



QUALYS SECURITY CONFERENCE 2019

Securing the Digital Transformation with DevOps

Cloud & Container Security Automation

Badri Raghunathan

Director of Product Management, Qualys, Inc.

Agenda

Digital Transformation in 2019

Accelerate DevOps with Qualys Security Platform

- Recent cloud, container security product updates

The road ahead

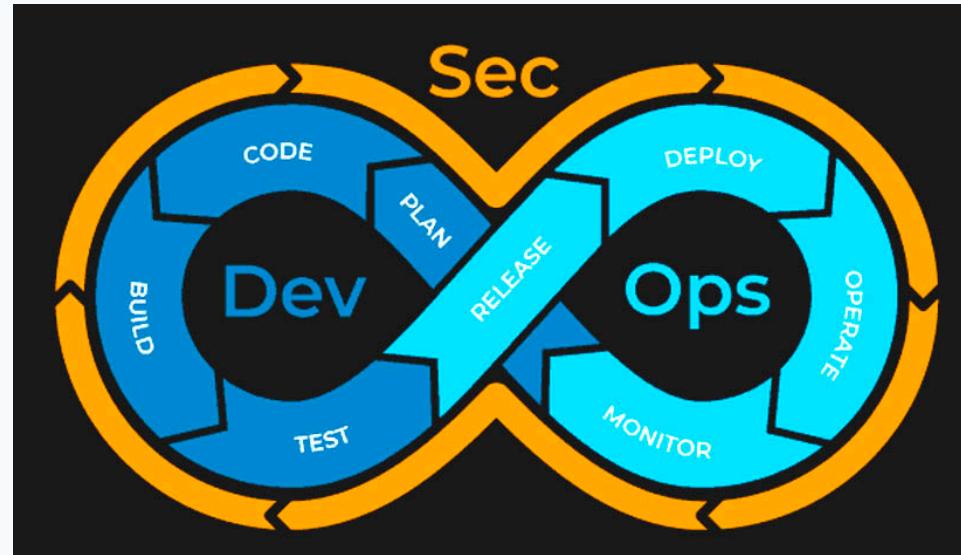
Qualys value proposition for cloud & container security



Digital Transformation

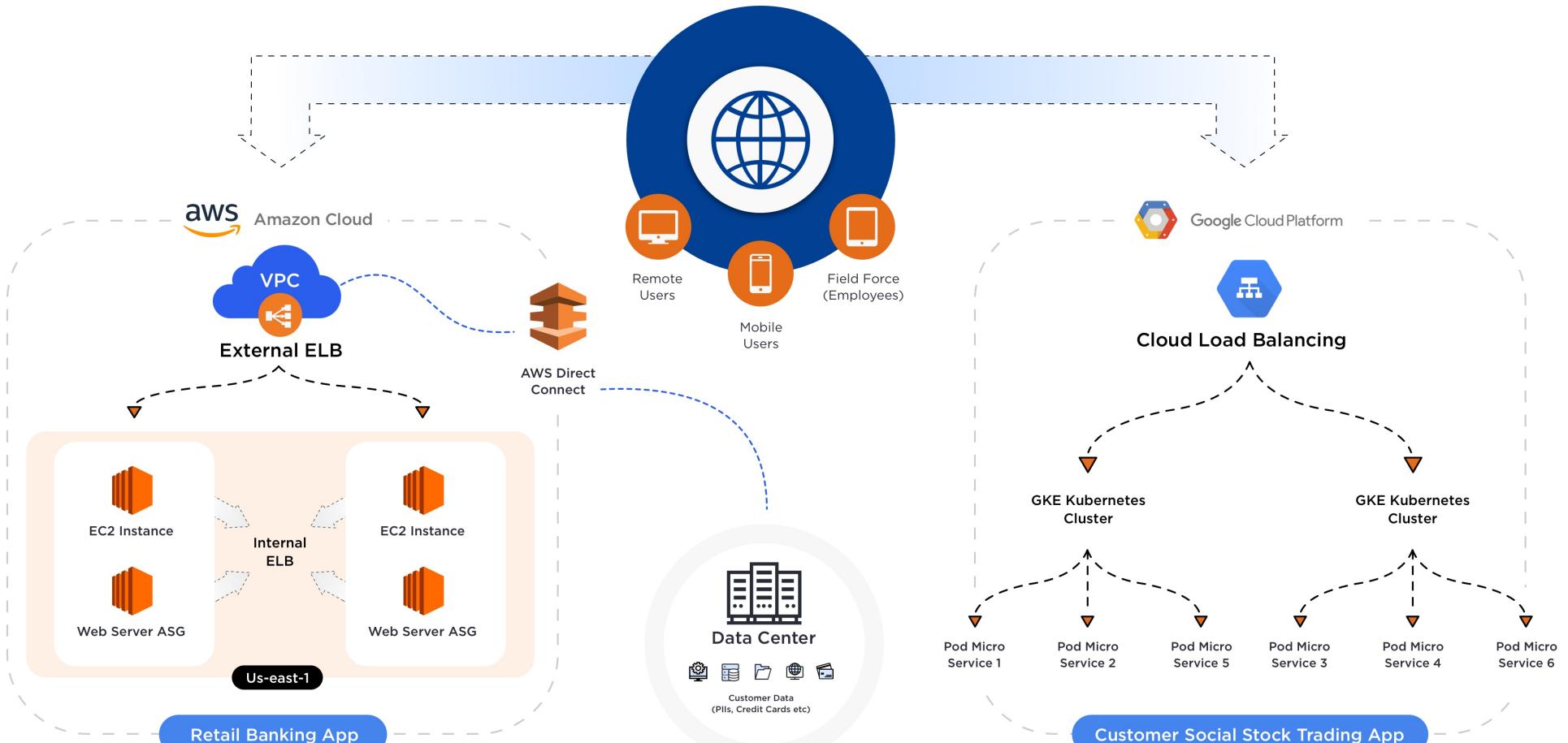
The Changing Role of Security

Security selects,
builds the
security tooling



DevOps
operationalizes,
uses the
security tooling

Example Customer Scenario



Security Challenges in the Cloud

Lack of visibility or control on cloud resources

- Instances, containers, serverless

Misconfiguration of cloud services

Multi cloud environment magnifies security challenges

Lack of a unified toolset for implementing security controls for on-prem & cloud workloads

Securing Your Cloud Deployments

IaaS EC2 Instance, Azure VM, GCP Instance	PaaS RDS, Azure SQL Database, Elastic Beanstalk, Containers	SaaS Google Suite, Office 365
Cloud Infrastructure S3 Bucket, Security Group, Network Security Group, Storage Blobs, Load Balancers, Firewall Rules		

Cloud Security

Securing Cloud Workloads

Hardening and Standardizing

VULNERABILITY MANAGEMENT

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management

POLICY COMPLIANCE

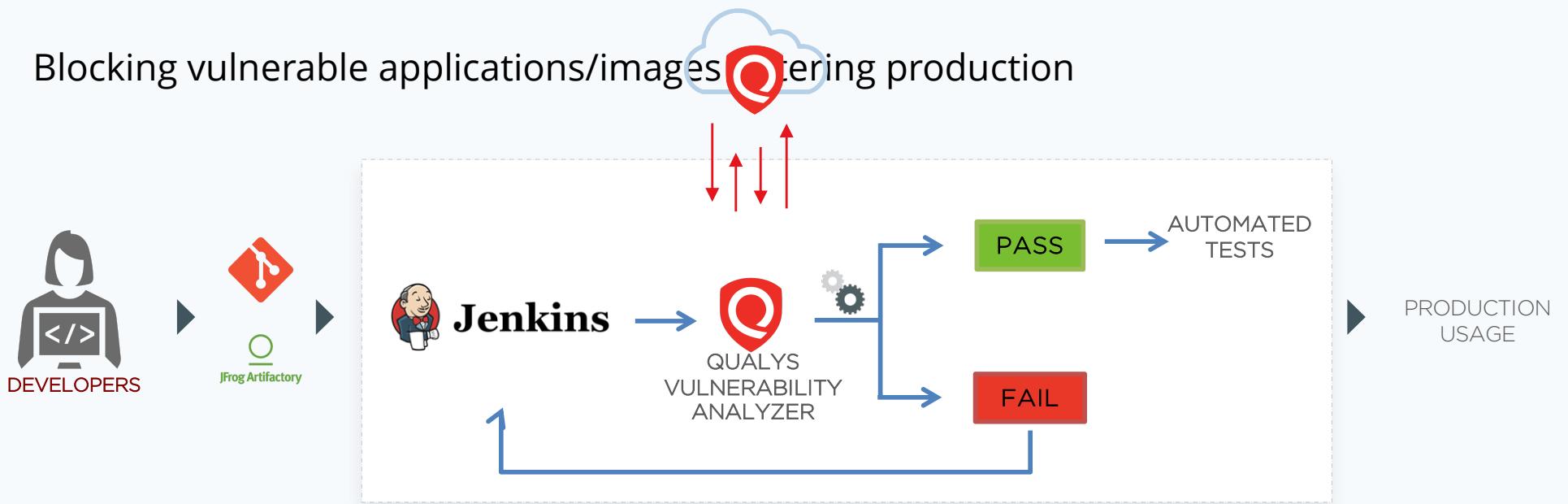
- Policy Compliance (incl. Secure Configuration Assessment)
- File Integrity Monitoring

APPLICATION SECURITY

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall
- API Security*

* Upcoming feature

Vulnerability Analysis in CI/CD



Supports evaluating – IPs/Hosts, Cloud Instances, and Web Applications

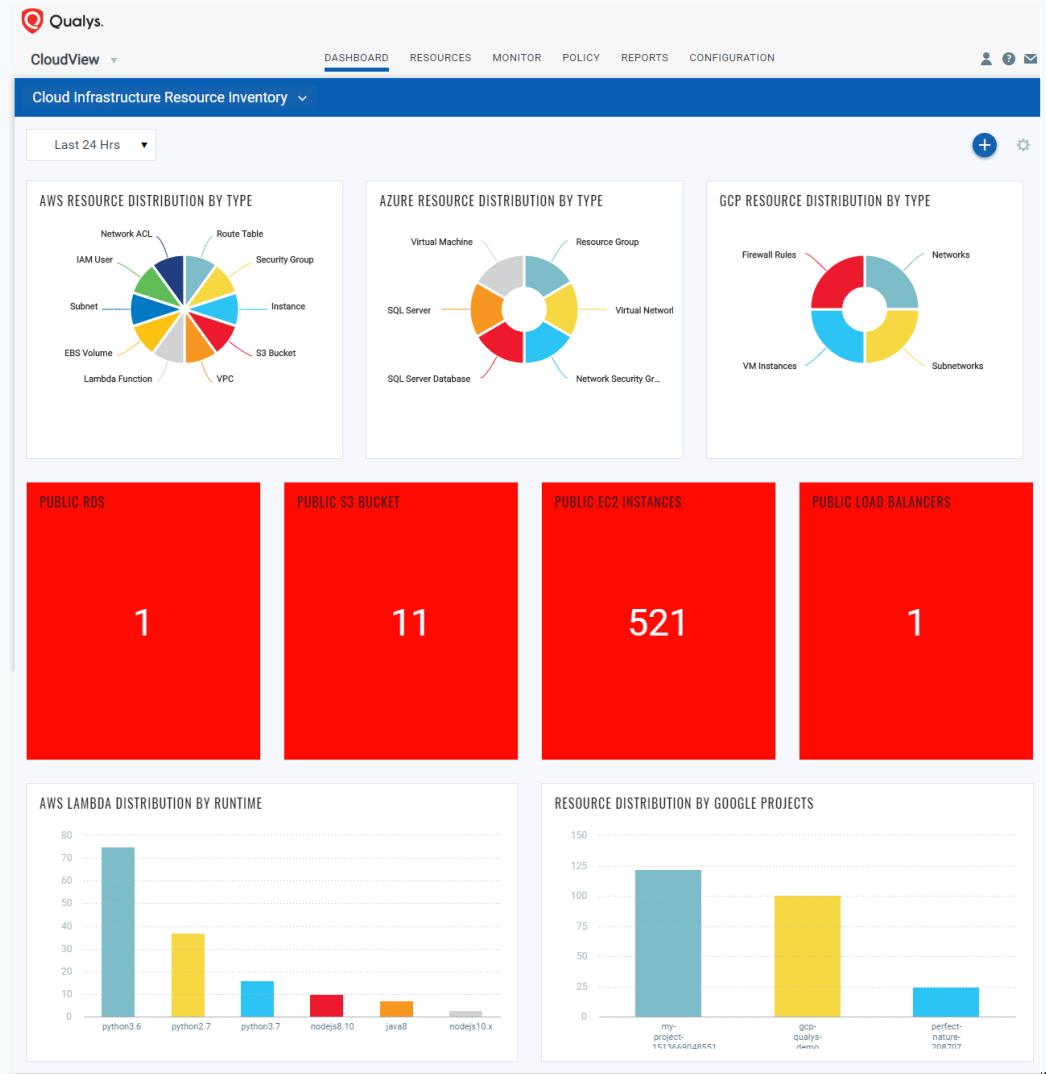
Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

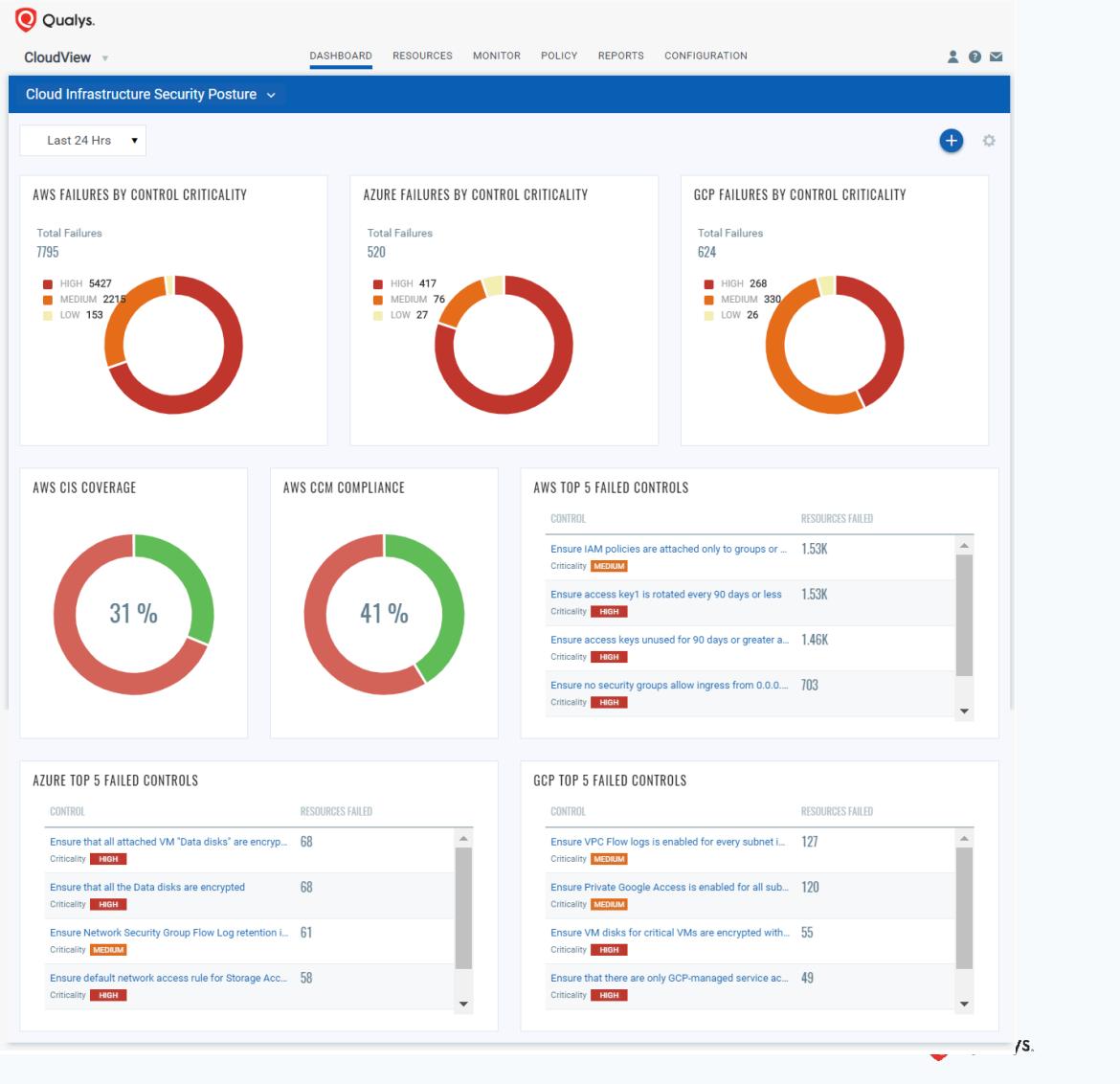


Compliance Assessment

Identify misconfigured resources

Detect resources that are non-compliant against standards such as CIS Benchmark

Identify top failed controls/account for prioritizing the remediation efforts



Correlate with Vulnerability Data

Identify vulnerable instances with public IP and associated with the misconfigured security groups

Use vulnerability information for cloud instances to prioritize threats better

The screenshot shows the Qualys CloudView interface for Amazon Web Services. At the top, there's a search bar with the query: `vulnerability.threatIntel.easyExploit:true and securitygroup.inboundRule.ipv4Range:0.0.0.0`. Below the search bar, it says "Last 24 Hrs". The main dashboard displays "28 Total Instances" across three regions: N. Virginia (16), London (7), and Mumbai (5). On the right, there are three summary metrics: "0 Without Agents", "21 With Public IP", and "2 Docker Hosts". The central part of the screen is a table titled "Resource Summary" showing 28 EC2 instances. The columns include EC2 INSTANCE ID, ACCOUNT ID, REGION, TYPE, STATE, and FIRST DISCOVERED ON. The table lists several instances, such as i-09877e1ab68f05330, i-03c8e8468ca299184, i-0e8258f50a903cc4f, i-0de3c0e9cc738bcf0, i-08ad24b40b2eaf29a, i-0ab2ff3ca465eef42, i-06f41ddd375f62144, and i-0afd7b51095e0db68, all discovered in October 2019 or earlier.

EC2 INSTANCE ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-09877e1ab68f05330 demo-aws-ue1-windows-2016-public-B	636123215182	N. Virginia	t2.medium	Running	October 13, 2019 4:46 AM
i-03c8e8468ca299184 demo-aws-ew2-windows-2016-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0e8258f50a903cc4f demo-aws-ew2-ubuntu-16-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0de3c0e9cc738bcf0 demo-aws-ue1-ubuntu-16-public-B-2	636123215182	N. Virginia	t2.micro	Running	September 19, 2019 1:02 AM
i-08ad24b40b2eaf29a demo-aws-ew2-windows-2019-public-C	636123215182	London	t2.medium	Running	August 27, 2019 7:48 PM
i-0ab2ff3ca465eef42 demo-aws-ue1-centos-7-private-B	636123215182	N. Virginia	t2.medium	Running	August 27, 2019 7:48 PM
i-06f41ddd375f62144 demo-aws-mumbai-windows-2016-publ...	636123215182	Mumbai	t2.medium	Running	August 26, 2019 7:41 AM
i-0afd7b51095e0db68 demo-aws-ue1-windows-2008-public-B	636123215182	N. Virginia	t2.medium	Running	August 24, 2019 7:31 PM

Serverless Visibility

NEW

Serverless Visibility
– Inventory support
for AWS Lambda
functions

Best practices
policy for
identifying
misconfigurations

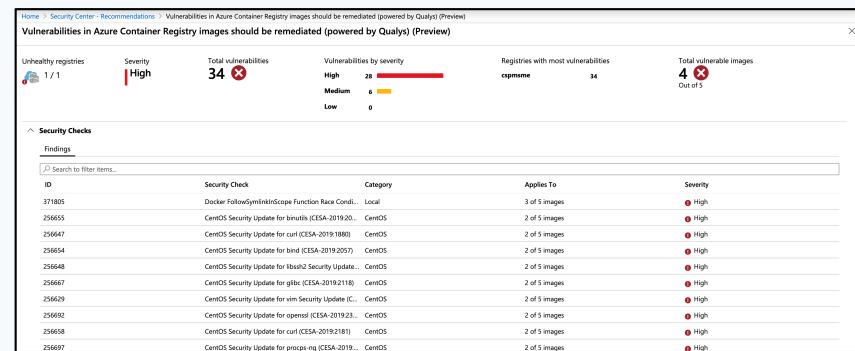
The screenshot displays two views of the Qualys Express CloudView interface. The left view shows an inventory of 21 total Lambda functions across various regions, runtimes, and layers. The right view shows a security audit of 11 controls evaluated, with 1.61K total evaluations. It highlights findings related to the AWS Lambda Best Practices Policy, including 948 Passes, 667 Fails, and 122 Low severity failures. A detailed list of 107 specific Lambda function configurations is provided, each with its control ID, name, criticality, service, and security posture.

Control ID	Control Name	Criticality	Service	Security Posture
97	Ensure that Lambda function has tracing enabled	HIGH	Lambda Function	15 / 133 Total Resources: 148
98	Ensure that Lambda Function is not using an IAM role for more than one Lambda function	HIGH	Lambda Function	91 / 57 Total Resources: 148
99	Ensure that Multiple Triggers are not configured in Lambda Function	MEDIUM	Lambda Function	136 / 12 Total Resources: 148
100	Ensure that Lambda Runtime Version is latest and not custom	LOW	Lambda Function	26 / 122 Total Resources: 148
101	Ensure that Lambda function does not have Admin Privileges	HIGH	Lambda Function	142 / 6 Total Resources: 148
102	Ensure that Lambda function does not have Cross Account Access	HIGH	Lambda Function	148 / 0 Total Resources: 148
103	Ensure that Lambda Environment Variables at-rest are encrypted with CMK	HIGH	Lambda Function	111 / 37 Total Resources: 148
104	Ensure that Lambda Environment Variables are encrypted using AWS encryption	MEDIUM	Lambda Function	112 / 36 Total Resources: 148
105	Ensure that Lambda function does not allow anonymous invocation	HIGH	Lambda Function	147 / 1 Total Resources: 148
106	Ensure that VPC access for Lambda Function is not set to default(Null)	HIGH	Lambda Function	9 / 126 Total Resources: 135
107	Ensure that AWS Lambda excess Permissions are removed	HIGH	Lambda Function	11 / 137 Total Resources: 135

NEW

Built-in Security with Cloud Providers

- Send findings into Azure, AWS, GCP Security Hubs
- Access & investigate findings from within the Cloud Provider Security console
- Native integration of vulnerability assessment of hosts, containers (MSFT Azure - Powered by Qualys)



Azure Host, Container Scanning (Powered by Qualys)

Comprehensive Coverage Across Public Clouds



Amazon Web Services



Microsoft Azure



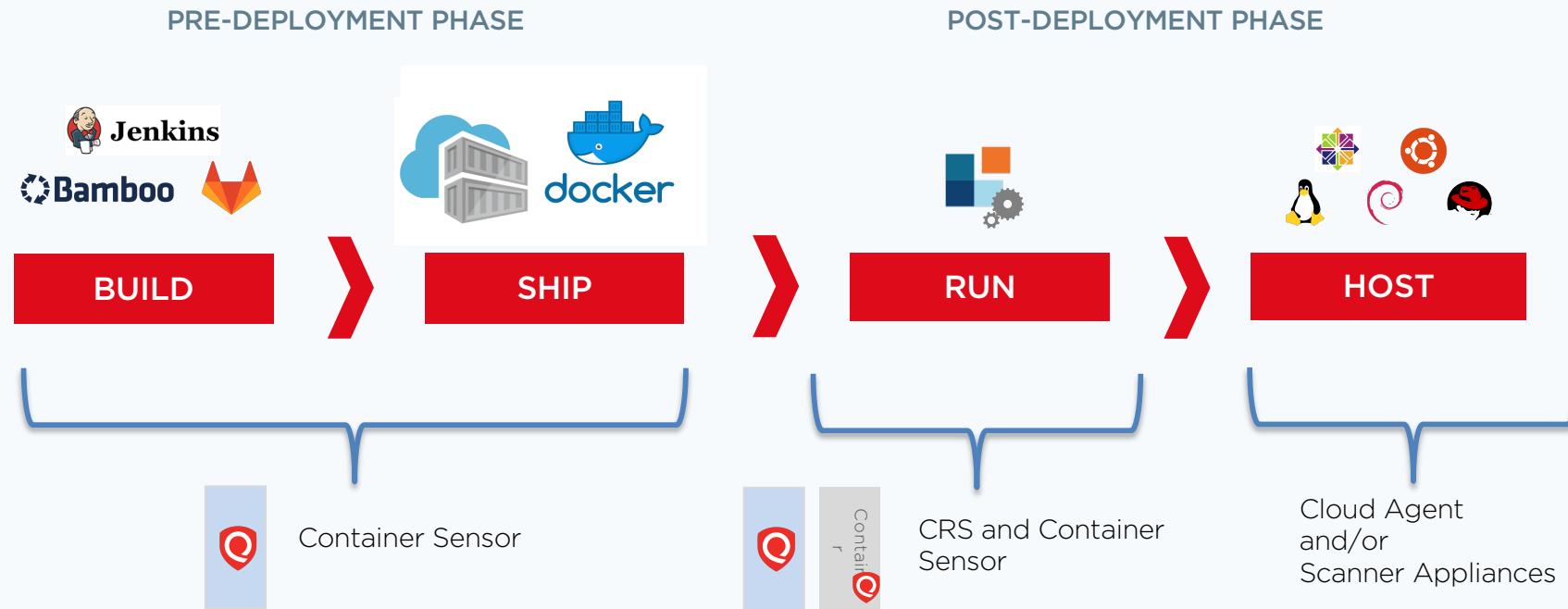
Google Cloud

Google Cloud Platform

- Inventory
- Best practices like CIS benchmarks
- Cloud provider best practices policy benchmarks
- Mandates like PCI, CCM ISS
- Control customization

Container Security

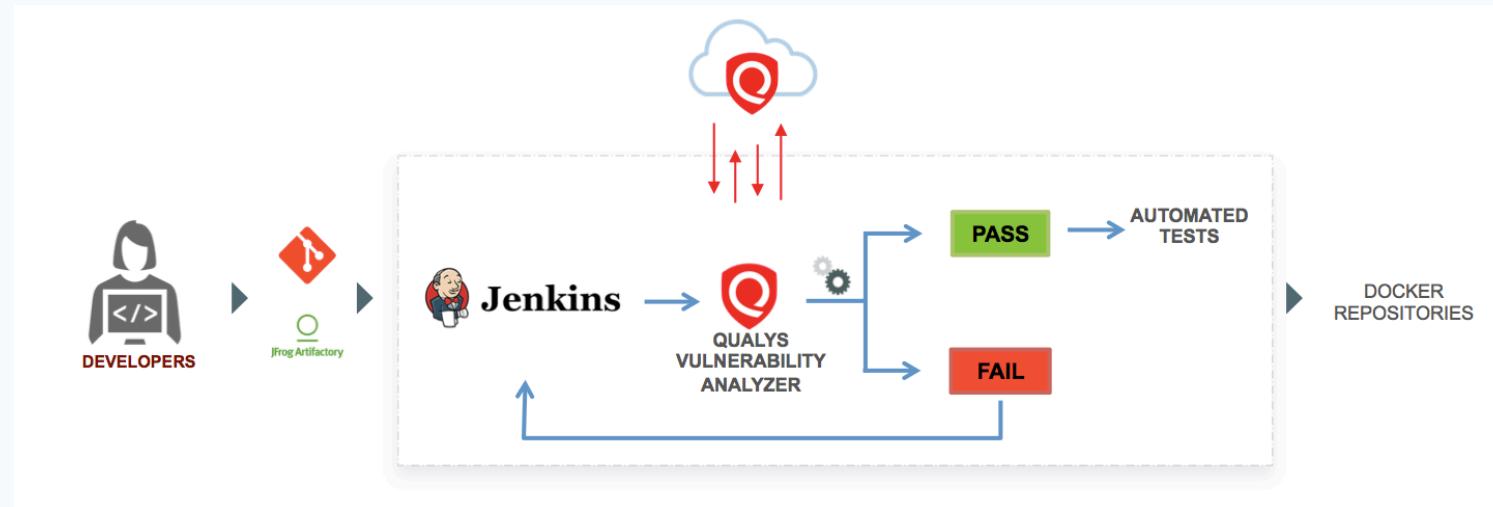
Security across the Container Lifecycle



CRS - Container Runtime



Scanning Containers in CI/CD



1. DevOps friendly container scanning using a plug-in
2. Actionable, detailed, high-accuracy vulnerability info for DevOps

Actionable Vulnerability Information for DevOps

Jenkins 3 search P

Jenkins > pipeline-project > #78 > Qualys Report For e8d112ff7588

Qualys

Build Summary
Vulnerabilities
Installed Software
Layers

BUILD REPORT - e8d112ff7588

Build Status: Failed Image ID: e8d112ff7588 Tags: latest Size: 828 MB

Build Summary

The vulnerabilities count by severity for image id e8d112ff7588 exceeded one of the configured threshold value :
Configured : Severity 1 > 0; Severity 2 > 0; Severity 3 > 0; Severity 4 > 0; Severity 5 > 0;
Found : Severity 1: 0, Severity 2: 1, Severity 3: 11, Severity 4: 2, Severity 5: 0

Vulnerabilities Trend

Confirmed vulnerabilities in current build (blue bars) and Comparing with build #77 (grey bars).

Severity	Current Build (Confirmed)	Build #77 (Comparing)
Sev 5	0	0
Sev 4	1	0
Sev 3	11	0
Sev 2	2	0
Sev 1	0	5

Confirmed Vulnerabilities (10)

Severity	Count
Sev 5 (0)	0
Sev 4 (1)	1
Sev 3 (9)	9
Sev 2 (0)	0
Sev 1 (0)	0

Potential Vulnerabilities (4)

Severity	Count
Sev 5 (0)	0
Sev 4 (1)	1
Sev 3 (2)	2
Sev 2 (1)	1
Sev 1 (0)	0

Patchability

Status	Count
Yes (12)	12
No (2)	2

Qualys Report For e8d112ff7588 ENA

INSTALLED SOFTWARE

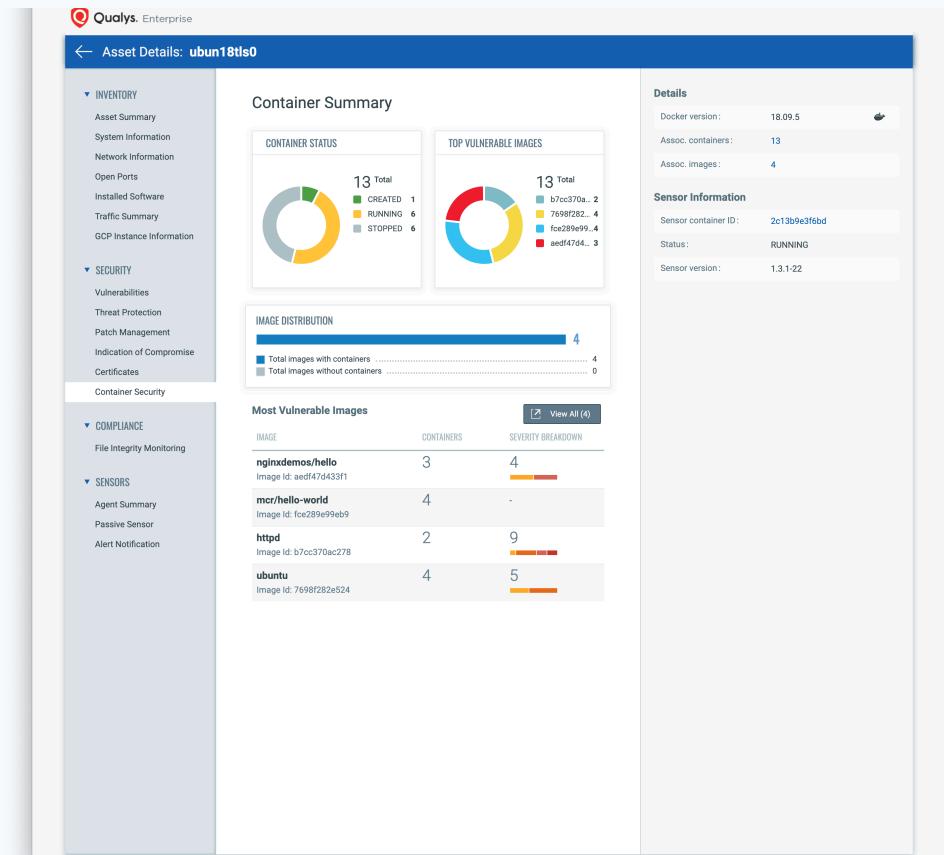
Show 10 entries Search: QID=176259

Name	Installed Version	Fixed In Version
libmagickwand-dev	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	⚠ 8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4

NEW

Visibility into Container Infrastructure

- Free inventory for all your container infrastructure
- Visibility into containers via Scanner, Cloud Agent, Container Sensor
- Tracking DockerHub official images
- Upgrade for security across DevOps pipeline

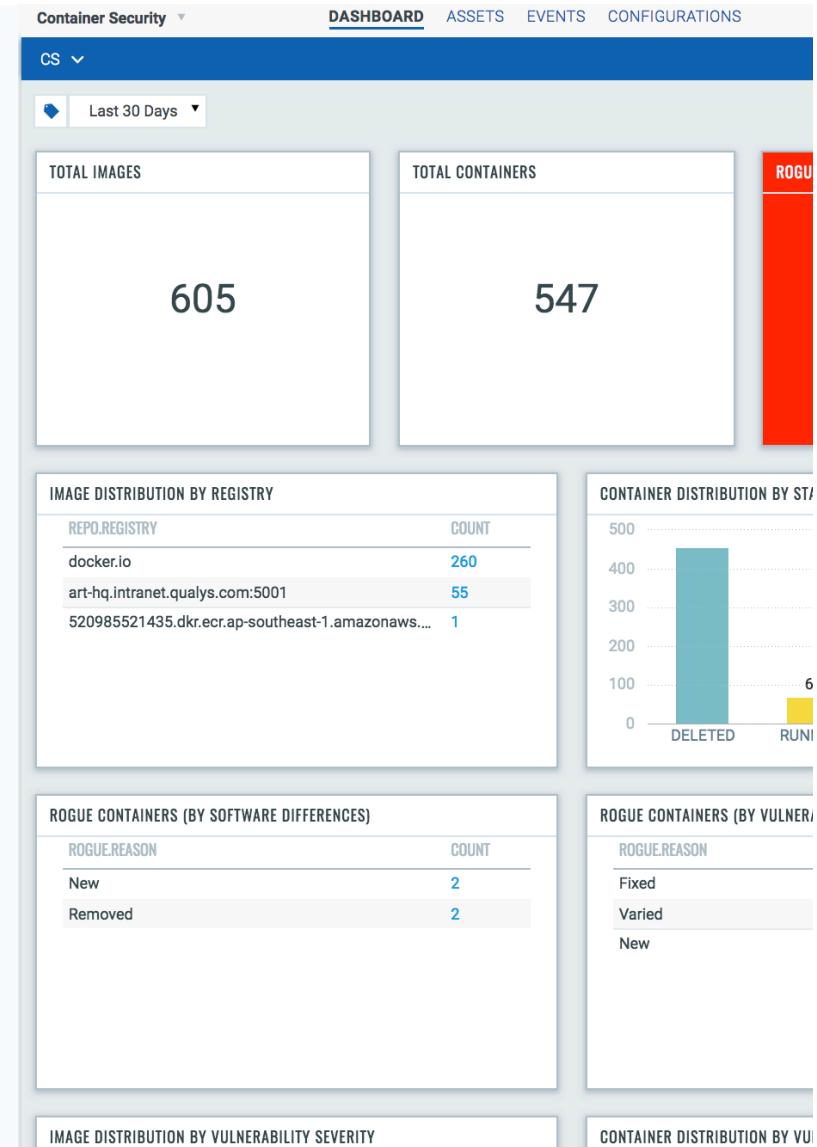


Deeper Visibility Into Containers

Inventory & security posture widgets

- Count of images, containers
- Containers by state
- Vulnerable images

Personalize and add custom widgets



Correlating with vulnerability data

The screenshot shows the Qualys Container Security interface. On the left, there's a sidebar with sections for Labels, Registry, and Vulnerabilities. The main area is titled 'Assets' and shows '68 Total Images'. A search bar at the top contains the query: 'vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"'. Below the search bar is a table with columns: REGISTRY, REPOSITORY, CREATED ON, TAGS, CONTAINERS, and VULNERABILITIES. The table lists various Docker images from docker.io, including elasticsearch, redis, kibana, node, httpd, cassandra, solr, tomcat, and another kibana entry. Each row shows the image details, its creation date, latest tag, number of containers it runs on, and the count of vulnerabilities found. A red box highlights the 'httpd' row, and a red arrow points from the text 'Preset quick search filters' to this box. Another red arrow points from the text 'Search based on all attributes' to the search bar.

Search based on all attributes

Preset quick search filters

- Identify images by application labels

- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

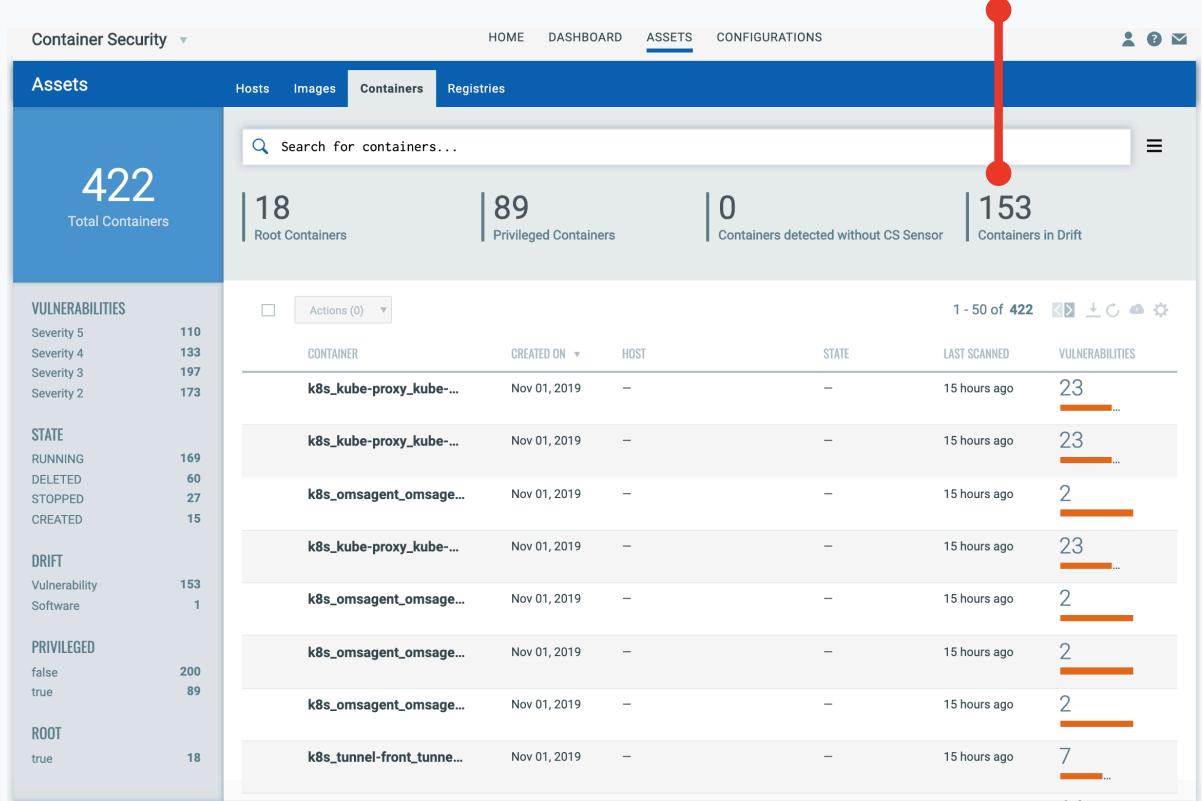


Detecting Runtime Drift

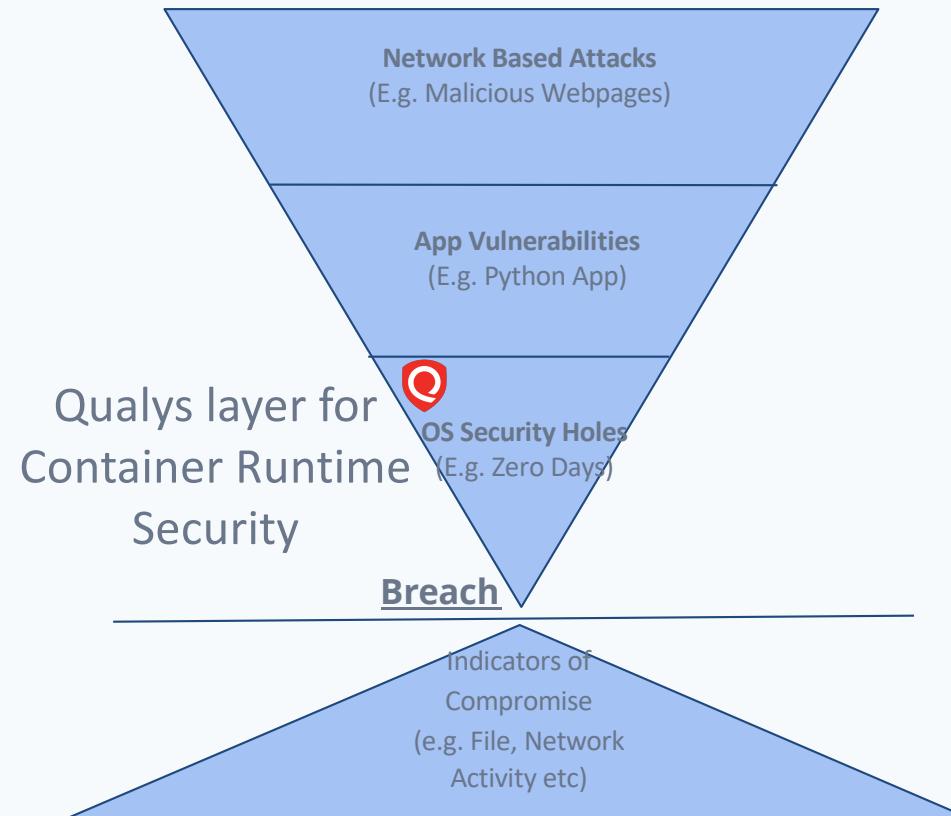
Detect Containers
breaking off from
“immutable” behavior

Identify potential breaches in containers

“Drift” Containers, differ from their
parent Images by vulnerability, software
package composition, behavior, etc



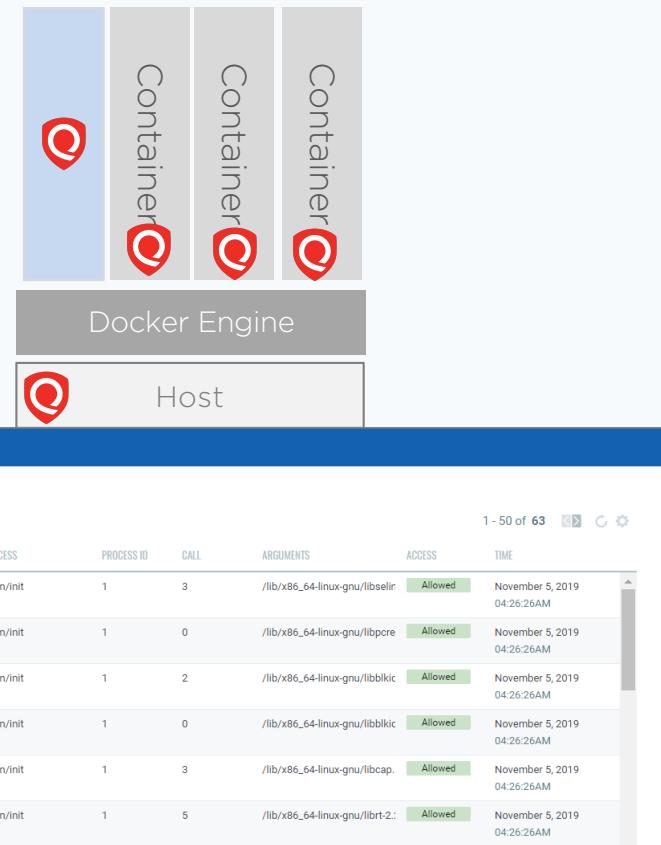
Protecting Containers at Runtime



NEW

Protect Against Attacks with Container Runtime Security

- Integrated into Qualys Platform
- Function level firewall for containers
- Granular security policies to control file, network, process behavior
- Built-in policies from Qualys Threat Research

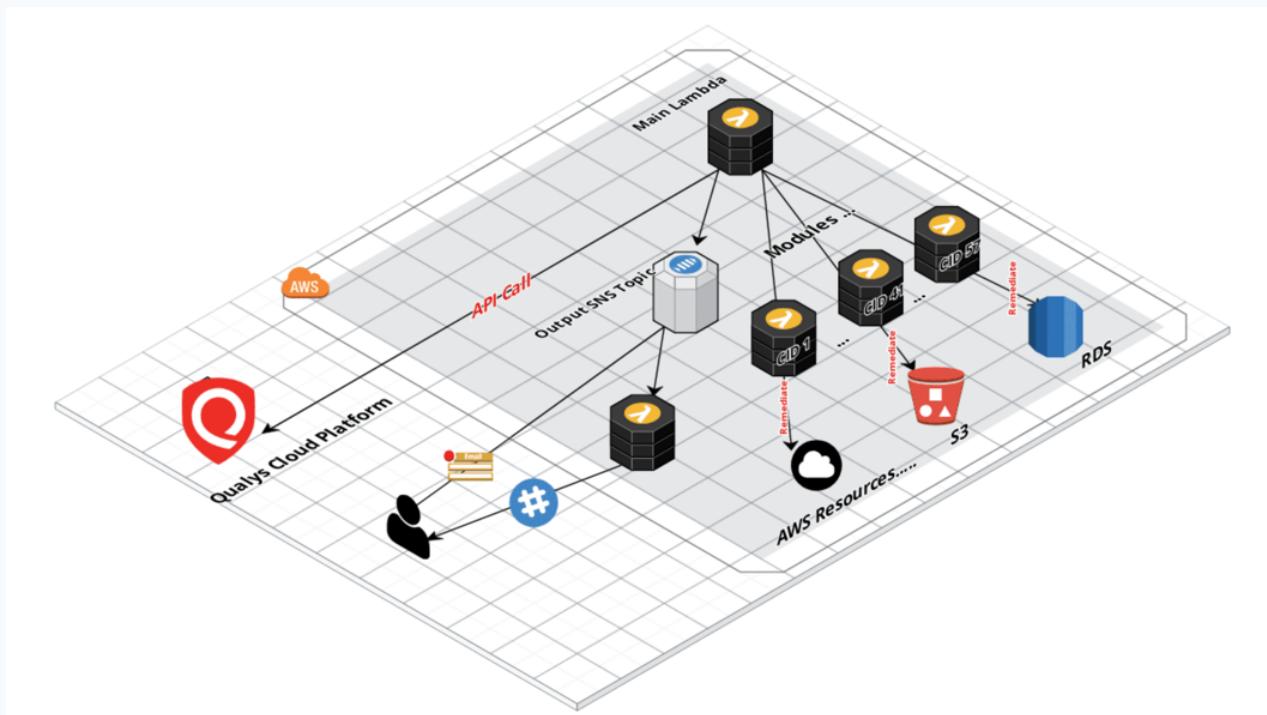


DEMO



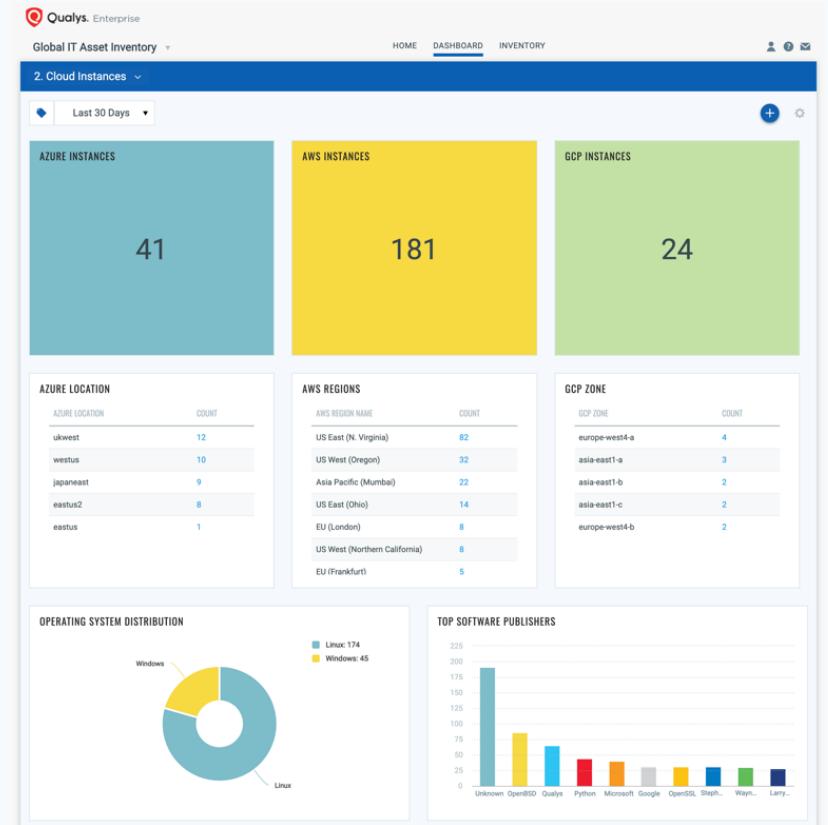
The Road Ahead

Moving Towards Automated Remediation

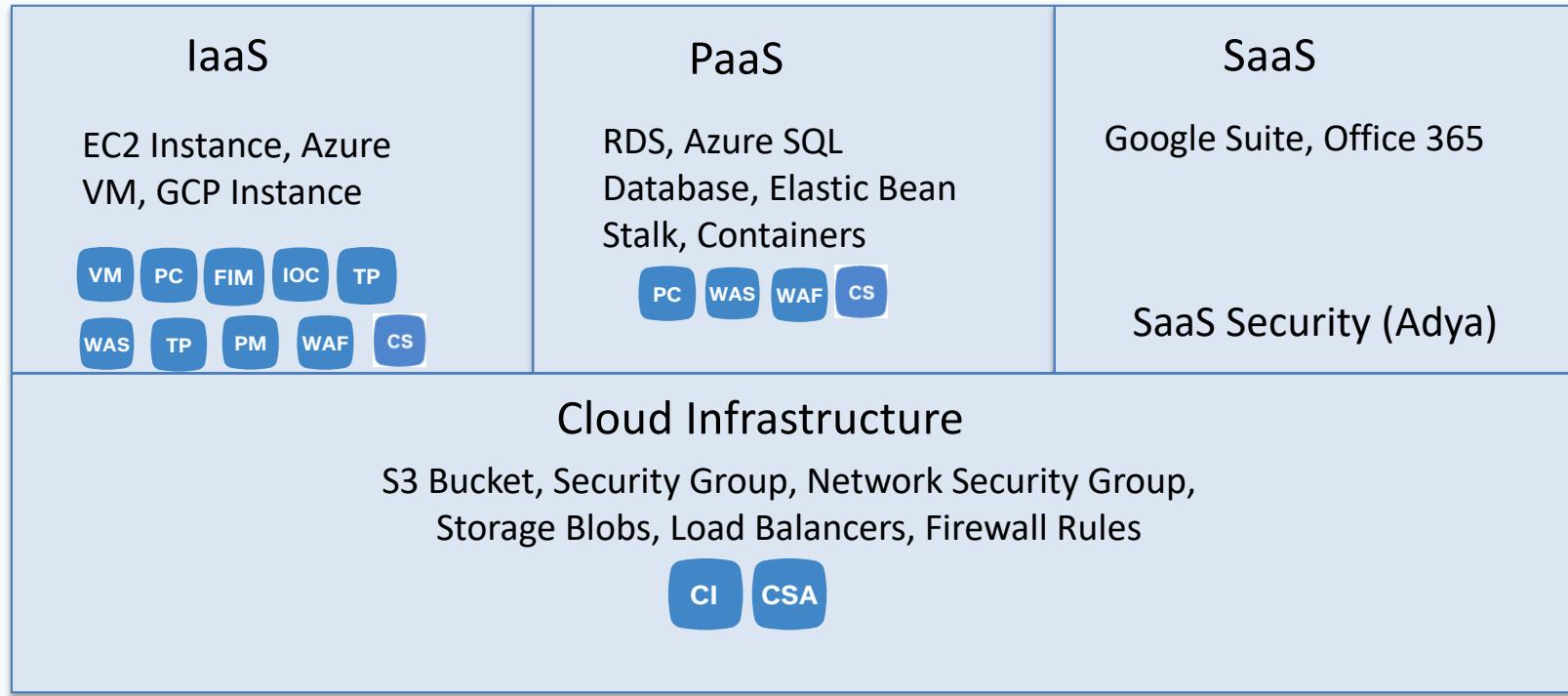


Towards Seamless Visibility

- Across application stack (Hosts, Kubernetes Pods, Containers, Serverless)
- Correlate cloud inventory data with containers



Qualys Cloud Security Coverage



Qualys GitHub for DevOps

- Automation scripts for sensors
- Best practice process automation
- Open source community around Qualys ecosystem

<https://github.com/qualys>





QUALYS SECURITY CONFERENCE 2019

Thank You

Badri Raghunathan
braghunathan@qualys.com