Tenable.io Container Security Competitive Comparison

Top reasons to select Tenable.io Container Security

1. Deep vulnerability assessment

Tenable.io Container Security performs an in-depth vulnerability assessment on each layer of the container image - as soon as the container image is imported into the Tenable.io Container Security application - to determine if any vulnerabilities are present in the container image. In addition, Nessus complements Tenable.io Container Security by scanning for vulnerabilities at the host level as well.

2. Malware detection

Tenable.io Container Security uses its own custom-built malware detection engine to look for malware types specific to container environments to ensure images are malware free.

3. Continuous monitoring

New vulnerabilities are identified all the time. The Tenable.io Container Security cloud-based vulnerability database notifies Tenable.io about these new vulnerabilities, and Tenable.io Container Security then immediately rescans and re-assesses all the container images it stores against the new vulnerability.

4. Dashboards

Dashboards serve as a unified view into the security posture of container images for IT security teams. IT security teams can view vulnerability, malware, and other security metrics for all of the container images, as well as the distribution of vulnerabilities across images by CVSS score and risk level.

5. Policy enforcement

With policy enforcement, write container security policies that align to your organization's security goals and objectives, then notify developers right during the build process when a developer creates a container image that exceeds your container image risk threshold.

6. CI/CD integration

Continuous Integration/Continuous Development (CI/CD) is a methodology developers used for building software. Tenable.io Container Security seamlessly integrates into CI/CD development environments, and provides a number of out-of-the box integrations with common tools used in CI/CD environments, as well as a fully documented and supported REST API.

7. Private container registry

At its heart, Tenable.io Container Security is a Docker container registry "built with security in mind," that IT security teams can use to assess the security posture of the container images being built by the organization's software development teams.

Tenable is relied upon by over 20,000 organizations worldwide

Tenable Confidential - For use with Tenable resellers and customers only and should not be redistributed or disseminated.

Tenable.io Container Security Competitive Comparison

Tenable.io Container Security Competitive Landscape

Vendor	Container Vulnerability Assessment	Visibility Inside Containers	Malware Detection	Continuous Monitoring	CI/CD Integration	Policy Enforcement	Public & Private Registries
Tenable.io Container Security	✓	✓	✓	✓	✓	✓	✓
Qualys	✗	✗	✓	✗	✗	✗	✗
Rapid7	✗	✗	✗	✗	✗	✗	✗
Docker Security Scanning	✓	✓	✗	✓	✓	✓	✗
Twistlock	✓	✓	✗	✓	✓	✓	✗
Aqua Security	✓	✓	✗	✓	✓	✓	✗
Black Duck	✓	✗	✗	✗	✓	✓	✗

Tenable is relied upon by over 20,000 organizations worldwide

Tenable Confidential - For use with Tenable resellers and customers only and should not be redistributed or disseminated.