

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.



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.



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.



Meets Regulatory Mandates and Industry Recommendations

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



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.



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.



Workloads Firewall

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



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.

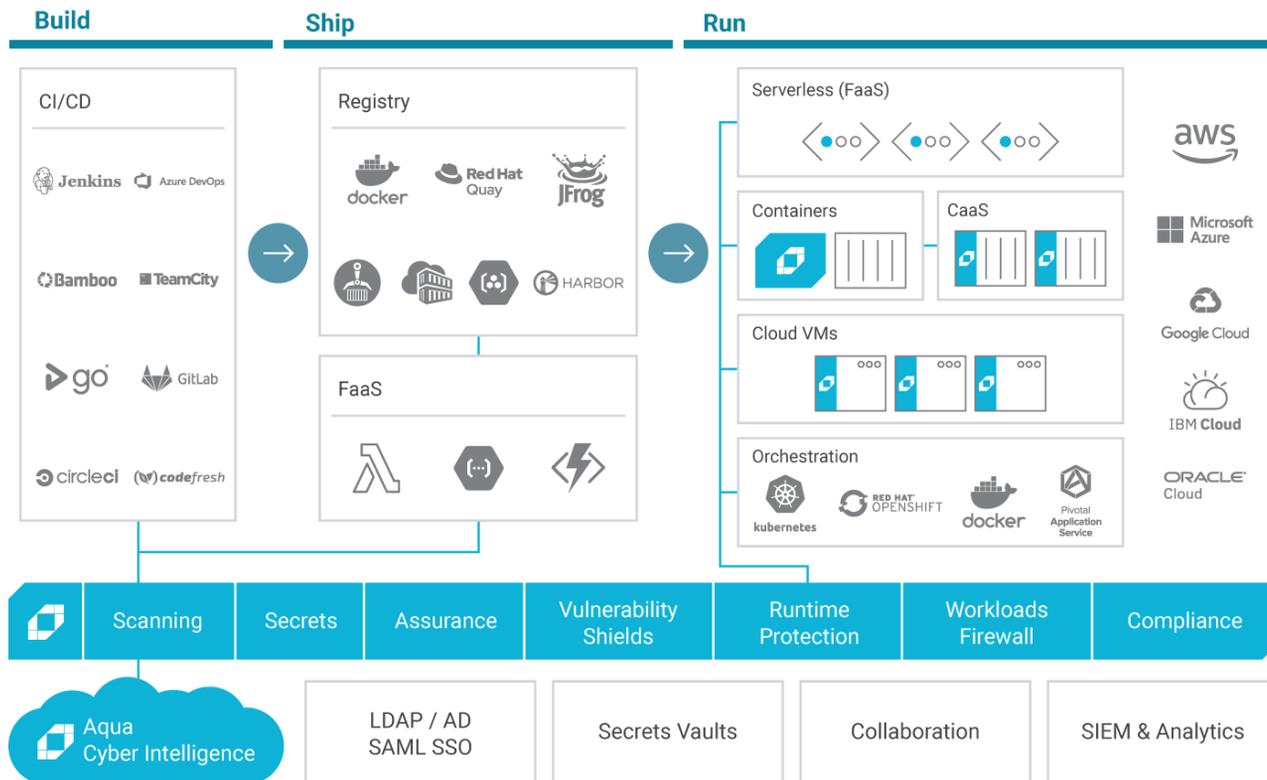
Aqua Cyber Intelligence Feed Aggregates and correlates multiple sources, including NVD, vendor advisories, and proprietary research, providing continuous, up-to-date information to Aqua's vulnerability scanning, malware detection, and threat mitigation features.

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).

The screenshot shows the Risk Explorer interface. At the top, it says "Risk Explorer" and "Auto-Refresh Off" with a toggle switch. Below this, there are statistics: "Namespaces 6" and "Controllers 28 / 28 (Reset)".

On the left, there is a sidebar with "29 Images" and "2 Hosts". The "Images" section is expanded, showing a list of images with their Docker Hub sources and the number of running containers. The list includes:

- httpd:2.4.28 (Docker Hub, 1 Running Container)
- jboss/wildfly:10.0.0.Final (Docker Hub, 1 Running Container)
- mysql:8.0.0 (Docker Hub, 1 Running Container)
- quay.io/coreos/flannel:v0.11.0-localhost (localhost, 2 Running Containers)
- rabbitmq:3.6.8 (Docker Hub, 1 Running Container)
- weaveworksdemos/carts:0.4.8 (Docker Hub, 1 Running Container)
- weaveworksdemos/front-end:0 (Docker Hub, 1 Running Container)
- weaveworksdemos/orders:0.4. (Docker Hub, 1 Running Container)
- weaveworksdemos/queue-mas (Docker Hub, 1 Running Container)
- weaveworksdemos/shipping:0 (Docker Hub, 1 Running Container)

The main area is a risk map showing various namespaces: website, kube-system, aqua, blog, sock-shop, and default. Each namespace contains colored circles representing controllers, with colors indicating risk levels (red for high, orange for medium, green for low, purple for negligible). Annotations include:

- "Review only the objects that are part of the running workloads" pointing to the website namespace.
- "Filter based on high risk objects" pointing to the risk assessment legend.

On the right, there is a "Risk Assessment" legend with categories: Critical (10), High (7), Medium (9), Low (0), Negligible (0), and None (2). Below that is a "Containers per Controller" filter with buttons for >3, 2-3, and 1. At the bottom right, there are navigation icons for zooming in and out.

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

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.

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.

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.)

Images > centos:7

Risk Vulnerabilities Resources Sensitive Data Malware Information Scan History Audit

Image Is Non-Compliant
Image scanned on 2019-10-27 | 01:50 PM

Rescan Image

Image Assurance

Policy: Default Failed

Image Scan Completed	Package Blacklist Passed	Custom Compliance Checks Failed	CVE Blacklist Passed	MicroEnforcer Failed
OSS Licenses Blacklist Passed	Malware Passed	Vulnerability Score Failed	Vulnerability Severity Failed	OS Package Manager Passed
Required Packages Passed	Super User Failed	Sensitive Data Passed	OSS Licenses Whitelist Failed	

Actions Needed

Details

centos:7
Created 2 months ago

High Medium

Total: 59

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

Assurance Policies > Aqua-Demo (image policy)

* Scope

Aqua

aqua.registry.aquademo

Actions

Block/alert on images that failed image assurance policy

- Create an audit message when an image fails this policy
- Fail the Aqua step in CI/CD
- Mark failed images as non-compliant

Exceptions

Set temporarily acknowledgment rules what will be deleted after defined amount of days

- Ignore vulnerabilities that have no available fix
- Ignore vulnerabilities that were published in the last days
- Ignore specific vulnerabilities
- Ignore vulnerabilities and malware found in specific path

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

Controls

- + Super User
- + CVE Blacklist
- + Package Blacklist
- + Required Packages
- + Vulnerability Severity
- Vulnerability Score
- + Approved Base Image

Sensitive Data

This control checks if images have sensitive data such as private RSA keys

- Enable sensitive data control

Vulnerability Score

This control checks if images have vulnerabilities that exceeded or matched the selected score

- Enable vulnerability score control

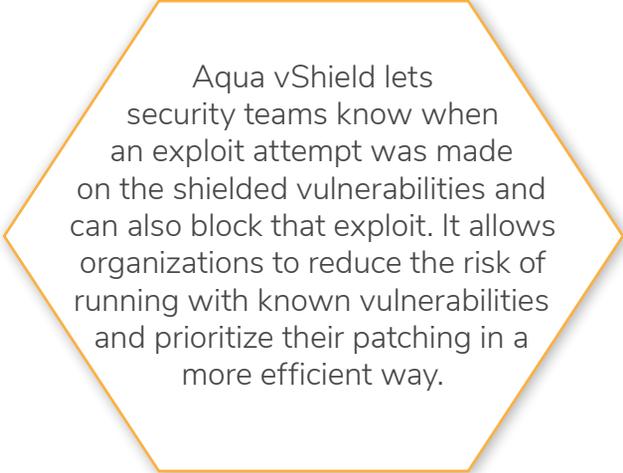


Malware

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.

Vulnerabilities

Vulnerability	Image	Severity	Workloads	Resource	Vendor Fix	vShield Status	Acknowledgment
CVE-2018-14721	jboss/wildfly:10.0.0.Final	Critical	1	/opt/jboss/wildfly/modules/system/layers/base/com/fasterxml/jackson/core/jackson-databind/main/jackson-data	✓	vShield	Acknowledge
RHSA-2017-11100	jetbi/demo:3.0	Critical		nas	✓		Acknowledge
RHSA-2019-1587	jetbi/demo:3.0	Critical		python	✓		Acknowledge
RHSA-2019-0710	jetbi/demo:3.0	Critical		python	✓		Acknowledge
DLA-1499-1	wordpress:4.7.0-apache	Critical		curl	✓		Acknowledge
DSA-3952-1	wordpress:4.7.0-apache	Critical		libxml2	✓		Acknowledge
DSA-3746-1	wordpress:4.7.0-apache	Critical		libxml2	✓		Acknowledge
DLA-1580-1	wordpress:4.7.0-apache	Critical		systemd	✓		Acknowledge
CVE-2016-5636	orders-apache:1.0	Critical		python2.7	✓	vShield	Acknowledge
DLA-1580-1	orders-apache:1.0	Critical		systemd	✓		Acknowledge
DSA-3952-1	orders-apache:1.0	Critical		libxml2	✓		Acknowledge
DSA-3746-1	orders-apache:1.0	Critical		libxml2	✓		Acknowledge
DLA-1499-1	orders-apache:1.0	Critical		curl	✓		Acknowledge
CVE-2008-0697	orders-apache:1.0	Critical		jdk	✓		Acknowledge
CVE-2018-14618	struts-attacker:1.0	Critical		curl	✓	vShield	Acknowledge
DLA-1224-1	struts-attacker:1.0	Critical		mercurial	✓		Acknowledge
CVE-2016-4448	struts-attacker:1.0	Critical		libxml2	✓		Acknowledge
CVE-2016-4658	struts-attacker:1.0	Critical		libxml2	✓		Acknowledge
CVE-2017-7376	struts-attacker:1.0	Critical		libxml2	✓		Acknowledge
CVE-2003-0890	wordpress-plugins	Critical		php	✓		Acknowledge
CVE-2003-0861	wordpress-plugins	Critical		php	✓		Acknowledge
CVE-2004-1019	wordpress-plugins	Critical		php	✓		Acknowledge

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

Vulnerabilities > vShield

This is a vShield policy created by Aqua. You can change only the Enforcement Mode; if you select Audit mode, you can also add a Scheduler. You can also delete this vShield policy.

Policy Name
AQP_DVE-2016-3082_orders-apache:1.0

Description
Auto generated vShield orders-apache:1.0 Policy

Scope
Aqua Host Logical Name value

Image.name.orders-apache:1.0 AND (image.prefix.aquadem.azurecr.io)

Status: Enabled Enforcement Mode: Audit Enforce

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

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

File Block
Prevent containers from reading, writing, or executing the files listed below:

Enter file name: Add

Enable file blacklist

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.

Integrations

Image Registries

Serverless Applications

Log Management

Monitoring Systems

Secret Key Stores

LDAP Authentication

SSO Authentication

Notification Feed

Qualys Integration

Service Fabric Integration

Create New Key Store

* Key Store Name

Provide secrets store integrations (e.g, CyberArk, Hashicorp, AWS KMS, Azure Vault)

Key Store Name

* Key Store Type

Select Key Store Type...

Azure Key Vault (Secrets)

Azure Key Vault (Keys)

Amazon Key Management Store

HashiCorp Vault

HashiCorp Vault V2

CyberArk Enterprise Password Vault

Cyberark Conjur

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.

Filter container view by image package, security issues (privileged, root, vulnerabilities), hosts, status, and uptime

Container Name*	Host	Security Issues	Image Runtime Profile	Uptime
jenkins-4.5	local-dev-agent.demo896-vm0	Image Unregistered	None	48 Minutes
k8s_app-server_app-server-d777d9969-5c7n4_website_dbbea8...	local-agent.demo896-vm1	2 41 72 23 3	None	27 Minutes
k8s_app-server_web-server-5b04d94474-5q6dt_website_dbc82...	local-agent.demo896-vm1	2 2 25 14 23	None	27 Minutes
k8s_carts_db_carts-db-6c3b649b49-kbz7l_sock-shop_ef77762cf...	local-agent.demo896-vm1	0 0 2 14 3	None	26 Minutes
k8s_carts_carts-6df0cd59f8-kzms_sock-shop_ef7c791e-f896-1...	local-agent.demo896-vm1	10 32 33 19	None	26 Minutes
k8s_catalogue-db_catalogue-db-b6948db75-qvztd_sock-shop...	local-agent.demo896-vm1	0 0 5 11 15	None	27 Minutes
k8s_catalogue_catalogue-7d7f9f87f-mk7cj_sock-shop_001539...	local-agent.demo896-vm1	0 3 12 15	None	26 Minutes
k8s_coredns_coredns-79f0cf6894-v6cm9_kube-system_e76e0c...	local-dev-agent.demo896-vm0	0 1 1 228 10	None	49 Minutes
k8s_coredns_coredns-79f0cf6894-vm9n6_kube-system_e774f1...	local-dev-agent.demo896-vm0	0 1 1 228 10	None	49 Minutes
k8s_etcd_etcd-demo896-vm0_kube-system_236ede55d071dc...	local-dev-agent.demo896-vm0	0 0 0 1 4	None	50 Minutes

Review container security issue indicators

Apply least-privilege security profiles out of the box to popular images

Monitor container uptime

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)

Runtime Policies > PCI DSS (container policy)

Controls to check compliance with PCI DSS security requirements for containers

* Scope

Aqua

Host Logical Name

value

Add

container.name.*

Status

Disabled

Enforcement Mode

Audit

Enforce

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

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

Fork Guard

Prevent fork bombs in the container. In this control, you set the limit for any one process.

✓ Enable fork bomb protection

Process Limit

- 2 +

Port Scanning Detection

Audit Only

Linux Only

Enable port scanning inside containers.

✓ Enable port scanning detection

IP Reputation

Detect and prevent communication from containers to IP addresses known to have a bad reputation.

✓ Enable IP reputation security

Limit Container Privileges

Linux Only

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"."kubernetes-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 running 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

Enforce a 'least privilege' default even in no defined policies are in place, restricting containers' admin access only to their owners

Commands Assignment

Command Type

- Docker
- Network
- Node
- Secret
- Service
- System
- Swarm

Commands

- 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

Define users access privileges according to role, allowing/preventing specific actions such as view, run, stop, view logs and more

Control which resources user is allowed to access across the entire environment, even in multi-tenant setups

User Access Control > rule-admin-containers

* Name

Description

Accessors

Accessor	Accessor Value
<input type="text" value="Select"/>	<input type="text" value="Select"/> + Add
Users	<input type="text" value="root"/> <input type="text" value="NT AUTHORITY\SYSTEM"/>
Groups	<input type="text" value="Administrators"/> <input type="text" value="vcap"/>

Role

* Role

Resources

Resource	Resource Name
<input type="text" value="Select"/>	<input type="text" value="Select"/> + Add
<input type="text" value="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

Functions > myConcurrencyConfig

Risk Vulnerabilities Resources Sensitive Data Activity Trends Permissions Information

Function Is Non-Compliant
Function scanned on 2019-10-27 10:41 AM

Assurance Policy
Policy: Default Failed

Function Scan Partial	CVE Blacklist Passed	Excessive Permissions Passed	Function Integrity Passed	Vulnerability Score Failed	Vulnerability Severity Failed	Sensitive Data Passed
---------------------------------------	--------------------------------------	--	---	--	---	---------------------------------------

Details
myConcurrencyConfig
Created 9 months ago

High Medium OK

Total: 2

Actions Needed

- Fix function vulnerabilities to reduce security issues
- Fix function vulnerabilities to reduce security issues

Detect secrets embedded in functions

Functions > awsAndSshKeys

Risk Vulnerabilities Resources **Sensitive Data** Activity Trends Permissions Information

AWS ACCESS KEY

File name	Full Path
lambda_function.py	/lambda_function.py

AWS SECRET KEY

File name	Full Path
lambda_function.py	/lambda_function.py

RSA PRIVATE KEY

File name	Full Path
lambda_function.py	/lambda_function.py

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 Kubernetes 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

Audit

230 Alert 7 Block 59 Detect 266 Success 562 All Audit Type All Time Interval All More Filters User Search...

Event	Audit Type	Status	Time
Host local-agent.demo896-vm1 is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:28 AM
Function arn:aws:lambda:us-east-2:934027998561:function:Test is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:28 AM
Function arn:aws:lambda:us-east-2:934027998561:function:myConcurrencyConfig is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:28 AM
Image jboss/base:latest is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image weaveworksdemos/shipping:0.4.8 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image etcd-amd64:3.2.18 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image weaveworksdemos/catalogue:0.3.5 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image registry.aquasec.com/enforcer:4.5.19296 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image kube-apiserver-amd64:v1.11.10 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image kube-scheduler-amd64:v1.11.10 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image orders-apache:1.0 is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image postgres:9.5 is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image weaveworksdemo-cataloguedb:1.0 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image mysql:8.0.0 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image quay.io/coreos/flannel:v0.11.0-amd64 is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image struts-attacker:1.0 is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image registry.aquasec.com/scanner:4.5.19296 is non-compliant due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM
Image jboss/wildfly:10.0.0.Final is non-compliant; container(s) already running due to policy Default	Alert	Alert	Oct 27, 2019 11:09 AM

Total 230 50/page < 1 2 3 4 5 >

Entity:
Host
Image:
local-agent.demo896-vm1
Action taken:
Host is marked as non-compliant
Policy:
Default
Failed controls:
Custom Compliance Checks
Aqua Response
Alert
Time Stamp
Oct 27, 2019 11:28 AM

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

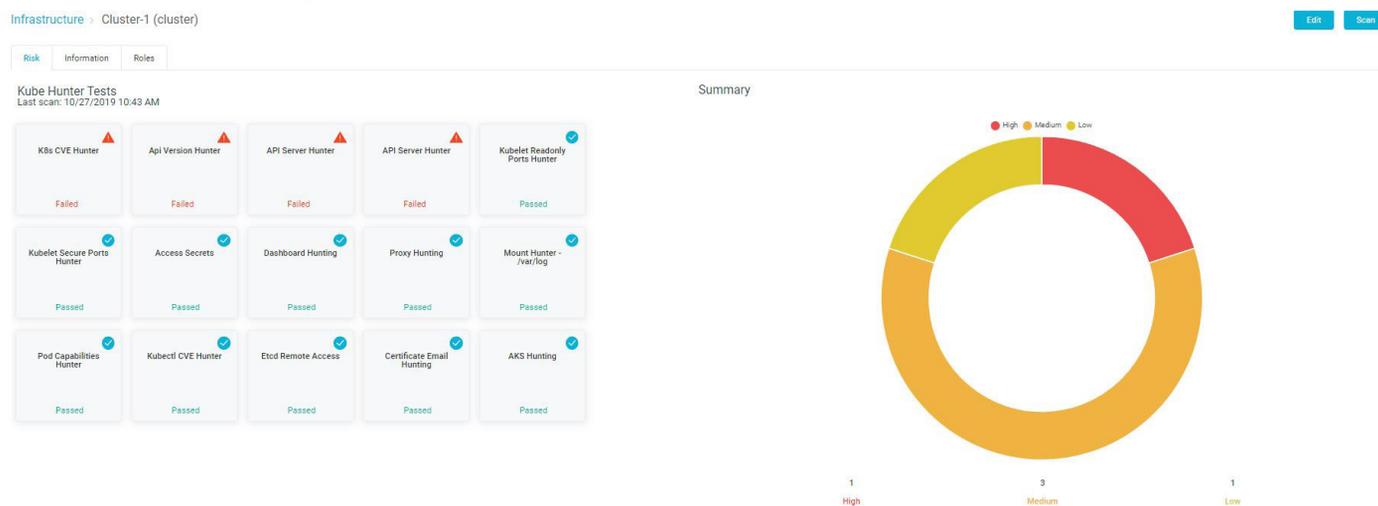
Hardening the Host and Orchestrator Environment

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
(Docker, K8s & Linux)

Latest Compliance Results

Last scan time: 2019-10-27 | 11:33:07 AM [Scan Now](#)

		25	56	24	0
		Failures	Warnings	Passes	Info
▼ Docker CIS Benchmark Totals					
> 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		11	2	12	0
		Failures	Warnings	Passes	Info
> 2.1. Kubelet		9	1	5	0
> 2.2. Configuration Files		2	1	7	0
▼ Custom Check Totals - custom-benchmark.yaml (Default)		0	1	2	0
		Failures	Warnings	Passes	Info
> 1. Host Configuration		0	1	2	0
▼ Linux CIS Benchmark Totals		98	140	81	0
		Failures	Warnings	Passes	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 with Aqua's VM Enforcer.

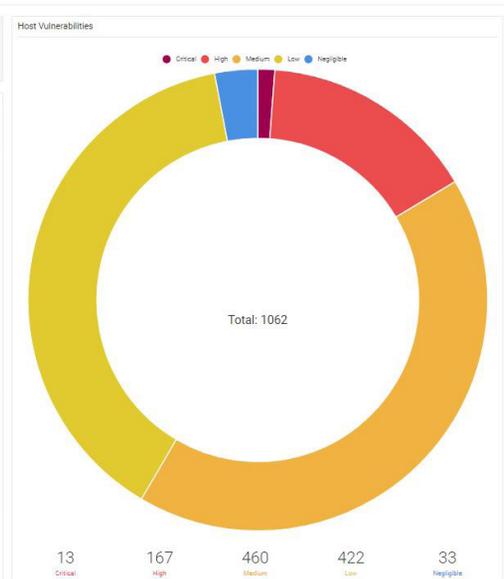
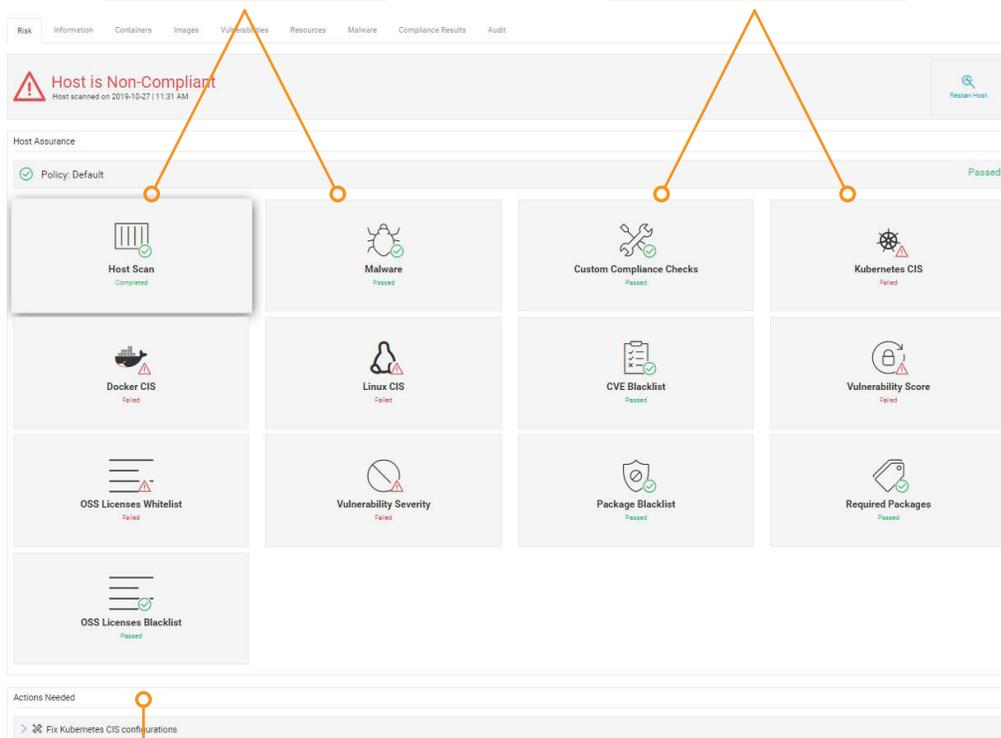
- Prevents access to the host by specified users and/or groups of users
- Audits user activity on the host VM
- Monitors files, file attributes and directories on your hosts for read, write, and modify operations
- Scans hosts for known vulnerabilities
- Applies runtime policies to ensure host immutability
- 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

Cloud metadata service

Allow

Deny

* Port Range

e.g. '80','0-65535'

* Destination

Select

* IP Address

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

Defines network policies to enforce inbound/outbound communication for your workloads

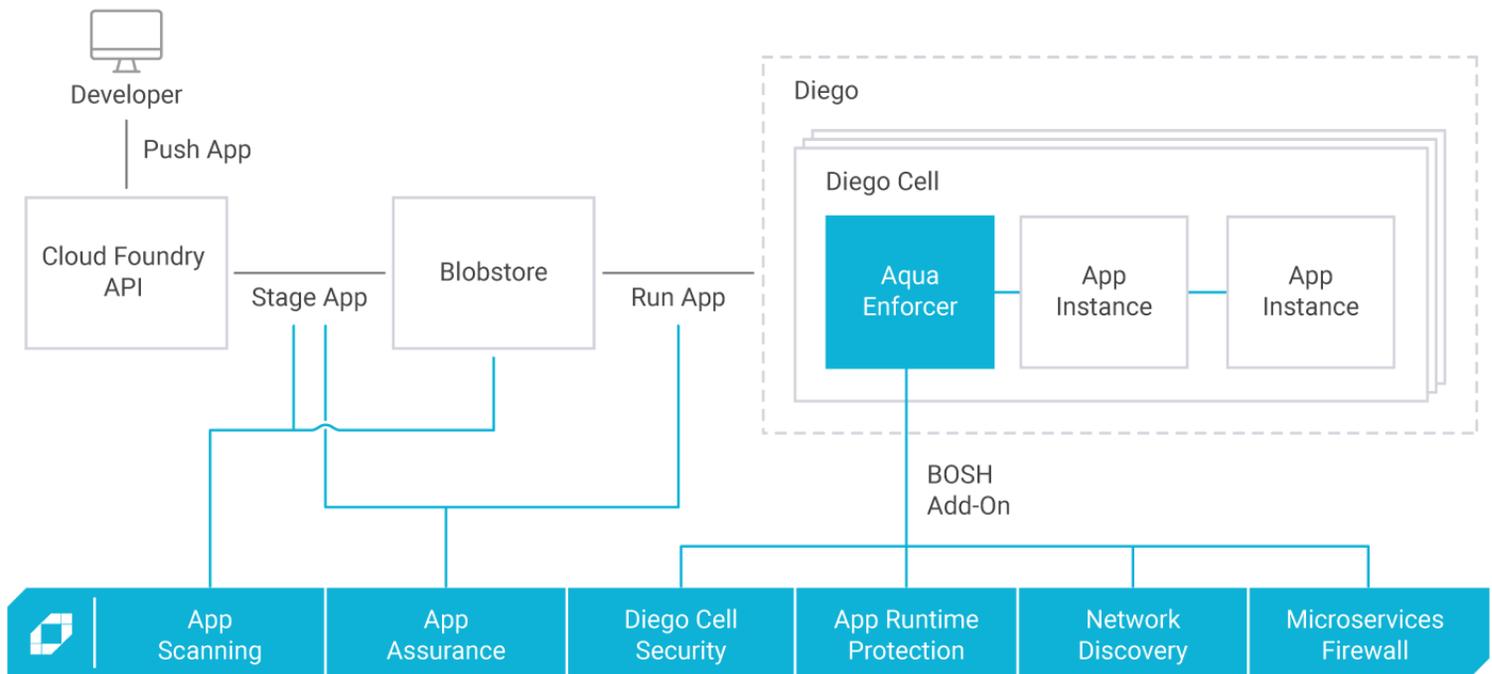
A Full Lifecycle Security Solution for Pivotal Application Service (PAS) Containers

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.



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

```
bash-3.2$ trivy knqyf263/test-image:1.2.3
2019-05-13T15:19:03.912+0900 INFO Updating vulnerability database...
2019-05-13T15:19:05.983+0900 INFO Detecting Alpine vulnerabilities...
2019-05-13T15:19:05.987+0900 INFO Updating npm Security DB...
2019-05-13T15:19:07.048+0900 INFO Detecting npm vulnerabilities...
2019-05-13T15:19:07.048+0900 INFO Updating pipenv Security DB...
2019-05-13T15:19:08.507+0900 INFO Detecting pipenv vulnerabilities...
2019-05-13T15:19:08.508+0900 INFO Updating bundler Security DB...
2019-05-13T15:19:09.574+0900 INFO Detecting bundler vulnerabilities...
2019-05-13T15:19:09.575+0900 INFO Updating cargo Security DB...
2019-05-13T15:19:10.441+0900 INFO Detecting cargo vulnerabilities...
2019-05-13T15:19:10.441+0900 INFO Updating composer Security DB...
2019-05-13T15:19:11.649+0900 INFO Detecting composer vulnerabilities...

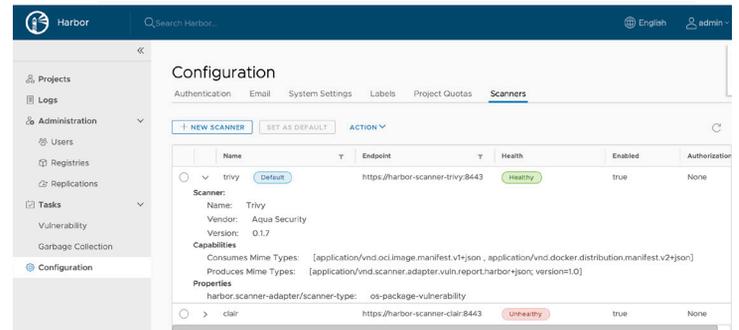
knqyf263/test-image:1.2.3 (alpine 3.7.1)
-----
Total: 26 (UNKNOWN: 0, Low: 3, MEDIUM: 16, HIGH: 5, CRITICAL: 2)
-----
+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| curl    | CVE-2018-14618   | CRITICAL | 7.61.0-r0         | 7.61.1-r0     | curl: NTLM password overflow |
|         | CVE-2018-16839   | HIGH     |                   | 7.61.1-r1     | curl: Integer overflow leading |
|         | CVE-2019-3822    |          |                   | 7.61.1-r2     | curl: NTLMv2 type-3 header |
|         | CVE-2018-16840   |          |                   | 7.61.1-r1     | curl: Use-after-free when |
|         | CVE-2018-16890   | MEDIUM  |                   | 7.61.1-r2     | curl: NTLM type-2 heap |
|         | CVE-2019-3823    |          |                   |                | curl: SMTP end-of-response |
|         | CVE-2018-16842   |          |                   | 7.61.1-r1     | curl: Heap-based buffer |
| git     | CVE-2018-19486   | HIGH     | 2.15.2-r0        | 2.15.3-r0     | git: Improper handling of |
+-----+-----+-----+-----+-----+-----+
```

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 operations 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	KBs 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

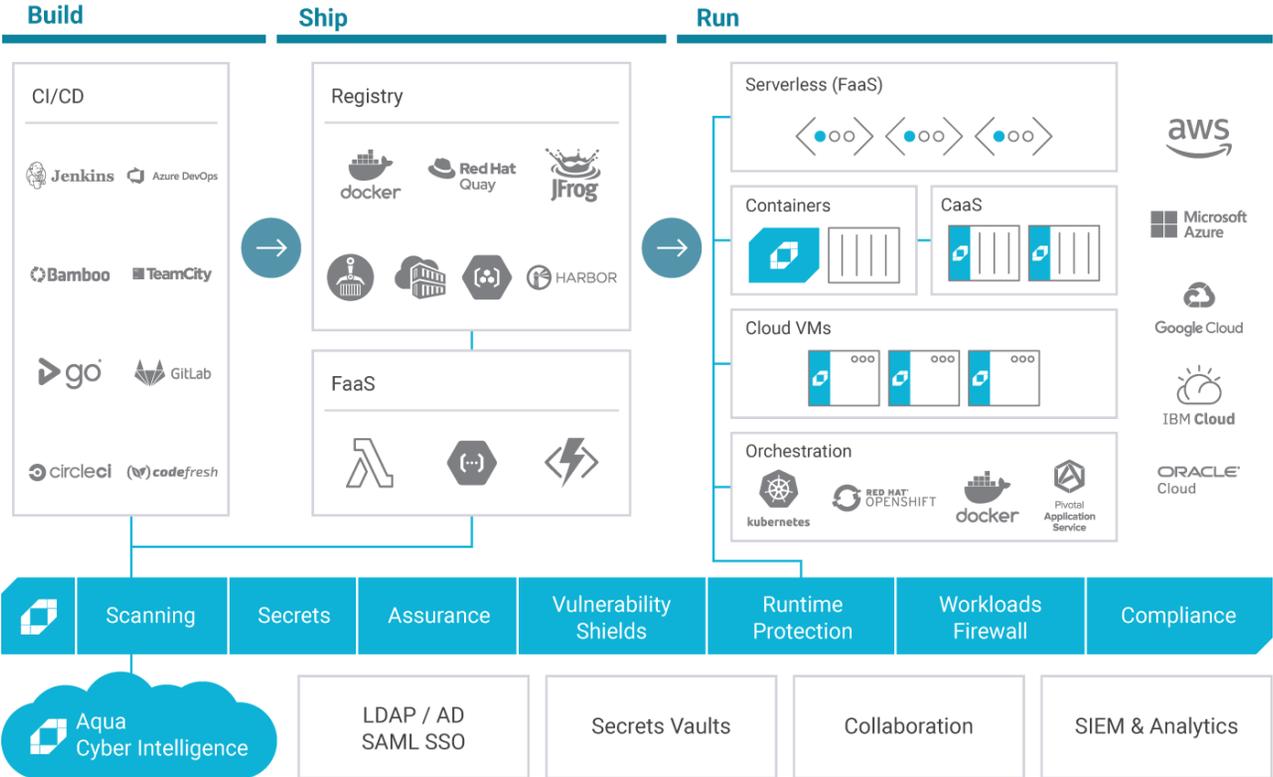
The only solution that provides real, automated security without sacrificing business continuity. We offer granular blocking that only prevents suspicious actions without stopping the application, and secrets rotation, with no container restart.



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

