WIZ + expel

Name of the product to integrate with Wiz

Expel Managed Detection and Response

Executive summary of the integration

This integration brings together Wiz's prioritized cloud security Issues with Expel's cybersecurity experts. Expel can ingest and analyze Wiz Issues for evidence of post-exploit behavior. These issues are automatically investigated and remediated by Expel's cybersecurity experts with status updates in real time. Mutual customers can reduce the time it takes to fix cloud risks or threats by alerting Expel's team with contextualized and prioritized issues with remediation steps.

Benefits of the integration

By choosing a partner-driven approach, Wiz and Expel provide you with:

- **End-to-end detection to response strategy**: Prioritized cloud risks and real-time threat detections that Expel's cybersecurity team can triage to improve your security posture and reduce threat damage.
- **Extend Wiz capabilities:** Establish a tight feedback loop with Expel experts triaging, fixing, and documenting remediation workflows for threats detected by Wiz.
- **Unified security context:** Add cloud security context and correlate Wiz Issues to security data from SIEM, Network, SaaS apps, Kubernetes, and cloud infrastructure in Expel.

Better Together

Thanks to a robust integration, the partnership between Wiz and Expel brings together what you love about Wiz's CDR capabilities and provides a managed component from Expel. Expel is able to ingest and analyze Wiz Issues for evidence of post-exploit behavior and includes issues via Wiz's Kubernetes runtime sensor. These issues are automatically investigated with status updates in real-time. This allows customers to feel secure responding to the biggest threats in their cloud environments. Expel MDR provides 24/7 detection and response across multiple attack surfaces. Expel's technology-driven approach to MDR leverages automation and AI to deliver best-in-class results by eliminating the noise and prioritizing what matters to the business—with speed, accuracy, and transparency. This partnership takes everything you love about Wiz and couples it with Expel MDR to detect, enrich, and resolve incidents swiftly.

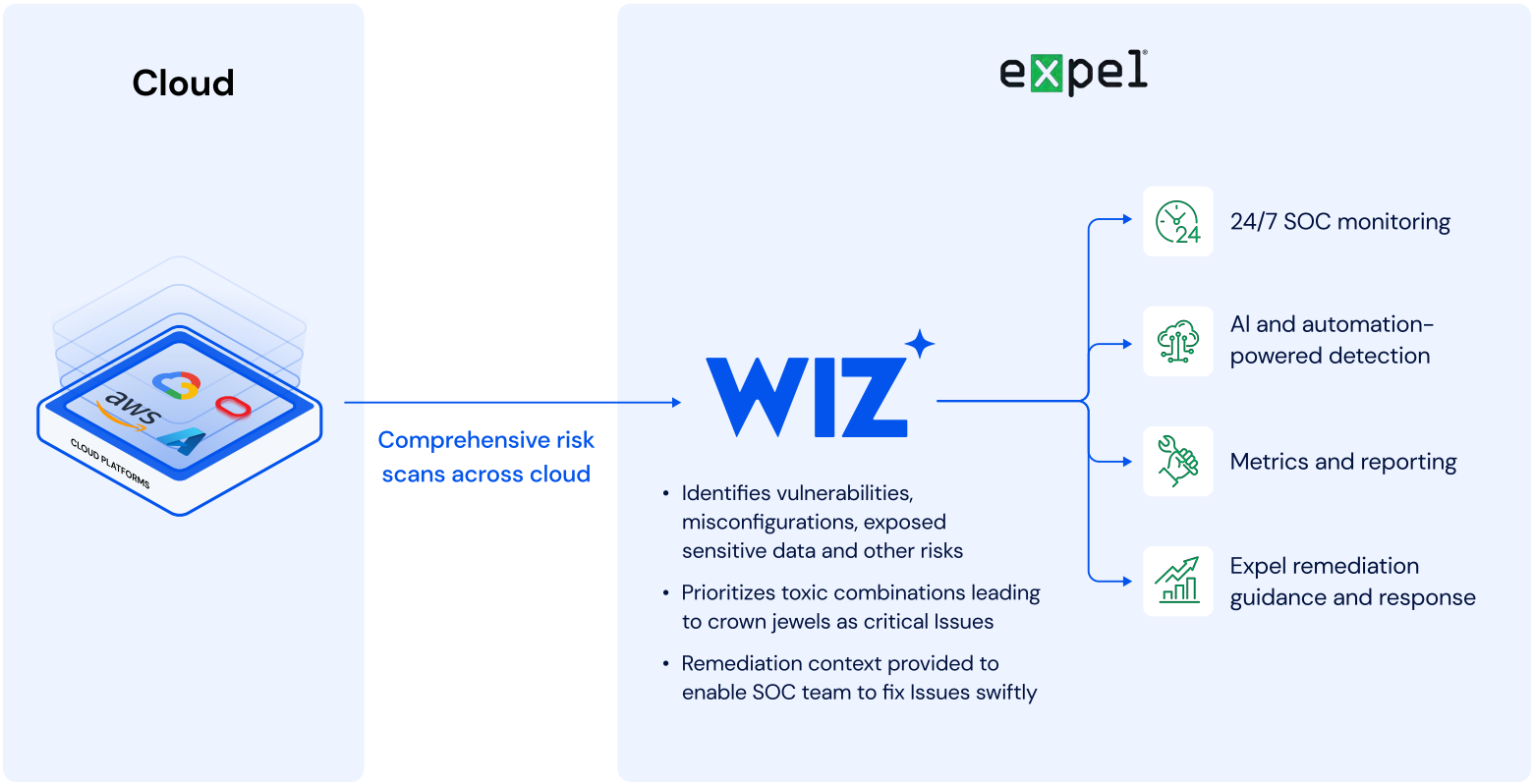
Use case overview

Challenge

As more organizations move to the cloud, the need for a robust cloud security plan remains a top priority. However, many don't know where to start in terms of managing their cloud environments or if they have the right people to do the job. Visibility and coverage gaps caused by cloud modernization are an increasing problem, but often more pressing security problems take priority.

Solution

Expel adds a managed component to what Wiz's customers love about their CDR capabilities. Expel ingests and analyzes Wiz issues for evidence of post-exploit behavior to eliminate the extra work on the customer. This allows for investigations and status updates in real-time to allow customers to feel more secure responding to the biggest threats in their cloud environments.



About Expel

Expel is the leading MDR provider trusted by some of the world's top brands to expel their adversaries, minimize risk, and build security resilience. Expel's 24/7/365 coverage spans attack surfaces, including cloud, with 100% transparency. We combine world-class security practitioners and our AI-driven platform, Expel Workbench™, to ingest billions of events monthly.

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.