Solution Brief

aqua

Protecting Cloud VMs in Modern Cloud Native Stacks

Virtual machines (VMs) that run in public clouds require a modern security approach, without the baggage of older tools used to secure data enter servers. Cloud VMs necessitate a lightweight solution that is easy to automate in an orchestrated environment, easy to deploy and manage at scale, and will not tax cloud resources.

Since cloud native environments might include combinations of container, serverless and VM workloads, there is a strong benefit in using a single pane of glass view and unified policy enforcement. In comparison to containers and functions, VMs might run for days or longer, providing opportunity for attackers to targets them and persist. It is therefore crucial for security teams to get VM visiblity, compliance and security controls as an integral part of their unified cloud native security platform.

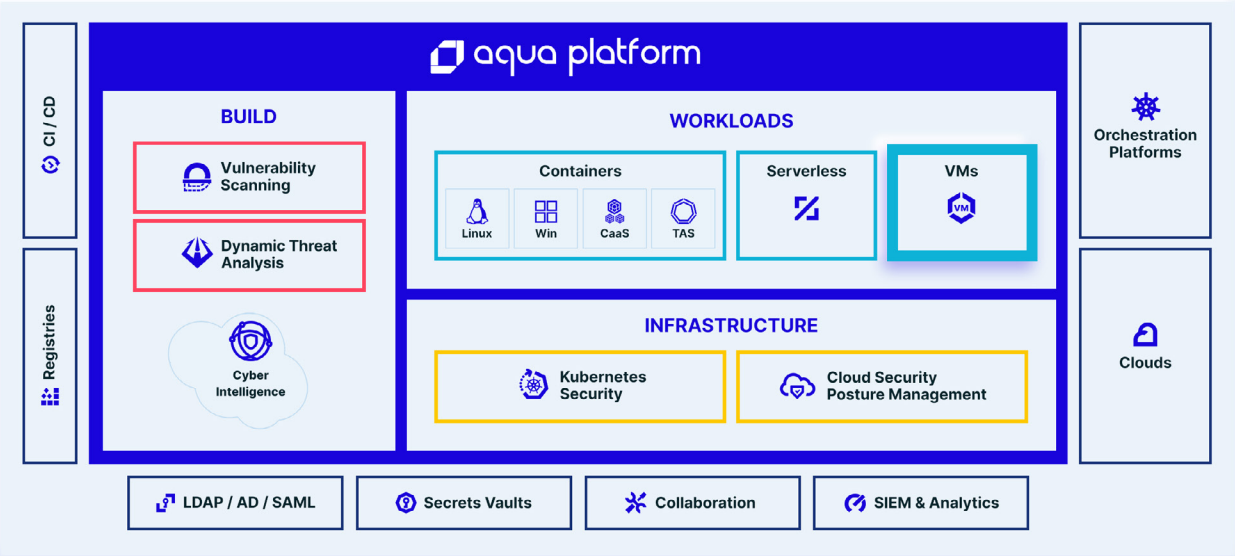
Evaluating your cloud instances for security and compliance standards like PCI-DSS, NIST-53, NIST 800-190, and ISO 27002 requires businesses to implement “best possible” security controls to prevent intrusions and safeguard data. These controls range from system integrity monitoring, including file integrity (FIM), malware protection, firewalling, to authentication & authorization controls as well as encryption. It is very common for organizations to implement disparate tools during their cloud migration journey, but it doesn’t take long before they realize the pitfalls of maintaining multiple tools and struggling to follow the sequence of events across their cloud native stack.

Organizations therefore need a cloud workload protection platform (CWPP) that provides:

- Comprehensive compliance and security capabilities
- Visibility and proof of compliance, as well as protection against threats and breaches
- A single-pane-of-glass view of the compute stack, regardless of where the cloud native infrastructure is hosted, or the makeup of its workloads
- The ability to quickly track suspicious or malicious activity across a stack of Virtual Machines, Containers, Kubernetes clusters, and Pods.
- A holistic view of wide-scale, multi-vector attacks to help in defending against sophisticated attackers

A Complete Workload Protection Platform

Aqua's VM Security offering provides security controls for heterogeneous VM workloads including a wide range of Linux and Windows operating systems. Using a cloud native, purpose-built, and containerized platform provides low friction, low footprint, and a quick deployment model.



Our goal is to secure VM workloads at all stages of their lifecycle (provisioning, image build, pre-production, production) with minimal friction and effort. Aqua monitors and controls instantiated containers to prevent any unauthorized activities using a single Aqua Enforcer container, which offers flexibility to protect virtual machines as well as containers running on the VMs. In an orchestrated environment, a Kubernetes node can be protected using Aqua Enforcer to prevent privilege escalation attacks, thus offering a layered set of controls for prevention against multi-faceted attack vectors.

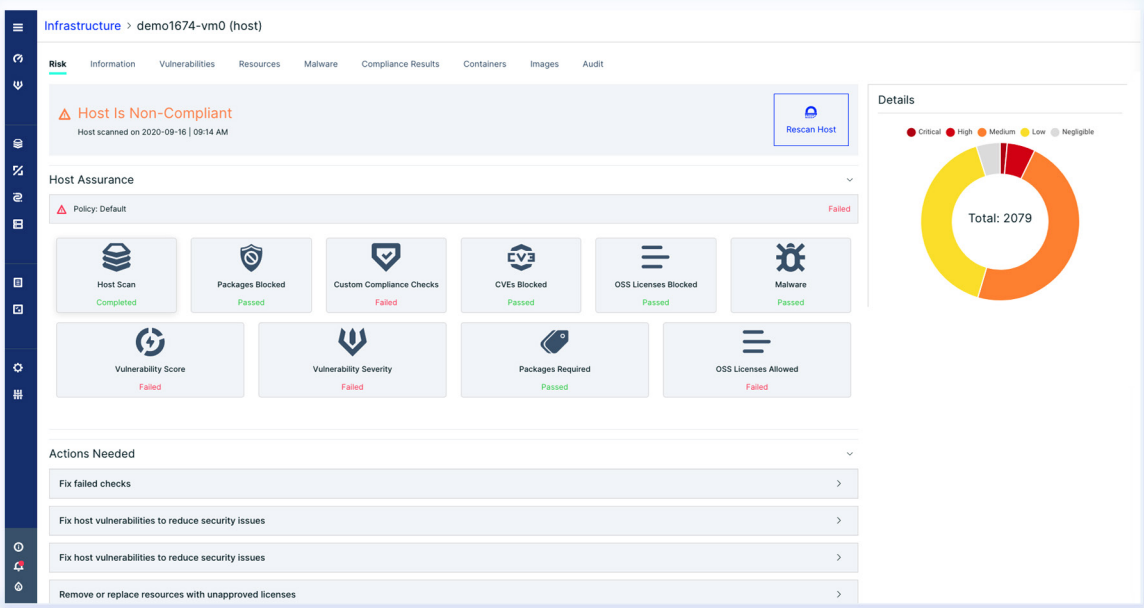
By combining policies and control points across the entire lifecycle, we enable a zero-trust, "prevention first" model. This is complemented by deterministic, behavioral runtime controls that together provide more robust and reliable enforcement when compared to older signature-based or probabilistic EDR methods.

Aqua's Protection for Cloud Instances

Aqua's unique approach for protecting cloud instances is a combination of DevSecOps, prevention first, and leveraging immutability and automation. The following section summarizes the Aqua VM security controls used to define virtual machine security posture:

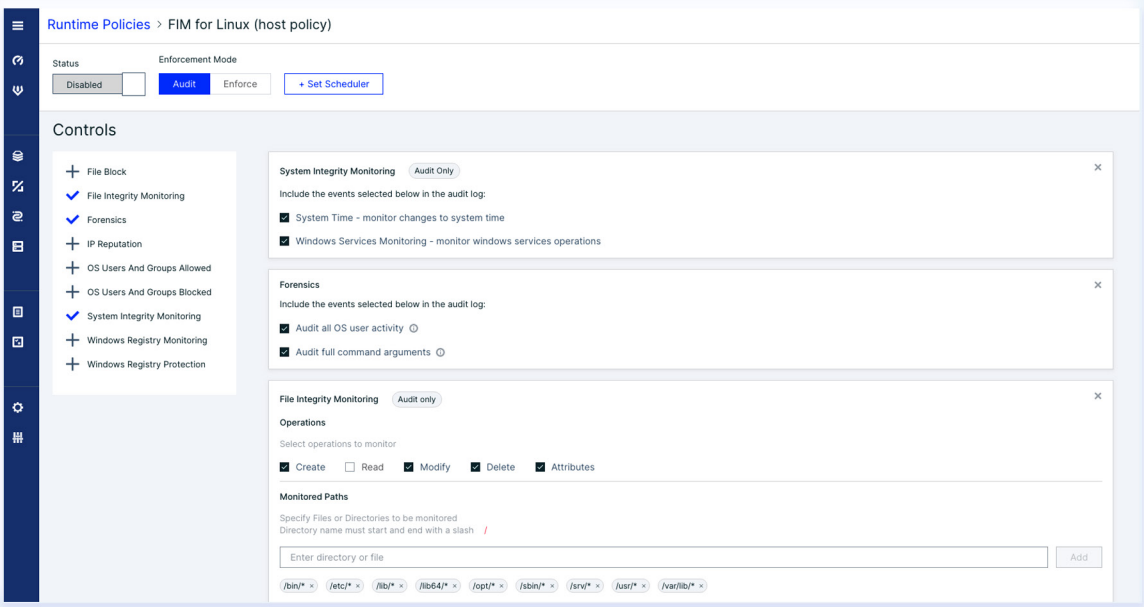
Cloud VM Assurance Polices

Scan your cloud VMs (Linux and Windows operating systems) for known security issues (vulnerabilities, open-source, and malware), check OS configuration, and ensure compliance by aligning with regulatory standards. Create a compliance baseline for your cloud VMs, identify non-compliant VMs, gain full visibility into the infrastructure elements that set your environment at risk, and get actionable steps for remediation.



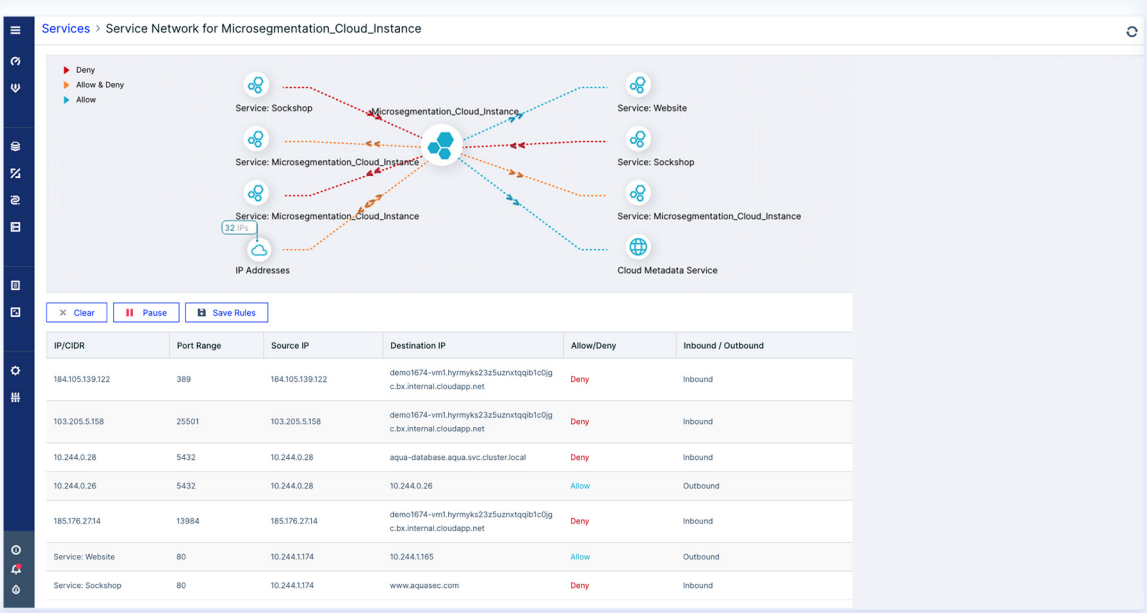
Runtime Protection for Cloud Instances

Prevent malicious runtime behaviors by monitoring user activity, file access, and system integrity, preventing disallowed activities and processes in real-time.



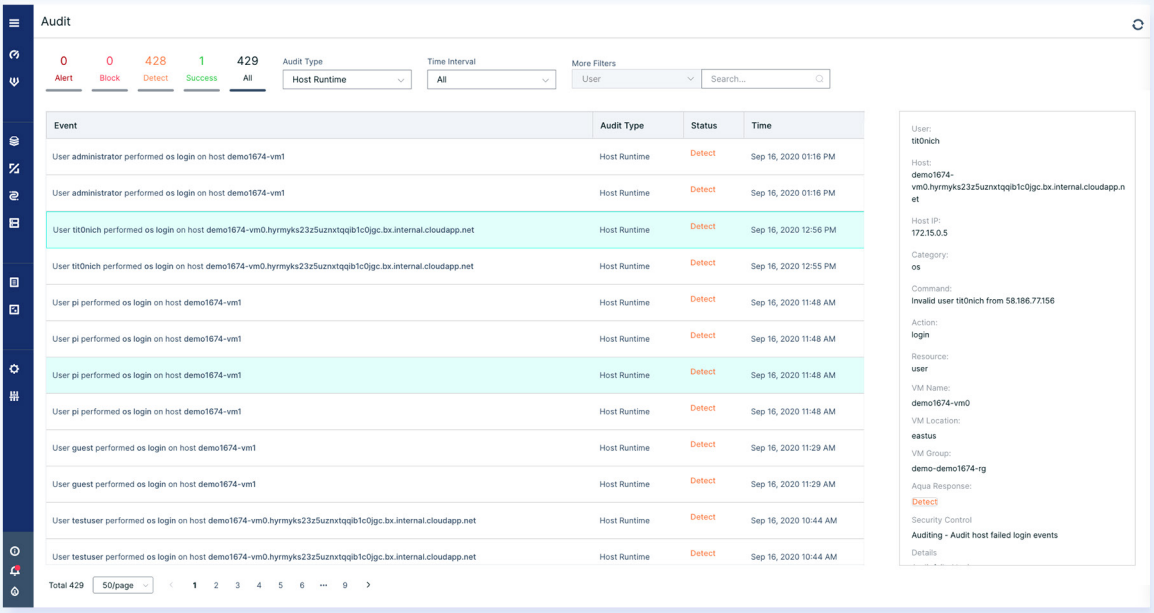
Workload Segmentation

Implement workload segmentation and uniform policies that can easily be maintained and applied dynamically on VM workloads and new servers, across different environments. Provide full visibility into cloud VMs' network activity, divide workloads into distinct security segments, define security policies and deliver services for each unique segment.



Forensics Analysis

Track user activity and command-line arguments including system calls, view event logs for alerting, forensic analysis, log aggregation, as well as reporting. Get alerts for specific anomalies, such as port scans, directly to your SIEM system, providing your security teams granular visibility into vulnerabilities and threats.



Unified Enforcement of Security Posture for Cloud Instances

Aqua provides organizations a unique solution suited for modern hybrid, multi-cloud environments, providing full visibility and control over the entire stack (physical machines, virtual machines, containers, and serverless workloads):

Proving Compliance

- Address compliance requirements such as PCI-DSS, HIPAA, CIS Benchmark, and other.
- Scan for malware and vulnerabilities and validate that VMs are properly hardened.

Real-Time Security Controls

- Dynamic security to adjust its behavior based on the dynamic nature of VMs, location, type, and K8s context.
- Ensure VM Immutability and monitor user actions and suspicious activity (OS Logins, File changes).

Single Pane of Glass Across the Entire Lifecycle

- Events from Windows, Linux virtual machines as well as containers and Kubernetes environments offer a single pane of glass view to monitor risks and prevent threats.
- Monitor and protect containers K8S nodes as well as virtual machines with the same enforcer.

Go Cloud Native with the Experts!

Get a Demo

aqua

aquasec.com

contact@aquasec.com

@Aqua Security

@AquaSecTeam

in/Aqua Security

@AquaSecTeam