QSC 18 | QUALYS SECURITY CONFERENCE 2018

Web Applications & APIs

The Soft Belly of the Cloud

Dave Ferguson
Director of Product Management, WAS

Remi Le Mer
Director of Product Management, WAF

Agenda

- Web Apps & APIs in the Cloud
- Qualys Web Application Scanning
  - Review
  - What's New
  - Roadmap
- Qualys Web Application Firewall
  - Review
  - What's New
  - Roadmap
- Q&A

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

Apps in Public Clouds

Public-Facing Web Apps

REST APIs

Internal Web Apps

New Apps under Development

Web Application Scanning

Review

Qualys WAS

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

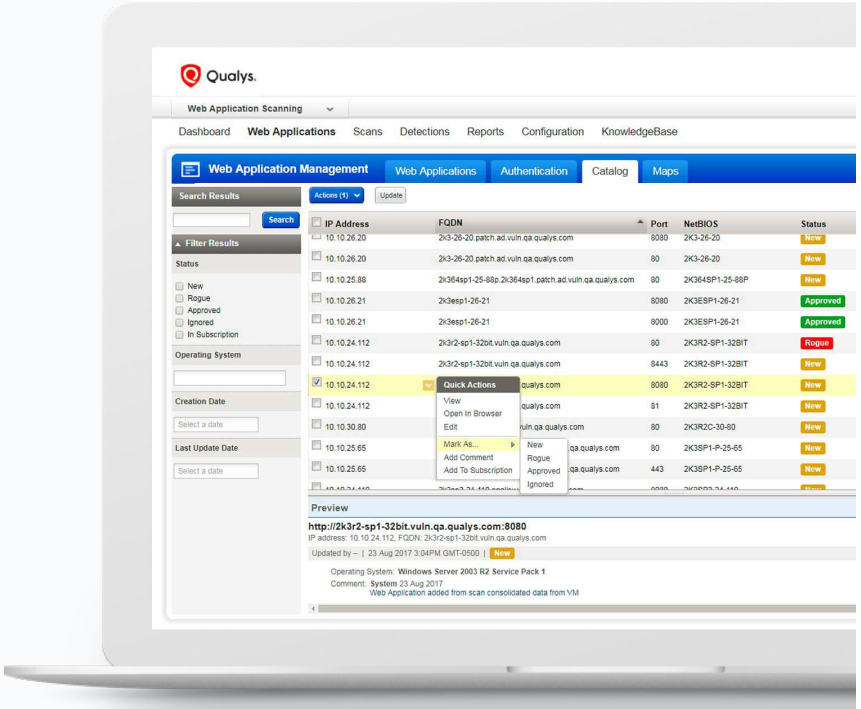
Identifies app-layer vulnerabilities

- OWASP Top 10
- CWEs
- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



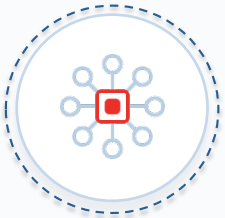
Qualys.

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

What's New in Qualys WAS

Scanning REST APIs

https://
swagger.io

https://
www.openapis.org

Swagger is specification that describes a set of REST APIs

Swagger file typically available from dev team

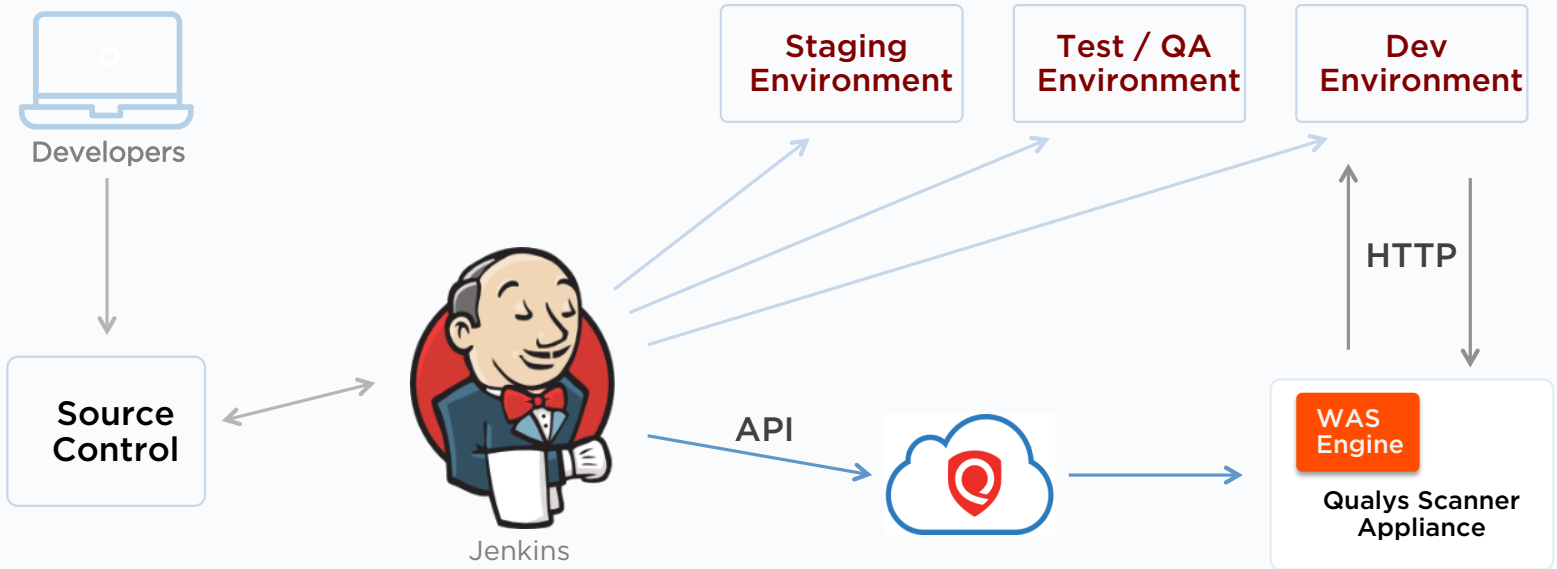
Set Swagger file as target URL in Qualys WAS

API endpoints are automatically tested for vulnerabilities

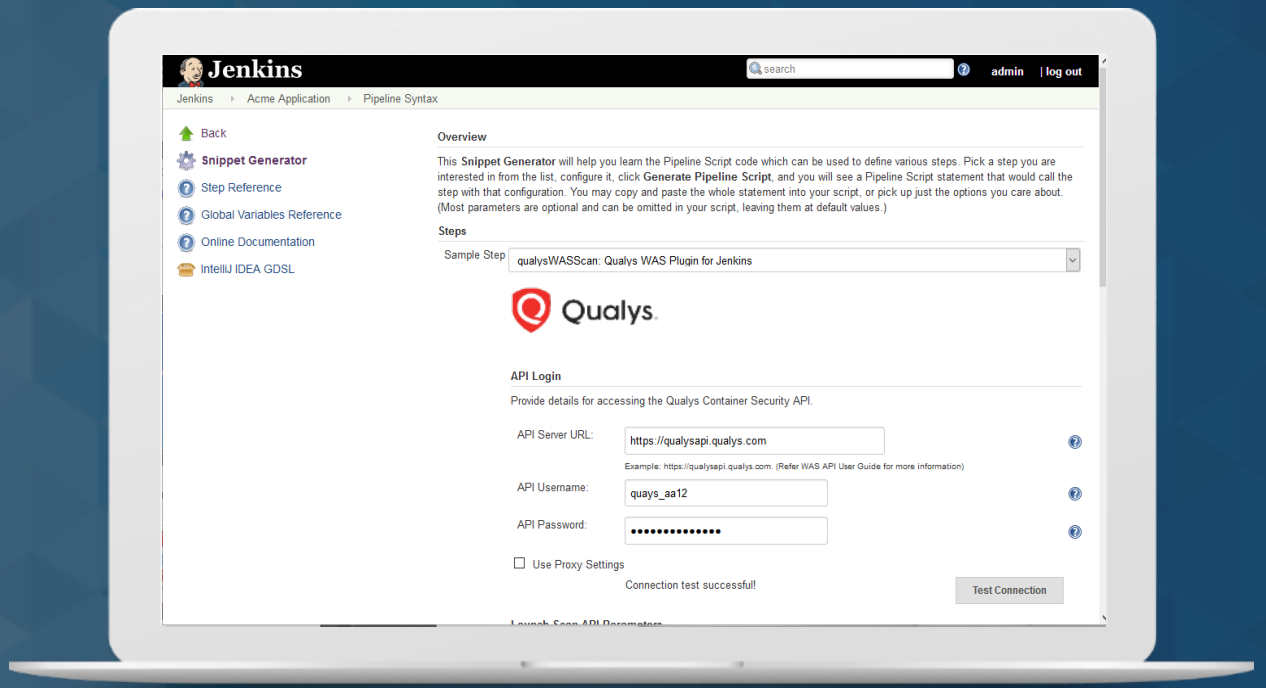
Swagger v2 JSON format currently supported

Qualys.

Automate Scans in CI/CD with Qualys WAS



Jenkins Plugin for WAS



Manual Testing Complements WAS

Dynamic application testing is one piece of the AppSec puzzle

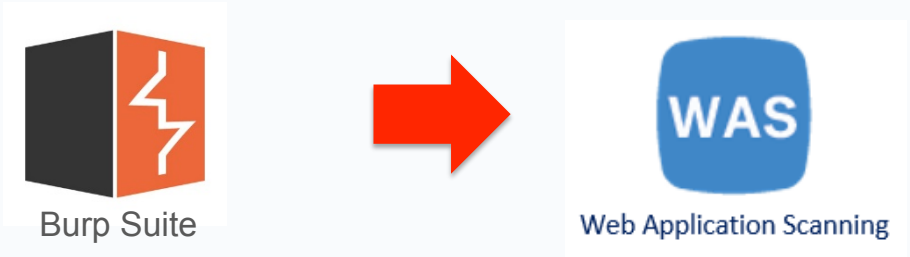
Manual penetration testing important for your business-critical apps

Qualys WAS offers:

- Bugcrowd integration
- Burp Suite integration
- Partnerships with consulting shops

Bi-directional Integration with Bugcrowd

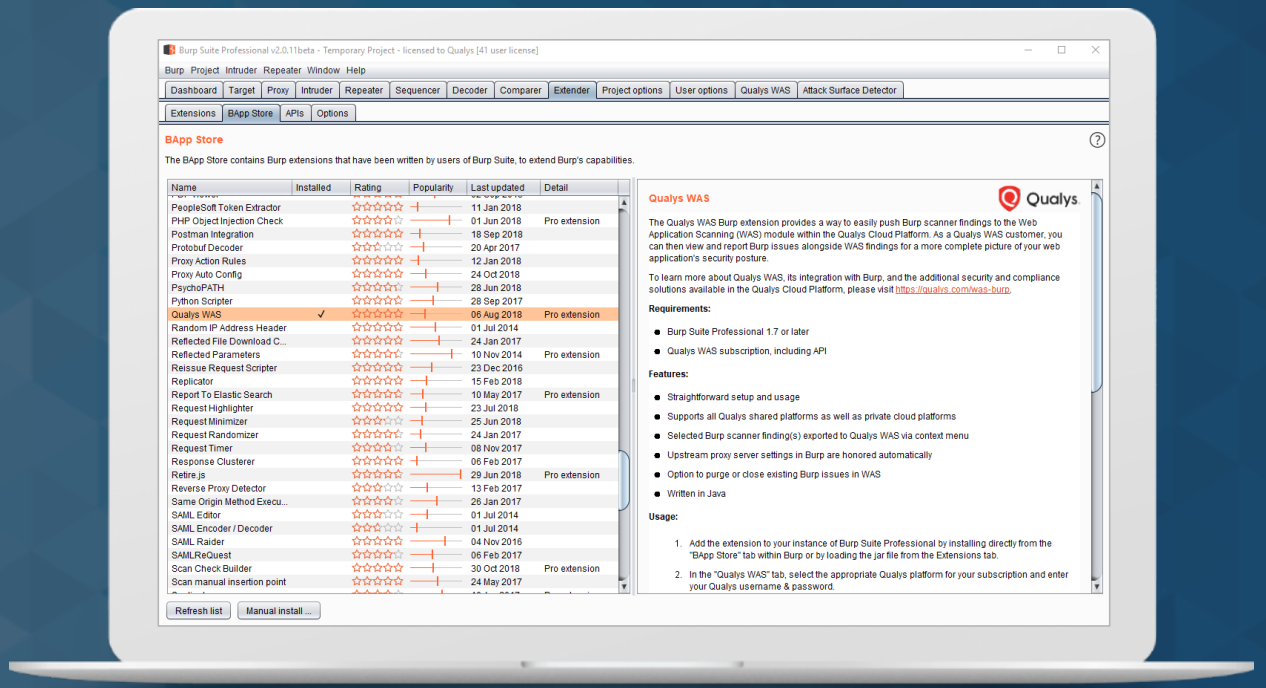
Qualys WAS Burp Extension



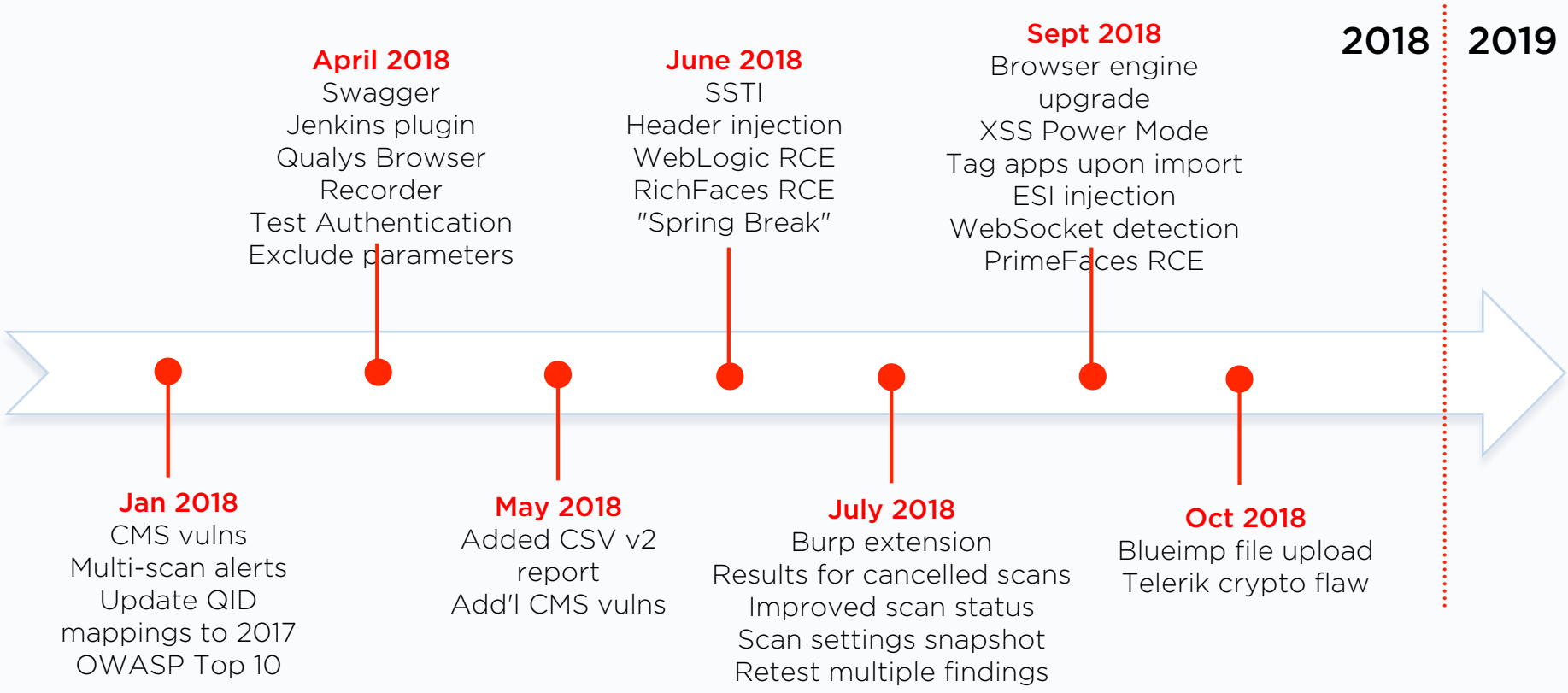
A quick, intuitive way to send Burp-discovered issues into WAS
Provides centralized viewing/reporting of WAS detections + Burp issues

Available in Burp's BApp Store

Qualys WAS Burp extension



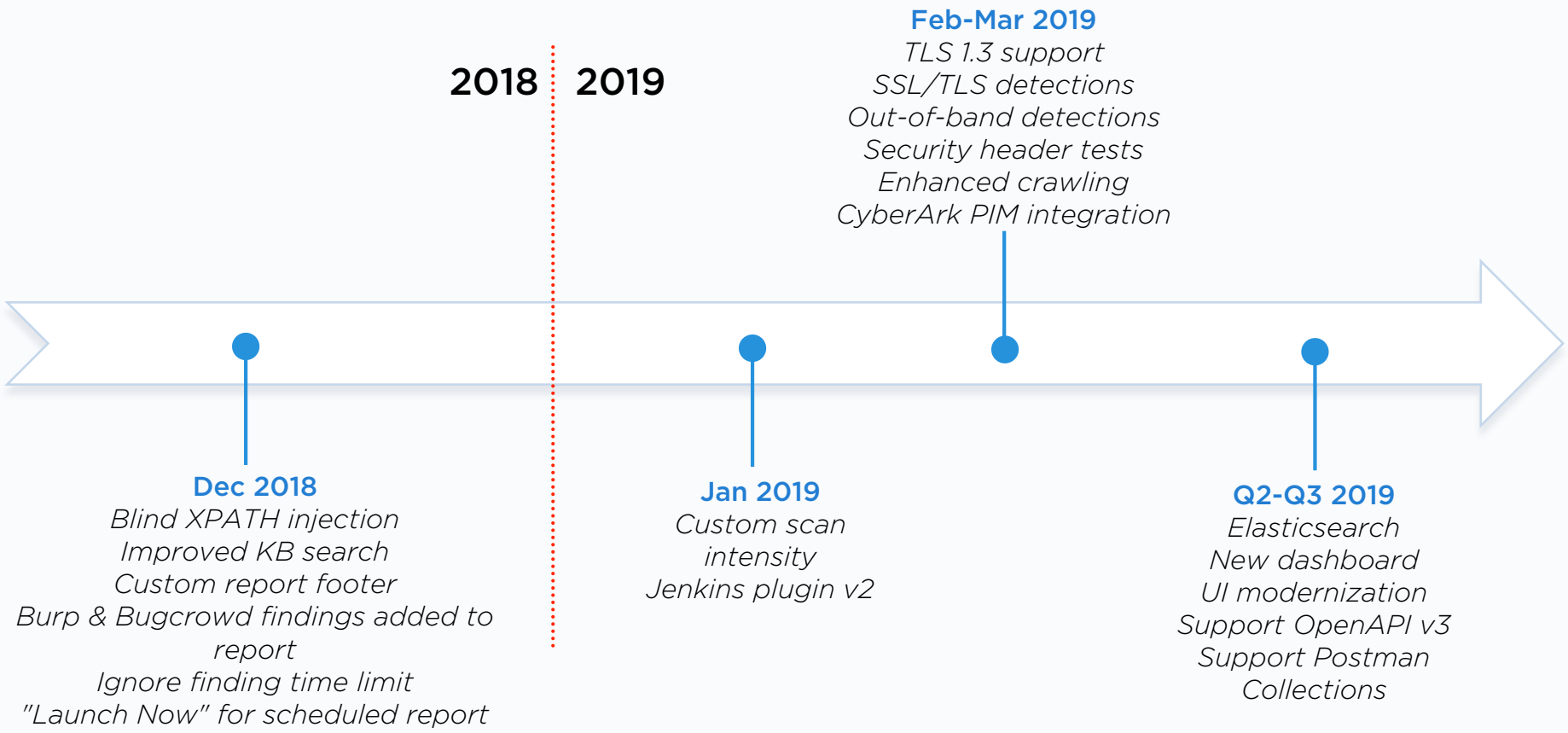
WAS Enhancements, YTD



Qualys.

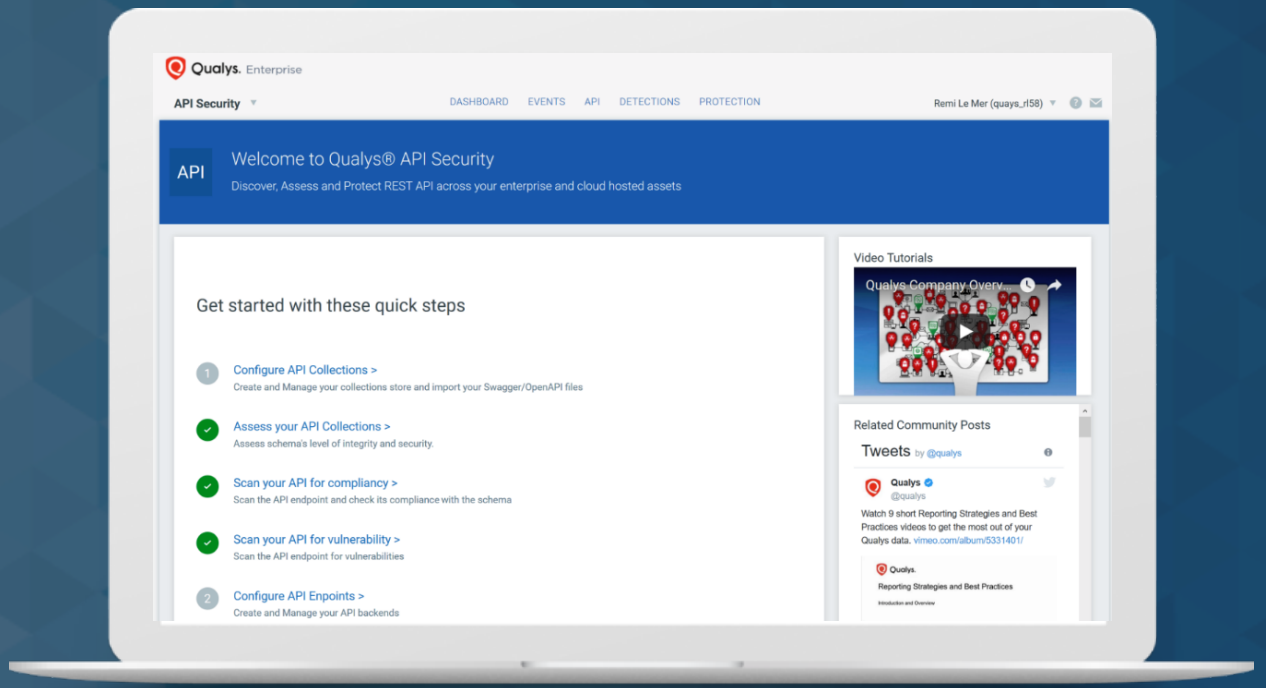
Qualys WAS Roadmap

WAS Roadmap



Qualys.

And Coming in 2019

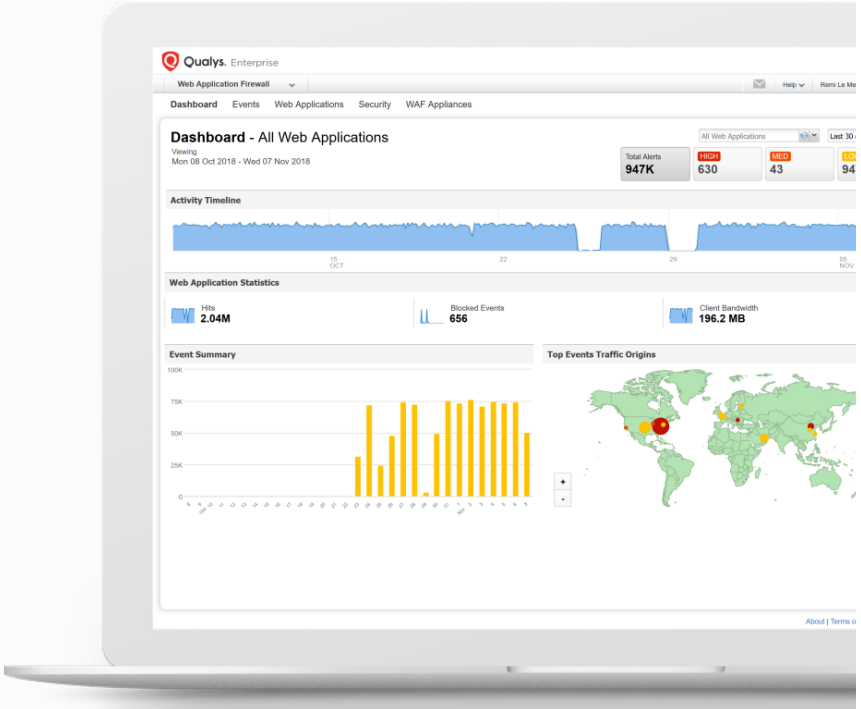


Web Application Firewall

Review

Qualys WAF

Integration with WAS
Architecture improvements
Integration with Docker
Security Improvements
Roadmap – standalone
Roadmap – Integrated Suite

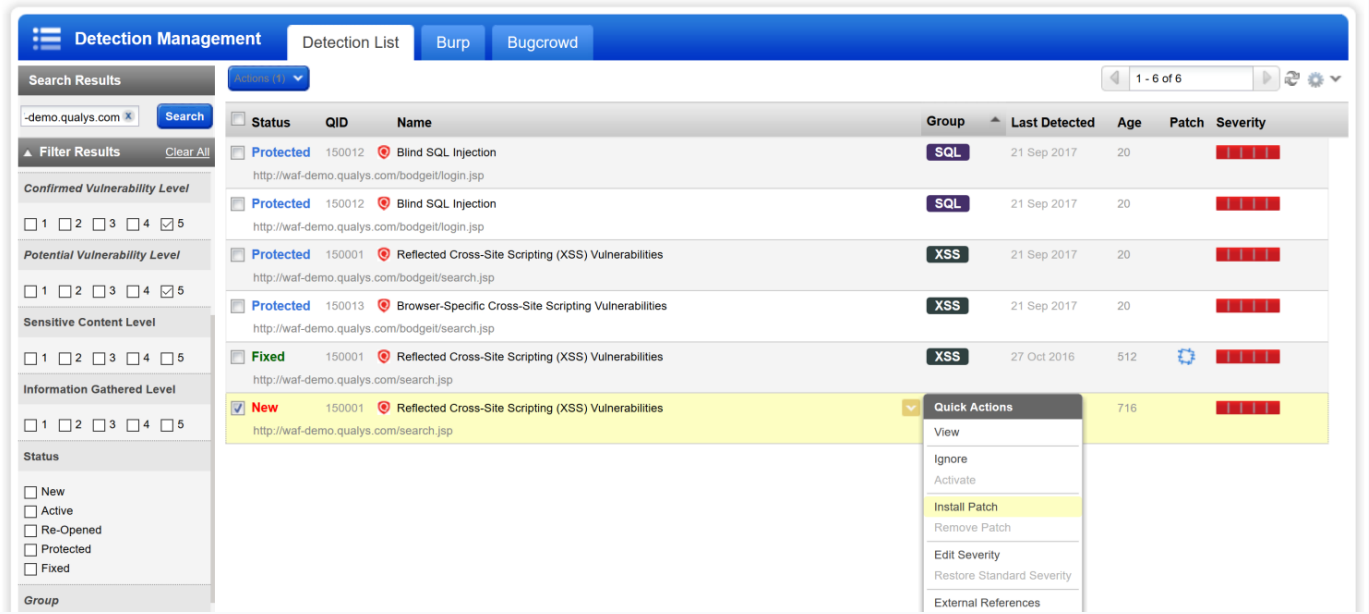


Qualys.

WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection

Assess both the application and the policy that protects it

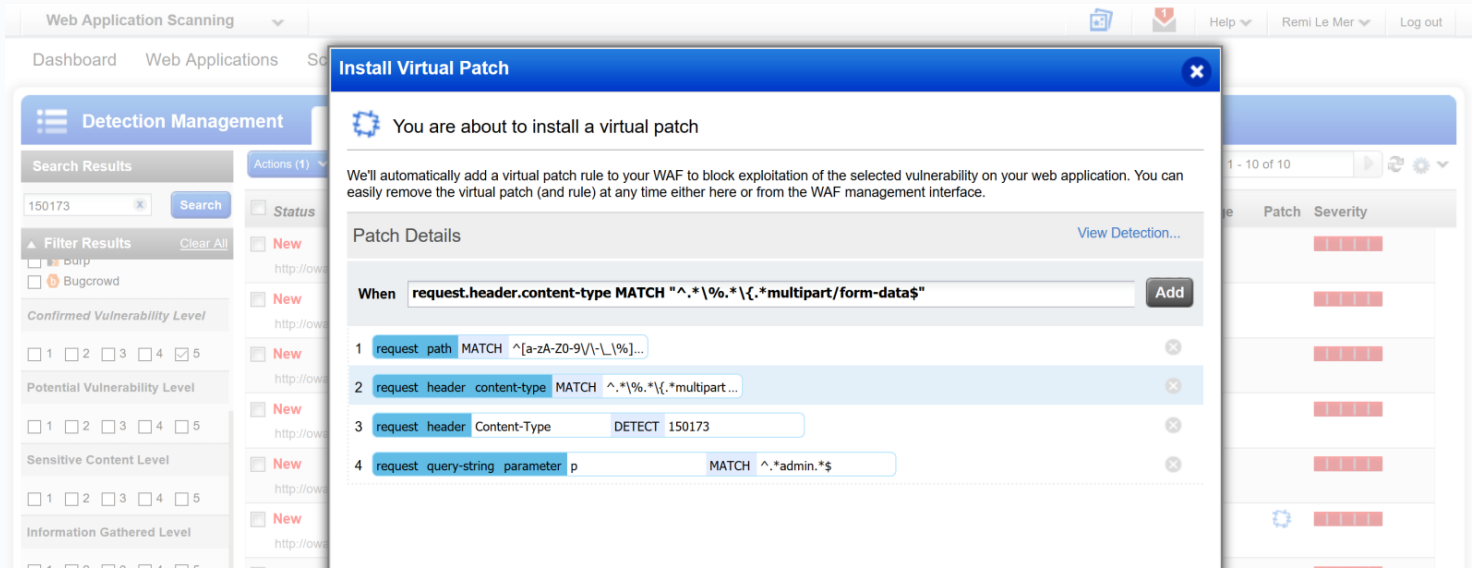


Qualys.

WAS / WAF Integration: Virtual Patch

Virtual Patch : One-click mitigation tool for CISO teams

Run from within WAS to address confirmed threats



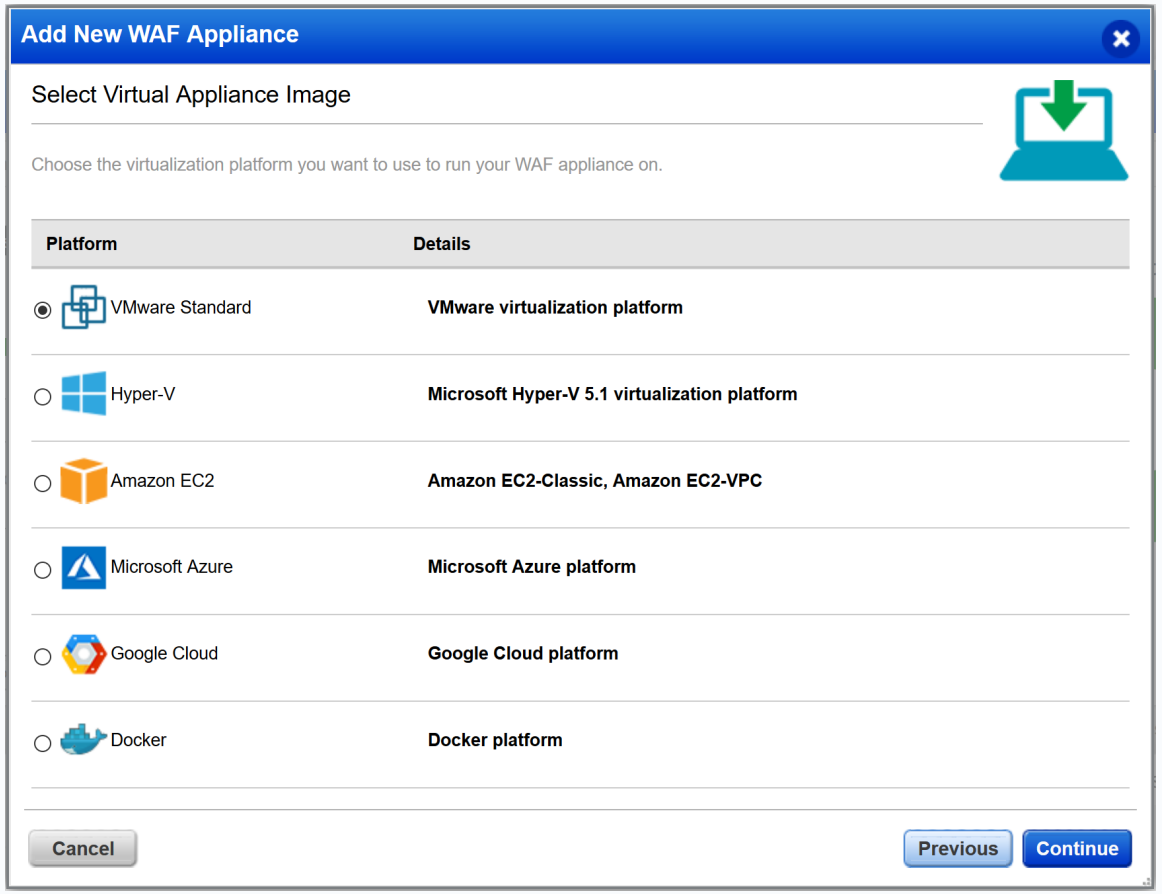
Qualys.

What's New in Qualys WAF

Supported Platforms

Shared and Private

Qualys Cloud Platforms



WAF Architecture Improvements

Easy and usable Architecture

- Virtual Reverse-Proxy
- Cluster-able within hybrid topologies
- Load-Balancing capabilities
- SSL/TLS cipher suite categories

WAF Architecture Improvements

Virtual Appliance & Container (v1.5.3)

XML/JSON content inspection

Docker Host integration for backend automation

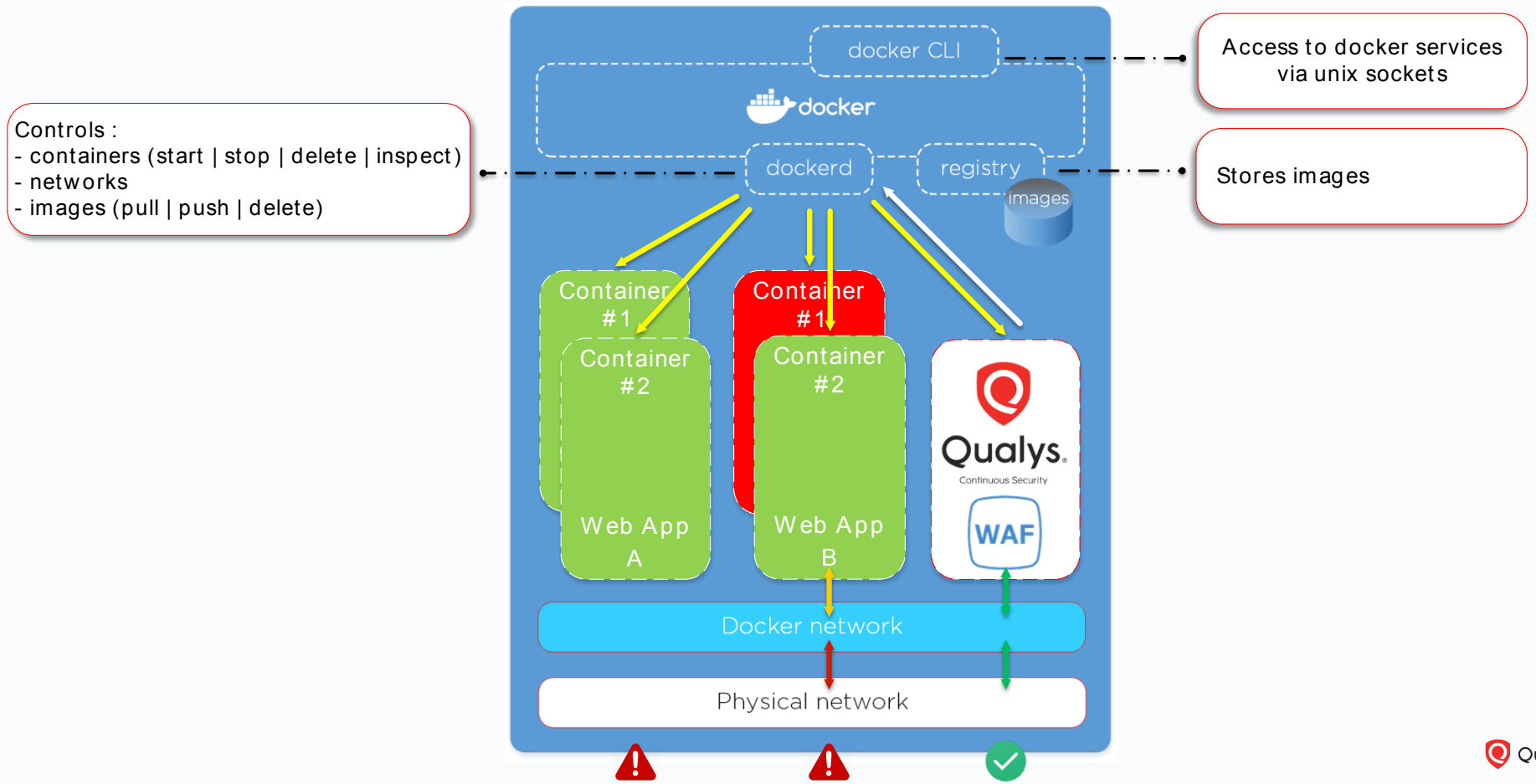
Better performance

Scheduled upgrades

Orchestration via Qualys API

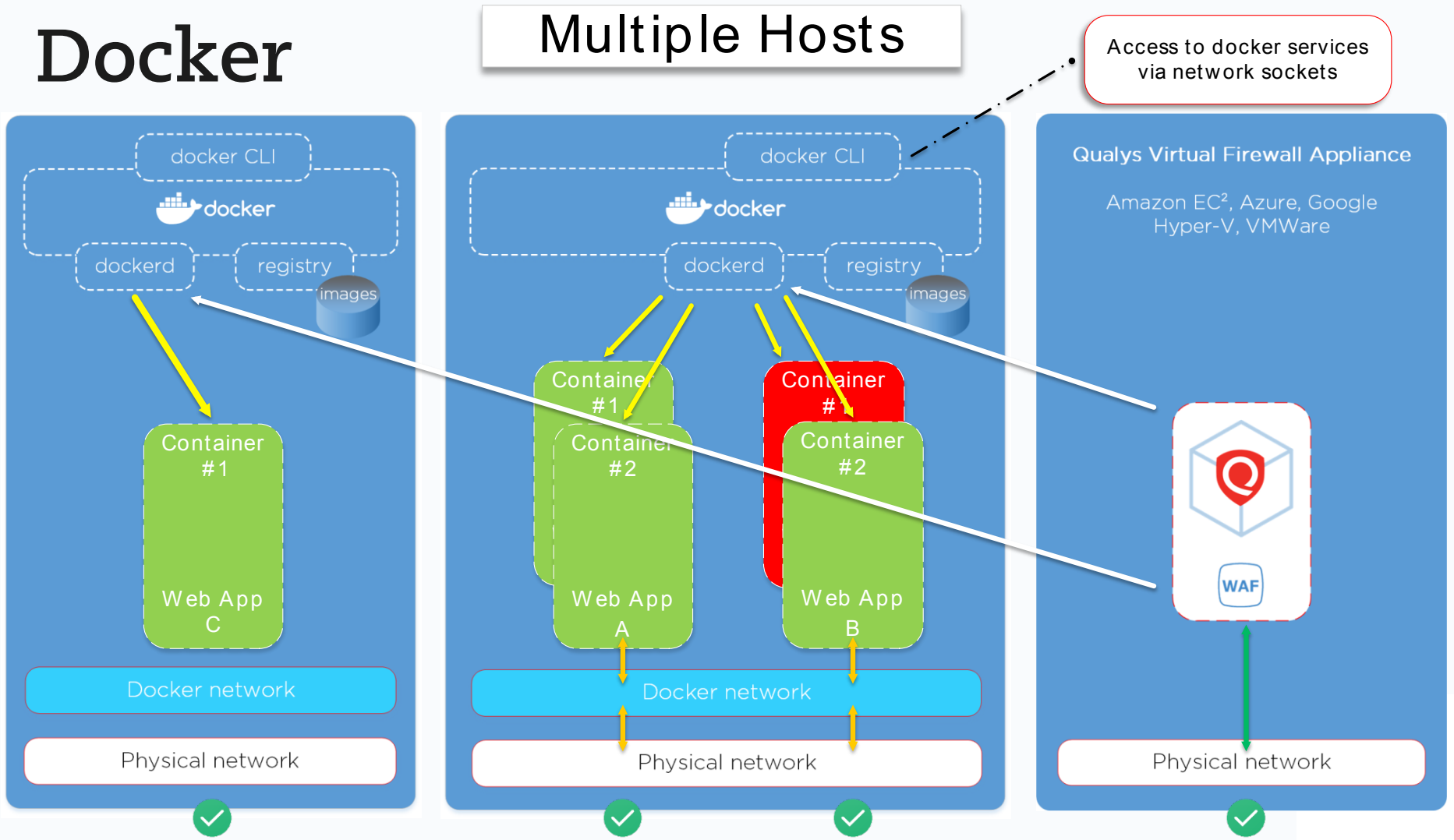
Docker

Single Host



Qualys

Docker


Multiple Hosts
Access to docker services via network sockets
docker CLI
docker
dockerd
registry
images
Container #1
Web App C
Docker network
Physical network
docker CLI
docker
dockerd
registry
images
Container #1
Container #2
Web App A
Container #1
Container #2
Web App B
Docker network
Physical network
Qualys Virtual Firewall Appliance
Amazon EC², Azure, Google Hyper-V, VMWare
WAF
Physical network

Security Improvements

Custom Rules: write and manage your own filters

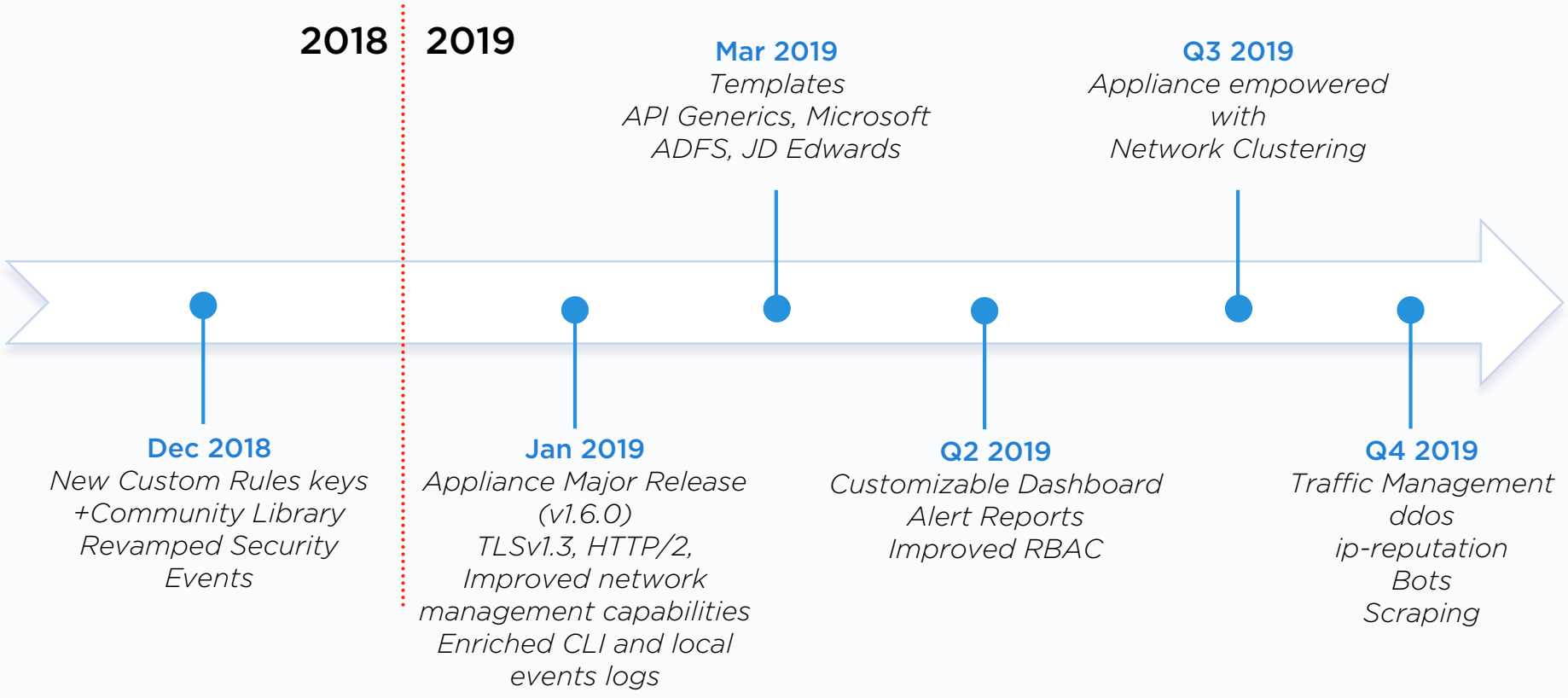
- XML/JSON inspection
- Virtual Patches and Event Exceptions
- Latency control
- Rewriting capabilities (headers)

Qualys Rulesets and Templates

- DAG based inspection, programmable logic
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x
- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x
- Qualys Generics for unknown apps

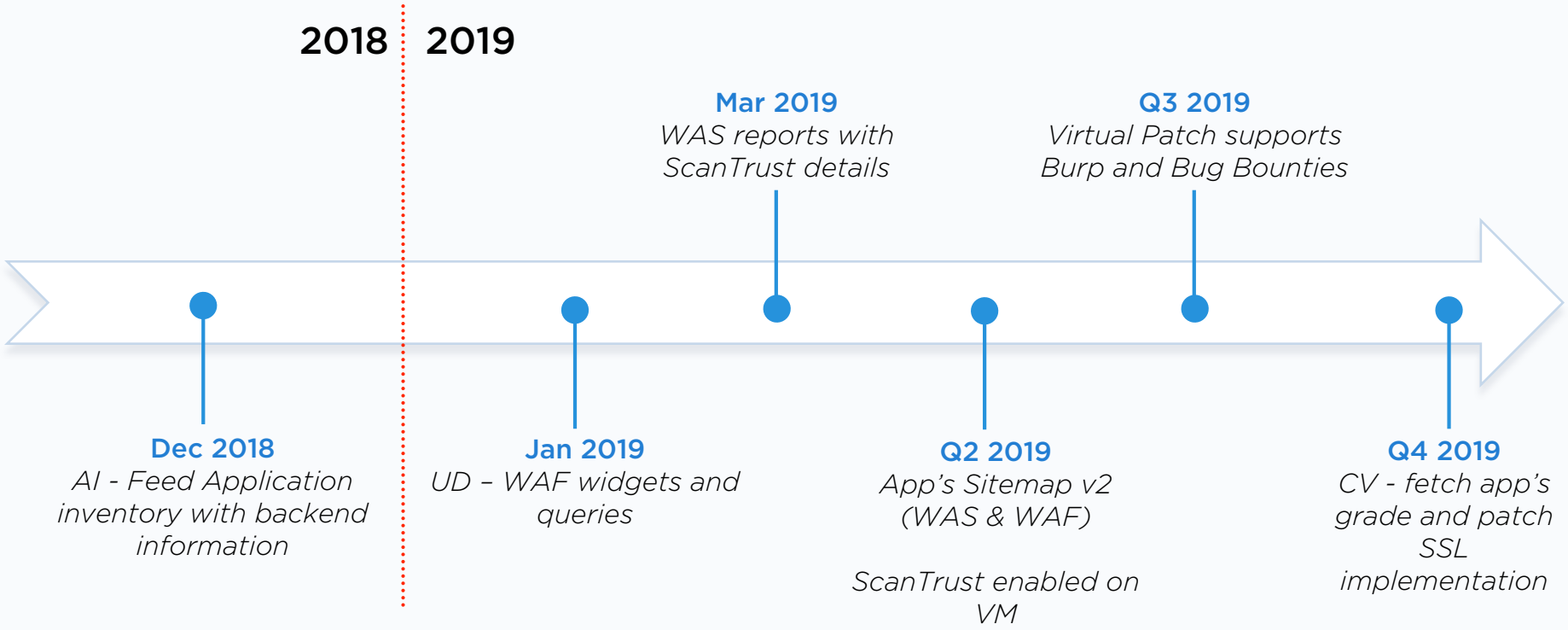
Qualys WAF Roadmap

WAF Roadmap - Standalone



Qualys.

WAF Roadmap – Integrated Suite



Thank You

Dave Ferguson - dferguson@qualys.com
Remi Le Mer - rlemer@qualys.com