WIZ + docker

Executive Summary

Proactively monitoring and remediating container vulnerabilities are key to securing open source components in software supply chains. The Docker-Wiz integration enables organizations to enhance their security posture by providing OpenVEX documents and OSV advisories, minimizing false positives in vulnerability reporting and allowing better technology tracking across their environments in the Wiz platform. The integration also facilitates migration to Docker Hardened Images by providing better visibility into image SBOMs and allowing them to prioritize and manage their security efforts.

Benefits of the Integration

Increased Accuracy in Vulnerability Reporting

By integrating Docker's OpenVEX documents and OSV advisory, customers will experience reduced false positives and more precise vulnerability assessments.

Enhanced Technology Tracking

Customers can track technology usage across their environment, with Docker images being detected as technologies in the Wiz platform.

Improved Base Image Identification

The integration provides more accurate base image identification, moving away from the current guessing approach.

Easier Migration to Docker Hardened Images

Customers will have better visibility into their migration journey to hardened images, allowing them to prioritize and manage their security efforts effectively.

Access to Comprehensive SBOMs

Customers will have access to detailed SBOMs, including SPDX snippets for source-compiled components, ensuring full transparency of dependencies.

Proactive Vulnerability Management

The integration will enable proactive management of vulnerabilities through the use of Docker's advisories and Wiz's scanning capabilities

Use Case Overview, Challenge, and Solution

Use Case: Accelerating Vulnerability Remediation for DevSecOps Teams

By leveraging accurate base image identification and OpenVEX documents, DevSecOps teams using the Docker + Wiz integration can quickly identify and address critical vulnerabilities, reducing false positives, resolution time, and increasing accuracy. This proactive approach enhances security posture and minimizes potential risks.

CHALLENGE
Slow and Noisy Vulnerability Triage

Inconsistent Open Source Image Quality
Public images often include outdated or vulnerable components, creating additional noise and uncertainty during triage.

Unclear Base Image Context
Security teams lack visibility into the exact base image used, making it difficult to assess impact.

High False Positive Volume
Vulnerabilities are flagged without context, leading to wasted effort on non-exploitable issues.

Delayed Remediation Workflows
Developers and security teams spend time manually validating issues instead of quickly resolving real risks.

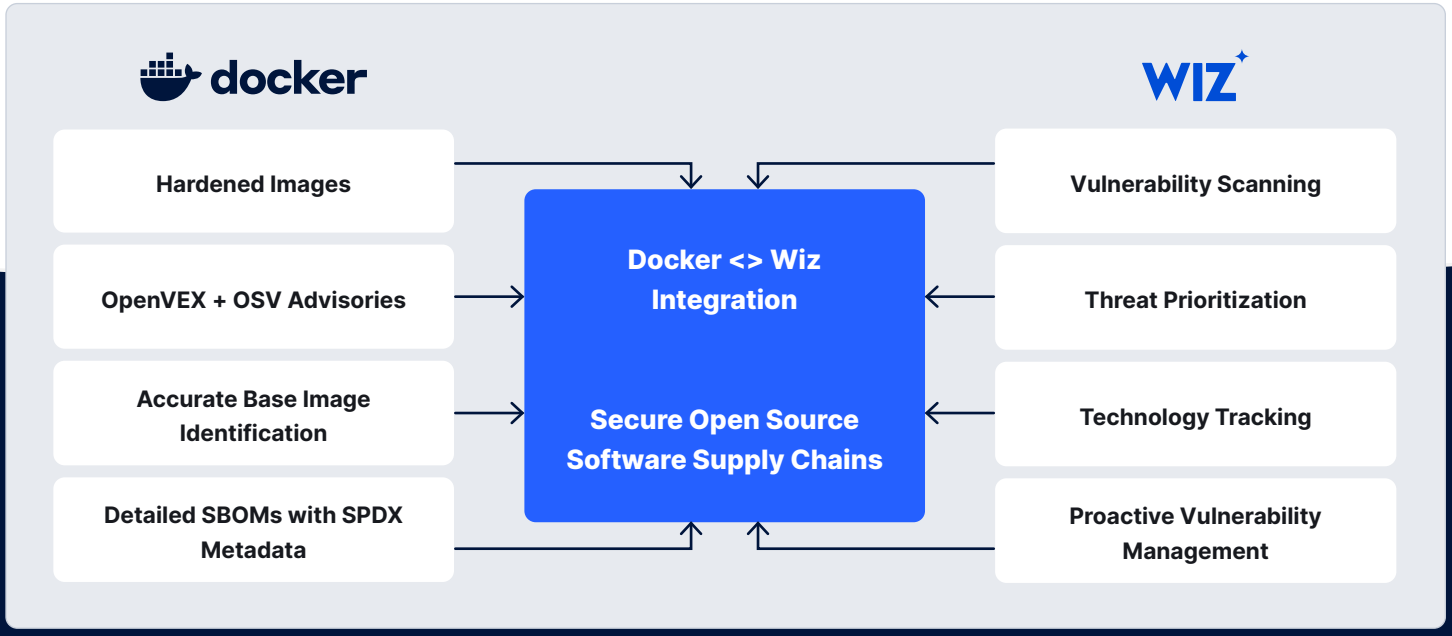
SOLUTION
Enhanced Security and Efficiency with Docker-Wiz Integration

Automate Base Image Identification
Use accurate base image identification to provide security teams with clear visibility, reducing uncertainty and improving impact assessment.

Provide Detailed Vulnerability Context
Deliver OpenVEX documents and OSV advisories to minimize false positives, allowing teams to focus on exploitable issues.

Streamline Remediation Workflows
Enable quick resolution of real risks by integrating detailed issue summaries, reducing manual validation efforts.

Enhance Image Quality Assurance
Maintain up-to-date package metadata and SPDX snippets to ensure transparency and reduce noise from outdated components.



About Docker

Docker is the AI containerization platform helping teams securely build, share, test and run all kinds of applications. Docker's verified components and minimal images with zero CVEs help developers and security teams protect their software supply chains by embedding security across the development lifecycle without slowing down innovation.