

CONTAINER IMAGE AND REGISTRY SCANNING WITH TENABLE CLOUD SECURITY

Identify host **OS vulnerabilities** in container images and registries. Integrate security testing as part of **automated DevOps workflows**.

Cloud-native technologies are built for dynamic auto-scaling, and require security teams to shift their focus from reactive runtime environment scanning to pre-deployment validation. As businesses move their operations into the cloud, maintaining security standards is essential, and cloud-native technologies like containers present significant security challenges. Containers may lack IP addressability, have short lifespans, and exist in massive volume. Just as easily as containers can be spun up, vulnerabilities can be propagated throughout the cloud and capitalized on by attackers.

According to the [2022 Public Container Report](#) produced by **Slim AI**:

- 60% of the top public containers had more vulnerabilities today than they did a year prior
- Container vulnerabilities were detected at a rate that's four times faster than the remediation rate
- Only about 1 in 4 of the developers polled had the skills to harden their containers for use in production

Tenable Cloud Security Key Benefits:

Visibility:

Give Security Operations teams visibility into the security posture of the container images they deploy.

Secure Images Early:

Enable dev teams to validate container images before they build and publish them to artifact repositories.

Tools You Trust:

Leverage as part of the Tenable One Platform

Enforce Security Policies:

Block insecure deployment and ensure compliance with security policies

Facilitate Collaboration:

Allow security teams to create governance models and processes that can be enforced by the development team in existing workflows.







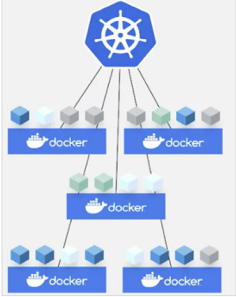


Powered by Tenable Research:

Leverage Tenable's industry-leading research data to see new vulnerabilities in your environment without having to run new scans.



Tenable Cloud Security Brings You Unparalleled Visibility Across the Container Lifecycle from Build to Deployment

Gaining pre-production visibility into containers is critical so you can understand the potential risks in containerized applications before they are deployed. You get the information you need to quickly remediate vulnerabilities early in the development process, reducing risk prior to deployment

Tenable Cloud Security's Approach to Container Vulnerability Management			
BUILD SECURELY	MANAGE SECURELY	DEPLOY SECURELY	MINIMIZE RISKS
 	 Amazon ECR  JFrog Container Registry 	 Jenkins 	 
<p>Enable developers to validate and remediate public container images before building. Automate checks as part of local build processes.</p>	<p>Discover, prioritize and remediate artifacts based on VPR and CVSS scores as they are checked into container registries as part of automated workflows.</p>	<p>Automate checks as part of pipelines and stop risky containers from being deployed. Ensure proper Kubernetes configurations and access controls are in place.</p>	<p>Validate scan results and remediation status in Tenable Cloud Security UI along with supporting infrastructure misconfigurations.</p>

With container security insights integrated into Tenable One, the broader Tenable Exposure Platform, you get unparalleled visibility, context and prioritization of the entire attack surface and a unified approach to security strategy that breaks down silos between teams.



Key Features

Integrated Container Vulnerability Management

Monitor, report and remediate vulnerabilities across all your Docker and OCI images in one place as part of your overall cloud security program with Tenable Cloud Security. See container security vulnerabilities across the development lifecycle and continuously monitor for outdated OS images, OS level vulnerabilities, policy violations, and exposed ports with context into your clusters.

Comprehensive Insights, Prioritization and Targeted Remediation Advice

Inventory container components and evaluate images before they are deployed. This fast and comprehensive view of vulnerabilities provides a detailed assessment of container image risk by repository, ensuring developers don't waste time searching for vulnerabilities or fixing issues by manually combing through the source code or dependent packages. This enables developers to push secure code even faster because security is already baked into the process. Inventory your assets, assess their risk and prioritize based on industry-leading threat intelligence and VPR and CVSS scoring.

Single Policy Framework and Customizable Support

Employ a single-policy framework from IaC-scanning to deployment, and align teams under one security strategy. Create custom policies easily with the Tenable no-code policy editor so you can ensure that industry and corporate security standards are met and Tenable Cloud Security findings are most relevant to your unique security strategy.

Visibility into Deployed Kubernetes Clusters

View containers by Kubernetes cluster in user-configurable widgets inside the Tenable Cloud Security dashboard and via API. Gain key insights into the most critical vulnerabilities, like which clusters are public, what is running in your container infrastructure and the top five Kubernetes misconfigurations - even if they're running in multi-cloud or hybrid-cloud environments.

Continuous Assessment and Live Results Powered by Tenable Research

See new vulnerabilities automatically in the dashboard without having to execute a new scan. Tenable Cloud Security is integrated with the Tenable research feed so when new vulnerabilities, such as zero-days or cyber exposure alerts are discovered, they will automatically be integrated into the container dashboards and identified in your environment.

Integration into the DevOps Toolchains

Enables teams to seamlessly embed security testing as part of existing workflows while maintaining governance by the security team. Supported integrations include Jenkins, Bamboo, Shippable, CircleCI and others, as well as with other continuous integration/continuous deployment tooling used by software developers.

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact



COPYRIGHT 2023 TENABLE, INC. ALL RIGHTS RESERVED.
TENABLE, NESSUS, LUMIN, ASSURE, AND THE TENABLE
LOGO ARE REGISTERED TRADEMARKS OF TENABLE, INC. OR
ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES ARE
TRADEMARKS OF THEIR RESPECTIVE OWNERS.