IBM QRadar for Cloud Security

Detect threats across cloud-based and on-premises environments with a single, unified security analytics solution

Highlights

- Gain visibility into high-risk network, application and user activity in public cloud environments, such as AWS
- Start detecting and monitoring threats in AWS environments with pre-configured rules and reports available from the IBM Security App Exchange
- Uncover Shadow IT by identifying cloud users and the services they use
- View the most critical threats across your on-premises and cloud-based environments from a single, unified console
- Choose the deployment method that best fits your needs, be it on-premises, on cloud, or as a managed service

From shadow IT used by individual employees to company-wide Infrastructure-as-a-Service (IaaS) strategies led by enterprise IT teams, sensitive data is now more distributed and has less oversight than ever before. Despite their best efforts, security teams cannot protect sensitive data if they have no visibility into the environments in which this data resides. As cloud adoption continues to increase, security teams need a way to regain visibility into the data and assets stored in these new environments. Without this baseline visibility, security teams will be unable to effectively protect the organization from threats that lurk across the complex, highly distributed IT landscape.

IBM QRadar enables security teams to monitor activity within cloud-based environments to rapidly detect and respond to potential attacks. In addition, the solution helps discover the use of unauthorized cloud-based services to provide new insight into where data is stored or moved and how it is used. Armed with this knowledge, security and IT teams are now empowered to update policies and either accept or remediate risks accordingly. Whether you are just starting your journey to the cloud or you are already managing multiple cloud deployments, QRadar can help you gain the comprehensive visibility needed to effectively detect, investigate and respond to threats. The solution:

- Correlates and analyzes security data, network traffic anomalies, threat intelligence and user behavior to help rapidly detect threats and potential breaches
- Automatically prioritizes alerts so you can more easily identify the most critical incidents
- Provides a single-pane-of-glass view into security events, vulnerability data and user activity across both on-premises and cloud-based environments
- Offers flexible deployment options including on-premises, on cloud, and as a service (SaaS)

Detect Threats in Cloud Environments

In real-time, QRadar analyzes security data across on-premises and cloud environments to provide security analysts with a single unified, prioritized view of threats – wherever they may occur. With more than 500 out-of-the-box integrations, QRadar can help you gain visibility into activity in traditional network systems and applications, private cloud, SaaS and public cloud environments.

QRadar for Public Cloud

Adopting IaaS offers a number of benefits, including elastic pricing and scaling, but it may also create yet another security silo. Many cloud providers offer their own native security monitoring capabilities. While this is beneficial in theory, it can be extremely difficult for already overstretched security teams to keep track of multiple systems, much less correlate, analyze and detect threats across different environments. To minimize complexity and improve security operations, security teams should look for a security analytics solution that brings together security data from multiple siloed environments, analyzes this data in real-time to detect potential incidents, and provides a single, unified, and enterprise-wide view into threats.

This is where QRadar comes in. QRadar offers deep integrations with multiple cloud services, including Amazon Web Services (AWS), to help security teams better detect and respond to threats in cloud environments.

From the centralized QRadar console, security analysts can:

- View, monitor and analyze API history with AWS CloudTrail events to see which users and accounts made which API calls, as well as the source IP address and time of each call
- Analyze network activity within a Virtual Private Cloud (VPC) using VPC Flows, and correlate that activity with threat intelligence to more effectively detect and respond to threats
- Monitor and alert on EC2 instance usage using AWS CloudWatch logs to help better protect your cloud resources
- View and track Amazon GuardDuty findings from a central security analytics solution to help eliminate the need for multiple isolated systems
- Run pre-built rules and reports tailored to AWS with an AWS Content Pack (available in the IBM Security App Exchange)

In addition to AWS, QRadar collects and analyzes logs from Microsoft Azure, as well as from a growing list of SaaS solutions to help detect and prioritize threats across the entire enterprise IT environment – all from a unified management console.

QRadar for SaaS Environments

Many organizations trust SaaS providers everyday with highly sensitive information. Even if your organization does not officially use SaaS solutions, there's a high probability your employees do. Like it or not, thanks to the ease of use of many SaaS offerings, there's a growing likelihood that your company's files are stored and/or shared in dozens of cloud systems you have limited visibility into.

To help you take back control of your data, QRadar offers out-of-the-box integrations with the leading SaaS providers, such as Salesforce.com, Office365 and Okta. These integrations enable you to more easily analyze user and application activity to rapidly detect and prioritize threats to your data. In addition, the QRadar Cloud Discovery App, which easily snaps into existing SIEM deployments, analyzes network traffic to help identify connections to sanctioned and unsanctioned cloud environments and provide insight into which cloud solutions are actively used. Using this information, security and IT teams are empowered to either accept or remediate associated risks.

In Conclusion

As more and more of your applications and data move to the cloud, your number of security analytics tools shouldn't have to grow as well. The IBM QRadar Security Intelligence Platform enables you to centrally collect and analyze log, network flow, vulnerability and user data across traditional on-premises, private cloud, SaaS and public cloud environments, giving you a single, risk-prioritized view into the most critical threats. The platform can be deployed on-premises or in a supported public cloud, or it can be delivered as SaaS or a managed service. With QRadar, you're empowered to proactively detect, investigate and respond to threats to ultimately keep your data safe – wherever it resides.

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: www.ibm.com/qradar. To download apps referenced in this document visit: https://www.ibm.com/security/engage/app-exchange/

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

November 2017