WIZ + Jed Security

Executive summary of the integration

The integration between Jed Security and Wiz provides value by leveraging Wiz's comprehensive cloud inventory and vulnerability insights. Jed retrieves the full inventory of multi-cloud assets, maps external applications to internal cloud routing paths, and builds accurate end-to-end attack paths with blast radius. Using read-only permissions for Wiz resources, Jed empowers security teams with enhanced visibility, prioritized risks, and actionable insights by aggregating data from Wiz and other connected security tools to deliver comprehensive threat analysis.

Market challenge

It's laborious to turn information into action. Jed automates the previously manual process of threat triage and creates the action plan teams need to maximize value from Wiz with the least number of resources. Jed pulls Wiz Issues, vulnerabilities, and inventory to provide validated attack paths, leading to focused effort on critical issues. Jed connects workflows from Wiz and other tools to decrease time to remediation.

Benefits of the integration

- Shadow IT Asset Discovery: Mapping the entire network infrastructure allows us to isolate threats and simulate attack scenarios with proven end to end attack steps.
- End-to-End Attack Path Analysis: Validates threats with a full attack path from the application layer to exploitable components, ensuring only meaningful threats are prioritized.
- Automated Triage: By surfacing only threats with proven exploitability, the platform is able to streamlines threat identification and prioritization for efficient resolution.

The better together story

Jed takes the wisdom of Wiz, understands the context of remediation, and drives remediation. Jed Security and Wiz complement each other by combining their strengths:

• Comprehensive Threat Visibility: Wiz provides an extensive overview of cloud vulnerabilities, while Jed focuses on only threats with proven exploitability.

• Actionable Insights: Jed filters vulnerabilities to provide a prioritized list of exploitable threats. This allows security teams to focus on critical issues without switching platforms.

• Enhanced Efficiency: With the Jed integration, security teams can work more effectively, leveraging both platforms' capabilities to address current business-impacting threats.

Use case overview, challenge and solution

Overview

A security team using Wiz to manage vulnerabilities in the cloud faces challenges when addressing threats across interconnected systems and non-cloud assets.

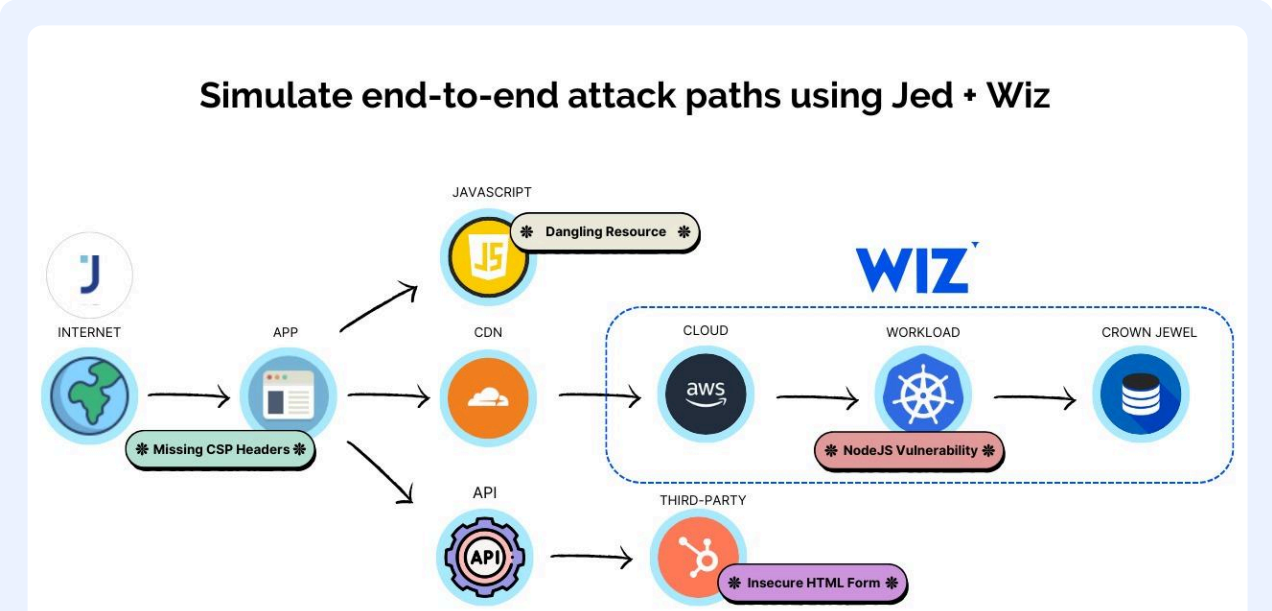
Challenge

The sheer volume of potential vulnerabilities generates significant noise, making it hard to discern exploitable threats. Without Jed integration, teams spend time toggling between platforms and dealing with gaps in threat visibility.

Solution

The Jed-Wiz integration bridges this gap by:

- Providing a single pane of glass for monitoring both cloud-specific and broader infrastructure threats.
- Enabling Shadow IT asset discovery to address unmanaged assets that pose a security risk.
- Prioritizing exploitable threats with validated attack paths from the application layer, enabling efficient triaging and remediation within the Wiz interface.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 45% 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 Jet Security

Jed is the market's first cloud-native CTEM (Continuous Threat Exposure Management) platform. We identify threats with validated end to end attack paths with proven exploitability. Tasks are automatically generated and can be deployed directly to the appropriate component owner.