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

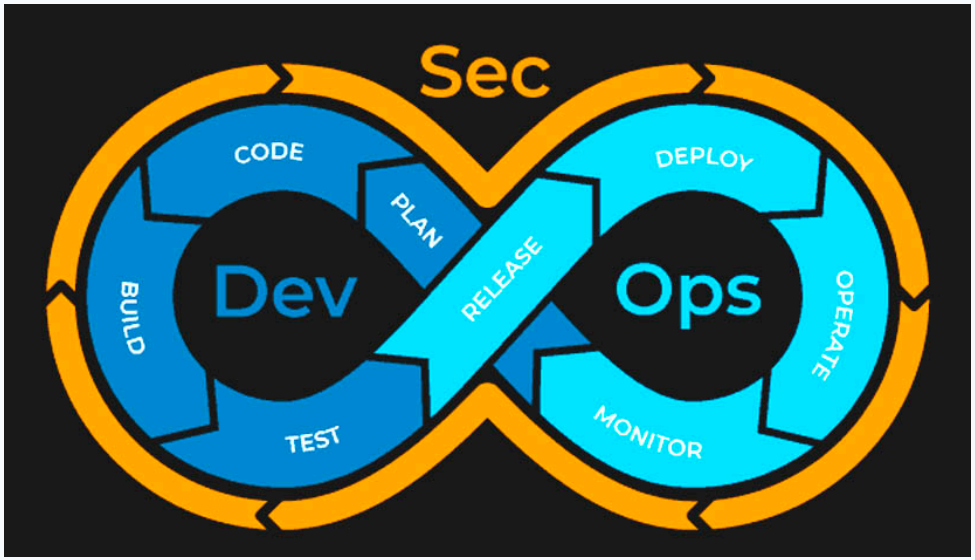
The road ahead

Qualys value proposition for cloud & container security

Digital Transformation

The Changing Role of Security

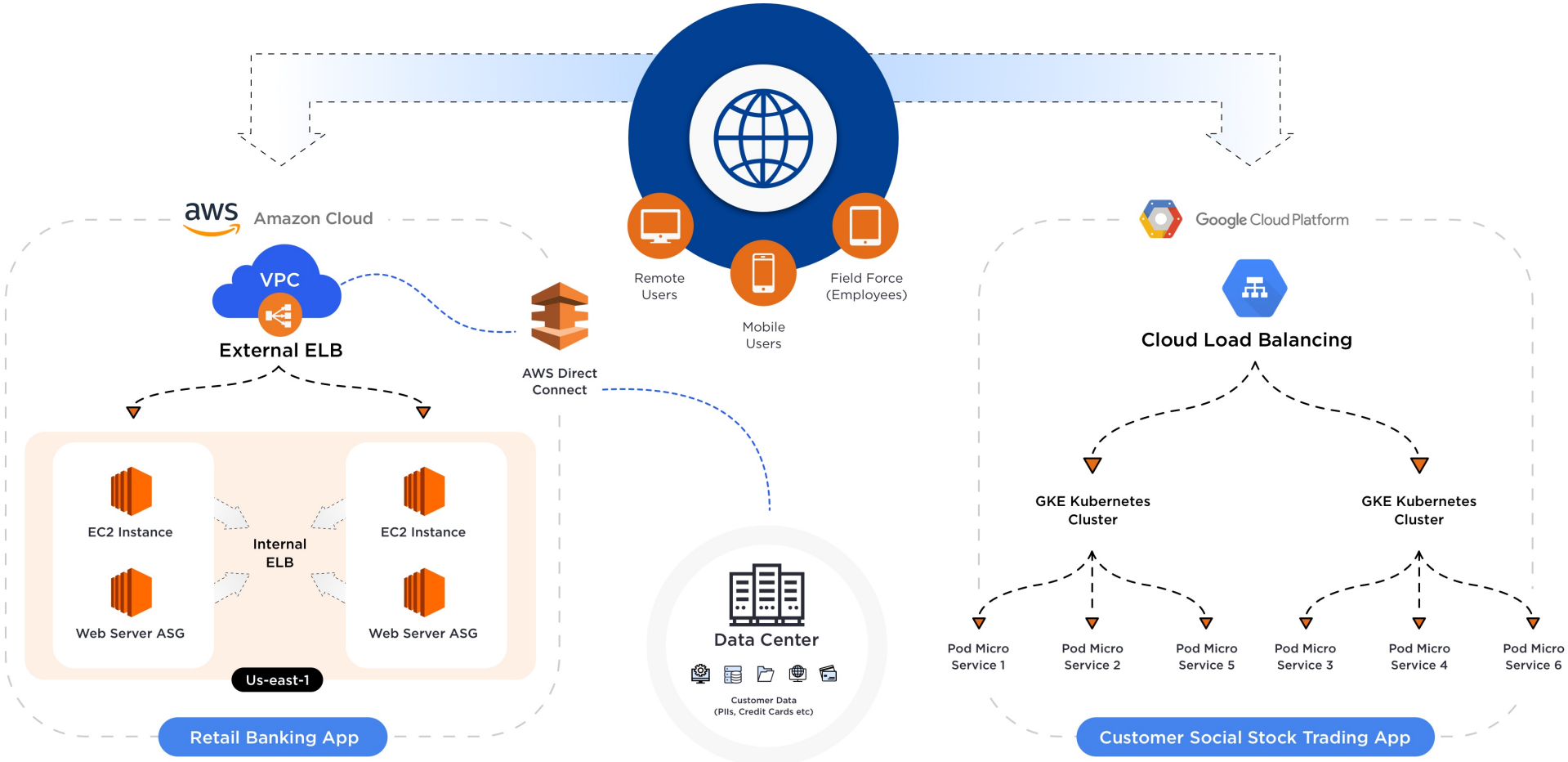
Security selects, builds the security tooling



DevOps operationalizes, uses the security tooling

Qualys.

Example Customer Scenario



Security Challenges in the Cloud

Lack of visibility or control on cloud resources

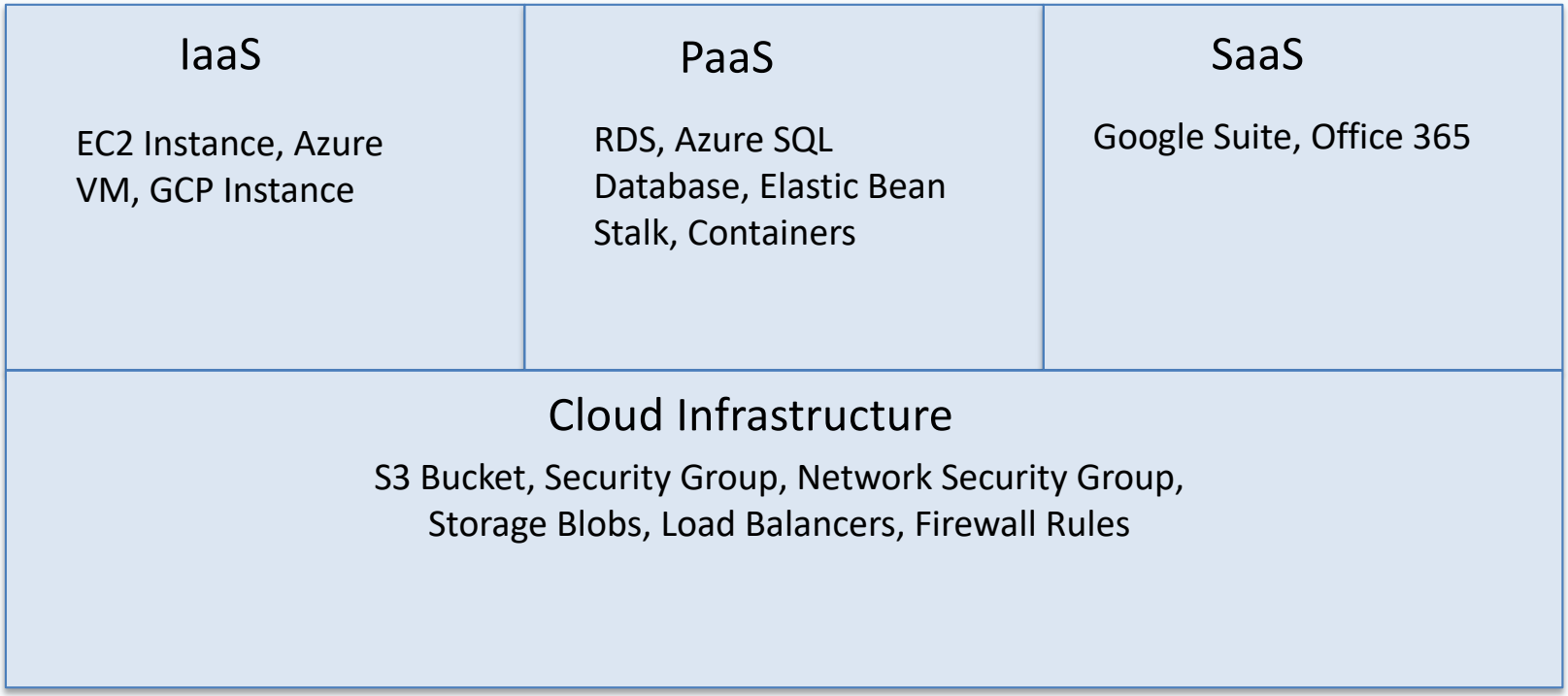
- Instances, containers, serverless

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



Qualys.

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

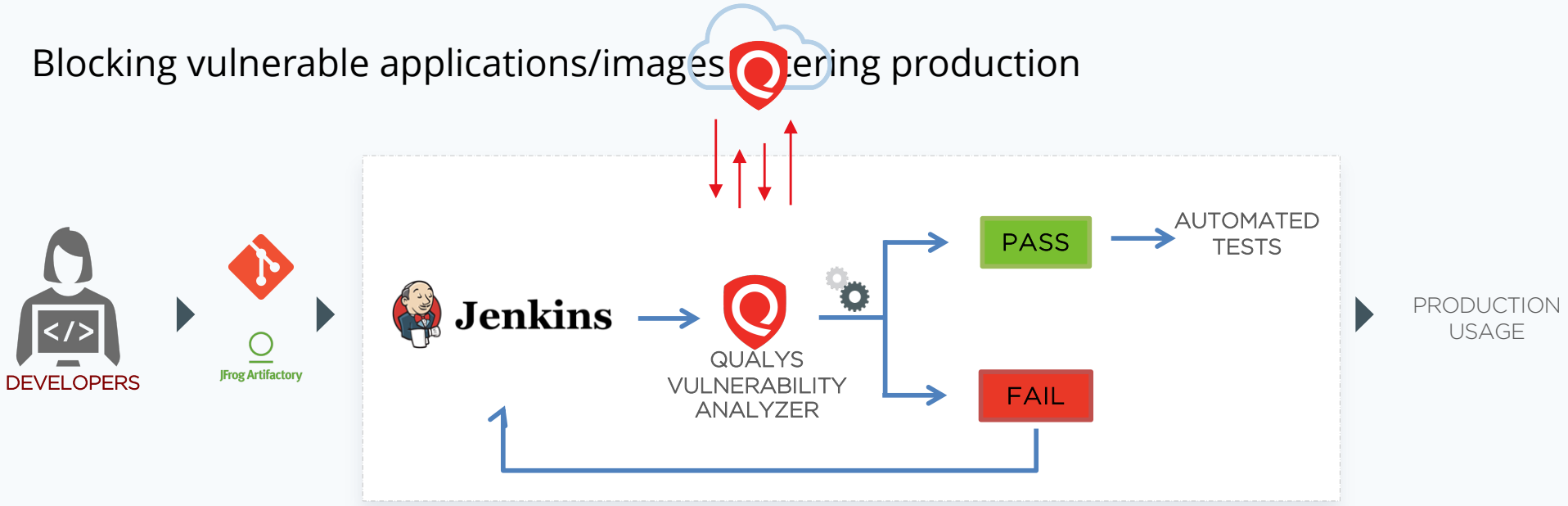
APPLICATION SECURITY

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

* Upcoming feature

Vulnerability Analysis in CI/CD

Blocking vulnerable applications/images entering production



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

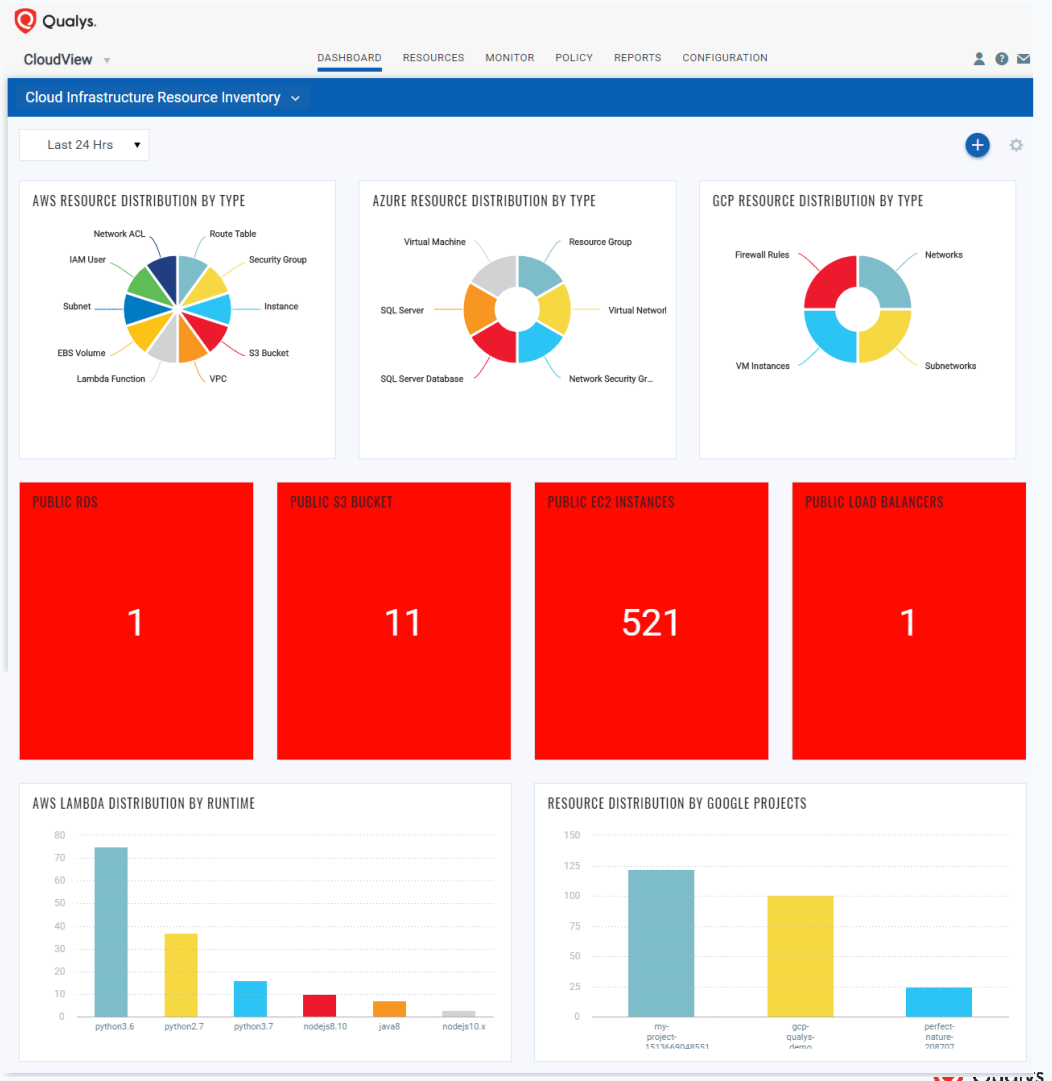
Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

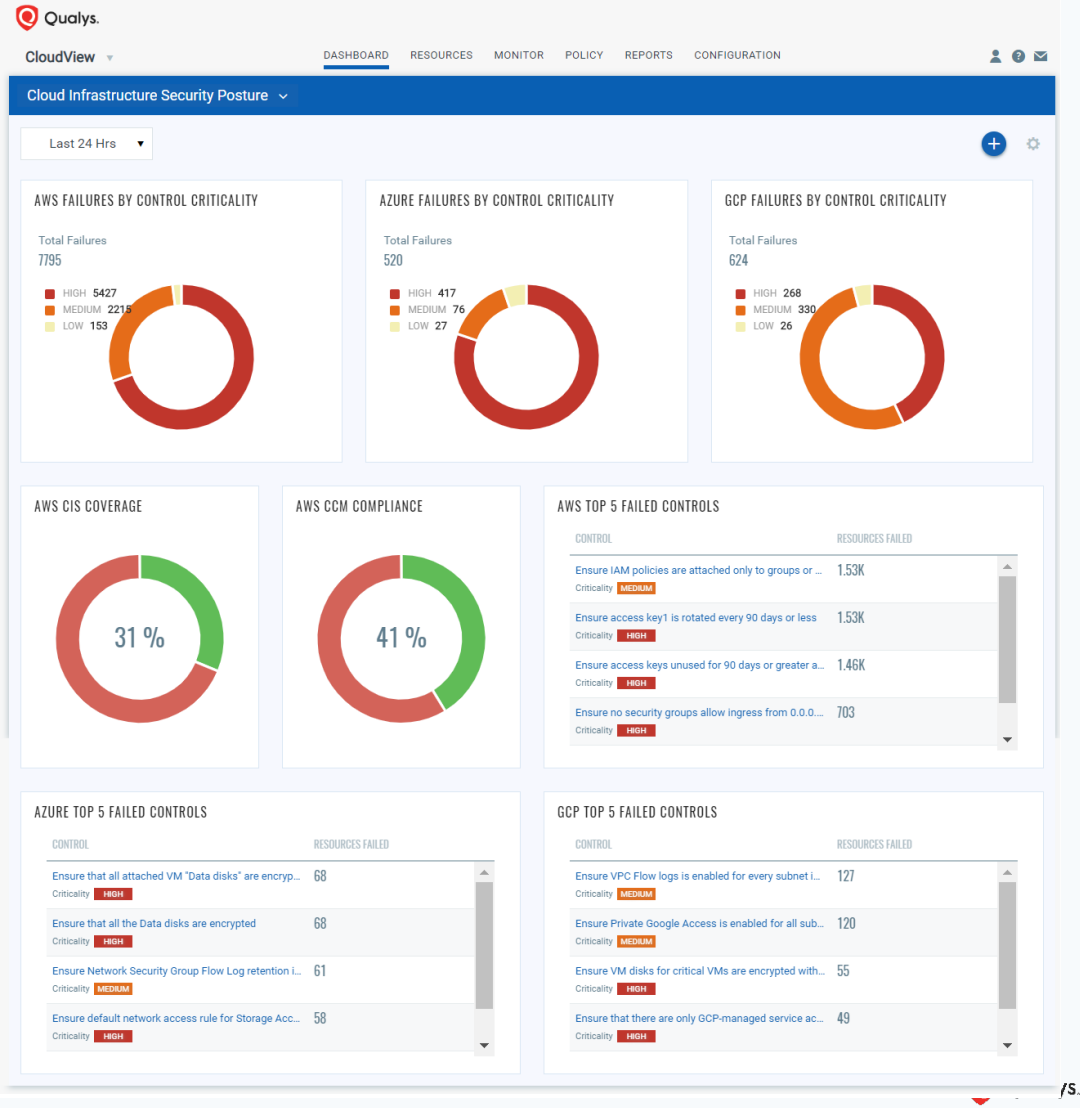


Compliance Assessment

Identify misconfigured resources

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

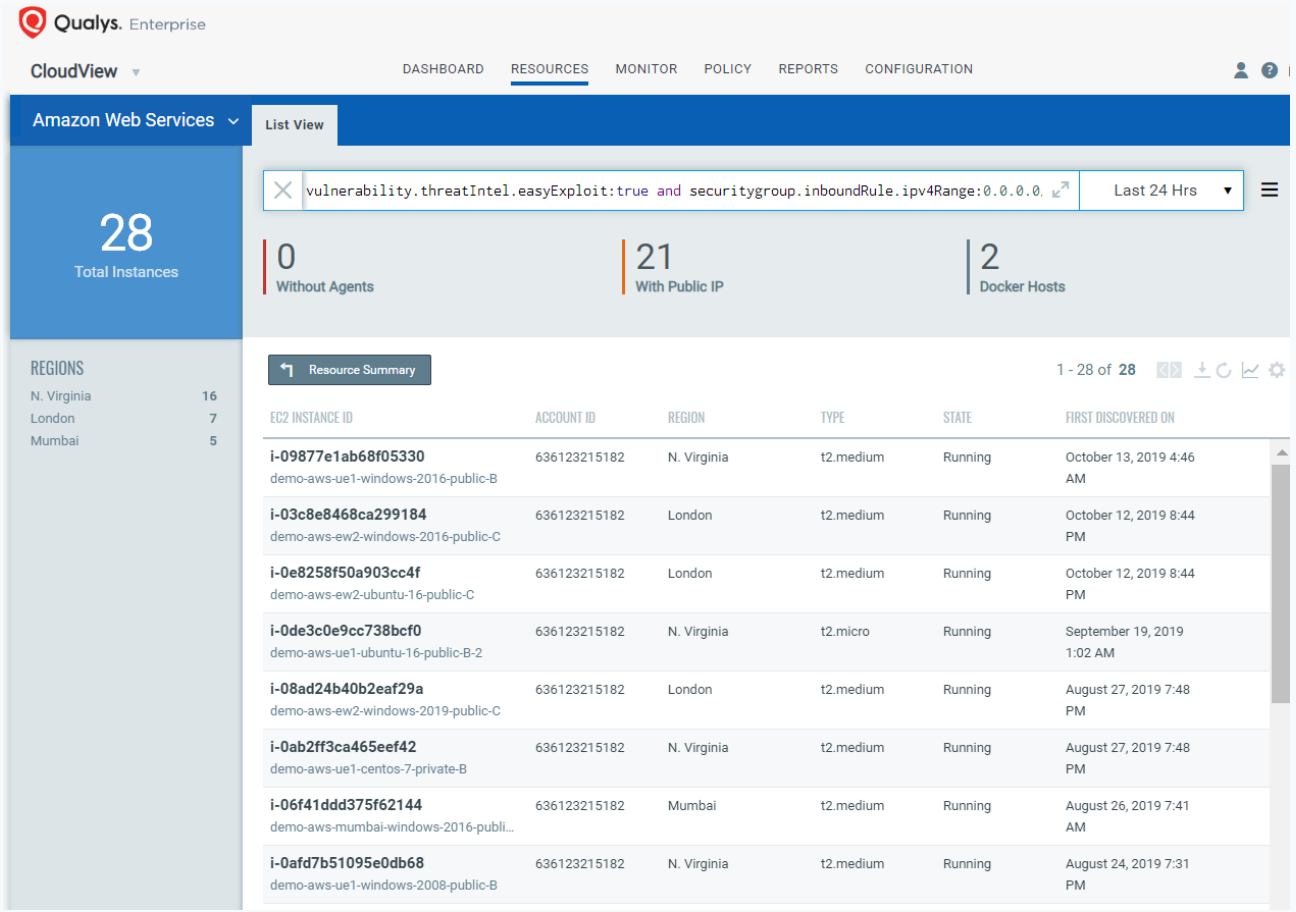
Identify top failed controls/account for prioritizing the remediation efforts



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

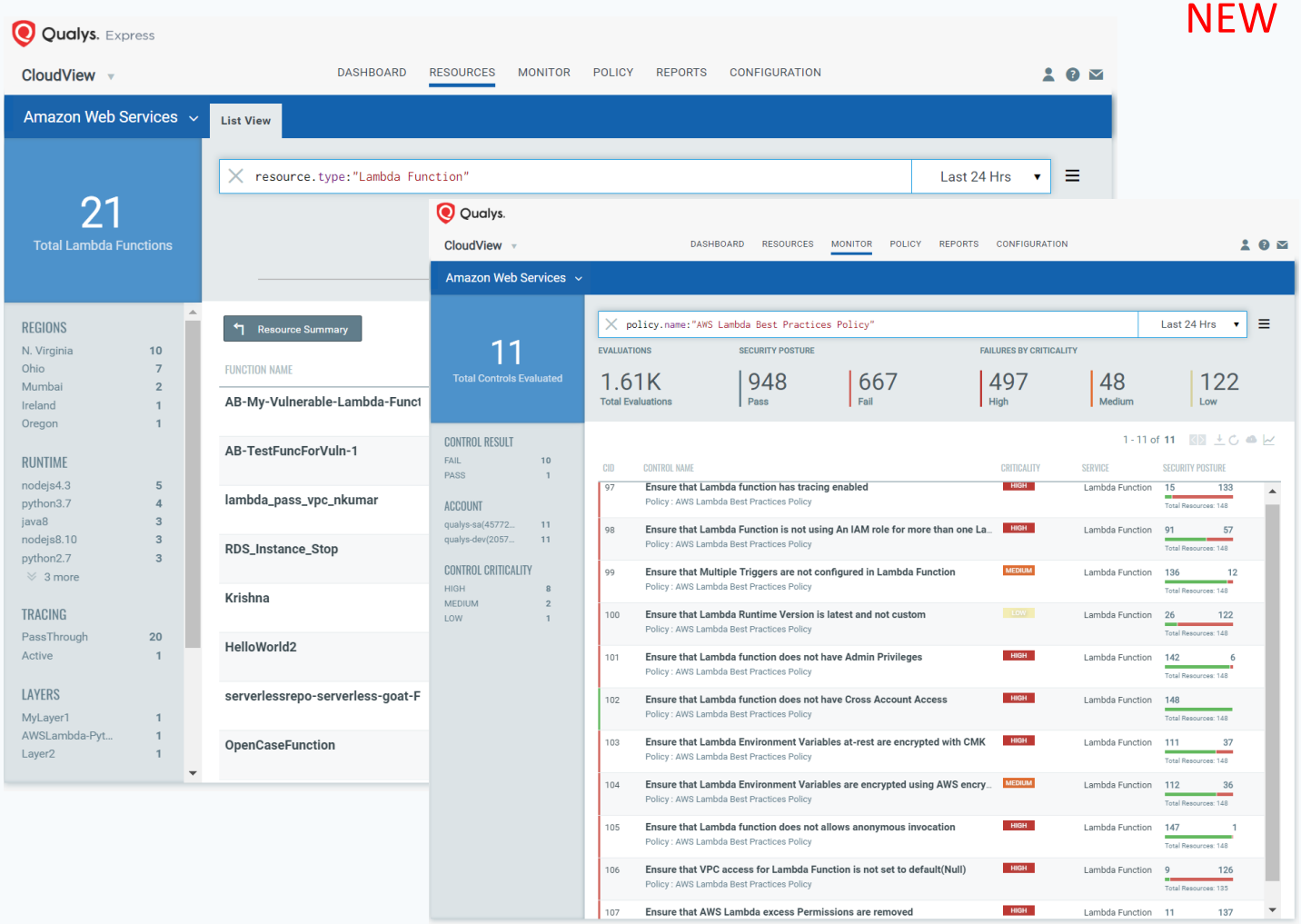


Serverless Visibility

NEW

Serverless Visibility – Inventory support for AWS Lambda functions

Best practices policy for identifying misconfigurations

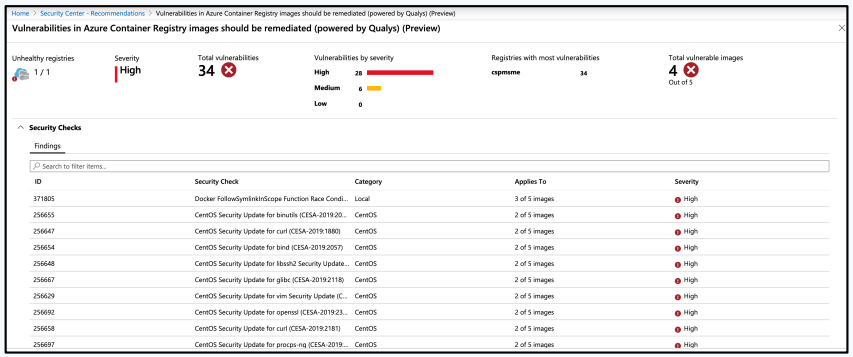


Qualys.

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)

Qualys.

Comprehensive Coverage Across Public Clouds

Amazon Web Services

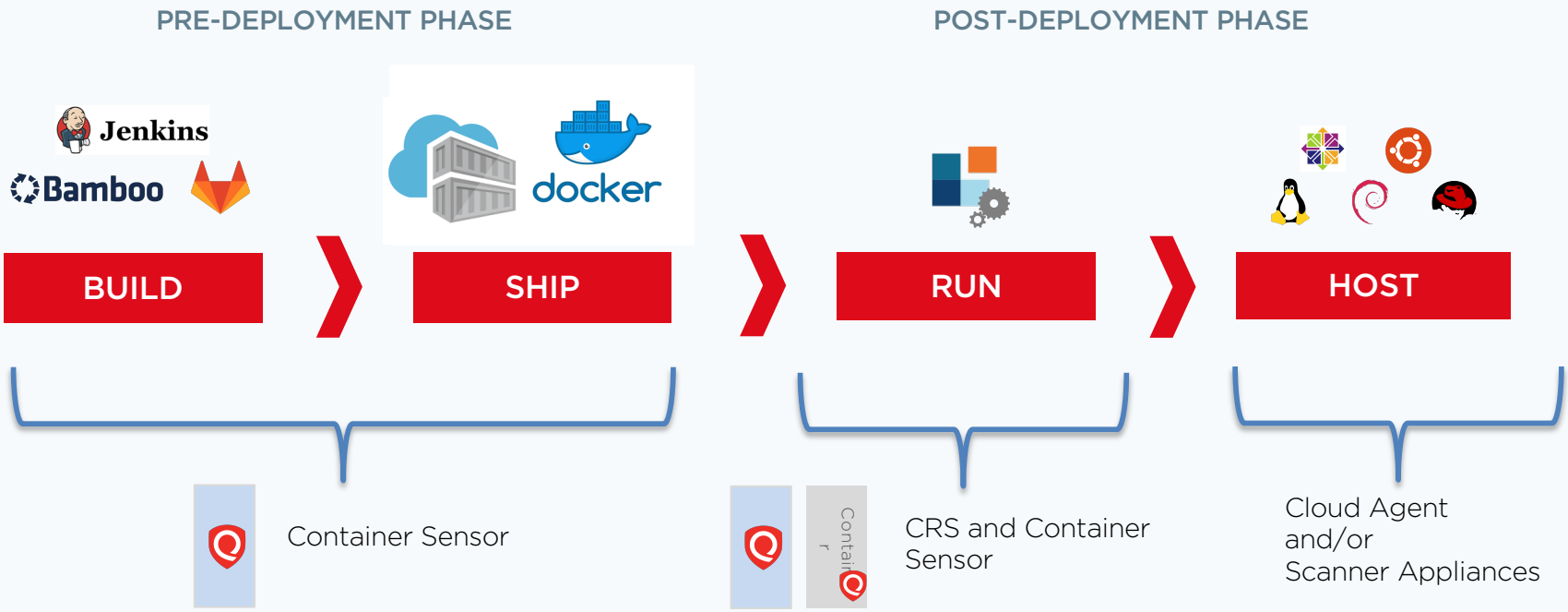
Microsoft Azure

Google Cloud Platform

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

Container Security

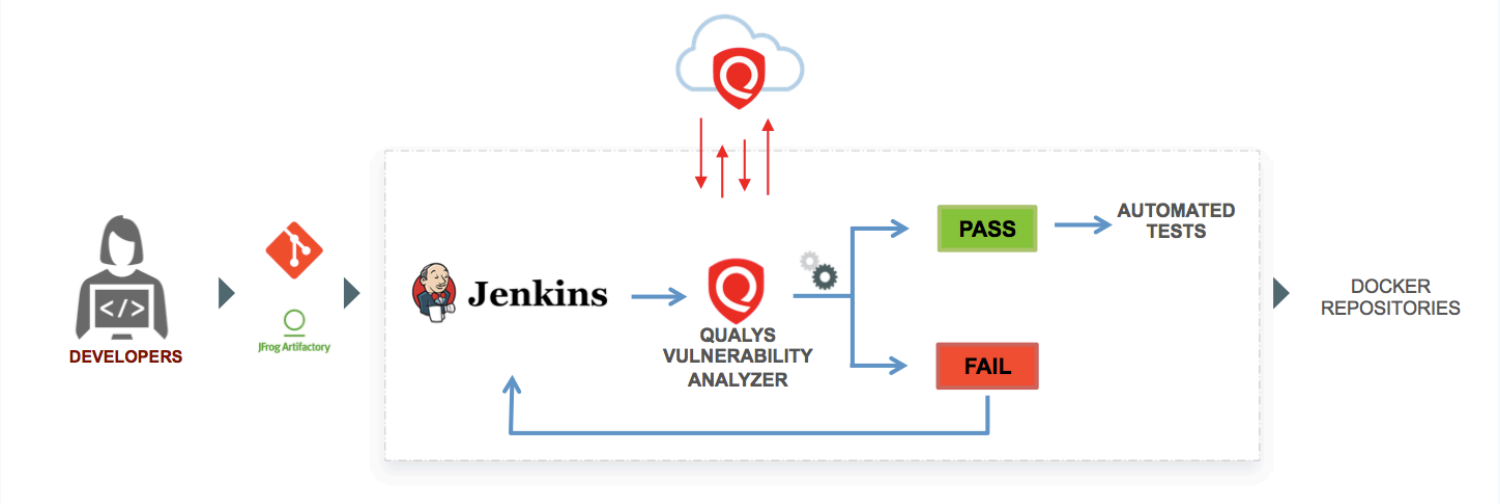
Security across the Container Lifecycle



CRS – Container Runtime

Qualys.

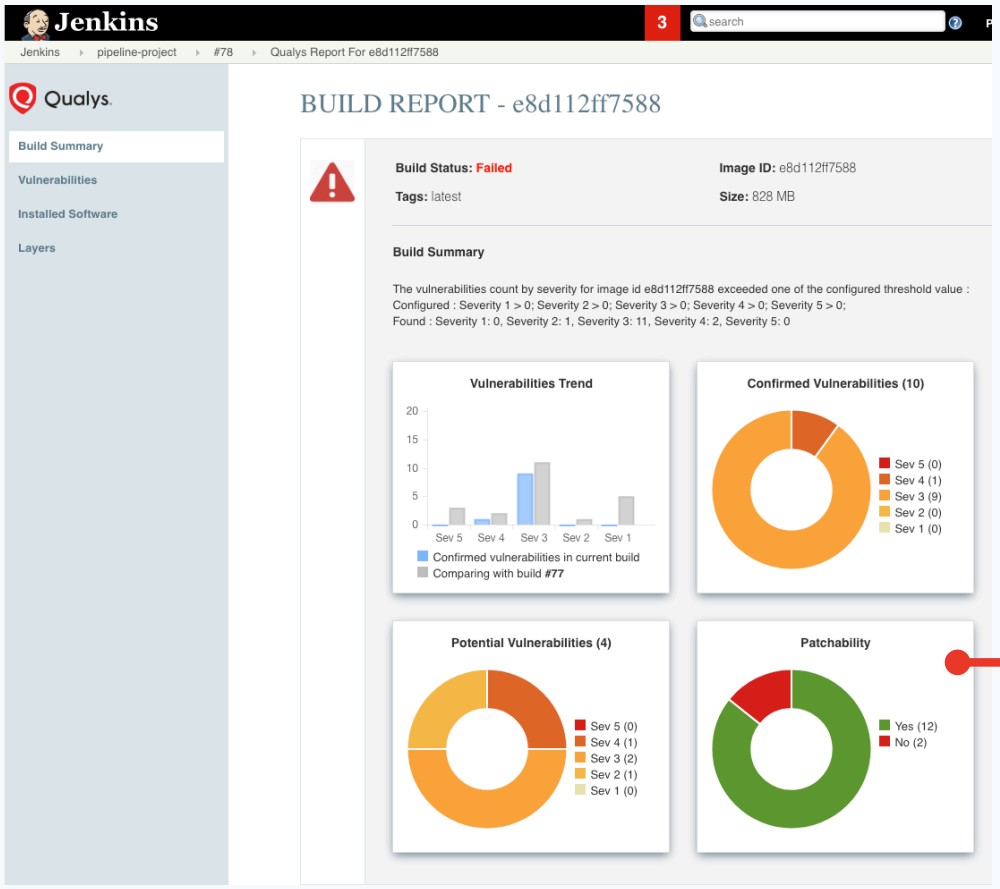
Scanning Containers in CI/CD

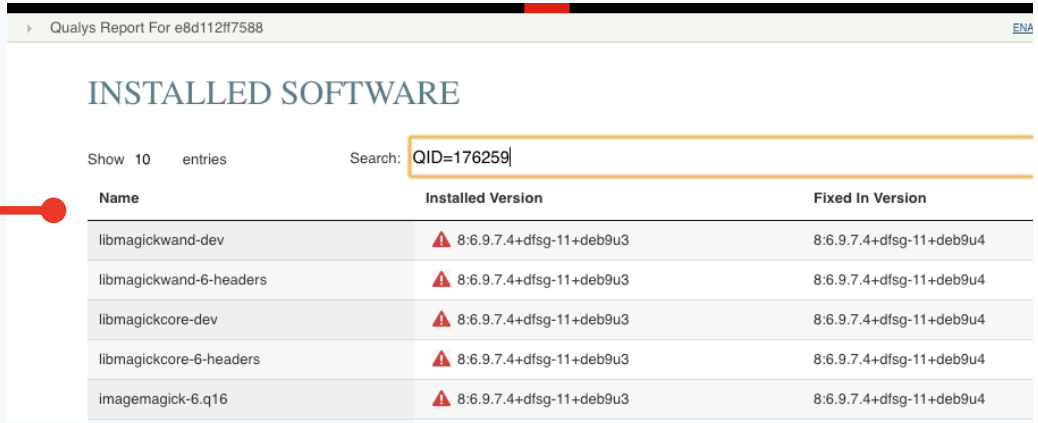


1. DevOps friendly container scanning using a plug-in
2. Actionable, detailed, high-accuracy vulnerability info for DevOps

Qualys.

Actionable Vulnerability Information for DevOps



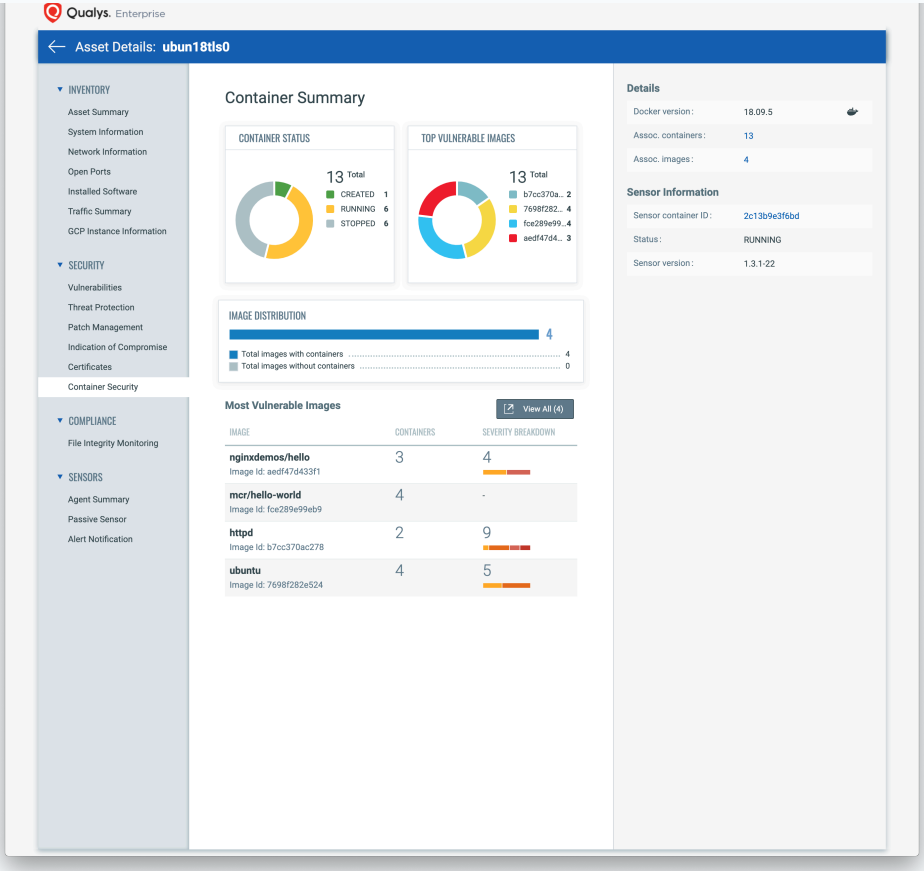


Qualys.

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



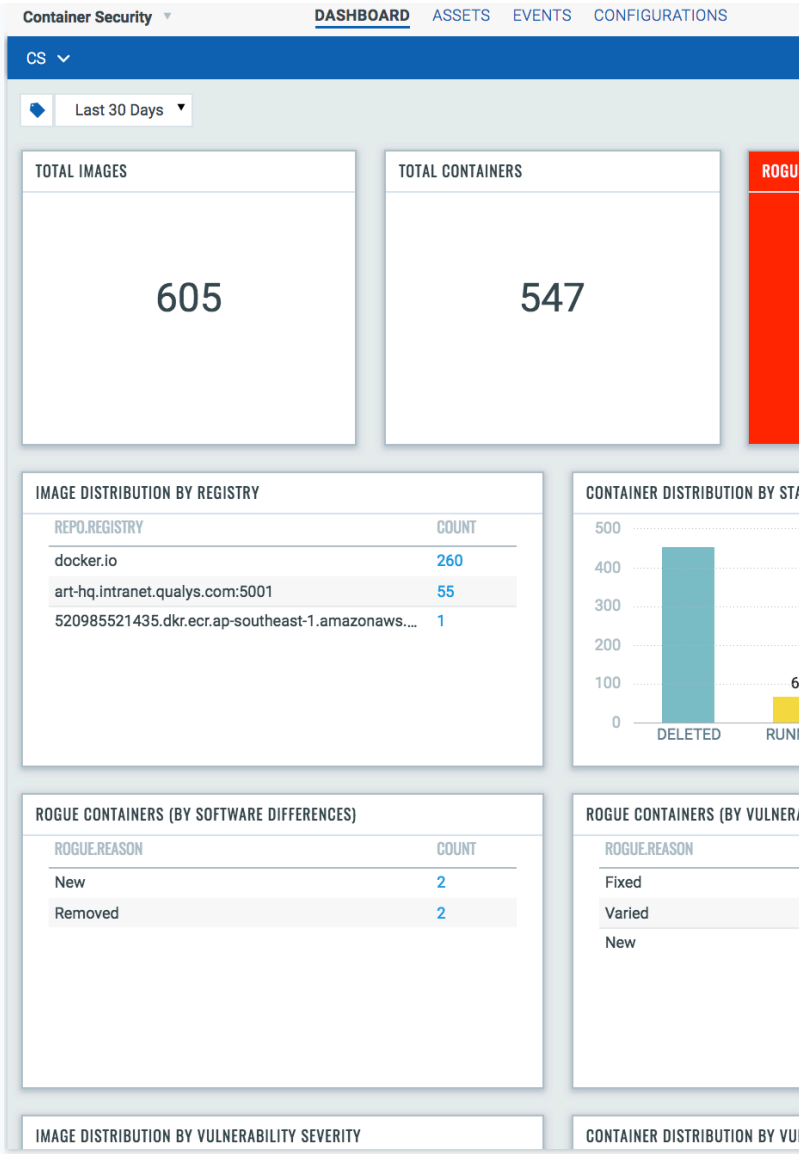
Qualys.

Deeper Visibility Into Containers

Inventory & security posture widgets

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

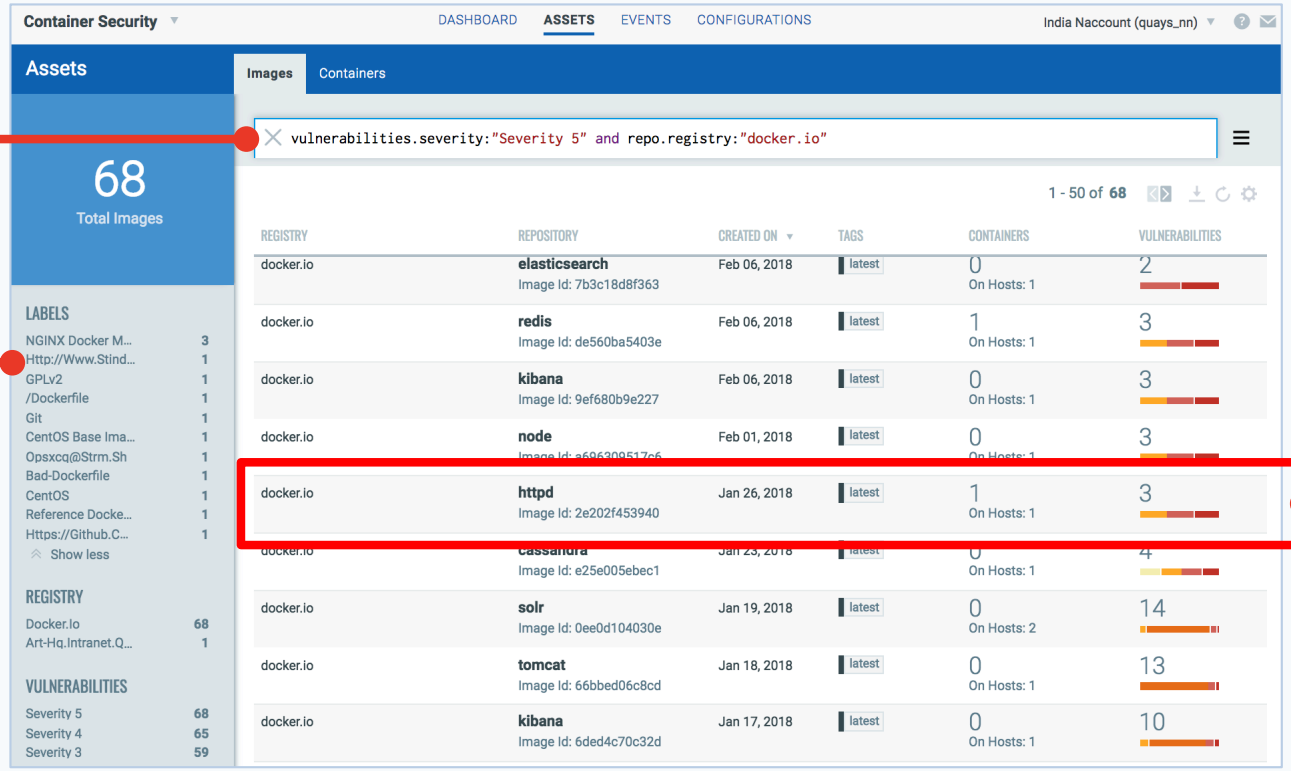
Personalize and add custom widgets



Correlating with vulnerability data

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

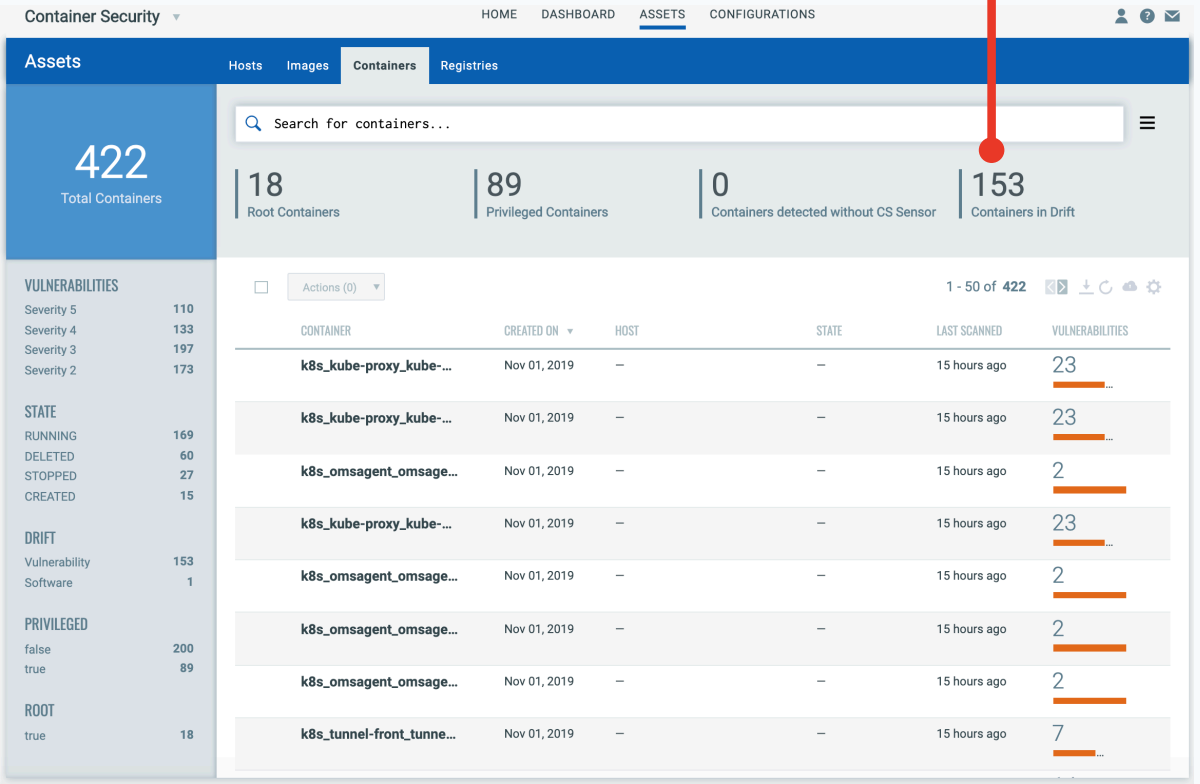
Qualys

Detecting Runtime Drift

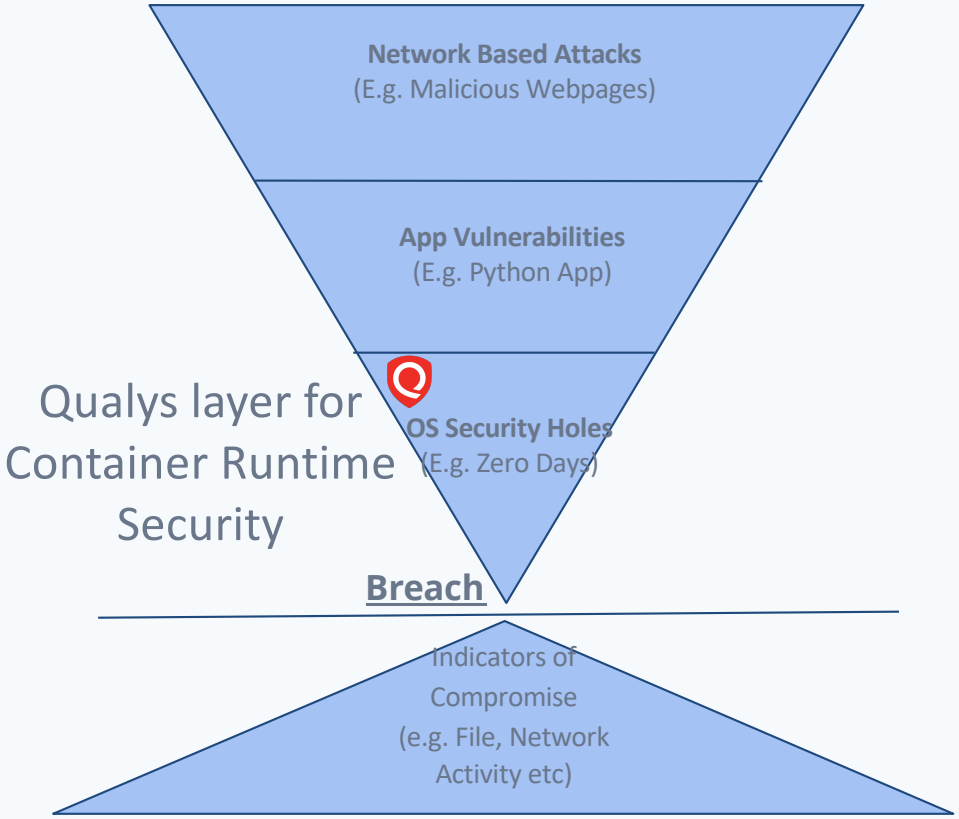
Identify potential breaches in containers

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

Detect Containers breaking off from "immutable" behavior



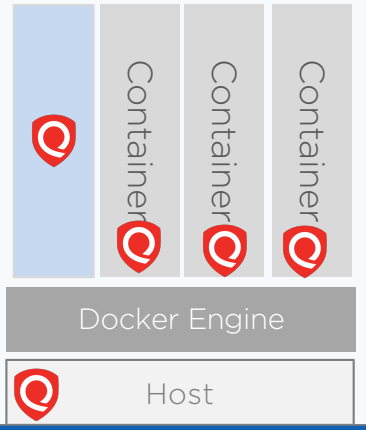
Protecting Containers at Runtime

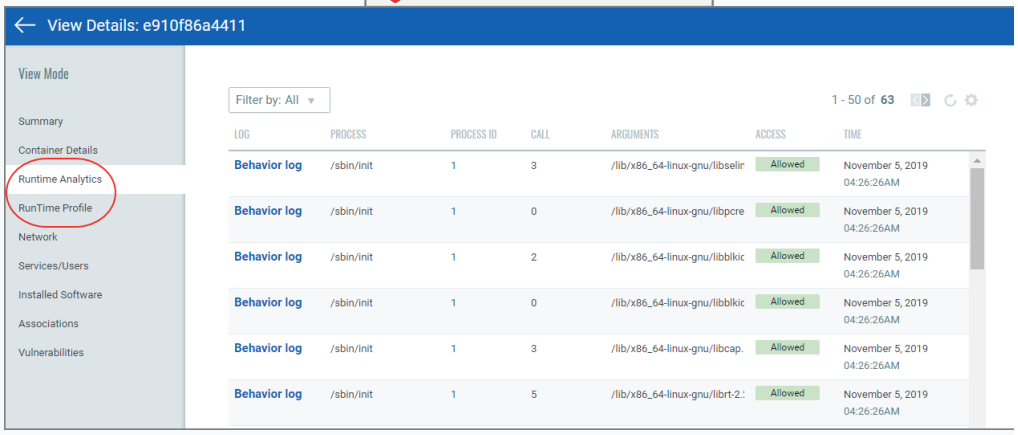


NEW

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

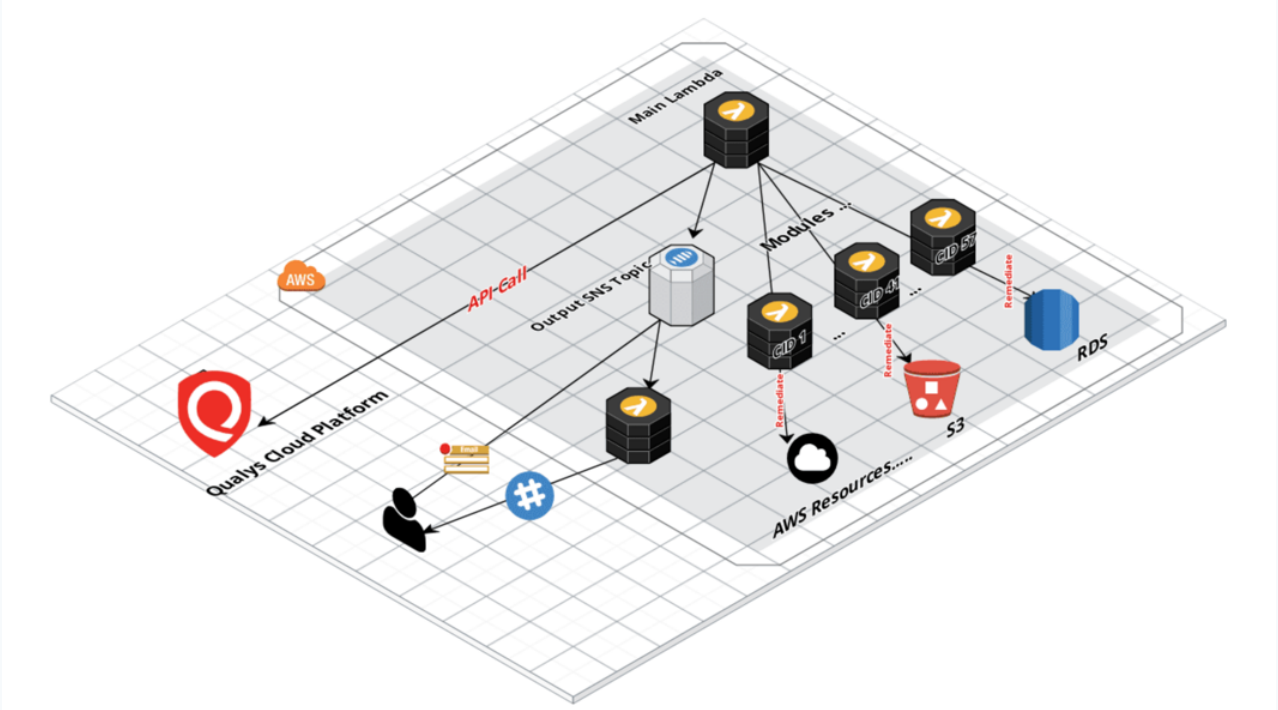




DEMO


The Road Ahead

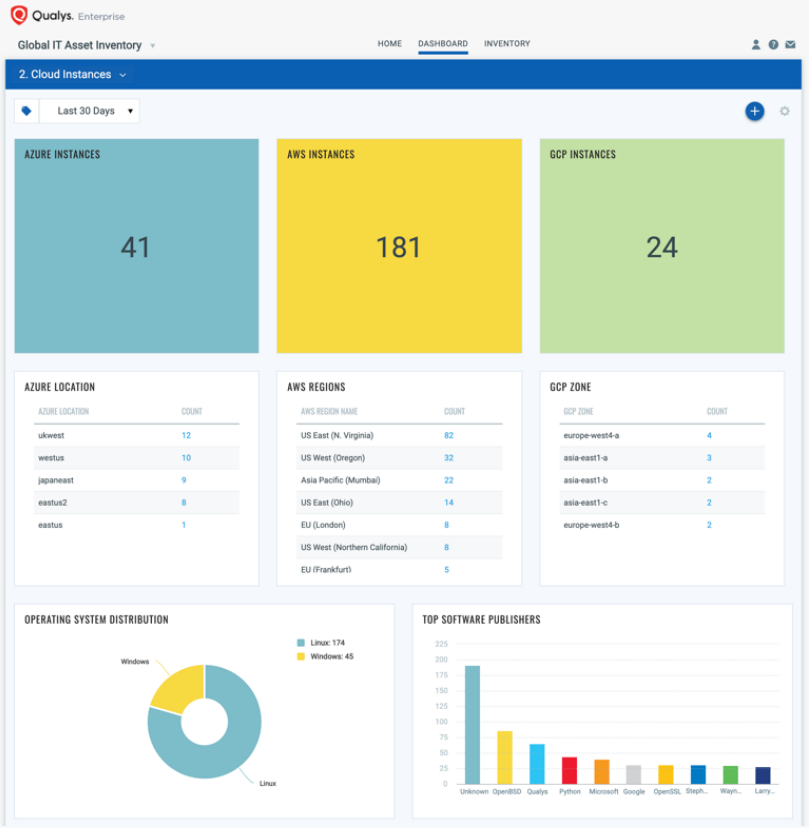
Moving Towards Automated Remediation



Qualys.

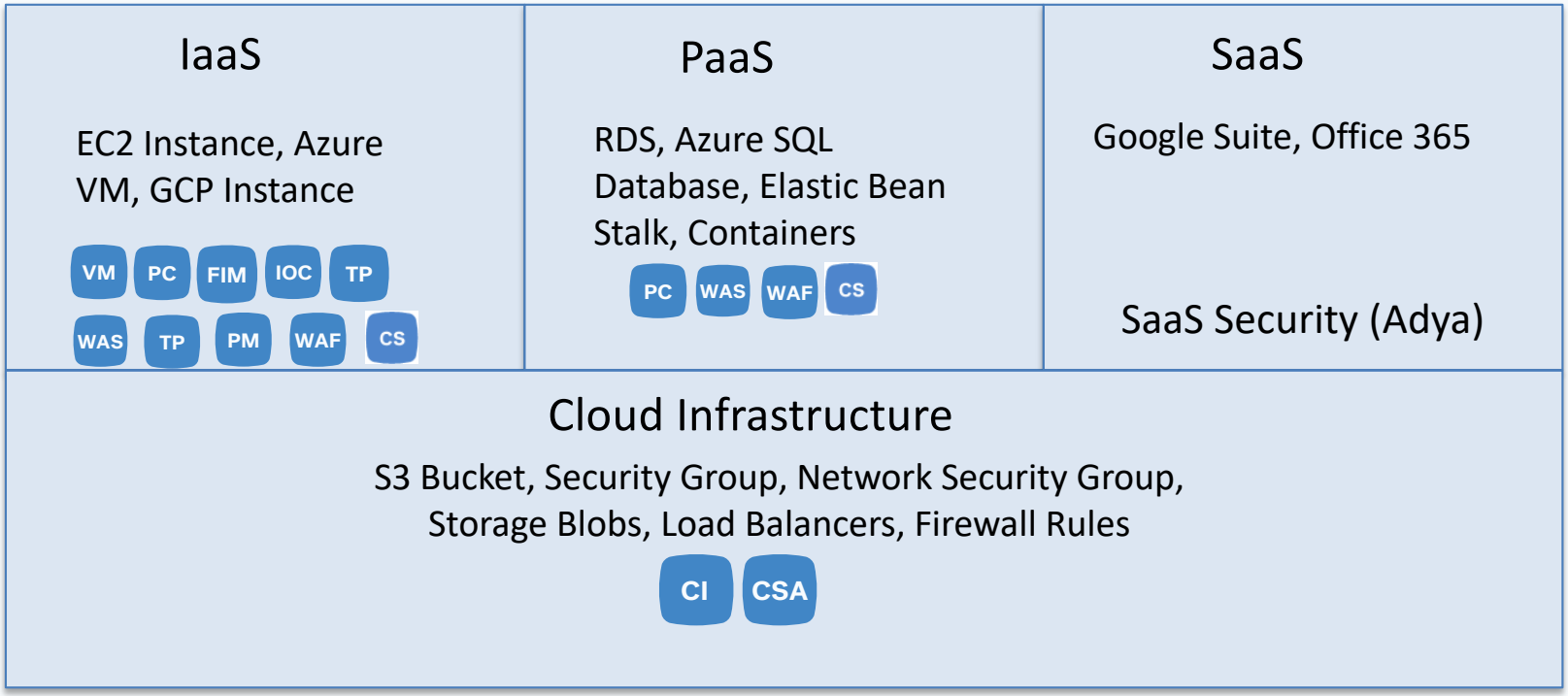
Towards Seamless Visibility

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



Qualys.

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

Thank You

Badri Raghunathan
braghunathan@qualys.com