Securing Containers, Serverless and VMs for Cloud Native Applications

Looking to Secure Containerized Applications Across any Platform, Orchestrator, or Cloud?

Aqua's security platform provides full visibility and control over cloud native applications, with tight runtime security controls and intrusion prevention capabilities, at any scale.

Shift-Left Security

Integrate security into the CI/CD pipeline to provide image/function risk analysis and rapid remediation early during the build, with full automation and no compromise on security.

Deploy Only Approved Images

Create and enforce an image/function assurance policy that only allows images that adhere to security and compliance guidelines to be deployed - including vulnerabilities, embedded secrets, malware, secure configuration, and more.

Protect Workloads in Runtime

Zero-touch runtime controls ensure container integrity and immutability, host and orchestrator hardening, and least-privilege enforcement on container behaviors, without sacrificing application performance and availability.

Workloads Firewall

Visualizes workload network connections, automatically creates whitelist firewall rules that enforce network segmentation, blocking unauthorized connections, and preventing network traversal.

Defines and Controls User Access Policies

Granularly controls user access and defines permitted commands. This enforces segregation of duties and least privilege principles, and detects and blocks unauthorized activities.

Meets Regulatory Mandates and Industry Recommendations

Automates compliance (e.g., PCI-DSS, HIPAA, and NIST) best practices across your hybrid cloud environment.

Secure Once, Run Anywhere

Apply automated, consistent control to images, containers (host-based/CaaS, serverless), nodes and clusters across any orchestration platform, on Linux and Windows, and across cloud providers.

Risk-based analysis

Provides a live map of all the hosts and images that are part of the running workloads. Risk Explorer provides the ability to identify the namespaces and objects and their respective risk levels and perform a root cause investigation.

Aqua Cloud Native Security Platform

Aqua Server A central management component that can be deployed on multiple instances for high availability. It provides policy management, image and function scanning, image/function lifecycle controls, monitoring, and reporting. It also integrates with image/functions registries for scanning, with CI/CD tools for security testing as part of the build, and with SIEM/analytics to generate audit and alert data.

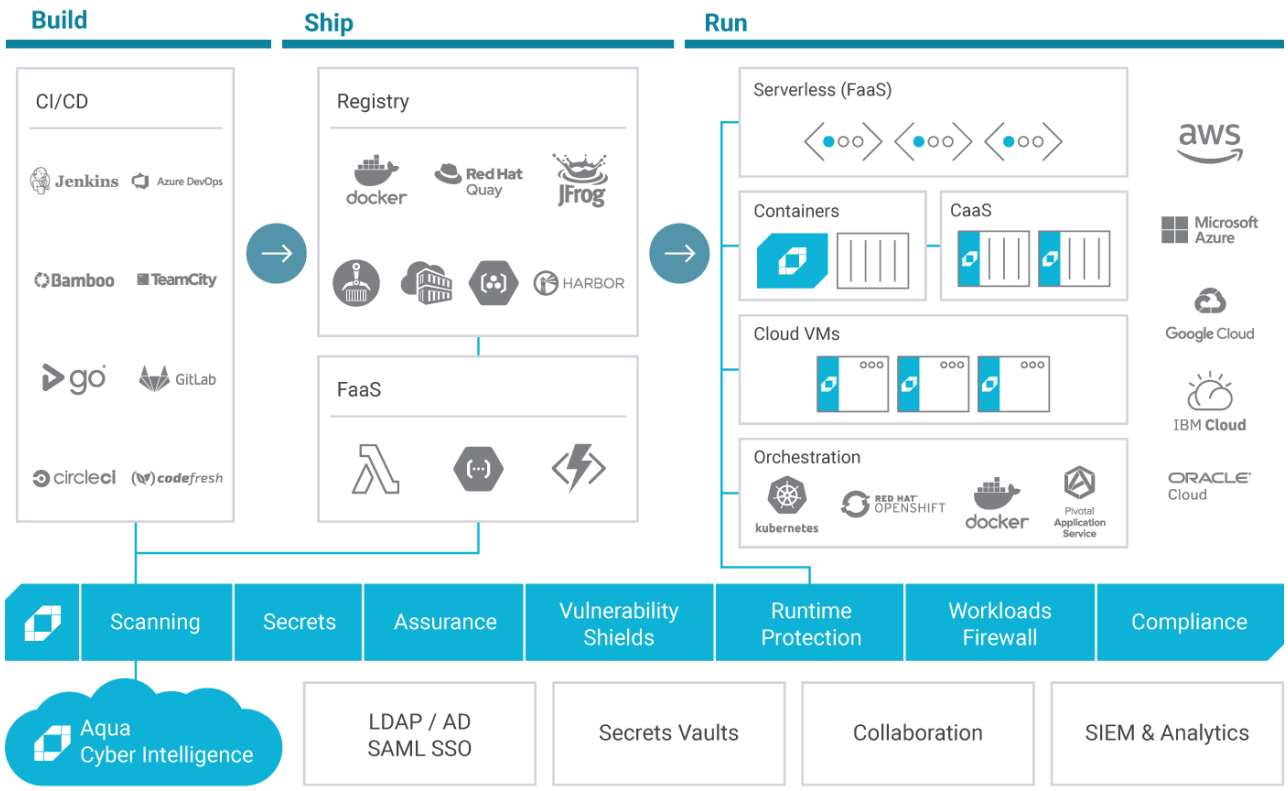
Aqua Cyber Intelligence Feed Aggregates and correlates multiple sources, including NVD, vendor advisories, and proprietary research, providing continuous, up-to-date information to Aqua's vulnerability scanning, malware detection, and threat mitigation features.

Aqua Enforcer Monitors the runtime activity of containers and hosts and provide for their runtime security.

VM Enforcer Provides protection for hosts (virtual machines) without Docker or Kubernetes, monitors the host image, and provides Host Runtime Policies to restrict and monitor specified runtime activities.

Aqua MicroEnforcer Provides runtime protection for containers in PaaS environments, in which a host-based solution cannot be deployed.

Aqua NanoEnforcer Provides runtime protection for AWS Lambda functions, provides protection against malicious executables, controls the types of executables that can run, and detects malicious behavior in runtime.



Prioritize Threats In Running Workloads In Real-Time

Do you have all the correct information on your running containers to perform a real-time analysis?

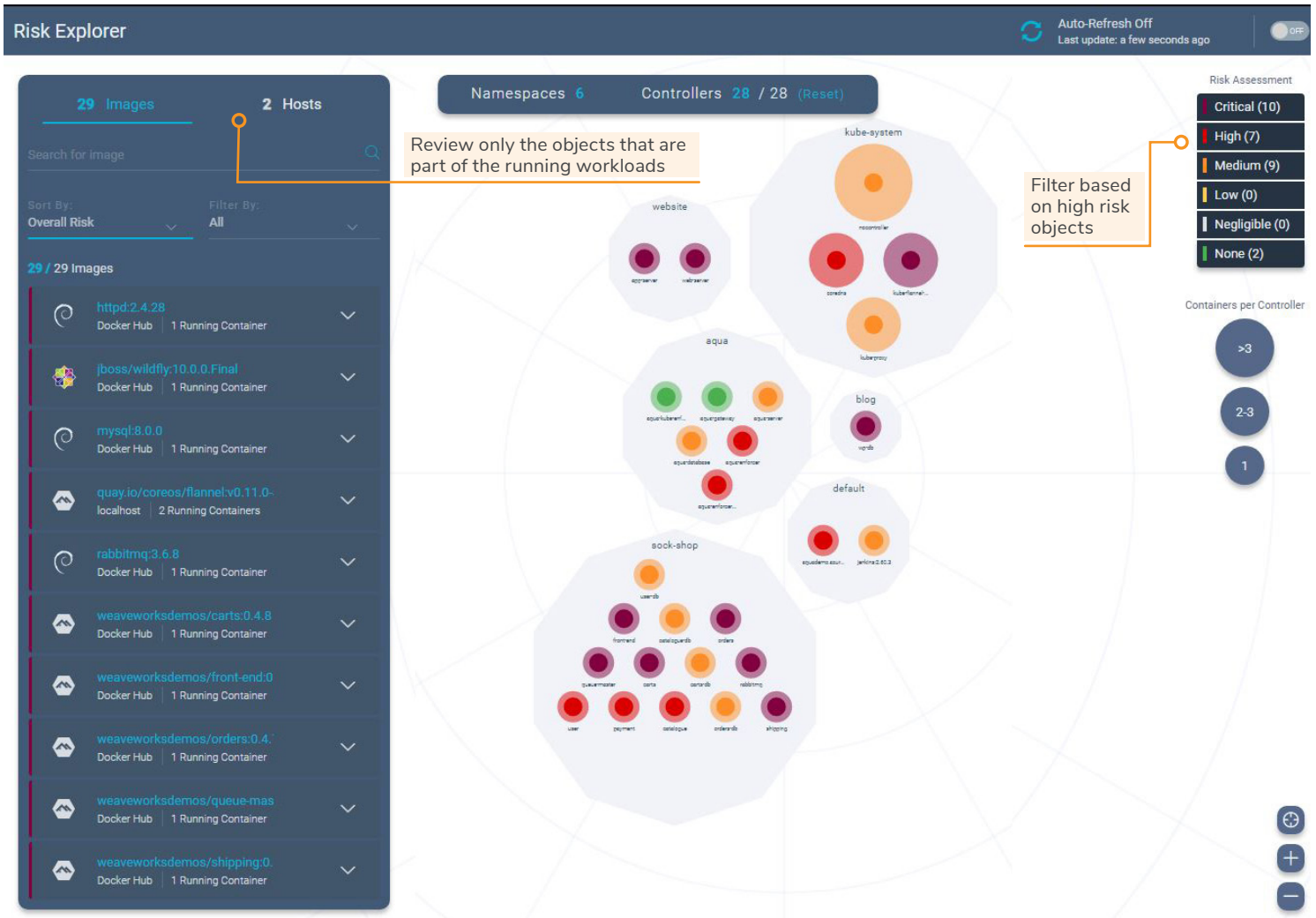
Are you able to make quick decisions and mitigate the most critical risks at the right time?

Risk Explorer provides a clear view of all active workloads and a snapshot of the security posture of your applications. The user can navigate through his running workloads and namespaces and jump to other areas of the Aqua UI (e.g., images and vulnerabilities) that are relevant to risk management of his container environment.

- Displays detailed top-down information on a selected object and all the components that are associated with it and reviews the reason why Aqua defined it as a risky object
- Helps security teams save time by viewing a live map of all running workloads and focuses on the high-risk objects
- Automatically discovers all running workloads in your environment
- Prioritize vulnerabilities to be remediated or mitigated
- Provide insight into areas that need to be improved
- Uses risk-based vulnerability management for prioritization to improve the security posture of your running workloads

Automatically Discovers all Running Workloads

Displays a live map that reflects the risk level in all running workloads that shows the user all the namespaces and controllers (which represent a deployment \ daemonset \ job).



Ongoing Image Risk Assessment

Can you ensure images are free from known vulnerabilities, secrets, and configuration errors?

Do you have access to actionable remediation information for detected vulnerabilities?

Aqua integrates security into the CI/CD pipeline to provide image risk analysis and rapid remediation early during the build, enabling you to "fail fast" while avoiding security roadblocks.

- Multiple source feeds (public CVEs, vendor-issued, proprietary vulnerability data streams, and malware)
- Identify containers with vulnerabilities and known bad packages
- Scan images/image streams within the CI tool (Jenkins, Microsoft VSTS, Bamboo, etc.) to mitigate risks during build
- Scan images in registries and on hosts for known vulnerabilities, malware, secrets, and configuration errors
- Scan OS packages (RPM and Deb) and 40+ language packages (e.g. Java, NodeJS, Ruby, PHP, Python, C/C++)
- Get image bill of materials (packages, files, OSS license information and layer history)
- Gain actionable remediation information for detected vulnerabilities

Allow developers to scan their code locally, or as part of the CI process and based on your security policy. Applies image policies based on usage context, to ensure the continuity of development efforts.

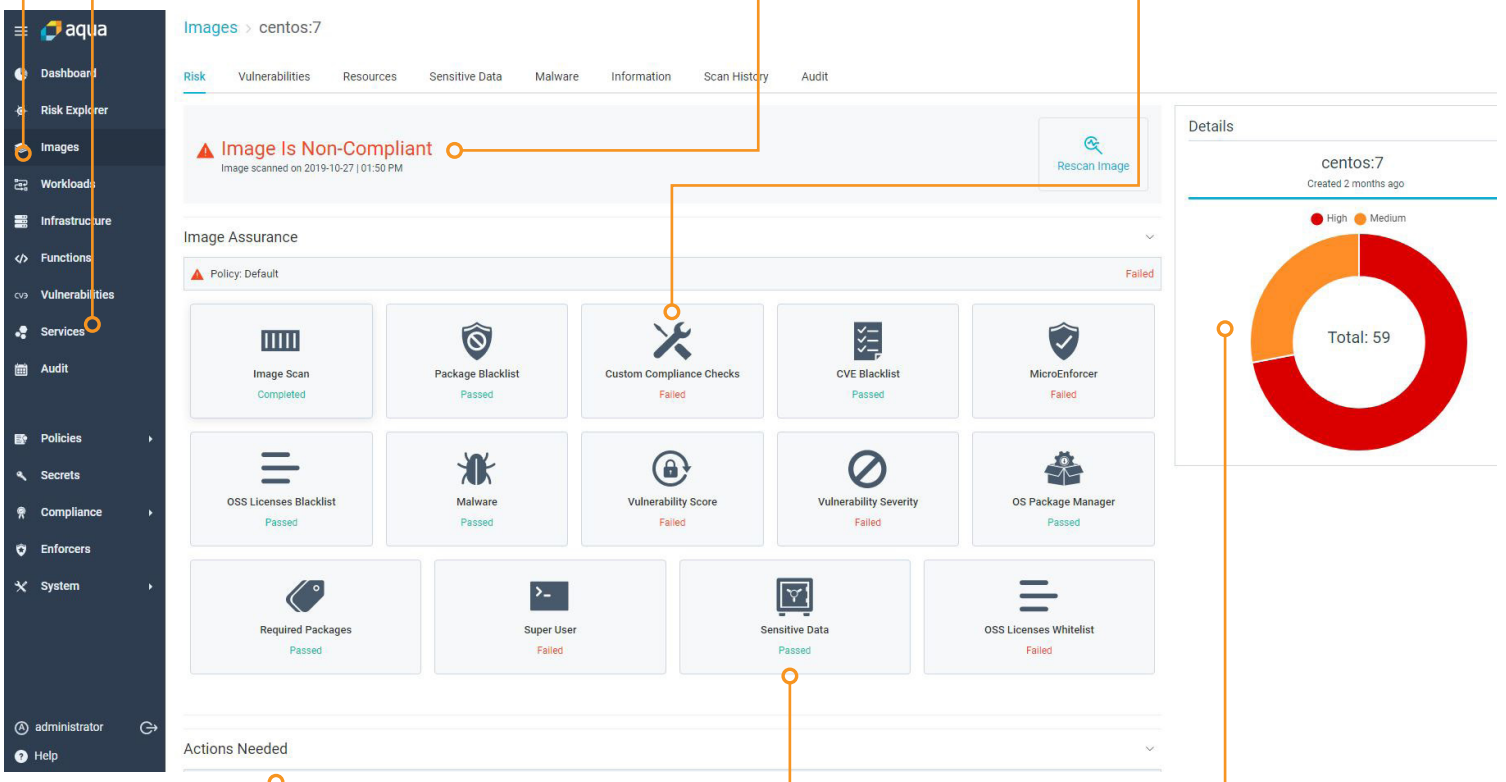
The most effective way to maintain image hygiene and enable early remediation is to scan images immediately after the build, upon image push to registries, as well as when images are pulled from outside the pipeline, in case they will be used as a base image.

Real-time view of running containers (vulnerabilities, uptime, packages, etc.)

Group multiple containers into services and set service-oriented firewall policies and network segmentation, regardless of where the container runs

Determine image acceptance based on security controls

Use custom compliance checks for non-compliance with security mandates (GDPR, PCI, etc.)



Provide actionable remediation information for detected vulnerabilities

Detect secrets (API keys, SSH keys, RSA keys, DSA keys, etc.) embedded in images

View vulnerability origins throughout the image hierarchy/layers and validate chain of custody

Image Assurance Policy Settings & Enforcement

Can you ensure that only approved images will run in your environment?

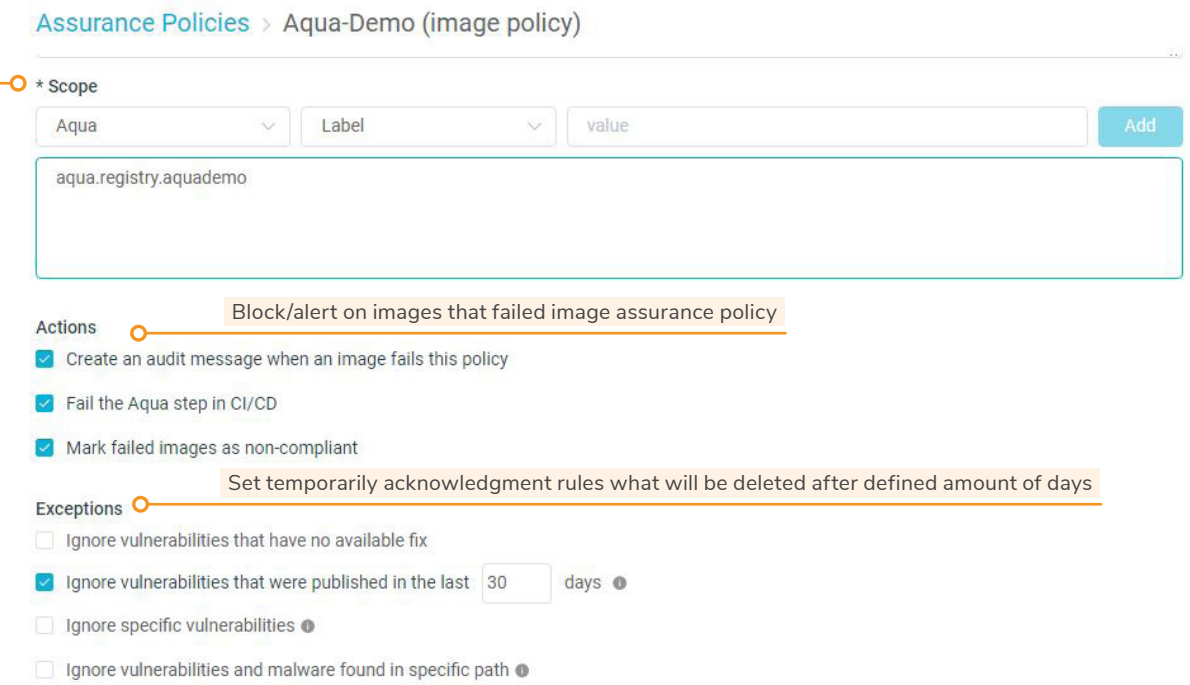
Aqua's image assurance provides persistent controls to ensure image integrity throughout its lifecycle, and to prevent unapproved or unvetted images from running.

- Use multiple image assurance policies to determine the conditions an image must meet in order to run
- Ensure only the latest, authorized images are being instantiated across your IT environments
- Control promotion of images from staging to production
- Cryptographic digest uniquely identifies images and ensures their integrity, preventing the tampering with or spoofing of images from dev to production
- Identify and flag containers that cannot be traced back to approved images
- Aqua Image assurance policy works across multiple orchestration tools (e.g., K8s, OpenShift, DC/OS, Docker Swarm, and PAS.)
- Encrypt images during build, using Aqua MicroEnforcer for high-value information protection such as sensitive data and intellectual property. Aqua MicroEnforcer decrypts the images in runtime

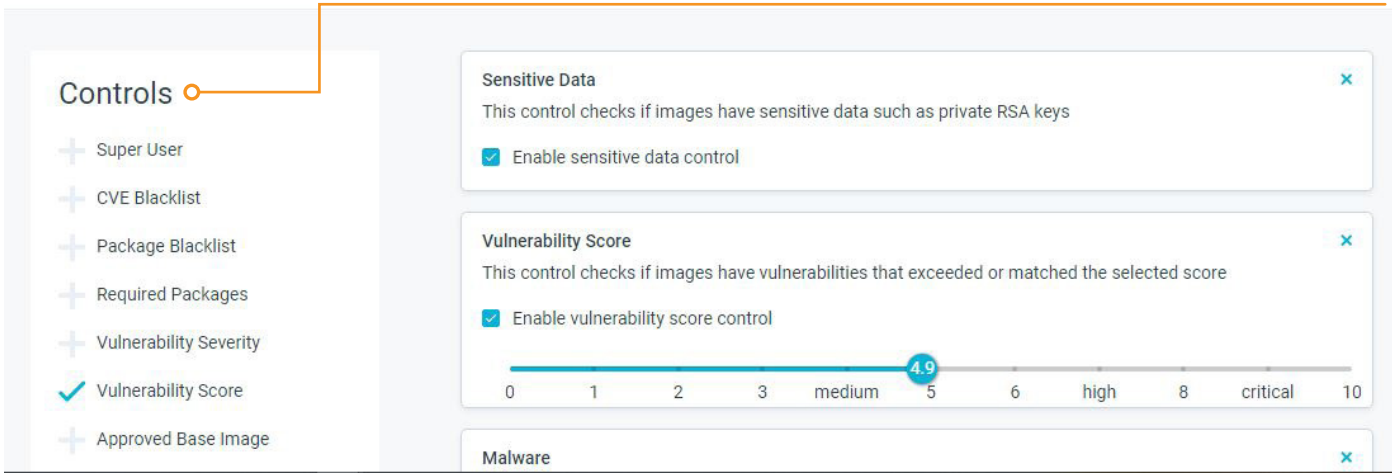
Apply stricter image policies to images in staging, and less stringent policies to images that are still in development or testing. A 'Disallow running images with medium severity' policy can be applied to images in the staging registry. If an image is in the development or testing stage, it can run with medium severity, as it does not pose any risks at this stage.

Only allow images from approved registries. Only allow images from pre-approved base images.
Ensure that every release automatically includes the latest security updates.

Enable multiple image assurance policy settings (per image name, label, registry) to effectively balance risk vs. efficiency



Provides a broad set of predefined image assurance policies for popular Docker images (e.g., Nginx, MySQL)

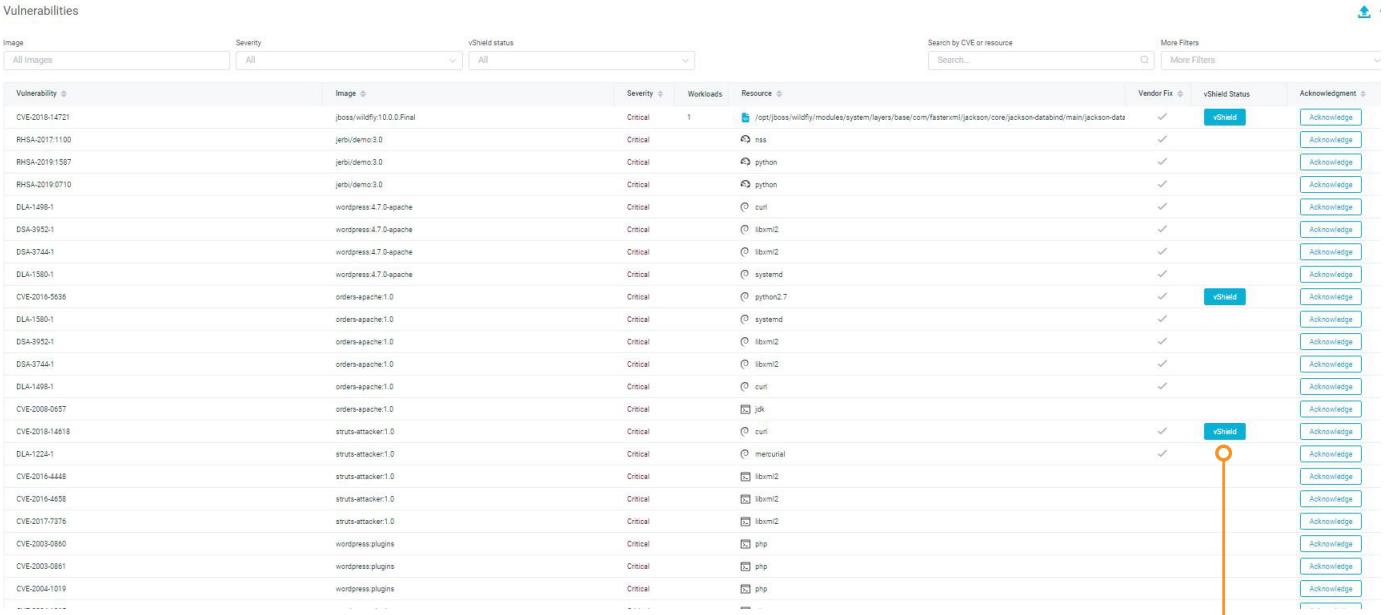


Mitigate Known Vulnerabilities in Container Images

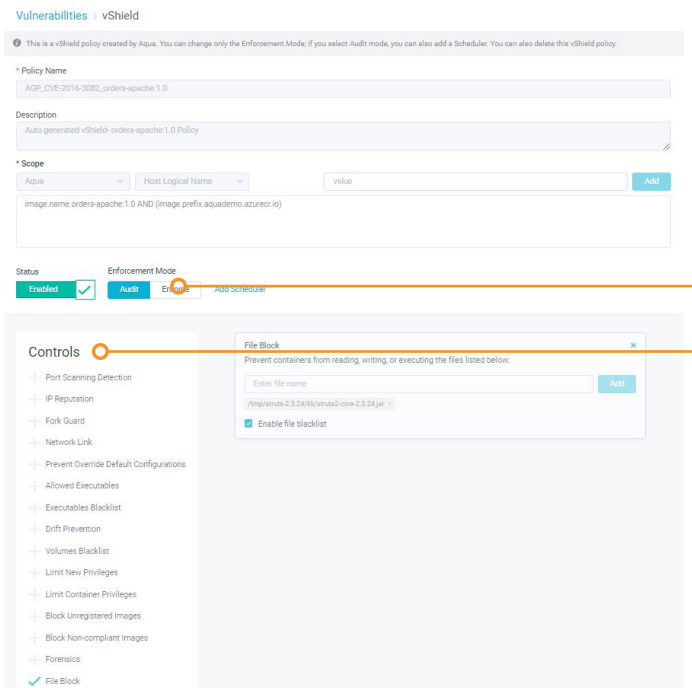
Aqua Vulnerability Shield (vShield) provides a compensating control for known vulnerabilities detected in container images. vShield leverages Aqua's dynamic runtime capabilities to provide a "virtual patching" mechanism that automatically detects, and can prevent, attempts to exploit the vulnerability to which it is applied.

- Provides business continuity by dynamically patching running workloads, ensuring that mission-critical applications are not impacted
- Non-intrusive and does not change the image code, so no developer intervention is required
- Aqua vShields are automatically generated for newly discovered vulnerabilities
- Protects against various type of vulnerabilities: network / file system / packages / executables
- Enables compliance teams to demonstrate having controls in place for specific vulnerabilities
- Provides visibility into exploit attempts of known, vulnerable components

Aqua vShield lets security teams know when an exploit attempt was made on the shielded vulnerabilities and can also block that exploit. It allows organizations to reduce the risk of running with known vulnerabilities and prioritize their patching in a more efficient way.



Identify the appropriate vShield for this specific CVE, which is displayed in the vulnerability scan results



vShield automatically moves to enforce mode once the required learning time of the potential impact on running containers has elapsed

Provides protection for different types of vulnerabilities

Securely Deliver and Rotate Secrets

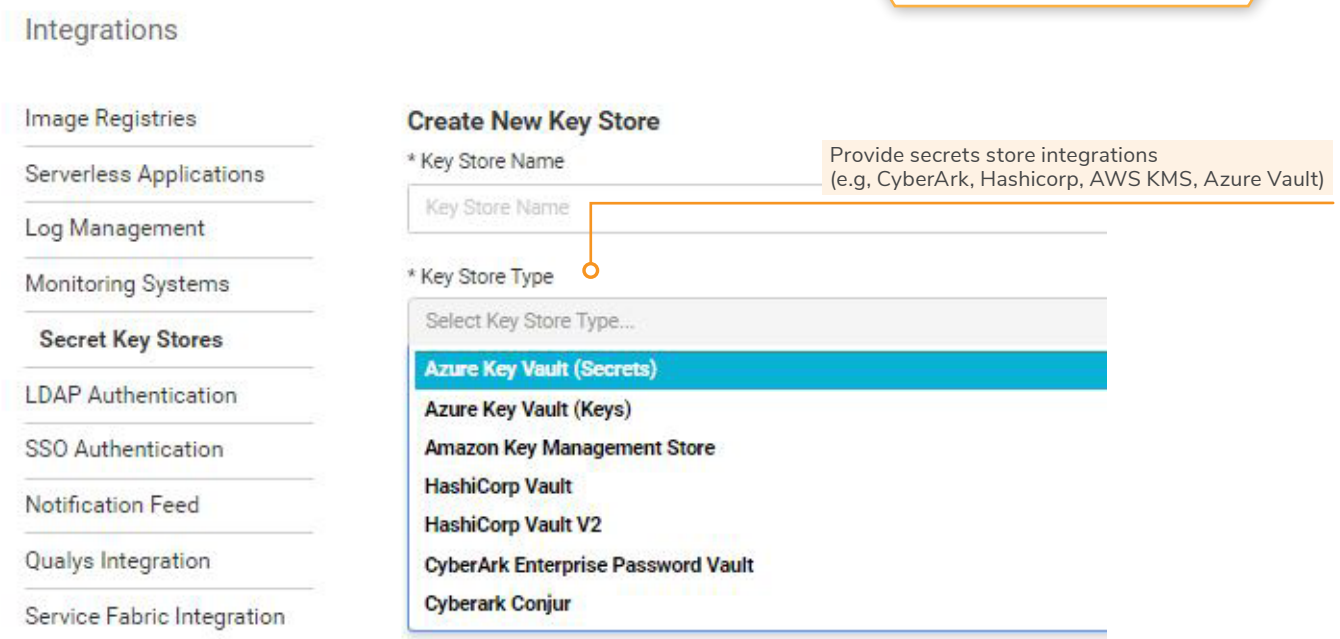
Can you do routine rotation with no downtime or restart to the running container?

Can you ensure that only certified, designated running containers can retrieve secrets?

Aqua securely delivers secrets to runtime containers in memory, with no persistence on disk. Secrets can be rotated, updated, and revoked with no container downtime or restart, managed by existing third-party enterprise secrets vaults.

- Securely deliver 'secrets' across environments
- Encrypt secrets in transit
- Secrets injection/rotation in runtime with no container downtime
- Manage and monitor container secrets activity

Don't leave cleartext secrets in database, images, and containers. Secrets, by default, are unencrypted and left in AES-CBC databases, in images, and in containers. Encrypts secrets at rest (and in transit). Once malicious users gain access to the database, this can mean "game over" for the organization. Secrets should be rotated based on security mandates with no container downtime to support business continuity.



Real-Time Workload Visibility

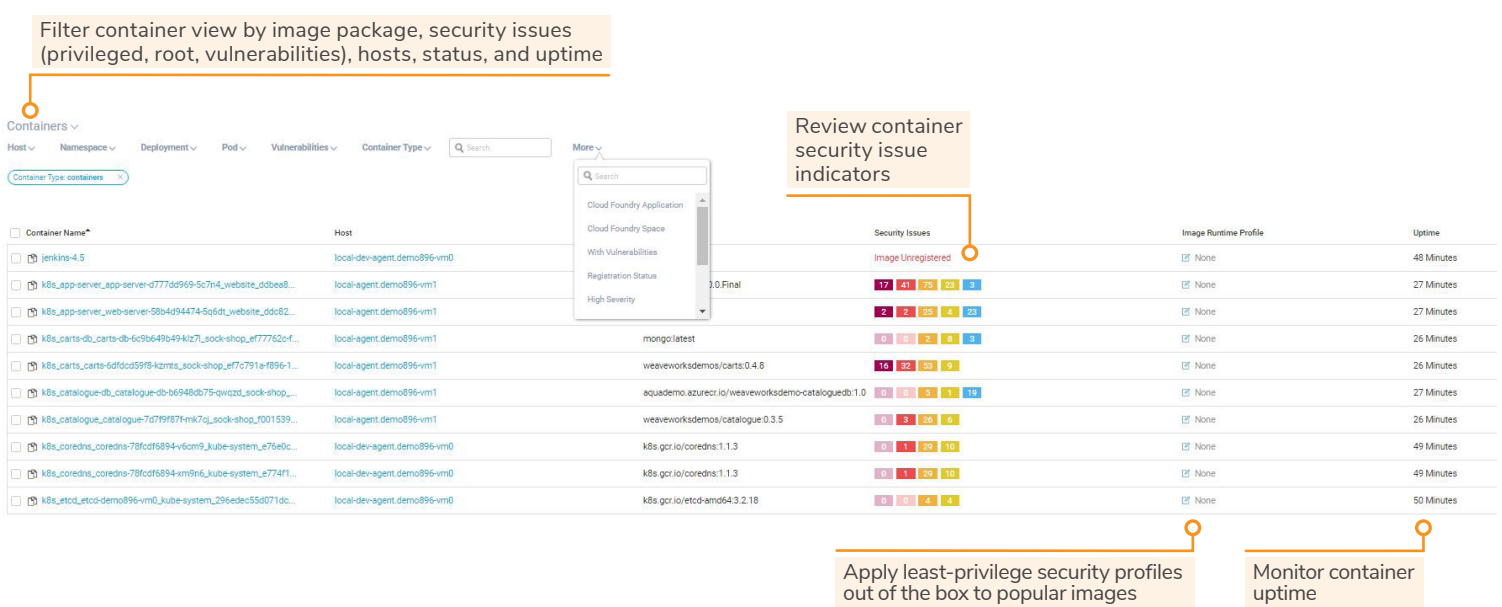
Can you perform instant impact analysis and list all workloads that have a specific vulnerability?

Can you immediately locate all workloads that have a certain package?

Easily filter workload data to clearly view, measure risks and remediation efforts.

- Provide real-time workload inventory
- Identify workloads with vulnerabilities and known bad packages
- Identify rogue workloads that are not registered or approved
- Identify workloads that do not comply with security mandates
- Identify privileged workloads and containers running as root
- Manage runtime controls per workload
- Sort and filter workload inventory according to uptime, status (stop/run), host, and image
- View running workload grouped by hosts/pods/Kubernetes namespaces and more

Image/container rotation is a security best practice. Recycled containers are more secured than stale, unpatched ones. To maintain a trusted production environment, continuously scan your images and recycled containers as needed.



Protect Workloads in Runtime - Global Controls

Control and monitor container activity in real-time based on automated, machine-learned runtime profiles. Automatically block and alert to SIEM based on suspicious activity.

Can you stop suspicious container activity without stopping or killing the container?

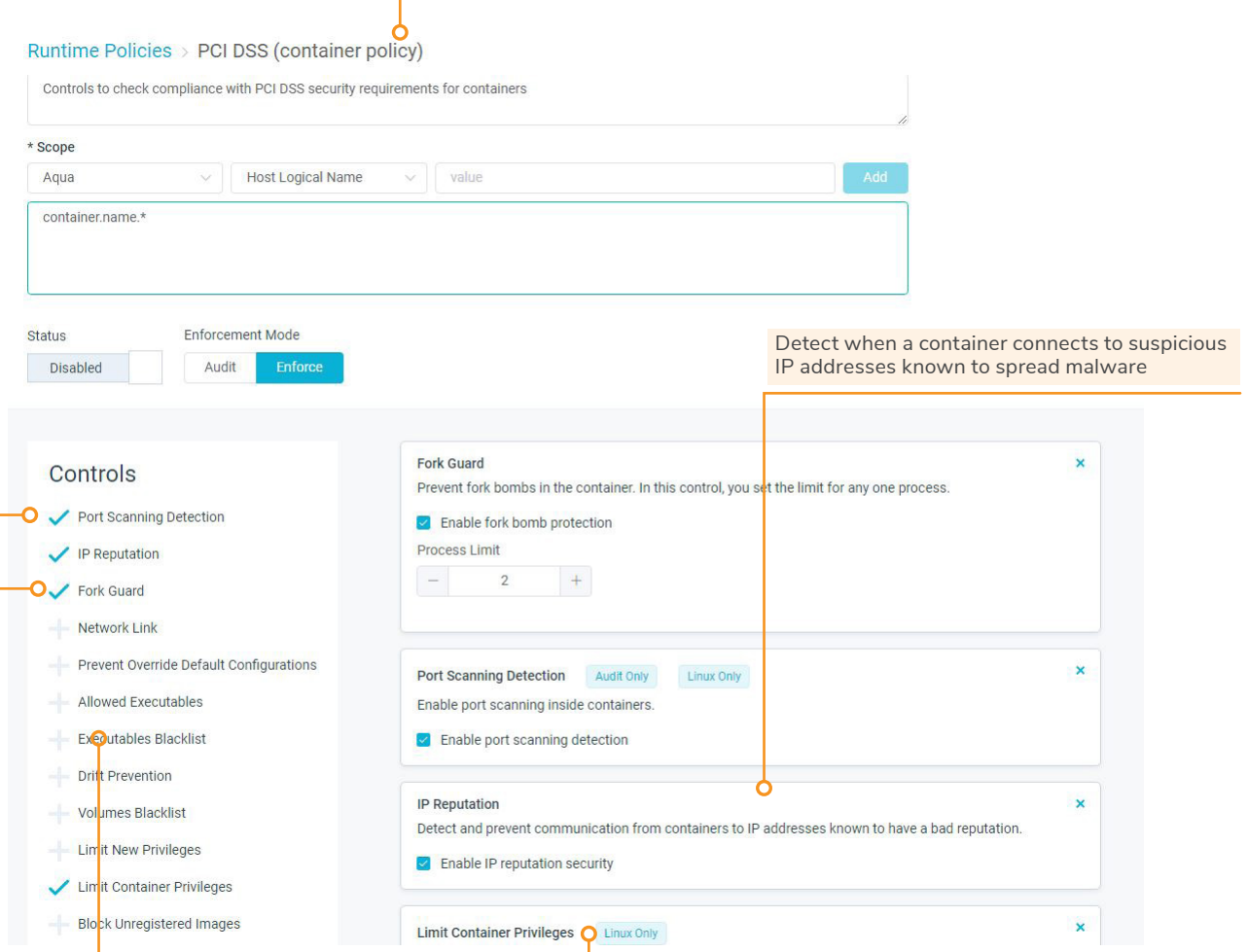
Can you detect rogue containers?

Global runtime controls are applicable to all containers, permitting only legitimate behaviors, to prevent several types of privilege abuse and attack vectors.

- Protect workloads running on hosts and in "hostless" CaaS environments (e.g., AWS Fargate and Azure Container Instances)
- Prevent containers from running as root, or with elevated privileges
- Set of pre-defined runtime policies based on security standards, such as NIST, CIS, PCI, and HIPAA
- Detect and prevent any change to containers (binaries, hash, system calls), compared with its originating image
- Prevent malicious behaviors such as port scanning, fork bombs and connections to suspicious external IPs
- Stop a container's unauthorized processes with no downtime to the running container itself
- Enforce policy changes without impacting running apps
- Apply and enforce custom runtime policies to specific runtime environments (e.g., apply blacklisted executables per namespace, or disallow unregistered images in a PCI cluster)

Prevent containers from scanning for open ports, an indication of malicious intent

Pre-built settings and alerts for key compliance mandates (PCI, HIPAA, NIST SP 800-190)



Detect when a container connects to suspicious IP addresses known to spread malware

Prevent a container from repeatedly opening processes, a DoS attack known as a “fork bomb”

Block any blacklisted executable from running in any container, with no container downtime

Maintain container least privileges principle & prevent privilege escalation

Protect Workloads in Runtime - Enforcing Immutability

With Aqua runtime policies and the image profile feature, you will get zero-touch runtime controls that ensure workload integrity and immutability (Image / Host / Function) without sacrificing application performance and availability.

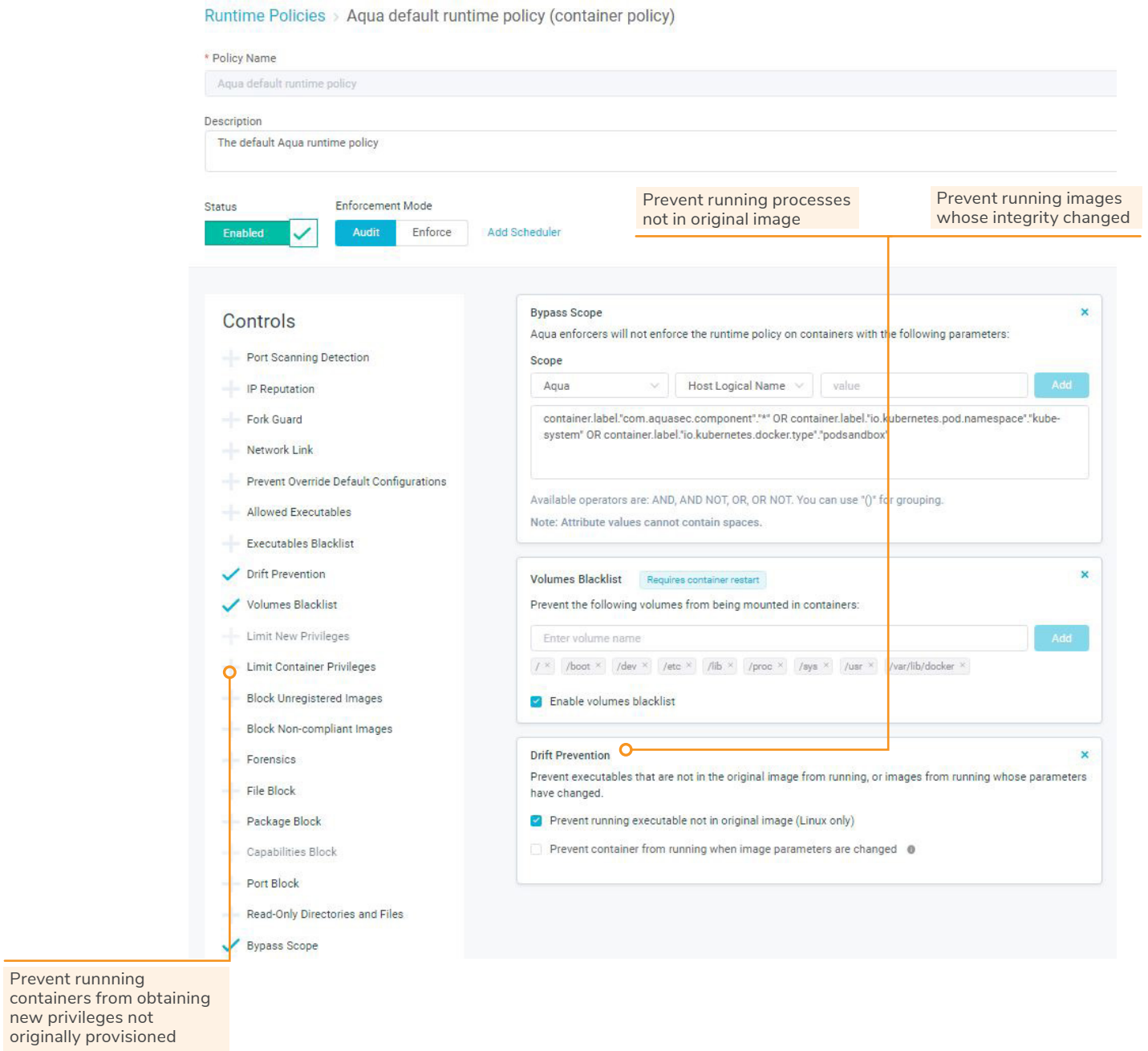
Can you ensure that containers currently running are identical with their originating images?

This is by far the most effective preventive measure you can take to protect your runtime environments from Zero-day threats, privileged user error, and insider threats.

- Prevents any attempt to alter workloads in runtime. For example, it adds new executables or files
- Enforces immutability in which updates are only pushed through the CI/CD pipeline, with no patching or changes allowed in runtime
- Creates cryptographic image fingerprinting for all layers within the image to ensure image integrity
- Enforce image-container integrity across staging and production environments

Image Runtime Profiles provide a set of controls to define authorized image activities. These profiles apply to containers instantiated from a specific image. They can be selected from predefined policies, machine-learned based on actual container activity, or assigned manually.

Aqua's unique Drift Prevention feature automatically prevents the running of executables which were not in the original image and seamlessly enforces immutability.

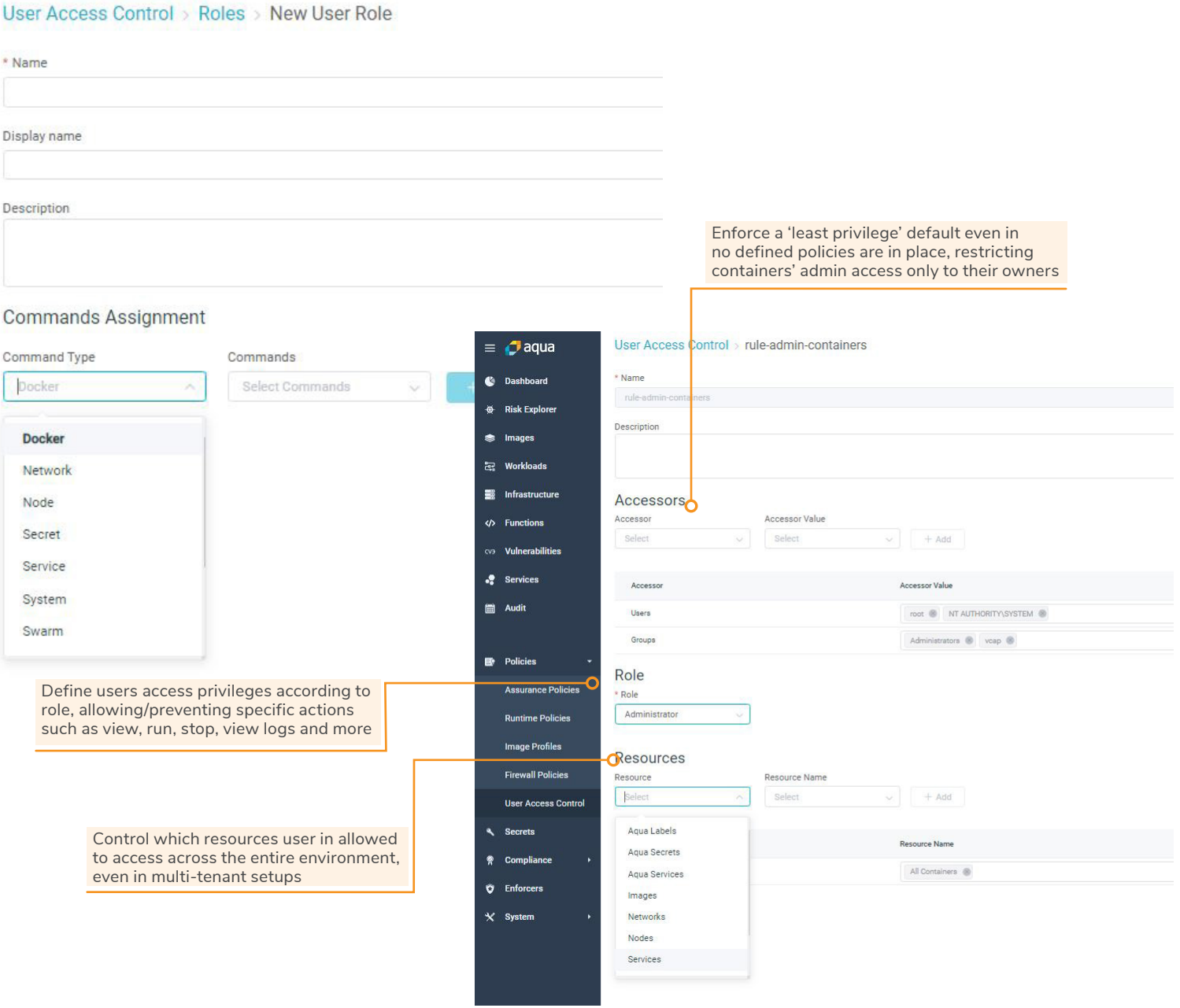

Runtime Policies › Aqua default runtime policy (container policy)
* Policy Name
Aqua default runtime policy
Description
The default Aqua runtime policy
Status
Enabled
Enforcement Mode
Audit
Enforce
Add Scheduler
Prevent running processes not in original image
Prevent running images whose integrity changed
Controls
Port Scanning Detection
IP Reputation
Fork Guard
Network Link
Prevent Override Default Configurations
Allowed Executables
Executables Blacklist
Drift Prevention
Volumes Blacklist
Limit New Privileges
Limit Container Privileges
Block Unregistered Images
Block Non-compliant Images
Forensics
File Block
Package Block
Capabilities Block
Port Block
Read-Only Directories and Files
Bypass Scope
Bypass Scope
Aqua enforcers will not enforce the runtime policy on containers with the following parameters:
Scope
Aqua
Host Logical Name
value
Add
container.label."com.aquasec.component"."*" OR container.label."io.kubernetes.pod.namespace"."kube-system" OR container.label."io.kubernetes.docker.type"."podsandbox"
Available operators are: AND, AND NOT, OR, OR NOT. You can use "()" for grouping.
Note: Attribute values cannot contain spaces.
Volumes Blacklist
Requires container restart
Prevent the following volumes from being mounted in containers:
Enter volume name
Add
/ /boot /dev /etc /lib /proc /sys /usr /var/lib/docker
Enable volumes blacklist
Drift Prevention
Prevent executables that are not in the original image from running, or images from running whose parameters have changed.
Prevent running executable not in original image (Linux only)
Prevent container from running when image parameters are changed
Prevent runnning containers from obtaining new privileges not originally provisioned

Manage and Control User Access

Can you assign and enforce user access permissions to container resources?

Aqua provides a fine-grained access control model that enforces access privileges at the container level from development to production, providing full accountability.

- Provide Role Based Access Control (RBAC) to limit super-user permissions, tasks and container resources access (e.g., images, containers, nodes, clusters, pods, volumes)
- Derive user access privileges based on application definitions in your orchestration system
- Assign Docker sub-commands to users on a specific host
- Assign Kubernetes master node operations to users by cluster, deployment, and node
- Provide self-service portals for auditors, security admins and developers to maintain segregation of duties while fostering collaboration
- Identify and trace the actual end-user identity behind the container account, with full audit trail and accountability
- Derive roles and privileges from existing AD/LDAP groups, and authenticate users


User Access Control › Roles › New User Role
* Name
Display name
Description
Commands Assignment
Command Type
Docker
Commands
Select Commands
Docker
Network
Node
Secret
Service
System
Swarm
Enforce a 'least privilege' default even in no defined policies are in place, restricting containers' admin access only to their owners
Define users access privileges according to role, allowing/preventing specific actions such as view, run, stop, view logs and more
Control which resources user in allowed to access across the entire environment, even in multi-tenant setups
aqua
Dashboard
Risk Explorer
Images
Workloads
Infrastructure
Functions
Vulnerabilities
Services
Audit
Policies
Assurance Policies
Runtime Policies
Image Profiles
Firewall Policies
User Access Control
Secrets
Compliance
Enforcers
System
User Access Control › rule-admin-containers
* Name
rule-admin-containers
Description
Accessors
Accessor
Accessor Value
Select
Select
+ Add
Accessor
Accessor Value
Users
root
NT AUTHORITY\SYSTEM
Groups
Administrators
voap
Role
* Role
Administrator
Resources
Resource
Resource Name
Select
Select
+ Add
Aqua Labels
Aqua Secrets
Aqua Services
Images
Networks
Nodes
Services
Resource Name
All Containers

Secure Function-as-a-Service

Ensure that serverless functions are free from known security risks through continuous discovery, scans, and monitoring.

Can you apply the same image controls to functions for consistent security governance and compliance?

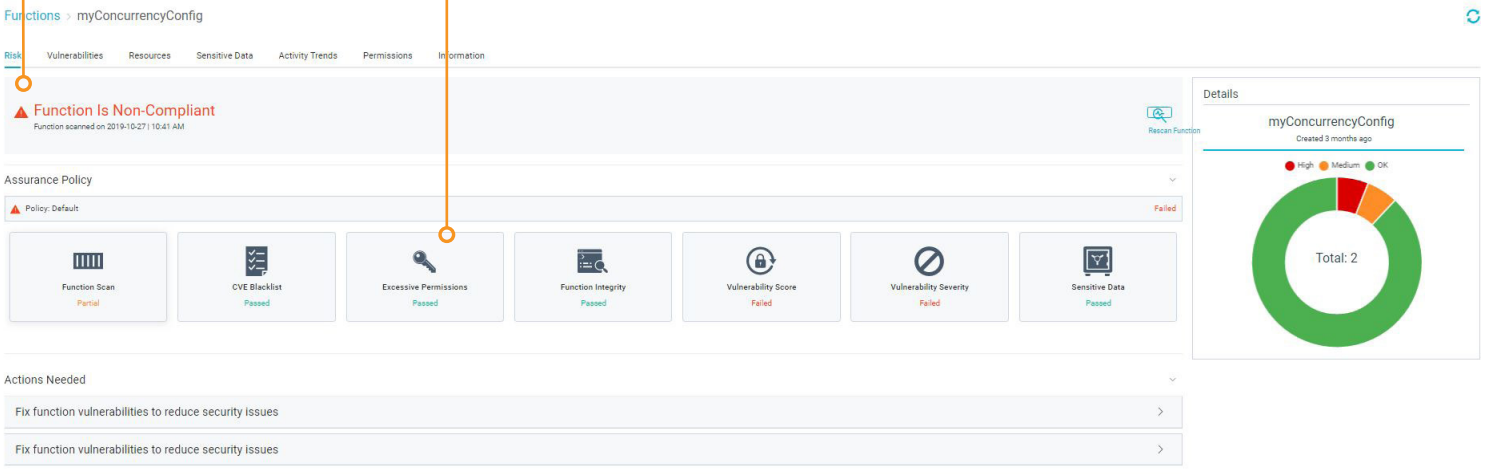
Can you ensure functions are authorized to run?

- Automatically discover and maintain secure function inventory
- Scan functions to detect vulnerabilities, embedded secrets, configuration errors, and sensitive data
- Quickly detect risks and amend IAM permissions issues associated with functions
- Detect secrets embedded in functions
- View actionable remediation information on detected vulnerabilities
- Generate granular audit trails of all scan events, vulnerability status, scan timelines, and remediation trends
- Gain top down security governance for all types of workloads (FaaS, CaaS, Microservices) across any platform or environment
- Controls the types of executables that are included in functions
- Blocks malicious code injection ("child processes") from being added to a running function
- Identifies abnormal usage trends in function runtime duration and invocation frequency
- Identifies unused roles and permissions to allow the reduction of unnecessary exposure
- Detects a function's attempt to run executables during the function's invocation from /tmp and blocks it

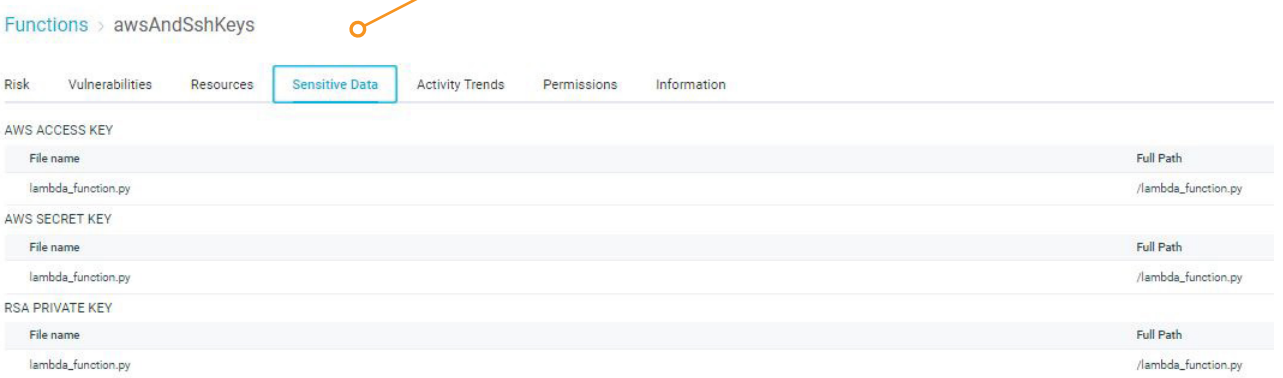
As opposed to containers, it's hard to control where and how serverless functions are used. Furthermore, disabling serverless functions is difficult because it's hard to determine which other services depend on the function. It is, therefore, critical to scan functions for known vulnerabilities, secrets, configuration errors, and over-provisioned privileges as a preventive measure.

Automatically discover and maintain secure inventory of functions based on assurance policy

Quickly detect risks to help amend privileges issues association with functions



Detect secrets embedded in functions



Risk Analysis & Compliance

Can you generate audit reports to demonstrate regulatory compliance around user/container access and activity?

Can you perform instant impact analysis to remediate a specific vulnerability?

Can you locate all containers that have a specific package immediately?

Aqua facilitates regulatory compliance by automating CIS benchmark testing for both Kubernetes and Docker, scanning images and hosts for malware and vulnerabilities, and collecting granular container-level events for auditing and reporting.

- Generate granular audit trails of all access activity, scan events and coverage, Docker/K8s commands, container activity, secrets activity and system events
- Provide full user accountability and controlled super-user permissions
- Pre-built alerts and reports for key compliance mandates (PCI, GDPR, HIPAA, NIST SP 800-190)
- Automated CIS Docker and CIS Kubernets benchmark reports
- Integrations to analytics and SIEM tools including Splunk, ArcSight, QRadar, and more
- Track changes in vulnerability status, timeliness of scan, and remediation trends

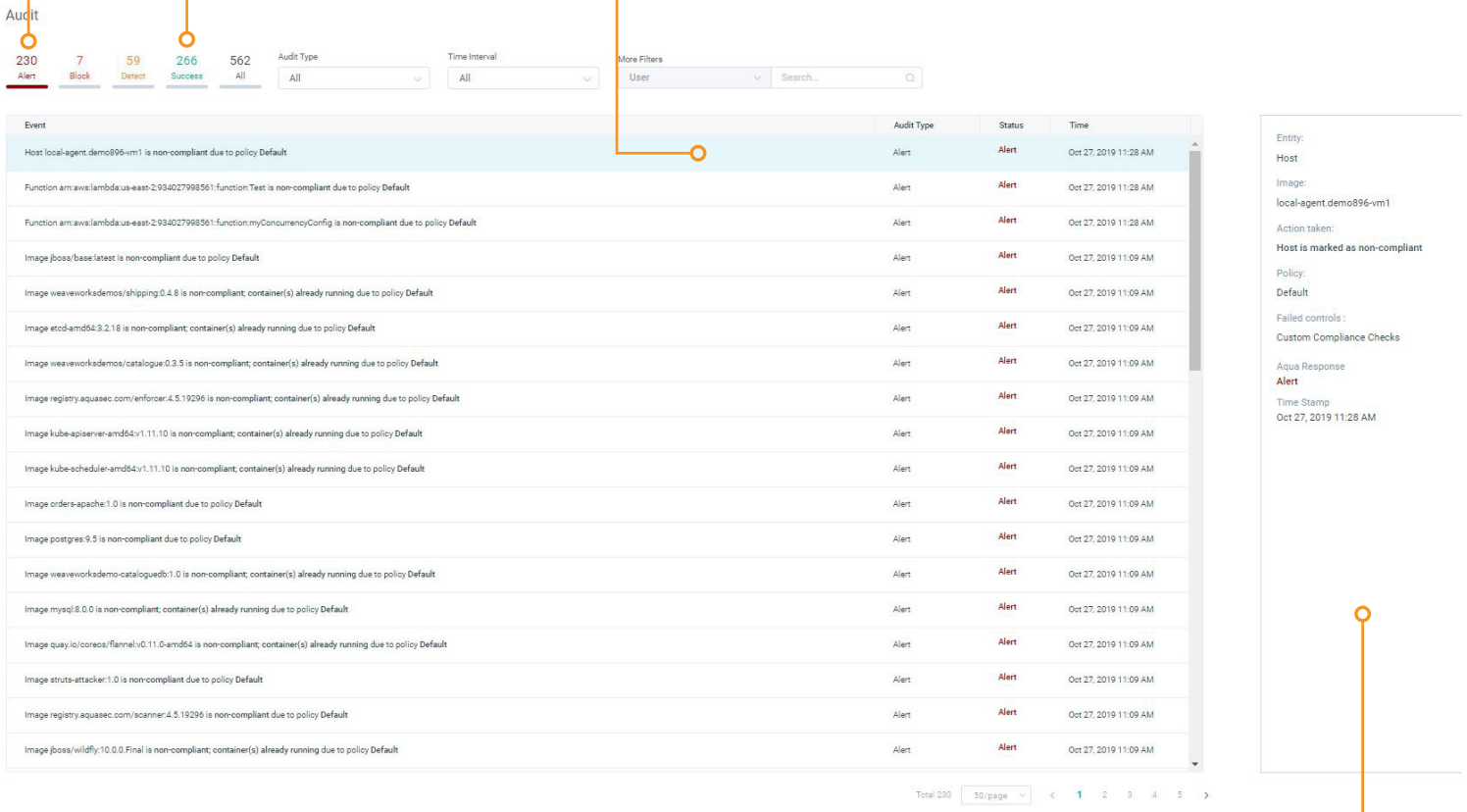
Run compliance checks of your Kubernetes environment according to the CIS Kubernetes Benchmark – it's an ideal framework to start mitigating risks.

Always log. Collect Kubernetes-specific logs, such as pod name, type, deployment and namespace data, in addition to user access (both failed and successful login attempts), container start/stop, etc. This data is crucial for compliance and makes it possible to conduct thorough forensics and incident response.

Get real-time alerts on policy violations

Ability to track changes in vulnerability status

Granular event audit log, with integrations to analytics and SIEM tools including Splunk, ArcSight, QRadar, and more



Displays additional information about each audit event. The information varies based on the event type

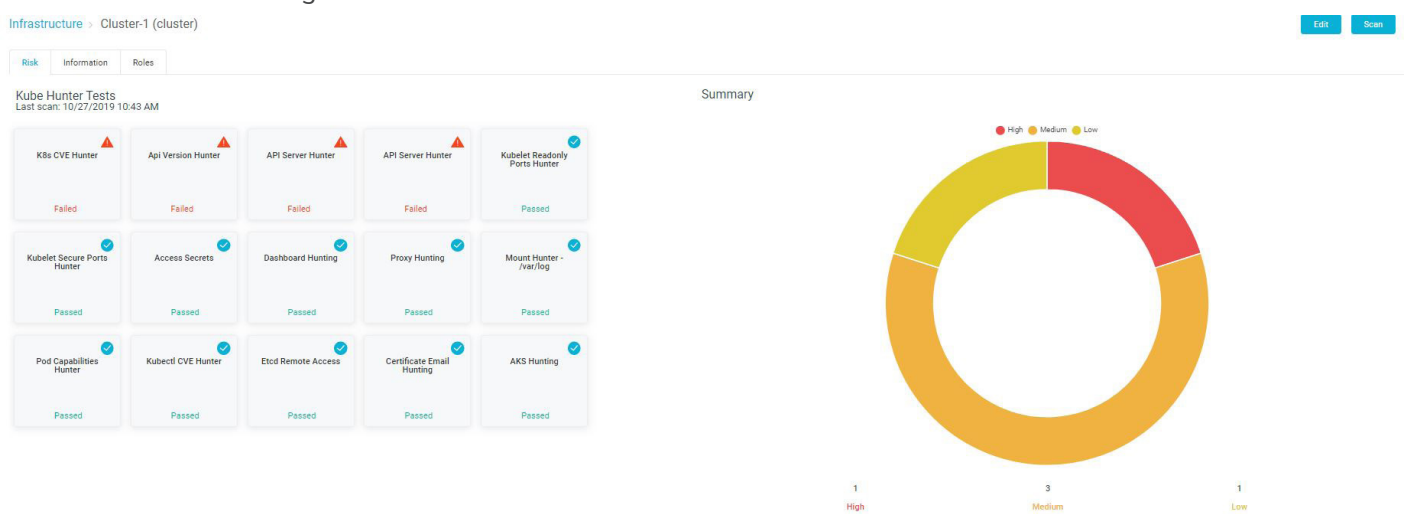
Hardening the Host and Orchestrator Environment

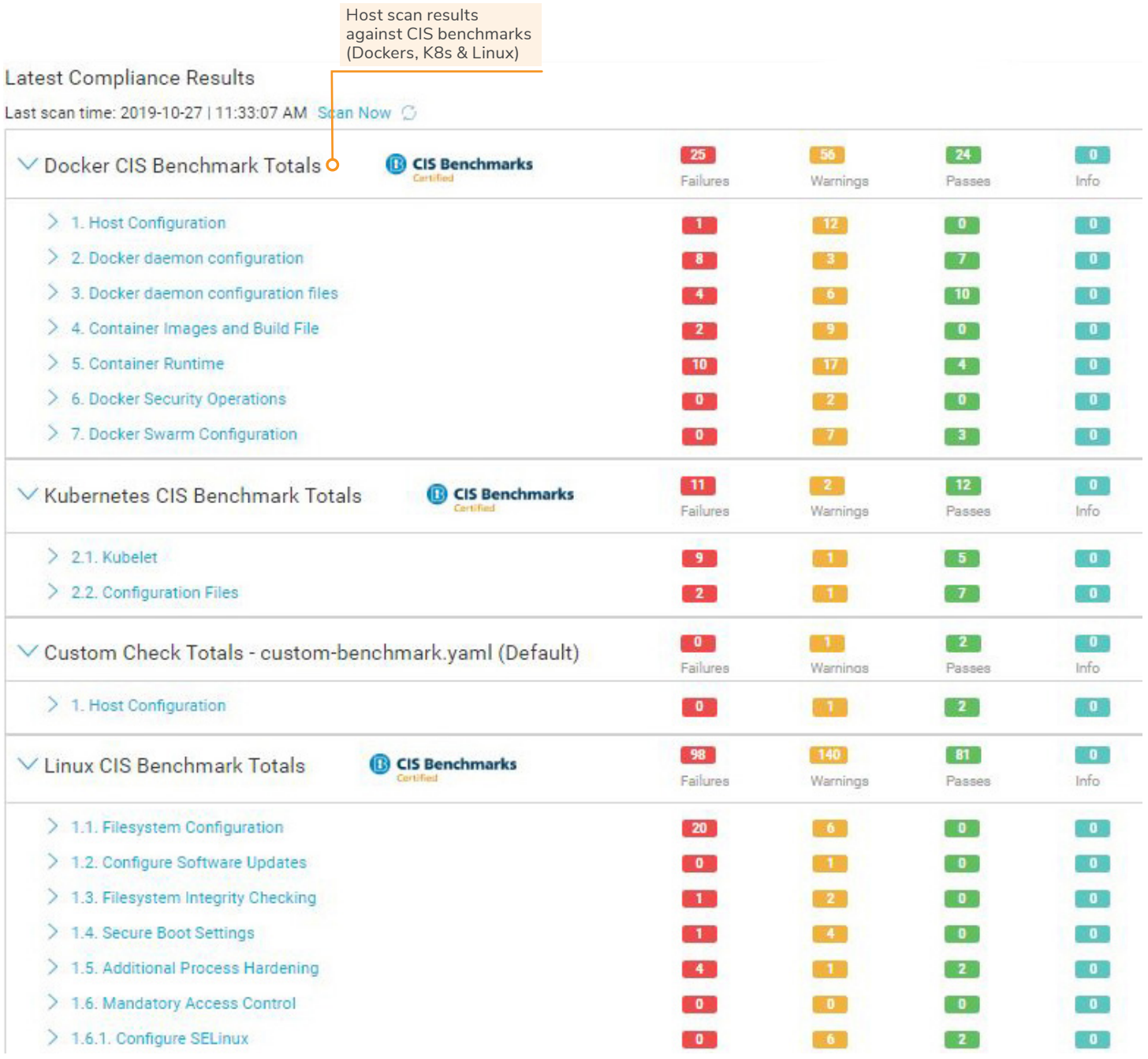
Can you ensure that the OS and the container engine versions are up to date and fully patched?

Can you ensure that your Kubernetes environment is properly secured, and that access control, networking and authentication are all in check?

Aqua performs host integrity checks, including vulnerability scan, malware and CIS tests to ensure hosts are secured and that user access is controlled and monitored.

- Automatically scan hosts for OS vulnerabilities, malware, and login attempts
- Ensure OS level controls, such as SELinux/AppArmor are enforced
- Alert on suspicious host activities, such as brute force login attacks
- Control and monitor container access rights to OS and host resources
- Creates custom compliance checks to be evaluated on the host
- Scans your Kubernetes cluster for security issues with Kube-Hunter, probes for open Kubernetes-related ports, and tests for any configuration issues that might leave your cluster exposed to attackers
- Generates a full report that highlights the security concerns that reside in your environment
- Control and monitor user logins to host




Host scan results against CIS benchmarks (Dockers, K8s & Linux)
Latest Compliance Results
Last scan time: 2019-10-27 | 11:33:07 AM Scan Now
Docker CIS Benchmark Totals
CIS Benchmarks
25 Failures
56 Warnings
24 Passes
0 Info
1. Host Configuration 1 12 0 0
2. Docker daemon configuration 8 3 7 0
3. Docker daemon configuration files 4 6 10 0
4. Container Images and Build File 2 9 0 0
5. Container Runtime 10 17 4 0
6. Docker Security Operations 0 2 0 0
7. Docker Swarm Configuration 0 7 3 0
Kubernetes CIS Benchmark Totals
CIS Benchmarks
11 Failures
2 Warnings
12 Passes
0 Info
2.1. Kubelet 9 1 5 0
2.2. Configuration Files 2 1 7 0
Custom Check Totals - custom-benchmark.yaml (Default)
0 Failures
1 Warnings
2 Passes
0 Info
1. Host Configuration 0 1 2 0
Linux CIS Benchmark Totals
CIS Benchmarks
98 Failures
140 Warnings
81 Passes
0 Info
1.1. Filesystem Configuration 20 6 0 0
1.2. Configure Software Updates 0 1 0 0
1.3. Filesystem Integrity Checking 1 2 0 0
1.4. Secure Boot Settings 1 4 0 0
1.5. Additional Process Hardening 4 1 2 0
1.6. Mandatory Access Control 0 0 0 0
1.6.1. Configure SELinux 0 6 2 0

Protection for Your Virtual Machines

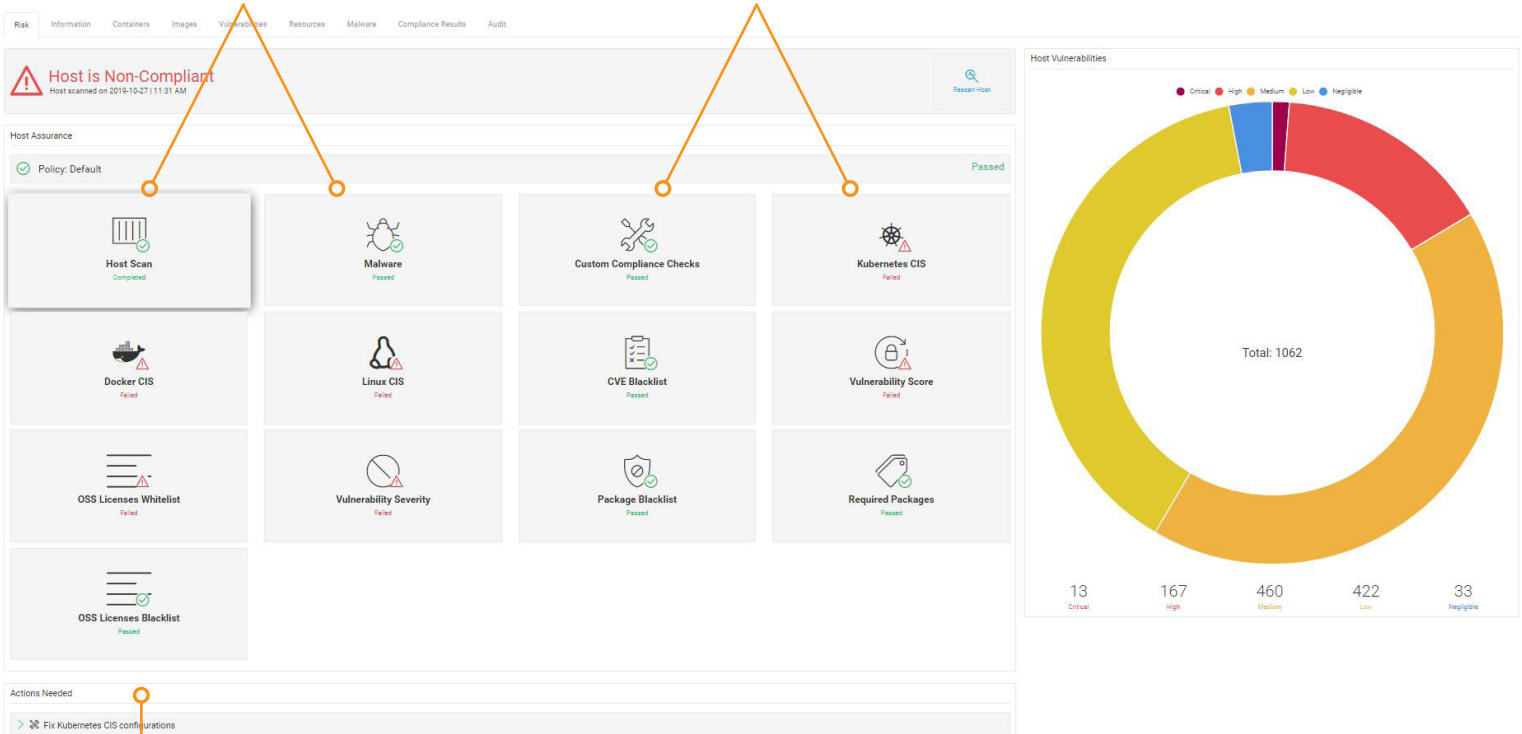
VM Enforcers provide protection for hosts (virtual machines) with no dependency on either Docker or Kubernetes. Both Windows and Linux hosts can be protected wit Aqua's VM Enforcer.

- Prevents access to the host by specified users and/or groups of users
- Audits user activity on the host VM
- Monitors files, file attributes and directories on your hosts for read, write, and modify operations
- Scans hosts for known vulnerabilities
- Applies runtime policies to ensure host immutability
- Checks for sensitive data such as private RSA keys on the host VM
- Automatically records of all inbound and outbound network traffic
- Define a compliance baseline for your VMs

Scan your VM for vulnerabilities and malware and align with industry security standards, such as Linux CIS and PCI-DSS

Scan cloud VMs for known vulnerabilities and malware

Define a compliance baseline for VMs by using built-in and custom configuration checks



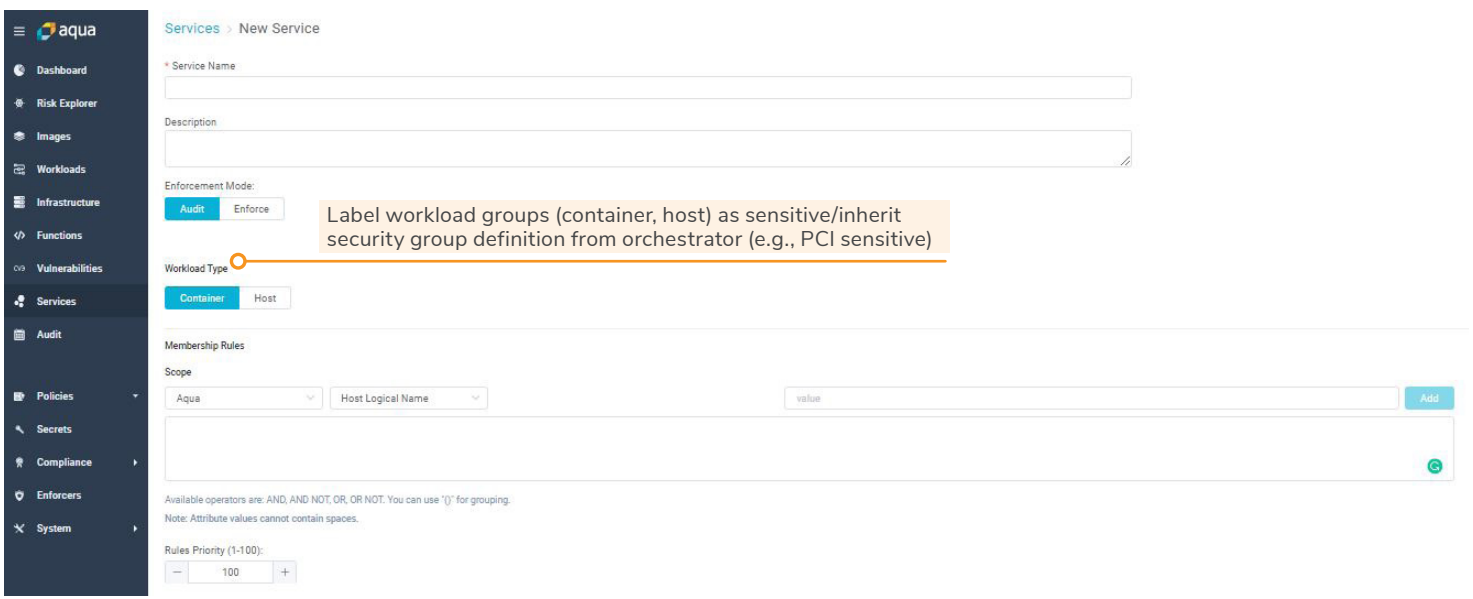
Review actionable remediation steps

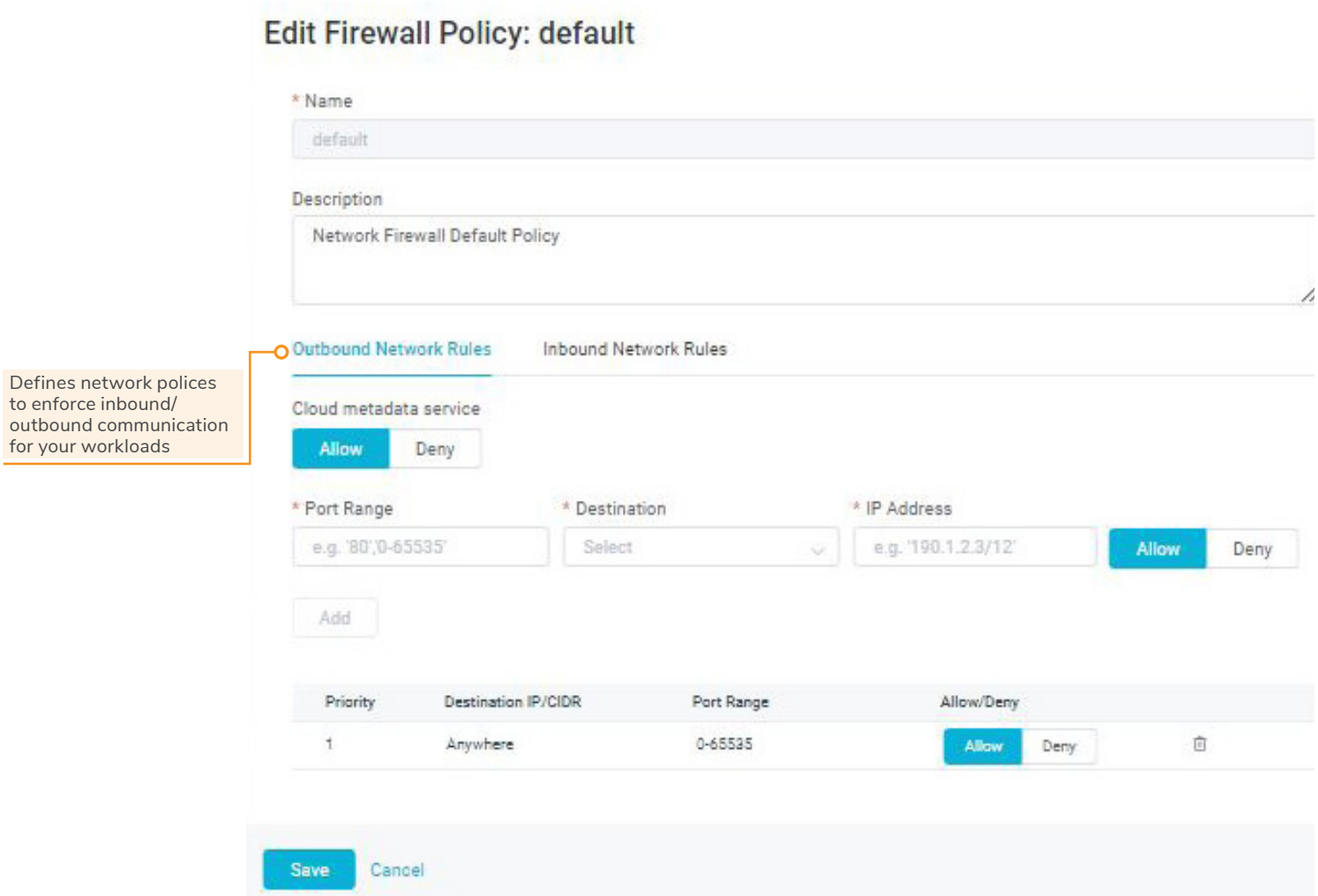
Workload Firewall

Can you control network traffic between containers, across different hosts, or even on the same host?

Limits the "blast radius" of attacks by controlling the communications between your workloads in your cloud native environment and defines nano-segments based on the microservices context. Automatically discovers container network topology, both within a host and across hosts/pods, and applies context-based firewalls.

- Automatically recommends firewall rules to microservices that whitelist permitted connections
- Automatically sets alert on and blocks unauthorized communication flows with no downtime
- Limits network traffic to a specific process within a container/host
- Provides content-rich visibility to network traffic for cloud native workloads
- Defines container network connections based on orchestrator concepts (pod name, namespaces), IP/CIDR addresses, and DNS
- Manually modifies communication rules/policy based on actual activity, without impacting performance and availability




Edit Firewall Policy: default
* Name
default
Description
Network Firewall Default Policy
Outbound Network Rules
Inbound Network Rules
Defines network polices to enforce inbound/ outbound communication for your workloads
Cloud metadata service
Allow
Deny
* Port Range
* Destination
* IP Address
e.g. '80',0-65535'
Select
e.g. '190.1.2.3/12'
Allow
Deny
Add
Priority
Destination IP/CIDR
Port Range
Allow/Deny
1
Anywhere
0-65535
Allow
Deny
Save
Cancel

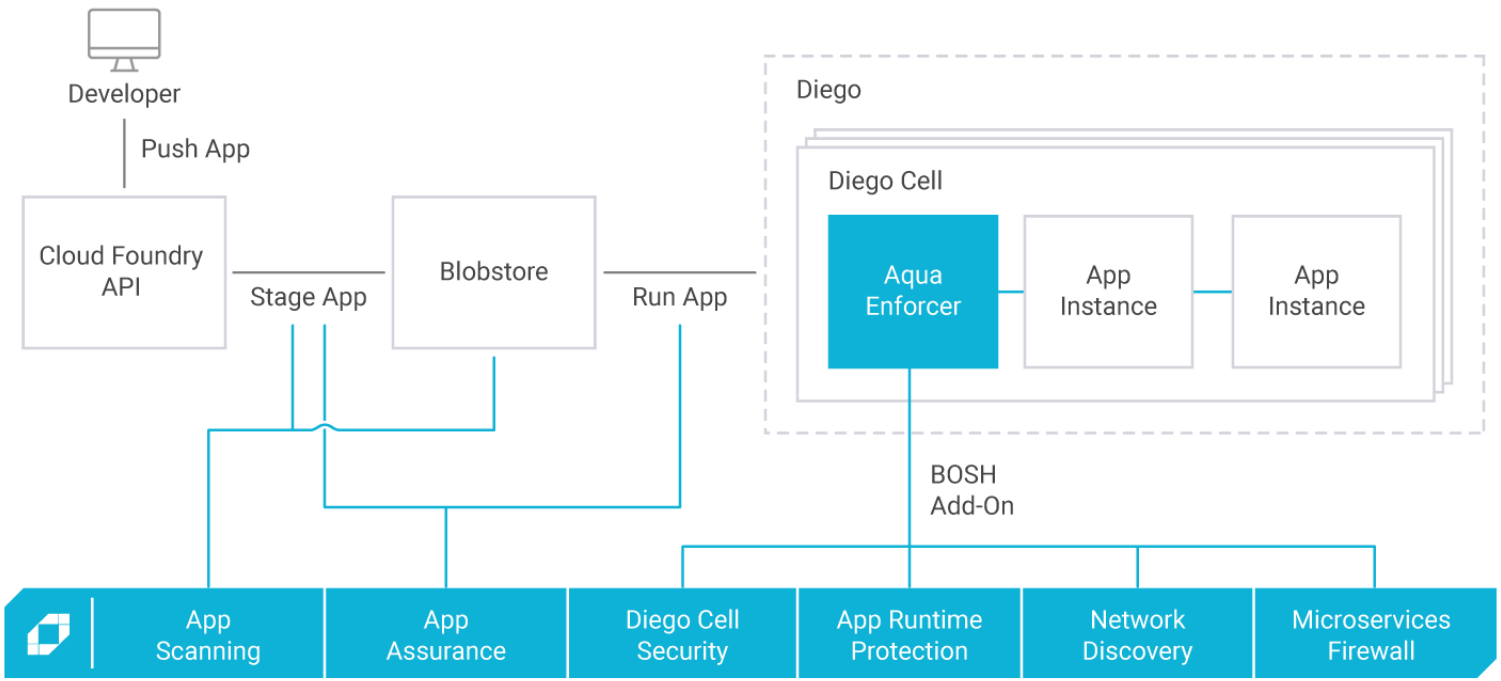
A Full Lifecycle Security Solution for Pivotal Application Service (PAS) Containers

Aqua provides a full lifecycle solution for Pivotal Application Service workloads, from scanning and deployment assurance, policies for new runtime controls using a single pane of glass for policy management and visibility, and native capabilities that are easy to apply across all PAS applications.

- Scans applications in CI and in the Blobstore for known vulnerabilities, embedded secrets, and malware
- Blocks non-compliant Droplets from being staged in the Blobstore and from running on Diego cells
- Prevents running executables that weren't in the original droplet
- Automated profiling and whitelisting of processes used in the running instance
- Monitors and protects Diego cells (hosts) against vulnerabilities, malware, and suspicious user activity
- Discovers the network connections within an application and creates firewall rules

Aqua for PAS provides a unified security solution across both PAS environments and Kubernetes-based environments (including PKS), using a single pane of glass for policy management and visibility, and native capabilities suited to each mode of cloud native deployment.

PAS users can integrate Aqua with their existing CI/CD tools for security testing as part of the build, with Active Directory/ LDAP for user authentication, and with SIEM/analytics to generate audit and alert data.

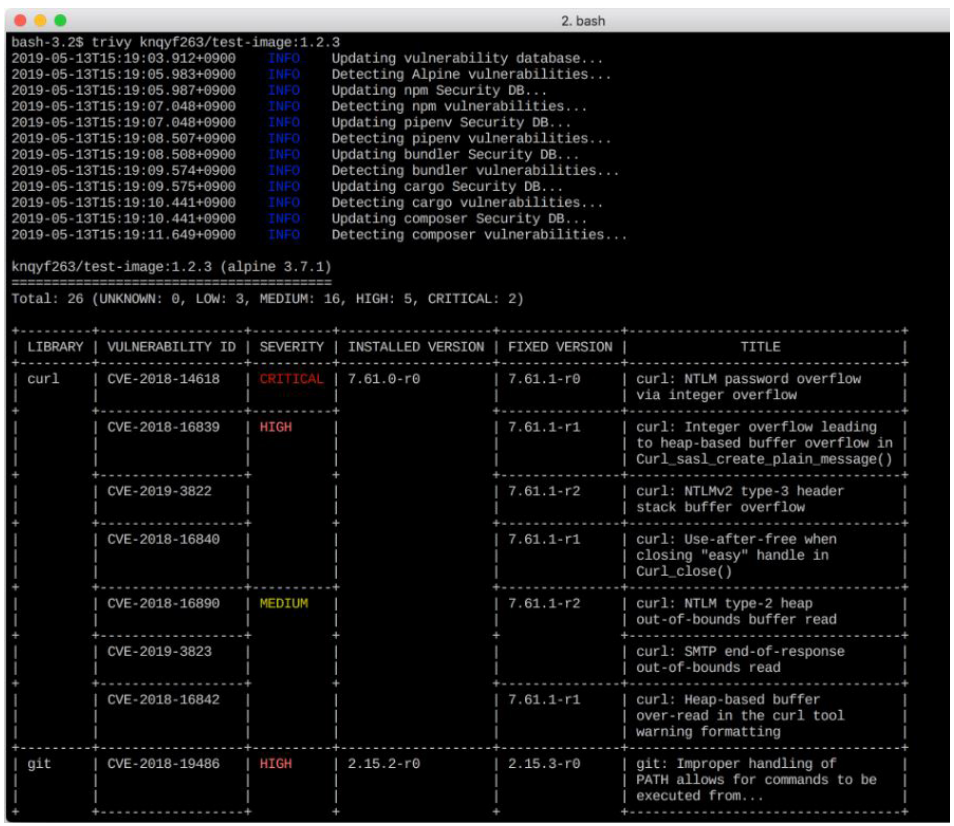

Developer
Push App
Cloud Foundry API
Stage App
Blobstore
Run App
Diego
Diego Cell
Aqua Enforcer
App Instance
App Instance
BOSH Add-On
App Scanning
App Assurance
Diego Cell Security
App Runtime Protection
Network Discovery
Microservices Firewall

Open Source Projects

Aqua is committed to helping the container ecosystem deliver more secure code. We dedicate some of our resources to create and maintain open source projects, and we contribute to existing ones. Here are some of our most popular open source projects:

Trivy A unique, open source project that provides static analysis of vulnerabilities in containers' images. It detects vulnerabilities of OS packages and application dependencies. You just need to install the binary, provide Trivy with the image name of your container, and start scanning.

github.com/aquasecurity/trivy

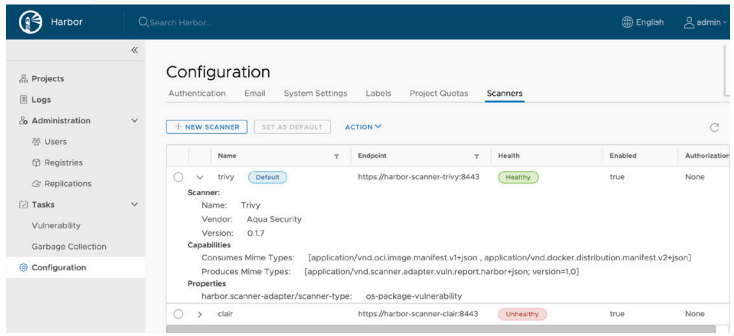


Integrate Trivy into your CI pipeline and embed vulnerability scanning as a step in your build.

Harbor Vulnerability Scanning

We are working with CNCF's Harbor project to enable you to plug in the vulnerability scanner of your choice into the Harbor registry, including Trivy and Aqua's commercial scanner. The main propose of this project is to allow you the freedom to choose which vulnerability scanner you want to work with and implement any Open Source or commercial vulnerability scanner by making a simple configuration change.

github.com/aquasecurity/harbor-scanner-trivy



Kube-hunter probes your cluster for security issues and thereby increases awareness and visibility of the security controls in Kubernetes environments:

- Pen-test responsibly: Arms Kubernetes admins, operators, and engineers with an easy way to identify weaknesses in their deployments
- Passive and active "hunters": Conducts tests that probe for potential access points (like open ports) within your cluster and looks for common misconfiguration.

kube-hunter.aquasec.com/

172.17.0.1
Node / Master

6 vulnerabilities

SEVERITY	CATEGORY	VULNERABILITY	DESCRIPTION	EVIDENCE
High	Remote Code Execution	Dashboard Exposed	All oprations on the cluster are exposed	nodes: minikube
High	Remote Code Execution	Anonymous Authentication	The kubelet is misconfigured, potentially allowing secure access to all requests on the kubelet, without the need to authenticate	
Medium	Information Disclosure	K8s Version Disclosure	The kubernetes version could be obtained from logs in the /metrics endpoint	v1.10.0
Medium	Information Disclosure	Cluster Health Disclosure	By accessing the open /healthz handler, an attacker could get the cluster health state without authenticating	status: ok

Kube-bench automates CIS Kubernetes benchmarks and enables you to immediately see if your setup conforms to best practices in key areas such as:

- Proper user authentication and authorization
- Securing data in transit
- Securing data at rest
- Using least privileges

github.com/aquasecurity/kube-bench

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
```

Why the Global 2000 Rely on Aqua

Full Lifecycle Security

The only solution that is designed to secure the entire lifecycle of containerized applications, from development through testing to production, whether they are Windows or Linux containers, Container-as-a-Service, or serverless functions.

Multi-Tenancy Management

The only solution that enables multi-tenancy by providing universal policy management across tenancies, while also delegating customer policy management capabilities at the tenant level. Data and reports from the tenant levels roll up to the top level, allowing admins to monitor and enforce policies on a global level.

Superior Runtime Protection

The only solution that enforces image immutability and least privileges principle to prevent 0-day attacks, enabling the lockdown of container activity to allow only legitimate behavior, in addition to enforcing container runtime network profiles to minimize false positives and maximize protection.

Secure Once, Run Anywhere

The only solution that secures workloads running on-premise and on multiple cloud environments such as AWS, Azure, and Google, using any platform and orchestrator, including Kubernetes, RedHat OpenShift, Pivotal Cloud Foundry, Docker Enterprise Edition, with any runtime engine, e.g. Docker, ContainerD, CRI-O.

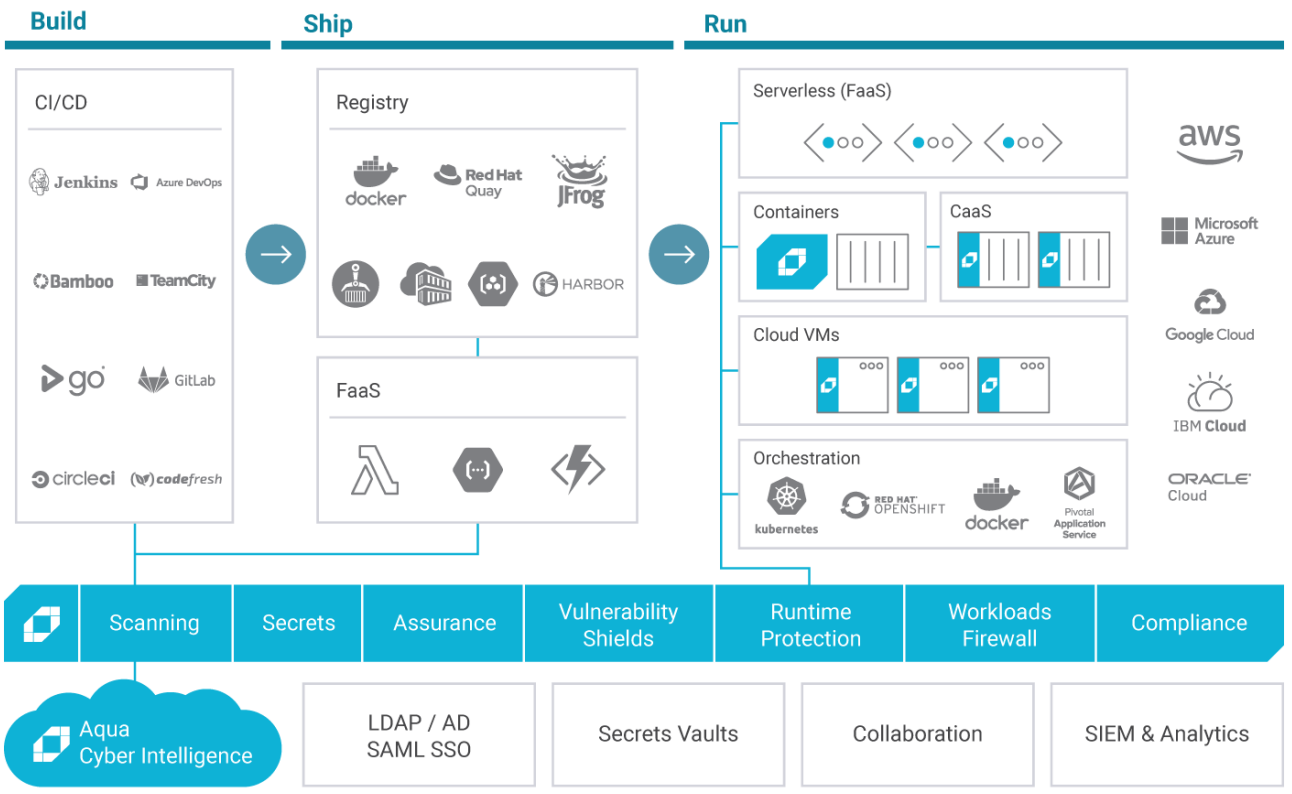
Ensure Business/Mission-Critical Applications' Continuity

The only solution that provides real, automated security without sacrificing business continuity. We offer granular blocking that only prevents suspicious actions without stopping the application, and secrets rotation, with no container restart.

Unrivaled Support

Our stellar customer success team is committed to your success, where every customer is guaranteed comprehensive onboarding, training, and technical support. We partner with our customers to ensure their needs and requirements are met – every step of the way. At Aqua, we put our customers first.

Aqua Cloud Native Security Platform



To learn more, visit our Resource Center
www.aquasec.com/resources

Schedule a 1-on-1 demo
www.aquasec.com/demo