WIZ + Microsoft Sentinel

WIZ INTEGRATION NETWORK (WIN)

Executive summary

The Wiz and Microsoft Sentinel integration empowers organizations to secure their cloud environments with enriched visibility, enhanced investigations, and automated responses. Wiz surfaces critical cloud risks, including vulnerabilities, misconfigurations, and toxic combinations, while Microsoft Sentinel centralizes these findings for deep analysis and automated remediation. Together, Wiz and Microsoft Sentinel break down security silos, providing SecOps teams with the tools to detect, investigate, and respond to cloud threats effectively.

Benefits of the integration

- **Consolidated Risk Visibility:** Aggregate Wiz Issues, vulnerabilities, and audit logs into Microsoft Sentinel for a single source of truth in your cloud security operations.
- **Enhanced Investigations:** Use Sentinel's query and analysis capabilities to explore Wiz findings, enabling comprehensive investigations and incident timelines.
- **Proactive Threat Detection:** Correlate Wiz's cloud-native insights with other security data to detect and respond to threats faster and more accurately.
- **Automated Remediation Workflows:** Automate response actions like notifying owners, paging on-call teams, and integrating with case management systems, such as Jira.
- **Track Security Metrics Over Time:** Measure your team's progress in identifying, protecting, detecting, responding, and recovering from security threats with detailed reporting across business units and projects.

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.

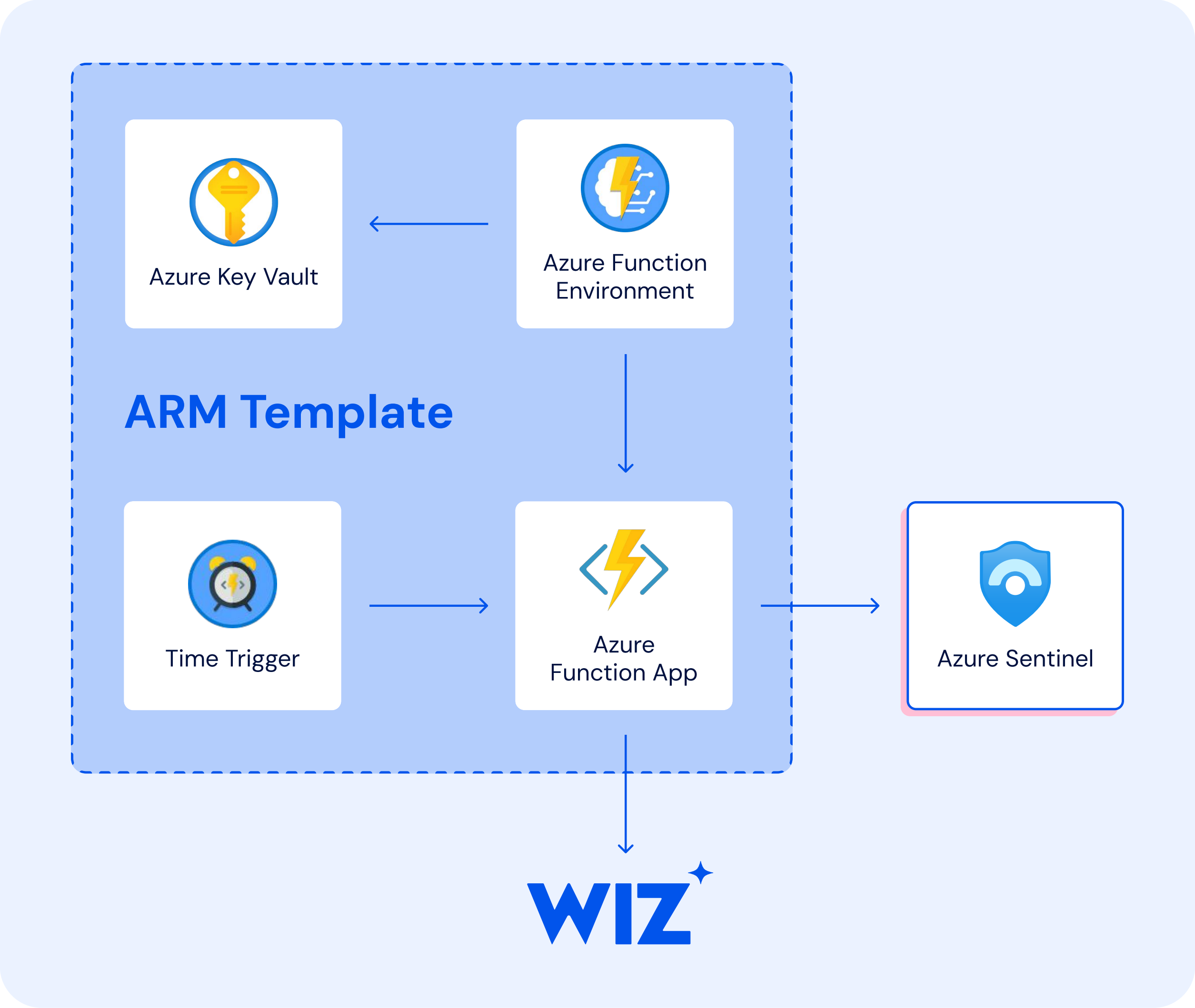
Challenge: Managing Cloud Risks with Traditional SIEMs

- **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 Azure Sentinel

The Azure Microsoft cloud platform is more than 200 products and cloud services designed to help you bring new solutions to life—to solve today's challenges and create the future. Build, run, and manage applications across multiple clouds, on-premises, and at the edge, with the tools and frameworks of your choice.