Aqua Security App

This application has been developed by Aqua Security. For technical questions, please contact Aqua Security at community.plugins@aquasec.com.

Product Description: Aqua Security's Cloud Native Security Platform runs on-premise or in the cloud to secure cloud native workloads -- from development in a CI/CD pipeline to production in runtime, providing granular visibility into container activity to detect and prevent suspicious activity and attacks. Aqua allows you to configure automated security controls to enforce container immutability in runtime, and even provides "compliant by default" templates to facilitate compliance with less hassle.

App description: The Aqua Security App for Sumo Logic provides users with a holistic cyber-security monitoring and forensics solution for containerized and cloud native environments.

The app consists of the following four dashboards:

Dashboard	Description
Overview	Provides a comprehensive summary of security events, risks and vulnerabilities in your containerized and cloud native environment, including suspicious and unauthorized runtime activities, as well as images impacted with severe vulnerabilities and compliance issues. It also provides an overview of host compliance issues and nodes failing CIS benchmarks.
Image Security and Compliance	Provides detailed information about image scanning results and assurance events from Aqua such as image vulnerability, malware, exposed sensitive data and compliance issue findings.
Host Security and Compliance	Provides detailed information about nodes/hosts that failed to pass industry benchmarks such as CIS Kubernetes, Docker and Linux standards, as well as the company's custom compliance regulations.
Runtime Security	Provides detailed information about detected or blocked security events in runtime: • Unregistered or uncompliant images pushed to production • Unauthorized or suspicious programs or file activities • Unauthorized or suspicious network activity

Aqua Page

Aqua Security's Cloud Native Security Platform runs on-premise or in the cloud to secure cloud native workloads -- from development in a CI/CD pipeline to production in runtime, providing granular visibility into container activity to detect and prevent suspicious activity and attacks.

The Aqua Security App for Sumo Logic provides users with a holistic cyber-security monitoring and forensics solution for containerized and Cloud Native applications.

Log Types

The Aqua Security app processes the following logs:

- Aqua image scanning and assurance test logs
- Aqua host scanning and assurance test logs, including industry benchmarks like CIS Linux, CIS Kubernetes, etc.
- Aqua runtime protection events, including detected and blocked events of malicious or suspicious runtime behavior. For example – an attempt to push an unregistered or non-compliant image, an attempt to run unauthorized or suspicious programs within a container, or unauthorized or suspicious network activity.

For more information please see the Aqua Documentation.

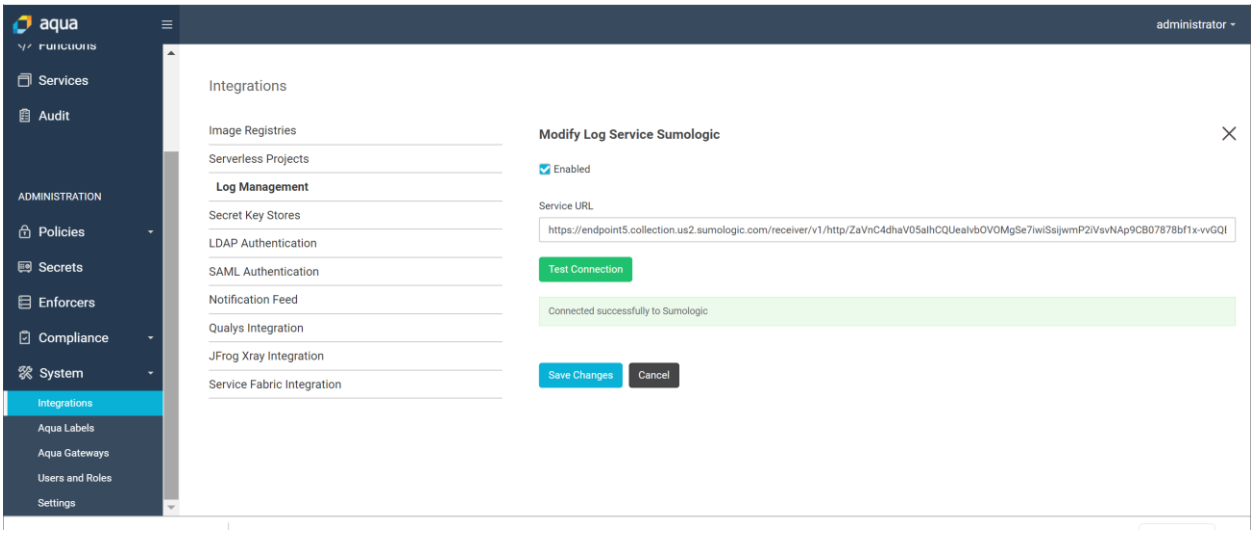
Collect Logs for the Aqua Security App

Aqua has a native integration with Sumo Logic. Take the following steps to connect your Aqua security solution to Sumo Logic:

1. Access your Sumo Logic instance and add a new HTTP Source Collection using the instructions documented on this page.

2. Access your Aqua server go to Settings->Integrations->Log Management->SumoLogic and enable this integration

3. You will be required to insert the HTTP Source URL that was generated by SumoLogic in step 1



4. You will be able to test the connection directly from the Aqua console. Make sure the connection works before you continue.

Sample Queries

Now that once you have established the HTTP Source Collector you start investigating security event. For example, using one of the following queries –

Use the following query to fetch all images that failed the image assurance policies:

```
_sourceCategory="aqua"
| json "type","action","result","category","image"
| parse "blocking\\\":*," as blocked
| where type="alert" and action="policy.failure" and category="image" and result>1
| count_distinct(image,blocked)
```

Use the following query to fetch all hosts that failed the host assurance policies:

```
_sourceCategory="aqua"
| json auto
| toLowerCase(user) as policy
|  where type="alert" and action="policy.failure" and policy="host.policy" and result>1
| count_distinct(image)
```

Use the following query to fetch all recent runtime security events:

```
_sourceCategory="aqua"
```

```
| json field=_raw "rule_type", "result", "category"
| where rule_type="runtime.policy" AND (result=2 or result=3)
| timeslice 1h
| count by _timeslice
```

Install the Aqua Security App and View the Dashboards

To install the app, do the following:

Locate and install the app you need from the Sumo Logic App Catalog. If you want to see a preview of the dashboards included with the app before installing, click Preview Dashboards.

1. From the App Catalog, search for and select the app.
2. To install the app, click Add to Library and complete the following fields.
    a. App Name. You can retain the existing name, or enter a name of your choice for the app.
    b. Data Source. Select either of these options for the data source.
        i. Choose Source Category and select the source category you set in the Collect Logs section (e.g. aqua).
        ii. Choose Enter a Custom Data Filter and enter a custom source category beginning with an underscore. Example: (_sourceCategory=MyCategory).
    c. Advanced. Select the Location in Library (the default is the Personal folder in the library) or click New Folder to add a new folder.
    d. Click Add to Library.

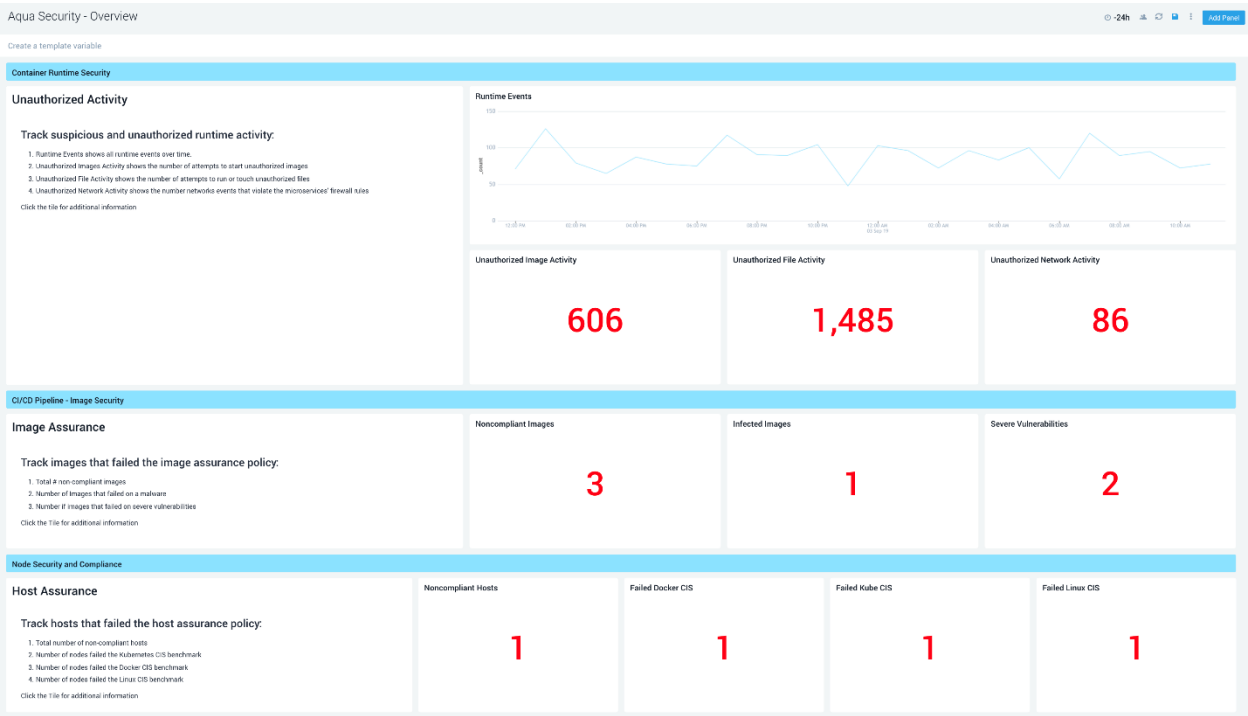
Once an app is installed, it will appear in your Personal folder, or another folder that you specify. From here, you can share it with your organization.

Panels will start to fill automatically. It's important to note that each panel slowly fills with data matching the time range query and received since the panel was created. Results won't immediately be available, but with a bit of time, you'll see full graphs and maps.

Aqua Security – Overview Dashboard

The Overview dashboard is a holistic dashboard designed to provide DevSecOps teams with a high-level overview of vulnerabilities and security events in their containerized and cloud native environments. It provides critical security insights at three dimensions –

- Runtime security events including unauthorized and suspicious runtime behavior
- Image vulnerabilities and risks throughout the CI/CD pipeline
- Node vulnerabilities, risks, and compliance

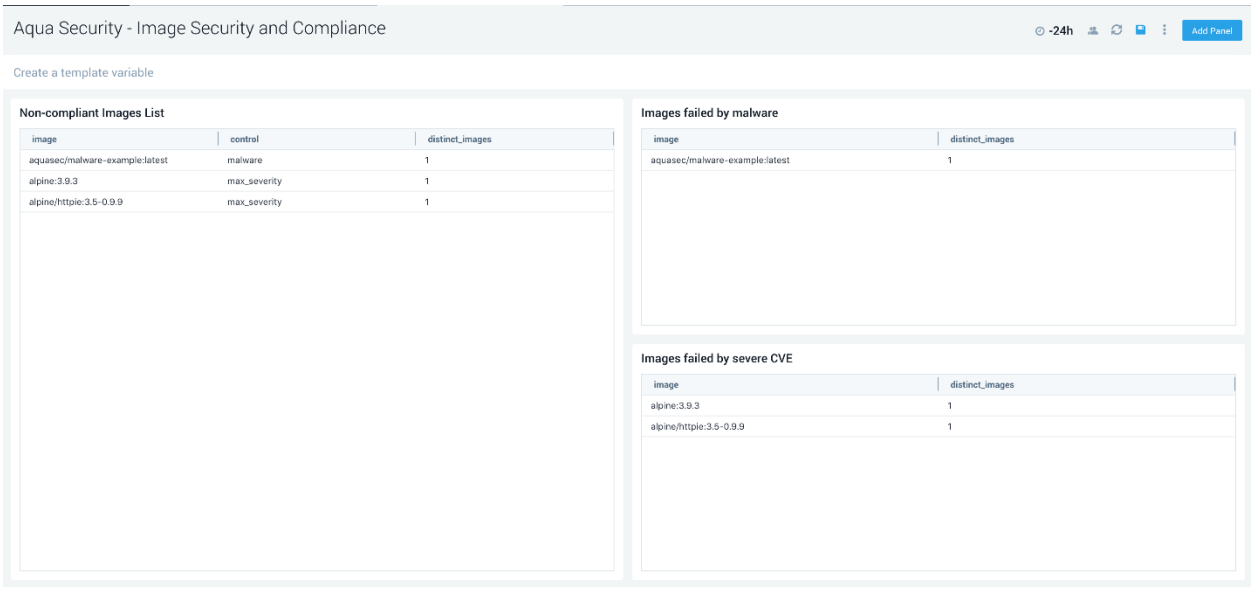


Use this dashboard to:

- Get a bird’s-eye view of vulnerabilities, risks, and security events across your cloud native environment
- Monitor and investigate runtime security events in real-time
- Monitor and manage risks and vulnerabilities in images
- Monitor and manage risks and vulnerabilities in nodes

Image Security and Compliance Dashboard

The Image Security and Assurance dashboard provides a high-level breakdown of the images that failed the security and compliance tests and the failure reasons.

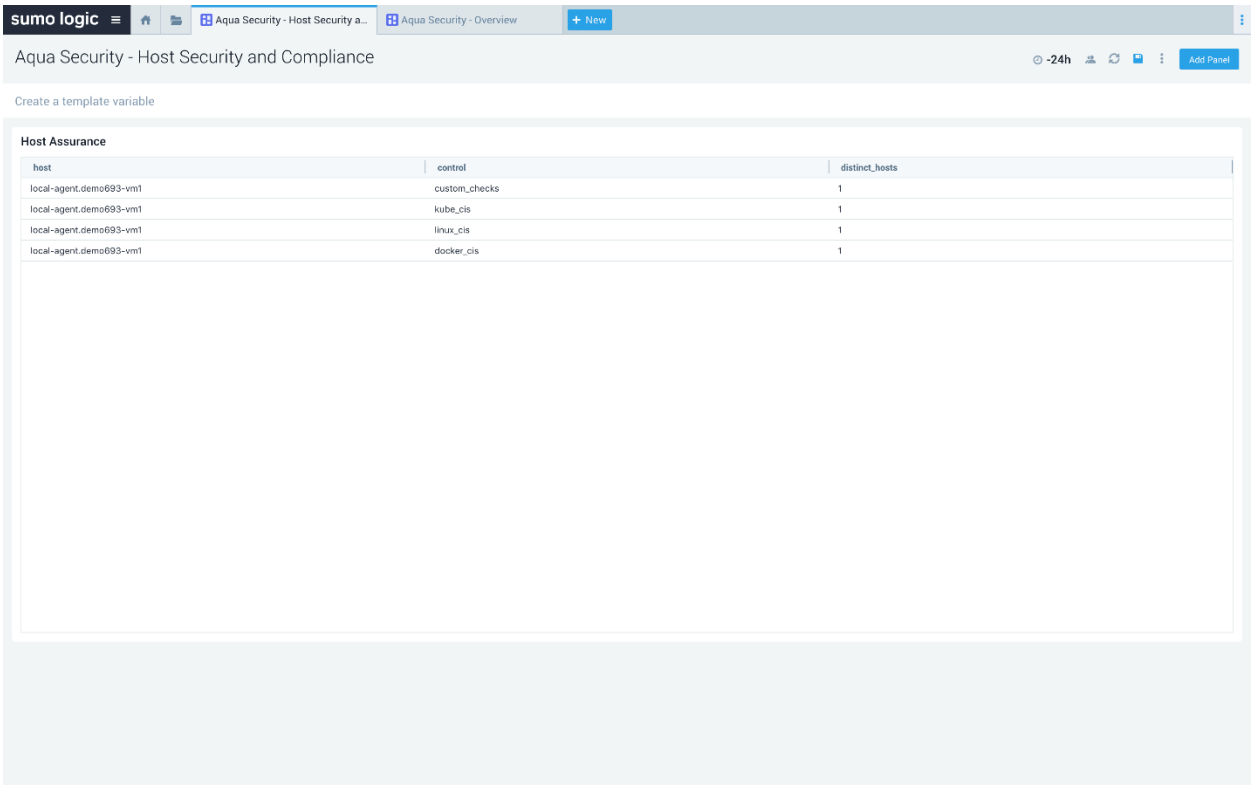


Use this dashboard to:

- See the list of images that failed to pass the security and compliance tests
- See which compliance test failed your images

Host Security and Compliance Dashboard

The Host Security and Assurance dashboard lists all hosts that failed the host security and compliance tests and provides insights into which tests or benchmarks have failed the host.

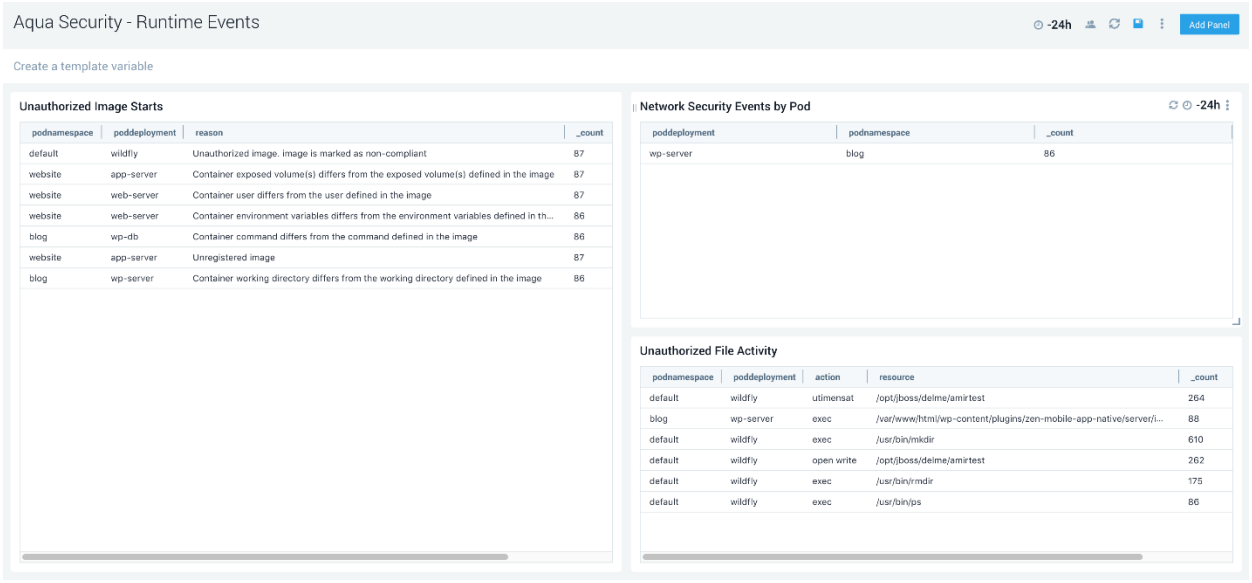


Use this dashboard to see the list of hosts that have failed security and compliance tests and that expose your applications to risks.

Runtime Events Dashboard

The Runtime Events dashboard provides details information about recent runtime security events. The dashboard contains three security events categories:

1. Unauthorized or unregistered images push to the cluster
2. Unauthorized or suspicious program execution or file access
3. Unauthorized or suspicious network activity across the cluster



Use this dashboard to:

- Monitor and respond to real-time threats and attacks
- Identify and manage rouge images
- Identify suspicious lateral movement or privilege escalation