aqua

Supporting PCI-DSS Compliance for Cloud Native Environments

Executive Summary

This guide is intended to support your effort to address Payment Card Industry Data Security Standard (PCI DSS) requirements in your cloud-native environments related to Aqua Security technology.

Cloud native environments are characterized by elastic infrastructure and often ephemeral orchestrated workloads. Securing access to payment cardholder data, as required by PCI-DSS can pose a significant challenge when applications are transient and deployed across multiple environments, with no permanence of location or traditional network segmentation.

As such, compliance means meeting requirements from the infrastructure to the operating system, and then on to the network level. The distributed-layer architectures of cloud environments add complexity and require a change in how access, privileges, and networking are governed, monitored, and audited. Traditional security tools lack the ability to track changes and provide context in such environments and will not ensure compliance as they have done in traditional environments.

PCI-DSS checklist for cloud native deployments

Cloud-native technology introduces dramatic changes to application development. It sometimes involves an increased use of open-source components, introducing vulnerabilities and evading vetting processes based on existing version and configuration management. It also accelerates the software development timeline, which challenges established security checkpoints to keep up.

Cloud native environments impact PCI compliance in a few key areas:

Network security Containerized and serverless applications Introduce challenges in tracking where your workloads are running. The network connections between the different workloads should be identified, at any given time, to prevent network traversal and intrusion

Vulnerability management

Cloud-native applications that use open-source components may contain vulnerabilities. These applications should be monitored for security vulnerability information and mitigated before being used in production

User access control, segregation of duties

Workloads should be accessible only to specific individuals with specific job-related needs

Threat analysis and mitigation

One of the pillars of any given cloud native environment is its policy-based security rules that can maintain an automated check for ongoing monitoring and prevention of malicious activity

Data protection, real-time visibility, and event audit trails

Access to PCI-sensitive data and systems is required to be logged and audited. Besides, access to these files must be restricted and backed-up regularly. When working with containers, existing audit methods may not have sufficient functionality to track this kind of data in a cloud native environment

How Aqua Helps Address PCI-DSS Compliance

The following points detail examples and explanations for how Aqua addresses many PCI DSS requirements for applications that span public cloud services, VMs, containers, and serverless functions

Cloud Account Compliance Overview

Aqua CSPM offers compliance reports to match your cloud infrastructure scan results to industry standards and compliance controls. Audit your cloud infrastructure accounts for configurations and security controls required as part of many popular compliance programs, detecting bad configurations and remediating them

Vulnerability assessment

Aqua provides in-depth vulnerability assessment for container images, preventing vulnerabilities from getting into applications before deployment. Natively enrich vulnerability management with risk-related contextual factors such as running containers and exploitability. Gain insights on actively used packages using an advanced application scoping

Policy-based security

Aqua provides out of the box assurance and enforcement policies that you can configure across the build, workload, and infrastructure. This includes Kubernetes, CI/CD pipeline, functions, essentially across the entire cloud native life-cycle.

Aqua admins can detect, assess, and review any security issues in cloud-native images. The goal is to deploy policies that ensure the security of your applications.

For example, Aqua assurance policies secure your applications and infrastructure before runtime. You can configure policies to block the deployment of non-compliant images, functions, and Kubernetes workloads

Secrets management

Aqua provides central management and secure distribution of secrets and cryptographic keys into running containers. Centrally control secrets and how containers access them and inject secrets into a running container, ensuring that secrets only run in a container's memory. Aqua integrates with secret management tools, including Amazon KMS, HashiCorp Vault, Azure Key Vault, and CyberArk Enterprise Password Vault

Separation of duties and access control

In a cloud native environment, the development team should have limited access to production. Aqua's multi-tenant, role-based access control (RBAC) capability supports the segregation of duties between different applications to limit access by assignments. Maintain productivity and support all types of deployment, security, and organizational structures

Identity-based segmentation

To monitor and secure all network connections, Aqua provides a network firewall that prevents unauthorized network connections and nano-segmentation of the network to observe the relationship between workloads. Aqua networking capabilities offer full visibility for cloud-native applications that run on a single/hybrid cloud

Full event logging

Aqua provides a granular audit trail of several kinds of events: both regular and those indicating security exposures. This includes policy violations, configuration drifts, FIM, and user activity monitoring. Integration with third-party tools, such as Splunk and various SIEM tools, allows events to be centrally collected, analyzed, and protected from being deleted

The distributed architectures of cloud native environments add layers of technology and complexity that challenge traditional assessment methods. These layers impact how PCI DSS compliance is managed in a cloud native environment, how network segmentation is implemented, how individual PCI DSS requirements are validated, and which party will perform validation activities. In the following sections, we list how the Aqua Platform addresses the relevant PCI requirements and supports PCI DSS compliance.

Requirement 1

Install and maintain a firewall configuration to protect cardholder data

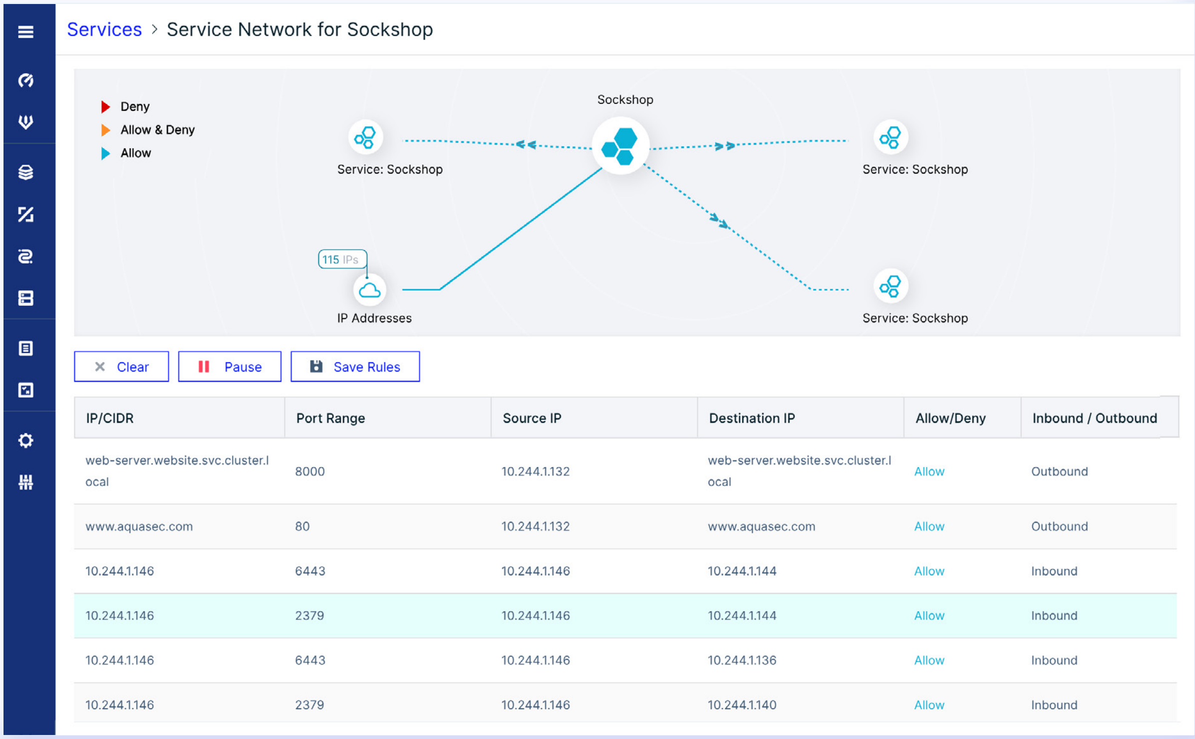
All systems must be protected from unauthorized access from untrusted networks. Whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources.

PCI-DSS Requirement	How Aqua Helps
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Aqua helps you to detect and map internal and external network connections automatically. Admins can view a visual representation of the network topology and associated relationships of a service. This map enables admins to capture monitored connections and use them as a base for the firewall policy
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	
1.1.4 Requirements for a firewall at each Internet connection between any demilitarized zone (DMZ) and the internal network zone	Aqua's Workload Firewall automatically discovers workload network topology, both within a host and across hosts, and applies identity-based firewall rules that alert or prevent unauthorized network connections. This capability allows the creation of network boundaries across services, where admins can control which networks are accessible for each service. Also, admins can manually modify communication rules/policies based on actual activity without impacting workload performance and availability
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment	Aqua's workload firewall admins can limit the network connectivity between services by applying a firewall-like concept for the cloud native environment. This capability allows the creation of network boundaries across services, where admins can control which networks are accessible for each service – and these can be mapped to cloud native constructs such as CI/CD pipelines, registries, clusters and K8s namespaces, to create natural boundaries between environments. Aqua's identity-based management enables you to label groups of workloads as PCI-sensitive. Aqua admins can use labels and services to automatically group cloud native assets deployed on separate nodes and network segments

PCI-DSS Requirement	How Aqua Helps
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and specifically deny all other traffic	Aqua provides several ways to limit the workload's network traffic. In addition to identity-based micro-segmentation (explained in 1.1.2,1.13, 1.1.4, and 1.2), workloads' security profiles can categorically deny outbound or inbound connections. For example, a database container will typically not require outbound connectivity to be rejected automatically
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. Aqua Covers all 1.3.x Requirement excluding 1.3.5	Aqua's workload firewall functionality can be used to create global rules that prevent containers tagged with a specific label (for example – PCI-DSS compliance) from having outbound or inbound connections. The functionality might permit some workloads to access specific IP addresses/URLs

For more information on how Aqua supports Requirement 1

Aqua Services Overview ›



Services › Service Network for Sockshop

IP/CIDR	Port Range	Source IP	Destination IP	Allow/Deny	Inbound / Outbound
web-server.website.svc.cluster.local	8000	10.244.1.132	web-server.website.svc.cluster.local	Allow	Outbound
www.aquasec.com	80	10.244.1.132	www.aquasec.com	Allow	Outbound
10.244.1.146	6443	10.244.1.146	10.244.1.144	Allow	Inbound
10.244.1.146	2379	10.244.1.146	10.244.1.144	Allow	Inbound
10.244.1.146	6443	10.244.1.146	10.244.1.136	Allow	Inbound
10.244.1.146	2379	10.244.1.146	10.244.1.140	Allow	Inbound

Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily found via public channels.

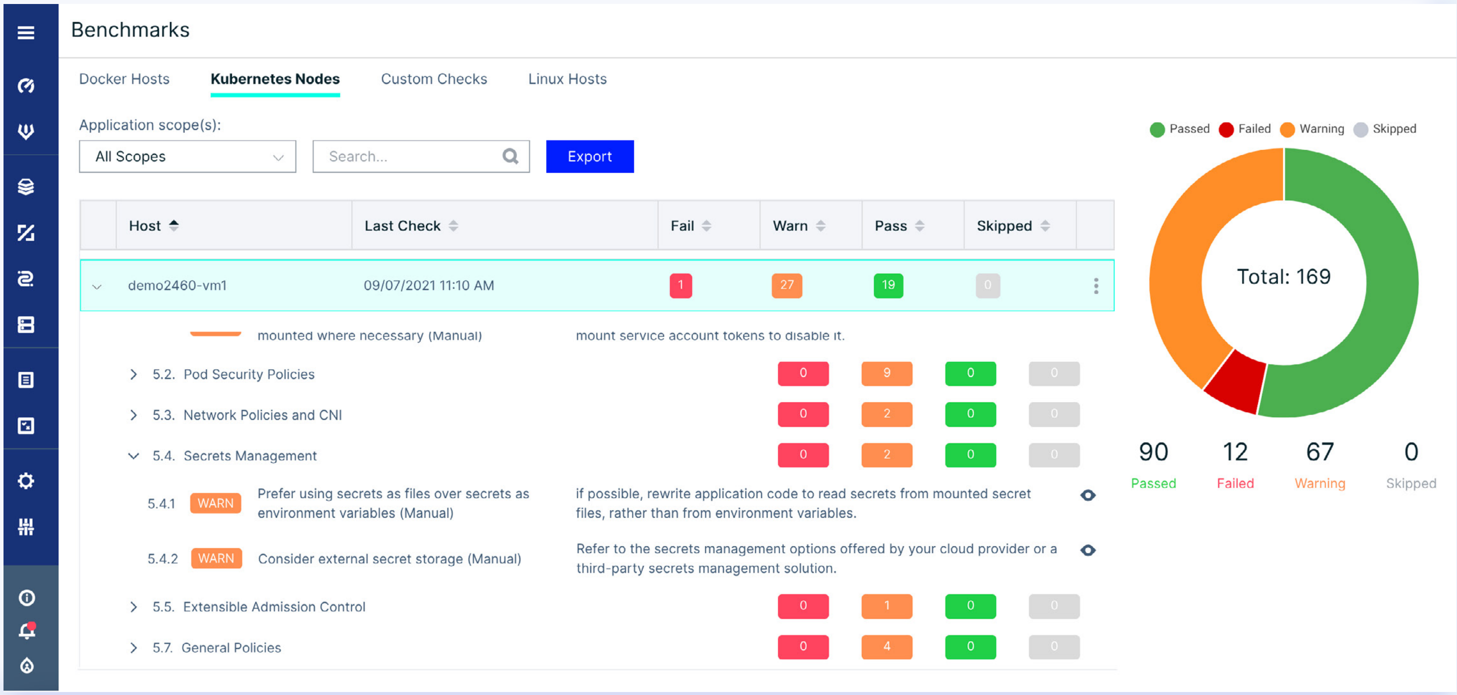
PCI-DSS Requirement	How Aqua Helps
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.	You can integrate Aqua secrets management with several third-party key vaults and services, using the Aqua UI. CSPM checks whether default passwords have been reconfigured to ensure vendor defaults haven't been used and supports key management best practices in Azure, AWS, and GCP
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ● Center for Internet Security (CIS) ● International Organization for Standardization (ISO) ● SysAdmin Audit Network Security (SANS) Institute ● National Institute of Standards Technology (NIST)	Aqua supports the CIS Docker, Kubernetes, and Linux benchmarks for host hardening, compliance reports per host, and a comprehensive image vulnerability report. The Host CIS screen provides information regarding compliance with the CIS Benchmarks, which has best practices for an engine configuration, container runtimes, and host configurations. Aqua also supports the AWS, Azure and GCP Foundation CIS Benchmarks, to secure IaaS & PaaS cloud account configurations, enabling organizations to follow critical configuration guidelines, and implement auto-remediation in some cases

PCI-DSS Requirement	How Aqua Helps
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system	Follows behavioral workload security profiles that whitelist legitimate activities and enforces the least functionality
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure	Employs global security controls that enforce configuration and provides workload-specific threat mitigation capabilities. Aqua's security policies are available for assurance, before running production, and also in runtime. For example, we can ensure that images don't contain excessive packages. Drift prevention prevents any changes made to a running workload to ensure any potential unknown threats are blocked in runtime. File Integrity Monitoring for Containers and VMs provide a complete audit trail of any changes made. Aqua's network segmentation capabilities allow users to create granular segments within the cloud infrastructure. An organization can limit the size of the network's attack surface by breaking it into small pieces. If a particular segment is compromised, all other segments are blocked and protected
2.2.4 Configure system security parameters to prevent misuse	
2.4 Maintain an inventory of system components that are in scope for PCI DSS	Aqua provides a precise inventory of cloud native assets, covering the different repositories, container images, functions, cloud VMs, and running workloads in the organization. Aqua connects to your cloud native registries and enumerates all assets stored in them. Aqua also processes all images stored on the hosts that were not pulled from an image registry and creates a package inventory for every image. With Aqua CSPM Aqua will automatically discover new cloud service accounts at the Folder level. For other cloud platforms when you onboard cloud service accounts Aqua will automatically discover misconfigurations.

For more information on how to comply with Requirement 2

Aqua's documentation ›   Runtime Policies ›   Environment Variables ›

Benchmarks ›   Image Assurance ›



Benchmarks

Docker Hosts | **Kubernetes Nodes** | Custom Checks | Linux Hosts

Application scope(s): All Scopes

Search...

Export

	Host	Last Check	Fail	Warn	Pass	Skipped
⌄	demo2460-vm1	09/07/2021 11:10 AM	1	27	19	0
	mounted where necessary (Manual)	mount service account tokens to disable it.				
›	5.2. Pod Security Policies		0	9	0	0
›	5.3. Network Policies and CNI		0	2	0	0
⌄	5.4. Secrets Management		0	2	0	0
5.4.1	WARN Prefer using secrets as files over secrets as environment variables (Manual)	if possible, rewrite application code to read secrets from mounted secret files, rather than from environment variables.				
5.4.2	WARN Consider external secret storage (Manual)	Refer to the secrets management options offered by your cloud provider or a third-party secrets management solution.				
›	5.5. Extensible Admission Control		0	1	0	0
›	5.7. General Policies		0	4	0	0

90	12	67	0
Passed	Failed	Warning	Skipped

Requirement 3

Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data without the proper cryptographic keys, the data is unreadable and unusable to that person.

PCI-DSS Requirement	How Aqua Helps
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary	Aqua provides central management and secure distribution of secrets and cryptographic keys into running containers and functions with no downtime/ restart. Admins can define a secret in the Aqua Management console and assign access control policies that authorize users or groups to run containers that use the secret. CSPM ensures that the right configurations are set up for cloud services as well, such that it: ● Ensures at-rest encryption is setup for RDS instances ● Ensures KMS keys are set to rotate on a regular schedule ● Ensures EBS volumes are encrypted at rest ● Ensures SQS encryption is enabled
3.6.2 Secure cryptographic key distribution	
3.6.7 prevention of unauthorized substitution of cryptographic keys	Aqua integrates with several secret stores, including HashiCorp Vault, Amazon KMS, Azure Vault, and CyberArk, thereby allowing organizations to leverage these central stores and extend them for use with containers. BYOK for a higher level of data access control

Requirement 3

Protect stored cardholder data

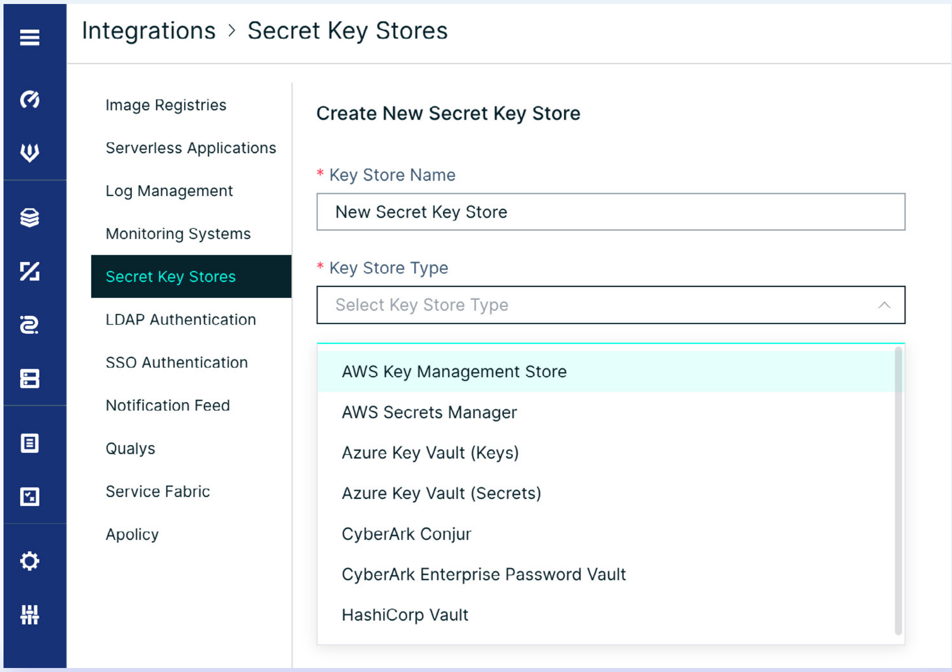
Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data without the proper cryptographic keys, the data is unreadable and unusable to that person.

For more information on how to comply with Requirement 3

Aqua's documentation ›

Integration of Secret Key Stores ›

Manage Secrets ›



Integrations › Secret Key Stores

Create New Secret Key Store

* Key Store Name: New Secret Key Store

* Key Store Type: Select Key Store Type

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware” including viruses, worms, and Trojans enters the network during many business-approved activities, including employee e-mail and use of the Internet, mobile computers, and storage devices. In the worst-case scenario, it results in the exploitation of system vulnerabilities.

PCI-DSS Requirement	How Aqua Helps
5.1 Deploy anti-virus software on all systems commonly affected by malicious software	You can integrate Aqua secrets management with several third-party key vaults and services, using the Aqua UI. CSPM checks whether default passwords have been reconfigured to ensure vendor defaults haven’t been used and supports key management best practices in Azure, AWS, and GCP Aqua supports the CIS Docker, Kubernetes, and Linux benchmarks for host hardening, compliance reports per host, and a comprehensive image vulnerability report. The Host CIS screen provides information regarding compliance with the CIS Benchmarks, which has best practices for an engine configuration, container runtimes, and host configurations. Aqua also supports the AWS, Azure and GCP Foundation CIS Benchmarks, to secure IaaS & PaaS cloud account configurations, enabling organizations to follow critical configuration guidelines, & implement auto-remediation in some cases Follows behavioral workload security profiles that whitelist legitimate activities and enforces the least functionality
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software	
5.2 Ensure that all anti-virus mechanisms are maintained as follows: ● Are kept current ● Perform periodic scans ● Generate audit logs which are retained per PCI DSS Requirement 10.7	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period	Aqua’s RBAC feature ensures that administrative access to the policies which can enable or disable Drift Prevention, DTA, and malware protection for images and Virtual Machines, is limited to the appropriate individuals and teams. Access can further be segregated by projects or applications to fit any organizational structure, maintaining teams’ productivity. Further, these capabilities are deployed or installed/uninstalled as system services using a privileged account. Non-privileged users cannot uninstall the capabilities or change the policies

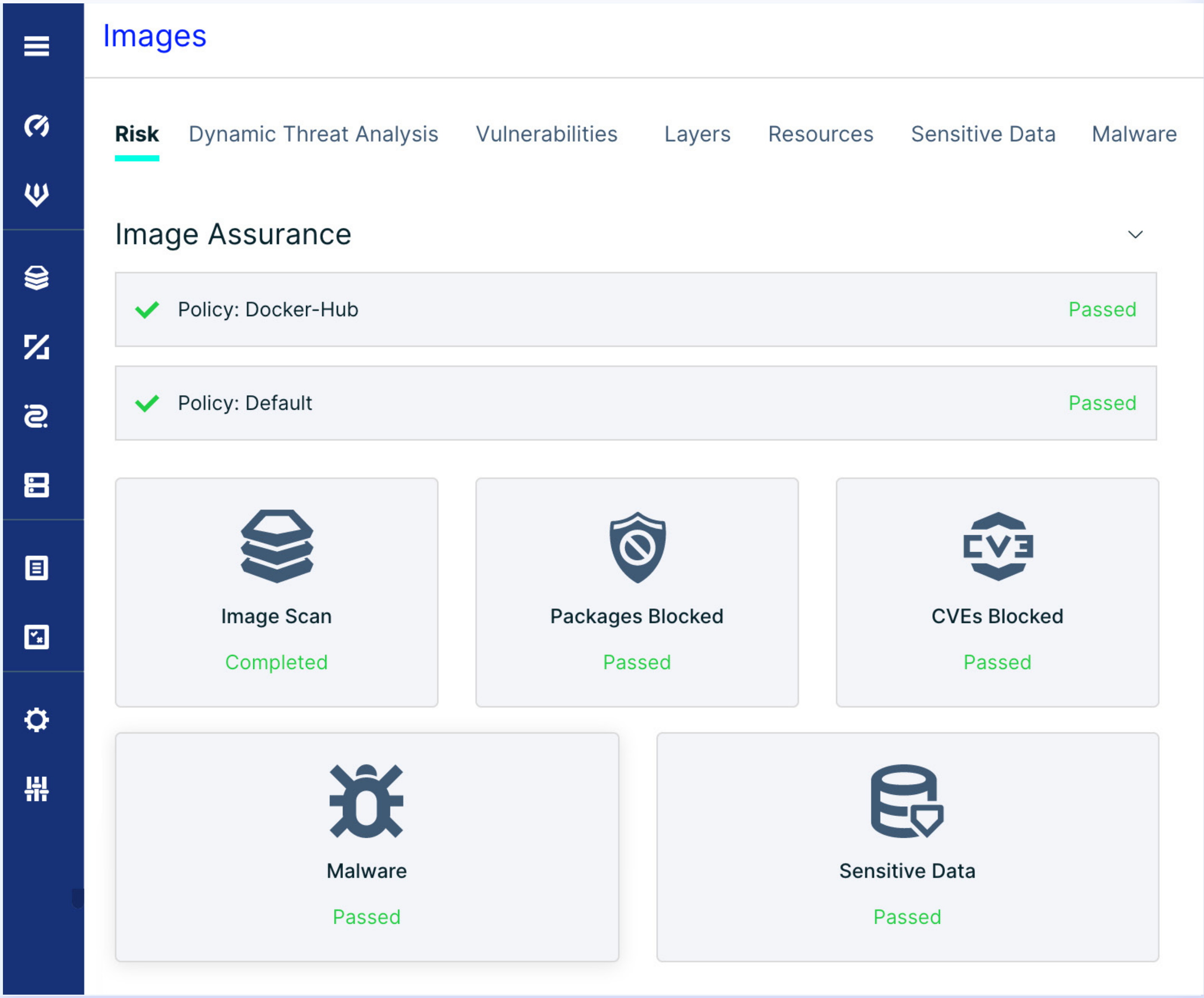
For more information on how to comply with Requirement 5

Aqua's documentation ›

Runtime Policies ›

RBAC Overview ›

Aqua Dynamic Threat Analysis (DTA) ›



Images

Risk | Dynamic Threat Analysis | Vulnerabilities | Layers | Resources | Sensitive Data | Malware

Image Assurance

✓ Policy: Docker-Hub — Passed

✓ Policy: Default — Passed

Image Scan — Completed

Packages Blocked — Passed

CVEs Blocked — Passed

Malware — Passed

Sensitive Data — Passed

Requirement 6

Develop and maintain secure systems and applications

All systems must have all appropriate software patches to protect them against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

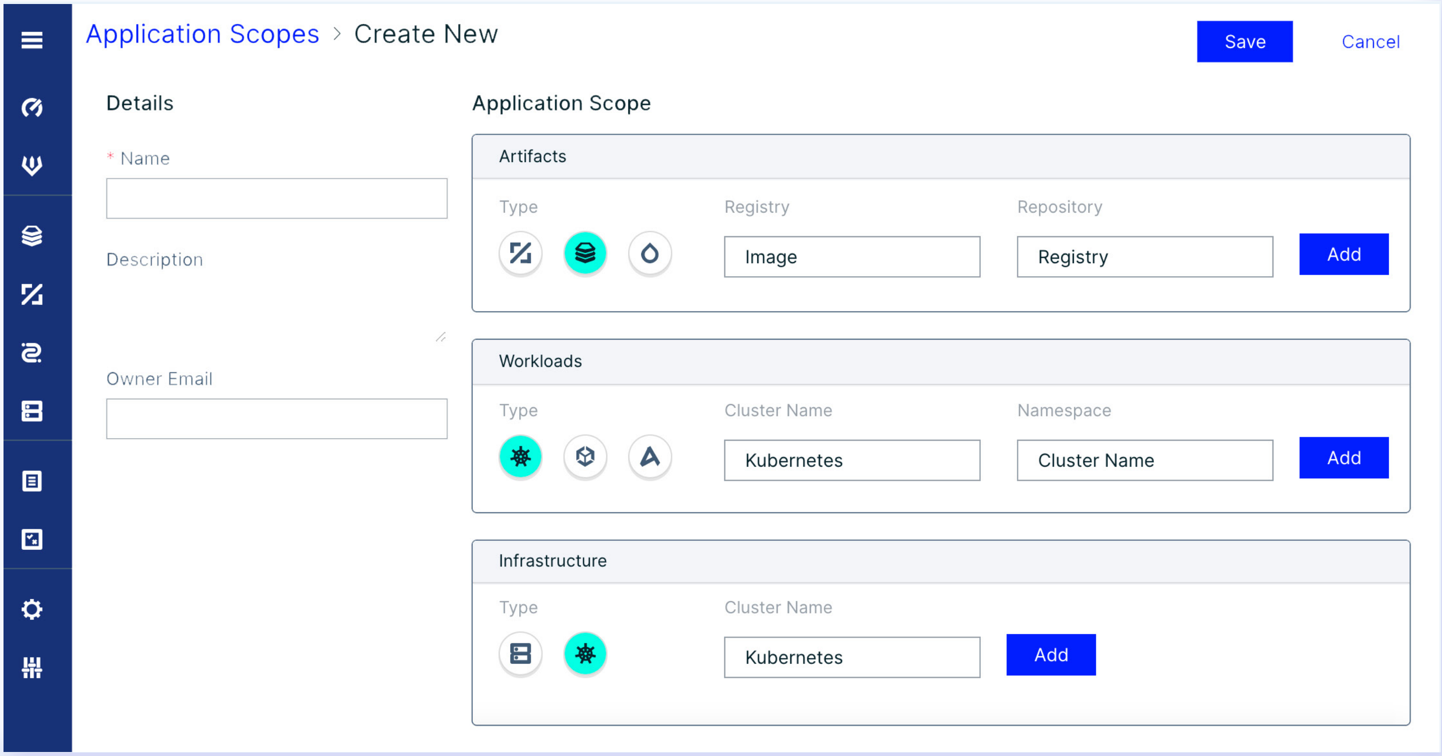
PCI-DSS Requirement	How Aqua Helps
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities	Aqua scans images, functions, registries, and hosts for known vulnerabilities, configuration errors, embedded secrets, and malware to impact the system's information assurance and security. Each vulnerability is ranked from low to high based on its Common Vulnerability Scoring System (CVSS3 and CVSS2). The scanning process is performed by integrating the Aqua Command Center with an image/function registry. Also, Aqua can scan images within CI tools (such as Jenkins, Microsoft VSTS, and Bamboo) to mitigate risks during the Build. Each image is scanned for vulnerabilities in both its OS packages and in the development language files. All new and old identified vulnerabilities are audited and can be automatically mitigated by creating image assurance policies. With Aqua's Risk-based Insights view you can focus on the most important and urgent vulnerabilities to manage. Aqua also providers actionable mitigation information for detected vulnerabilities for fast remediation
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release	In cloud-native environments, Aqua offers remediation guidance to address vulnerabilities early on in the development lifecycle integrating into the CI/CD pipeline and developer workflows. Aqua Trivy is our open-source vulnerability scanner that is simple to use and has broad coverage. In the Aqua platform, when vulnerabilities can't be fixed in the build, for example, when there is no fix available, Aqua offers vShield for automatically mitigating exploits in runtime. Aqua is continually updating new vulnerability data, culled from several sources (commercial, public, and proprietary) with the Aqua CyberCenter feed for continuous improvement. It checks and rechecks registries and images for ongoing monitoring. Aqua CyberCenter: • Constantly monitors various security trackers, software vendors' security-related information, websites, and other threat intelligence sources • Builds an up-to-date, dynamic, & comprehensive database of known vulnerabilities & malware that could impact images, containers, and their hosts • Maintains an IP address blacklist, consisting of IP addresses with known reputations for inadequate security

PCI-DSS Requirement	How Aqua Helps
6.4 Follow change control processes and procedures for all changes to system components	Aqua enforces the immutability of containers by preventing changes to a running container. This feature is called drift prevention. Easily monitor any changes in your system with Aqua’s System Integrity Monitoring and File Integrity Monitoring. Monitor files and directories for read, write, and modify operations. Generate audit events for Windows host for any changes made to system time and Windows services operations. CSPM config tracking ensures that AWS config service is enabled to detect changes to account resources to properly record and deliver logs
6.4.1 Separate development/test environments from production environments and enforce the separation with access controls	By using Aqua, organizations can separate their development pipeline from their production deployments in an easy way. Organizations can integrate Aqua into the development pipeline by adding Aqua as a build step in CI/CD tools such as Jenkins and TeamCity. This also ensures that developers are not exposed to Aqua’s console while they continue working with their existing tools. Admins can define access and permissions within their Aqua deployment that maintain separation of duties between application teams while maintaining the least privilege of permissions by role. Ensure that access to all elements of an application is limited to relevant stakeholders
6.4.2 Separation of duties between development/test and production environments	

For more information on how to comply with Requirement 6

Aqua’s documentation ›   Aqua Lable ›   RBAC Overview ›

Aqua CyberCenter ›   Image Assurance ›



Application Scopes › Create New

Save Cancel

Details

* Name

Description

Owner Email

Application Scope

Artifacts

Type	Registry	Repository	
	Image	Registry	Add

Workloads

Type	Cluster Name	Namespace	
	Kubernetes	Cluster Name	Add

Infrastructure

Type	Cluster Name	
	Kubernetes	Add

Requirement 7

Restrict access to cardholder data by business need to know

PCI-DSS Requirement

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on the need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

How Aqua Support this requirement?

Aqua enables organizations to define access and permissions within their Aqua deployment that maintain separation of duties between application teams while maintaining least privilege permissions by role. This enables separation of access between teams that handle cardholder data vs. those who don’t, and even within the teams that handle cardholder data, ensure that each role can view or change only those areas under its responsibility – for example, handling vulnerabilities, or runtime policies, or event auditing.

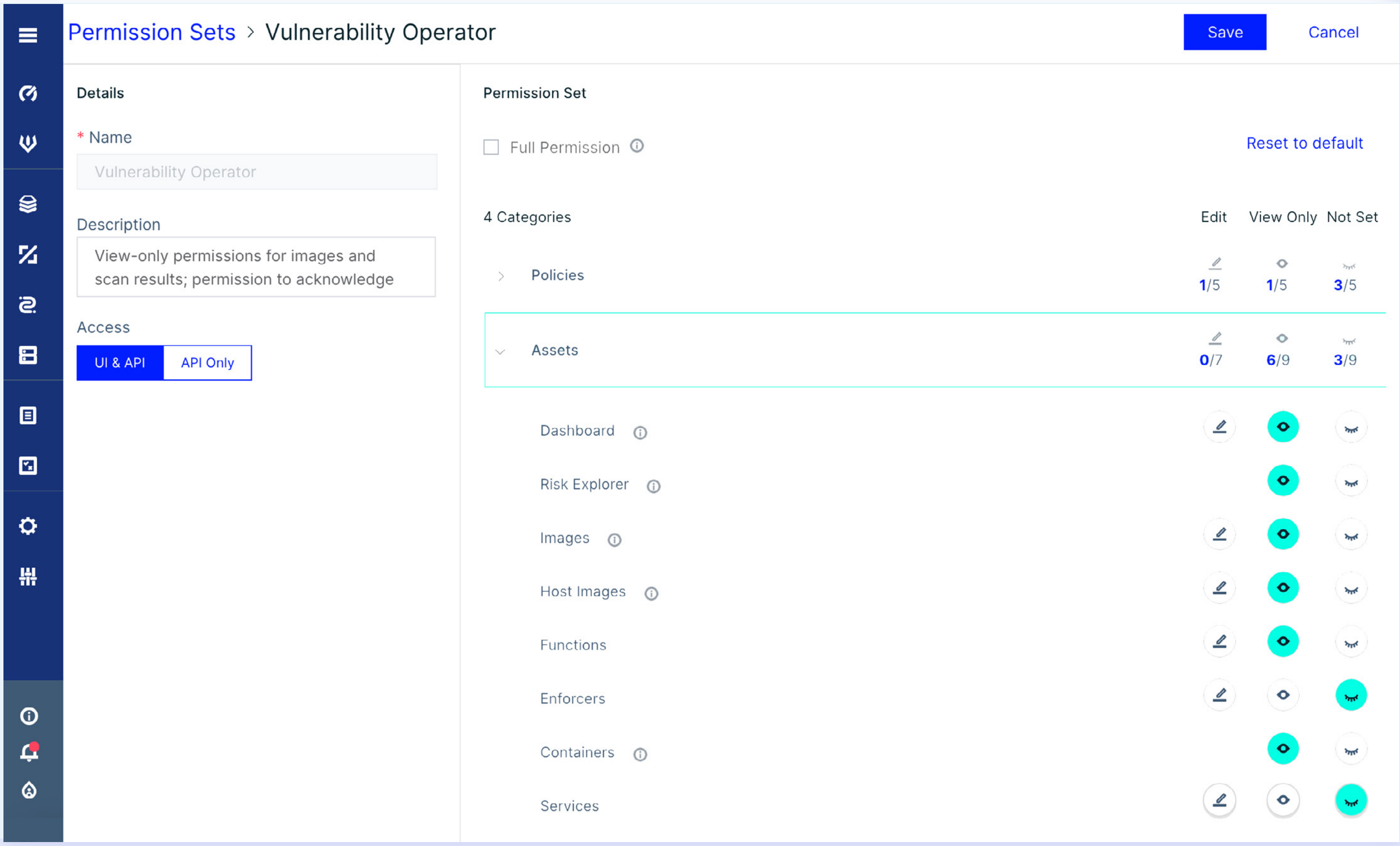
PCI-DSS Requirement	How Aqua Helps
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access	Aqua's extensive RBAC model is made to accommodate every possible team and role structure. There's separation between product teams based on parameters such as registry, pipeline, labels, clusters, namespaces. In addition to predefined roles, roles can be customized to tightly control read-only or editing access to permissions around policy creation, auditing, vulnerability management, etc. The roles and scopes can be applied to certain elements of the Aqua admin console as well as application scopes; for example who has access to DockerHub, registries, Kubernetes Clusters, etc. Permissions can also be applied to monitor and secure all network connections with the workload firewall that prevents unauthorized network connections and nano-segmentation of the network to observe the relationship between workloads. So for example, a developer from Team A will have visibility into vulnerabilities and issues in Team A's images, but will not be able to see or alter security policies, while a global compliance officer might see reports and audit events across all applications, but will not be able to change runtime policies. Aqua Enterprise provides the following predefined roles: ● Administrator - full access to Aqua operations and system resources ● Auditor - Includes read-only permissions to a limited set of Aqua UI pages and API calls ● KubeEnforcer - has REST API permissions for KubeEnforcer utilities only ● Scanner - for Scanner utility user only. ● Vulnerability Operator - read-only access to images and scan results ● Vulnerability Shield (vShield) Operator - Includes all permissions of the Vulnerability Operator, as well as: create vShields (and other Container Runtime Policies) ● Custom, user-defined roles with granular access definition to screens and APIs
7.1.1 Define access needs for each role, including: ● System components and data resources that each role needs to access for their job ● Function Level of privilege required (for example, user, administrator, etc.) for accessing resources	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities	
7.1.3 Assign access based on individual personnel's job classification and function	
7.1.4 Require documented approval by authorized parties specifying required privileges	
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: ● **7.2.1** Coverage of all system components ● **7.2.2** Assignment of privileges to individuals based on job classification and function ● **7.2.3** Default "deny-all" setting ● **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties	

For more information on how to comply with Requirement 7

Aqua's documentation ›

RBAC Overview ›

User Authentication ›



Details

* Name: Vulnerability Operator

Description: View-only permissions for images and scan results; permission to acknowledge

Access: [✓ UI & API] API Only

Permission Set

□ Full Permission

4 Categories	Edit	View Only	Not Set
› Policies	1/5	1/5	3/5
⌄ Assets	0/7	6/9	3/9
Dashboard	○	●	○
Risk Explorer		●	○
Images	○	●	○
Host Images	○	●	○
Functions	○	●	○
Enforcers	○	○	●
Containers		●	○
Services	○	○	●

Requirement 8

Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems can be traced to known and authorized users and processes.

PCI-DSS Requirement	How Aqua Helps
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data	The use of all Aqua functionality (via the UI, the REST APIs, or the command line) requires user login and authentication, which is usually implemented using SAML and single-sign-on via Okta, Auth0, or OneLogin. Combined with Aqua's Multi-Application Role-Based Access Control (RBAC) feature, admins can support environments with multiple teams working on different projects, with different sets of system resources. RBAC allows system administrators to precisely control, for all users: ● What actions the user can perform on Aqua ● Which system resources the user can view or edit (create, modify, and delete) inside Aqua
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	When creating a new user, the Aqua admin can check "User must change password at next login". The new PW will compliance with the configuration in the Authentication section

For more information on how to comply with Requirement 8

Aqua's documentation ›   RBAC Overview ›   User Authentication ›

Requirement 9

Restrict physical access to cardholder data

PCI-DSS Requirement

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

How Aqua Support this requirement?

Aqua is a self-hosted or a SaaS solution so this requirement is not relevant.

Requirement 10

Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong.

PCI-DSS Requirement	How Aqua Helps
10.1 Implement audit trails to link all access to system components to each individual user	Aqua generates granular audit trails of all access activity, scan events and coverage, Linux, Docker and Kubernetes commands, container activity, secrets activity, system events, and cloud account misconfigurations. Also, it provides full user accountability and controlled super-user permissions.
10.2 Implement automated audit trails for all system components to reconstruct specific events	Aqua admin can use pre-built alerts and reports for key compliance mandates including PCI-DSS
10.3 Record at least the following audit trail entries for all system components for specific event: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6** Identity or name of affected data, system component, or resource	All audit messages generated by Aqua Enforcers are sent to the Aqua server and are available from the console's audit screen. Admins can also configure forwarding of events to external SIEM and analytics tools, such as Splunk, ArcSight, AWS CloudWatch, Datadog, Elasticsearch, Sumo Logic, and more. The audit display results appear in table format per time, audit type, and provides a brief description
10.5 Secure audit trails so they cannot be altered	Use Aqua's Multi-application role-based control and FIM protection to ensure that the current audit trail files are protected from unauthorized modifications via access control mechanisms, and network segregation. Administrators can precisely control which system resources the user can view or edit (create, modify, and delete) inside the Aqua platform

For more information on how to comply with Requirement 10

Aqua's documentation ›

RBAC Overview ›

User Authentication ›

Audit ›

Log Management ›

Requirement 11

Regularly test security systems and processes

System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI-DSS Requirement	How Aqua Helps
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel	Aqua can be configured to scan all registered images and hosts regularly (for example, nightly). This will ensure that your cloud native assets are scanned at least daily for the latest security issues
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, & alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date	Aqua audits the activity in your cloud native environment and blocks any prohibited activities in runtime. Within Aqua, one or more runtime policies can be configured to restrict the runtime activities of workloads according to your organization's security requirements. Aqua can be used to monitor or block any suspicious behavior in the workload's file system and manages network communication to and from it
Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly	Aqua's Drift Prevention (Runtime control) enforces immutability and detects any unapproved changes to workloads. Aqua Protects high-value information, such as sensitive data and intellectual property. Aqua provides File Integrity Monitoring capability that monitors files and directories for read, write, and modify operations; System Integrity Protection, that ensures that Linux OS parameters and Windows Registry settings are not tampered with; and Forensics capabilities that audit users, processes, network activity, and full command line arguments

For more information on how to comply with Requirement 11

Aqua's documentation ›

Host Assurance Policies ›

Proactive Risk Management ›

Runtime Policies ›

Requirement 12

Maintain a policy that addresses information security for all personnel

A firm security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel with access to the cardholder data environment should be aware of data sensitivity and their responsibilities for protecting it.

PCI-DSS Requirement	How Aqua Helps
12.2 Implement a risk-assessment process that: ● Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), ● Identifies critical assets, threats, and vulnerabilities ● Results in a formal, documented analysis of risk	The Aqua platform provides continuously updated vulnerability data and a full picture of the runtime environment. A risk-based insights interface automatically considers risk-related contextual factors, such as exploitability and their presence within running workloads. It allows teams to prioritize vulnerabilities for remediation and mitigation. Aqua's Risk Explorer visualizes risky components in Kubernetes clusters, allowing further identification of risk due to vulnerabilities, exposed secrets, bad configuration, and network connections

For more information on how to comply with Requirement 12

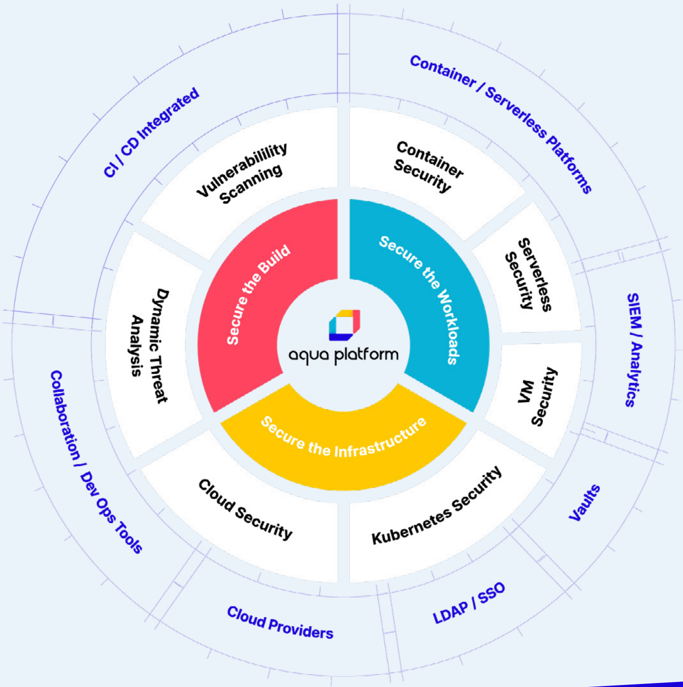
Aqua's documentation ›

Vulnerabilities Screen Operations ›

Reactive Risk Management ›

Aqua Security; The Complete Cloud Native Security Platform

Aqua Security helps organizations to secure their cloud native applications and infrastructure. Aqua bridges the gap between DevOps and security, promoting business agility, and accelerating digital transformation. Aqua's platform provides full visibility and security automation across the entire application lifecycle, using a modern zero-touch approach to detect and prevent threats while simplifying regulatory compliance. Working across all clouds and platforms and secured workloads that run across containers, VMs, and serverless functions. Aqua is the only vendor entirely dedicated to cloud native security. It provides the complete approach to protecting cloud native applications: securing the Build, infrastructure, and workloads that makeup cloud native applications.



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.