WIZ + splunk>

Executive summary

The Wiz and Splunk integration empowers security teams to seamlessly detect, investigate, and respond to cloud-native threats. Wiz surfaces critical vulnerabilities, toxic combinations, and audit log data from cloud resources, while Splunk provides a centralized platform for correlation and analysis. This partnership enables organizations to enhance incident response, track remediation progress, and gain actionable insights across multi-cloud environments. Together, Wiz and Splunk streamline cloud security operations, helping organizations mitigate risks faster and more effectively.

Benefits of the integration

- **Centralized Security Visibility:** Consolidate Wiz Issues, vulnerabilities, and audit logs into Splunk to gain a unified view of security risks across cloud-native environments.
- **Enhanced Incident Analysis:** Use Wiz's contextual data, such as application, container, and microservices details, to support Splunk's incident response workflows and forensic investigations.
- **Real-Time Threat Detection and Response:** Leverage Wiz's cloud resource risk data to trigger automated alerts and response flows in Splunk for faster threat mitigation.
- **Progress Tracking and Reporting:** Monitor key security metrics, such as open vulnerabilities by severity, SLA compliance, and resolution progress, across multi-cloud environments.
- **Seamless Multi-Cloud Integration:** Analyze data from AWS, GCP, and Azure in Splunk to support cloud-native SOC operations.

Use case overview, challenge and solution

Use Case: Streamlining Cloud-Native Incident Management

Organizations operating in complex, multi-cloud environments need to detect and respond to threats quickly and effectively. By integrating Wiz's advanced risk prioritization with Splunk's centralized monitoring and analysis, teams can streamline incident detection, response, and remediation across cloud-native infrastructures.

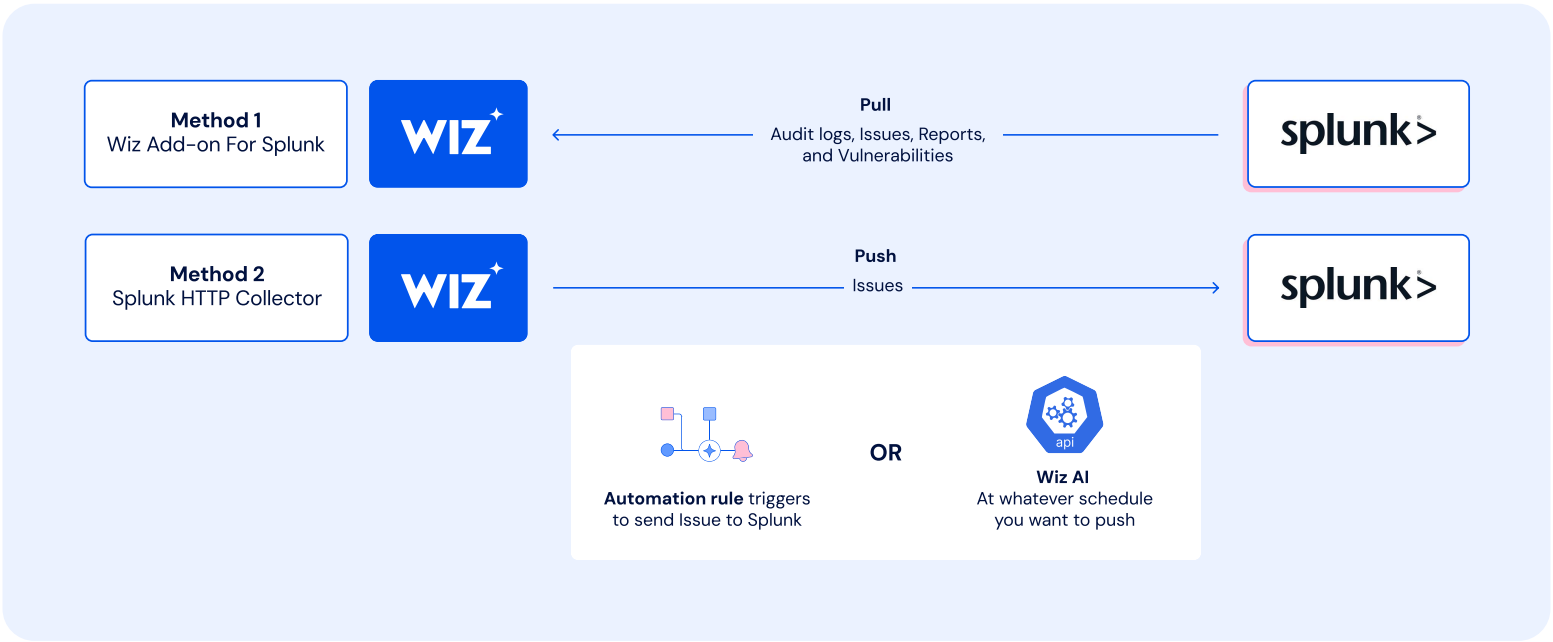
Challenge: Managing Cloud Security at Scale

- **Fragmented Data:** Security teams often struggle to correlate data across cloud environments, leading to blind spots in threat detection.
- **Limited Context:** Identifying risks without sufficient context, such as interconnections between misconfigurations, identities, and vulnerabilities, delays effective response.
- **Inefficient Reporting:** Tracking remediation progress across cloud environments manually is time-consuming and prone to errors.

Solution: Unified Security Insights with Wiz and Splunk

The Wiz and Splunk integration addresses these challenges by:

- **Centralizing Data:** Aggregating Wiz's vulnerabilities, audit logs, and Issues into Splunk for correlation and analysis.
- **Providing Contextual Insights:** Enriching Splunk data with Wiz's security graph to visualize attack paths and toxic combinations.
- **Automating Threat Response:** Leveraging Splunk's automation capabilities to trigger alerts and workflows based on Wiz findings.
- **Enhancing Reporting:** Tracking key metrics, such as SLA compliance and issue resolution, to maintain visibility into security posture.



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 Splunk

Splunk has helped organizations explore the vast depths of their data like spelunkers in a cave (hence, "Splunk").Our purpose is to build a safer and more resilient digital world. Every day, we live this purpose by helping SecOps, ITOps, and engineering teams keep their organizations securely up and running. In 2024, Splunk was acquired by Cisco to help customers continue to build resilience across their entire digital footprint. Today, many of the world's largest and most complex organizations rely on Splunk to protect their mission-critical systems.