QUALYS SECURITY CONFERENCE 2020

Securing Cloud & Container Workloads

Badri Raghunathan
Director, Product Management, Qualys, Inc.

Security Challenges in the Cloud

Lack of visibility or control on cloud resources

Misconfiguration of cloud services

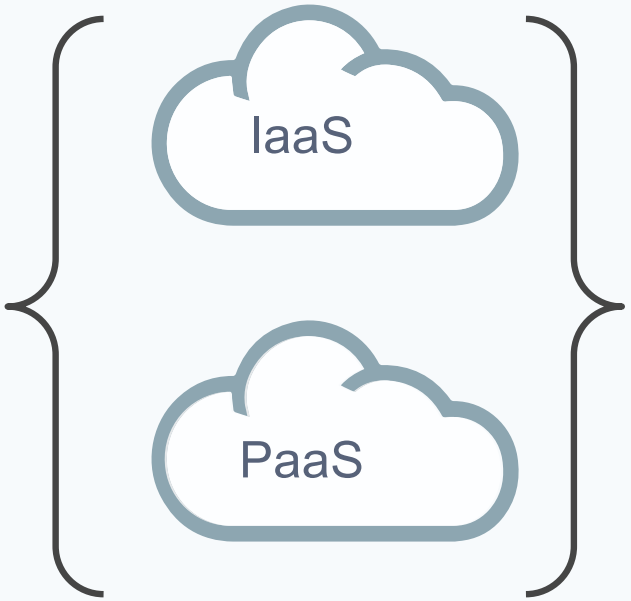
Multi cloud environment magnifies security challenges

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

Qualys.

Cloud Security

Cloud Workload Security with Qualys



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

Qualys.

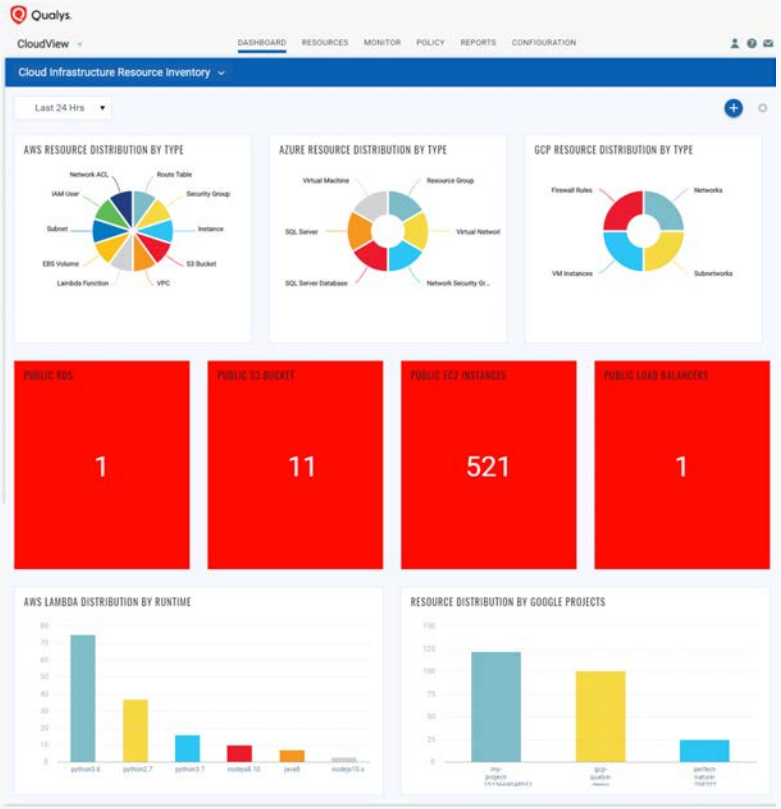
Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius



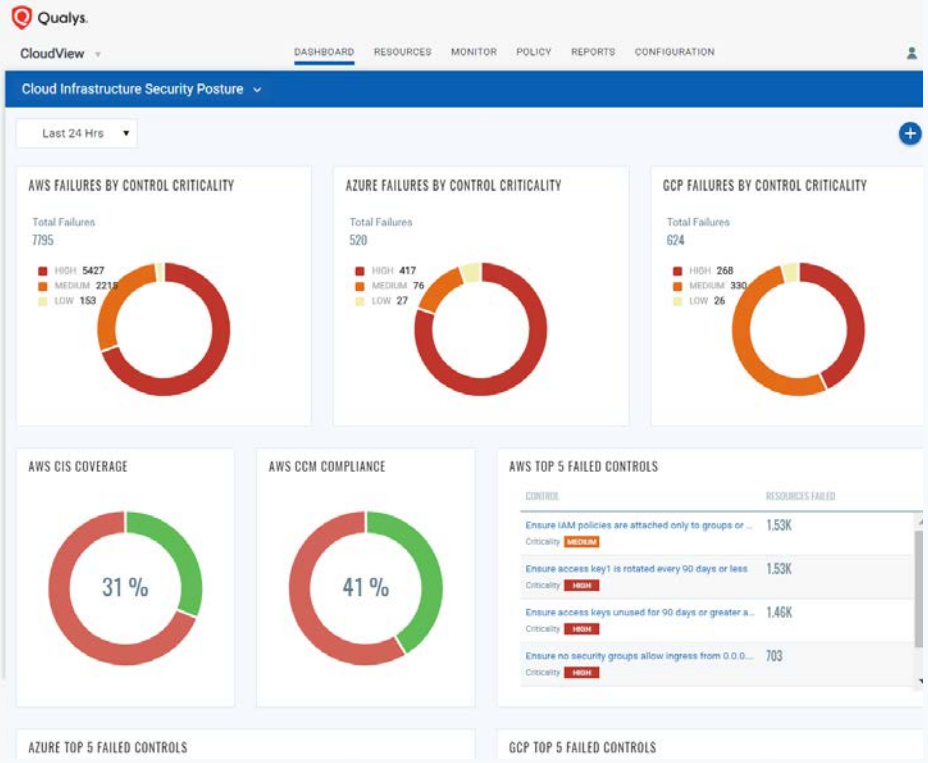
Qualys.

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

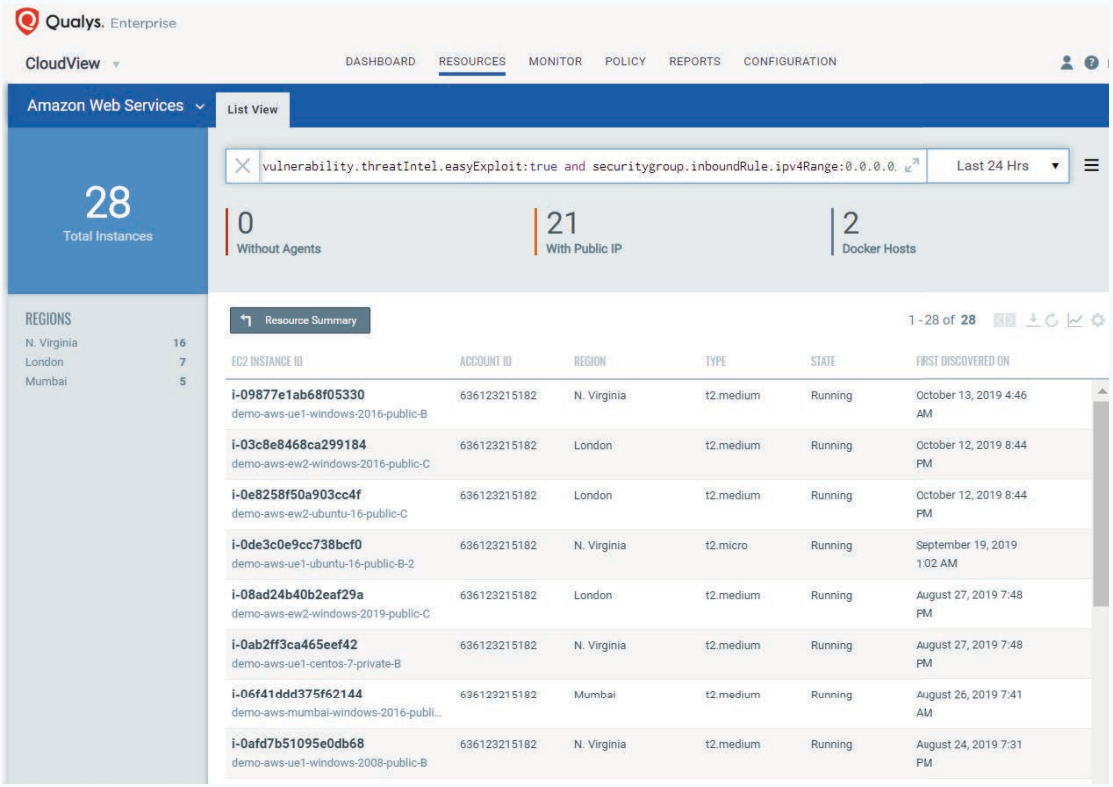


Qualys.

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



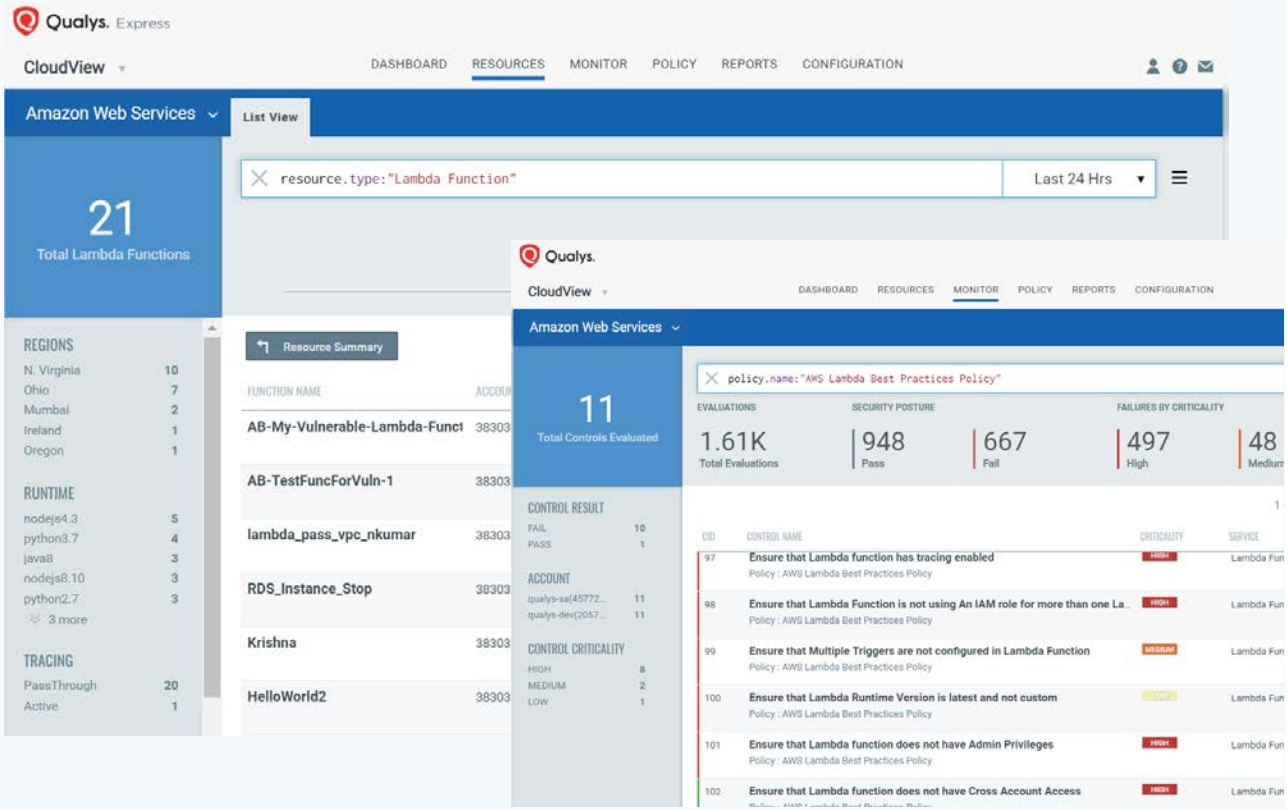
Qualys.

NEW

Serverless Visibility

Serverless Visibility – Inventory support for AWS Lambda functions

Best practices policy for identifying misconfigurations



Qualys.

NEW

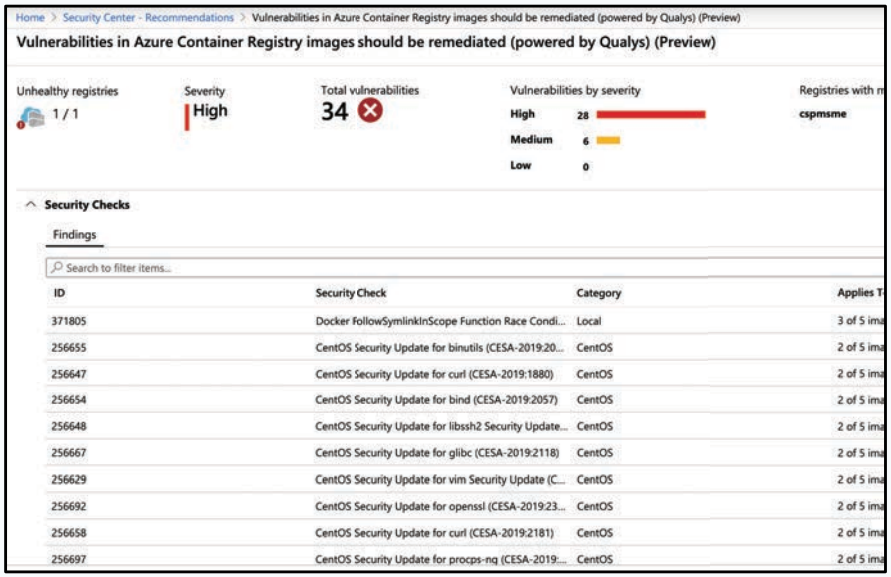
Built-in Security with Cloud Providers

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)



Native Azure Host, Container Scanning (Powered by Qualys)

Qualys.

Container Security

NEW

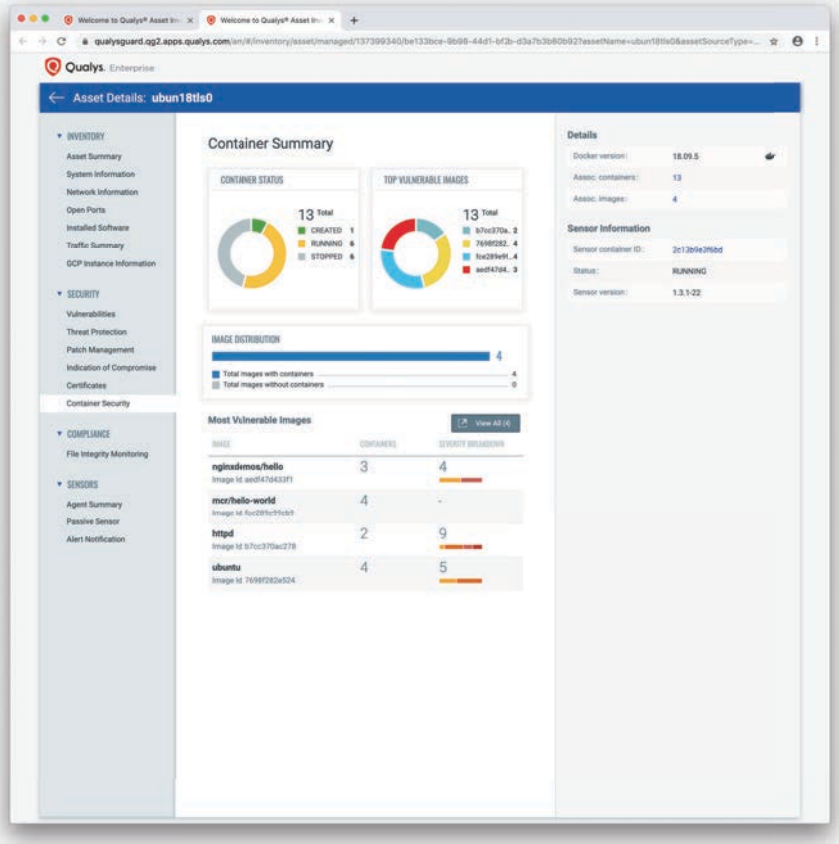
Visibility into Container Infrastructure

Inventory for all your container infrastructure (Included with VMDR)

Visibility into containers via Scanner, Cloud Agent, Container Sensor

Tracking DockerHub official images

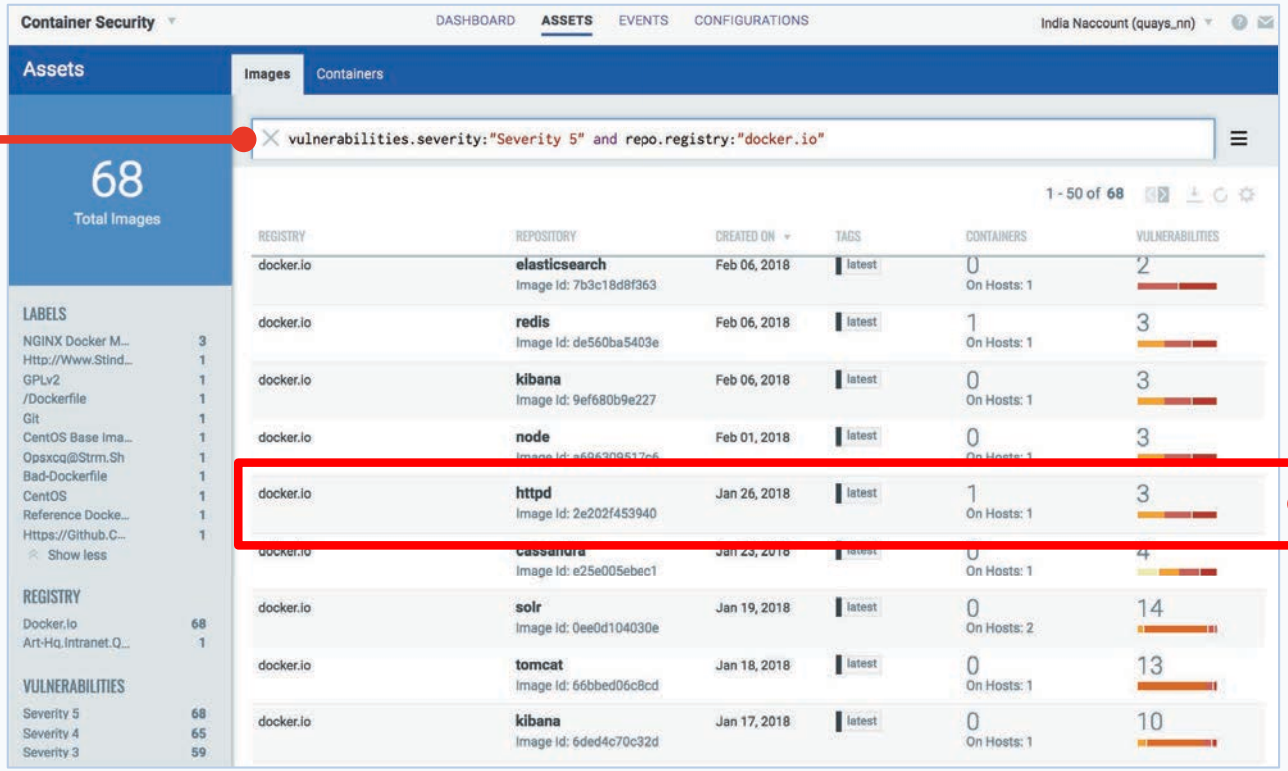
Upgrade for security across DevOps pipeline



Qualys.

Correlating with Vulnerability Data

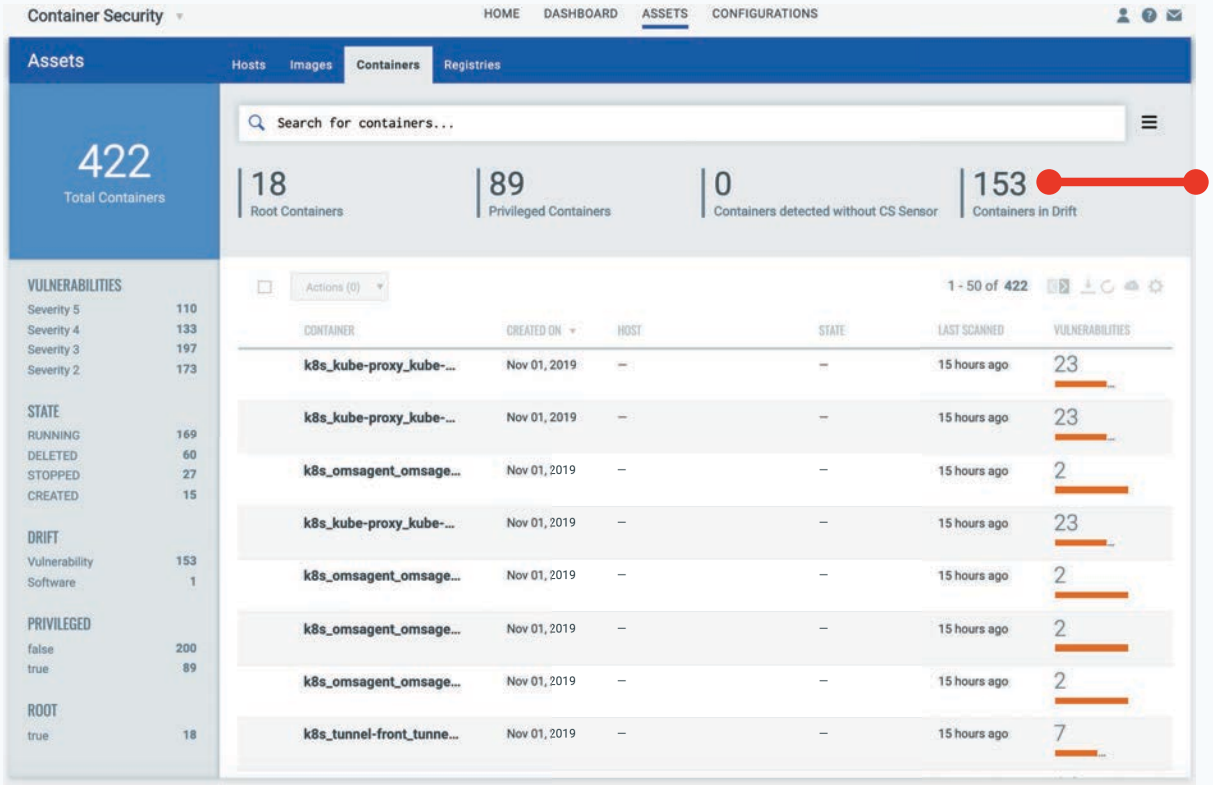
Search based on all attributes



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

Qualys.

Detecting Runtime Drift

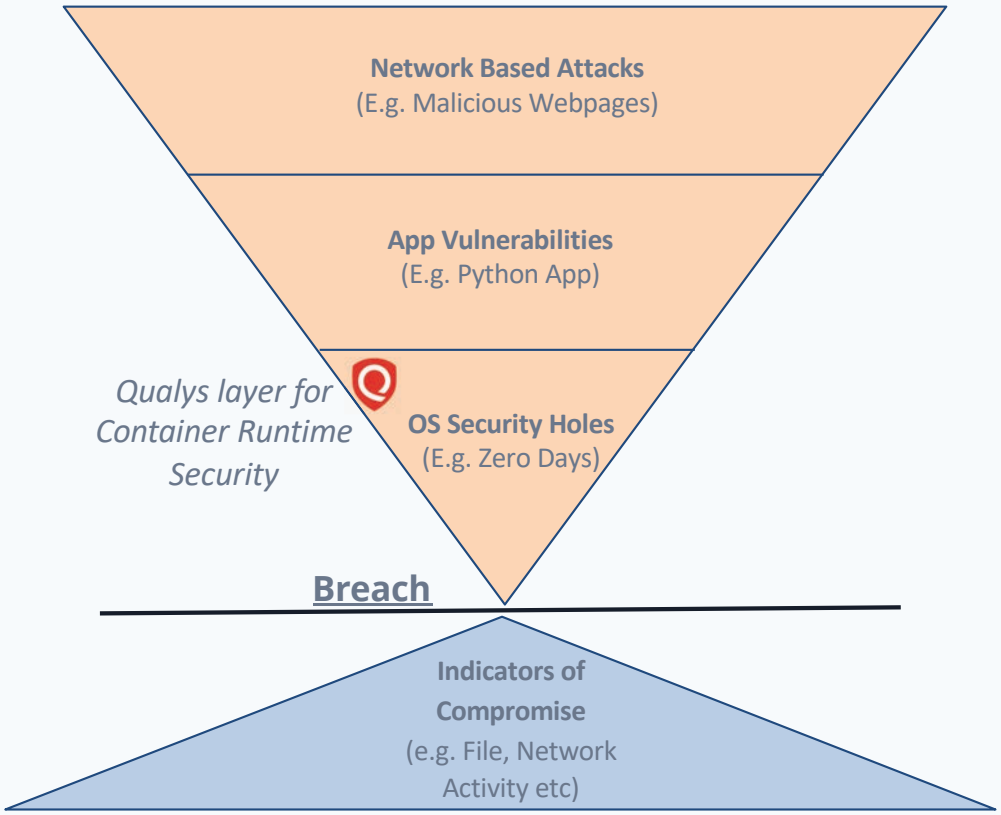


Identify potential breaches in containers

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

Qualys.

Detection, Response for Containers



Qualys.

NEW

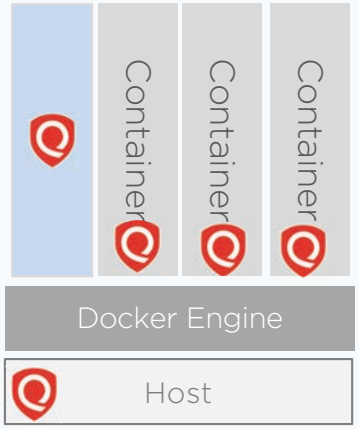
Container Runtime Security

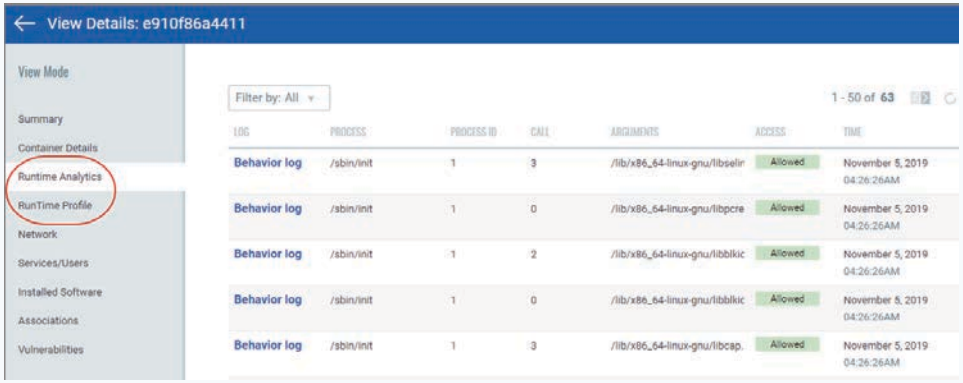
Integrated into Qualys Platform

Function level firewall for containers

Granular security policies to control file, network, process behavior

Built-in policies from Qualys Threat Research



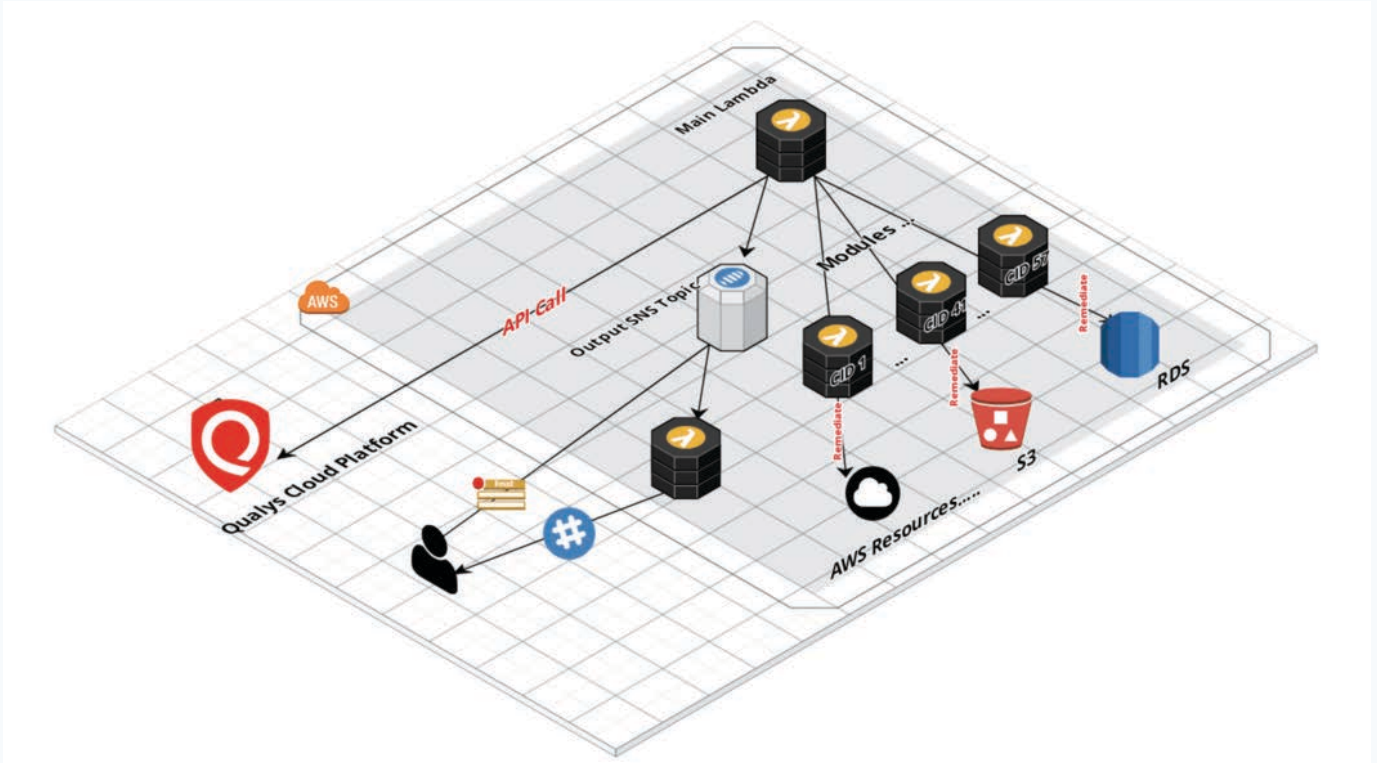


Qualys.

DEMO


The Road Ahead

Towards Automated Remediation

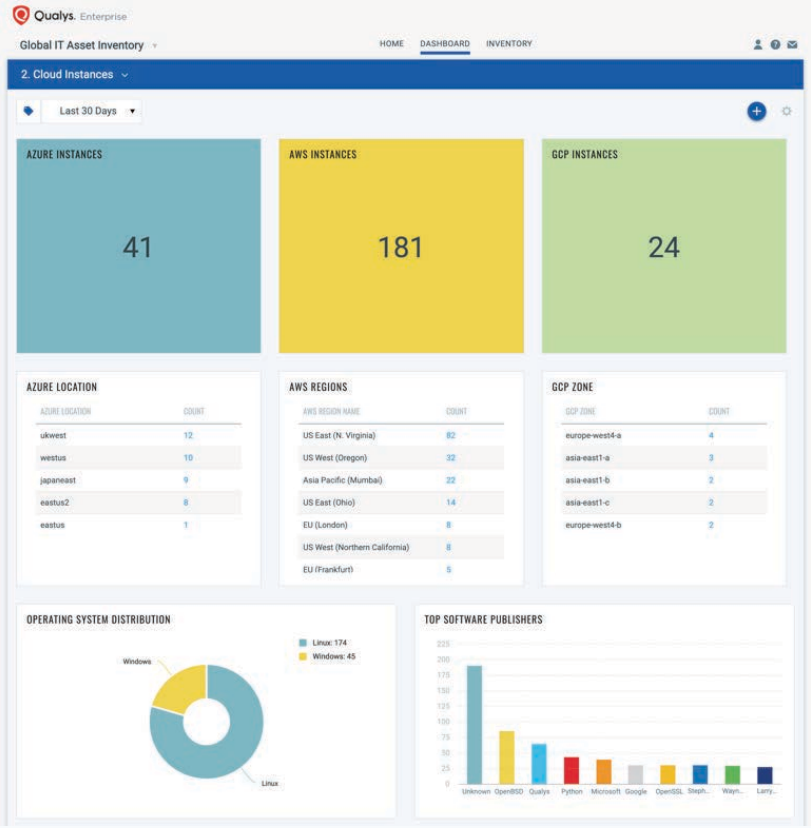


Qualys.

Towards Seamless Visibility

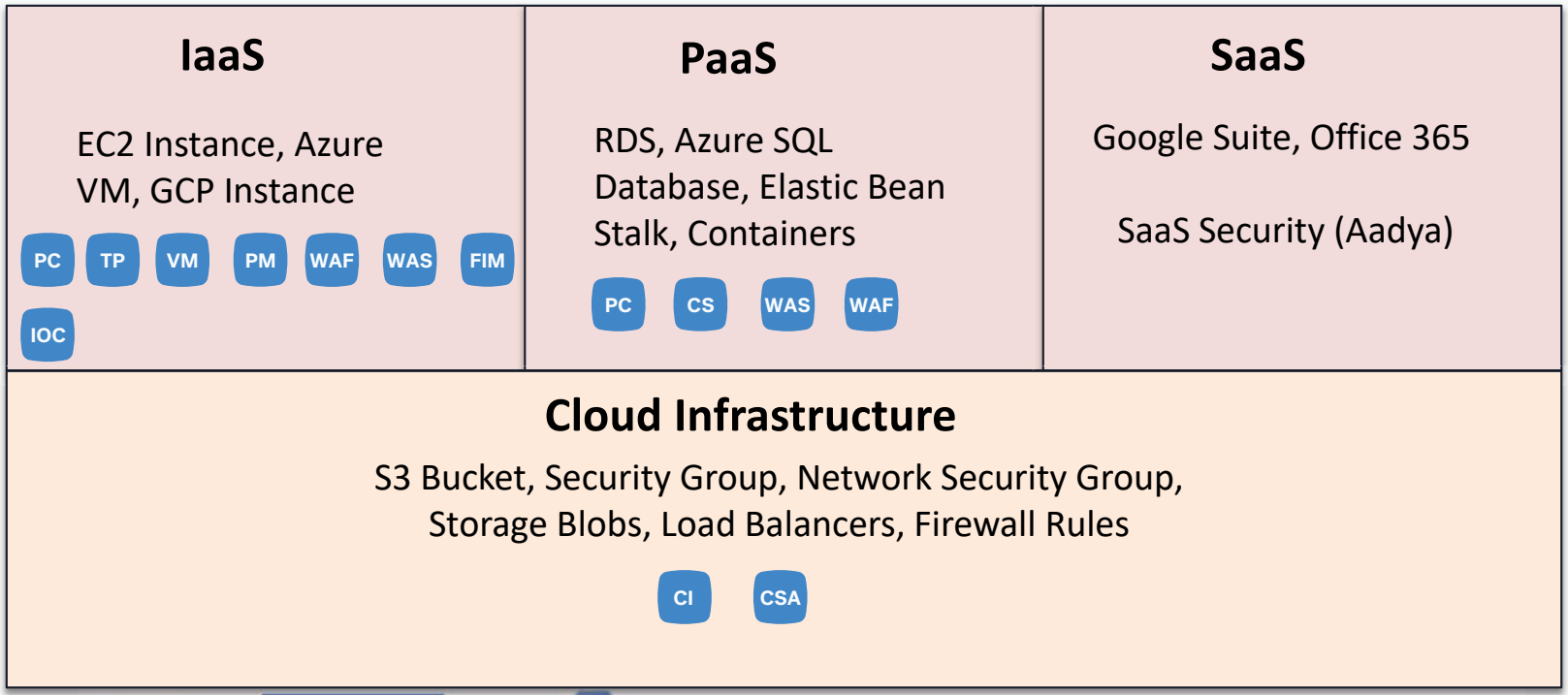
Across application stack (Hosts, Kubernetes Pods, Containers, Serverless)

Correlate cloud inventory data with containers



Qualys.

Securing Your Cloud Deployments



Thank You

Badri Raghunathan
braghunathan@qualys.com