Security analytics for your multicloud deployments

IBM Security QRadar SIEM solution

IBM

Contents

01

The multicloud revolution is gaining momentum

Modern enterprise needs intelligent security

Hybrid, multicloud adoption is only growing, and with it, an increasing number of data, applications, and workloads are moving to cloud. As more employees work from home and interactions shift from in-person to online, cloud usage is expected to hit a new high.[1]

Gartner estimates that the public cloud services industry will grow exponentially through 2022. The fastest growing cloud market segment will be infrastructure as a service (IaaS), which Gartner forecasts will grow to USD 76.6 billion by 2022.[2]

Security should be at the heart of these cloud initiatives. Cloud security breaches can cost companies more than USD 50,000 in less than an hour.[3] Organizations that rely on IaaS must proactively secure their operating systems, manage network configurations and, of course, protect the data running on these systems.

To keep critical business information safe, security analysts need complete visibility into their entire IT ecosystem—networks, applications, and activities—running on premises and in the cloud. They need the ability to detect threats in real time, identify the use of unauthorized cloud services, and gain clear visibility into whether their cloud accounts and resources are properly configured to maintain security.

> 1 billion lost records

Misconfiguration of cloud environments led to more than one billion lost records in 2019.[3]

> USD 50,000 losses in less than an hour

Cloud security breaches can cost companies more than USD 50,000 in less than an hour.[3]

02

Unleash the power of IBM Security QRadar solutions

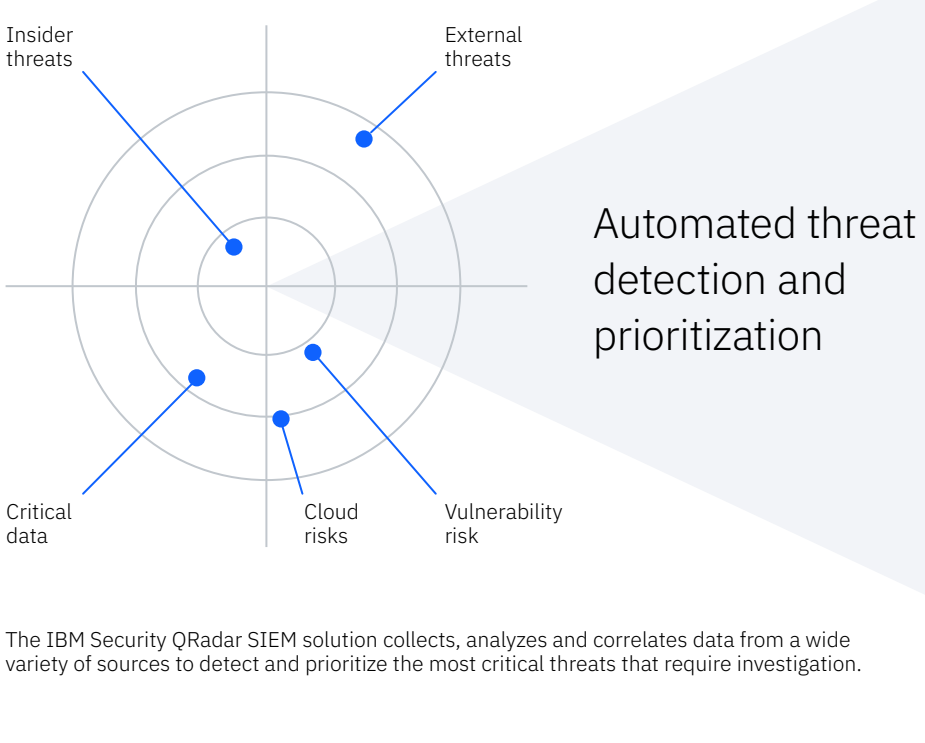
Gain comprehensive visibility across cloud services

The IBM Security QRadar security information and event management (SIEM) solution offers deep integrations with multiple cloud services, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365, IBM Cloud®, and more.

Collecting and normalizing security information from both cloud-based and on-premises environments, the QRadar solution applies advanced analytics to sort through millions of events automatically. The solution helps identify the most critical threats, and provides prioritized, meaningful alerts on potential incidents to protect on-premises and multicloud hybrid environments.

Furthermore, the solution provides security analysts with a unified interface where they can see the most critical threats, review the chronological chain of events that led to each alert, and gain immediate insight into potential attacks. Strong out-of-the-box features help ensure fast deployment and scalability in virtually any supported environment.

Learn more about how the QRadar solution can help you secure your cloud environment →



The IBM Security QRadar SIEM solution collects, analyzes and correlates data from a wide variety of sources to detect and prioritize the most critical threats that require investigation.

03

Integrate the QRadar solution with Amazon Web Services (AWS)

Extend visibility into AWS for better security posture

About 76% of organizations use AWS in some capacity.[1] As this transition from traditional on-premises computing to cloud-based computing continues, security teams need visibility into their cloud-based infrastructure, applications, and data—just as they would in an on-premises environment.

Identify risks that can expose data
Some of the largest breaches in the past few years weren't caused by malicious attackers. Instead, they were the result of accidental misconfigurations in Amazon Simple Storage Service (Amazon S3) buckets that left sensitive data exposed to the public.

Using the QRadar solution, security teams can proactively scan their AWS environments, either on an ad hoc basis or as part of a regular scanning program, to actively look for these misconfigurations and alert analysts when they are discovered. With these alerts in hand, security teams can begin the response process to close holes and protect their data.

Detect threats to cloud data and workloads
As more sensitive data and business-critical assets move to the cloud, AWS is becoming a prime target for attackers. If AWS accounts become compromised, either directly through spear phishing or in the process of lateral movement, AWS data and workloads could end up under the control of an attacker.
To prevent damage, it's critical to have unified, early warnings about threats. The QRadar solution brings AWS security data, including AWS CloudTrail, AWS CloudWatch, and AWS Virtual Private Cloud (VPC) Flow Logs, into a centralized security analytics solution that security operations teams can use to track both external and insider threats from a single pane of glass.

The QRadar solution can collect events from your security products by using a plug-in file that's called a **Device Support Module**.

Using supported protocols and Device Support Modules (DSMs), the QRadar solution integrates with the following AWS components to enable advanced security analysis:

AWS CloudTrail. The QRadar integration provides visibility into user activity by recording actions taken on your account. It supports audit events that are collected from Amazon S3 buckets, and from a log group in the AWS CloudWatch Logs.

AWS Security Hub. This integration uses an integrated system of analytics and real-time defenses to give security teams extended visibility into high-priority security alerts and automated compliance checks on a single security operation center (SOC) dashboard. By integrating with the AWS Security Hub Amazon Findings Format (AFF), the QRadar solution can optimize aggregation of events across multiple AWS security capabilities, instances, and AWS Partner Network (APN) security solutions for deeper security analysis.

Amazon GuardDuty. With this integration, users can analyze continuous streams of metadata generated from their account and network activity found in AWS CloudTrail events, Amazon VPC Flow Logs, and domain name server (DNS) logs.

Amazon VPC Flow Logs. This integration allows customers to collect, store, and analyze network flow logs. It can be used to monitor and troubleshoot connectivity and security issues to ensure network access rules are working as expected.

Amazon AWS Content Extension. This content extension provides new event data parsing on top of the QRadar solution's built-in AWS and accelerates parsing of critical event data. Data, such as instance ID, filename, role name, storage name, and more, is made readily available to users to monitor changes and report on the relative security of their cloud environments.

IBM Security QRadar Cloud Visibility app. This app provides specific AWS dashboards and enhancements, such as:

- Simplified log source management
- Identity and access management (IAM) 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

Why use the QRadar solution to monitor AWS environments?

- Offers centralized visibility into risks and threats across cloud deployments
- Allows security analysts to proactively look for misconfigurations that require a response
- Eliminates silos to help understand the full end-to-end chain of events related to an incident
- Utilizes machine learning to identify high-risk users and spot insider threats faster

Learn more about the IBM Security QRadar Amazon AWS Content Extension →

04

Integrate the QRadar solution with Microsoft Azure

Improve visibility and process events from millions of devices

Microsoft Azure adoption has increased steadily over the years, with 61% of organizations reporting they use the service.[1] As more data and workloads move into Azure, security practices must adapt to protect assets in this new environment. The QRadar solution provides strong out-of-the-box features to bring Azure security data into an enterprise-wide security analytics program.

Using supported protocols and DSMs, the QRadar solution integrates with the following Azure components to help enable advanced security analysis:

Azure Activity Logs. The Azure native event collection service ingests vast amounts of telemetry data and events. This information can easily be sent to the QRadar solution to give security teams deeper insight into potential risks and threats in Azure environments.

Azure Active Directory. The QRadar solution's integration with Azure Active Directory offers security teams the ability to monitor identity, access management, and security events from external resources, such as Microsoft Office 365 and Microsoft Azure.

Microsoft Graph Security API. With the QRadar Microsoft Graph Security API protocol, organizations can ingest alerts from Microsoft Graph Security API, enabling security analysts to quickly investigate offenses.

QRadar Cloud Visibility app. The QRadar solution can detect potential problems in Azure environments and address security use cases. Once offenses are created, the QRadar Cloud Visibility app helps users manage these offenses in the Azure Offense Overview dashboard.

The Azure Offense Overview dashboard displays active offense data in the following charts:

- All users by magnitude
- All users by related rule
- Most severe offenses
- All users by number of offenses
- Magnitude level indicator

IBM Security QRadar Content Extension for Azure. The QRadar Azure content extension adds rules, reports, and saved searches to build on the existing QRadar event parsing capabilities for Azure deployments.

This content extension is specifically aimed at network security management, security rules modification, and virtual network management.

Why use the QRadar solution to protect and monitor Azure components?

- Detect abnormal behavior patterns throughout the IT infrastructure using security rules.
- Monitor and diagnose network traffic through Azure network security groups.
- Manage virtual networks more efficiently.
- Collect event logs and network flow security data in local network gateways.
- Monitor performance and usage of web applications running in Azure.

Learn more about the QRadar→ Content Extension for Azure

05

Integrate the QRadar solution with Google Cloud Platform

Quickly detect anomalies and uncover threats in real time

The Google Cloud Platform is one of the leading cloud solutions with a growing user base at 35%.[1] The solution offers a suite of cloud services that uses the Google infrastructure. The IBM Security QRadar solution offers advanced integration with Google Cloud Platform. It provides centralized visibility by collecting, searching, and analyzing hundreds of data from workloads that reside across environments. Your security teams will be able to better detect and respond to threats regardless of where they occur.

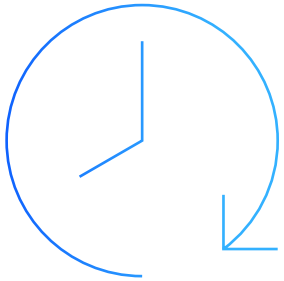
Using supported protocols and DSMs, the QRadar solution integrates with the following Google Cloud Platform services to enable advanced security analysis:

Google G Suite activity reports. The QRadar solution has visibility into audit activity events generated within the Google G Suite platform, including login, user account, Google Drive, and Google Admin.

Your security team will be able to gain insights into the following use cases:

- Account disabled due to suspicious activity
- User information downloaded as a comma-separated values (CSV) file
- Admin privileges revoked by user
- Actor has changed account recovery secret question or answer
- Actor has changed user sharing permissions
- Actor moved an item from the source folder to the destination folder
- User has been suspended

Google Cloud Pub/Sub protocol. With the QRadar protocol for Google Cloud Pub/Sub, users can have improved visibility into anything that creates a sink in Pub/Sub, enabling security teams to act more quickly.



06

See into SaaS

Monitor data from your SaaS applications using QRadar DSMs

Businesses are already using software-as-a-service (SaaS) applications to become more agile, work faster, and support revenue-generating projects—and SaaS adoption is only increasing. Gartner predicts that this service-based cloud solution will be worth USD 143.7 billion by 2022.[2]

The QRadar solution helps organizations gain visibility into SaaS application usage and empowers security teams to detect and block threats more effectively. Prebuilt DSMs enable seamless integration with other solutions in your environment. DSMs are tested and validated by the IBM Security team prior to deployment.

The QRadar solution is designed to help your team easily start monitoring data from your SaaS applications, including Salesforce.com, Office 365, Box environments, and more. When this data is brought into your security analytics program, your team will be able to gain advanced insight into potential threats and uncover potential incidents targeting data in these solutions. Your security analysts will be better armed to spot malicious insiders early in their attack cycle and prevent them from compromising sensitive data stored within these applications and services.

Learn more about DSMs supported by the QRadar solution →

The QRadar solution provides integration through DSMs with a variety of popular SaaS and IaaS offerings.

Amazon CloudTrail
Amazon CloudWatch
Amazon VPC Flows

Microsoft Azure Event Hubs

Microsoft Office 365

Box.com

Netskope Active

Cloudera Navigator

CloudPassage Halo

Skyhigh Networks

OpenStack

Cisco Cloud Web Security

VMware

Salesforce

Okta

Google Cloud Platform

Red Hat® Ansible® platform

07

Empower your security team with the right tools

Explore the QRadar product family

To summarize, IBM Security QRadar solutions are designed to provide the critical insight you need for your growing cloud environments. Using this family of solutions, you can bring multiple silos of data together into a single platform for comprehensive visibility, security analysis, and threat detection. You can identify anomalous behavior to help protect against insider and external threats, identify vulnerabilities that accidentally put sensitive data at risk, and uncover the use of unauthorized cloud services.

Together, these capabilities help provide a comprehensive view of system, network, and user activity within your organization, and they can provide intelligent insights into proactively combatting risks and threats.

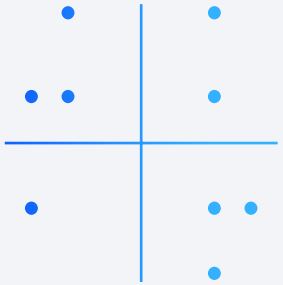
The QRadar solution centrally collects and analyzes data feeds and threat insights from multiple sources across multiple environments, including AWS, Azure, IBM Cloud, SaaS applications, private clouds, and traditional on-premises infrastructures. You can choose to deploy hardware or software on premises, deploy virtual machines in IaaS environments, or consume the QRadar solution as a cloud service from IBM.

As you continue your journey to multicloud, you can count on the same capabilities for security, monitoring, and analytics across the enterprise.

Learn more →

IBM was named a leader in the latest Gartner Magic Quadrant for Security Information and Event Management (SIEM) **for the 11th consecutive time.**

Read the report →



08

Why IBM Security solutions?

IBM operates one of the world's broadest security research, development, and delivery organizations

IBM Security solutions offer one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security intelligence to help organizations holistically protect their infrastructures, data, and applications. It offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security, and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media, and other enterprise business architectures.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. IBM provides full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit ibm.com/financing.

For more information

To learn more about the QRadar security intelligence solution, please contact your IBM representative or IBM Business Partner, or visit ibm.com/security/security-intelligence/qradar.

IBM monitors **billions** of security events per day in more than **130 countries**, and holds more than **3,000 security patents**.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2020

1 10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera, *Forbes*, 2 May 2020

2 Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, Gartner, 2 April 2019

3 Cloud Threat Landscape Report 2020, *IBM Security X-Force® Incident Response and Intelligence Services,* May 2020