WIZ + NETOGRAPHY

Executive summary of the integration

Netography integrates with Wiz to show you in real-time when threat actors target vulnerable assets in your multi-cloud or hybrid network and when they have compromised those assets. This integration combines the asset awareness of Wiz's Cloud-Native Application Protection Platform (CNAPP) with network security and observability from Netography Fusion's AI-powered platform. Wiz continuously analyzes vulnerabilities, exposures, and other issues across all your cloud workloads. Netography maps your risks with real-time network activity it observes to alert you when it detects malicious activity targeting those workloads or when your assets exhibit post-compromise activity, such as lateral movement and data exfiltration from ransomware.

Market challenge

Knowing when threat actors are targeting your vulnerable or exposed assets spread across multiple cloud platforms is critical to responding before threats like ransomware or data exfiltration can disrupt operations. Operations teams lack a holistic view of all network activity across those platforms because of the challenge of orchestrating and analyzing the data generated by the diverse platforms and tools.

Benefits of the integration

- Reduced risk of operational disruptions from ransomware or data exfiltration from Wiz identifying vulnerable or exposed assets and Netography detecting anomalous communication with those assets and post-communication lateral movement, data harvesting, and exfiltration
- Reduced MTTD & MTTR to active threat actors in your multi-cloud or hybrid network by Netography generating real-time high-confidence detections when threat actors target assets identified by Wiz as vulnerable or exposed, enabling you to initiate response workflows as soon as activity exceeds normal thresholds
- Increase resilience to malicious activity with a real-time view of all network activity targeting vulnerable or exposed assets
- Increased security and observability with a holistic view of assets and network activity

The better together story

The Wiz and Netography integration gives you holistic visibility of risks targeting your vulnerable assets and when those assets exhibit post-compromise behavior like lateral movement, data harvesting, or data exfiltration from ransomware. The integration utilizes the Wiz platform's ability to discover and prioritize your vulnerable and exposed assets across all cloud platforms without deploying agents or configuring external scans. The Fusion platform monitors all network activity with AI-powered analytics and a frictionless architecture that eliminates the burden of deploying sensors or agents.

Fusion integrates data from the Wiz platform to identify any anomalous or malicious communication with vulnerable or exposed assets in your network. Your operations teams receive context-rich, high-confidence alerts of malicious or anomalous activity related to your vulnerable assets real-time, enabling them to mitigate the threat before operational disruptions occur.

Use case overview, challenge and solution

Overview

Cloud assets with high-severity vulnerabilities or network exposures detected by Wiz are at higher risk of being exploited and becoming the source of malicious activity. Netography Fusion combines Wiz's insights with AI-powered network monitoring to detect and respond to active threats targeting your at-risk assets.

Challenge

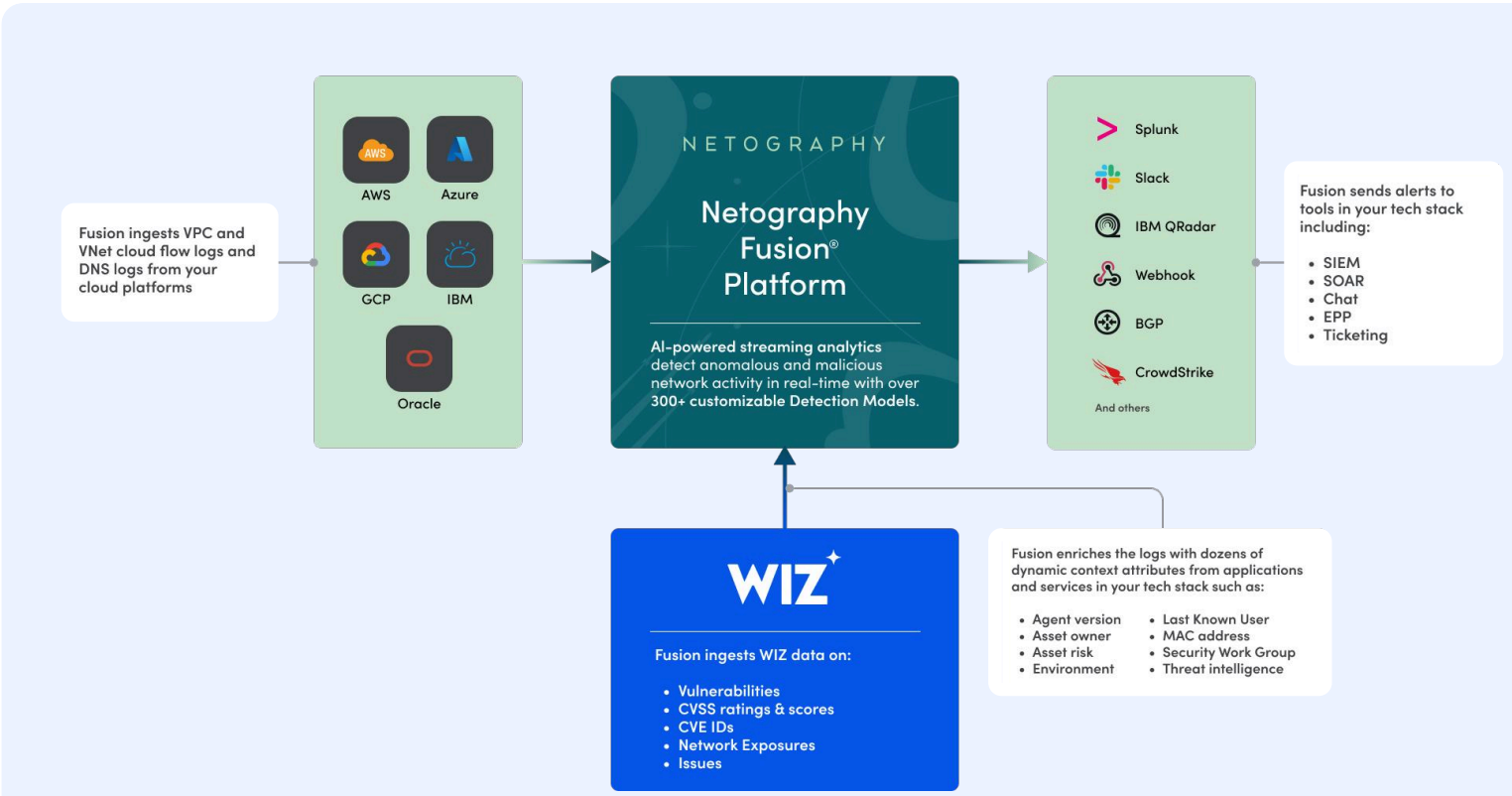
Operations teams lack of comprehensive continuous network monitoring in dynamic, large-scale cloud environments, leaving them unable to detect active threat actors:

- Cloud vendors' proprietary network analytics tools create data silos and provide limited detection of malicious activity.
- Cloud security platforms lack real-time visibility into network activity or forensic capabilities.

Solution

Netography monitors all the network activity across your cloud resources. By integrating Wiz context (such as Vulnerabilities, CVSS ratings & scores, CVE IDs, Network Exposures, and Issues) into Fusion, you can:

- Elevate monitoring of exposed cloud resources with dashboards that focus on activity to/from exposed and vulnerable assets.
- Create escalation workflows for network activity, such as network scanning or exfiltration, when the source is an exposed or vulnerable asset
- Build custom detections that include the Wiz context of the asset in the logic from a library of over 300 open detection models.
- Start monitoring in minutes without sensors or agents.



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 Netography

Netography is the leader in using context-enriched metadata to detect malicious and anomalous activity across your multi-cloud or hybrid network. Netography's AI-powered analytics generate high-confidence alerts that enable your operations teams to respond before threat actors can disrupt operations. Netography Fusion is a 100% SaaS, cloud-native platform that eliminates the burden of deploying sensors or agents.