WIZ + tenable

Executive Summary

Together, Tenable and Wiz give security teams a single platform to manage hybrid infrastructure by uniting on-premises vulnerability data with cloud-native risk context. The integration brings Tenable SC's host-level vulnerability findings into Wiz, normalizing them as resources on the Security Graph, so teams can correlate vulnerabilities across on-prem and cloud environments for faster prioritization and response.

Market challenge

Modern enterprise environments are increasingly complex, spanning hybrid architectures where mission-critical applications rely on public cloud infrastructure alongside stateful databases running on-premises. However, traditional security operations remain severely siloed. Traditional vulnerability management scanners maintain host-level context in isolation, forcing security teams to parse disconnected spreadsheets or data lakes without broader environment awareness.

Compounding this problem, the rise of advanced technologies and frontier AI models has compressed the timeline between a vulnerability disclosure and active exploitation down from days to hours. Security teams are left drowning in a never-ending backlog of low-context alerts, spending excessive time manually triaging findings and tracking down asset owners instead of executing swift, high-impact remediation.

Key Benefits of the Integration

- **Centralized Hybrid Visibility:** Consolidate on-premises scan data from Tenable SC and cloud-native insights from Wiz into a single pane of glass, creating a comprehensive inventory of your hybrid attack surface.
- **Contextual Prioritization:** Enrich Tenable host-level findings with Wiz's cloud-runtime context via the Wiz Security Graph, eliminating noise and automatically identifying true risk paths.
- **Unified Governance & Ownership:** Organize on-premises Tenable assets into vertical Wiz Projects alongside cloud resources, making asset ownership clear and ensuring accountability across security and infrastructure teams.
- **Flexible Connection Architecture:** Connect securely based on your environment's needs—either through a direct connection for internet-facing deployments or via the outbound-only Wiz Broker for sensitive on-premises networks.

The "Better Together" Story

Tenable and Wiz bridge the historic divide between legacy on-premises infrastructure and modern cloud architecture. While Tenable SC excels at identifying host-level vulnerabilities and findings across endpoints and physical or virtual servers using Nessus scanners, Wiz places those findings within a horizontal, cloud-aware operating model.

Through this partnership, Tenable scan findings, specifically those containing CVEs, are automatically fetched and normalized into the Wiz platform. Rather than viewing these CVEs in a vacuum, Wiz correlates them with critical risk factors on the Security Graph, such as misconfigurations, external exposure, and sensitive data access. Together, Tenable and Wiz empower security leaders to pivot away from isolated infrastructure vulnerability patching to holistic, risk-based exposure management across the entire enterprise.

Use Case Overview: Unified Exposure Management

The Challenge: A vulnerability scan flags a critical CVE on an on-prem database server. It's one of hundreds in the backlog. But that server connects to a cloud workload that's publicly exposed and has access to customer PII. The on-prem scanner doesn't know that, and the cloud platform doesn't see the CVE. The risk relationship is invisible, and with AI compressing the window between disclosure and exploitation, the team can't afford the time it takes to manually connect the dots.

The Solution: The Tenable SC integration fetches on-prem vulnerability findings and normalizes them as resources on the Wiz Security Graph. That critical CVE is automatically correlated with cloud-runtime context - the misconfiguration, the external exposure, the sensitive data access - turning a routine backlog item into a prioritized, exploitable attack path with a clear owner.

On-prem assets are organized into Wiz Projects alongside cloud resources, so every finding routes to the right team. No more toggling between tools or manually stitching spreadsheets together.

All the while, connectivity is flexible with a direct connection for internet-facing deployments, or the outbound-only Wiz Broker for sensitive on-prem networks.