IBM **Security**

IBM Managed Security Services for AWS Edge Solutions

Are you experiencing similar security challenges in your cloud environment?

Protecting against Distributed Denial of Service attacks or protecting web application at the Edge

Balancing the shared responsibility of cloud native controls with your Cloud environment

Ensuring the proper security controls are in place across your AWS environment

Increased risk of cloud misconfigurations due to varying levels of access

The growing security and cloud skills gap that exists within organizations

IBM

IBM Security can help you adopt, configure, and manage cloud native security controls at the Edge

Configuring and managing security controls built into the cloud platform – or platforms – you rely upon can be incredibly challenging, even for the most mature IT/security teams.

If you're struggling with the adoption, configuration, or management of cloud native security controls for Edge functions, IBM Security can help:

- Protecting Web Apps with Web Application Firewall (AWS WAF) including configure and deploy AWS WAF, policy, rules, and AWS Firewall Manager.
- Enable, configure and manage DDoS controls including configure, deploy, monitor and manage AWS Shield Advanced.
- Proactive monitoring and response of cloud native telemetry, alerts, and threats to your organization
- Management and governance of core cloud native controls, as well as security maturity, threat recommendations, and periodic assessments

Managed Network Security Services

Managing network and Edge security devices can help organizations prevent threats. However, the costs and complexity may be high. Resources or expertise are required to take care of the finer details like designing and deploying the right security policy and monitoring and managing operations.

For organizations that need to reduce the cost and complexity of managing network and Edge technology on AWS, IBM Security Services provides management, monitoring, and alerting of Edge security controls in the cloud.

Managed Web Application Firewall (WAF)

This service delivers a steady state support for the native network security features of AWS Web application firewall (AWS WAF) and other WAF ISV solutions.

- Steady state support for WAF with standard 8x5 support provided and severe business interruptions (Severity 1) technician available 24/7 (on-call)
- On-boarding or off boarding of externally facing web applications into WAF
- Health checks to ensure the WAF gateway system are functioning as designed
- Investigate WAF performance issues and generate monthly web traffic management reports

Distributed Denial of Service (DDoS) Mitigation

This service delivers a steady state support for the native network security features of AWS Shield Advanced and other DDoS ISV partners

- DDoS policy management, blocking malicious web traffic/ DDoS flooding
- Investigate performance issues and generate monthly web traffic management reports. Manage allow list/ blocklist IP addresses working with network teams for websites (Geo tagging allow/block)
- Deploy redirect rules on specific websites as and when required.
- Regular operational reviews

Why IBM Security?

- Cloud and vendor-agnostic consulting and managed security services that provide centralized visibility, management, and monitoring of security operations across hybrid multi-cloud environments
- Comprehensive cloud strategy and risk consulting capabilities coupled with leading cloud deployment and managed security operations expertise
- Leader in 15 security segments with 8,000+ security employees and 20+ security acquisitions
- Over 1,000 AWS certified consulting professionals including security specialists

For more information

Learn more about IBM Security Services for Cloud

See our AWS Marketplace listing

aws
PARTNER
Premier Tier
Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency

Contact IBM

IBM Security