrastructure changes in real-time

- 
Update content in real-time: Detection rules, playbooks, reports automation rules and hunting queries, updated via CI/CD pipelines.
- 
Deploy through scripts: Save resources without deploying new virtual machines or hardware, for faster time to insight.
- 
Upgrade your security culture: Automate scanning and testing, catalog best practices, and standardize security across every workspace and project.

A Managed XDR solution delivers unparalleled confidence in enterprise security

-  Mitigates the cybersecurity skills gap
-  Gives 24/7 extended visibility
-  Guarantees the use of best-of-breed tools
-  Eliminates alert fatigue for internal teams
-  Ensures incident response in real-time

Ready to speak to an expert?

[CONTACT US →](#)