IBM Security QRadar & AWS

IBM | aws

Accelerate your AWS cloud journey with security confidence

Organizations are accelerating their move to cloud to drive business innovation and customer success. At the same time, cloud poses new cybersecurity challenges as the number and types of security threats continue to grow.

As analyst Gartner projects, 90% of SIEM solutions will have capabilities like log storage, analytics, or incident management that are only delivered through the cloud, a leap from the current 20%. With hybrid adoption growing so rapidly, organizations need to extend their security approach to their workloads in the cloud. Yet security teams often lack the baseline visibility.

To provide analysts with a comprehensive view of risks and threats, IBM® Security QRadar® extends visibility to cloud solutions and platforms by collecting, normalizing and analyzing events. Deep integration with Amazon Web Service (AWS) native services helps security teams better detect and respond to threats regardless of where they occur.

1 2020 Cost of a Data Breach Report by Ponemon Institute, sponsored by IBM

Data stats

90%

Of workloads predicted to migrate to the cloud by 2023[1]

$3.58 million

Average amount saved from fully deploying security automation

Better detect threats to AWS workloads

QRadar delivers centralized visibility and insights into the most critical threats across AWS environments such as cloud misconfigurations, policy changes and suspicious user activity. Security teams can easily visualize, filter and prioritize offenses across users, networks, endpoints and cloud.

By leveraging the extensive integrations between AWS services and QRadar, organizations can accelerate their migration to AWS while maintaining visibility and control across the threat landscape.

Extend AWS visibility for better security posture

QRadar integrations with AWS include advanced rules, reports, saved searches, and cloud dashboards for visibility across AWS workloads. The IBM Security QRadar Cloud Visibility app helps detect cloud misconfigurations in AWS environments and address security use cases. The app includes:

– Simplified log source management

– Identity and access management for accounts, users, and IAM roles

– Auto-population of QRadar Network Hierarchy

– Amazon VPC flow log visualization

– Integration with AWS Security Hub and Amazon Detective

Learn more:

– QRadar Apps and Extensions for AWS

Product integrations

QRadar support for AWS native security services includes:

– AWS CloudTrail

– AWS Security Hub

– AWS Network Firewall

– Amazon GuardDuty

– Amazon Detective

– Amazon CloudWatch

– VPC Flow Logs and more

Learn more:

– QRadar on AWS marketplace

– QRadar for Cloud Security website

Need to talk to a security expert?

Contact Us