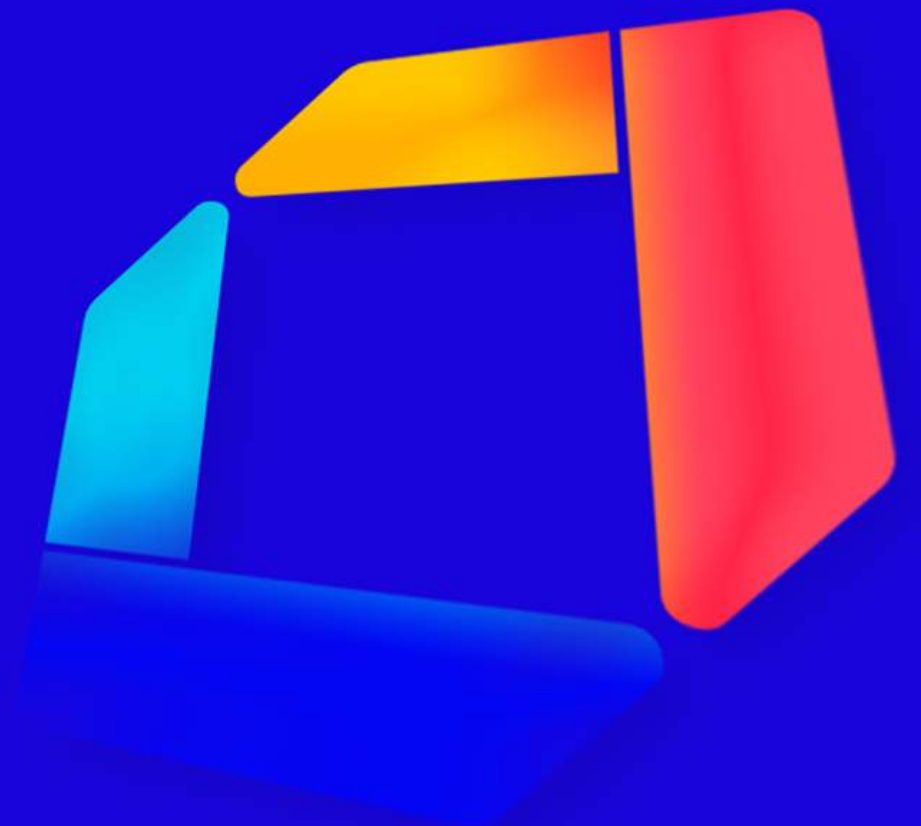




Securing the Build, Infrastructure, and Workloads Across Cloud Native Environments

An illustrated guide to cloud native security with Aqua



The Value of Cloud Native Security

Aqua Security helps organizations to minimize their security risk exposure and enforce compliance across their cloud native application lifecycle and infrastructure. Aqua's solutions empower security, operations, and DevOps teams to facilitate best practices without impeding established workflows. Aqua provides comprehensive controls and deep, actionable insight to accurately detect and prioritize risks and to accelerate remediation.

Aqua can be delivered as a SaaS-based or on-prem solution, designed to address security and operational requirements of any cloud native maturity and can be tailored for organizations of any size. Aqua functions across all platforms and clouds (public, private, and multi-cloud scenarios), and helps to secure containers, virtual machines (VMs), and serverless functions.

Aqua's core capabilities are part of a unique three-pronged approach to cloud native security, aligned to the industry's premier standard for minimizing risk in applications across modern cloud ecosystems.

The Aqua Approach

Secure the Build



Prevention First

- Help developers address issues earlier in fast-moving pipelines of code artifacts
- Shift security left: Analyze images/functions and remediate risks during the build
- Create and automatically enforce policies to ensure security before deployment

Secure the Infrastructure



Harden the Environment

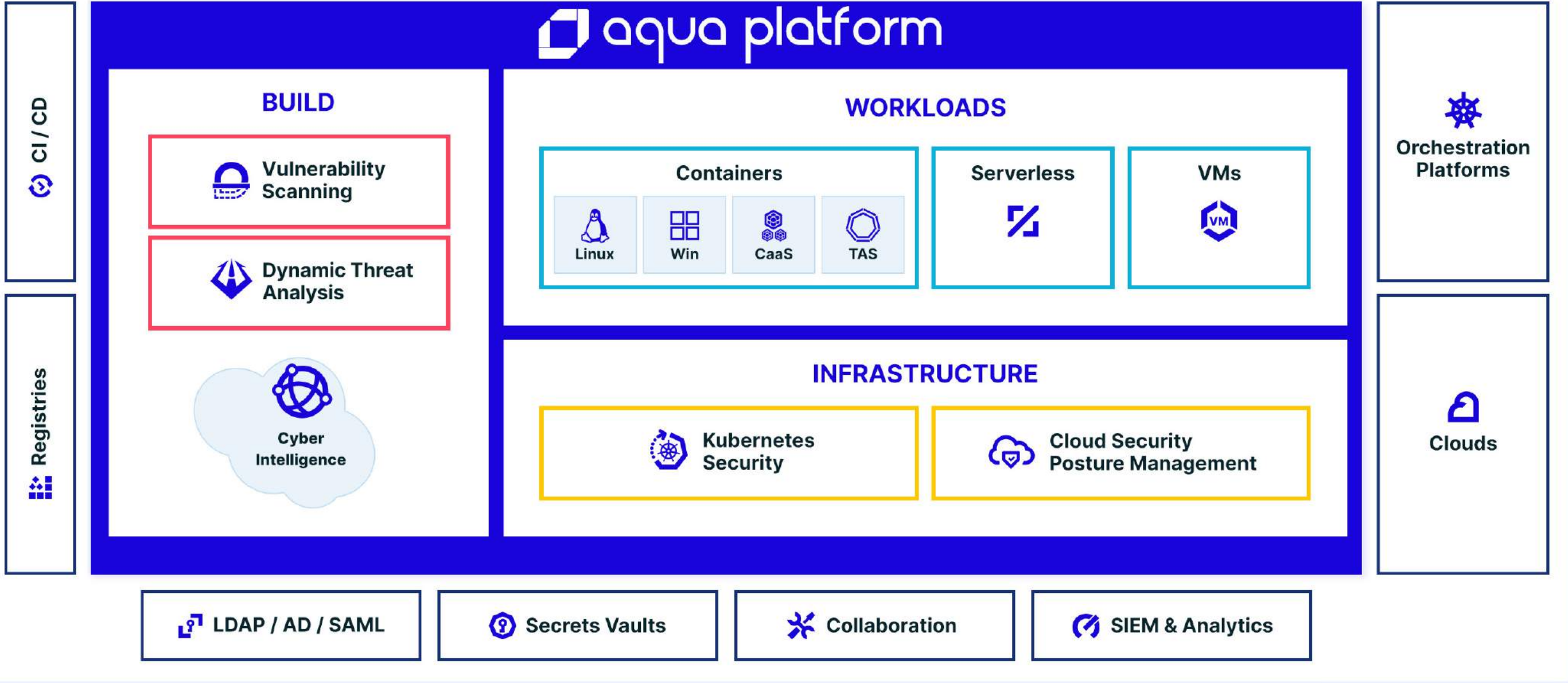
- Leverage a single pane of glass to manage your cloud security posture
- Automate compliance for public cloud and Kubernetes infrastructure
- Apply consistent controls on any orchestration platform and across cloud providers

Secure the Workload



Protect Runtime Workloads

- Ensure immutability and least-privilege enforcement of behaviors
- View running workloads, namespaces, and risks for root cause investigation
- Visualize workload network connections and prevent unauthorized connections



Prioritize Threats in Running Workloads in Real Time

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

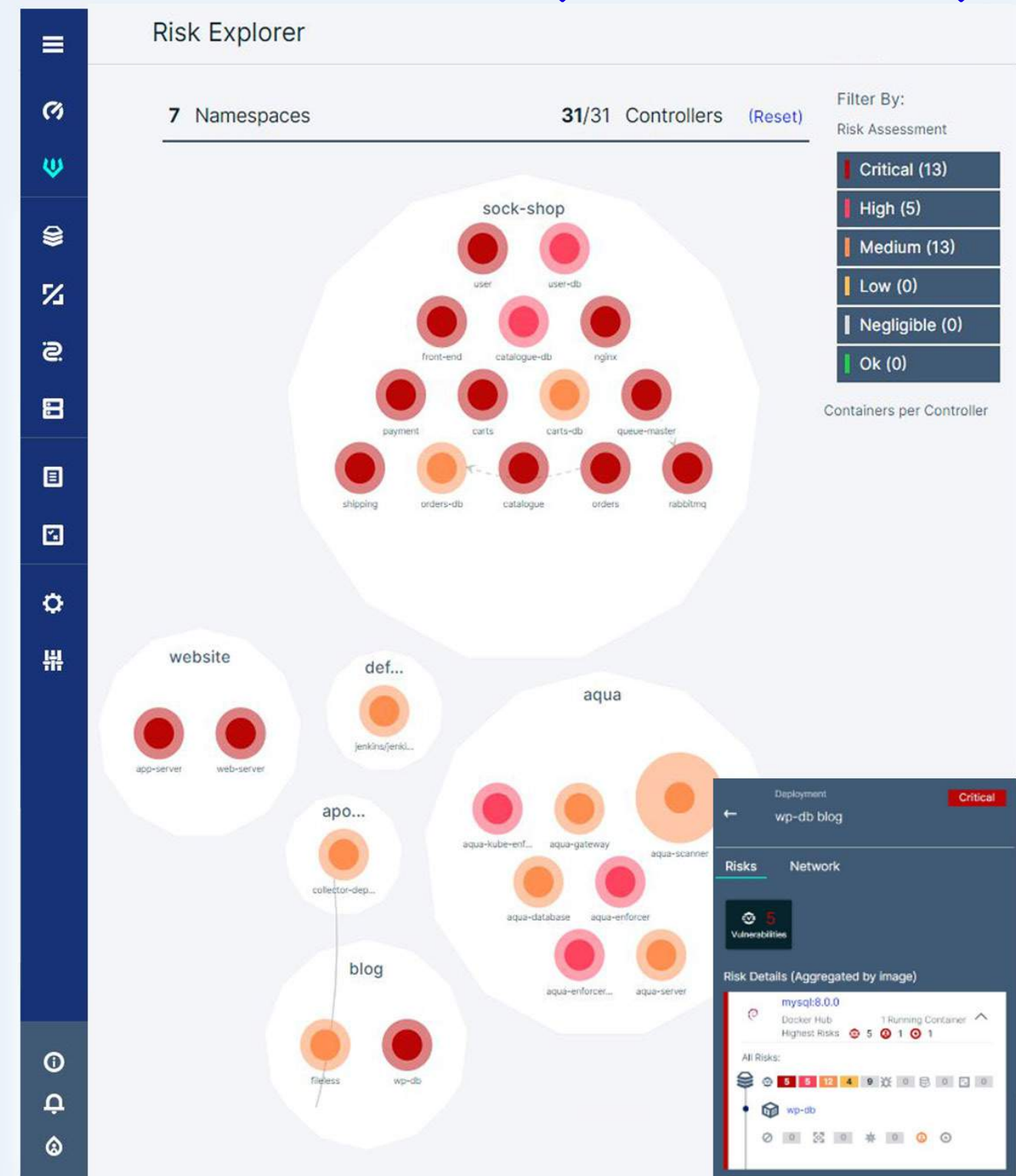
Are you able to make quick decisions and mitigate the most critical risks at the right time?

Aqua Risk Explorer simplifies security risk management in large production environments where security risk assessments often present unwieldy amounts of results without effective prioritization. Aqua Risk Explorer provides a dynamic, real-time, logical view of running workloads in Kubernetes environments and associated security risk insights. This helps DevSecOps teams to identify the most vulnerable deployments and nodes and to prioritize remediation efforts.

- Help security teams save time by viewing a live map of all running workloads, focus on the high-risk items, and take steps to improve security
- View detailed risk information on a selected item and all the components that are associated with it, including the reasons for its risk classification
- Drill down into namespaces, deployments, nodes (hosts), containers and their originating images, as well as network connections between, and within, namespaces
- View risks associated with vulnerabilities, embedded secrets, bad configurations or policy violations, and malware
- Support regulatory compliance initiatives, such as PCI-DSS requirements 6 & 10

Gain insight into clusters, namespaces, deployments, nodes, containers, and images

Filter view based on risk severity



Drill down into risks at the container & node/ host level (e.g., vulnerabilities, exposed secrets, bad configs, malware)

Shift-Left Security Scanning for DevOps

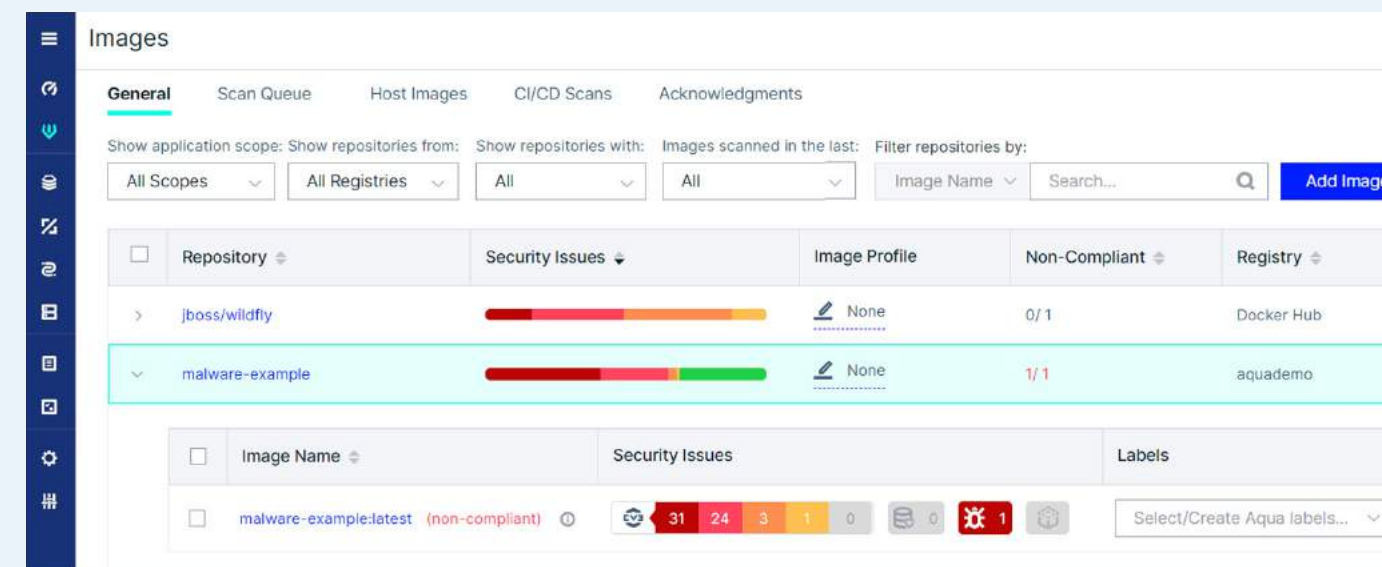
Can you automate image scanning for vulnerabilities, secrets, and configuration errors across CI/CD pipelines, in function stores, and in registries?

Do you have access to actionable risk insight in CI environments to accelerate remediation?

Aqua helps to “shift security left,” scanning directly within the CI/CD pipeline, function stores, and image registries to provide complete risk analysis and to facilitate rapid remediation before the build.

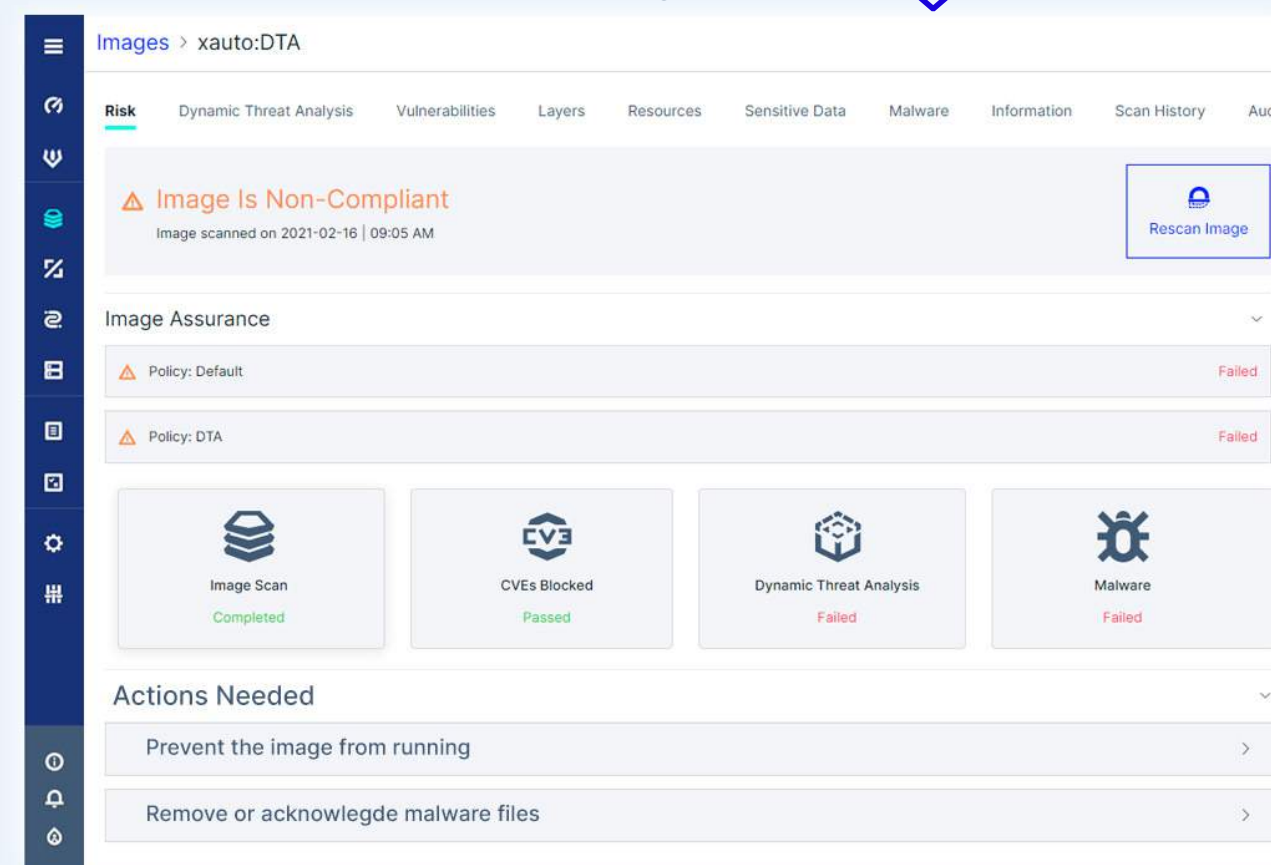
- Scan VM images, container images, and serverless functions
- Detect and identify known vulnerabilities, hidden malware, embedded secrets, open source license issues, configuration errors, and over-provisioned permissions
- Configure automated, scheduled scans at regular intervals to detect emergent vulnerabilities
- Identify and analyze OS packages (RPM and deb) and 40+ language packages (e.g., Java, NodeJS, Ruby, PHP, Python, C/C++)
- Generate an image bill of materials, detailing packages, files, OSS license information, and layer history
- Leverage the Aqua CyberCenter data feed, which is curated and refined to provide accurate detection and analysis of CVEs, vendor-issued advisories, proprietary Aqua cybersecurity research, and malware
- Focus on the most urgent security issues first using Aqua’s risk-based insights (discussed further in the next section)
- Use Aqua’s flexible assurance policies to set risk thresholds that flag artifacts as non-compliant and prevent their progression through the pipeline to production (discussed further in later sections)

Quickly filter all image scans by application, registry, risk type, and scan recency, or search for specific images



View at-a-glance summary of risk (vulnerabilities, malware, embedded secrets, OSS licenses, configuration errors, permissions)

Easily view policies which the scanned image has violated



Quickly identify necessary actions to achieve policy compliance or remediate risks

Intelligently Prioritize and Remediate Vulnerabilities

Can you easily identify the greatest risks from a lengthy list of identified vulnerabilities?

Do you have visibility into vulnerability severity metrics, exploits, and impacted running workloads from one location?

Only Aqua's risk-based insights enable teams to invest time and effort efficiently, where their activities can have the most impact, and to effectively scale existing resources to address the remediation requirements of large deployments. Risk-based insights automatically consider risk-related contextual factors to generate a complete list of vulnerabilities that can be narrowed down and refined based on factors like exploitability, severity, and whether the workloads are running, helping to clearly prioritize vulnerabilities for remediation.

- Refine vulnerability scan results to manage remediation priorities and scale efforts effectively
- Easily prioritize vulnerabilities present in actively used packages
- Mitigate vulnerabilities with ready access to vendor fixes (when available) or using Aqua's proprietary vShield technology (discussed further in the next section)

Identify running workloads with the associated vulnerability



Vulnerabilities (4,214)

Risk-based Insights
Filter vulnerabilities by the context of their environment and risk factors

IMPORTANT ——— Medium to Critical (2.96 K) ——— Network Attack Vector (2.99 K) ——— Available Exploit (243) ——— Remote Exploit (124) ——— Exploitable Workloads (57) ——— IMPORTANT & URGENT

Filtered by: Vulnerabilities with an exploit, and present in running workloads

Vulnerability	Image	Severity	Workloads	Resource	Exploit Availability	Vendor Fix	vShield Status	Acknowledgement
CVE-2014-7186	nginx:1.7.1	Critical	2	bash	✓	✓	vShield	Acknowledge
CVE-2014-6277	nginx:1.7.1	Critical	2	bash	✓	✓	vShield	Acknowledge
CVE-2017-12629	jboss/wildfly:10.0.0	Critical	1	lucene-core	✓	✓		Acknowledge
CVE-2020-1938	artifactdemo:1.2.2	Critical	2	tomcat-embed-core	✓	✓		Acknowledge
CVE-2014-7169	nginx:1.7.1	Critical	2	bash	✓	✓	vShield	Acknowledge

Triage results based on risk-related factors



CVE-2014-7186
nginx:1.7.1 (aquademo)

CRITICAL NVD Based on NVD CVSSv2 10.0

Exploit Available Workloads Running

The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue. [see less](#)

Installed Resource	bash 4.3-7
Fixed Version	4.3-9.2
Published by NVD	2014-09-28
CVSS Score	NVD CVSSv2 10.0

Exploit Details

Type	Remote
------	--------

Apply Aqua's vShield to mitigate vulnerabilities without a fix or until a fix can be applied

View detailed vulnerability insight and remediation guidance, sourced and curated by the Aqua cybersecurity research team

Mitigate Known Vulnerabilities in Container Images

How do you protect vulnerable components against potential exploit when no fix is available?

Can you attest to compensating controls that mitigate specific vulnerabilities for compliance?

Aqua Vulnerability Shield (vShield) provides a compensating control for known vulnerabilities detected in container images when a patch or vendor fix is unavailable. Aqua vShield leverages Aqua's proprietary 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.

- Maintain business continuity by virtually patching running workloads, ensuring that mission-critical applications are not impacted
- Avoid interruption to developer workflows with non-intrusive vShields that do not change the image code
- Generate vShields to protect against newly discovered vulnerabilities
- Protect against multiple attack vectors that target networks, file systems, packages, and executables
- Enable compliance teams to demonstrate compensating controls for high-risk vulnerabilities
- Automatically notify security teams of exploit attempts and block the exploit

Define the scope for which a vShield will be applied



Receive notifications of risk in Audit mode, or automatically apply virtual patching in Enforce mode



The screenshot shows the Aqua vShield configuration page. At the top, it displays the policy name 'AGP_CVE-2014-7186_nginx:1.7.1' and its description 'Auto generated vShield- nginx:1.7.1 Policy'. The scope is set to 'Global'. Under 'Additional Scope Criteria', there is a table with columns for 'Aqua', 'Enforcer Group', and 'name'. A single criterion is listed: 'container.image.aquademo.azurecr.io/nginx:1.7.1'. The enforcement mode is currently set to 'Audit', and the status is 'Enabled'. A 'Set Scheduler' button is visible. A modal window titled 'Enforce mode Change' is open, showing a 'Change to enforce mode (in days):' field set to '1' and 'Days' as the unit. Below the main configuration, there are 'Controls' for 'Block Container Exec', 'Block Non-Compliant Images', and 'Block Non-Compliant Workloads'. A 'Package Block' section is also visible, with 'Linux Only' selected and 'Enable Package Block control' checked.



Clearly define actions to be taken when a vShield is invoked



Configure a schedule that establishes a period of Audit before Enforcement

Dynamically Detect Hidden Malware Before Deployment

Can you detect hidden, polymorphic malware in your pipeline?

Can you safely trace and categorize the steps of an attack kill chain?

Increasingly sophisticated attacks in the wild use evasion techniques that poison the cloud native supply chain with malware that is undetectable using signatures or static scanning methods. Only Aqua's Dynamic Threat Analysis (DTA) ensures that those advanced threats and malware in container images are detected before they are pushed to production. Aqua DTA helps to mitigate the risk of data theft, container use for DDoS, and resource abuse by advanced persistent threats and polymorphic malware.

- Run and test images in a secure, pre-production sandbox environment to identify hidden and sophisticated risks
- Analyze container behavior directly from your registries and CI pipelines and help incident response to "shift left"
- Identify indicators of compromise (IOCs) like container escapes, reverse shell backdoors, malware drops, cryptocurrency miners, code injection, and network anomalies
- Map communications between containers and external destinations, including file downloads, C&C servers, and data exfiltration destinations
- Trace and visualize key activities in the kill chain to understand attacks before they happen
- Support SecOps and forensics by automatically classifying detected behaviors by the MITRE ATT@CK framework

Identify malicious or suspicious behaviors, including weaponization, propagation, communications, and data collection and exfiltration

Images > xauto:DTA

Risk **Dynamic Threat Analysis** Vulnerabilities Layers Resources Sensitive Data Malware Information Scan History Audit

Behaviors and Findings

Initial Execution	Weaponization	Propagation	Communication	Collection & Exfiltration
0	9	4	7	2

- Systemd service (which manages background daemon processes) used during runtime
- Attempt by the container to fingerprint the host detected during runtime
- Network utility used to fetch remote resources during runtime
- fingerprinting binary was executed during runtime
- Encoding function (base64) detected during runtime
- Secure Shell (SSH) protocol used during runtime
- CPU fingerprint detected during runtime

View a detailed, step-by-step breakdown of the attack kill chain

Network Activity

13 outbound connections detected

Destination address	Country
104.82.6.133	US
104.82.7.122	US
127.57.65.153	United States
104.82.6.133	Switzerland
185.612.312.32	Norway

Quickly detect and trace network activity and identify anomalous communications

Securely Deliver and Rotate Secrets

Can you securely deliver secrets from a central vault to the containers that need them?

Can you rotate secrets with no downtime or restart to the running container?

Can you ensure that secrets are not visible on the host, orchestrator, or network?

Aqua helps to ensure the security of your secrets to protect sensitive data and intellectual property and to avoid tampering. 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, all managed by using your existing enterprise secrets vaults.

- Centralize control of secrets and the way containers access them
- Deliver secrets securely across environments and encrypt secrets in transit
- Accomplish secrets injection and rotation in runtime with no container downtime
- Manage and monitor container secrets activity
- Manage secrets seamlessly using AWS KMS, HashiCorp Vault, Azure Key Vault, and CyberArk Application Access Manager and Enterprise Password Vault



Integrations > Secret Key Stores

Image Registries

Serverless Applications

Log Management

Monitoring Systems

Secret Key Stores

LDAP Authentication

SSO Authentication

Notification Feed

Qualys

Service Fabric

Apolicy

Create New Secret Key Store

* Key Store Name

* 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

Configure and Enforce Assurance Policies

Can you ensure that only trusted artifacts run in your environments?

Can you unify policies across platforms and tools?

Aqua assurance policies help to verify that the artifacts (images, functions, VMs, Kubernetes pods) that run within your environments are trusted per your compliance and security standards and ensure that a workload does not pass a threshold for risk tolerance. Assurance policies provide persistent controls to ensure artifact integrity throughout the full lifecycle and to prevent unapproved or unvetted artifacts from running.

- Define and automatically enforce the conditions an artifact must meet to run, applicable to images, functions, VMs, and Kubernetes pods
- Ensure that only the latest, authorized artifacts are being instantiated across your IT environments
- Prevent image tampering, spoofing, and control promotion from staging into production
- Identify and flag artifacts that cannot be traced back to approved images
- Prevent the execution of untrusted or risky functions, such as those that have unused roles, over-provisioned permissions, high-risk CVEs, or that contain sensitive data
- Apply advanced application scoping to manage policies and establish scope across clusters, labels, registries, and more
- Enforce assurance policies across multiple orchestration tools (e.g., Kubernetes, OpenShift, DC/OS, and Tanzu)
- Establish policy-driven security gates to enforce best practices on Kubernetes, compatible with Open Policy Agent (OPA) using Rego expressions to add out-of-the-box and custom rules to support your own distinct security requirements

Select desired actions when an artifact violates a policy



Balance risk and efficiency with policy applicability scope criteria (e.g., image name, label, registry)



The screenshot shows the configuration interface for an Aqua-Demo image policy. It includes fields for Policy Name (Aqua-Demo), Description (Images pulled from aquademo registry), and Scope (Global). Under the Actions section, three options are checked: 'Create an audit message when an image fails this policy', 'Fail the Aqua step in CI/CD', and 'Mark failed images as non-compliant'. The Exceptions section includes options to ignore vulnerabilities based on availability of fixes, publication date (set to 30 days), specific vulnerabilities, or specific paths.



Easily define exception criteria to policy violations

The screenshot shows the configuration for a 'Vulnerability Score' control. It lists several control types: Approved Base Image, Custom Compliance Checks, CVEs Blocked, and Dynamic Threat Analysis. The Vulnerability Score control is enabled, and a slider is set to a score of 8, which is labeled as 'high'.



Select and customize dozens of controls to refine precise policies (e.g., Vulnerability Score)

Protect Workloads in Runtime – Controls

Do you have full visibility into workload behavior in runtime and an ability to detect suspicious activities?

Can you establish granular policies that create a zero-trust “safe zone” for how workloads behave, limiting privileges, access to resources, and behaviors?

Can you enforce consistent runtime policies across the entire cloud native spectrum (VMs, containers, and functions)?

Aqua enables you to configure runtime controls that are applicable to all containers, functions, and VMs, permitting only legitimate behaviors and preventing several types of privilege abuse, suspicious behaviors, and attack vectors. Get alerted to configuration violations and view detailed remediation steps.

- Set policies scoped by workload profile (defining preapproved image actions) or runtime profiles (defining general runtime characteristics, privilege management, etc.) to create zero-trust zones for specific applications, VMs, or cloud environments and requirements
- Enforce policy changes or stop unauthorized processes with no downtime to running workloads
- Support containers running on Linux and Windows hosts, multiple flavors of Kubernetes, and container-as-a-service environments (e.g., AWS Fargate, ACI)
- Implement file integrity monitoring, system integrity monitoring, user activity monitoring, and other runtime protection controls to ensure VMs are properly hardened
- Leverage a set of pre-defined runtime policies based on security standards such as NIST, CIS, PCI, and HIPAA, or customize runtime policies to specific runtime environments (e.g., per namespace or cluster)

Quickly locate and review policy details at a glance



Easily add and customize a new policy



Name	Workload Type	Description	Status	Enforcement Mode	Application Scopes
Aqua default runtime policy	Container	The default Aqua runtime policy	Enabled	Audit Only	Global
Block Non-compliant Images	Container	Block images that are marked as non-compliant images	Disabled	Enforce	Global
Block Unregistered Images	Container	Block images that are not registered in the Aqua server	Disabled	Enforce	Global
CIS	Container	Controls to check compliance with CIS security guidelines for containers	Disabled	Enforce	Global
Demo Cluster	Container	Runtime policies for demo cluster	Enabled	Enforce	Global
HIPAA	Container	Controls to check compliance with HIPAA security requirements for containers	Disabled	Enforce	Global
NIST	Container	Controls to check compliance with NIST security guidelines for containers	Disabled	Enforce	Global
PCI DSS	Container	Controls to check compliance with PCI DSS security requirements for containers	Disabled	Enforce	Global
Aqua default function runtime policy	Function	The default Aqua function runtime policy	Enabled	Audit Only	Global
LambdaBlock	Function		Enabled	Enforce	Global
Aqua default host runtime policy	Host	The default Aqua host runtime policy	Enabled	Audit Only	Global



View all container, function, and VM policies



View a policy’s active status and whether it will audit or take enforcement actions upon violation

Protect Workloads in Runtime – Enforce Immutability

Can you ensure that currently running workloads are identical to their originating images or artifacts?

Can you stop zero-day attacks by preventing code injection and unauthorized changes to running workloads?

Aqua enables you to ensure workload integrity and immutability (image, host, function) without sacrificing application performance and availability. Detect and prevent any change to running workloads, as compared to their originating images or artifacts, and leverage Aqua's proprietary Drift Prevention feature to prevent any attempt to alter workloads in runtime (e.g., adding new executables or files).

- Enforce immutability and ensure that updates are pushed only through the CI/CD pipeline, with no patching or changes allowed in runtime
- Protect Linux and Windows machines against drift and tampering by enforcing immutability of VM configurations
- Create cryptographic image fingerprinting for all layers within the image to ensure image integrity
- Detect and block attempts to add components or inject code into running workloads, preventing drift from the originally trusted images or artifacts

Customize enforcement actions to be taken upon policy violation



Prevent running containers from obtaining new privileges not originally provisioned



Runtime Policies > Aqua default runtime policy (container policy)

Select Enforcer Type

- + Block Container Exec
- + Block Non-Compliant Images
- + Block Non-Compliant Workloads
- + Block Unregistered Images
- + Bypass Scope
- + Capabilities Block
- ✓ Drift Prevention
- + Executables Allowed
- + Executables Blocked
- + File Block
- + Forensics
- + Fork Guard
- + IP Reputation
- ✓ Limit Container Privileges
- + Limit New Privileges
- + Package Block
- + Port Block
- + Port Scanning Detection
- + Read-Only Directories And Files
- + Registries Allowed
- ✓ Volumes Blocked

Limit Container Privileges

Prevent containers from running with the privileges selected below:

Linux Only

- Access to host network
- Adding capabilities with --cap-add
- Configured with 'root' user
- Privileged containers
- Use the host IPC namespace
- Use the host PID namespace
- Use the host user namespace
- Use the host UTS namespace

Linux and Windows

- Port binding lower than 1024

Volumes Blocked Requires container restart

- Enable Volumes Blocked control

Prevent the following volumes from being mounted in containers:

Enter volume name

/ x /boot x /dev x /etc x /lib x /proc x /sys x /usr x /var/lib/docker x

Drift Prevention Linux only

Prevent executables that are not in the original image from running.

- Enable Drift Prevention Control



Prevent processes not in the original image, or images whose integrity has changed, from running

Identity-Based Workload Segmentation Across Environments

Can you control network traffic between various cloud native workloads, no matter where they run?

Can you easily identify legitimate network connections and implement contextual firewall rules to allow them as trusted connections?

Aqua enables you to limit the blast radius of attacks by controlling the communications between workloads in your cloud native environment and implementing identity-based segmentation based on the application context. Aqua automatically discovers network topology and suggests firewall rules that allow legitimate connections.

- Visualize network connectivity for cloud native workloads within, and across, clusters
- Define network connections based on orchestrator concepts (pod name, namespaces), IP/CIDR addresses, and DNS
- Permit legitimate connections based on service identity, URLs, or IPs
- Alert on or block unauthorized communication flows automatically or limit network traffic to a specific process within a container or host without experiencing downtime

Firewall Policies > Default Host Firewall Policy

* Name: Default Host Firewall 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

Define network policies for workload communications



Define the scope of the workload segmentation

Services > Edit Service: Database

Scope

* Select one or more application scope(s)

Global X

Additional Scope Criteria AND Remove

Aqua Enforcer Group name Add

Clear all

container.name.wp-db OR kubernetes.deployment.wp-db

Available operators are: AND, AND NOT, OR, OR NOT. You can use "()" for grouping.

Note: Attribute values cannot contain spaces.

Rules Priority (1-100): - 100 +

Firewall Policies

Select Add New Show Effective Rules

Name

Select firewall policies to be included in the segmentation

Securely Configure Public Cloud Services

Can you ensure your public cloud accounts are securely configured and in compliance?

Can you prioritize and fix configuration errors before they are exploited?

Can you automate these activities continuously and consistently across multiple clouds?

Aqua CSPM (cloud security posture management) delivers unprecedented control over your cloud security posture across public and multi-cloud ecosystems. Scan, monitor, and remediate configuration issues on AWS, Azure, Google Cloud, and Oracle Cloud. Aqua CSPM provides self-securing capabilities to ensure cloud accounts don't drift out of compliance, with risk alerts and detailed remediation guidance.

- Define policies to identify specific configurations to be automatically fixed if they drift out of compliance
- Verify and demonstrate compliance with PCI-DSS, HIPAA, Well-Architected Framework, GDPR, SOC 2, and custom requirements
- Gain real-time visibility into control-plane API calls and analyze events for security-sensitive changes or potentially malicious activity
- Leverage an extensible architecture, based on an open source core, that uses plugins for hundreds of individual checks that can be easily customized

Clearly identify configuration issues across clouds



Dashboard Try our new dashboard!

TOTAL SECURITY RISKS **778** NEW SECURITY RISKS **0** ENABLED CLOUD ACCOUNTS **100%** AQUA WAVE PLAN **PREMIER** [Edit](#)

Cloud Account Scan Summaries [Connect New](#)

Search

CLOUD	ACCOUNT	STATUS	NEW RISKS	SUMMARY
aws	aqua-cspm-aws-dev Default	Scanned		2886 55 408 2
	aqua-cspm-google-dev Default	Scanned		252 0 31 0
aws	aqua-cspm-sandbox-remediations Default	Scanned		2579 38 170 0
	aqua-cspm-azure-dev Default	Scanned		4300 0 70 4



View a detailed breakdown of risk by cloud account



Shift-Left Security for Infrastructure-as-Code (IaC)

Can you easily identify and remediate risks in IaC templates?

Can you ensure that your infrastructure is correctly configured before running applications?

Aqua provides powerful IaC template scanning capabilities to identify potential security risks as they are checked into source control before the infrastructure itself is deployed.

- Analyze AWS CloudFormation and HashiCorp Terraform templates for numerous security risks
- Detect misconfigurations services defined in IaC templates as part of your CI/CD workflow to prevent vulnerable infrastructure from being deployed
- Save time when managing IaC templates in multi-cloud scenarios



View code snippets of identified issues



The screenshot shows the Aqua interface for scanning CloudFormation templates. At the top, it displays 'CloudFormation Scan Results' with a 'Show source data' toggle. Below this, a code snippet of an AWS CloudFormation template is shown. Underneath the code is a 'Filter results' input field. The main part of the screenshot is a table with the following columns: Resource, Result, and Message.

Resource	Result	Message
AccessKey	FAIL	IAM access keys should not be defined in CloudFormation templates since it risks exposing the secret.
CloudFrontDistribution	WARN	CloudFront distribution does not have logging enabled. This is not required but may be helpful for incident response.
CloudFrontDistribution	FAIL	CloudFront distribution uses an S3 origin without an access identity.
CloudFrontDistribution	FAIL	CloudFront distribution does not specify a default root object and may expose the contents. Ensure a file is used as the default root object.
InstanceSecurityGroup	PASS	Security group is being created in a VPC.
LaunchConfig	FAIL	Launch configuration may associate a public IP address with instances. To prevent public exposure, ensure this value is set to false unless the instance requires public access.
LaunchConfig	PASS	Launch configuration does not specify inline block device mappings.



Quickly view and filter resource security risks to prioritize remediation



Get detailed rationale for risk classification and helpful insight for resolution

Holistic Kubernetes Security for the Enterprise

Can you ensure proper configuration of Kubernetes environments to minimize security risk exposure?

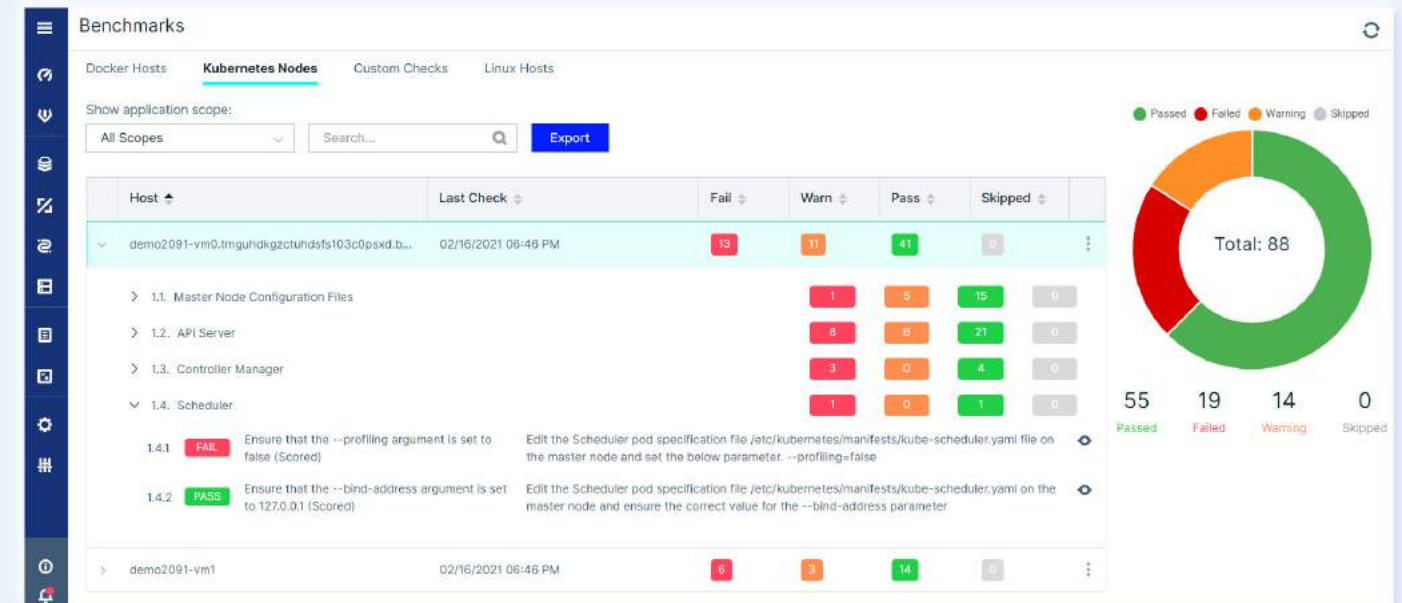
Do you have an automated way to identify and prioritize risks in Kubernetes environments?

Aqua KSPM (Kubernetes security posture management) helps to minimize the Kubernetes attack surface, prevent administrator errors, and protect against common attack vectors. Aqua KSPM enables security and compliance teams to enforce policy-driven security configurations and governance, and helps to secure the essential orchestration layer of cloud native applications with continuous security risk assessment and remediation.

- Validate Kubernetes configurations against CIS benchmarks for Kubernetes
- Detect security blind spots and automate identification of exploitable paths in Kubernetes clusters using Kube-hunter, Aqua's open source pentesting tool
- Ensure least-privilege access in Kubernetes environments while maintaining proper privileges for each user
- View a dynamic map of Kubernetes clusters and their associated risks, including all running workloads, namespaces, deployments, nodes (hosts), containers, and network connections
- Enhance the security posture of your Kubernetes workloads by controlling image contents, configurations, and pod attributes; use Aqua's image assurance policies to prevent the deployment of unsafe and non-compliant workloads
- Provide workload runtime protection in any managed or unmanaged Kubernetes environment without using a privileged container on the host
- Achieve visibility into Kubernetes security events to facilitate compliance, forensics, and incident response

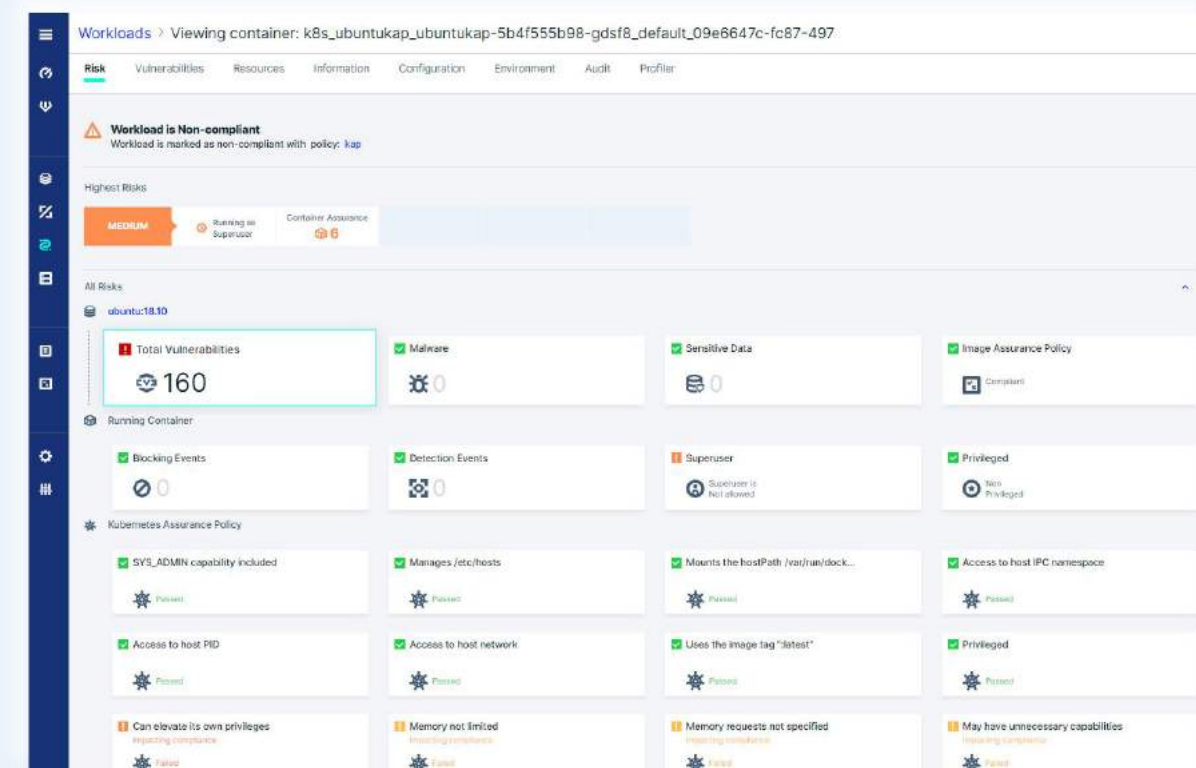


Gain a holistic view of risks in your Kubernetes clusters



View a detailed breakdown of risks measured against CIS benchmarks

Easily identify workloads that conflict with pre-defined policies



View a detailed breakdown of risks and assurance policy violations

Support Security Compliance Initiatives

Do you have an automated way to support PCI-DSS, NIST, GDPR, and HIPAA compliance requirements?

Can you generate audit reports and track user activities to demonstrate regulatory compliance?

Do you have visibility into vulnerabilities and configuration issues across the entire application lifecycle?

Aqua helps organizations to maintain compliance with an array of regulations and standards, from the build and into production. Automate testing of public cloud and Kubernetes configurations to support hardening requirements. Collect detailed image-level and host-level data that documents security practices and events for auditing and reporting.

- Generate granular audit trails of all workload activity, including access events, scan events, Docker and Kubernetes commands, container activity, secrets activity, and system events
- Enable full user accountability and control super-user permissions
- Leverage pre-built alerts and reports for key compliance mandates, including PCI-DSS, GDPR, HIPAA, NIST 800-53, and NIST SP 800-190
- Automate checks against CIS benchmarks, including Linux, Docker, Kubernetes, and the various cloud foundation benchmarks
- Craft a complete audit trail by tracking changes in vulnerability status, frequency of scans, and remediation trends
- Leverage Aqua's vShield to demonstrate established compensating controls for specific vulnerabilities



ISO 27001
ISO 27001 is an international standard that helps organizations manage information security.

Default

Control	Description	Plugins
A.5.1.1 Policies for Information Security	A set of policies for information security shall be defined.	View
A.6.1.1 Information Security Roles and Responsibilities	All information security responsibilities shall be defined and allocated. This mainly relies on Role Based Access Control (RBAC) that can help organizations define and allocate responsibilities set forth in the information security policy.	View
A.6.1.2 Segregation of Duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	View

HIPAA
HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

Default

Control	Description	Plugins
164.312(a)(1) Access Controls	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	View
164.312(a)(2)(iv) Encryption and Decryption (Addressable)	Implement a mechanism to encrypt and decrypt electronic protected health information.	View
164.312(b) Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	View

PCI
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

Default

Control	Description	Plugins
Requirement 1 - Firewalls	Install and maintain a firewall configuration to protect cardholder data.	View
Requirement 2 - Defaults	Do not use vendor-supplied defaults for system passwords and other security parameters.	View
Requirement 3 - Cardholder Data	Protect stored cardholder data.	View

Separation of Duties Across Multiple Application Teams

Do you have a simple automated way to manage security across multiple teams, applications, and stakeholders in an environment that still requires separation of duties?

Can you provision least-privilege access to security controls and vulnerability data?

Aqua's comprehensive role-based access controls (RBAC) deliver effective separation of duties (SoD) to support security and compliance initiatives in complex cloud native and multi-cloud deployments and provide the flexibility to support all deployment configurations and organizational structures. Aqua enables organizations to configure hierarchies and role-based permissions based on defined scopes, including distinct definitions of applications and environments.

- Separate projects or applications with multi-tenant RBAC to limit access to limit access by assignment, displaying information and providing capabilities only to those who need them
- Set scopes that encompass all aspects of an application and assign granular permissions (such as read-only or edit access to an asset or a capability) to specific roles
- Provide specific users with one or many roles, with the potential to map to LDAP or Active Directory groups, eliminating the need to define security groups or user roles from scratch
- Leverage out-of-the-box roles or customize roles from scratch, then combine roles with defined application scopes to maximize flexibility

Define the scope across which a role will be applied for assigned users and groups



Select pre-defined permissions sets for a given role



Define permissions relevant to policies, assets, compliance, & systems



Configure permissions for Editing or View Only access



Centralize Your Cloud Native Security Insights

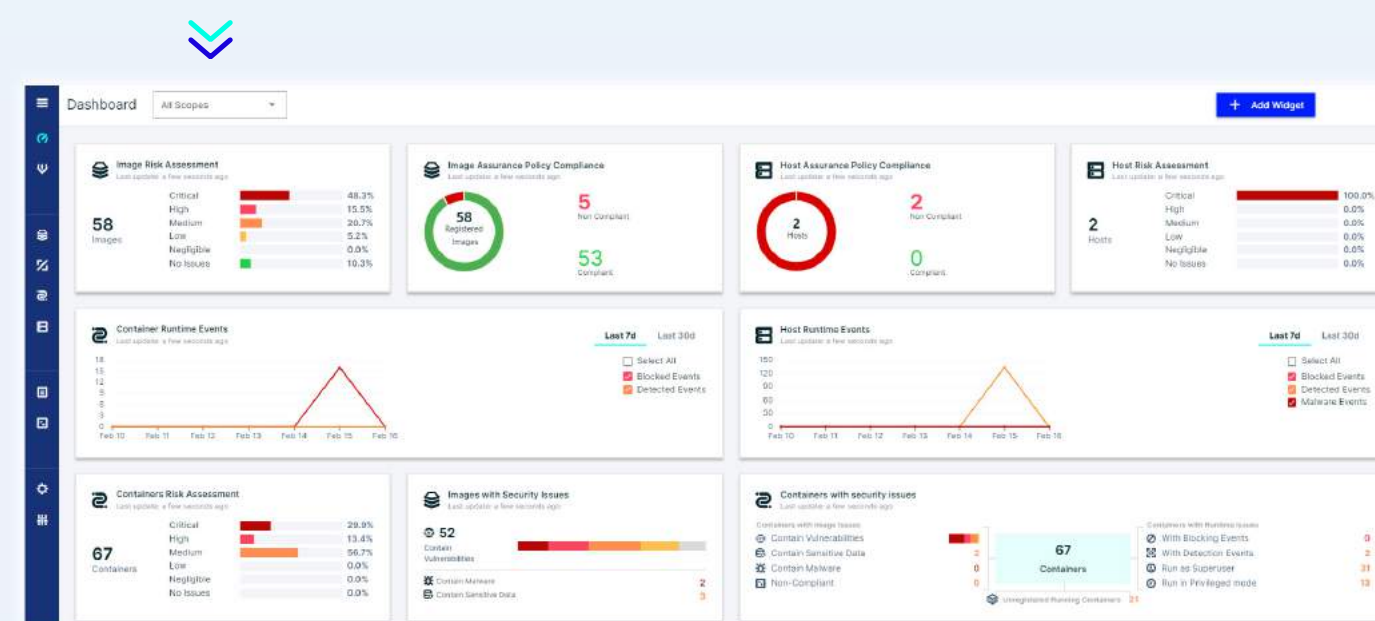
Can you see security risk metrics of all workloads and environments in one location?

Are you and your colleagues able to customize security dashboards to reduce the noise and clearly present the most relevant information?

Aqua makes it possible to distill large amounts of diverse security risk metrics into clear, actionable insight and present the most relevant data to each user or team. The Aqua dashboard delivers complete flexibility for users to customize the datasets they require to carry out their day-to-day tasks to support security and compliance across all types of workloads and all stages of the cloud native application lifecycle.

- View real-time risk data across all workloads and environments, including public, private, and multi-cloud deployments
- Customize the Aqua dashboard with more than 20 possible widgets
- Leverage drag-and-drop widgets for easy-to-use WYSIWYG customization
- Save, reuse, and share dashboard templates with users across your organization

Select the scope of information to be displayed in the dashboard



Add widgets to provide at-a-glance insight into assets and risks

The screenshot shows the Aqua Widget Gallery with the following components:

- Widget type:** Assets, Risk (selected).
- Widgets (6):**
 - Assets with Security Issues:** Number of assets with vulnerabilities, malware, and sensitive data.
 - Asset Risk Assessment:** Number of assets per risk assessment.
 - Vulnerability Trends:** Asset vulnerability trends.
 - Registry Risk Assessment (By Images):** Registries with the most images containing security issues.
 - Assets with new Security Issues:** Number of new vulnerabilities.
- Risk Widgets (6):** A list of risk-related widgets, with 'Risk Widgets (6)' highlighted.
- Runtime Protection (2):** A list of runtime protection widgets.
- Policy Violations (3):** A list of policy violation widgets.
- DONE:** A button to complete the dashboard customization.

Seamless Integration Across the Ecosystem

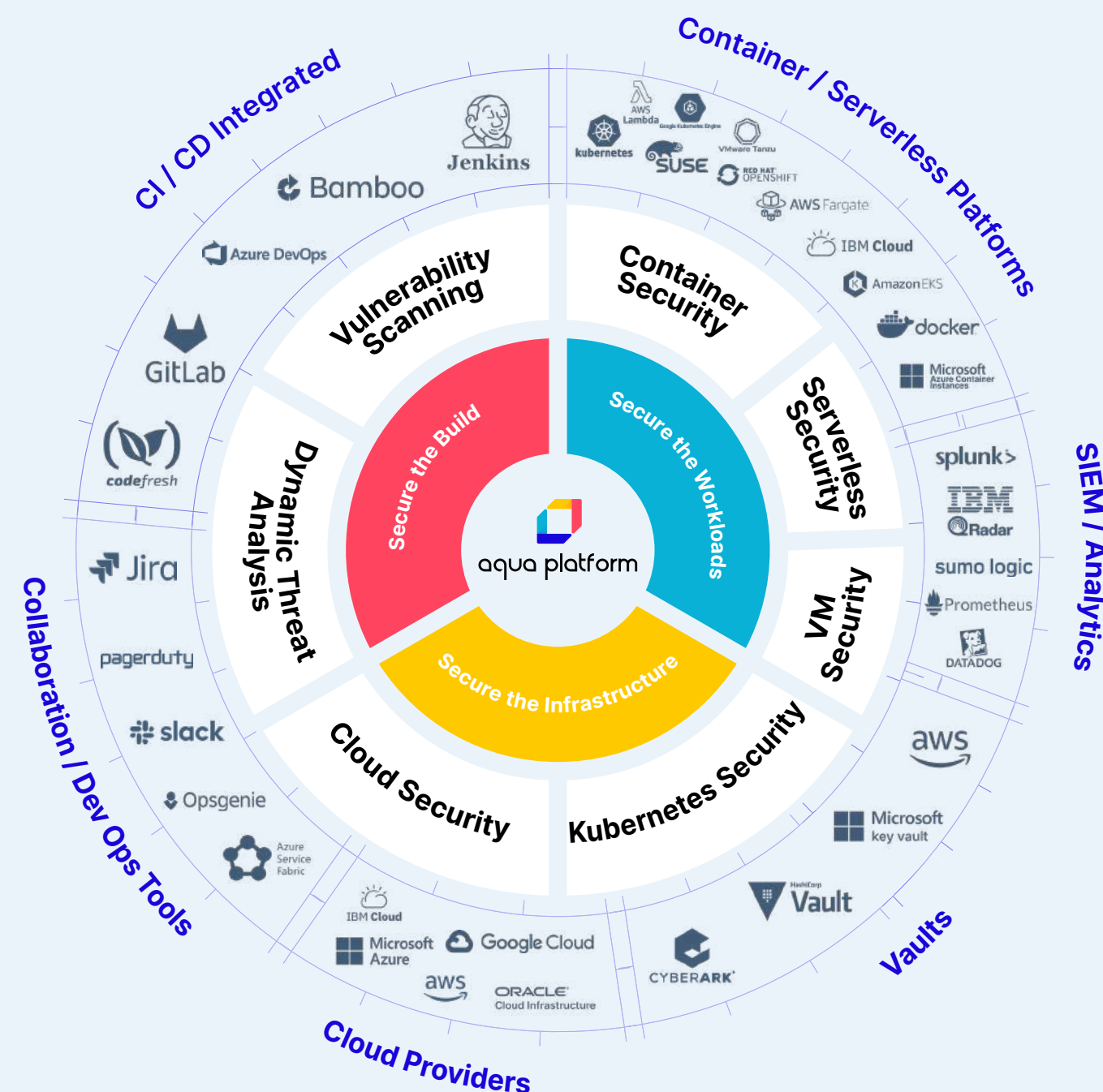
Can you support the whole cloud native ecosystem and full application lifecycle with security risk analysis?

Can you integrate security risk insight and fix information directly into your security toolset (e.g., SIEM) to accelerate remediation and facilitate collaboration?

Aqua provides a wide range of integrations for all stages of the application lifecycle and across public and multi-cloud environments. Aqua integrations help security to shift left, support compliance initiatives, and ensure security of running workloads.

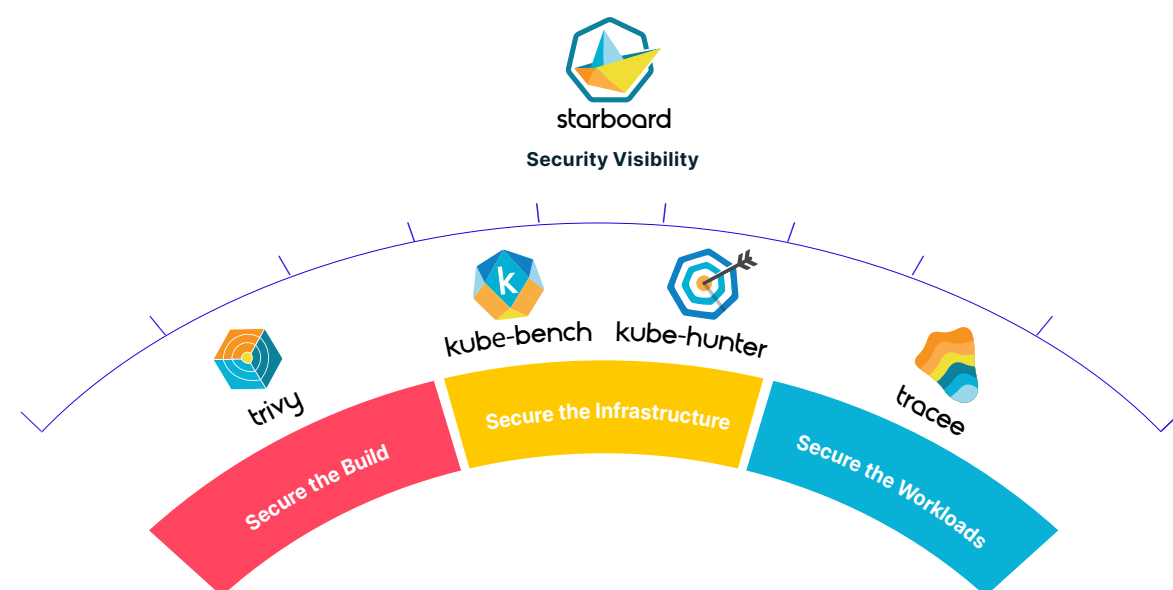
Aqua integrations help to manage risks and instill security best practices within:

- Software development and delivery
- Infrastructure
- Security and response
- Collaboration and issue management



For a full list of Aqua's most notable integrations, please visit www.aquasec.com/integrations/

Innovating Cloud Native Security with Open Source



Aqua believes in the viability of open source solutions for cloud native security for DevSecOps and encourages individuals and organizations to explore new security practices by testing out a full portfolio of open source projects supported and maintained by Aqua.



Trivy detects vulnerabilities in open source software and provides a brief explanation of risk so developers can make more informed decisions regarding the components they incorporate into their applications and containers to secure the application before it ships. github.com/aquasecurity/trivy



Kube-bench is a Kubernetes configuration security checker, helping to secure the infrastructure for cloud native application deployment and providing a way to constantly test a Kubernetes cluster to see if it complies with the CIS Kubernetes Benchmark. github.com/aquasecurity/kube-bench



Kube-hunter is an open source penetration testing tool for Kubernetes that helps detect potential security risks or bad configuration issues in the Kubernetes cluster. Kube-hunter does what an attacker would do, looking for potential entry points or weaknesses that could be exploited. github.com/aquasecurity/kube-hunter



Tracee is a lightweight container and system-tracing tool, implemented using eBPF, that runs the container, observes system calls and system events in real time, and enables users to improve runtime security for cloud native workloads. github.com/aquasecurity/tracee



Starboard enables results from vulnerability scanners, workload auditors, and configuration benchmark tests to be incorporated into Kubernetes custom resource definitions (CRDs) and accessed through the Kubernetes API. This means you can run solutions of your choice, integrate them into Kubernetes, and consume or compare their reports in the same location. github.com/aquasecurity/starboard

Aqua Cloud Native Security Platform Architecture

Aqua Server

Central management component that can be deployed on multiple instances or fully hosted for high availability. Provides capabilities for scanning, lifecycle controls, policies, monitoring, and reporting

Aqua Gateway

Provides connectivity between the Aqua Server and the Aqua Enforcers

VM Enforcer

Provides protection for hosts (VMs), monitors host images, and enforces host runtime policies to monitor and restrict unapproved runtime activities

Kube-Enforcer

Aqua's cloud security posture admission controller, which ensures that only scanned, non-compromised or compliant images can be run in your Kubernetes environments

Aqua CyberCenter

Aqua's security risk intelligence database, curated and refined to provide accurate detection and analysis of CVEs, vendor-issued advisories, proprietary Aqua cyber security research, and malware

Aqua Enforcer

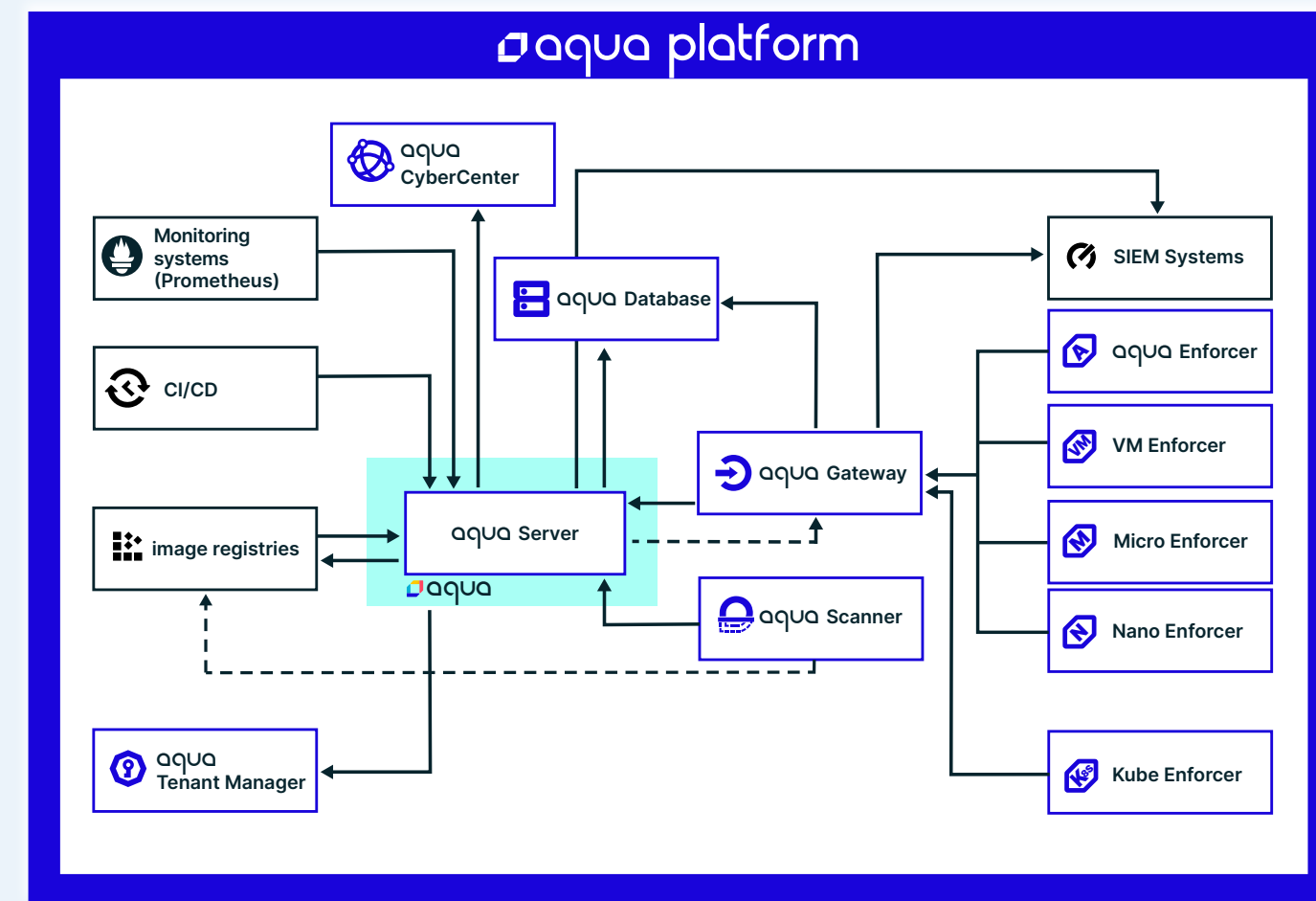
Monitors workload runtime activity and ensures security by enforcing defined controls

Micro-Enforcer

Provides runtime protection for containers in PaaS environments where host-based solutions cannot be deployed

Nano-Enforcer

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



Why Choose Aqua

Aqua empowers organizations by providing unparalleled insight into cloud native security for large production environments and is the vendor of choice to more than 400 organizations worldwide. Among these are the world's largest banks, financial institutions, manufacturers, retailers, internet providers, media vendors, transportation giants, and government organizations. The Aqua approach emphasizes five key areas that drive evolution in security technologies and security operations.

We are committed to driving change in the market and cloud native community

Open Source

We can handle any size of deployment, across heterogeneous environments and teams

Built for Enterprise Scale

We specialize in cloud native, invest in security research, and foster innovation across the ecosystem

Cloud Native Focus

We share our security expertise to guide you on your cloud native journey

Customer Partnership

We secure complex cloud native stacks and support evolving DevSecOps methodologies

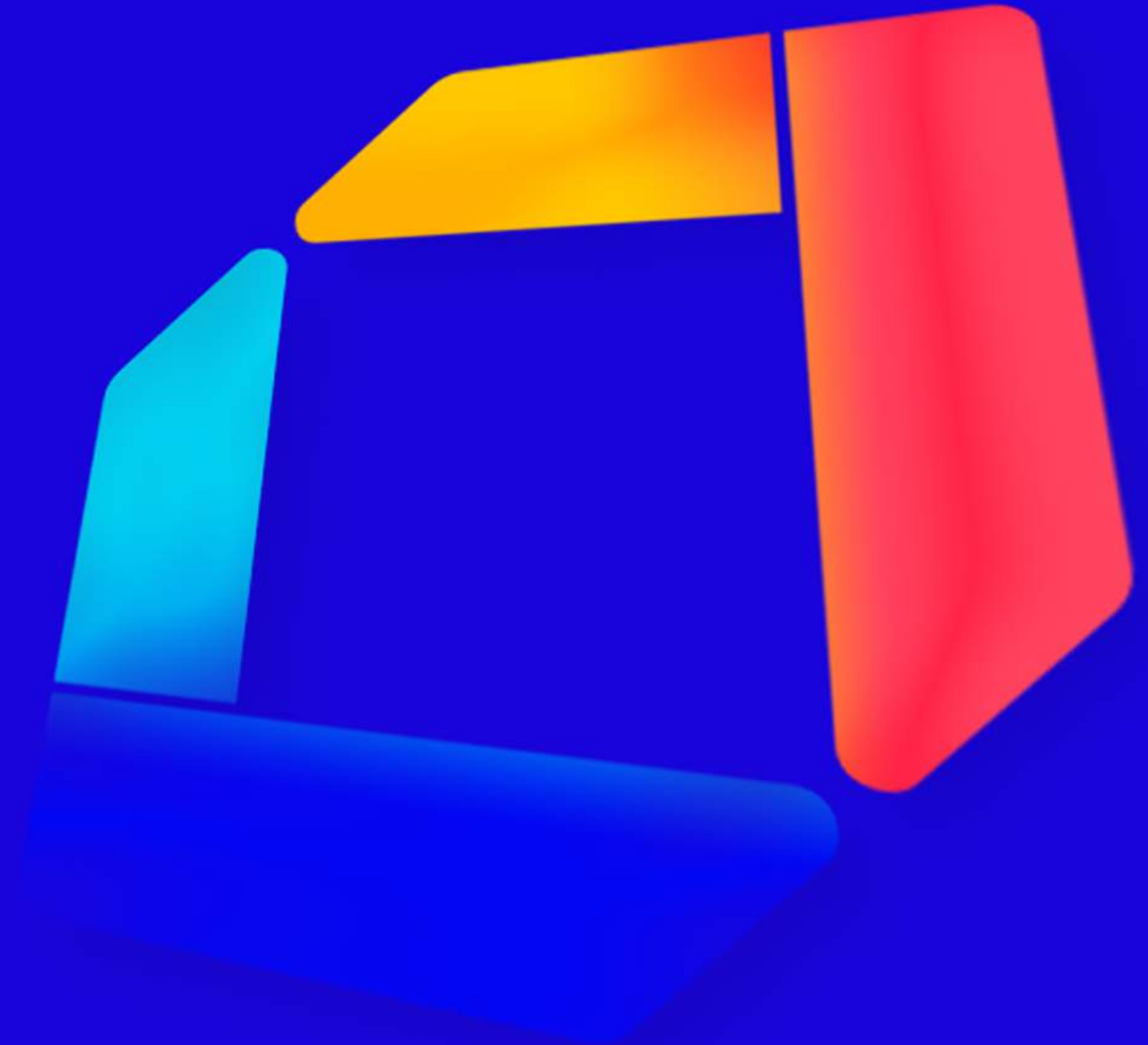
Broad Platform Support



Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure, and secure running workloads wherever they are deployed.

Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing, and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions, and cloud VMs.

aquasec.com



@AquaSecTeam



Aqua Security