IBM Security QRadar SIEM

Accelerate your cloud journey with security confidence

Key benefits

- **Gain actionable insights**
  Leverage a wealth of out-of-the-box integrations, analytics and correlation rules to gain full visibility into risks and threats across cloud deployments via a single pane of glass.
- **Reduce alert volume**
  Eliminate silos and chain related events across networks, users, and cloud into a single, prioritized offense.
- **Accelerate threat investigation** Apply artificial intelligence (AI) to quickly uncover the root cause and scope of a threat, helping accelerate investigation processes by up to 50 times.
- **Easily scale with your changing needs**
  Leverage a flexible, scalable architecture that can be deployed on-premises, in the cloud, or as a hybrid model as you grow.

aws partner network

Advanced Technology Partner

Security Competency

Product overview

IBM Security QRadar SIEM provides comprehensive visibility and insights into the most critical threats, enabling security teams to better detect and respond to threats across hybrid environments. A leading security information and event management (SIEM) and security analytics platform, QRadar provides deep integrations with a broad range of AWS services, advanced rules, reports, searches, and dashboards so that teams can easily visualize and prioritize threats wherever and whenever they occur.

Product features

Complete visibility

Leverage deep integrations with AWS native services to ingest a broad spectrum of AWS logs and network flows into QRadar. Gain full visibility and insights across AWS and hybrid cloud workloads via a single pane of glass.

Real-time security analytics

Automatically analyze and correlate activity across networks, users, endpoints, and cloud platforms to detect known and unknown threats.

Prioritized threats

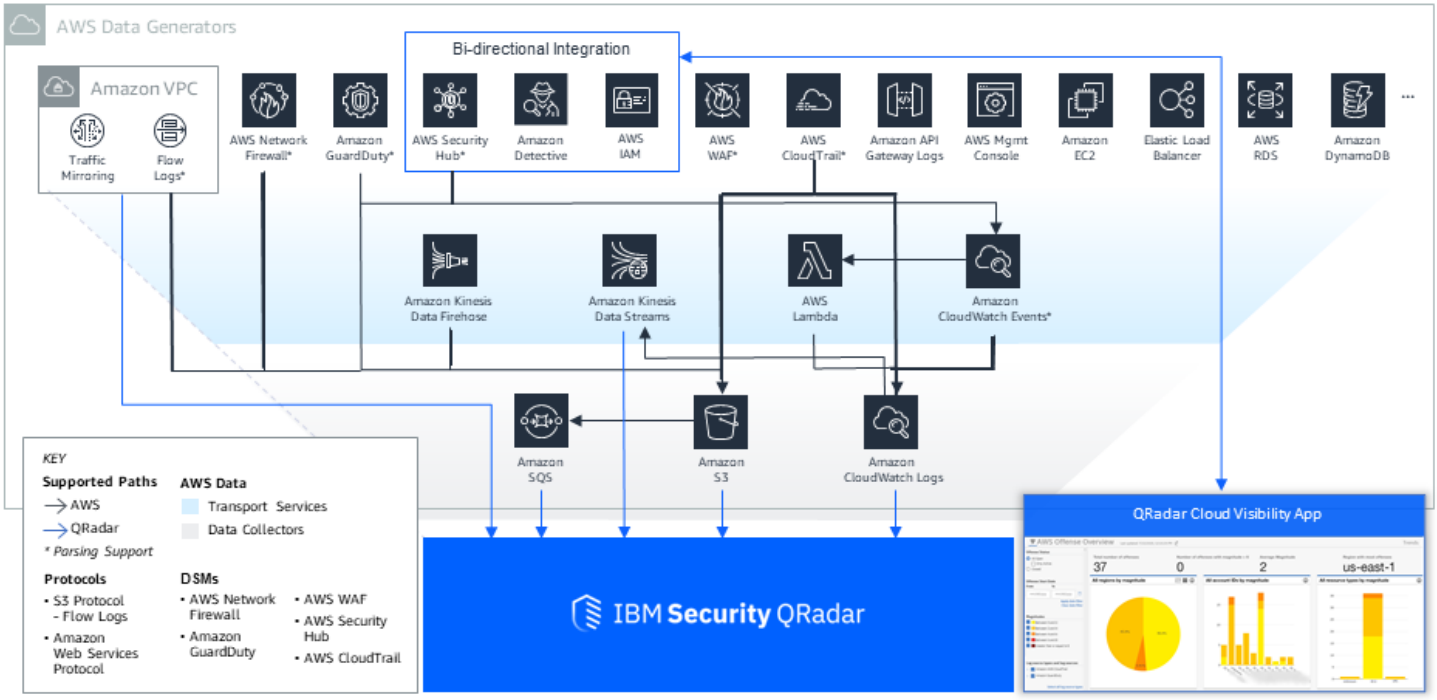
Leverage QRadar's ability to correlate security events across multiple data sources into a single offense to reduce response time. Gain deep insights into key AWS threat vectors including cloud misconfigurations, policy changes, and suspicious user activity.

How it works

QRadar can be leveraged by organizations to rapidly detect critical security threats such as cloud misconfigurations and insider threats, enabling teams to accelerate their cloud journey with security confidence. QRadar can deliver this capability due to its broad set of continually expanding integrations with AWS native services. These integrations extend visibility into AWS environments by collecting, parsing, and analyzing event logs and network flows.

QRadar supports several mechanisms for AWS data ingestion, data parsing, normalizing, and advanced analytics. QRadar leverages AWS transport services to send event logs and flows from AWS services to AWS data collectors (ex. Simple Storage Service, or S3, buckets) which are then sent to QRadar. The QRadar S3 Protocol, for example, supports multi-account, multi-region, and VPC Flow Logs for visibility into network traffic in AWS.

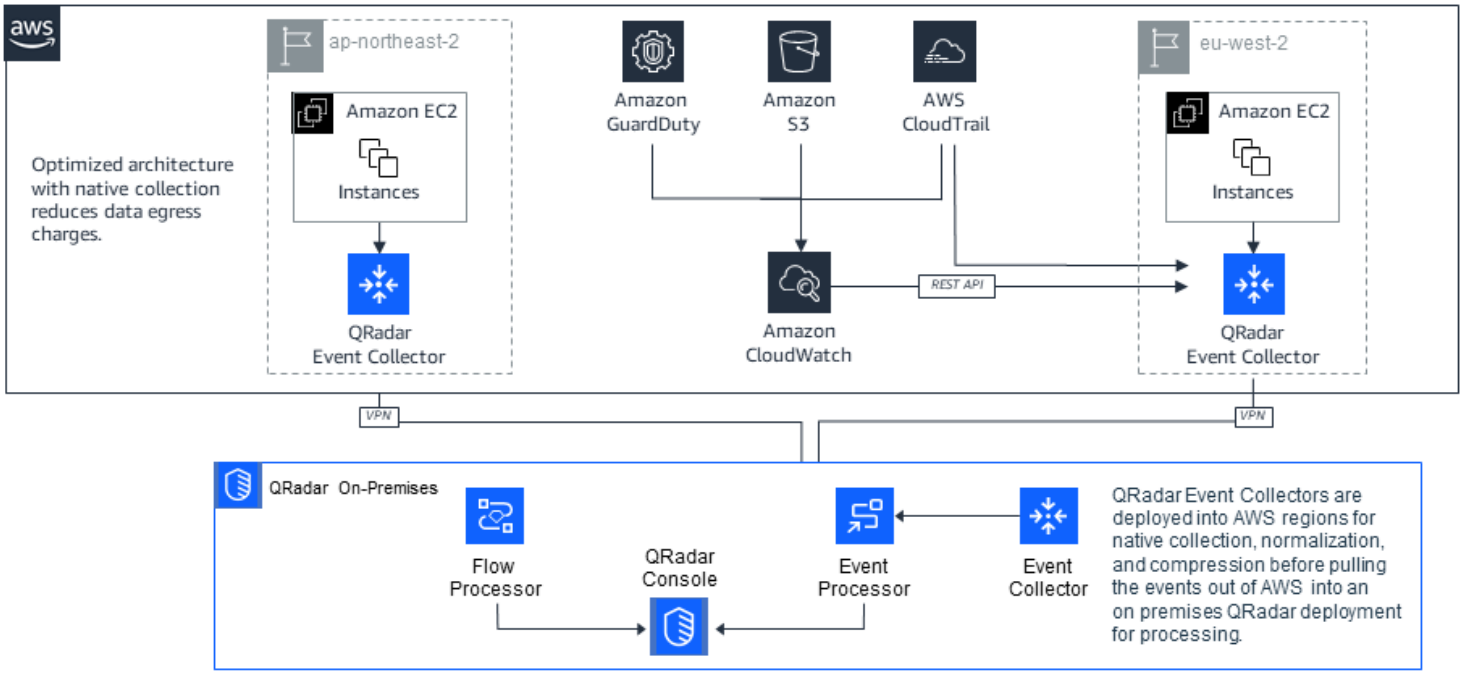
IBM Security QRadar visibility into AWS



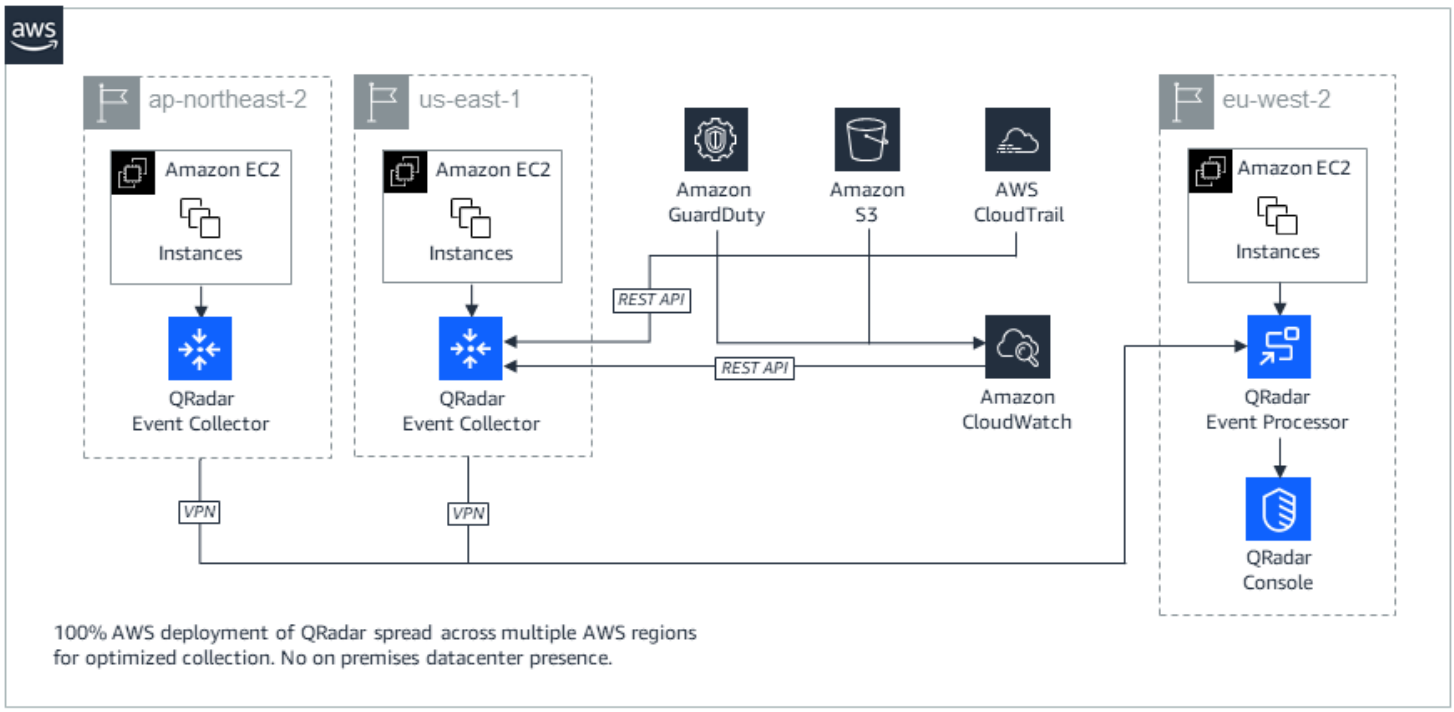
Flexible deployment models

QRadar is built on a flexible, scalable architecture that provides organizations with a range of deployment models to meet diverse business and security needs. QRadar includes the following components: event collectors, event processors, flow collectors, flow processors, data nodes and a central console. All components are available as hardware, software or virtual appliances. Software and virtual appliance options can be deployed on-premises, in IaaS environments or distributed across hybrid environments. There are 4 primary deployment models that customers can implement to secure resources across the enterprise, including AWS environments: On Premises, Hybrid, Cloud, SaaS. Below we showcase the Hybrid and Cloud deployment models.

Hybrid cloud deployment - QRadar event collectors in AWS multi-region



Full cloud deployment - QRadar console, event processors and event collectors in AWS multi-region



ReliaQuest accelerates customer time to value with IBM Security QRadar

Challenge

As more organizations accelerate their move to cloud to drive business innovation and customer success, security teams are struggling to extend visibility across distributed environments leading to siloed data. Without a centralized view or ability to recognize these blindspots, organizations are left vulnerable to attacks.

Solution

ReliaQuest leverages IBM Security QRadar to deliver threat-centric visibility across networks, users, endpoints and AWS environments. By partnering with QRadar, ReliaQuest enables customers with industry-leading visibility, automated threat detection and response, and comprehensive metrics to realize the full power of their security investments.

Benefits

- Visibility into the most critical threats across AWS environments mapped to kill chain stages and MITRE ATT&CK framework
- Unified threat response and investigation workflow, enriched with on-demand data from QRadar, EDR, AWS and third-party apps
- Reduced complexity and risk along with industry benchmarked metrics demonstrating ROI for additional investments and team optimization

> "We're seeing organizations invest a significant amount of resources towards the cloud - whether it's a full cloud or hybrid environment, the support we provide remains consistent across our customer base because of QRadar's flexible deployment model."
>
> **- Mason Vensland, Tier 3 Functional Engineer, ReliaQuest**

RELIAQUEST

About ReliaQuest

ReliaQuest is a global leader in cybersecurity focused on helping organizations achieve desired security outcomes. ReliaQuest does this through GreyMatter which is a SaaS-based, unified threat detection, investigation and response platform that delivers an open approach to Extended Detection and Response (XDR).

> "Cybersecurity, monitoring, detection… it's all a constant race and ReliaQuest is our answer to stay in that race. They're constantly on the mark, making us better – they understand what's going on, what our gaps are and how to fix them."
>
> **- Director of Security Operations, $10.5B Global Management Consulting Firm**

IBM Security

About IBM Security

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, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

Differentiators

- **Accelerate client journey to AWS** via deep and broad integrations with AWS native services while maintaining visibility and control across the threat landscape.
- **Pre-built rules and analytics** start providing insights right away without requiring significant and costly customization efforts.
- **Offense chaining** uniquely identifies and tracks related events so analysts can have end-to-end visibility into a potential incident and all its associated events and flows from one single screen.
- **Addresses the most critical security use cases** across cloud misconfigurations, policy changes, and suspicious user activity, powered by 11 years SIEM leadership in the Gartner Magic Quadrant.
- **Advanced threat detection powered by Watson** goes beyond individual alerts to identify and prioritize potential incidents, applying artificial intelligence (AI) to accelerate investigation processes by 50 percent.

Trends

95%
Workloads expected to migrate to cloud in next 5 years

90%
By 2023 SIEM solutions with capabilities only delivered by the cloud

Additional resources

- QRadar on AWS Marketplace
- Customer success story
- IBM Security and AWS website
- QRadar apps and extensions for AWS

Solution available in AWS Marketplace