aws partner network | competency level 1 MSSP

aws marketplace

24/7 Managed Security for Your AWS Environment

Work with AWS Partners with Level 1 Managed Security Service Provider (MSSP) Competency to help protect your AWS environment and receive remediation guidance.

Industry-first Managed Security Services

Level 1 Managed Security Services include ten specific 24/7 security service areas each with technical and operational requirements designed to help MSSPs to provide protection, monitoring, and response services for essential AWS resources.

AWS Partners with Level 1 MSSP Competency:

- Meet or exceed Level 1 Managed Security Services requirements
- Fully operationalize native AWS security services such as Amazon GuardDuty, AWS Security Hub with 24/7 response
- Detect misconfigured AWS resources to improve cloud security posture and reduce business risk

Protect your AWS environment

When customers adopt AWS services, the responsibility of security is shared between AWS and the customer. AWS assists customers by ensuring security *of* the cloud, and the customer (in choosing which services to consume and configure from the AWS portfolio) must make risk-based security decisions when it comes to security *in* the cloud. Customer responsibilities can include patching of operating systems, data protection decisions, application-layer security etc.

Whether you're an emerging startup, small to mid-sized business, or a multi-national enterprise, adding the expertise of an AWS Partner with Level 1 Managed Security Service Provider (MSSP) Competency to your organization is a valuable way to increase your security posture and help you manage the customer portion of the Shared Responsibility Model.

Who are AWS Partners with Level 1 MSSP Competency?

These partners have worked closely with AWS security experts to develop offerings combining security tools, skillsets, and processes leveraging native AWS security services, AWS Solutions Implementations, and third-party solutions from AWS Partners with a SecurityCompetency ISV.
They are validated every year for their technical capabilities and operational procedures to meet the baseline standard of quality called Level 1 Managed Security Services. This baseline spans ten specific 24/7 security service areas each with requirements revised annually by AWS security experts.

Why work with an AWS Partner?

AWS Partners with Level 1 MSSP Competency provide at minimum 24/7 security protection and monitoring required in the baseline, and they may offer additional security assessment, design, implementation, and training to support your cloud journey as well.

Partners can integrate, join forces, and work alongside your security teams or provide full outsourcing for your AWS security operations.

They operationalize both native AWS security services such as AWS Security Hub, Amazon GuardDuty, and third-party Security Competency (ISV) Partner products providing the skillsets needed to implement tooling according to AWS recommended best practices, event management with enrichment and triage analysis, and 24/7 remediation support.

Level 1 Managed Security Services Offered by Partners

These offerings are uniquely designed to help protect and monitor your essential AWS resources, delivered to you as a fully managed service available for purchase in AWS Marketplace in the MSSP solution area or directlyfrom AWS Partners with Level 1 MSSP Competency.

AWS infrastructure vulnerability scanning

Routine scanning of AWS infrastructure resources for known software vulnerabilities. AWS metadata for scanned AWS infrastructure is available as part of scan results to better enable reporting and decision making.

24/7 incident alerting and response

Receive notification of high-priority security events and expert guidance on recommended remediation steps 24/7.

AWS resource inventory visibility

Continuous scanning and reporting of all AWS resources and their configuration details, updated automatically with newly added or removed resource.

Distributed Denial of Service (DDoS) mitigation

A system backed by technology and security experts monitoring 24/7 for DDoS attacks against your AWS applications.

AWS security recommended best practices for monitoring

Detect when AWS accounts and the configuration of deployed resources do not align to security best practices.

Managed Intrusion Prevention System (IPS)

Protect your environment from known and emerging network threats that seek to exploit known vulnerabilities.

AWS compliance monitoring

Scanning your AWS environment for compliance standards on two or more of the following: CIS AWS Foundations, PCI DSS, HIPAA, HITRUST, ISO 27001, MITRE ATT@CK, AND SOC2.

Managed Detection and Response (MDR) for AWS-based endpoints

A combination of technology and cloud-security experts working to continuously detect, investigate, and remove threats from within your AWS endpoints.

Security events monitoring and triage

A combination of automated tooling and security experts continuously monitor aggregated AWS resource logs across network, host, and API layers to analyze security events. Alerts and remediation guidance is provided to help customers resolve issues in their environments.

Managed Web Application Firewall (WAF)

A firewall managed service designed to protect web-facing applications and APIs against common exploits.

24/7 Security

Level 1 Managed Security Services have been designed to help customers without increasing complexity or adding unnecessary cost. AWS Partners with Level 1 MSSP Competency provide security services through a combination of AWS-native and third-party security technology. Where possible, this allows customers to utilize familiar or previously purchased tools.

Get started with a Level 1 MSSP today

AWS Partners with Level 1 MSSP Competency can help fully operationalize your cloud security to increase staff efficiency, provide full security visibility across your AWS environment, and add 24/7 expert monitoring and remediation guidance.

Connect with AWS Partners with Level 1 MSSP Competencythrough the AWS Marketplace.