tenable.io
Container Security

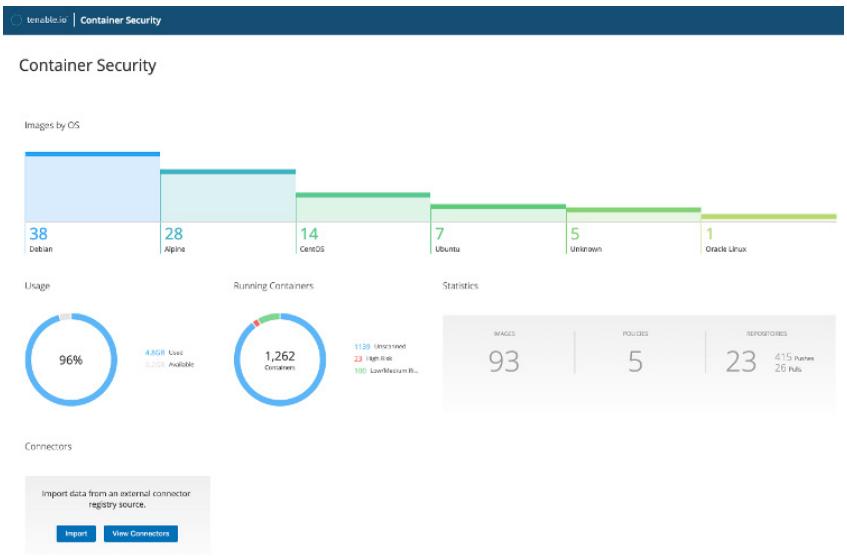
DATASHEET

Integrate Security Into Your DevOps Pipeline

As organizations increasingly depend on software to provide competitive advantage, 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 lifespans and sheer volume and variety of containers mean securing containers is an ongoing challenge.

Gaining pre-production visibility into containers is critical so that you can understand the potential risks in containerized applications before they are deployed. 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.

Whether purchased as a standalone module to Tenable.io, or as a core component of the Tenable Exposure Platform (Tenable.ep), Tenable.io Container Security integrates into your DevOps pipeline to eliminate security blind spots without slowing down software development. Tenable.io Container Security delivers end-to-end visibility of Docker container images, providing vulnerability assessment, malware detection and policy enforcement prior to and after deployment. Compatible with the DevOps toolchain your developers already use, Tenable.io Container Security brings proactive visibility and security to solve the security challenges of containers at the speed of DevOps.



Tenable.io Container Security provides "at-a-glance" visibility into your container environment, including images, policies,repositories and key operational information.

Key Benefits

- **Securely Accelerate DevOps**
  Assess container images for vulnerabilities and malware as fast as 30 seconds from within the DevOps toolchain to avoid slowing down code velocity.

- **Decrease Remediation Costs**
  Dramatically reduce remediation costs by up to 85% by discovering and fixing software defects during development before application release.

- **Gain Accurate, In-Depth Visibility**
  Understand the individual layers of container images to gain an accurate view of cyber risk, reduce false positives and provide detailed remediation guidance.

- **Protect Running Containers**
  Gain visibility into running containers and detect new vulnerabilities and security issues that may emerge after deployment.

- **Enforce Security Policies**
  Block new container builds that exceed your organizational risk thresholds to ensure containers are compliant with your security policies prior to deployment.

Key Capabilities

For Security Teams:

"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.

Malware Protection for Containers
Tenable.io Container Security is one of the only container security solutions 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.

Scan Running Containers
Gain visibility into the security posture of your running containers with Tenable.io Container Security. Access important container operational data such as IP addresses, container ID, scan status and risk score. The product identifies container images running in production that have not yet been tested for vulnerabilities and detects whether containers have changed after deployment with details on which packages were modified.

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.

Integrated Container Security and Vulnerability Management
Container security isn't a standalone requirement, but an integral part of a vulnerability management program. Tenable was the first vulnerability management provider to offer integrated container security with Tenable.io Container Security, a modular element of the Tenable Cyber Exposure platform.

For DevOps Teams:

Targeted 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.

Integration into the DevOps Toolchain
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 integrates 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.

For More Information: Please visit tenable.com
Contact Use: Please email us at sales@tenable.com