







Solution Sheet

Aqua's Cloud Workload Protection Platform (CWPP)

Aqua's Cloud Workload Protection Platform (CWPP) is powerful, cloud-born security solution designed to prevent, detect, and respond to attacks targeting applications that are running in cloud native workloads such as containers, virtual machines (VMs), and serverless functions, as well as Kubernetes and platform-as-a-service (PaaS) environments.

Aqua's CWPP solution provides visibility into applications running in cloud workloads, identifies and prioritizes vulnerabilities and other risks, and protects running workloads against threats and attacks. CWPP offers real-time anti-malware protection, behavioral monitoring, drift prevention, and various application controls that are designed specifically for the unique nature of cloud native technology stack.

Key Benefits

-  Save time with simple deployment in minutes
-  Gain forensic-level visibility across workloads
-  Efficiently prioritize risk and rapidly reduce the attack surface
-  Prevent attacks before they gain workload access
-  Investigate and respond instantly to suspicious activity
-  Report accurately and meet compliance requirements

Gain complete workload visibility

Discover vulnerabilities and risks with real-time cloud workload scanning for full-spectrum visibility. Detect suspicious activity and monitor attack patterns at the kernel level with eBPF technology.

Real-time scanning for vulnerabilities and risks

Automatically discover and scan for vulnerabilities and other risks with Trivy, the world's most popular cloud native security scanner for complete visibility into your workloads.

Observe suspicious behavior and attack patterns

Identify threats and suspicious activity using real-time malware scanning and behavior-based detection analysis at the kernel level to pinpoint attacks.

Detect threats with kernel-level visibility

Gain deep visibility into the kernel level with eBPF technology to ensure that every malicious action is captured and surfaced in an incident timeline.

Prioritize risk and reduce the attack surface

Immediately prioritize the most critical vulnerabilities and risks in your running workloads to reduce the attack surface and make vulnerability and incident management easier and more effective.

Prioritize attack surface risk in real time

Improve decision-making with expert guidance for better identification, coverage, and prioritization of risks and vulnerabilities to reduce the application attack surface and prevent exploits.

 **Mitigate container risk and cluster hygiene** Ensure compliance across the entire cluster with assurance gates that prevent non-compliant resources from running even after initial scanning.

Identify cloud workload threats

Identify threats by looking for suspicious behavior patterns to catch known exploit attempts and identify unknown ones. Enforce unique cloud native security controls such as a container drift to monitor and ensure container immutability.

Defend runtime workloads against attacks

Stop attacks at any point with a multi-layered runtime protection strategy that prevents drift, ensures immutability, and surgically removes malware and blocks attacks.

Secure all cloud workloads

Observe what's happening within running workloads and automatically block or restrict suspicious or unapproved activity across running containers, virtual machines, serverless functions, and Kubernetes and PaaS environments.

Prevent zero-day attacks

Harden your environment and stop zero-day attacks with patented drift prevention that automatically blocks any lateral movement or escalation within or between your cloud workloads.

Protect against malware

Immediately identify malware, malicious file hashing, or other resources with known signatures to instantly alert, remove, or block known and unknown malware using a combination of detection methods that catch what others miss, like fileless attacks.

Leverage real-world threat intelligence

Protect workloads faster with pre-populated, research-backed, runtime security policies developed from in-the-wild threats discovered by Team Nautilus, taking the hassle out of customizing configurations.

Faster, more effective runtime protection

Use robust behavioral detection techniques to detect suspicious activity fast and immediately stop attacks with the Lightning Enforcer, a lightweight, compatible agent that preserves application performance and provides comprehensive runtime protection on day one.

Optimize response and streamline incident management

See everything in detail and automatically create an incident timeline to quickly view and understand exactly what's happening in running workloads.

Manage incidents and respond faster

Access forensic-level insights that provide a detailed outline of an attack process and deliver clear, actionable remediation steps so that incident response teams are alerted the moment a malicious security event is detected.

Streamline cloud security management

Easily access reports, update policies, manage incidents, and secure your VMs, containers, and serverless workloads with one user-friendly interface that makes managing your cloud workload security seamless and intuitive.

Save time with simple deployment

Achieve simple and scalable deployment with a lightweight agent that offers superior protection, eliminates cloud workload complexity, and provides immediate value.

Report accurately and meet compliance requirements

Prove compliance to auditors with simplified reporting from a single dashboard that details when an attack took place and can trace the origins back to the original development code for complete workload protection.

Report attack impact easily

Provide a detailed report of the entire attack timeline by mapping techniques to the MITRE ATT&CK framework and assessing impact during each stage of the attack.

Meet compliance mandates

Ensure compliance with frameworks such as PCI-DSS, NIST-53, NIST 800-190, and ISO 27002 with system integrity monitoring, file integrity monitoring, malware protection, firewalling, authentication and authorization controls, and encryption.



Aqua Security stops cloud native attacks across the application lifecycle and is the only company with a \$1M Cloud Native Protection Warranty to guarantee it. As the pioneer in cloud native security, Aqua helps customers reduce risk while building the future of their businesses. The Aqua Platform is the industry's most integrated Cloud Native Application Protection Platform (CNAPP), protecting the application lifecycle from dev to cloud and back. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries. For more information, visit <https://www.aquasec.com/>.



[Schedule demo ›](#)