Qualys CloudView Adds Security for Infrastructure as Code Enabling DevSecOps Teams to Start Secure and Stay Secure

November 2, 2021

New capability shifts security left by detecting security risks in cloud resource configurations before they are deployed

FOSTER CITY, Calif., Nov. 2, 2021 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today announced it is adding Infrastructure as Code (IaC) scanning to its CloudView app. This will enable detection and remediation of misconfigurations early in the development cycle, removing risk in the production environment.

As noted in the (ISC)^2 2021 Cloud Security Report , security professionals' biggest threat with public clouds is the misconfiguration of resources. Misconfigurations are often detected post-deployment, leaving companies with a much larger attack surface and more vulnerable to exploits. Increasingly, organizations are using IaC to deploy cloud-native applications and provision their cloud infrastructure. Thus, it's important to shift security left to identify and remediate misconfigurations at the IaC template stage. Detecting security issues earlier in the development cycle accelerates secure application delivery and fosters greater collaboration between DevOps and security teams. More importantly, it enforces better security policies in the production environment.

"Security and risk management leaders managing cloud infrastructure security should create safe-to-fail environments to facilitate developer innovation by integrating intelligent security tooling with delivery pipelines (such as infrastructure-as-code [IaC] scanning) to identify risks early and alert on unsafe workloads before they are deployed." Gartner®, *Cool Vendors™ inCloud Security Posture Management*, Tom Croll, Neil MacDonald, Mark Wah, Prateek Bhajanka, June 9, 2021.

Qualys CloudView allows complete visibility and security control of public cloud workloads and now assesses IaC templates for misconfigurations. IaC assessments are integrated into the software development cycle to ensure that only code conforming to the organization's security standards is deployed. Qualys' Cloud Platform approach delivers complete visibility, bringing together runtime and build-time posture and the drift between the two into a single view.

The new capabilities enable organizations to:

Assess security posture throughout CI/CD pipeline
Organizations can now assess the security posture earlier in the development cycle, dramatically reducing security risk post-deployment. CloudView IaC Security provides a command line interface to perform a security assessment locally. To gate deployment if misconfigurations are detected, plug-ins for source code repositories at check-in and CI/CD platforms are also available.

Adhere to security best practices
CloudView IaC Security makes it easy for organizations to adopt security best practices promoted by cloud platform providers. CloudView IaC Security supports popular IaC languages like - Terraform, CloudFormation (CF), and Azure Resource Manager (ARM). It also checks configurations against thousands of security best practices as prescribed by Amazon Web Services, Azure, Google Cloud Platform, and standard bodies including the Center for Internet Security. Additionally, CloudView automatically provides remediation suggestions when a non-compliant configuration is detected.

Ensure compliance with industry mandates
Using CloudView IaC Security, organizations can assure compliance with more than 20 industry mandates such as PCI, HIPAA, and NIST 800-53. This reduces the burden on the DevOps security teams and ensures a streamlined process during mandatory compliance audits.

"With the addition of IaC assessment to CloudView, Qualys is extending its cloud security posture management (CSPM) solution to handle shift-left use cases," said Sumedh Thakar, president and CEO of Qualys. "Leveraging the Qualys Cloud Platform and its integrated apps, customers can now insert security automation into all stages of their application lifecycle ensuring complete visibility into both runtime and build-time posture via a unified dashboard."

Availability
Qualys CloudView with IaC Security is currently in beta and will be available later this year. If you would like to participate in the beta program, please sign up at qualys.com/iac-security-beta. To learn more, read the IaC Security blog.

Gartner disclaimer:
GARTNER and COOL VENDORS are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Additional Resources

- Read the Infrastructure as Code blog
- Details on the Qualys Cloud Platform
- Read about the Qualys Cloud Agents
- Follow Qualys on LinkedIn and Twitter

About Qualys
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions with over 19,000 active 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 across on premises, endpoints, cloud, containers, and mobile environments. Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, 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.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Media Contact:
Jackie Dutton
Qualys
media@qualys.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/qualys-cloudview-adds-security-for-infrastructure-as-code-enabling-devsecops-teams-to-start-secure-and-stay-secure-301414039.html

SOURCE Qualys, Inc.