Enhance cloud security with visibility and intelligence

Guard against security threats with IBM solutions and IBM Managed Security Services

Organizations are managing data across multiple repositories—on-premises, in private clouds, in public clouds, or a combination of the three. Yet the approach to securing data and guarding against threats in the cloud is necessarily different than the approach your organization takes to securing data on-premises.

One of the most challenging to address is how to gain true visibility and intelligence into threats, anomalies and activities across cloud environments.

Strengthen insights, wherever data resides

For organizations using public clouds, IBM QRadar extends the built-in security capabilities of AWS, Azure and other infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments by providing the insights security teams need to understand events and security posture across multiple cloud infrastructures. In addition, QRadar leverages the cognitive capabilities of IBM Watson for Cyber Security to aid security analysts in identifying and understanding sophisticated threats. It draws on security intelligence from millions of security blogs, online forums and white papers to uncover threats that may not be visible within other systems. With IBM, you can put tools into place to help trace suspicious activities, see newly deployed resources, and monitor application programming interface (API) calls and processes—as well as potential insider threats.
Every organization faces risks and needs security in the cloud

The growing use of the cloud has increased the surface area of security risk exposure. And advanced, multi-stage attacks on the cloud can evade detection by traditional security tools designed for on-premises use. What’s more, the dynamic nature of data that is continuously being shared and moved to various locations—from an on-premises database to a public cloud, for instance—adds to the difficulty in knowing who’s doing what, where and when. Development operations initiatives also have introduced faster infrastructure changes and shrinking threat detection opportunities.

That’s why it is important to use security solutions that will help you understand where users are going in the cloud, where traffic from outside sites is originating, and where that traffic is going.

Build in visibility and intelligence

An effective cloud security strategy can provide visibility into virtual infrastructures by collecting and analyzing data in real time across the various cloud components and services. It can enable security teams to correlate events happening both within and outside their firewalls, helping identify anomalies in patterns of user behavior that could indicate a security threat. An effective strategy uses tools that provide proactive monitoring and alerting to help speed remediation. And it provides technology that easily integrates with both on-premises deployments and deployments in a private cloud, a public cloud, or a hybrid combination of the three.

Monitor web application access

Meanwhile, end users who access web applications via your cloud that have not been authorized by the IT department cause an ongoing security threat that can result in damaging vulnerabilities—not to mention the challenges this presents around compliance and auditing.

78% of survey respondents say traditional network security solutions either don’t work or have limited functionality in the cloud.1

Learn why security professionals should be concerned about shadow IT.

Your cloud provider already delivers some security features

Recent high-profile security breaches related to misconfigured administrative rights have created an urgent need for organizations to gain increased visibility into cloud activity. The ability to confirm, for security and compliance purposes, proper access rights in your cloud environment and to detect suspicious activity when unknown users attempt to access your administrative accounts is crucial.

AWS and Azure come with a range of built-in security features that enable you to do just that.

**CloudTrail**

AWS CloudTrail enables you to gain visibility into all activity in your cloud environment, including API calls, and to apply identity and access management (IAM) tools such as IBM Security Privileged Identity Manager to ensure users have the proper credentials. CloudTrail helps improve the visibility of application activity, increase awareness of security enhancements and comply with regulatory audit requirements. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS software development kits, command line tools and other AWS services to provide an event history for simplified security analysis, resource change tracking and troubleshooting.

**Azure auditing and logging**

Azure auditing and logging options provide visibility into activity in your Azure environment, with the ability to centralize monitoring, logging, and analysis of systems to provide continuous visibility; receive timely alerts; and view reports to help you manage the large amount of information generated by devices and services. Azure log data can be exported to security information and event management (SIEM) systems for analysis and integrates with third-party auditing solutions.

- Learn more about AWS CloudTrail.
- Get details on Azure logging and auditing.
IBM adds visibility into your multi-cloud environment

QRadar is an industry-leading family of solutions that integrates with the security features in AWS and Azure, with a wide range of capabilities that show you who’s doing what, where and when within the cloud. It uses dashboards and advanced visualizations compressing thousands or millions of discrete incidents into indications of suspected trouble, and it preserves detailed records of any suspicious activity for future analysis. Advanced logging capabilities and report generation tools help you quickly comply with requirements such as regulatory reporting mandates.

To these capabilities, IBM now adds Watson for Cyber Security. It augments a cloud security analyst’s ability to identify and understand sophisticated threats, by tapping into unstructured data such as blogs, websites and research papers and correlating it with security offenses. IBM QRadar Advisor with Watson combines the cognitive capabilities of Watson and the IBM Security Intelligence Platform to uncover hidden threats and automate insights, revolutionizing the way security analysts work.

QRadar Advisor with Watson:
- Taps into more security information sources than is possible—for any human, or even a group of humans—to absorb
- Helps reduce human error and removes the dependency on research skills
- Repeats analysis automatically as the incident develops or new intelligence becomes available
- Leverages collaboration and crowdsourcing of threat intelligence and activity for more accurate insights
- Can be deployed in minutes with a download from IBM Security App Exchange

QRadar Advisor with Watson gathers context about security incidents by mining local data available in QRadar, then consults with Watson for Cyber Security to perform external knowledge and threat discovery on discrete observations about the incident.

Read what the analysts are saying about QRadar Security Intelligence Platform.
IBM adds still more to accelerate your response to threats

QRadar and Resilient IRP can empower cloud security analysts to reduce the time between detection and action.

First, identify threats in the cloud with QRadar, then, respond with Resilient IRP

Early visibility
In addition, QRadar UBA, an application available in IBM Security App Exchange, provides early visibility into insider threats and analyzes usage patterns of insiders to determine if their credentials or systems have been compromised. Incident response capabilities help support remediation in minutes or days, rather than weeks or months, and cognitive insights help to address security skills gaps, accelerate responses, and reduce the cost and complexity of dealing with cybercrime.

Event correlation
QRadar watches for connected events comparing user identities, source and destination IP addresses, and geographic locations where the activity originated. It examines these linked events for context to better distinguish true offenses from one-off instances of new behaviors.

Multi-cloud and on-premises integration
QRadar capabilities easily extend to multi-cloud infrastructures, as well as your on-premises infrastructure.

Monitoring and alerting
QRadar collects information on data shared across all your security intelligence modules. Once it observes and calculates thresholds for data flow norms on your network, it automatically senses events that violate these thresholds and alerts your security staff. Threshold rules can help detect anomalies such as unusually large outbound data transfers or a high number of login attempts from an unexpected IP address.

Accelerate incident response
Using Resilient IRP, security teams can create a central hub for response that orchestrates the full response process dynamically, enabling faster, more intelligent response and mitigation of cloud issues. Resilient IRP is one of the industry’s only platforms that enables complete incident response orchestration across people, processes and technology. Incident response capabilities help support remediation in minutes or days, rather than weeks or months, and cognitive insights help to address security skills gaps, accelerate responses and reduce the cost and complexity of dealing with cybercrime.
Deploy security quickly from the cloud

For security capabilities specific to the cloud, IBM QRadar on Cloud provides the same robust security capabilities of QRadar, enhancing the security features of AWS and Azure with:

- Delivery as a SaaS product
- No on-premises software or hardware to deploy
- Lower capital and operating expenses

Because it is a cloud-based service, QRadar on Cloud can typically be deployed in days, and helps avoid the cost and time of maintaining on-premises hardware and software.

The solution provides secure gateways that enable you to send your security data into an expertly deployed and managed cloud environment with predictable monthly operational fees. With a hosted, cloud-based solution, the time and associated expenses security staff spend on routine duties can be re-allocated to analysis and planning. System upgrades and application fixes can be conducted remotely by IBM specialists, and can take place without disrupting your local IT infrastructure.

SUCCESS STORY

Limiting risk exposure

A global retailer needed a way to gain visibility into cloud vulnerabilities and limit exposure to risks. QRadar on Cloud with the IBM QRadar Vulnerability Manager add-on enables them to accomplish their goals.

- Learn how the QRadar Data and Application Risk Scanner application supports GDPR compliance.
- Learn how to configure QRadar to collect AWS logs.
- Register for the on-demand webinar, “Five Advantages of Cloud-Based SIEM for Security Intelligence and Operations.”
Use QRadar to monitor SaaS usage

For SaaS applications running in the cloud, QRadar can provide value for discovery and monitoring usage. The IBM Cloud App Analytics for QRadar application, available for download from IBM Security App Exchange at no additional charge, helps detect web application usage within an organization, providing views into what applications are used on your networks as well as their X-Force Threat Intelligence risk scores.

Once your security team has sanctioned use of SaaS applications, QRadar can integrate via APIs to extract critical data, such as usage of Salesforce, to track suspicious login activities as well as changes to sensitive Salesforce Developer Community business objects.

By using IBM Cloud App Analytics for QRadar, you can obtain dashboard views of application and user data on discovered applications, applications that are not approved, high-risk applications, users, high-risk users, rogue activity and incoming traffic.

SUCCESS STORY

Protecting the perimeter

A large, distributed financial institution sought a way to leverage SaaS capabilities while maintaining oversight of an expanded perimeter. Using QRadar on Cloud and device-specific modules for QRadar on Cloud, they were able to effectively protect the entire perimeter—including protection from cloud-borne threats.

QRadar can help you track user login activities, track changes and detect offenses with Salesforce business objects, and stay ahead of threats through close-to-real-time notifications on the dashboard.

Learn how to use QRadar to monitor Salesforce.
Strengthen cloud security with IBM services

Overtaxed security teams can augment their teams’ skill sets and bandwidth when managing their cloud environment with the following IBM services:

- **Adaptive security for hybrid cloud from IBM** offers an extensive set of managed services, all with a single-pane-of-glass view, across IBM and third-party products spanning a multi-cloud environment.
- **IBM Managed Cloud Network Security** uses a vendor-neutral approach to provide security management and monitoring for unified threat management and firewall agents.
- **IBM Vulnerability Management Service** streamlines security vulnerability management and compliance across on-premises and cloud workloads.
- **IBM Intelligent Security Monitoring for Cloud Workloads** enables cloud-based security events to be monitored centrally in client-operated QRadar.
- **IBM Server Workload Protection Services** optimizes endpoint protection in the cloud.
- **IBM Managed Web Defense Services** enhances distributed denial-of-service (DDoS) protection, including cloud workloads. This offering uses Akamai KONA to protect web infrastructure in cloud platforms.
- **Secure software-defined WAN (SD-WAN) service from IBM** provides consulting and integration to help clients enhance security, performance and agility within their wide area networks (WANs).
- **IBM Cloud Identity Service** provides a cost-effective and rapid time-to-value IAM solution.
- **IBM SIEM services** work in tandem with AWS and Azure to provide around-the-clock monitoring and reporting, a flexible design, and alignment of operations to your processes using industry best practices. SIEM services from IBM can provide threat assessment and expert analysis, help reduce potential exposure, and provide a flexible design to plan for future growth and changing technology.
- The **IBM X-Force Incident Response and Intelligence Services** (IBM X-Force IRIS) team can assist you in streamlining incident response by coordinating with your business stakeholders before an incident occurs.

- [Take](#) a tour inside the IBM Virtual Security Operations Center.
- [Watch](#) a video to learn how X-Force IRIS can provide you with proactive and faster reaction to a breach.
Why IBM?

QRadar and QRadar on Cloud can help enhance the security capabilities of AWS and Azure, providing comprehensive visibility and intelligence via powerful incident monitoring and alerts, event correlation, and integration across cloud deployments. Each solution works behind the scenes using the event correlation, monitoring and alerting, and multi-cloud and on-premises integration capabilities delivered by QRadar, as well as optional cognitive security capabilities of QRadar Advisor with Watson.

And, by protecting data and preserving a record of the security practices and events that enable protection in audit-ready form, QRadar helps comply with government and industry regulations such as the General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standards (PCI-DSS).

By enabling complete incident response orchestration across people, processes and technology, Resilient IRP can help you accelerate incident response from weeks or months to days or minutes. Leveraging the cognitive capabilities of Watson and the industry leading QRadar security analytics platform helps to empower security analysts to uncover hidden threats and automate insights. And, when in-house security teams need expert assistance, IBM Managed Security Services can help strengthen your security posture and remove the burden of managing cloud security entirely in-house.

For more information

To learn more about IBM Security solutions for cloud environments, 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 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 15 billion security events per day 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