IBM Security

aws partner network
Premier
Consulting Partner
Security Competency

aws partner network
Advanced
Technology Partner
Security Competency

aws partner network | competency
level 1 MSSP

One-minute brief

Security confidence for AWS migrations

Key topics

1 The what

Cloud security is a shared responsibility between AWS as the infrastructure provider and the user organization.

2 The why

Client challenges with cloud security can delay decisions for business migration and modernization to AWS Cloud.

3 The how

IBM Security™ is aligned to the AWS Cloud Adoption Framework and equipped to help optimize and accelerate execution of AWS shared responsibility model.

1 The challenges customers face

- AWS customers are responsible for overall configuration, compliance and security for their hybrid cloud enterprise.
- These customers face such obstacles as advanced threats, skills shortages, and regulatory and compliance requirements for data and privacy.
- Customers also need to implement policies and manage threats in their hybrid cloud environments.
- AWS has validated IBM Security as an AWS Security Competency provider for services and and technology to help increase their cloud security posture, monitoring and maintenance 24x7.

2 The role IBM Security plays in the program

As an AWS Competency Partner for both technology and services, IBM Security provides a broad set of security solutions to simplify and centralize controls management, visibility and threat management.

Extend

An extension of customer's team

- Protect the AWS Cloud environment with an active advanced security operations solution.
- Embrace expert AWS security guidance and 24x7 security operations assistance.
- Fulfill the requirements of the AWS shared responsibility model.

Optimize

Alignment of AWS native controls with enterprise controls

- Operationalize and manage AWS native controls to simplify and centralize visibility.
- Manage cloud configurations through resource visibility, best practice monitoring and compliance monitoring through a central dashboard.
- Offload elements of security operations to maximize coverage while freeing internal resources for strategic initiatives.

Accelerate

Rapid detection and response

- Improve critical time-to-remediation from the onset of threats to their resolution.
- Augment AWS native detection and response using IBM Security AI.
- Manage endpoint threats with threat hunting and AI-driven detection and response.
- Respond to security incidents using joint runbooks based on security orchestration, automation and response (SOAR).

3 What shared responsibility does

Cloud security confidence for AWS customers requires a comprehensive security program, regardless of where they are on their journey to AWS Cloud. IBM Security helps accelerate their confidence with a broad set of Security Consulting Services and Managed Security Services, and Security Technology for AWS to increase the customer's security effectiveness.

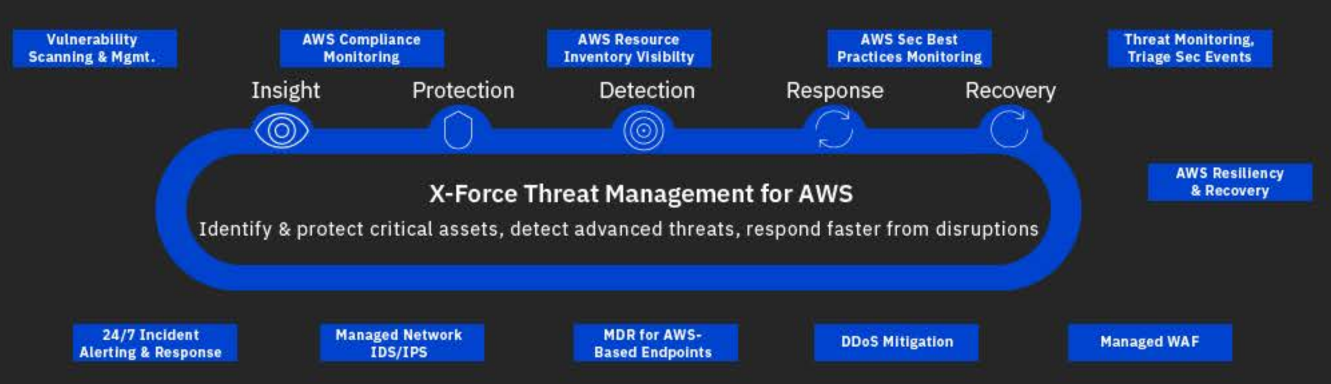
What benefits AWS customers need

IBM Security is a trusted partner with world-class AWS experts and global experience that helps user organizations embrace the AWS shared responsibility model 24x7. Customers get resource visibility, configuration management and end-to-end threat management for visibility, speed and efficiency in investigation and resolution of incidents. A governance model encourages continuous iteration for cloud security to meet business and regulatory requirements as well.

IBM Security Services for AWS Cloud

IBM Security

End-to-end security management and recovery services


Vulnerability Scanning & Mgmt.
AWS Compliance Monitoring
AWS Resource Inventory Visibilty
AWS Sec Best Practices Monitoring
Threat Monitoring, Triage Sec Events
Insight
Protection
Detection
Response
Recovery
X-Force Threat Management for AWS
Identify & protect critical assets, detect advanced threats, respond faster from disruptions
AWS Resiliency & Recovery
24/7 Incident Alerting & Response
Managed Network IDS/IPS
MDR for AWS-Based Endpoints
DDoS Mitigation
Managed WAF

IBM Security Services for AWS Cloud align to all ten capabilities specified by the AWS Level 1 MSSP Competency.

Next steps

Learn more about IBM Security

Study the benefits of our alignment to AWS for security, our expertise and resources, and much more.

Visit website >

Hear from our customers

Software stories
QRadar on AWS:
- ReliaQuest
- Smarttech247

Guardium AWS:
- Adaptive Systems
- Information Insights

Services stories
- Global Distribution
- Global Telecommunications

Visit AWS Marketplace

Purchase IBM Security services and products to complement AWS services for a comprehensive security architecture.

Discover Security Services >

Discover Security Technologies >

Leverage a threat management assessment

Customers can engage a low-cost, rapid AWS Cloud Security Maturity Assessment to identify and prioritize security program actions needed.

See what's covered >

Contact IBM Security at 1-877-426-3774 or

Email IBM Security >

IBM®

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
September 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.