WIZ + IONIX

Executive summary of the integration

The Wiz-IONIX integration reclassifies Wiz findings based on real-world exposure and confirmed exploitability, ensuring security teams address exploitable risks.

Benefits of the integration

- Automated threat analysis: AI-driven technology replicates human analyst decisions
- Validation of actual exploitability of issues and vulnerabilities identified by Wiz
- Confirmation of attack paths that are genuinely accessible to attackers
- Demonstrates real business impact through validated findings rather than theoretical scoring

The better together story

By integrating IONIX Cloud Exposure Validator with Wiz, customers benefit from a certified integration that helps security teams cut through the noise and focus on what truly matters, validating security exposures that present exploitable risk to your organization. Security teams gain in two key areas:

- **Automated Threat Analysis:** Uses AI-driven technology to replicate and scale the decision-making process of human threat analysts by continuously validating CNAPP alerts across environments, providing evidence of the attack scenario and the required remediations steps.
- **Exploitability Testing:** Incorporates real-time threat intelligence, exposure context and non-intrusive exploit testing to determine whether exposures can be actively exploited. In customer environments, IONIX was able to automate the analysis of over 80% of alerts related to external exposures - and reduced the severity of up to 40% of alerts, relieving alert fatigue and enabling security teams to zero in on genuine, exploitable risks.

Market challenge

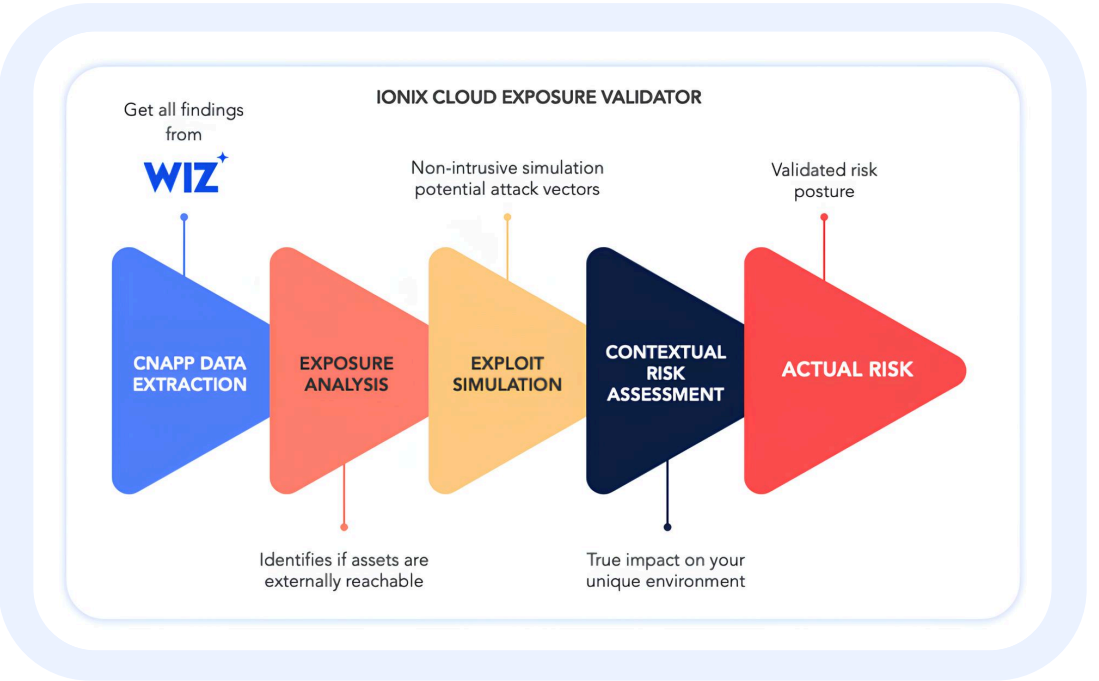
In today's complex cloud environments, security teams are overwhelmed with alerts and findings. Many of these identified vulnerabilities remain theoretical—they may or may not be exploitable in your specific environment. This uncertainty forces security teams to either address everything (an impossible task) or make educated guesses about what to prioritize.

Use case overview, challenge and solution

In today's complex cloud environments, security teams are overwhelmed with alerts and findings. Many of these identified vulnerabilities remain theoretical—they may or may not be exploitable in your specific environment. This uncertainty forces security teams to either address everything (an impossible task) or make educated guesses about what to prioritize.

- Automating Threat Analysis: AI-driven technology replicates human analyst decisions
- Validating the actual exploitability of issues and vulnerabilities identified by Wiz
- Confirming which attack paths are genuinely accessible to attackers
- Demonstrating real business impact through validated findings rather than theoretical scoring

IONIX automatically assesses findings related to external exposures and then reclassifies Wiz findings based on confirmed exploitability, ensuring security teams address actual threats rather than theoretical possibilities.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 50% 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 IONIX

IONIX delivers External Exposure Management that continuously maps, monitors, and validates security exposures across your entire internet facing digital footprint. IONIX discovers assets, pinpoints security issues and actively validates exploitability to help security teams focus on what matters. IONIX transforms overwhelming security data into validated, actionable intelligence with remediation guidance.