WIZ + panther

WIN
WIZ INTEGRATION NETWORK (WIN)

Executive summary

Panther and Wiz empower security teams with centralized, streamlined cloud detection and response. By integrating Wiz's cloud context into Panther's modern, cloud-native SIEM platform, teams gain a single source of truth for comprehensive threat monitoring. Panther's code-driven, real-time detections help correlate activity across Wiz and other infrastructure and security tools to generate more contextualized alerts for fast incident response and streamlined investigations. Panther helps eliminate operational overhead to drastically reduce total cost of ownership.

Market challenge

With legacy solutions, centralizing Wiz data with other critical cloud security data into a single source of truth is expensive and creates excessive ops overhead. Security teams often spend more time maintaining infrastructure and storage than optimizing their detection and response workflows. Black box detection features create noisy, irrelevant alerts and make it challenging to iterate and refine detections to match the pace at which adversaries adjust their attack patterns.

Benefits of the integration

- **Centralized Visibility:** pass through alerts from Wiz into Panther for a unified view of all your cloud security data to better understand your security posture.
- **Unified Correlation:** correlate Wiz signals on cloud workflows, resources, and configurations with other infrastructure and security logs to identify and mitigate complex threats.
- **Threat Coverage at Scale:** combine Wiz insights on cloud workflows, resources, and configurations with other infrastructure and security logs to uncover and address complex threats.
- **Streamlined Investigations:** store Wiz issues and vulnerabilities in Panther alongside other log data and expedite investigations with Panther's powerful query capabilities.

The better together story

Panther and Wiz unite to deliver centralized cloud security monitoring with a single source of truth. Panther's modern SIEM ingests high-volume security logs and analyzes them in real time for rapid detection and response. Wiz adds critical context on cloud risks and threats, enabling security teams to effectively identify, prioritize, and counter threats.

By correlating Wiz insights with other infrastructure and security data, Panther identifies complex attack patterns that traditional tools miss. Panther's Detection-as-Code and CI/CD workflows streamline rule management, reducing false positives and manual tuning. With Panther's cost-efficient data lake and intuitive query language, teams can quickly investigate Wiz incidents and related threats, accelerating response times.

Together, Panther and Wiz empower security teams to scale threat coverage, streamline investigations, and reduce risk in modern cloud environments.

Use case overview, challenge and solution

Use Case: Unified Cloud Threat Monitoring and Response

Security teams need to monitor diverse environments—cloud infrastructure, SaaS platforms, networks, and hosts—for threats such as data exfiltration, ransomware, and insider activity. Effective threat detection requires centralizing high-volume security logs into a single source of truth, enabling faster, more efficient response.

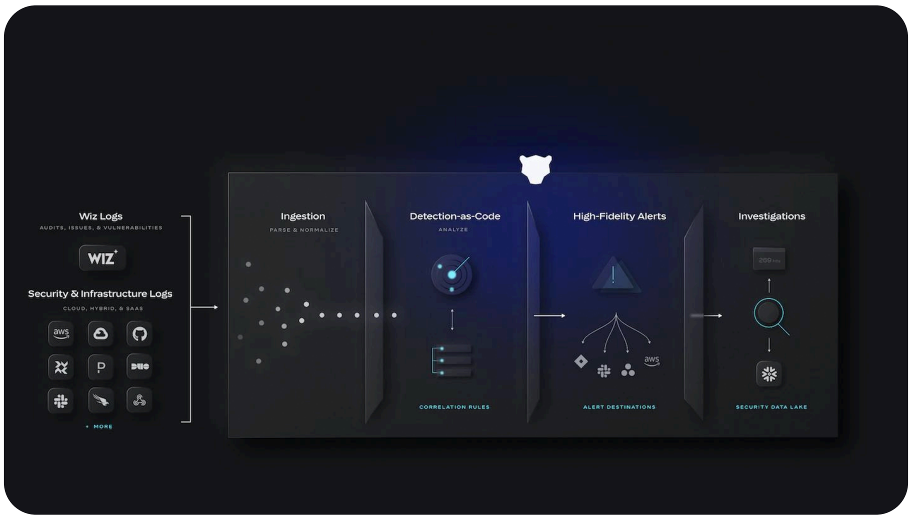
Challenge: Noisy Alerts and Operational Overheard

High log volumes present tradeoffs between scalability, performance, and costs. Traditional solutions struggle with black box detection workflows that create noisy, irrelevant alerts and overwhelm teams with low-priority signals. This slows down incident response and makes it difficult to detect complex, evolving threats in cloud environments.

Solution: Wiz and Panther Integration

Wiz and Panther empower security teams with centralized monitoring and seamless threat detection. Wiz alerts are passed into Panther, creating a unified view of cloud security data with high-scale ingestion pipelines. Panther's correlation rules enrich Wiz insights by connecting them to other infrastructure and security logs, uncovering complex threats. Pre-built Wiz detections offer rapid time to value, while Panther's Detection-as-Code enables teams to customize detections for nuanced threats.

With Panther's advanced search capabilities, teams can investigate Wiz issues and vulnerabilities alongside other critical security logs, streamlining response efforts and improving cloud security visibility. Together, Wiz and Panther offer a scalable, cost-effective solution to detect, prioritize, and mitigate threats efficiently.



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 Panther

Panther is modernizing SIEM with Detection-as-Code for actionable alerts at cloud scale. Our cloud-native platform accelerates detection, response, and investigations to dramatically improve SOC program efficiency. With high-scale ingestion, code-driven detections and correlations, and zero ops infrastructure, Panther customers dramatically improve efficiency and reduce SIEM-related total cost of ownership.