

Aqua Security for Microsoft Azure

0

Solution Sheet

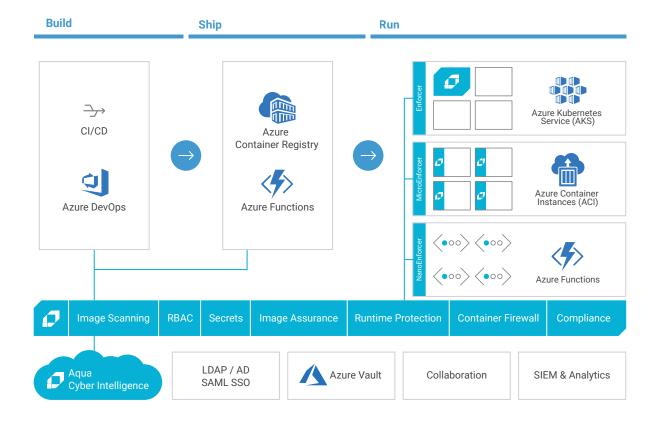
Full Lifecycle Security for Cloud Native Workloads





Microsoft Azure offers a wide variety of services for developing and deploying Cloud native applications. Azure Kubernetes Service (AKS) is used for Kubernetes-based container deployments, Azure Container Instances (ACI) for on-demand container scaling, Azure Functions for serverless functions, Azure Container Registry (ACR) for storing, managing and deploying Docker container images, and Azure Vault for securely storing and managing keys.

The Agua Cloud Native Security Platform provides a comprehensive solution for the entire lifecycle of containerbased and Cloud native applications, with consistent policies and controls, from image build to Cloud native Azure deployments and runtime.



Secure Your Image and Function Development Pipeline

Automatically scan images and functions in Azure DevOps, Azure Container Registry, and Azure Functions for known vulnerabilities, malware, configuration and permissions issues, secrets, and compliance issues:

- Discover and maintain up-to-date image inventory
- Scan for malware and known vulnerabilities based on multiple public, vendor-issued and proprietary sources
- Scan OS packages (RPM, Deb, Alpine), language packages (Java, C++, NodeJS, PHP, Ruby, Python, etc.)
- Detect and amend over-provisioned function privileges
- Generate image bill of materials (packages, layer history, OSS license information)

- Conduct custom compliance checks (SCAP, shell scripts)
- Get actionable guidance for fast and effective remediation
- Integrate with Azure DevOps and other CI/CD tools to automate security scanning in the build phase
- Integrate with Jira, Slack, and PagerDuty to provide developers with immediate feedback

Protect Runtime Workloads on AKS, ACI and Azure Functions

Employ both preventive and reactive runtime controls to ensure that applications are secure, detecting and stopping attacks in real-time.

Image Integrity Validation and Drift Prevention

- Lock down and prevent unauthorized images from running, whether due to policy violations or attempts to run unchecked or spoofed images
- Track images from creation to runtime, ensuring their integrity
- Prevent changes to running containers against their originating images' binaries, executables, and files

Container Runtime Profiles

- Automatically create whitelisting profiles based on container behavior
- Block access to unused executables, network connections, ports, file paths, and system calls
- Alert on or block processes that violate policy, without stopping containers
- Out-of-the-box runtime profiles for popular Docker images

Granular Role-Based User Access Control

- Role-based privileges that limit user access per container, pod, node, namespace, application and storage volume
- Allow/disallow specific user actions, like start/stop, log access, and read/write
- Log all user privilege escalation attempts

Runtime Workload Protection

- Block bad reputation IP addresses
- Visualize and automatically map container network connections, create microservice-level firewall rules to prevent network traversal
- Monitor and log resource activity and consumption, including network connectivity
- Send policy violations and activity data to 3rd party SIEM

Inject Secrets from Azure Vault

- Encrypt and securely distribute secrets stored in Azure Vault to running containers
- Maintain secrets visibility only inside the containers, with no visibility on hosts or persistence on disk
- Easily update, revoke, or rotate secrets with no need to restart containers and no downtime

Enable Regulatory Compliance

- Monitor AKS nodes for user activity and logins/attempted logins
- Scan AKS clusters for malware and known vulnerabilities
- Ensure segregation of duties between developers, SREs, and security teams
- Out-of-the-box policies for PCI, HIPAA, NIST and CIS compliance

About Aqua

Aqua Security helps enterprises secure their Cloud Native, container-based and serverless applications from development to production. Aqua bridges the gap between DevOps and security, promoting business agility and accelerating digital transformation. Aqua's Cloud Native Security Platform provides full visibility and security automation across the entire application lifecycle, using a modern zero-touch approach to detect and prevent threats while simplifying regulatory compliance. Aqua customers include some of the world's largest financial services, software development, internet, media, hospitality, and retail companies, with implementations across the globe spanning a broad range of cloud providers and on-Premises technologies. For more information, visit www.aquasec. com or follow us on twitter.com/AquaSecTeam

Contact

www.aquasec.com

♡ @aguasecteam

Inkedin.com/company/ aquasecteam