tenable

# tenable.io™

## Container Security

## Problem Overview

As organizations increasingly depend on software to provide competitive differentiation, revenue acceleration and customer loyalty, the enterprise requirements for secure, rapid and efficient delivery of software have never been greater. DevOps teams are answering the business requirement for speed and agility by streamlining software delivery processes. Increasingly, they utilize Docker containers to quickly build and stand up new services and applications. Containers, however, present significant security risks. The lack of IP addressability, short-lived nature of containers and sheer volume and variety of containers mean securing containers is an ongoing challenge. Tenable.io™ Container Security provides container security testing and audit capabilities, as a modular and independent element of the Tenable.io platform.

## Product Overview

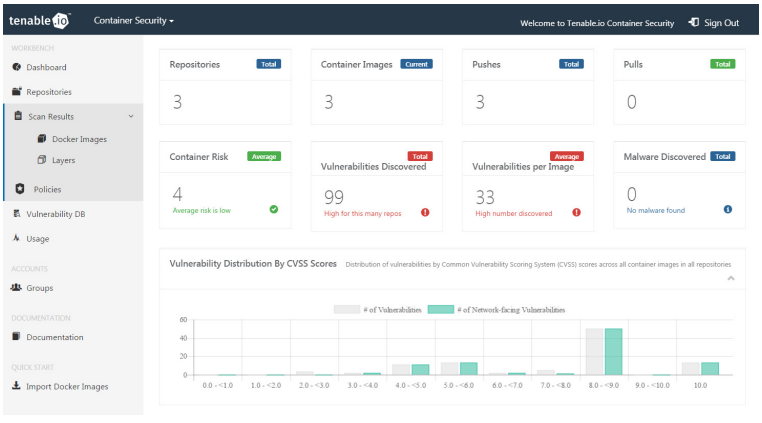
Tenable.io Container Security is a modern vulnerability assessment solution that eliminates container security blind spots without slowing down the application development process. Tenable.io Container Security delivers end-to-end visibility of Docker container images, providing vulnerability assessment, malware detection and policy enforcement prior to deployment. Compatible with the DevOps toolchain you already use, Tenable.io Container security includes out-of-the-box integrations with leading build and continuous integration systems and a RESTful API for custom integrations and dashboards.

Gaining pre-production visibility into containers reduces blind spots and risks. IT security teams can see the potential risks in containerized applications before they are deployed. Developers and DevOps teams get the information they need to quickly remediate vulnerabilities and malware in containerized images as early in the development process as possible, reducing risk prior to deployment and accelerating development.

By seamlessly supporting today's rapid development cycles, Tenable.io Container Security brings proactive visibility and security to solve the security challenges of containers at the speed of DevOps.

## Capabilities Overview

- Automated container image vulnerability testing
- Private container registry – integrate with your existing registry or use the product as a private registry
- DevOps toolchain integrations (build systems, test systems, etc.)
- Container malware detection
- Layer hierarchy intelligence
- Layer-specific vulnerability information and remediation guidance
- Sub-30 second assessment of containers
- Pre-built Security team focused reports and dashboards
- Customizable dashboards for DevOps teams
- Open API to pull data for custom dashboards or other integrations
- Binary inspection of new or non-cataloged code
- Continuous monitoring of stored container images for new vulnerabilities
- Continually updated vulnerability database
- Policy-based enforcement




*Dashboard provides "at-a-glance" visibility into security risks across repositories and images*

# Key Capabilities

## For Security Teams:

Tenable.io Container Security helps ensure Docker containers deployed into production are secure and compliant with enterprise policies. For security teams supporting growing DevOps practices, seamlessly identifying container risks and helping DevOps teams easily address them within the development lifecycle enable innovation without unknown or unacceptable risk.

### *"At-a-Glance" Dashboard Visibility*

Dashboards in Tenable.io Container Security give IT security managers "at-a-glance" visibility into both container image inventory and security. Security teams can view vulnerability, malware and other security data for all container images, as well as the distribution of vulnerabilities across images by CVSS score and risk level. The product also shows each image's OS, OS version and architecture.

### *Continuous Assessment Identifies New Threats*

In the evolving technology landscape, new vulnerabilities are identified daily. Tenable.io Container Security helps security teams quickly respond to new risks by continuously monitoring vulnerability databases for new vulnerabilities. When one is identified, Tenable.io Container Security automatically re-tests all stored container images against the new vulnerability. Subsequently, the product automatically tests new container images for the vulnerability, ensuring continuous protection.

### *Malware Protection for Containers*

Tenable.io Container Security is the only container security solution that assesses container image source code for malware. It uses a custom-built malware detection engine to analyze container image source code and help ensure images are malware free.

### *Enterprise Policy Enforcement*

Enterprise policy compliance can optionally be enforced by monitoring container images for factors such as overall risk score and the presence of malware. If an image is created that exceeds the organization's risk threshold, developers can be notified immediately, with layer-specific information provided to help them rapidly remediate. Policy violations can trigger alerting or can optionally block specific images from being deployed. Policies can apply globally or only to images in specific repositories.

### *Sync Images From Third-Party Registries*

Gain instant insight into container security risks by synchronizing your existing registry images into Tenable.io Container Security with one simple step. The product integrates with Docker Registry, Docker Trusted Registry, JFrog Artifactory and Amazon EC2 Container Registry.

### *Integrated Container Security and Vulnerability Management*

Container security isn't a standalone requirement, but an integral part of a vulnerability management program. Tenable is the only vulnerability management provider to offer integrated container security with Tenable.io Container Security, a modular and independent element of the Tenable.io platform.

## For DevOps Teams:

### *Accelerate DevOps by Pinpointing Security Risks and Delivering Specific Remediation Advice*

Tenable.io Container Security provides Development and Operations unprecedented insight into the security of their Docker container images. In addition to providing a view of images by repository, it performs an in-depth vulnerability assessment on each container image when the image is pushed into Tenable.io Container Security. It conducts an inventory of container components as well as an evaluation of images before they are deployed – listing all the layers and components, including the application, dependencies, libraries and binaries. This fast and comprehensive view of vulnerabilities combined with layer hierarchy intelligence provides a detailed assessment of container image risk, by repository, ensuring developers don't waste time searching for vulnerabilities or fixing issues that are mitigated in a higher layer. This enables developers to quickly remediate potential container risks and push secure code even faster.

### *Embed Security Into Your DevOps Toolchain and Drive Efficiencies Across the Team*

In DevOps environments, Tenable.io Container Security can optionally – and seamlessly – embed security testing into the software development tooling, without blocking or disrupting existing software development processes and workflows. The product provides out-of-the box integrations with common build systems such as Jenkins, Bamboo, Shippable, Travis CI and others, as well as with other continuous integration/continuous deployment tooling used by software developers.

Tenable.io Container Security also includes a robust, fully documented RESTful API for custom integrations with additional DevOps tooling, or data export to reporting tools used by the security team.

### *Go Deeper With More Detail*

DevOps teams can each get their own tailored dashboard that provides vulnerability metrics for their specific images and repositories, so they know immediately when one of their images requires remediation or exceeds the organization's container security risk threshold.