Securing Your Web Applications

Raúl Benito
Country Manager Iberia

Insecure Apps & APIs are a Problem

Your business depends on web applications

Any app or API can be a foothold into your organization

Developers are not incentivized for security

Cloud-based apps are easy for developers to deploy

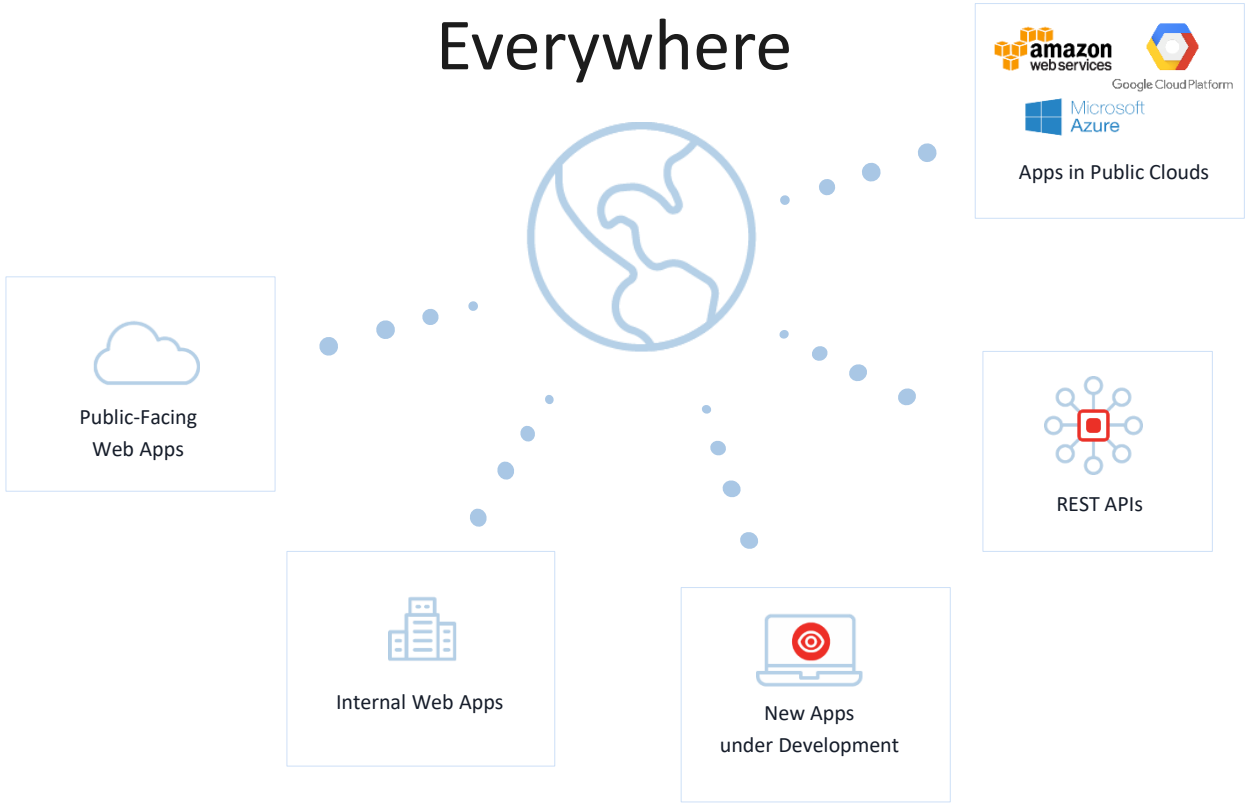
Web Applications are Being Targeted

- Most common data breach pattern *
- Top hacking vector *

Panera Bread	2018
Facebook (API)	2018
Google+ (API)	2018
MyFitnessPal (API?)	2017
Equifax	2017
Yahoo	2016
Ashley Madison	2015
OPM	2015

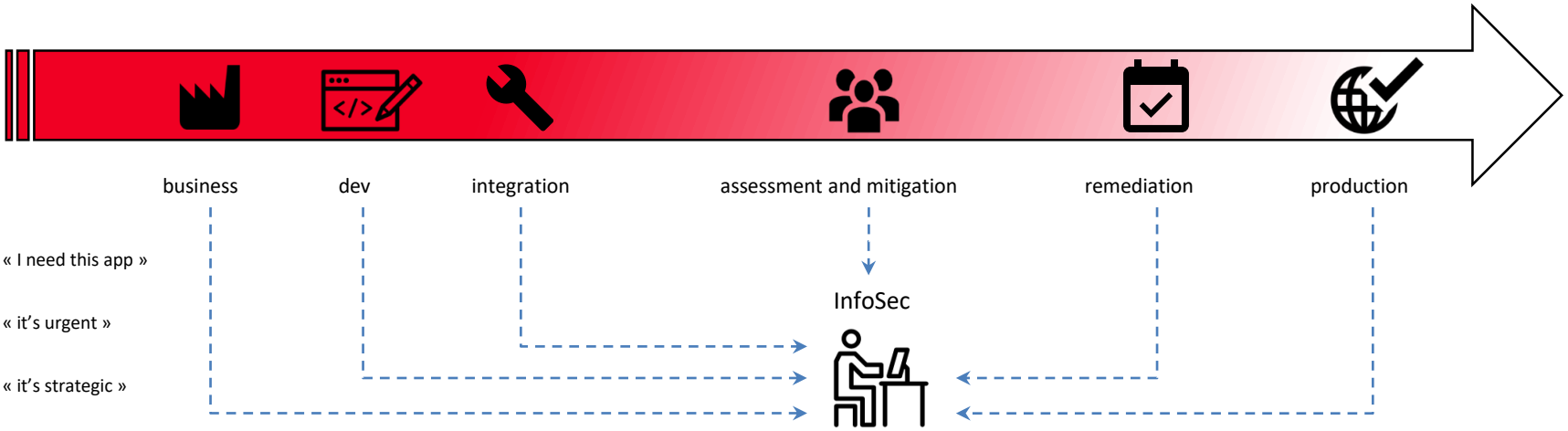
* Source: 2018 Verizon DBIR

Apps & APIs are Everywhere



Web Application Security is Complex

Increasing amount of technologies, frameworks, vulnerabilities, security tools and eventually teams involved, make appsec a complex topic in the Organization.



Qualys WAS

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

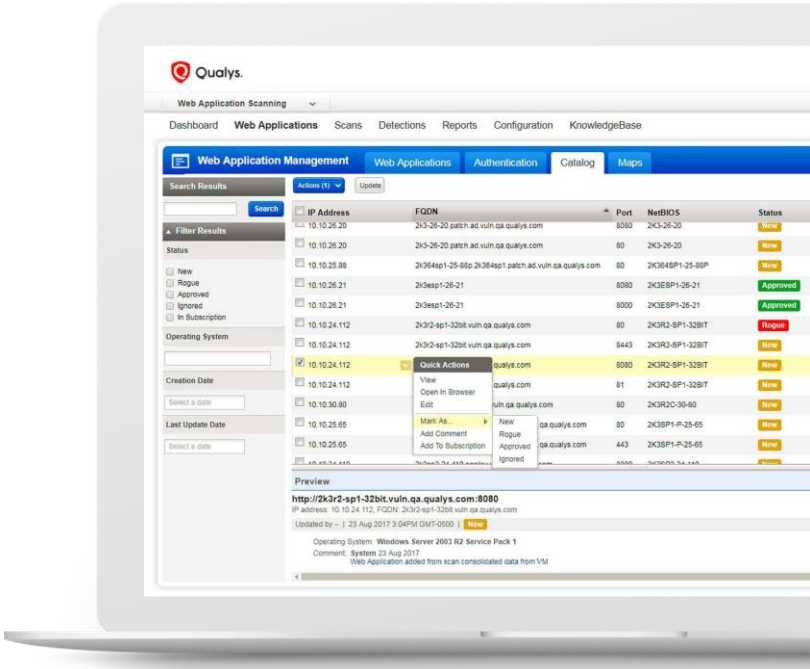
Identifies app-layer vulnerabilities

- OWASP Top 10
- CWEs
- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



Built for the Enterprise

Web App Discovery
Unlimited scans & users
RBAC
Tagging

Scheduled scans
Ad-hoc, targeted scans
Multi-site scans
Retest vulnerability
Scan for malware

Massive scalability
Detection history
Scheduled reports
Customizable reports
Swagger support

Robust API
CI/CD integration
Unique integration
w/Qualys WAF
Bi-directional integration
with Bugcrowd

Qualys Foundations

UNIFIED
Application Security Platform

Detect vulnerabilities AND deploy instant Virtual Patches with Web Application Scanning (WAS)

Use WAS trusted scans to challenge the WAF security policy with real detections

Empowered by the Qualys Suite (VM, AV, CA, and more)

POWERFUL
Dynamic Scanning

Scales to thousands of webapps

Highly accurate detections

Adapts to changing webapp technology landscape

INTELLIGENT
DAG based Inspection

Out-of-the-box Security Policies for WordPress, Joomla!, Drupal, OWA, and more

Developed by Qualys Security Researchers

FLEXIBLE
Deployment and Management

Compatible with major Virtualization Technologies and Cloud Vendors

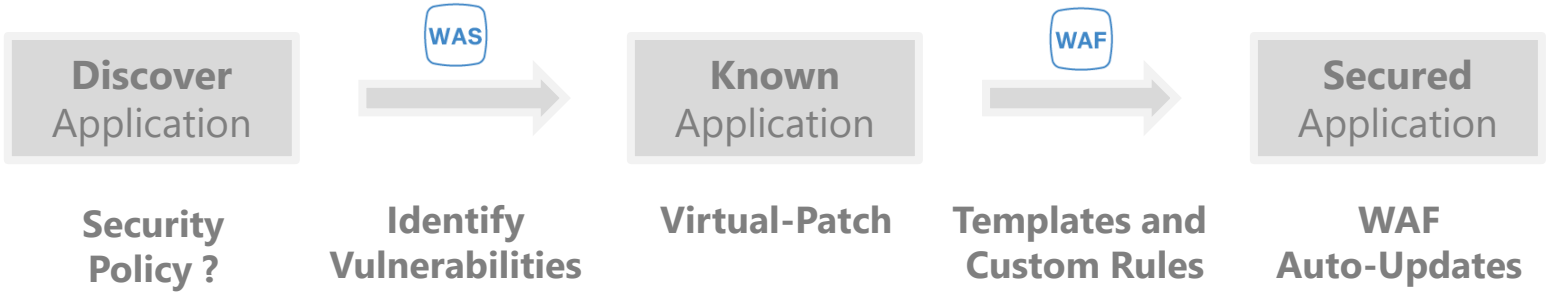
Powerful API

End-to-end management and actionable security data in Qualys Cloud Apps

Easy to integrate in DevOps and continuous testing workflows

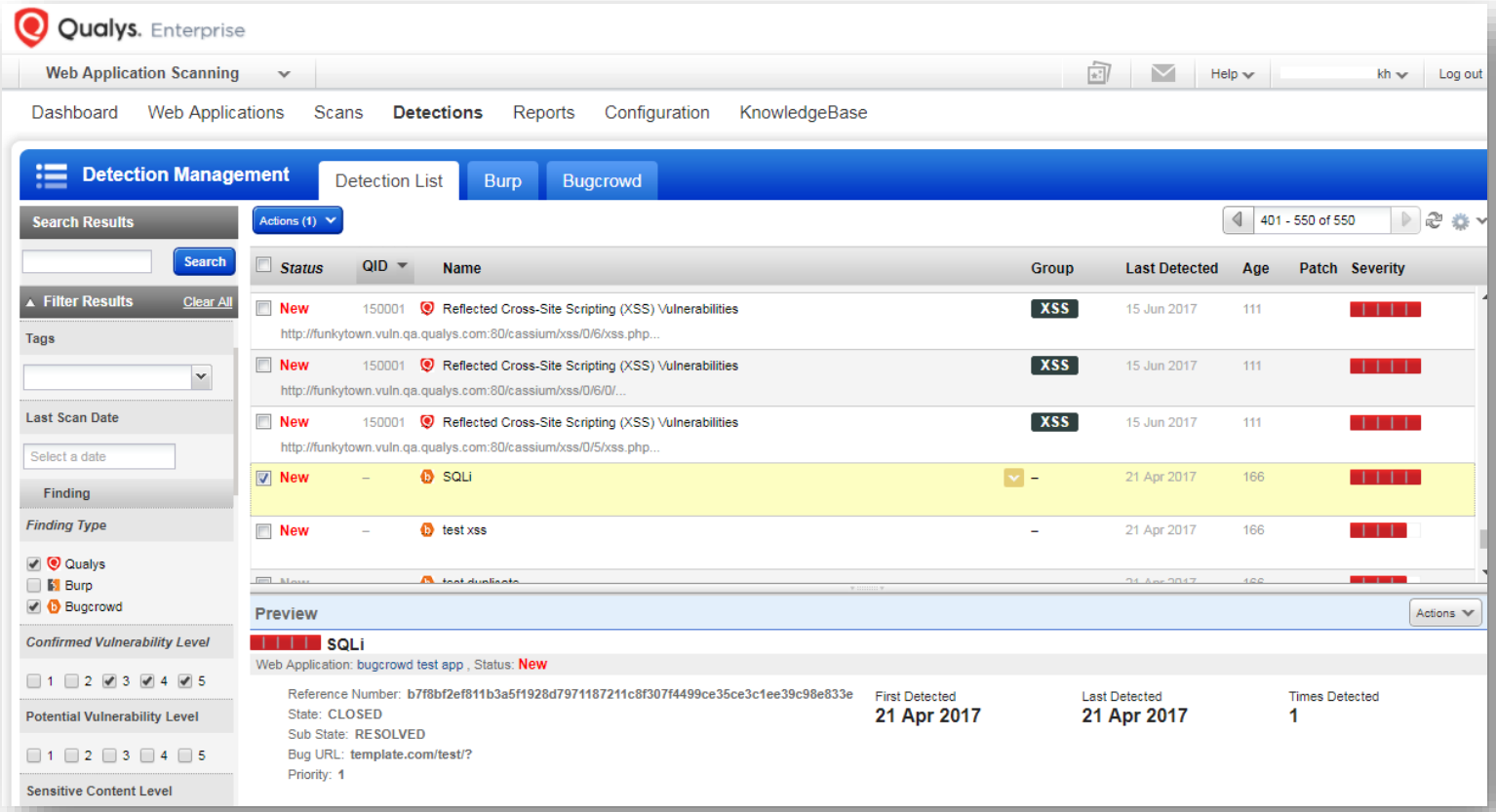
Qualys' approach

The scanner and the firewall can communicate through the Qualys Cloud Platform, making "one-click" virtual patches possible directly from within the scanning module



What's New in Qualys WAS

Integration Complete!

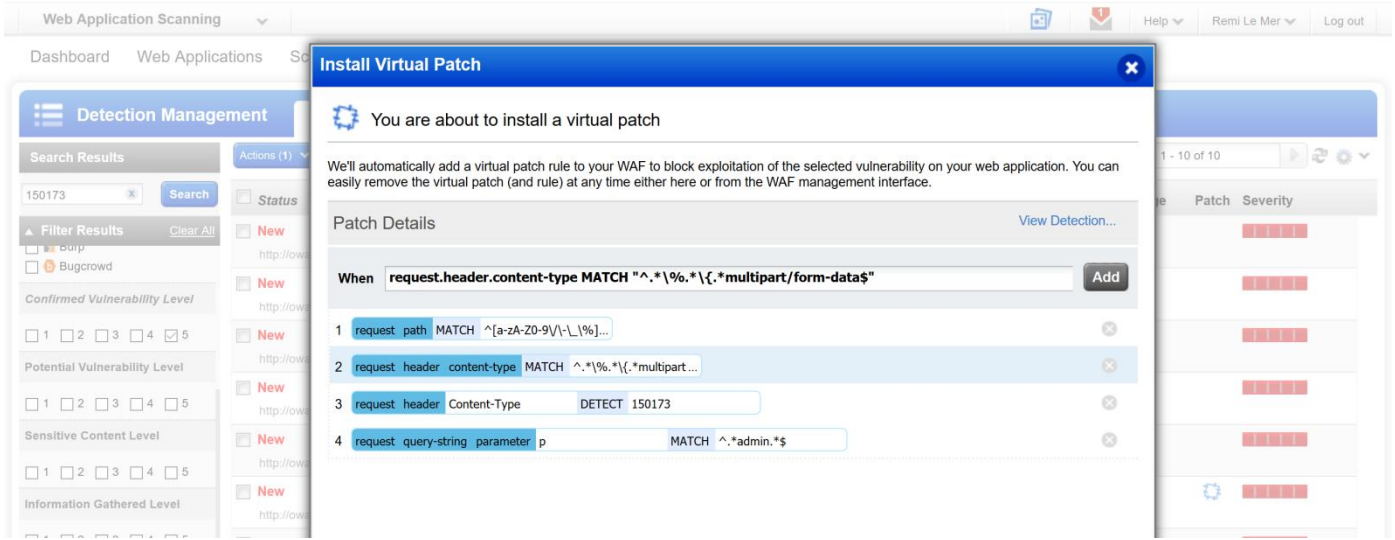

Qualys. Enterprise
Web Application Scanning
Help
kh
Log out
Dashboard
Web Applications
Scans
Detections
Reports
Configuration
KnowledgeBase
Detection Management
Detection List
Burp
Bugcrowd
Search Results
Search
Filter Results
Clear All
Tags
Last Scan Date
Select a date
Finding
Finding Type
Qualys
Burp
Bugcrowd
Confirmed Vulnerability Level
1 2 3 4 5
Potential Vulnerability Level
1 2 3 4 5
Sensitive Content Level
Actions (1)
401 - 550 of 550
Status
QID
Name
Group
Last Detected
Age
Patch
Severity
New 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities XSS 15 Jun 2017 111
http://funkytown.vuln.qa.qualys.com:80/cassium/xss/0/6/xss.php...
New 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities XSS 15 Jun 2017 111
http://funkytown.vuln.qa.qualys.com:80/cassium/xss/0/6/0/...
New 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities XSS 15 Jun 2017 111
http://funkytown.vuln.qa.qualys.com:80/cassium/xss/0/5/xss.php...
New – SQLi – 21 Apr 2017 166
New – test xss – 21 Apr 2017 166
Preview
Actions
SQLi
Web Application: bugcrowd test app , Status: New
Reference Number: b7f8bf2ef811b3a5f1928d7971187211c8f307f4499ce35ce3c1ee39c98e833e
State: CLOSED
Sub State: RESOLVED
Bug URL: template.com/test/?
Priority: 1
First Detected
21 Apr 2017
Last Detected
21 Apr 2017
Times Detected
1

What's New in Qualys WAF

Integration with WAS

Virtual Patch : one-click mitigation tool for CISO teams

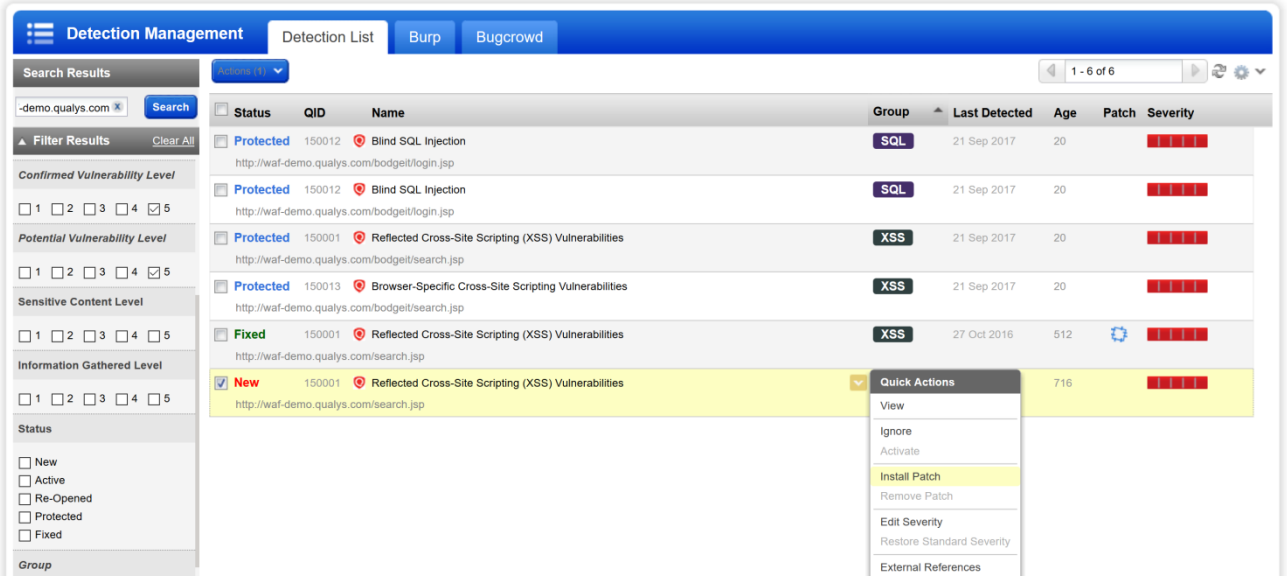
ran from within WAS console to address confirmed threats



Integration with WAS

ScanTrust : challenge your WAF protection

assess both the application and the policy that protects it

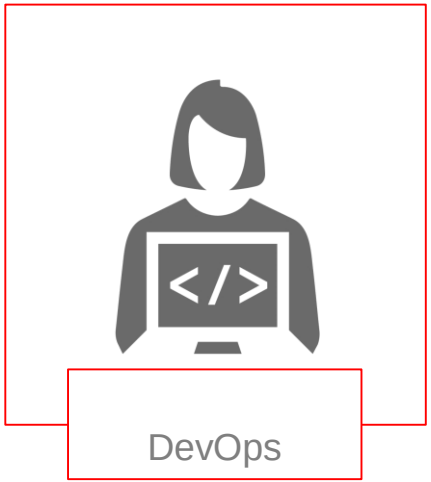


Container security

DevSecOps

Qualys Container Security Overview

Securing containers – New addition (DevOps)



SHIFT LEFT

What does DevOps want?

Can I identify the vulnerabilities in CI/CD process?

REST APIs for the integration into my build tool?

Info sec – Vulnerability Mgmt. Team Lead

Qualys Container Security

Total visibility and continuous security for containers

Discovery & Inventory

Vulnerability Management

Runtime Tracking & Events

REST API Integrations

Vulnerability Management:

Secure the complete container pipeline

PRE-DEPLOYMENT PHASE

POST-DEPLOYMENT PHASE

BUILD

Block vulnerable images from entering repositories. Get actionable data to developers to fix in the build pipe line.
Use Qualys Vulnerability Analysis Jenkins plug-in or REST APIs

REGISTRY*

Secure images pushed to Registry. Scan on-demand or automated to analyze any images in Registries

RUNTIME

Scan running container for vulnerabilities and anomalous behaviors, identify the rogue containers

HOST

Identify vulnerabilities and compliance posture of the docker hosts using Qualys Cloud Agents or scans via virtual scanner appliance

* Support coming Aug 2018

Qualys Container Native Sensor

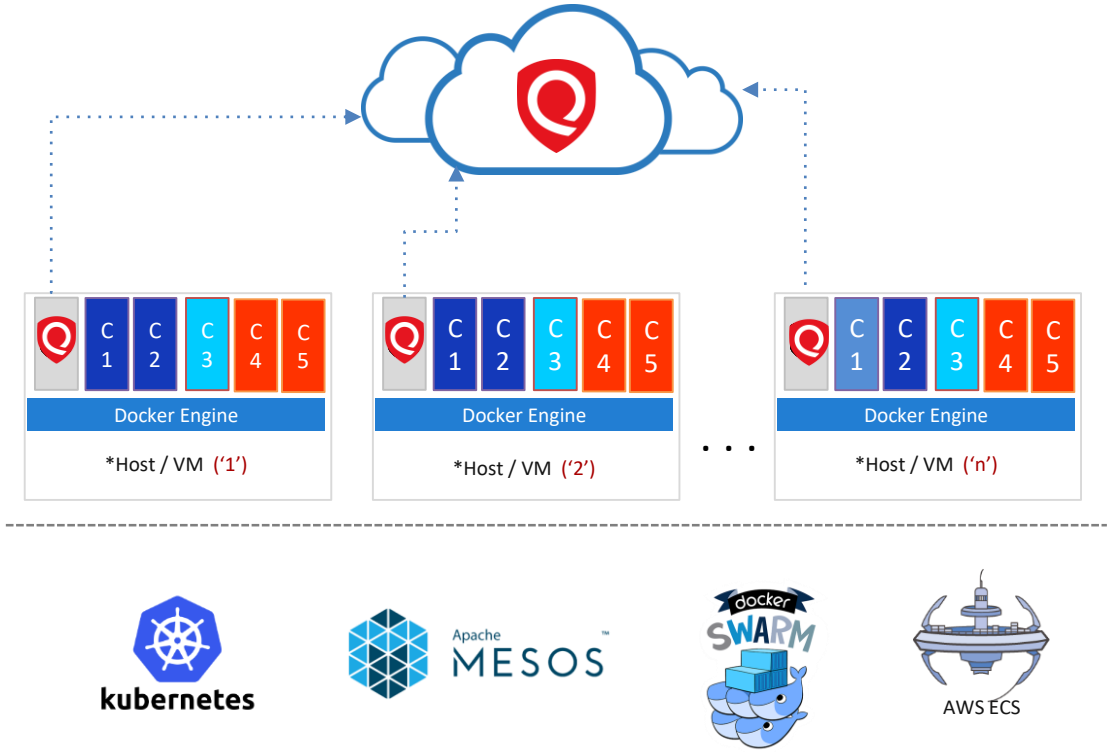
Download as docker Image, deploy as a container on every Docker hosts

Deployable into Kubernetes, AWS ECS, Docker Swarm, Mesos,..

Runs as non- privileged container

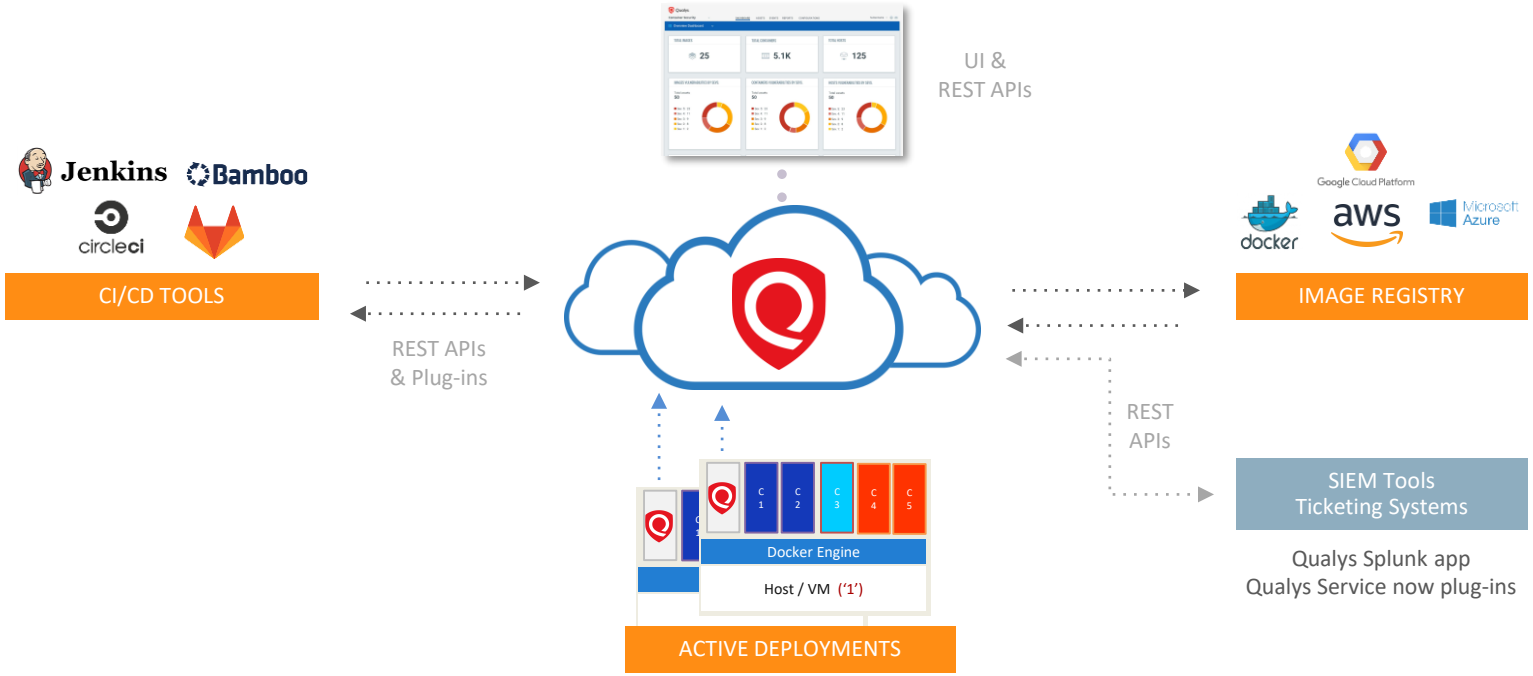
Qualys Container communicates to Qualys on port 443 via Egress only

Supports Proxy configuration



*Require Cloud Agent or remote Scanner for securing the Docker hosts

Qualys Container Security
Functional Overview



Qualys Container Security

Key Uses

Visibility into your container projects

Identify Hosts with Containers. Inventory of images, containers. Search images with vulnerabilities, labels, tags, packages,.. Build custom widgets.

Secure the CI/CD pipeline

Integrate images, vulnerability scans into the build. FAIL builds, not allowing unsecure images to enter the stream

Identify threats and impact across environments

Find out if older image versions are still active. Know all the containers with a specific exposed port or from a vulnerable image

Detect Container Runtime Drifting

Find containers whose runtime got changed of software packages or vulnerabilities.

Thank You

rbenito@qualys.com