

The three pillars of Cloud Native Security

protect supply chain,
infrastructure and run time

Thomas Laubrock
Solution Architect, Aqua Security



Let's Talk Cloud Native



Vulnerability
Scanning

Infrastructure as Code

CSPM

Azure

DevOps

DevSecOps

Runtime
Protection

Compliance

Zero Trust

CNAPP

Containers

CWPP

Custom Code

AWS

Multi Cloud

CI/CD

3rd Party Code

Software Supply Chain

Docker

Code Repositories

Visibility

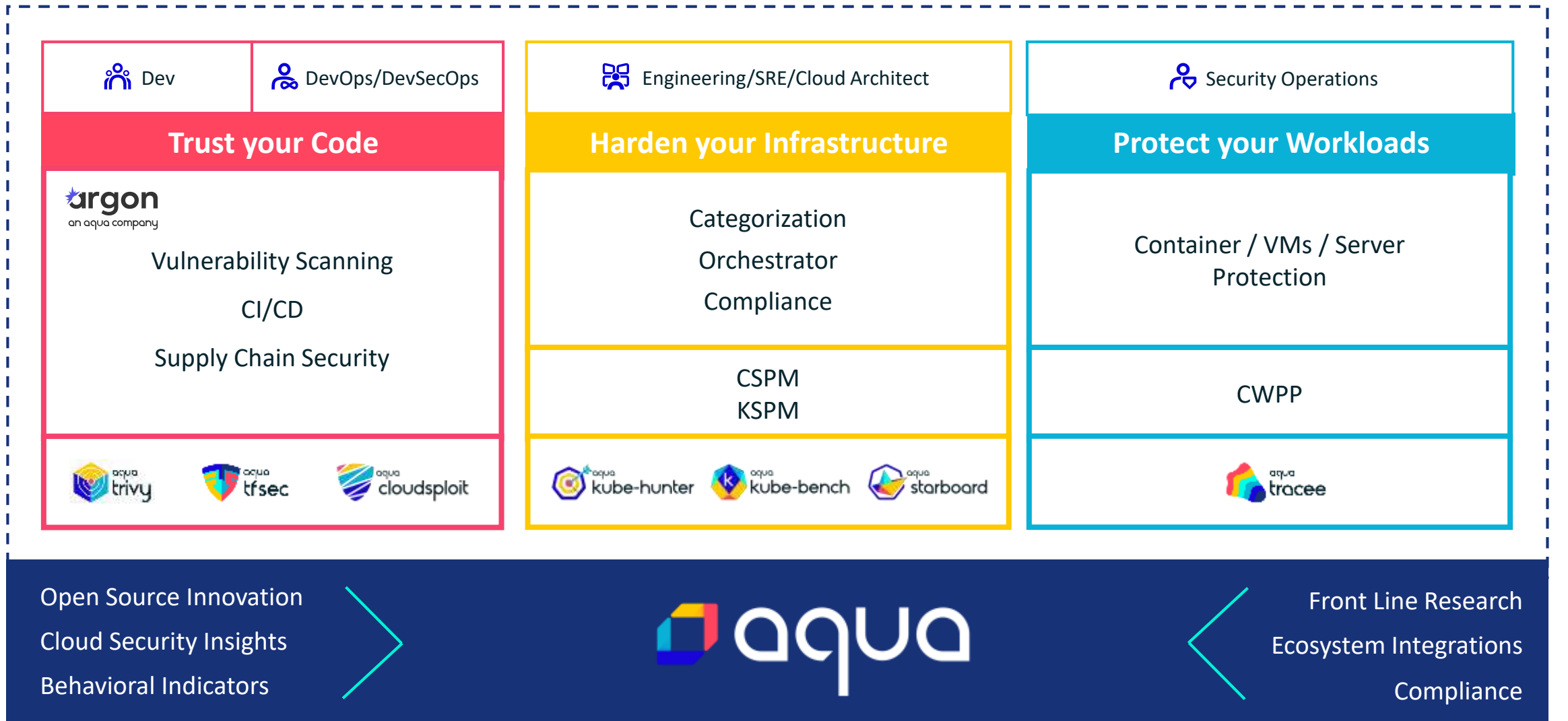
Open Source
security tools

Kubernetes

GCP

We **stop** cloud native attacks

The Cloud Native Application Protection Platform (CNAPP)



Universal Scanner – SCA, IaC, Sensitive Data, Licenses, dockers, etc...

Add files via upload #5

Open saargon wants to merge 2 commits into main from saargon:patch-5

Conversation 5 Commits 2 Checks 1 Files changed 3 +46 -1

saargon commented on Jun 16
No description provided.

saargon added 2 commits 2 months ago

- ✓ Add files via upload Verified ✓ 7c26c23
- ✓ Update aquasoc.yml Verified ✓ 90d9008

github-actions bot reviewed on Jun 16

View changes

```
secrets2/insecure-db.tf
1 + resource "aws_db_instance" "default" {
2 +   allocated_storage = 10
3 +   engine             = "mysql"
4 +   engine_version     = "5.7"
5 +   instance_class     = "db.t3.micro"
6 +   name               = "mydb"
7 +   username           = "foo"
8 +   password           = "foobarbaz"
9 +   parameter_group_name = "default.mysql5.7"
10 +  skip_final_snapshot = true
11 +  publicly_accessible = true
12 + }
```

github-actions bot on Jun 16

⚠ Aqua detected misconfiguration in your code

Misconfiguration ID: AVD-AWS-0077
Check Name: RDS Cluster and RDS instance should have backup retention longer than default 1 day
Severity: MEDIUM
Message: Instance has very low backup retention period.

Reviewers: github-actions

Assignees: No one assigned

Labels: None yet

Projects: None yet

Milestone: No milestone

Development: Successfully merging this pull request may close these issues. None yet

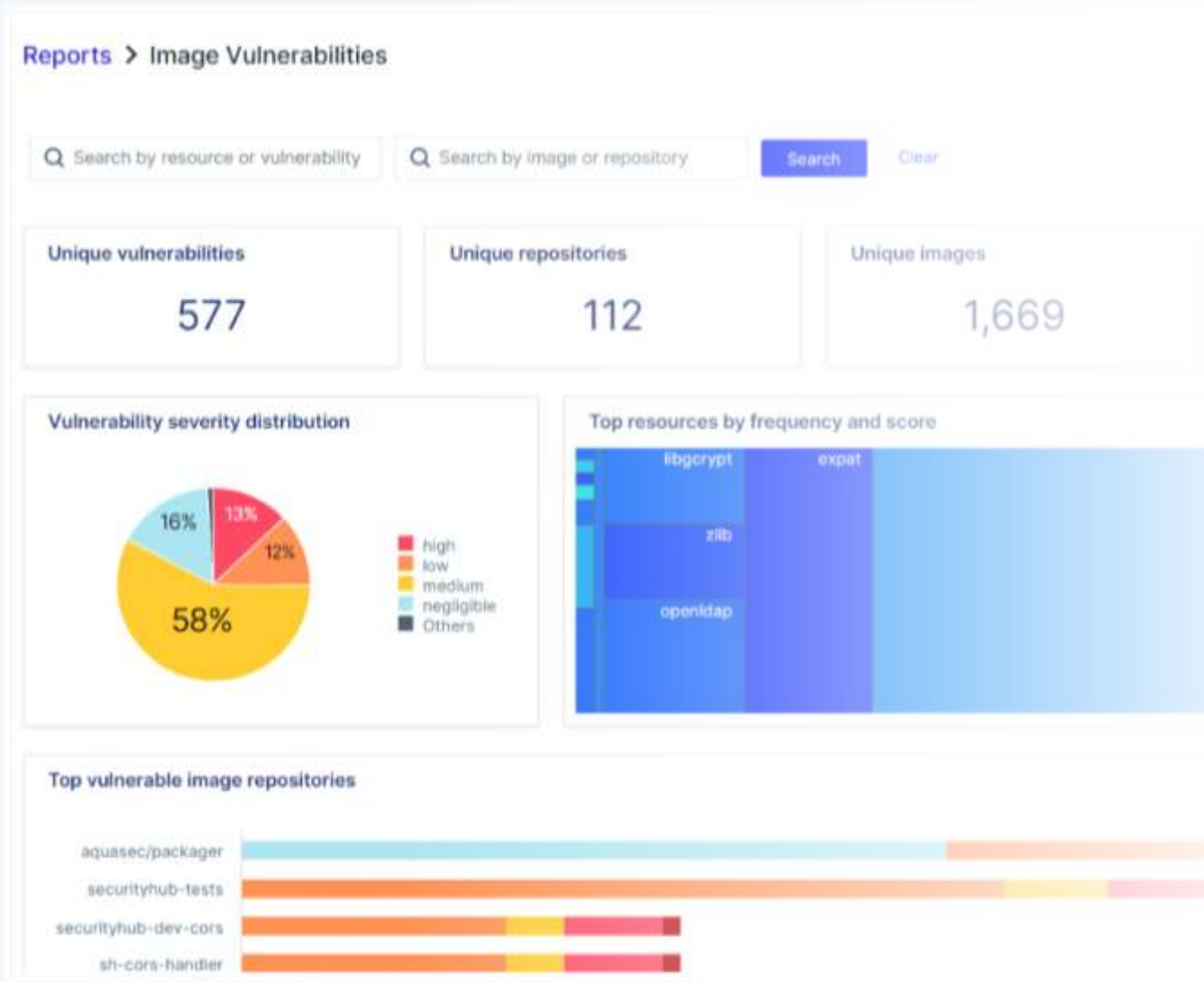
Notifications: [Subscribe](#) Customize

You're not receiving notifications from this thread.

1 participant

Empowering developers to fix risks found it within their flow.

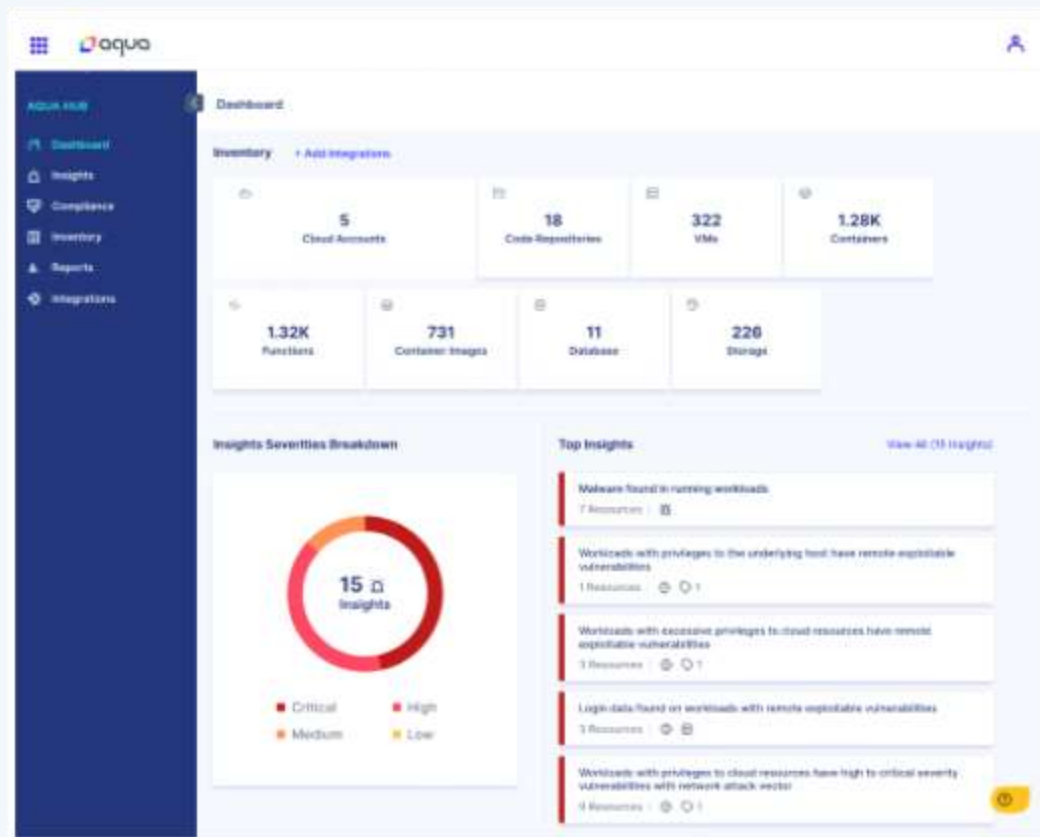
Vulnerability and Risk Scanning



Scan code, artifacts, and infrastructure for vulnerabilities, secrets, misconfigurations, malware, and permissions issues

Automate and integrate with existing workflows to reduce friction and maximize dev velocity

Risk based inventory

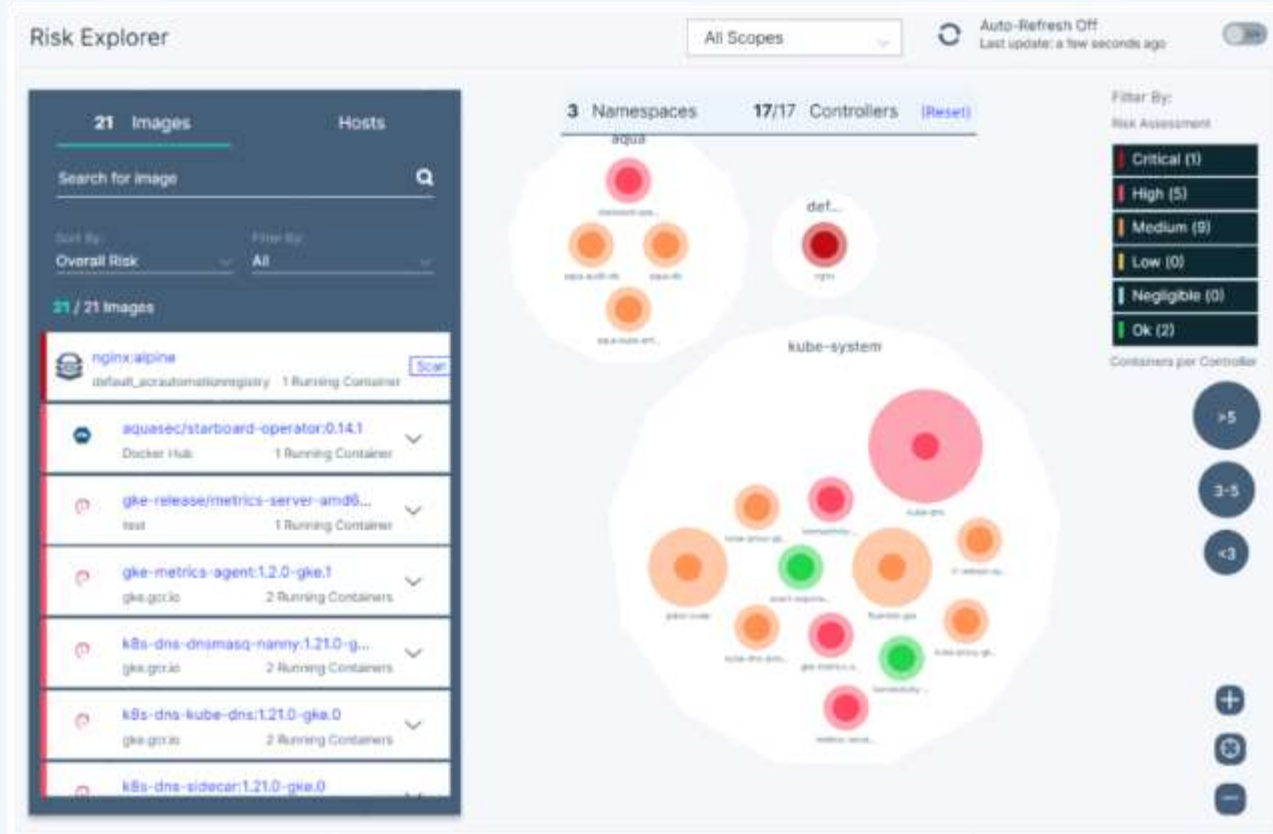


Inventory of all your Cloud account.

Automatic discovery and scanning.
Risk correlation and prioritisation.



Kubernetes Security



Automate Kubernetes security configuration and compliance

Set policies and control workload admission



Incident Handling - CNDR

The screenshot displays the 'Incidents > Drift Detection' interface. It features a 'Timeline' tab and a 'Create Suppression Rule' button. A search bar is present with the placeholder 'Search for event...'. Below the search bar, a timeline of events is shown. The events include:

- MITRE tactic: Defense Evasion**
MITRE technique: Masquerading (Mitre)
Oct 25, 2022 10:38:01 AM
- Drift Prevention - Prevent running execs image**
MITRE tactic: Privilege Escalation
MITRE technique: Hijack Execution Flow, Proce
- Shodan usage detected** (HIGH)
MITRE tactic: Discovery
MITRE technique: Network Service Scanning (Mitre)
Shodan search engine for internet connected devices was used. [View raw data](#)
- Evidence Found**
Command: /toolbin/shodan /search.txt /search-iplist.txt | Path Name: /toolbin/shodan | Return Value: 0
- Process Name:** shodan
PID: 12582
User ID: 0
Time Stamp: Oct 25, 2022 10:39:01 AM
- Block Cryptocurrency Mining**
MITRE tactic: Defense Evasion
MITRE technique: Resource Hijacking (Mitre)

Deep dive incident correlation.
Analyze runtime event in depth.
Block Cloud Native Attacks

The Cloud Native Application Protection Platform (CNAPP)



Detect, prioritize and reduce risk

Ensure compliance from code
to production



Protect the supply chain

Prevent cloud native attacks
before they happen



Stop attacks, not your business

Surgically stop attacks
in production without killing
workloads



Reduce noise, save time

A single unified platform for cloud native application protection



We Stop Cloud Native Attacks

Alliances



Awards

