

Solution Brief

Operationalize cloud native with Zero Trust Architectures

In theory, cloud native technologies meet NIST 800-207's specifications for a "pure zero trust architecture" through concepts like container immutability, microservices least privilege access and Kubernetes admission controllers. The practical reality is that for cloud native architectures, technical and operational complexity stands in the way of ensuring the zero trust principle of 'deny by default'.

Organizations struggle with a common definition of how to trust their workloads and the infrastructure that they run, and as a direct result, how to validate trust and monitor trust on an ongoing basis.

Unified Approach to Cloud Native Zero Trust Architecture



Define what is trusted

Policy-based approach to establishing trust for code, users, images, containers, resources, services & processes



Enforce and validate trust






Block non-compliant images & configs, continuous assessment of user, service accounts & pipeline access, integrate with secrets management



Detect & stop untrusted activity

Prevent untrusted activity in run time - Drift Prevention, behavioral policies & eBPF-based advanced detection

Key Benefits

-  Facilitates unified approach for of 'known good' settings, policies and workload profiles as a zero trust baseline - balancing security and business objectives
-  Standardizes controls across the lifecycle for zero trust policy enforcement - reducing risk, minimizing the attack surface
-  Validates and monitors zero trust policies for software artifact promotion, pipeline integrity and cloud native access requests conform
-  Logs, audits policy, violations, failed access attempts and integrates with SIEM, security reporting & observability tools
-  Automatically detects and blocks untrusted container activity at run time

To address the business objectives to automate, scale and move fast while minimizing risk, Aqua enables cross-functional teams – including DevOps, Kubernetes administrators, SREs and security engineers – to define, enforce and monitor zero trust policies across the cloud native application lifecycle. Aqua's Cloud Native Application Platform allows teams to operationalize zero trust architectures in complex cloud native environments through a unified approach spanning software bill of materials validation, DevOps and CI/CD pipeline integrity, vulnerability assessment, cloud account misconfiguration remediation, Kubernetes assurance and security, application scope least privilege and role-based access controls, logical micro define controls to determine 'known good' across the application lifecycle- trusted artifacts, validated access, assurance policies and container Drift Prevention. Standardize controls to limit problematic access and enforce baseline policies. Stop 'known bad' based on divergence from standardized controls and detection of untrusted activity

Trust your code

Ensure that only known good software code, artifacts, images and containers that are free from vulnerabilities and malware are promoted. Enforce assurance policies and security gates for malicious code scanning.

Prevent untrusted activity at run time

Detect and block untrusted users, processes and connections. Enforce container immutability for any unauthorized activity, block remote code execution, with monitoring and ongoing attack analysis

Secure the software supply chain

The Aqua Software Supply Chain Security solution performs code integrity checks, prevents code manipulation or injection attempts. Scan container images and identify malware, including host OSes.

Enforce ZT Assurance Policies

Define and enforce zero trust assurance policies for container images, container configurations, Kubernetes clusters and pods, Kubernetes admission controller policies, and cloud account & hyperscaler least privilege and best practices

Ensure CI/CD pipeline integrity

Enforce developer least privilege access to CI, perform misconfiguration checks for Infrastructure as Code templates and validate the software bill of materials based on security checks.

Cross-team RBAC & secrets mgt.

Define cross-cluster application scopes for least privilege access across teams and automate injection secrets at run-time with no user interaction through vault integration.

Stop untrusted Activity at run time

Enforce runtime policies based on workload behavior, unauthorized access, process or modification and detection to prevent untrusted activity. Enforce container immutability with Aqua Drift Prevention.

Visibility, risk insights and monitoring

Single pane of glass that consolidates reporting, findings and insights on compliance with policies, relative risk for images, configurations and Kubernetes clusters as well as incidents, with integration with SIEM, workflow and observability tools. Granular audit trails of all access activity



Aqua Security stops cloud native attacks, preventing them before they happen and stopping them when they happen. With Aqua, DevOps and Security teams prioritize risk in minutes across the entire development lifecycle while automating prevention to secure their cloud native applications on day one. Real cloud native attacks are stopped immediately without killing workloads. With a platform built on the most loved open source cloud native community and innovation from dedicated threat research, Aqua is a complete solution to cloud native security for transformational teams. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries.



[Schedule demo ›](#)