One for all: New parity for your enterprise security

IBM QRadar delivers the same powerful security for multiple cloud and on-premises environments.
Bring cloud services into your security analytics program

Cloud adoption is only growing, and with it, more and more data, applications and workloads are moving to the cloud.

According to one recent survey, 93 percent of organizations use cloud services in some form, and 74 percent store some—or even all—of their sensitive data there.1 The adoption of software as a service (SaaS) via the cloud is also here to stay, with the average organization today using 16 SaaS applications.2 And cloud-based infrastructure as a service (IaaS) is experiencing a phase of high growth. Fifty-nine percent of organizations are already using Amazon Web Services (AWS), and 85 percent of organizations are planning a multi-cloud strategy to diversify risk.3

Yet despite outsourcing infrastructure, enterprise security teams are still responsible for several layers of security within their IaaS environments. Among other things, IaaS customers 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 their own visibility into the systems, networks, applications and activities 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.

The power of IBM QRadar

IBM® QRadar® solutions offer deep integrations with multiple cloud services, including AWS, Microsoft Azure, Salesforce.com and Microsoft Office365, to better detect and respond to risks and threats from a single pane of glass. Collecting and normalizing security information from both cloud-based and on-premises environments, QRadar applies advanced analytics to sort through millions of events automatically, identify the most critical threats, and provide prioritized, meaningful alerts on potential incidents to protect on-premises and multi-cloud hybrid environments.

QRadar provides security analysts with a single-screen 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 ensure fast deployment and scalability in any supported environment.

---

Fifty-nine percent¹ of organizations have already adopted AWS in some capacity, and some organizations have opted to migrate their entire on-premises data centers to AWS. As this transition from traditional on-premises computing to cloud-based computing continues, security teams need visibility into the cloud-based infrastructure, applications and data—just as they would need in an on-premises environment.

**Identify risks that can expose data**

Some of the largest breaches in the past year weren’t caused by malicious attackers. Instead, they were the result of accidental misconfigurations in S3 buckets that left sensitive data exposed to the public. Using QRadar, 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 your AWS users become compromised, either directly through spear-phishing or in the process of lateral movement, your 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. QRadar brings AWS security data, including CloudTrail, CloudWatch and VPC Flow logs, into a centralized security analytics solution that security operations teams can use to track both external and insider threats across multiple environments from a single pane of glass.

**Why use QRadar to monitor AWS environments?**

- Gain centralized visibility into risks and threats across multiple environments
- Proactively look for misconfigurations that require a response
- Eliminate silos to understand the full end-to-end chain of events related to an incident
- Leverage machine learning to identify high-risk users and spot insider threats faster

---

Azure adoption increased dramatically from 2016 into early 2017, with 43 percent\(^1\) of organizations reporting they use the service. As more data and workloads move into Azure, security practices must adapt to protect assets in this new environment. QRadar provides strong out-of-the-box features to bring Azure security data into an enterprise-wide security analytics program.

Through an easily downloadable application available from IBM Security App Exchange, QRadar can start ingesting logs and events from Azure, using its out-of-the-box rules, reports and dashboards to help enhance visibility into the context of cloud threats. Based on the Azure Protocol, QRadar integrates with the following components to enable advanced security analysis:

- **Azure Event Hubs**: Azure’s native event collection service ingests vast amounts of telemetry data and events. That information can easily be sent to QRadar to give security teams deeper insight into potential risks and threats in Azure environments.
- **Azure Log Analytics**: This service collects log data from a variety of resources to enable IT operations teams to track performance and find the root cause of operational issues. QRadar leverages this data source and performs advanced security analytics on it to detect potential threats.

Use QRadar to protect and monitor Azure components
- Security rules
- Network security groups
- Virtual networks
- Local network gateways
- Web applications running in Azure

Learn about IBM QRadar Content Extension for Azure.

---

See into SaaS

Businesses are already using SaaS applications to become more agile, work faster and support revenue-generating projects—and SaaS adoption is only increasing. Seventy-three percent of organizations expect that by 2020, more than 80 percent of their business applications will be provided via SaaS.¹ Often, the data stored within these applications is highly sensitive—be it email, customer data or payroll information—and the security of this data is paramount.

QRadar helps organizations gain visibility into SaaS application usage to empower security teams to detect and block threats more effectively. Prebuilt Device Support Modules (DSMs), which are small plug-in files, enable seamless integration with other solutions in your environment. DSMs are tested by IBM Security and validated to work properly in customer environments.

With QRadar, you can easily start gaining insight into your Salesforce.com, Office365 and Box environments, among several other SaaS solutions. When this data is brought into your enterprise-wide security analytics program, you can gain advanced insight into potential threats, uncover potential incidents targeting data in these solutions and spot malicious insiders early in their attack cycle to prevent them from compromising data stored in these applications.

Learn about QRadar-supported DSMs.

Lines of business, cross-functional teams and individual users embrace shadow IT because, in many cases, it helps to make their day-to-day jobs easier. However, when shadow IT is adopted, sensitive enterprise data can end up in various cloud services, accessed by personal accounts and left unprotected from threats. While security teams are ultimately responsible for protecting the data stored in these applications, many find it difficult to know which applications are being used, who is using those applications and what exactly users are doing with them. This insight is vital to securing and protecting sensitive organizational data.

Using IBM QRadar Cloud Discovery, which easily snaps into IBM QRadar SIEM deployments, security teams can gain visibility into cloud services used by the organization, discover unauthorized shadow IT practices, assess cloud application usage and enable an understanding of potential data risks in the cloud.

By ingesting and analyzing firewall and proxy log events, QRadar Cloud Discovery can reveal which cloud applications have been accessed and what data transfers have occurred. It uses a built-in risk analytics engine to calculate application risk scores, understand the normal use of cloud applications and identify deviations that may indicate a risk, such as an abnormally large file transfer to a high-risk cloud service.

**What behavior is risky behavior?**

- Large unapproved upload to a cloud application
- User accessing more cloud applications than normal
- High activity to unapproved, high-risk web applications
Ensuring parity across on-premises and cloud-based environments

QRadar provides the critical insight you need for IaaS and SaaS 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 provide you with intelligent insights into how you can proactively combat risks and threats.

Most importantly, you can do all this—and more—with parity across multiple cloud and on-premises environments.

QRadar 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—into a single, powerful interface for analysis, reporting and insight. The solution can be deployed in multiple ways to support organizations wherever they are on their cloud journeys. Customers can choose to deploy hardware or software on-premises, deploy virtual machines in IaaS environments or consume QRadar as a cloud service from IBM.

With QRadar, as organizations continue their journey to the cloud, they can count on the same capabilities for security, monitoring and analytics across the enterprise.

Learn about IBM QRadar Security Intelligence.
To learn more about how IBM QRadar can help you achieve parity in security for your cloud and on-premises infrastructures, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering 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. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors one trillion security events per month in more than 130 countries and holds more than 3,000 security patents.

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