



QUALYS SECURITY CONFERENCE 2020

Securing the Digital Transformation with DevOps

Cloud & Container Security Automation

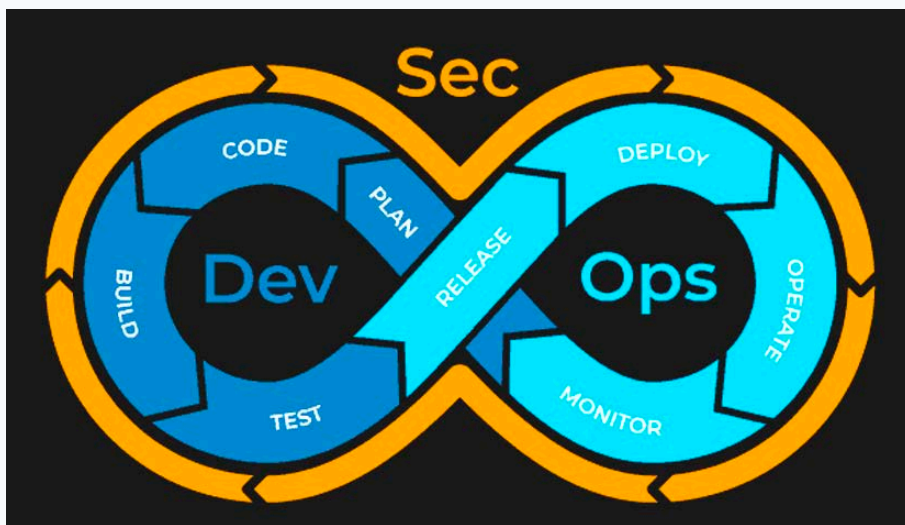
Badri Raghunathan

Director of Product Management, Qualys, Inc.



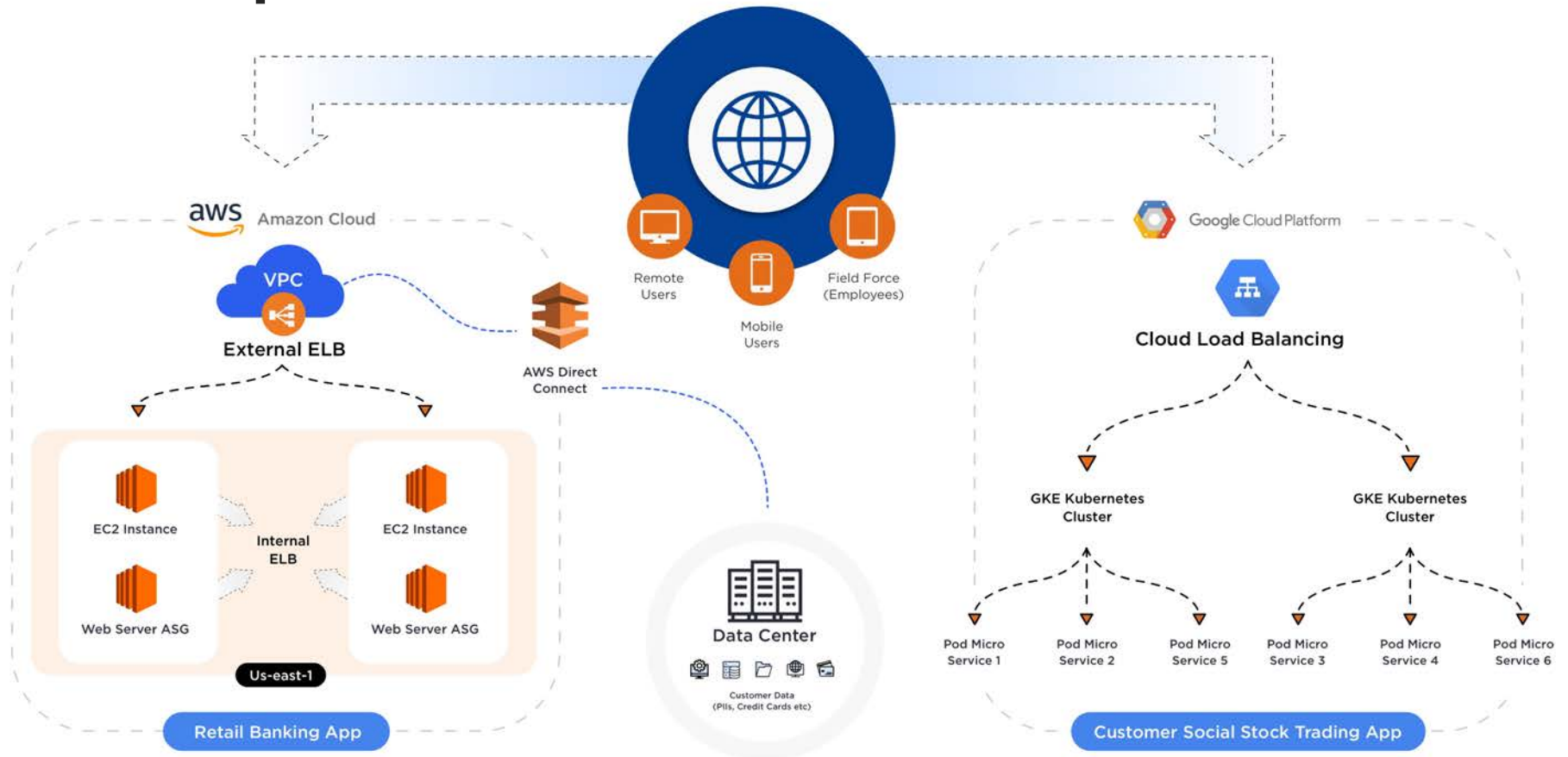
The Changing Role of Security

Security selects, builds the security tooling



DevOps operationalize the security tooling

Example Customer Scenario



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

Securing Your Cloud Deployments

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

The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted in red, one on the left side and two on the right side. The text "Cloud Security" is centered in the middle of the image.

Cloud Security

Securing Cloud Workloads

Hardening and Standardizing

Vulnerability Management

- Asset Inventory & Vulnerability Assessment (Internal & Perimeter)
- Prioritization using Threat Protection
- Indicators of Compromise
- Patch Management

Policy Compliance

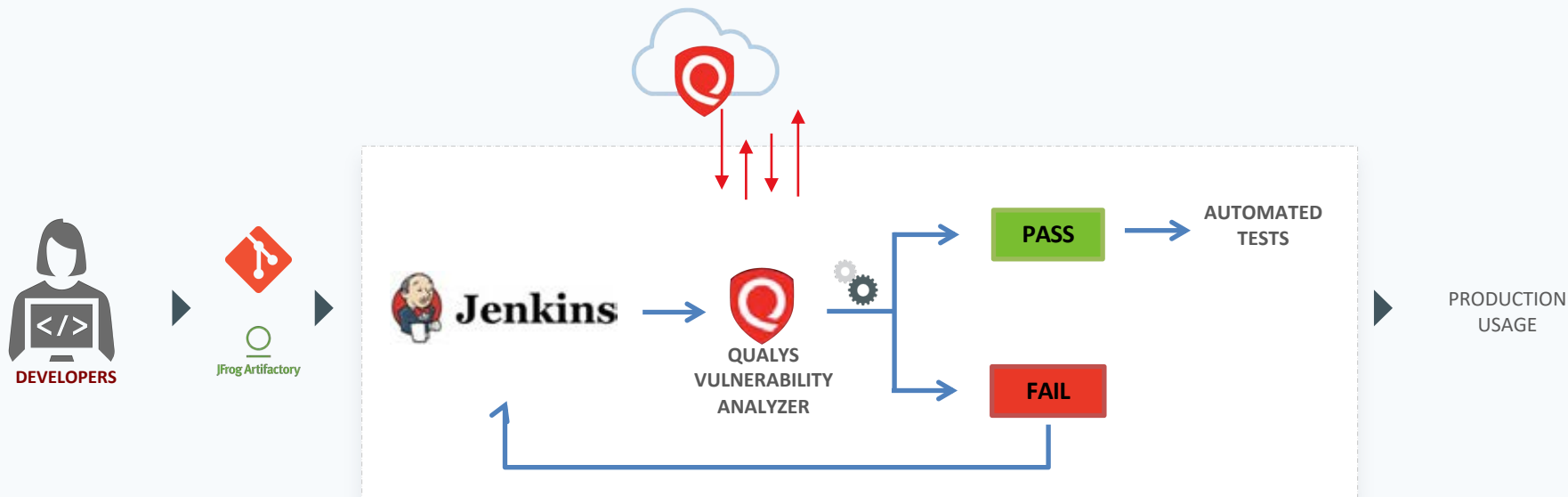
- Policy Compliance
- File Integrity Monitoring

Application Security

- Web Application Scanning
- Web Application Firewall
- API Security*

Vulnerability Analysis in CI/CD

Blocking vulnerable applications/images entering production



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

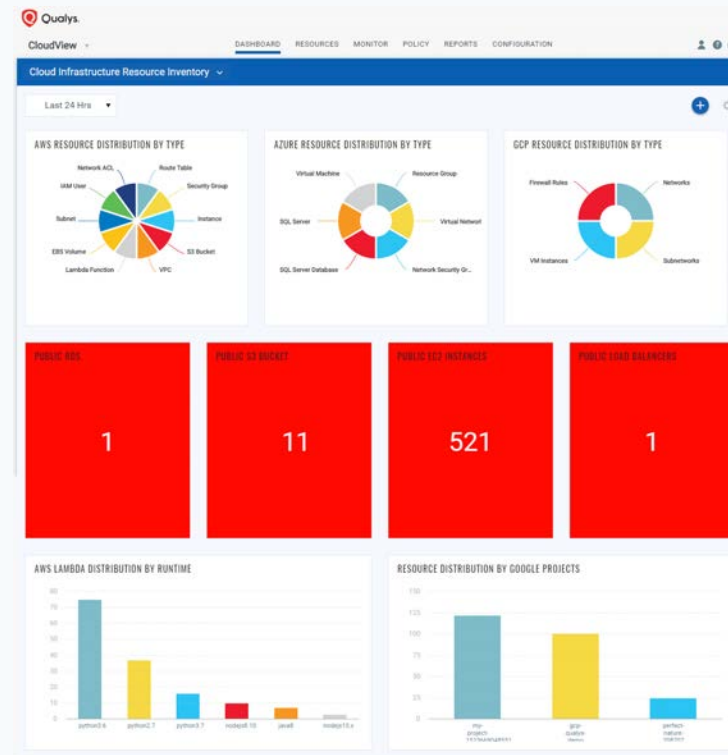
Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

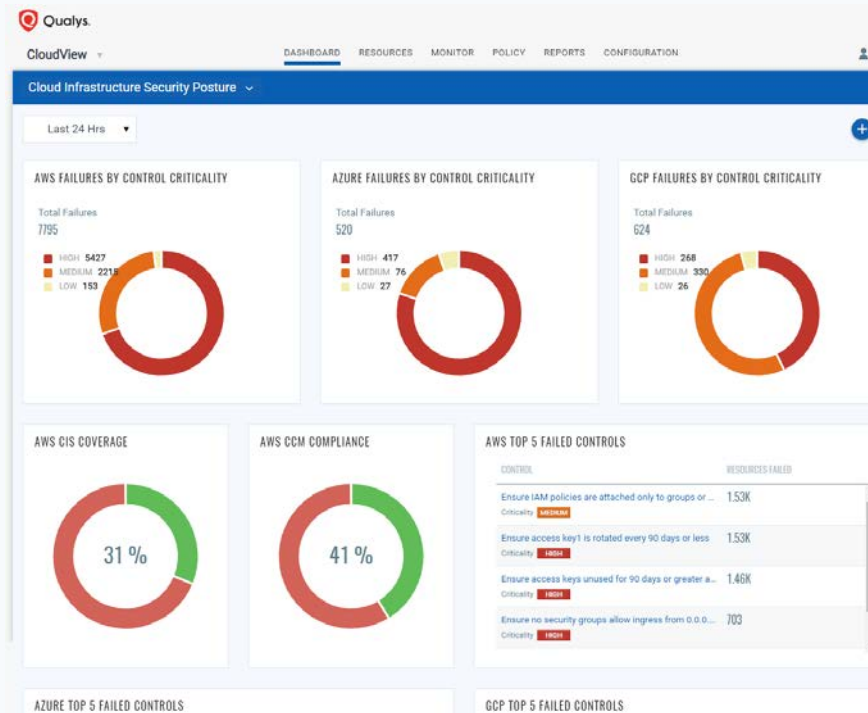


Compliance Assessment

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

The screenshot displays the Qualys Enterprise CloudView interface for Amazon Web Services. The search query is: `vulnerability.threatIntel.easyExploit:true and securitygroup.inboundRule.ipv4Range:0.0.0.0`. The summary shows 28 total instances, with 0 without agents, 21 with public IP, and 2 Docker hosts. The table below lists the instances with their EC2 Instance IDs, Account IDs, Regions, Types, States, and First Discovered On dates.

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

Serverless Visibility –
Inventory support for
AWS Lambda functions

Best practices policy for
identifying
misconfigurations

The screenshot displays the Qualys Express CloudView interface for Amazon Web Services. The top navigation bar includes Dashboard, Resources, Monitor, Policy, Reports, and Configuration. The main content area is divided into several sections:

- Amazon Web Services - List View:** Shows a search filter for "resource.type: 'Lambda Function'" and a count of 21 Total Lambda Functions. A sidebar lists regions (N. Virginia: 10, Ohio: 7, Mumbai: 2, Ireland: 1, Oregon: 1) and runtimes (nodejs4.3: 5, python3.7: 4, java8: 3, nodejs8.10: 3, python2.7: 3, and 3 more). A Tracing section shows PassThrough: 20 and Active: 1.
- Resource Summary:** A table listing Lambda functions:

FUNCTION NAME	ACCOUNT
AB-My-Vulnerable-Lambda-Funct	38303
AB-TestFuncForVuln-1	38303
lambda_pass_vpc_nkumar	38303
RDS_Instance_Stop	38303
Krishna	38303
HelloWorld2	38303
- Control Evaluation Summary:** Shows 11 Total Controls Evaluated. A table of control results:

CONTROL RESULT	Fails	Passes
FAIL	10	
PASS		1
- Policy Evaluation:** Shows the "AWS Lambda Best Practices Policy" with 1.61K Total Evaluations. A summary table:

SECURITY POSTURE	FAILURES BY CRITICALITY
948 Pass	667 Fail (497 High, 48 Medium)
- Control List:** A table of specific controls:

ID	CONTROL NAME	CRITICALITY	SERVICE
97	Ensure that Lambda function has tracing enabled	High	Lambda Fun
98	Ensure that Lambda Function is not using An IAM role for more than one La...	High	Lambda Fun
99	Ensure that Multiple Triggers are not configured in Lambda Function	Medium	Lambda Fun
100	Ensure that Lambda Runtime Version is latest and not custom	Medium	Lambda Fun
101	Ensure that Lambda function does not have Admin Privileges	High	Lambda Fun
102	Ensure that Lambda function does not have Cross Account Access	High	Lambda Fun

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)

Home > Security Center > Recommendations > Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)

Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)

Unhealthy registries: 1 / 1 Severity: High Total vulnerabilities: 34 Vulnerabilities by severity: High 28, Medium 6, Low 0

Registries with n... cspmsme

Security Checks

Findings

Search to filter items...

ID	Security Check	Category	Applies T
371805	Docker FollowSymLinkinScope Function Race Condi...	Local	3 of 5 ima
256655	CentOS Security Update for binutils (CESA-2019-20...	CentOS	2 of 5 ima
256647	CentOS Security Update for curl (CESA-2019-1880)	CentOS	2 of 5 ima
256654	CentOS Security Update for bind (CESA-2019-2057)	CentOS	2 of 5 ima
256648	CentOS Security Update for libssh2 Security Update...	CentOS	2 of 5 ima
256667	CentOS Security Update for glibc (CESA-2019-2118)	CentOS	2 of 5 ima
256629	CentOS Security Update for vim Security Update (C...	CentOS	2 of 5 ima
256692	CentOS Security Update for openssl (CESA-2019-23...	CentOS	2 of 5 ima
256658	CentOS Security Update for curl (CESA-2019-2181)	CentOS	2 of 5 ima
256697	CentOS Security Update for procps-ng (CESA-2019...	CentOS	2 of 5 ima

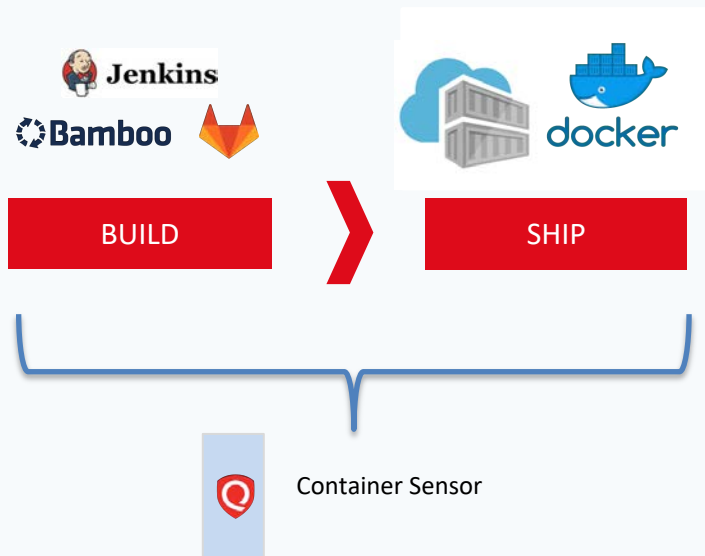
Native Azure Host, Container Scanning (Powered by Qualys)

The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted in red, one on the left side and two on the right side. The text "Container Security" is centered in the middle of the image in a white, sans-serif font.

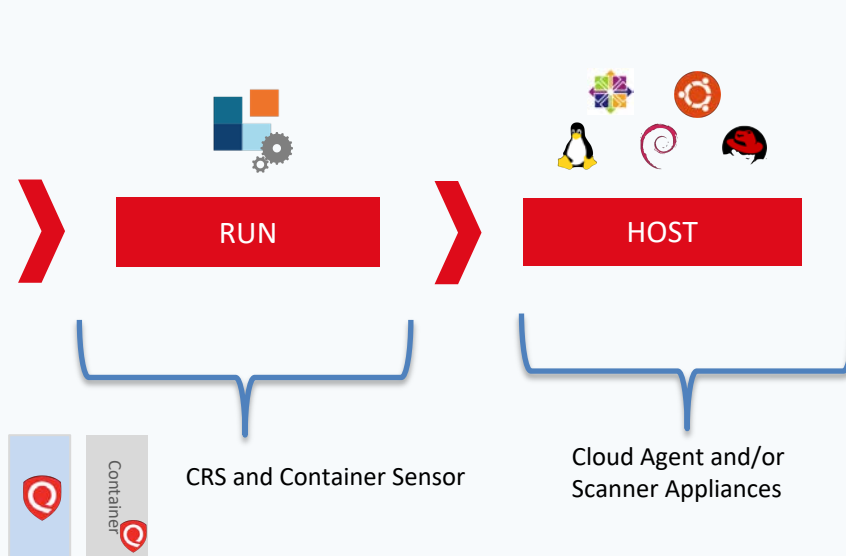
Container Security

Security across the Container Lifecycle

PRE-DEPLOYMENT PHASE



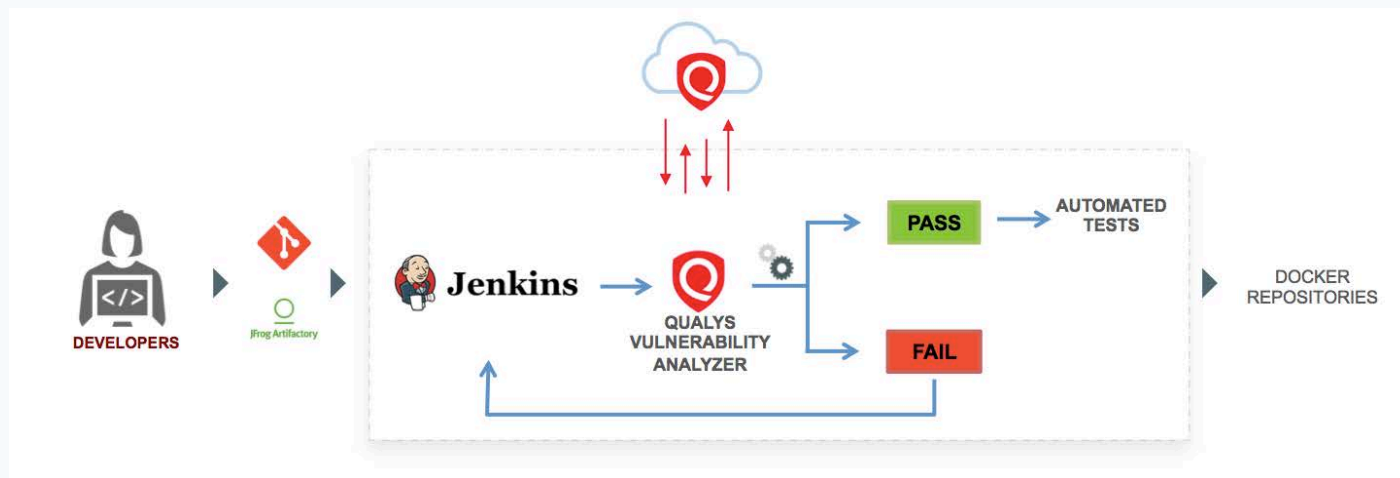
POST-DEPLOYMENT PHASE



Scanning Containers in CI/CD

DevOps friendly container scanning using a plug-in

Actionable, detailed, high-accuracy vulnerability info for DevOps



Actionable findings for Dev, DevOps

Jenkins 3 search

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

Severity	Confirmed in current build	Comparing with build #77
Sev 5	0	0
Sev 4	1	0
Sev 3	11	0
Sev 2	2	0
Sev 1	0	0

Confirmed Vulnerabilities (10)

Severity	Count
Sev 5	0
Sev 4	1
Sev 3	11
Sev 2	2
Sev 1	0

Potential Vulnerabilities (4)

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

Patchability

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

Qualys Report For e8d112ff7588

INSTALLED SOFTWARE

Show 10 entries Search: QID=176259

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

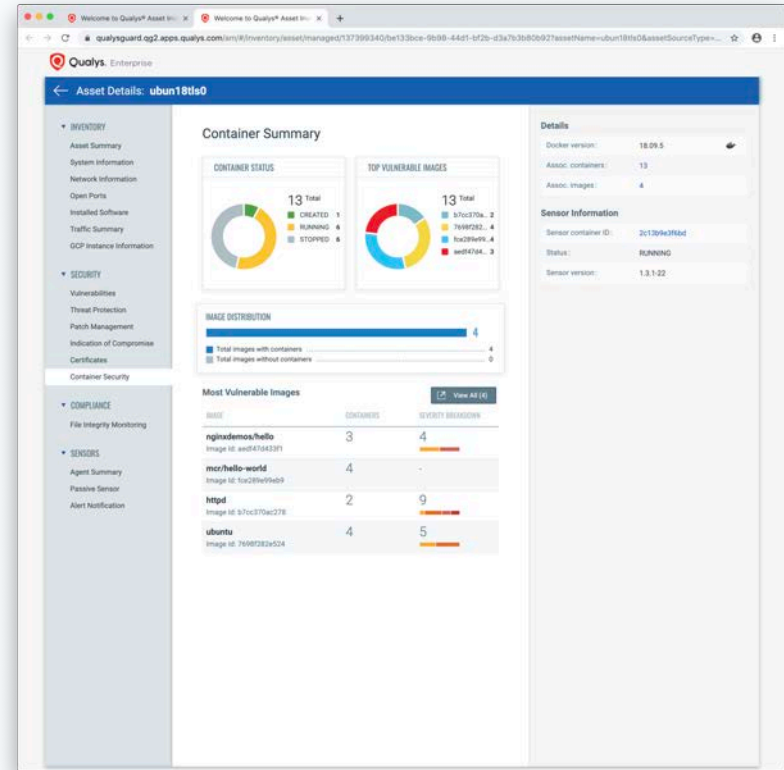
Visibility into Container Infrastructure

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

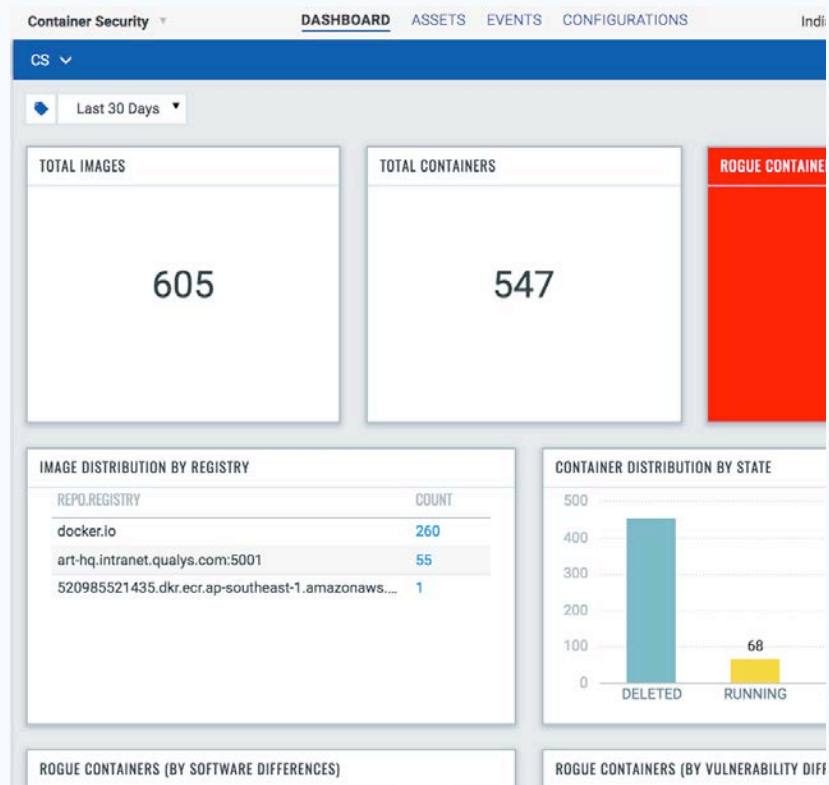


Deeper Visibility Into Containers

Inventory & security posture widgets

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

Personalize and add custom widgets



Correlating with Vulnerability Data

Search based on all attributes

Assets

68 Total Images

Labels

- NGINX Docker M... 3
- Http://Www.Stind... 1
- GPLV2 1
- /Dockerfile 1
- Git 1
- CentOS Base Ima... 1
- Opexcoq@Strm.Sh 1
- Bad-Dockerfile 1
- CentOS 1
- Reference Docke... 1
- Https://Github.C... 1
- Show less

Registry

- Docker.io 68
- Art-Hq.Intranet.Q... 1

Vulnerabilities

- Severity 5 68
- Severity 4 65
- Severity 3 59

Search: vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"

1 - 50 of 68

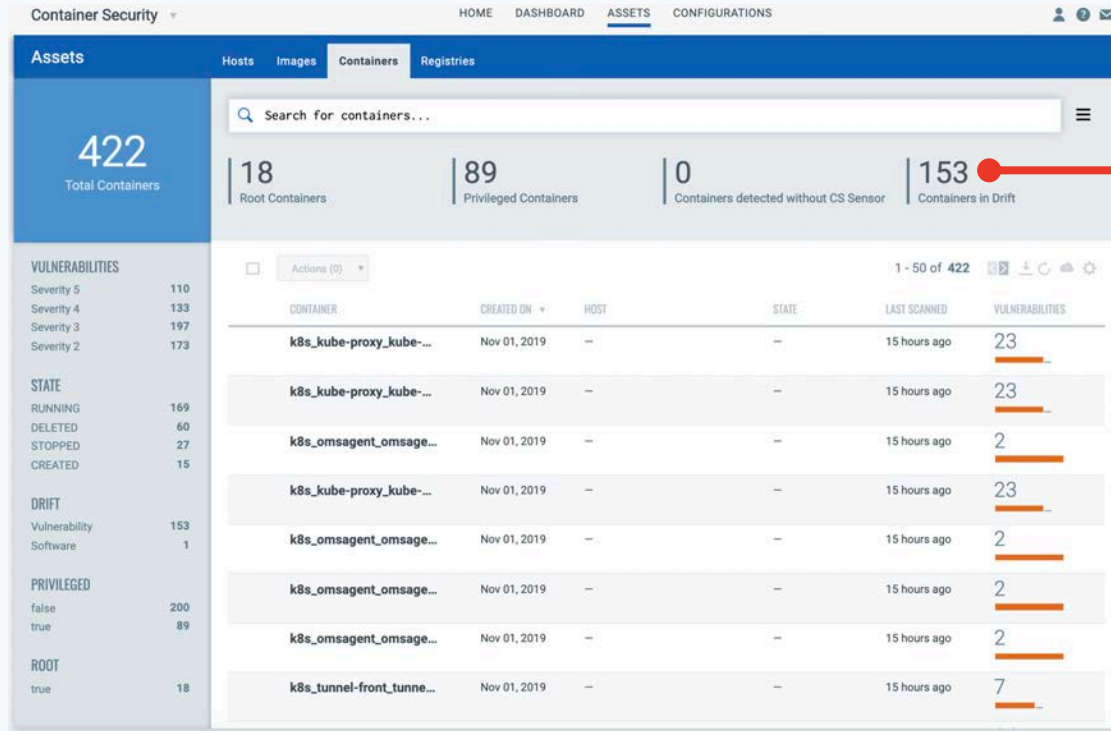
REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch Image Id: 7b3c18d8f363	Feb 06, 2018	latest	0 On Hosts: 1	2
docker.io	redis Image Id: de560ba5403e	Feb 06, 2018	latest	1 On Hosts: 1	3
docker.io	kibana Image Id: 9ef680b9e227	Feb 06, 2018	latest	0 On Hosts: 1	3
docker.io	node Image Id: e696309517c6	Feb 01, 2018	latest	0 On Hosts: 1	3
docker.io	httpd Image Id: 2e202f453940	Jan 26, 2018	latest	1 On Hosts: 1	3
docker.io	cassandra Image Id: e25e005ebec1	Jan 23, 2018	latest	0 On Hosts: 1	4
docker.io	solr Image Id: 0ee0d104030e	Jan 19, 2018	latest	0 On Hosts: 2	14
docker.io	tomcat Image Id: 66bbe06c8cd	Jan 18, 2018	latest	0 On Hosts: 1	13
docker.io	kibana Image Id: 6ded4c70c32d	Jan 17, 2018	latest	0 On Hosts: 1	10

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

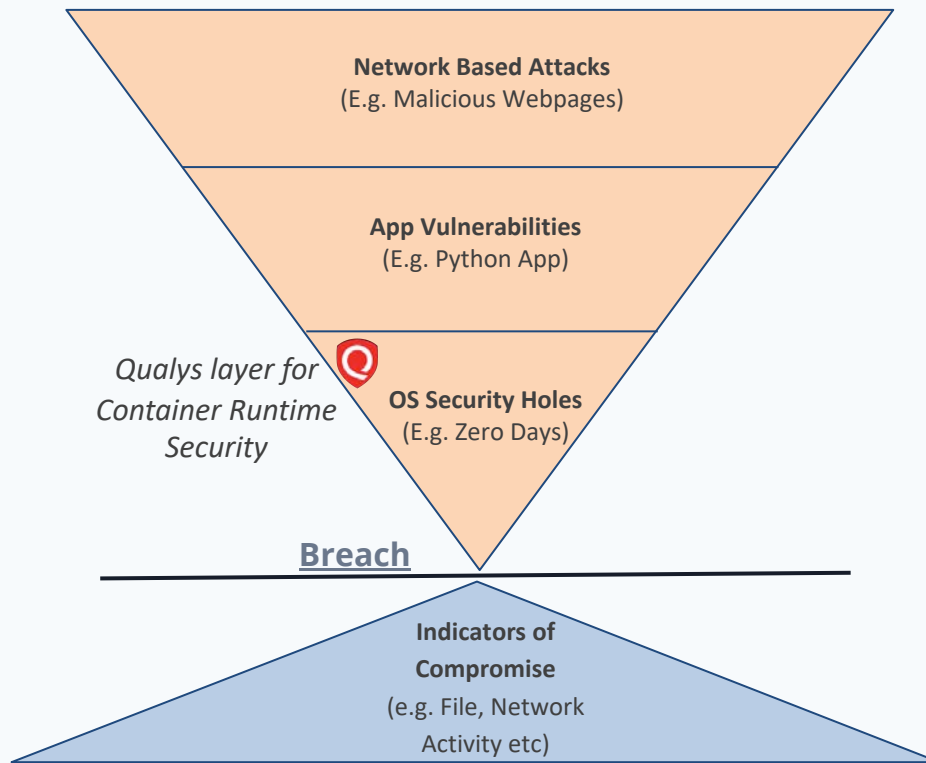
Detecting Runtime Drift



Identify potential breaches in containers

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

Hardening, Response for Containers



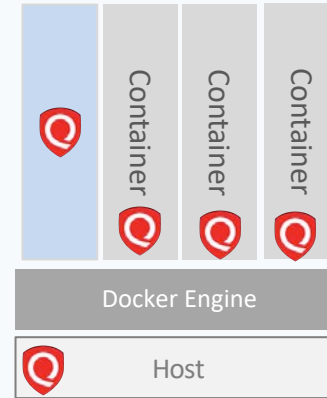
Container Runtime Security

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



← View Details: e910f86a4411

View Mode

Filter by: All

1 - 50 of 63

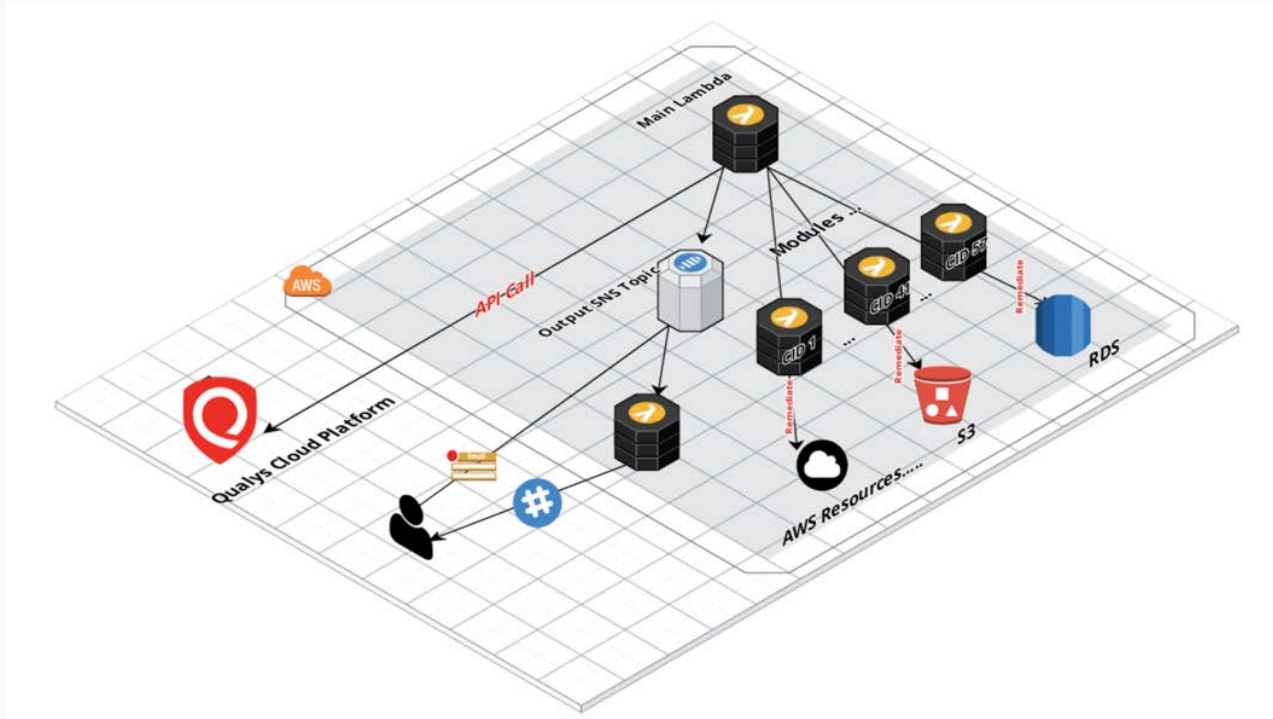
LOG	PROCESS	PROCESS ID	CALL	ARGUMENTS	ACCESS	TIME
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libselr	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libpcre	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	2	/lib/x86_64-linux-gnu/libblkid	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libblkid	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libcap	Allowed	November 5, 2019 04:26:26AM

DEMO

The Road Ahead



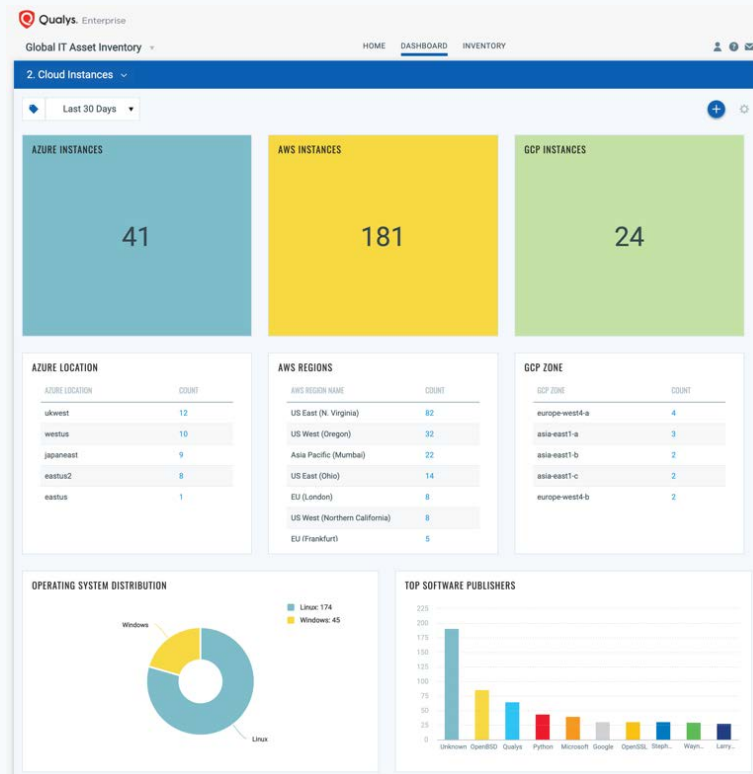
Towards Automated Remediation



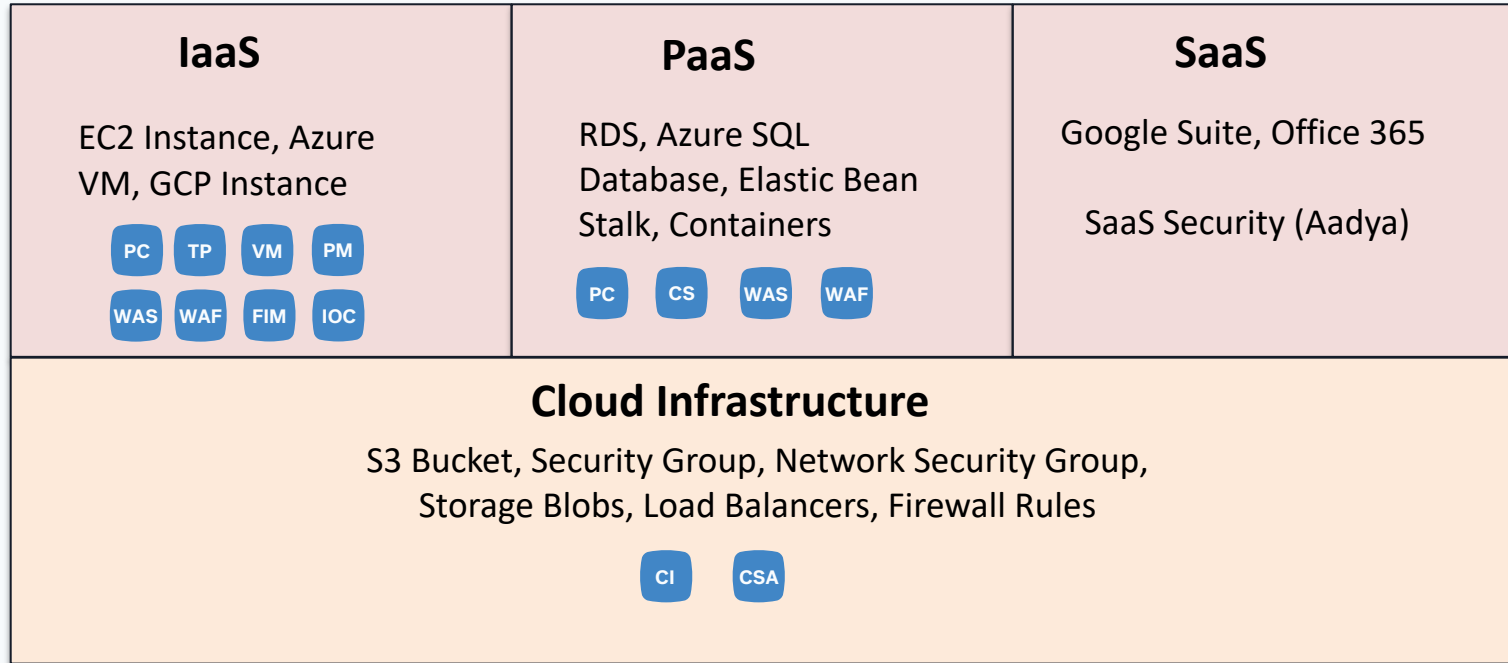
Towards Seamless Visibility

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

Correlate cloud inventory data with containers



Securing Your Cloud Deployments



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 2020

Thank You

Badri Raghunathan
braghunathan@qualys.com