

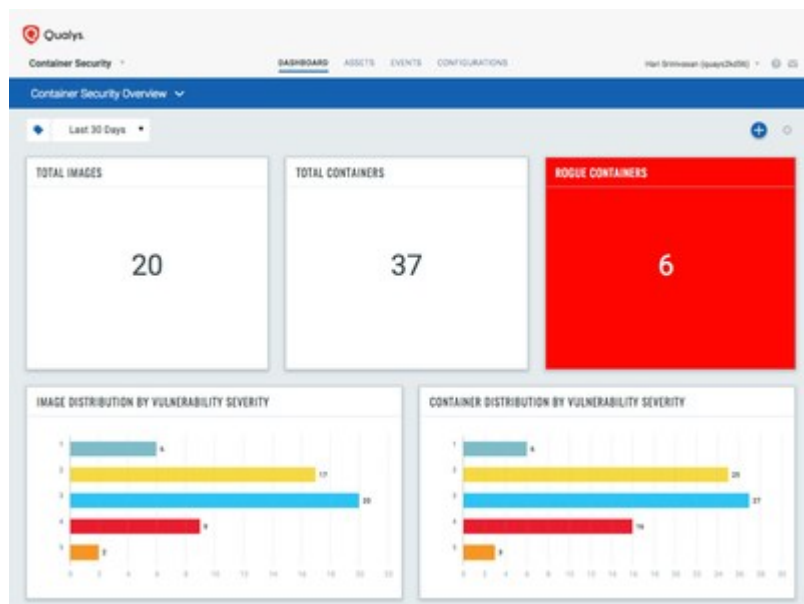


Qualys Releases Container Security (CS) App, Unifying Visibility and Security of Containers Across Hybrid IT Environments

June 12, 2018

New Cloud App enables customers to continuously assess security of containers from their DevOps pipeline to runtime deployments

SAN FRANCISCO, June 12, 2018 /PRNewswire/ -- **DockerCon 2018, Booth #G8** -- [Qualys, Inc.](http://Qualys.Inc) (NASDAQ: [QLYS](http://Qualys.Inc)), a pioneer and leading provider of cloud-based security and compliance solutions, today announced it has released Qualys Container Security (CS), a new Cloud App that enables customers to build continuous security into their global container deployments and DevOps processes at any scale, and integrate the results into one unified view of their global hybrid IT security and compliance posture, breaking down silos and lowering ownership cost.



Built on the [Qualys Cloud Platform](http://Qualys.Cloud.Platform), the new Qualys CS App delivers customers a container-ready security and compliance solution that extends visibility to container environments, and incorporates continuous visibility across the DevOps and CI/CD toolchain with that of existing traditional virtualization environments. Qualys CS performs inventory and real-time tracking of changes to containers deployed across on-premises and elastic cloud environments, and extends vulnerability detection and policy compliance checks to the image registries, containers and hosts.

"As businesses prioritize more responsive and adaptable IT, organizations need tools that optimize a variety of management demands to keep up with the pace of IT innovation," said Scott Crawford, Research Director, 451 Research. "Qualys' cloud platform strategy helps its customers meet many of these challenges, leveraging its early leadership in security offered as-a-service to consolidate and simplify the user experience across applications that address the security of new IT, including infrastructure deployed as containers and the automation that characterizes DevOps."

By integrating Qualys CS into their DevOps toolchain, organizations can identify and remediate risks early in development cycles and reduce those risks created by open development methods and their inherent sprawl. Security teams can participate in the DevOps process to gate vulnerable images entering the system, while developers get actionable data to remediate vulnerabilities. Qualys' high-accuracy vulnerability scanning also reduces the pain of clearing false-positives and allows security teams to focus on identifying and remediating actual risks.

"Containers are becoming an accelerator of the digital transformation and container security is now front and center," said Philippe Courtot, chairman and CEO of Qualys, Inc. "Our new Container Security App is designed to help customers transparently extend their continuous security and compliance capabilities into new cloud workloads through the use of DevOps and containers, allowing them to build security into their digital transformation initiatives."

Qualys Container Security offers customers:

- **Visibility into container projects:** Qualys CS provides auto-discovery that gives customers complete visibility of container hosts wherever they are within their global IT environment, whether on-premises or in clouds. It gathers comprehensive topographic information about container projects — images, image registries, and containers spun from those images. With dynamic, customizable dashboards, users can see complete inventory and security posture from containers to hosts.
- **Security for the entire DevOps pipeline:** Security teams can enforce policies to block the use of images that have

specific vulnerabilities, or that have vulnerabilities above a certain severity threshold. Developers can perform continuous vulnerability detection and remediation in the DevOps pipeline by deploying plugins for CI/CD tools like Jenkins or Bamboo, or via REST APIs.

- **Threat identification, impact assessment and remediation prioritization:** Teams can search for images with high-severity vulnerabilities, unapproved packages, and older or test release tags. They can then assess the impact by identifying all containers using unapproved, vulnerable images. Qualys CS helps determine if these images are cached on different hosts, and identify all the containers on exposed vulnerable network ports running with privileges, which could lead to attacks.
- **Container runtime protection:** CS helps teams scan, protect and secure their running containers. Customers can also detect runtime security and configuration drift that breaks the parent image's immutable behavior by using a different vulnerability posture and software configuration. Qualys CS also features policy-based orchestration to stop containers with vulnerable images from being spun up in Kubernetes clusters. Additionally, customers can understand how the host impacts the containers by easily drilling down to the host level to identify its vulnerabilities and patch compliance.

As a container-ready global IT security platform, the Qualys Cloud Platform consolidates visibility of container environments and other global infrastructure — on premises, at endpoints or in the cloud — into a single-pane-of-glass UI. Its revolutionary architecture provides customers a scalable, end-to-end solution for customers to consolidate their security stack across containerized and non-containerized environments, and also drastically reduce IT security spend by avoiding the cost and complexities that come with managing multiple security vendors.

Pricing and Availability:

Qualys Container Security is available today. Annual subscription pricing begins at \$995 per host.

Additional Resources:

- Follow Qualys on [LinkedIn](#) and [Twitter](#)
- Read more about the [Qualys Cloud Platform](#)
- Read more about the [Qualys Container Security App](#)

About Qualys

Qualys, Inc. (NASDAQ: [QLYS](#)) is a pioneer and leading provider of cloud-based security and compliance solutions with over 10,300 customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL Technologies, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The Company is also a founding member of the Cloud Security Alliance. For more information, please visit www.qualys.com.

Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

MEDIA CONTACT

David Conner
Qualys, Inc.
dconner@qualys.com
650-801-6196

 View original content with multimedia: <http://www.prnewswire.com/news-releases/qualys-releases-container-security-cs-app-unifying-visibility-and-security-of-containers-across-hybrid-it-environments-300664491.html>

SOURCE Qualys, Inc.