**Aqua – Runtime Policy – Enforcement Mode Document V1.0**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 03-Oct-24 | Initial Draft | NA | Mihirkumar |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Mihirkumar Jani | Consultant | Author | 03-Oct-24 |
| Kannan Kuppusamy | Technical Lead | Reviewer | 15-Nov-24 |
| Felix Jebamani | Lead Consultant | Reviewer | 15-Nov-24 |
| Salama, Omar | Lead | Reviewer | 19-Dec-24  [CST-1252](https://jira.esteeonline.com/browse/CST-1252) |
| Jamshid Abedi | Executive Director | Approver |  |

**Table of Contents**

[Objective of the Document 3](#_Toc182588966)

[1.0 Purpose and Scope 3](#_Toc182588967)

[2.0 AquaSec Enforcer Architecture Diagram 4](#_Toc182588968)

[3.0 AquaSec Runtime Enforcer Mode: 4](#_Toc182588969)

[Implementation Steps to ‘Enforce’ mode: 5](#_Toc182588970)

[Step 1: 5](#_Toc182588971)

[Step 2: 5](#_Toc182588972)

[Step 3: 5](#_Toc182588973)

[Aqua Runtime Enforcement Mode 5](#_Toc182588974)

[4.0 Aqua Enforce mode Process Workflow – Diagram: 6](#_Toc182588975)

[5.0 Reference document: 7](#_Toc182588976)

# Objective of the Document

This document outlines the process for enabling Enforcement mode on Aqua runtime controls, which helps enhance the security and resilience of Azure AKS cluster environments.

# 1.0 Purpose and Scope

The purpose of enabling Enforcement mode on Aqua runtime controls in Aqua SaaS is to prevent actions or activities when violations occur, thereby strengthening security in Azure AKS cluster environments through Aqua SaaS container security controls.

Enforce mode will apply to all of Estee Lauder Companies Inc. (the “Company”) Azure AKS clusters environment.

# 2.0 AquaSec Enforcer Architecture Diagram

Enforcers are the AquaSec components that provide enforcement (securing workloads during runtime) and other related functionality. Enforcement includes but is not limited to the following activities:

* Deciding, based on assurance compliance findings, whether to allow or block workloads (containers) from running
* Monitoring, restricting, and/or blocking specific runtime activities of workloads as determined by the organization's Runtime and Firewall Policies
* Reporting and logging audit events for the aforementioned activities and findings

Figure 1: High-level architecture diagram

A diagram of a cluster

Description automatically generated

# 3.0 AquaSec Runtime Enforcer Mode:

Through ‘Enforce’ or enforcement mode, we can stop the action/activity, in the event that a violation occurs on the specific control where the ‘Enforce’ mode is enabled.

Initially, identify the Aqua controls to enable ‘Enforce’ mode, using insights from past event alert reports and internal discussions within the cloud security team.

We will initiate discussions with the following teams and stake holder before enabling ‘Enforce’ mode on the Aqua control policy.

* DevSecOps Team
* CloudOps Team
* SRE team
* The AKS cluster teams and the AKS cluster owner or the application owner.

## Implementation Steps to ‘Enforce’ mode:

## Step 1:

Before enabling the ‘Enforce’ mode, we should inform and update the respective teams and the AKS cluster owner and/or the application owner.

## Step 2:

Will deploy phase wise enforcement mode on AKS clusters and keep the added AKS clusters under observation and then take immediate actions if required.

We can provide exemptions based on ServiceNow request which are to be submitted by the AKS cluster owner and/or the application owner.

## Step 3:

Phase wise implementation details:

Phase 1: Test AKS clusters

AKS cluster name: ‘AKS-AM-EastUS-NP-SREDO’

Phase 2: Non-Prod AKS clusters. [Will identify less critical AKS cluster and add the cluster in the enforce mode control policy, will follow ascending order of criticality (Low to High)]



Phase 3: Prod AKS clusters. [Will identify less critical AKS cluster and add the cluster in the enforce mode control policy, will follow ascending order of criticality (Low to High)]



## Aqua Runtime Enforcement Mode

* Keep the added AKS cluster under observation and take required actions immediately if any impact happens.
* We can provide exemptions based on ServiceNow request which are to be submitted by the AKS cluster owner/the application owner.

# 4.0 Aqua Enforce mode Process Workflow – Diagram:

Enable Enforce mode of Aqua runtime control

Identify  
less critical AKS cluster

Download and analyze old events reports of the cluster of 'Block Non-compliant Images' control

Remediate all events and make the AKS cluster clean

Before enable enforce mode on the less critical AKS cluster, needs to inform respective stack holders

Enable enforce mode on the less critical AKS cluster, we can provide exemption  
base on ServiceNow request if required

**Step 1**

**Step 2**

**Step 3**

**Step 4**

**Step 5**

**Step 6**

will  
follow ascending order of criticality (Low to High) and add AKS cluster in the control policy, and repeat the Step 1 to Step 6

# 5.0 Reference document:

<https://confluence.esteeonline.com/display/CST/Runtime+Policies+and+Controls?preview=/568779443/568779487/Block%20Non-compliant%20Images.pdf>

<https://confluence.esteeonline.com/display/CST/Runtime+Policies+and+Controls?preview=/568779443/568779485/Block%20Unregistered%20Images.pdf>

<https://confluence.esteeonline.com/display/CST/Runtime+Policies+and+Controls?preview=/568779443/568779484/Drift%20Prevention.pdf>

<https://confluence.esteeonline.com/display/CST/Kubernetes+Assurance+Policies+and+Controls?preview=/568779453/568779482/Sensitive%20Data%20%26%20Secret%20Data%20Control%20-%20V%201.0.pdf>

Note: FAQ document link will update after review and approval.