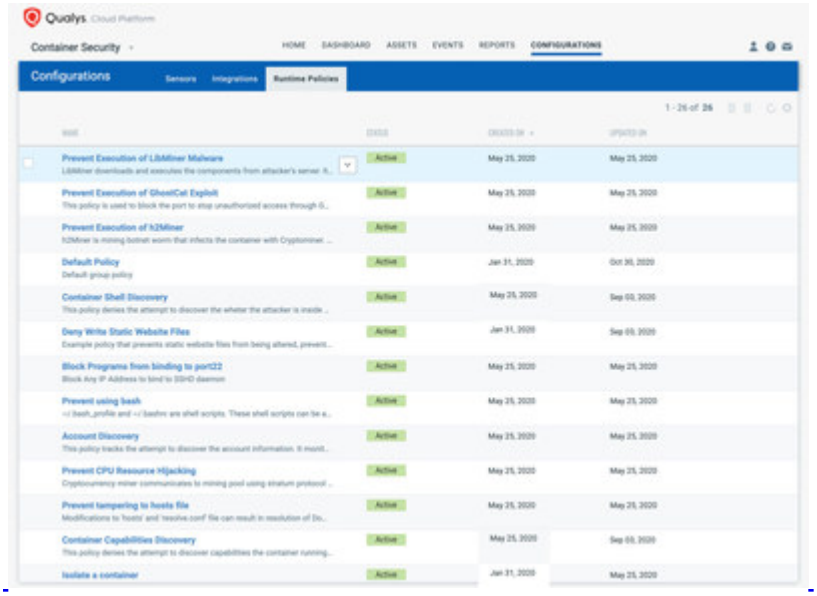
Qualys Adds Runtime Defense Capabilities and Automated Enforcement to its Container Security Solution

November 4, 2020

New solution brings deep visibility and runtime application protection across traditional server-based containers and newer container-as-a-service environments

FOSTER CITY, Calif., Nov. 4, 2020 /PRNewswire/ -- Qualys, Inc. (NASDAQ: QLYS), a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, today announced Container Runtime Security, which provides runtime defense capabilities for containerized applications.



This revolutionary new approach instruments an extremely lightweight snippet of Qualys code into the container image, enabling policy-driven monitoring, detection and blocking of container behavior at runtime. This capability eliminates the need for cumbersome management of sidecar and privileged containers by security solutions that are difficult to manage and administer on host nodes and don't work in container-as-a-service environments. Qualys Runtime Container Security, once instrumented in the image, will work within each container irrespective of where the container is instantiated and does not need any additional administration containers. This new solution addresses, in real time, container security use cases like critical file-access monitoring and blocking, network micro-segmentation, vulnerability and exploit mitigation, and virtual patching.

"At Zoom, we continue to enhance our comprehensive security program that addresses prevention, detection and response capabilities across all types of workloads," said Randolph Barr, Head of Security Operations at Zoom. "Enforcing security best practices, mitigating attacks and monitoring are key use cases for container runtime security. Qualys Container Runtime Security will be key to further extending our detection and response capabilities to containerized workloads running on any container infrastructure."

Now security teams can implement a comprehensive container security program with a single solution that includes vulnerability management, and detection and response across the build-ship-run container pipeline. With Qualys Container Runtime Security, customers can:

- Perform comprehensive, policy-driven monitoring and blocking of container runtime behavior including file access, network communications and process behaviors
- Create granular custom behavioral policies, use policies from the built-in policy library or automatically generate policies based on learned container behaviors
- Instrument container images in the CI/CD build pipeline with an innovative "follow the image" instrumentation approach which allows for standardized, guaranteed container runtime security across all types of container environments like Docker, Kubernetes, AWS Elastic Kubernetes Service, AWS Elastic Container Service, Azure Kubernetes Service, and Google Kubernetes Engine, as well as including container-as-a-service environments like Azure Container Instances, AWS Fargate and Google CloudRun.

"The growth of Kubernetes comes at a time when it is adept at solving many pertinent problems in IT and software development today. However, new tools are needed to secure containers, as container-based application development is a completely different approach to software," said Frank Dickson, program vice president, Security Products at IDC. "Kubernetes can be managed as immutable infrastructure; however, the reality is that container configurations can drift during runtime. The Qualys approach empowers security to follow the container image with built-in instrumentation, enabling visibility and behavior enforcement for running containers. The solution also facilitates a 'follow the container' approach, providing DevOps

and application teams future-proof development protection as applications migrate to more mature container and managed container environments such as Docker, Kubernetes, AWS Fargate and others."

"Detection and Response in a single application across the container DevOps pipeline is key to effectively secure the containerized applications, as the high-velocity DevOps container pipeline can be exploited by malicious actors at runtime," said Philippe Courtot, chairman and CEO of Qualys. "Therefore, we must build security into cloud workloads and extend protection into running containers. Qualys brings defense capabilities to our Container Security solution with the addition of policy-driven behavior detection and response capabilities to protect running containers on-premises, in private clouds or in container-as-a-service public clouds."

Qualys Container Security solution with runtime capabilities is now available. For a comprehensive demo of Container Runtime Security, please register for the virtual Qualys Security Conference (Nov 9 - 24).

Qualys Container Security
Built on the Qualys Cloud Platform, Qualys Container Security discovers, tracks and secures containers from build to runtime. Container Security continuously flags and responds to security and compliance issues in containers across your hybrid IT environment. The addition of runtime protection extends these capabilities, delivering full, granular visibility into running containers and the ability to enforce policies that govern containers' behavior. As a result, you can immediately detect and act upon containers that are drifting from their parent images and potentially creating a security risk due to vulnerabilities or misconfigurations.

Additional Resources

- Read the Container Runtime Security blog
- More information on Qualys Container Security
- Learn about the Qualys Cloud Platform
- Follow Qualys on LinkedIn and Twitter

About Qualys: One Cloud Platform – One Agent – One Global View
Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions with over 15,700 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 native Qualys Cloud Platform and its integrated Cloud Apps deliver 360-degree visibility across on premises, endpoints, cloud, containers, and mobile environments. The platform delivers the visibility businesses need to assess critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance, and protection for IT systems and web applications. Founded in 1999 as one of the first SaaS security companies, Qualys has built a large, impressive customer base and established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, as well as preeminent 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.

Media Contact:
Tami Casey
Qualys
(650) 801-6196
tcasey@qualys.com

View original content to download multimedia:http://www.prnewswire.com/news-releases/qualys-adds-runtime-defense-capabilities-and-automated-enforcement-to-its-container-security-solution-301166173.html

SOURCE Qualys, Inc.