Open Source and Commercial Vulnerability Scanning

A Cloud Native Security Case Study

Story Tweedie-Yates, Sr. Director Product Marketing

How to understand the decision process between open source and commercial

Cloud Native Security Case Study

The Decision Points; personal impact

The decision depends on your own needs and environment; there is no right or wrong

Time to value

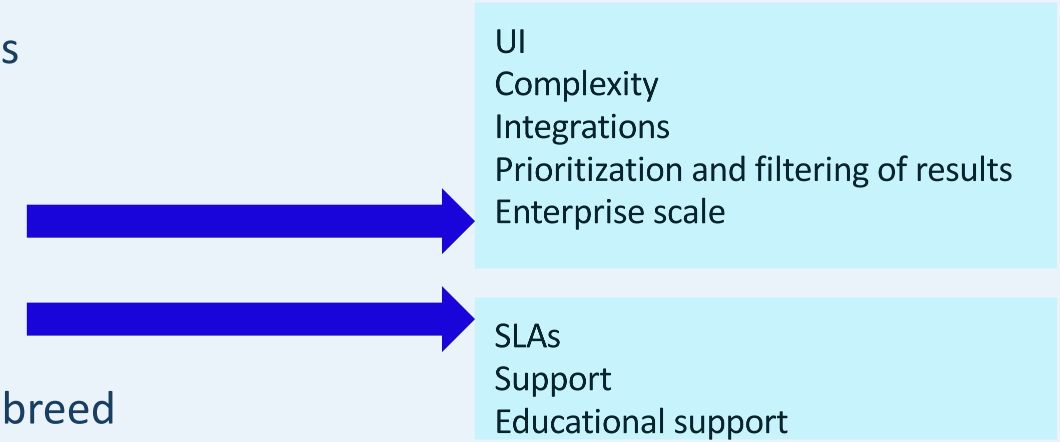
Fit with longer-term needs

Fit to purpose

Management overhead

Vendor guarantees

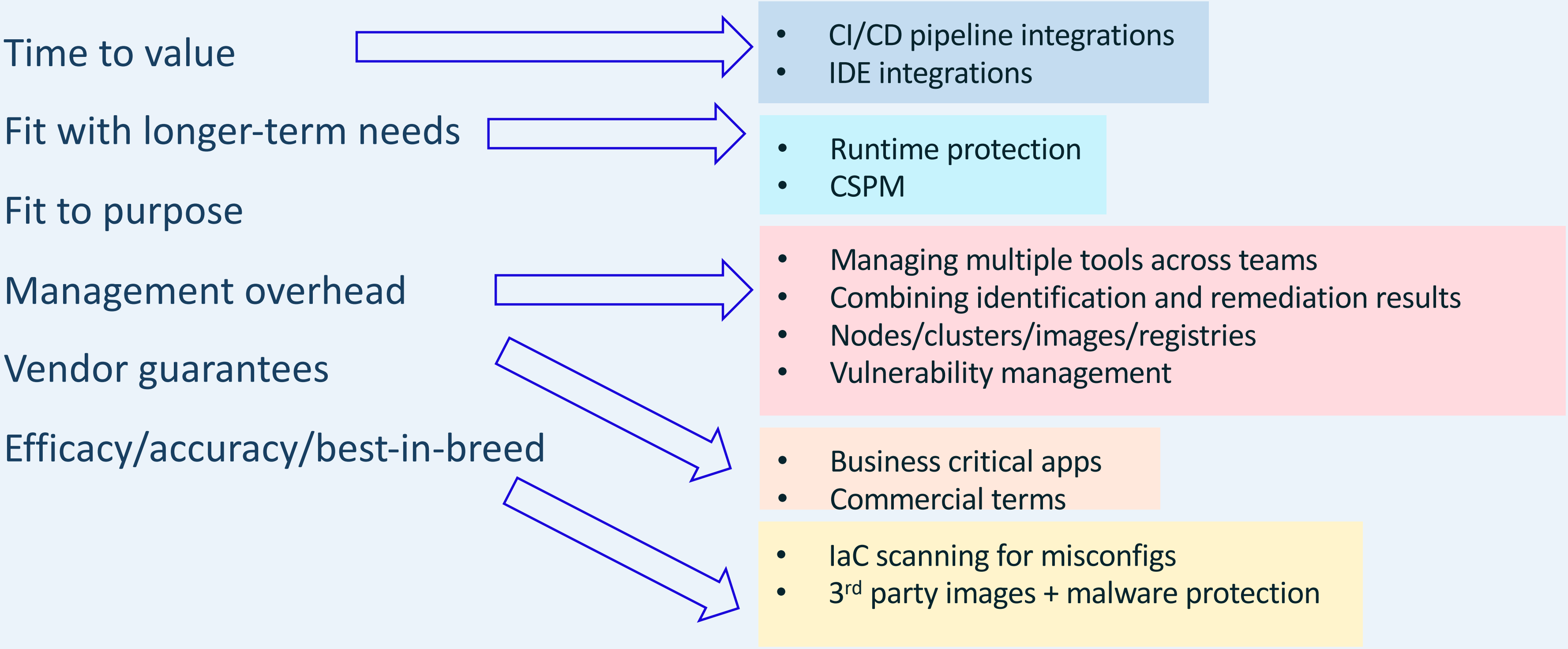
Efficacy/accuracy/best-in-breed



UI
Complexity
Integrations
Prioritization and filtering of results
Enterprise scale

SLAs
Support
Educational support

How personal impact applies to vulnerability scanning



Time to value

Fit with longer-term needs

Fit to purpose

Management overhead

Vendor guarantees

Efficacy/accuracy/best-in-breed

- CI/CD pipeline integrations
- IDE integrations

- Runtime protection
- CSPM

- Managing multiple tools across teams
- Combining identification and remediation results
- Nodes/clusters/images/registries
- Vulnerability management

- Business critical apps
- Commercial terms

- IaC scanning for misconfigs
- 3rd party images + malware protection

The Case Study

Use open source to get started with vulnerability scanning

aqua trivy

You are completing a cloud native security certification and courses and require a quick, easy scanning tool

You require vulnerability scanning for applications that are not business-critical

You will be working with less complex, less distributed architectures

Default scanner:

HARBOR GitLab ArtifactHUB

Use Aqua Enterprise when you need. . .

	aqua	aqua trivy
Lower management overhead for complex environments	Vuln. Mgmt: Actionable results, automation and a feedback loop	Command line and manually exporting into external visualization tool
Broadest security coverage	Also scans for standalone binaries	Will not scan files installed outside package managers
Meeting specific enterprise needs	Can be re-packaged by MSPs	Commercial licensing limitations
Continuous protection into runtime	Option for follow-up runtime policy	Fail or allow CI job based on vulnerability data

Use Aqua Enterprise when you need holistic vulnerability management

Actionable results and a feedback loop

aqua

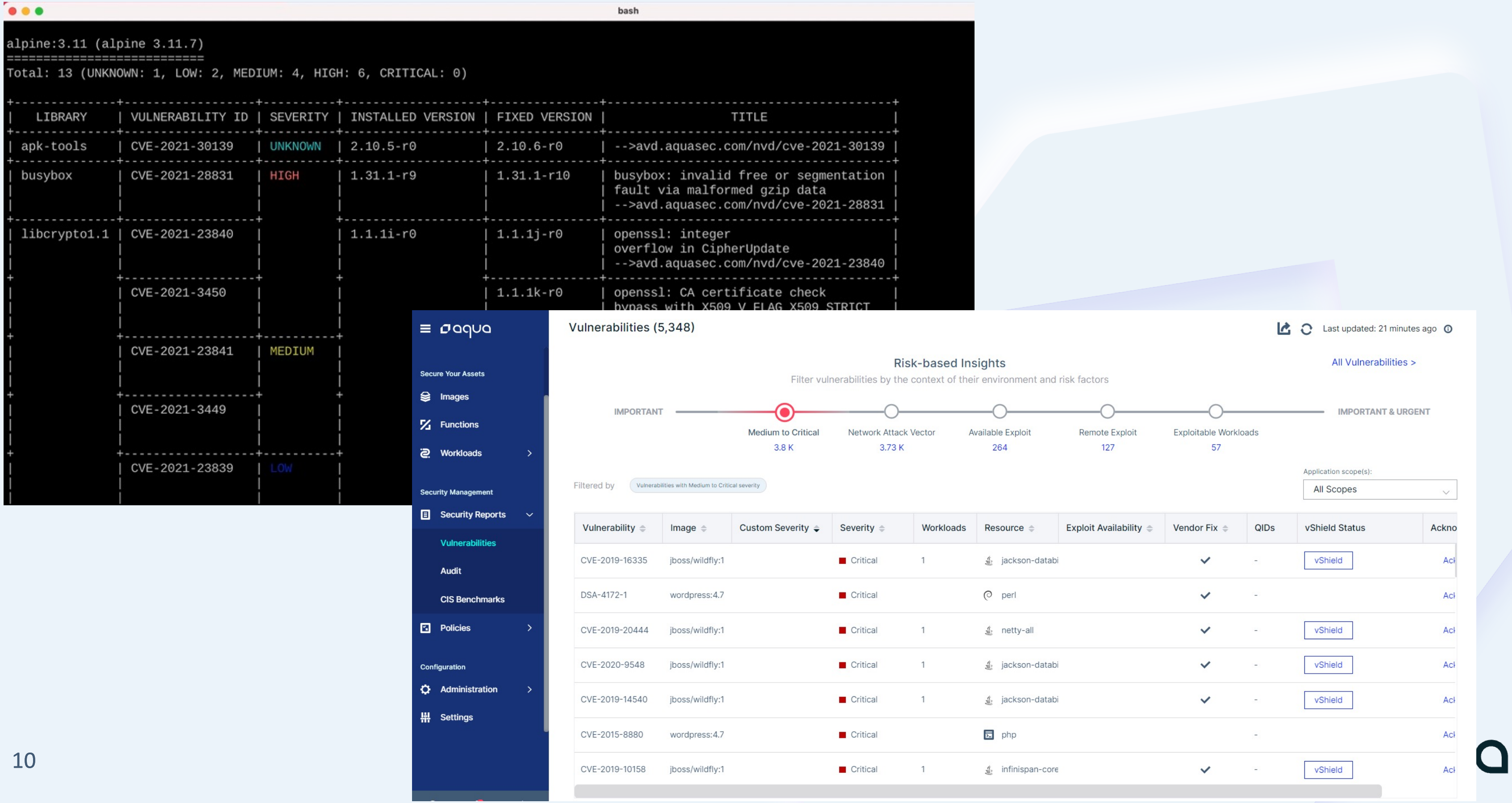
- Risk-based insights for visualization in relation to relevance and exploitability
- vShield with pre-built policies to mitigate without fixing or patching
- A feedback loop enables further prioritization of highest impact vulnerabilities for remediation

aqua trivy

- Vulnerabilities filtered in command line
- Integration with external tool required to visualize outside of the command line
- Exporting to a UI requires exporting and uploading

"Don't take this from us"
– SRE lead, Trivy user

Demo



```
alpine:3.11 (alpine 3.11.7)
===========================
Total: 13 (UNKNOWN: 1, LOW: 2, MEDIUM: 4, HIGH: 6, CRITICAL: 0)

+--------------+------------------+----------+-------------------+---------------+-----------------------------------------+
|   LIBRARY    | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |                  TITLE                  |
+--------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| apk-tools    | CVE-2021-30139   | UNKNOWN  | 2.10.5-r0         | 2.10.6-r0     | -->avd.aquasec.com/nvd/cve-2021-30139   |
+--------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| busybox      | CVE-2021-28831   | HIGH     | 1.31.1-r9         | 1.31.1-r10    | busybox: invalid free or segmentation   |
|              |                  |          |                   |               | fault via malformed gzip data           |
|              |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-28831   |
+--------------+------------------+          +-------------------+---------------+-----------------------------------------+
| libcrypto1.1 | CVE-2021-23840   |          | 1.1.1i-r0         | 1.1.1j-r0     | openssl: integer                        |
|              |                  |          |                   |               | overflow in CipherUpdate                |
|              |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-23840   |
+              +------------------+          +                   +---------------+-----------------------------------------+
|              | CVE-2021-3450    |          |                   | 1.1.1k-r0     | openssl: CA certificate check           |
|              |                  |          |                   |               | bypass with X509_V_FLAG_X509_STRICT     |
|              |                  |          |
+              +------------------+----------+
|              | CVE-2021-23841   | MEDIUM   |
|              |                  |          |
|              |                  |          |
+              +------------------+          +
|              | CVE-2021-3449    |          |
|              |                  |          |
|              |                  |          |
+              +------------------+----------+
|              | CVE-2021-23839   | LOW      |
|              |                  |          |
```

Vulnerabilities (5,348)

Last updated: 21 minutes ago

Risk-based Insights

Filter vulnerabilities by the context of their environment and risk factors

All Vulnerabilities >

IMPORTANT — IMPORTANT & URGENT

Medium to Critical	Network Attack Vector	Available Exploit	Remote Exploit	Exploitable Workloads
3.8 K	3.73 K	264	127	57

Filtered by: Vulnerabilities with Medium to Critical severity

Application scope(s): All Scopes

Vulnerability	Image	Custom Severity	Severity	Workloads	Resource	Exploit Availability	Vendor Fix	QIDs	vShield Status	Ackno
CVE-2019-16335	jboss/wildfly:1		🟥 Critical	1	jackson-databi		✓	-	vShield	Ack
DSA-4172-1	wordpress:4.7		🟥 Critical		perl		✓	-		Ack
CVE-2019-20444	jboss/wildfly:1		🟥 Critical	1	netty-all		✓	-	vShield	Ack
CVE-2020-9548	jboss/wildfly:1		🟥 Critical	1	jackson-databi		✓	-	vShield	Ack
CVE-2019-14540	jboss/wildfly:1		🟥 Critical	1	jackson-databi		✓	-	vShield	Ack
CVE-2015-8880	wordpress:4.7		🟥 Critical		php			-		Ack
CVE-2019-10158	jboss/wildfly:1		🟥 Critical	1	infinispan-core		✓	-	vShield	Ack

Management overhead is a real price tag

Complex build pipeline **spanning multiple registries and teams?**

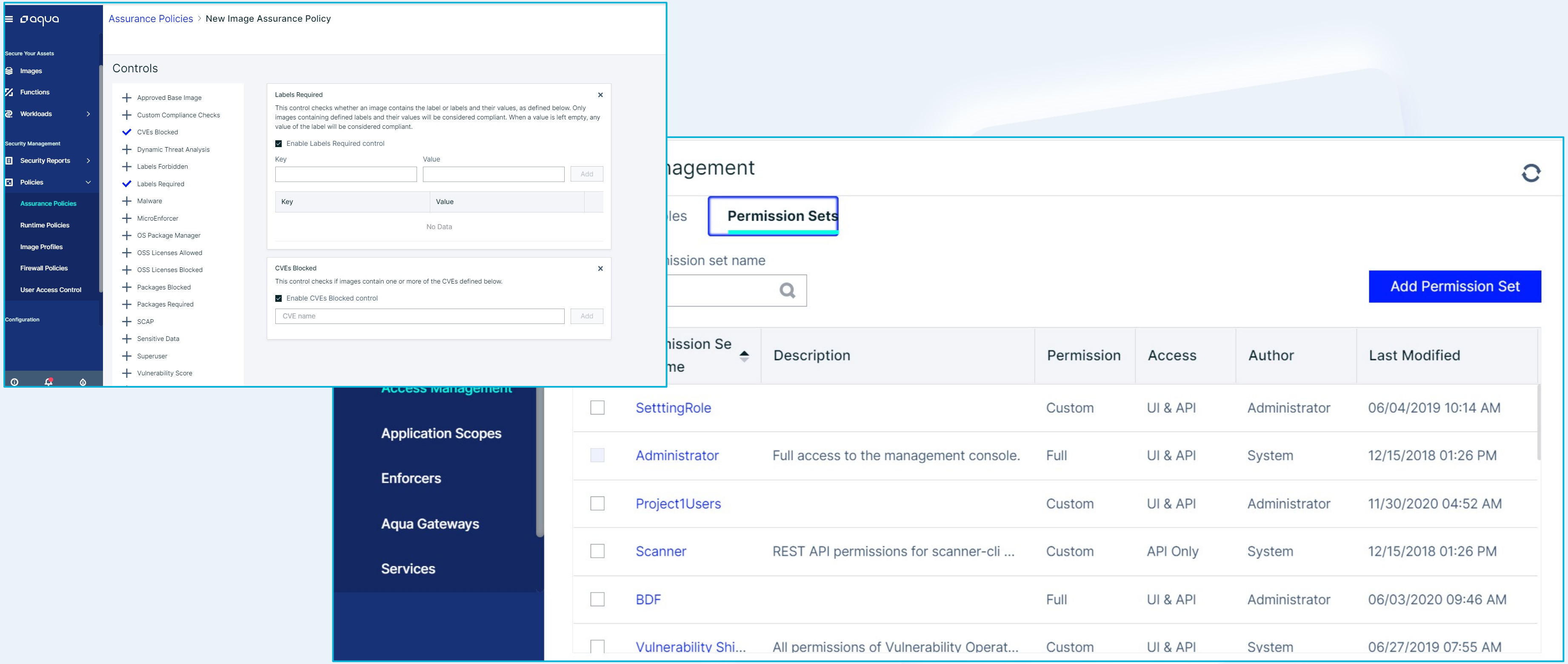
Concerned with management overhead of an entire suite of security tools?

Requirement to combine scanning and remediation **results into an external system?**

Are you protecting **business-critical apps?**

aqua	aqua trivy
• Data aggregation and assurance policies across all systems	• No default aggregation of data into a UI
• Details available directly in the UI & RBAC	• See detailed data info in separate screen with AVD
• OOTB integrations with 3rd party tools	• Basic plugin capabilities
• Runtime policies from drop-down menu	• Rego scripts for OPA policies based on vuln. data

Demo



Labels Required

This control checks whether an image contains the label or labels and their values, as defined below. Only images containing defined labels and their values will be considered compliant. When a value is left empty, any value of the label will be considered compliant.

☑ Enable Labels Required control

Key:

Value:

Key	Value
No Data	

CVEs Blocked

This control checks if images contain one or more of the CVEs defined below.

☑ Enable CVEs Blocked control

CVE name:

ission set name:

	ission Se me	Description	Permission	Access	Author	Last Modified
□	SetttingRole		Custom	UI & API	Administrator	06/04/2019 10:14 AM
□	Administrator	Full access to the management console.	Full	UI & API	System	12/15/2018 01:26 PM
□	Project1Users		Custom	UI & API	Administrator	11/30/2020 04:52 AM
□	Scanner	REST API permissions for scanner-cli ...	Custom	API Only	System	12/15/2018 01:26 PM
□	BDF		Full	UI & API	Administrator	06/03/2020 09:46 AM
□	Vulnerability Shi...	All permissions of Vulnerability Operat...	Custom	UI & API	System	06/27/2019 07:55 AM

But open source has great value for the right use-cases

GitLab Product Manager Sam White on their choice of Trivy for Auto DevOps:

“When we see an enhancement or we hear a need from our customers that’s shared by the Trivy product as well, we can push that upstream into the open source project and make that available for anyone and everyone who’s using Trivy, regardless of whether or not they’re using GitLab.”

Complex build pipeline spanning multiple registries and teams

"How can we patch more than 100,000 vulnerability findings in images across more than 1,300 image repositories, without chasing around 100 project teams and 1,700 engineers?"

- Medium article 3rd party example of real effort involved with staying open source

Broad security coverage requires more than vulnerability scanning

Does your security team require the **most accuracy possible?**

Is your security team responsible for **malware and an array of threats?**

Do any of your **images come from third parties** or public libraries?

Do you want a production pipeline **clean from more than vulnerabilities**?

aqua

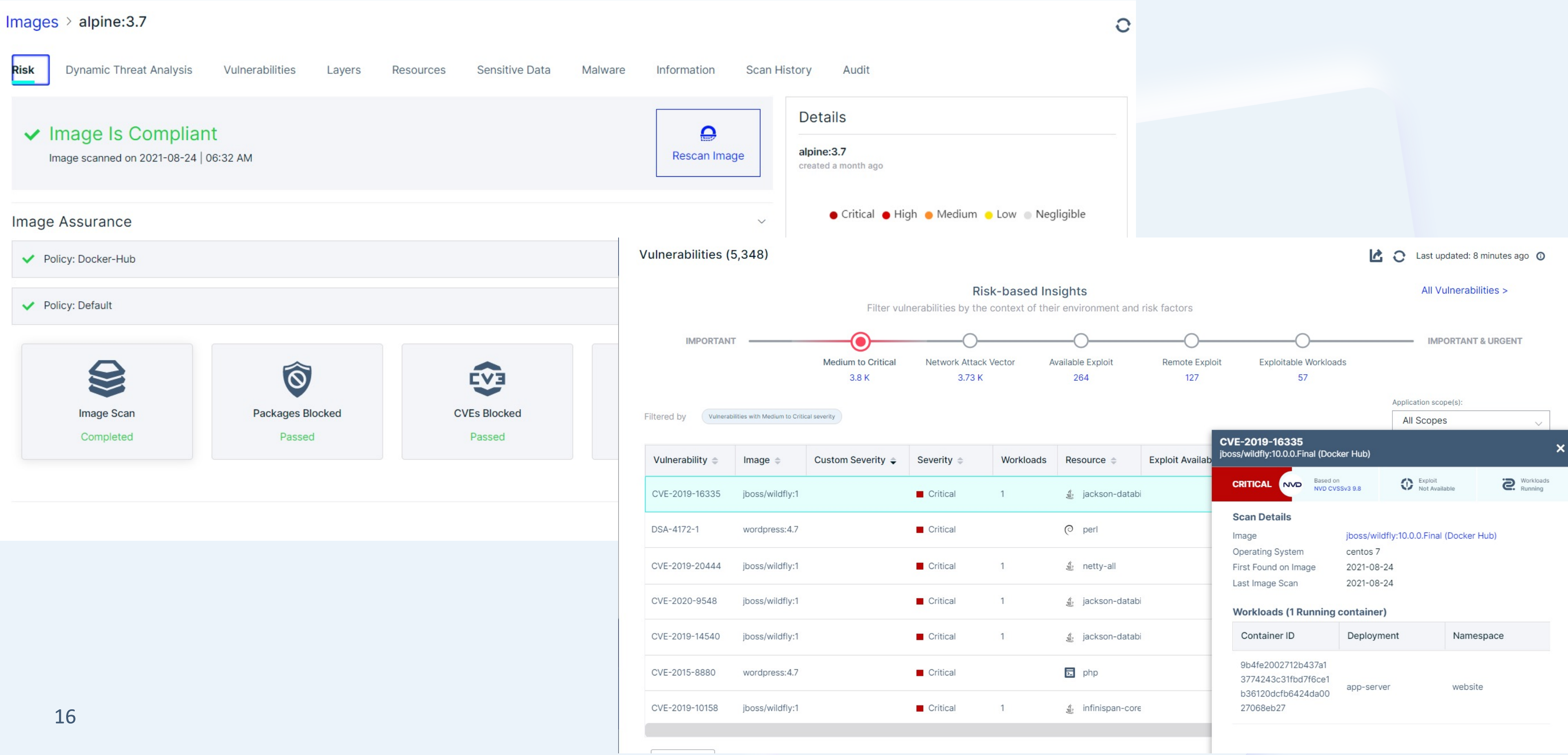
- Aqua Enterprise uses CyberCenter5, curated by our threat research team
- Scans for malware
- Scans serverless functions
- A container sandbox to identify supply chain attacks

aqua trivy

- Aqua Trivy's Aqua AVD is available publicly
- Vulnerability scanning

aqua tracee

Demo



Images > alpine:3.7

✓ Image Is Compliant

Image scanned on 2021-08-24 | 06:32 AM

Details

alpine:3.7

created a month ago

● Critical ● High ● Medium ● Low ● Negligible

Image Assurance

✓ Policy: Docker-Hub

✓ Policy: Default

Image Scan: Completed

Packages Blocked: Passed

CVEs Blocked: Passed

Vulnerabilities (5,348)

Last updated: 8 minutes ago

Risk-based Insights

Filter vulnerabilities by the context of their environment and risk factors

IMPORTANT	Medium to Critical	Network Attack Vector	Available Exploit	Remote Exploit	Exploitable Workloads	IMPORTANT & URGENT
	3.8 K	3.73 K	264	127	57	

Filtered by: Vulnerabilities with Medium to Critical severity

Application scope(s): All Scopes

Vulnerability	Image	Custom Severity	Severity	Workloads	Resource	Exploit Availab
CVE-2019-16335	jboss/wildfly:1		🟥 Critical	1	jackson-databi	
DSA-4172-1	wordpress:4.7		🟥 Critical		perl	
CVE-2019-20444	jboss/wildfly:1		🟥 Critical	1	netty-all	
CVE-2020-9548	jboss/wildfly:1		🟥 Critical	1	jackson-databi	
CVE-2019-14540	jboss/wildfly:1		🟥 Critical	1	jackson-databi	
CVE-2015-8880	wordpress:4.7		🟥 Critical		php	
CVE-2019-10158	jboss/wildfly:1		🟥 Critical	1	infinispan-core	

CVE-2019-16335

jboss/wildfly:10.0.0.Final (Docker Hub)

CRITICAL | NVD Based on NVD CVSSv3 9.8 | Exploit Not Available | Workloads Running

Scan Details

Image	jboss/wildfly:10.0.0.Final (Docker Hub)
Operating System	centos 7
First Found on Image	2021-08-24
Last Image Scan	2021-08-24

Workloads (1 Running container)

Container ID	Deployment	Namespace
9b4fe2002712b437a1 3774243c31fbd7f6ce1 b36120dcfb6424da00 27068eb27	app-server	website

To summarize

Decision points are not mutually exclusive . . . just doing the decision-point exercise that matters

In general, you are going to get more management overhead with open source, but quicker time to value

Vulnerability scanning should not be viewed in a vacuum . . . e.g. Trivy has IaC capabilities as well

Open source is being used in production regularly

Thank You!