SOLUTION BRIEF

Aqua Security on IBM Z and IBM LinuxONE

As organizations undergo digital transformation, their workloads can increasingly span diverse environments, including on-premises systems, public clouds, Kubernetes, VMs, containers, and serverless functions. Aqua is designed to provide unified, consistent security across these platforms, now extending its capabilities to applications running on the OpenShift Container Platform on IBM Z and LinuxONE.

IBM Z and LinuxONE are trusted by leading enterprises worldwide for their reliability, availability, and operational excellence in supporting mission-critical applications in hybrid cloud environments.[1] Notably, IBM Z serves as the backbone for 45 of the top 50 banks, four of the top five airlines, seven of the top ten global retailers, and 67 of the Fortune 100, making it the platform of choice for industries demanding high performance and resilience.

The Solution

Enterprises adopting hybrid cloud strategies face the critical challenge of securing containerized, business-critical workloads from malicious attacks. This challenge is compounded by the need to balance flexibility, innovation, and cost-effectiveness, particularly in regulated industries like finance, healthcare, and government, where public cloud Kubernetes infrastructure may not be a suitable option.

Containerized environments, orchestrated by platforms like Kubernetes, operate with dynamic and transient architectures that traditional security tools - designed for static VM-based systems - can struggle to protect. This constant flux may create gaps in security.

IBM Z and LinuxONE, when paired with container technologies, are designed to provide a secure, scalable infrastructure for hybrid architectures. Aqua complements this by delivering end-to-end security across the entire application lifecycle. It is built to strengthen the underlying infrastructure, enhances security posture, and offers both proactive and reactive controls, empowering enterprises to innovate securely and efficiently.

1. https://www.ibm.com/think/topics/mainframe

Application Lifecycle Protection

Scan container images for vulnerabilities, secrets and misconfigurations to reduce the attack surface before deployment.

Cloud Native Security

Designed for high security levels for Red Hat OpenShift Container Platform on IBM Z and LinuxONE with Aqua's leading container and Kubernetes security controls from development to production.

Accelerate Innovation and Improve Customer SLAs While Reducing Risk

Designed to empower engineering and platform teams to use modern CI/CD and microservices based architectures with confidence and remove security-related delays in deployment and incidents.

Risk Posture Management

Secure hardening of OpenShift, its Kubernetes infrastructure, and z/VM guest OS nodes.

Proactively Reduce Pipeline Risk and Improve mean time to respond (MTTR)

Designed to accurately detect vulnerabilities in the pipeline and at runtime and prioritize them, allowing dev teams to quickly remediate issues before they get to production, improving mean time to remediate.

Enable Continuous Compliance

Designed to enforce regulatory compliance controls for PCI-DSS, HIPAA, GDPR and beyond, reducing manual effort and improve audit pass rates.

Real-Time Runtime Protection

Protect container workloads, including drift prevention, malware protection, system and file integrity monitoring.

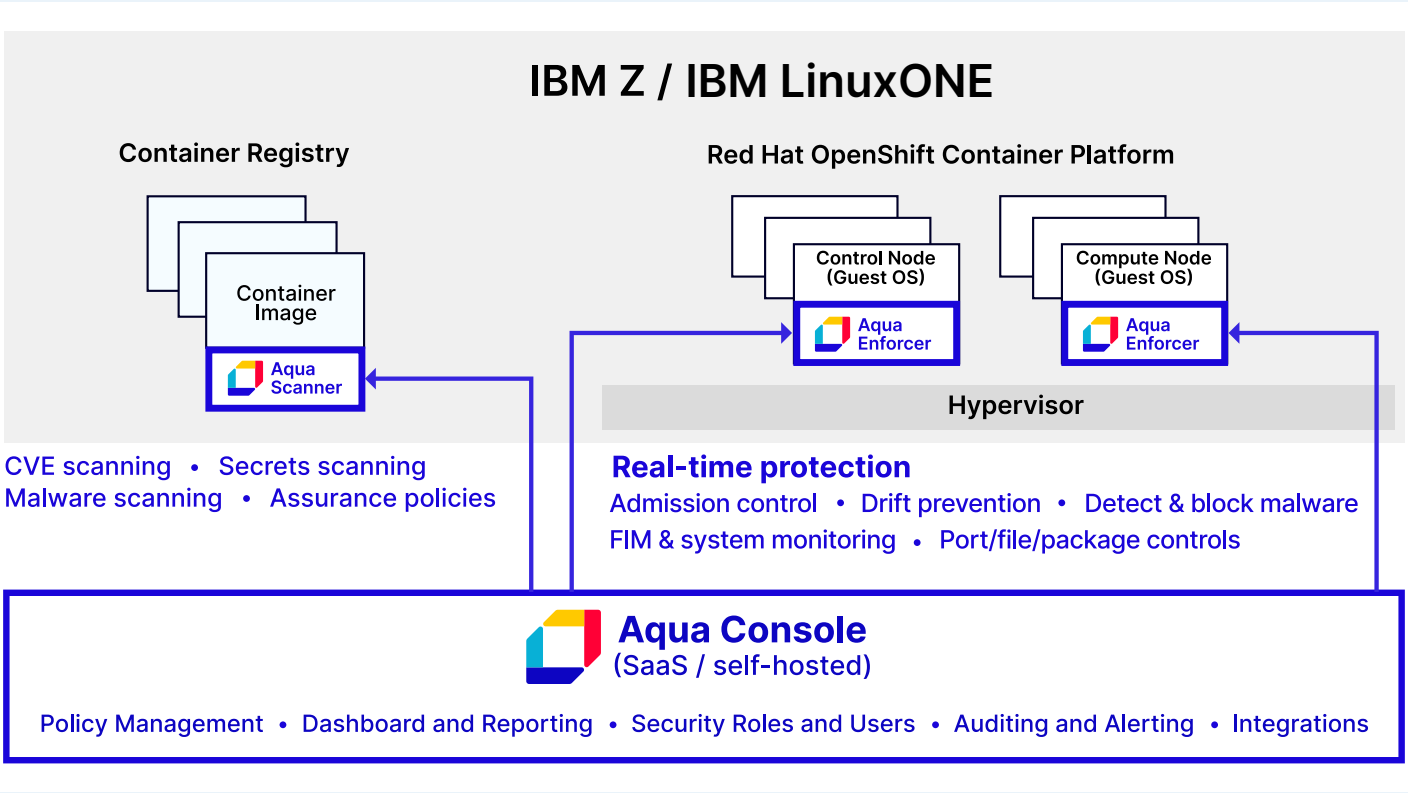
Benefit from Consistent Security Across Hybrid Cloud Environments

Utilize a single-pane-of-glass for visibility and unified controls across OCPz and other cloud native platforms and container and serverless stacks, across private and public clouds.

Detect Runtime Incidents in Real Time and Stop Breaches

Designed to Identify incidents as they unfold with Aqua's multi-layered runtime protection, detect malicious behaviors, enforce immutability and prevent malware at the orchestration, application and OS levels.

Aqua Security on IBM Z and LinuxONE



Protect applications across the entire Software Development Lifecycle (SDLC)

Mitigate risk early in the build pipeline, secure workloads, and orchestration layers to enable defense-in-depth against threats. Aqua's platform spans the entire SDLC from build to production.

Secure modern applications uniformly across on-prem and cloud infrastructure

Minimize noise and operational overhead by enabling unified policy enforcement across private and public infrastructure.

Facilitate regulatory compliance

Designed to meet the rigorous compliance needs of highly regulated industries including finance, healthcare, critical infrastructure and government. Aqua can help meet the compliance requirements needed to support hybrid cloud environments.

Gain real time insights and response capabilities

Detect and prevent drift, identify suspicious behaviors, alert on or block unauthorized processes. Protect against both known and zero-day attacks.

Aqua Security is the pioneer in securing containerized cloud native applications. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), enables organizations to secure every cloud native application everywhere, from code commit to runtime. With enterprise scale that doesn't slow development pipelines, Aqua secures your future in the cloud. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises. For more information, visit https://www.aquasec.com

aqua

Schedule demo ›

Reach out to learn more: bd@aquasec.com
Connect with the Aqua Account Team: cloud.sales@aquasec.com