MICRO FOCUS

Flyer

ArcSight
Aqua Container Security Platform

Detect and Prevent Container-Based Threats with ArcSight and Aqua Container Security Platform

Advanced threat detection and actionable insight in containerized environments

About Aqua Security:

Aqua Security enables enterprises to secure their container applications from development to production, accelerating container adoption and bridging the gap between DevOps and IT security. Aqua's Container Security Platform provides full visibility into container activity, allowing organizations to detect and prevent suspicious activity and attacks in real time.

About Micro Focus:

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. Our portfolio enables our 20,000 customers to build, operate and secure the applications and IT systems that meet the challenges of change. We are a global software company, committed to enabling customers to both embrace the latest technologies and maximize the value of their IT investments. Everything we do is based on a simple idea: the fastest way to get results from new technology investments is to build on what you have—in essence, bridging the old and the new.

With Docker adoption up by 40% every year, virtual containers are rapidly being adopted to build enterprise applications in both on premise and cloud settings.

Containers offer organizations significant speed, scalability and cost advantages, but at the same time they present unique security challenges. Furthermore, the fast-paced DevOps process that is often behind container deployments and their many open source components require tight governance of the process from the development phase and beyond.

Along with a new technology comes an opportunity to create a container security stack that covers container-specific security challenges such as finding vulnerabilities in images, enforcing approved images, give real-time visibility into container activity, provide event logging and real time alerting on suspicious activity, and enforce user access controls.

The Aqua Container Security Platform provides development-to-production lifecycle controls for securing containerized applications that run on-premises or in the cloud, on Windows or Linux, supporting multiple orchestration environments.

Aqua provides in-depth information for tracking and auditing events in your containerized applications, with real-time logging and granular event data. This enables real-time visibility into all container activity, including user access, executables, run/stop status, access to files and more.

By integrating Aqua and ArcSight, companies can detect suspicious user behaviour and prevent container based threats. Aqua's threat mitigation and prevention capabilities can be accessed directly from ArcSight and integrated into ArcSight incident correlation rules.

Key Benefits

- Collect and add Aqua threat intelligence with rich user and container context into Arcsight
- Generate user activity logs for ephemeral containers
- Detect abnormal container behaviour indicative of an attack
- Rapid incident response and forensics capabilities by leveraging Aqua's container forensics module

Use Cases

Aqua's comprehensive, purpose-built platform for container security provides full visibility and control over containerized environments, with tight runtime security controls and intrusion prevention capabilities, at any scale.

USE CASE 1: MONITOR DOCKER RELATED EVENTS & CONTAINER RUN TIME ACTIONS

Aqua provide important information about Docker related events and runtime actions. This is useful in order to immediate block or remediate unauthorized behavior. However, if organizations want to have in-depth analytics and insights of historic container events and actions they should continuously feed ArcSight with these events.

USE CASE 2: MONITOR COMMON VULNERABILITIES AND EXPOSURE (CVE) FOUND IN IMAGES AND CONTAINERS

Organization should constantly monitor that all applications are properly patched with software updates and feed the application patch status information into the ArcSight solution. Use Aqua CSP to continuously scan images for vulnerabilities and send information to ArcSight to continuously monitor patching process and status.

More Info

For additional Micro Focus® Security information visit: **marketplace.microfocus.com/arcsight**

For additional Aqua security information visit: **www.aquasec.com**

www.microfocus.com

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com