

Managed Detection and Response (MDR) for AWS

eSentire MDR for AWS delivers improved threat detection, 24/7 threat hunting, deep investigation, and a 15-minute mean time to contain.

eSentire offers MDR security solutions that integrate with native AWS security services. We address six critical security domains to protect your cloud environment, aligning with your organization's unique strategy and requirements within AWS.

AWS L1 Managed Security Service Provider

eSentire is a member of the AWS Partner Network and was awarded the AWS Level 1 MSSP competency after successfully completing a technical audit by AWS security experts.

24/7 AWS Managed Security

Managed Detection and Response <ul style="list-style-type: none">- 24/7 monitoring, investigation, and alerting of AWS security events	24/7 Security Operations Center (SOC) Cyber Analysts and Elite Threat Hunters detect and respond to events leveraging best-of-breed technology, proprietary AWS threat detectors, and our 100% AWS powered Altas XDR platform. We combine deep packet inspection in AWS cloud with proprietary attack pattern analysis to detect threats and disrupt them with multiple response mechanisms.
Host and Endpoint Security <ul style="list-style-type: none">- MDR for AWS-based resources	Full-scale visibility, threat hunting, and response to threats on virtualized endpoints within AWS leveraging best-of-breed endpoint technology and 24/7 SOC Cyber Analysts.
Cloud Security Posture Management <ul style="list-style-type: none">- AWS resource inventory visibility- AWS security best practices monitoring- AWS compliance monitoring	Full visibility and monitoring of your AWS resources with expert context and reporting against risks caused by misconfigurations, resource misuse, and improper configuration for regulatory compliance.
Vulnerability Management	Fully managed vulnerability scanning of your AWS infrastructure, including reports, dashboards, and service from dedicated experts to assist with prioritization of vulnerabilities to be remediated.
Network Security <ul style="list-style-type: none">- DDoS mitigation- Managed IDS/IPS	24/7 monitoring of potentially malicious traffic and DDoS attack patterns within your AWS infrastructure. Included professional services for the optimal configuration of AWS Shield Advanced.
Application Security <ul style="list-style-type: none">- Managed Web Application Firewall (WAF)	24/7 monitoring for exploits and attack techniques against your web-facing applications and APIs. Included professional services for the optimal configuration of AWS WAF.

Types of risks we monitor for in AWS environments

- Exposed services and data
- Improper resource usage
- Unusual privilege changes
- Unusual admin activity
- Data exfiltration
- Activity from known bad IPs

Team eSentire is here to harden your defenses and strengthen your AWS security

Everyone on Team eSentire has a role to play in keeping your business secure. With MDR for AWS you are supported by a Cyber Risk Advisor, 24/7 access to our SOC Cyber Analysts, Elite Threat Hunters, Threat Response Unit (TRU), and Managed Risk Services Consultants.