







## Partner Solution Brief

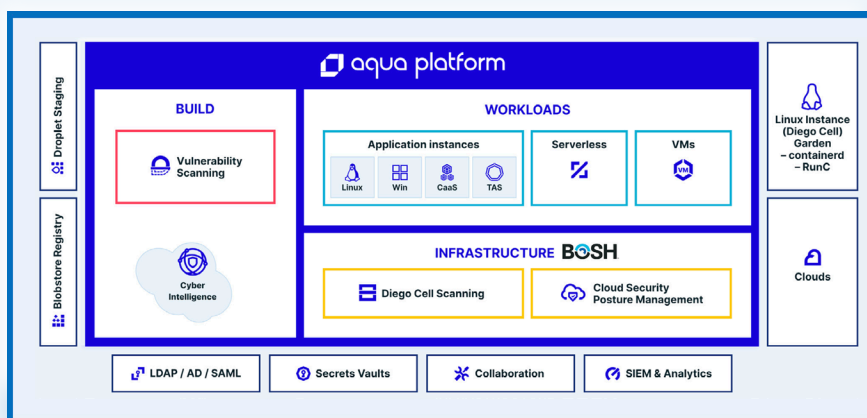
# Stop Cloud Native Attacks for VMware Tanzu Application Service and Kubernetes Grid

VMware Tanzu Application Service (TAS) is a faster and easier way to deliver and manage applications. But it also requires a full life cycle approach to cloud native application security, from code to production, that is optimized and certified for the unique protocols and components of TAS. Aqua has partnered with VMware to natively protect TAS applications, as well as both Tanzu Kubernetes Grid (TKG) and Tanzu Kubernetes Grid Integrated Edition (TKGI). Aqua's full life cycle security platform works seamlessly across TAS, TKG, and TKGI to stop runtime attacks and delivers actionable insights into container and Kubernetes risks and security concerns.

Aqua helps to prevent attacks before they happen through supply-chain security, malware detection, host assurance, and role-based access control (RBAC), providing consolidated visibility across cloud providers. Aqua's assurance policies, micro-segmentation, file integrity monitoring and CIS benchmarking further help customers to automate regulatory compliance. Aqua can operate in air-gapped environments to support the requirements of highly regulated industries and federal agencies.

## Key Benefits

-  Secure the software supply chain with Droplets and Blobstore vulnerability scanning and validated software bills of materials (SBOM).
-  Ensure that only compliant images, Droplets, and Kubernetes configurations are deployed—blocking non-compliant Droplets and settings.
-  Immediately stop malicious workload behavior for TAS applications in runtime.
-  Enforce compliance with a broad set of global regulations, and enforce RBAC by geo and app scope.
-  Unified platform for securing TAS, TKG, and TKGI with consolidated visibility, integrated with multi-cloud risk management.
-  Support for air-gapped environments



## Automate shift-left prevention

Secure your CI/CD pipeline and Blobstore, and scan Droplets in CI and the Blobstore for vulnerabilities across language packages. Provide image and Droplet risk analysis, fix issues early, and avoid security roadblocks. Identify malware, embedded secrets, and misconfigurations. Enforce Kubernetes security posture management with “compliant by default” templates and CIS benchmark assessment.

## Protect in real time

Enforce workload immutability to prevent unauthorized changes, detect and stop policy violations and suspicious behavior, monitor and harden Diego cells and Kubernetes nodes, and segment applications with workload firewalls. Mitigate threats including port scanning, reverse shell execution, connections to suspicious IP addresses, and cryptomining.

## Ensure continuous assurance

Prevent non-compliant images and Droplets from being deployed into production based on their vulnerability posture, embedded secrets, malware, and configuration non-compliance. Use consistent policies and controls to secure applications across TAS, TKG, and TKGI with support for multi-cloud account assurance. Evaluate Diego cells for compliance against regulatory and security mandates (GDPR, CIS Linux Benchmark configuration best practices) and maintain file integrity monitoring.

### Identify vulnerabilities and manage risk

Integrated with VMWare Harbor Registry and CI/CD pipelines, Aqua’s scanner identifies vulnerabilities, malware, and embedded secrets in Droplets and Blobstores and provides actionable remediation advice based on risk insights.

### Prevent attacks at runtime

Enforce workload immutability to prevent unauthorized user, process, or service activity, detect and stop external connections, and monitor and harden Diego cells and Kubernetes nodes. Limit the impact of zero-day attacks with runtime policies for Diego cells.

### **Ensure Diego cell security and assurance**

Protect the underlying Diego cell with advanced security controls, including malware detection. Evaluate Diego cells for compliance against the CIS Linux Benchmark configuration best practices and apply file integrity monitoring for compliance requirements.

### **Unified visibility and actionable alerts**

Enforce consistent policies and controls to secure apps across TAS, TKG, and TKGI. Maintain consolidated visibility into risks across cloud providers, and use actionable alerts tied to TAS and TKG resources.

### **Flexible management and air gap support**

Aqua's scanner can run in an air-gapped environment, providing an additional layer of threat prevention for disconnected environments. RBAC with application scopes to enforce cross-cluster least-privilege access.

### **Automate compliance**

Define custom policies and perform checks and validation of your application development and delivery pipeline for compliance with PCI DSS, HIPAA, EU GDPR, and regional regulatory requirements.



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 >](#)