WIZ + QRadar®

Executive summary

The Wiz integration with IBM QRadar SIEM and SOAR solutions provides organizations with unified cloud risk visibility, enhanced threat detection, and automated incident response. Wiz surfaces critical cloud vulnerabilities, misconfigurations, and audit logs, while QRadar SIEM consolidates these insights for centralized monitoring and investigation. Meanwhile, QRadar SOAR automates case management and orchestrates remediation workflows, enabling faster, more efficient risk mitigation. Together, Wiz and QRadar empower SecOps teams to manage cloud-native threats with clarity and confidence.

Benefits of the integration

- **Unified Security Insights:** Aggregate Wiz Issues and audit logs into QRadar for centralized monitoring, enriched context, and seamless investigation of cloud and on-prem threats.
- **Automated Workflows:** Automatically create, update, and resolve cases in QRadar SOAR with enriched context from Wiz, reducing manual effort and response times.
- **Enhanced Threat Detection:** Correlate Wiz's cloud-native security findings with QRadar's analytics to detect and prioritize critical risks more effectively.

Use case overview, challenge and solution

Use Case: Comprehensive Cloud Security Management

SecOps teams need tools to manage cloud-specific risks, detect active threats, and automate responses. By integrating Wiz with Microsoft Sentinel, organizations gain centralized visibility into cloud risks, streamlined investigations, and actionable insights to improve remediation workflows.

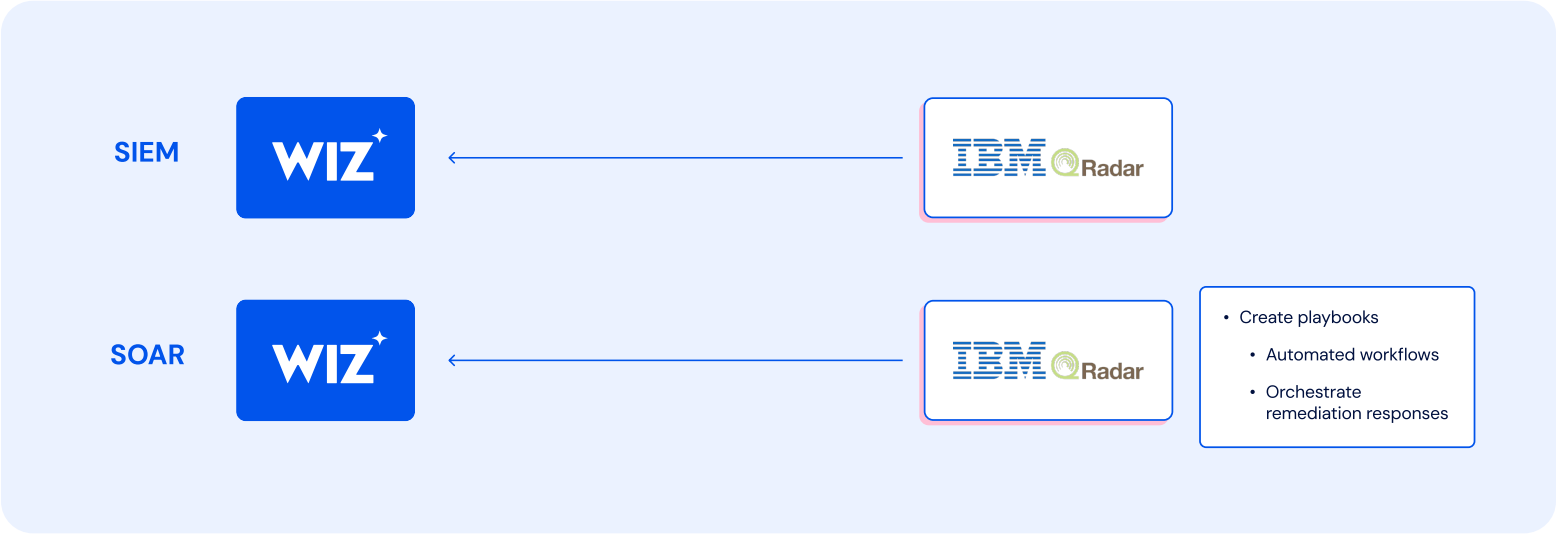
Challenge: Managing Cloud Risks with Traditional SIEMs

- **Complex Data Correlation:** Traditional SIEMs struggle to handle the diverse data formats, high volumes, and unique risks of multi-cloud environments.
- **Fragmented Workflows:** Security teams face inefficiencies due to siloed tools and disconnected data.
- **Limited Context:** Without enriched insights, SOC analysts spend valuable time triaging and investigating cloud threats.

Solution: Unified Threat Detection and Response with Wiz and Microsoft Sentinel

The Wiz and Microsoft Sentinel integration addresses these challenges by:

- **Enriching Cloud Investigations:** Consolidating Wiz's enriched Issues into Sentinel, providing detailed context for vulnerabilities, impacted workloads, and attack paths.
- **Leveraging Query Capabilities:** Using Sentinel's query language to develop a deep understanding of security issues and construct incident timelines.
- **Automating Workflows:** Enabling automated remediation steps, such as notifying stakeholders or creating tickets, directly within Sentinel workflows.
- **Tracking Progress:** Monitoring security metrics over time to measure the team's progress in addressing vulnerabilities and responding to incidents.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About QRadar

IBM QRadar® Suite is a modernized threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle. The portfolio is embedded with enterprise-grade AI and automation to dramatically increase analyst productivity, helping resource-strained security teams work more effectively across core technologies.