WIZ + ARMIS

Executive summary of the integration

The Armis Centrix VIPR Pro – Prioritization and Remediation integration with Wiz enables customers to fully operationalize the cloud security remediation lifecycle. VIPR Pro seamlessly ingests Wiz findings and enriches prioritization based on asset profile, business risk weighting, and root cause analysis. Armis then automates ownership assignment for remediation – for cloud engineering, DevOps, infra, or app teams – using their day-to-day workflows. With this integration, mutual customers maintain consolidated visibility and reporting across remediation teams of the status of findings identified by Wiz.

Market challenge

As their cloud footprint scales and grows more complex, security teams need to maintain visibility across their environments, identify security issues, and ensure that high-risk misconfigurations and vulnerabilities are remediated. To ensure that security teams can operate efficiently, and manage risk, they need to be able to automate prioritization of high-risk findings, and collaborate with multiple teams responsible for remediation.

The better together story

The VIPR Pro – Prioritization and Remediation integration with the Wiz Security Platform helps our mutual customers utilize Wiz's cloud risk visibility and security findings to drive the cloud security remediation lifecycle. Security teams leverage Wiz's visibility into their cloud environment to identify the most critical cloud security risks to their business. VIPR Pro's contextualization operationalizes ownership assignment using predictive AI, automates remediation activity at scale, and monitors remediation status through a holistic process. The integration also allows security teams to operate more efficiently: VIPR Pro groups potentially tens of thousands of Wiz findings with a common fix and automates ticket generation across remediation teams. VIPR Pro extends Wiz's cloud security visibility with code-to-cloud root cause analysis to pinpoint high-impact fixes for remediation teams.

Benefits of the integration

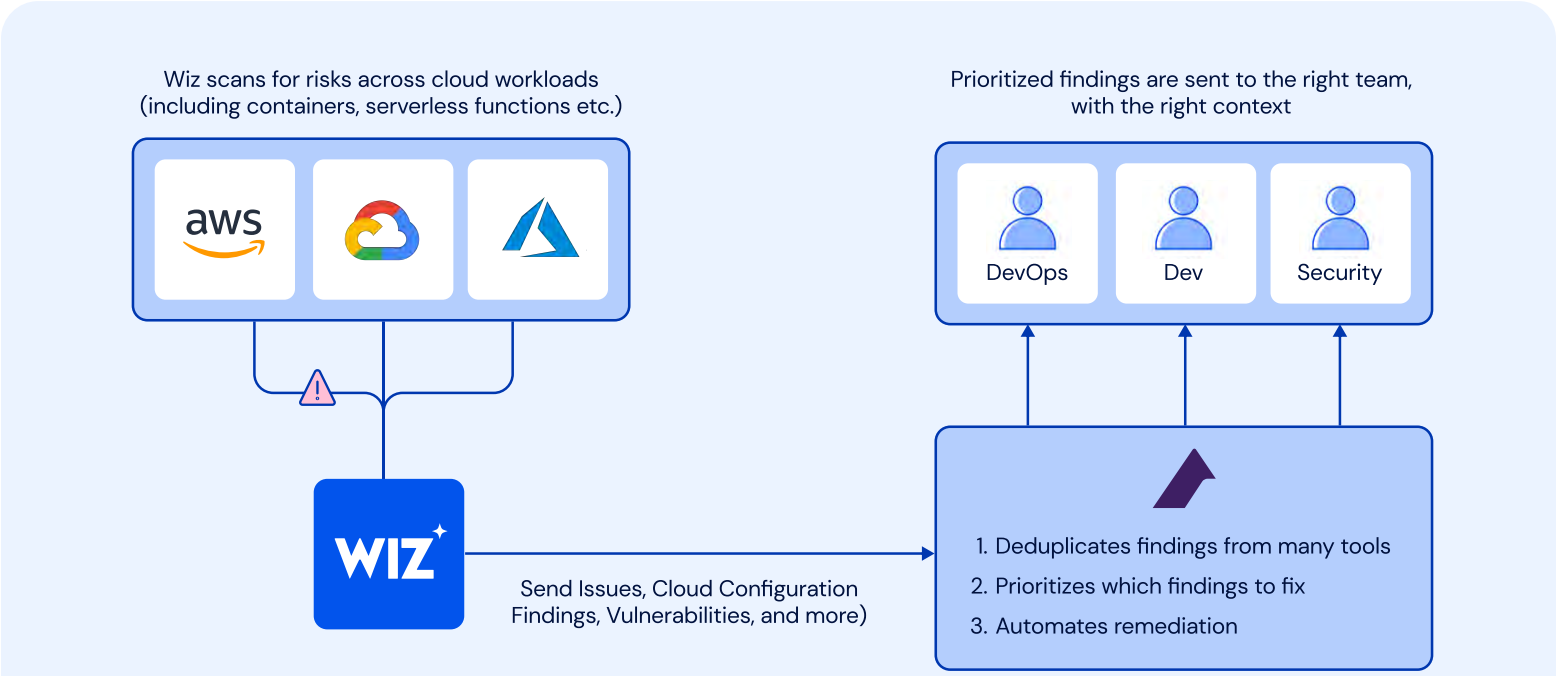
- **Operationalize the cloud security remediation lifecycle** – from Wiz findings to ownership assignment, remediation status, and trend reporting
- **Enrich and extend Wiz prioritization** with asset profiles, security risk weighting, and threat intelligence from other sources aggregated in Armis
- **Automate ownership assignment** for remediation responsibility based on predictive AI and asset policies
- **Identify high-impact fixes** with root cause analysis by linking code findings to Wiz issues and cloud asset visibility
- **Centrally track and monitor** remediation status and activity of Wiz findings across ticketing systems

Use case overview, challenge and solution

Cloud security remediation lifecycle operationalization

Security teams utilize Wiz to identify what cloud security issues need to be fixed, and this integration provides a holistic approach to remediate these issues. Security teams wrestle with assessing the relative priority of findings based on business-specific risks, which teams (DevOps, cloud engineering, infrastructure, and app teams) are responsible for the remediation task, and how they deal with remediation tasks. Also, because cloud security teams contend with limited resources, they need to be able to scale remediation processes across multiple remediation teams. This integration ensures that security teams can automate ownership assignments for high-risk findings, and centrally track and monitor the remediation status of issues.

- Reduces time spent in creating tickets for the same fix across different systems used by different teams
- Supports building remediation campaigns for Wiz findings by category, asset profile, or cloud resource type
- Centralizes tracking and reporting of remediation activity for Wiz findings
- Uses root cause to clearly pinpoint high-impact fixes that resolve multiple upstream findings



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 Armis

Armis Centrix™, the Armis cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time. Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects your entire attack surface.