



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

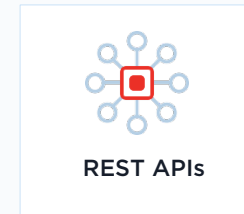
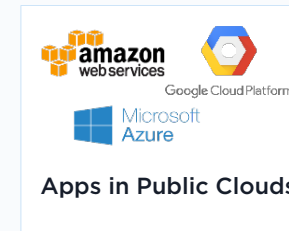
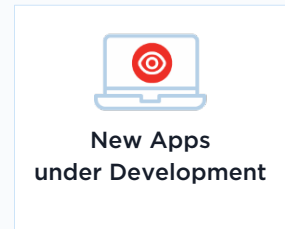
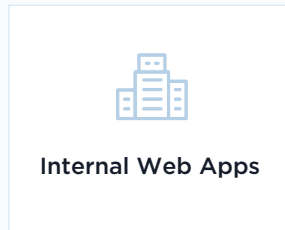
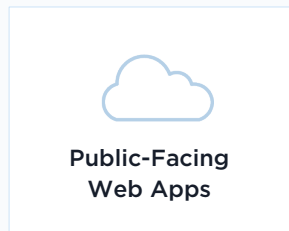
Web Applications are Being Targeted

- 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



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

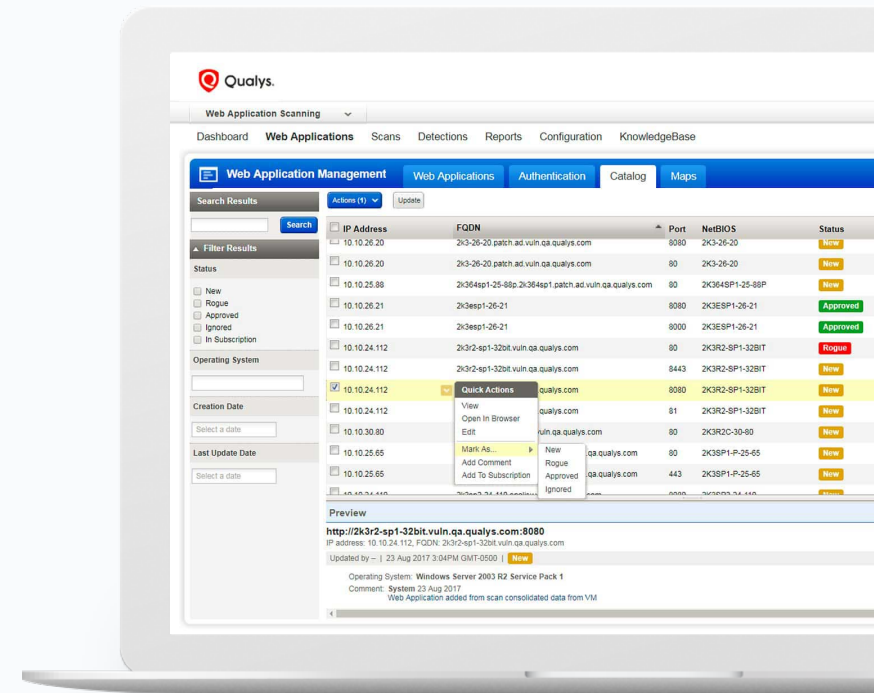
- CWEs

- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



Built for the Enterprise



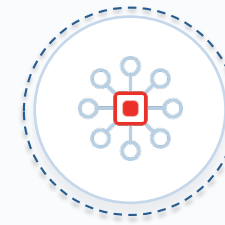
Web App Discovery
Unlimited scans &
users
RBAC
Tagging



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://swagger.io)



[https://
www.openapis.org](https://www.openapis.org)

Swagger is specification that describes a set of REST APIs

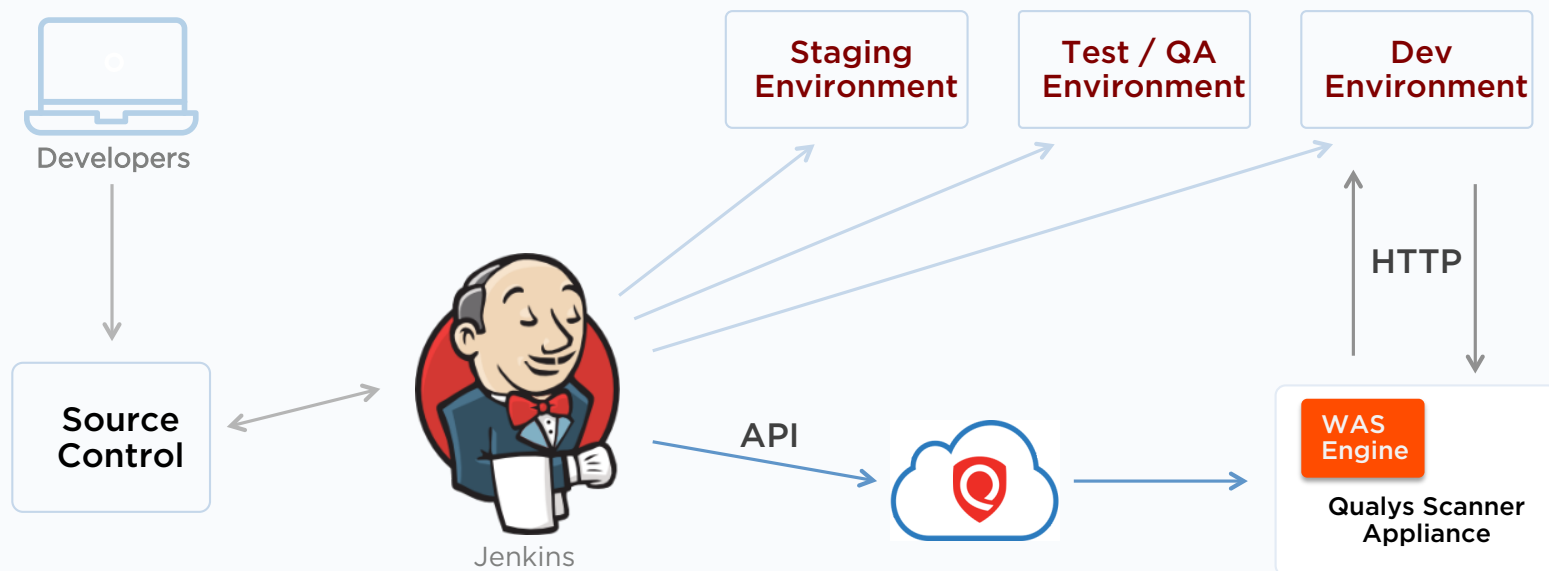
Swagger file typically available from dev team

Set Swagger file as target URL in Qualys WAS

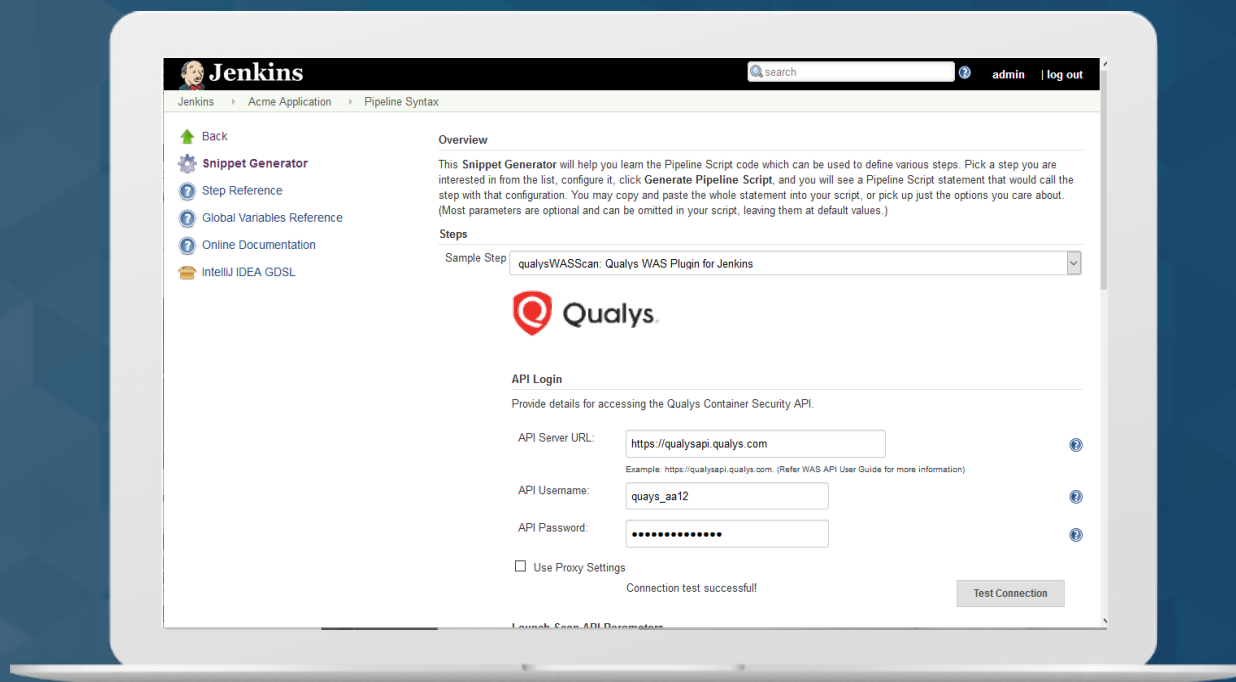
API endpoints are automatically tested for vulnerabilities

Swagger v2 JSON format currently supported

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

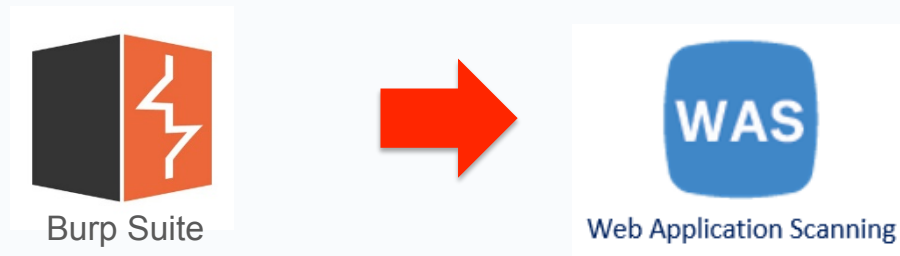
- Burp Suite integration

- 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

The screenshot shows the Burp Suite Professional interface with the BApp Store open. The 'Qualys WAS' extension is highlighted in the list. The details panel on the right provides information about the extension, including its description, requirements, features, and usage instructions.

Name	Installed	Rating	Popularity	Last updated	Detail
PeopleSoft Token Extractor		☆☆☆☆	→	11 Jan 2018	
PHP Object Injection Check		☆☆☆☆	→	01 Jun 2018	Pro extension
Postman Integration		☆☆☆☆	→	18 Sep 2016	
Protobuf Decoder		☆☆☆☆	→	20 Apr 2017	
Proxy Action Rules		☆☆☆☆	→	12 Jan 2018	
Proxy Auto Config		☆☆☆☆	→	24 Oct 2018	
PsychoPATH		☆☆☆☆	→	28 Jun 2018	
Python Scripter		☆☆☆☆	→	28 Sep 2017	
Qualys WAS	✓	☆☆☆☆	→	06 Aug 2018	Pro extension
Random IP Address Header		☆☆☆☆	→	01 Jul 2014	
Reflected File Download C...		☆☆☆☆	→	24 Jan 2017	
Reflected Parameters		☆☆☆☆	→	10 Nov 2014	Pro extension
Reissue Request Scripter		☆☆☆☆	→	23 Dec 2016	
Replicator		☆☆☆☆	→	15 Feb 2018	
Report To Elastic Search		☆☆☆☆	→	10 May 2017	Pro extension
Request Highlighter		☆☆☆☆	→	23 Jul 2016	
Request Minimizer		☆☆☆☆	→	25 Jun 2018	
Request Randomizer		☆☆☆☆	→	24 Jan 2017	
Request Timer		☆☆☆☆	→	08 Nov 2017	
Response Clusterer		☆☆☆☆	→	06 Feb 2017	
Retire.js		☆☆☆☆	→	29 Jun 2018	Pro extension
Reverse Proxy Detector		☆☆☆☆	→	13 Feb 2017	
Same Origin Method Execu...		☆☆☆☆	→	26 Jan 2017	
SAML Editor		☆☆☆☆	→	01 Jul 2014	
SAML Encoder / Decoder		☆☆☆☆	→	01 Jul 2014	
SAML Raider		☆☆☆☆	→	04 Nov 2016	
SAMLReQuest		☆☆☆☆	→	06 Feb 2017	
Scan Check Builder		☆☆☆☆	→	30 Oct 2016	Pro extension
Scan manual insertion point		☆☆☆☆	→	24 May 2017	

Qualys WAS

The Qualys WAS Burp extension provides a way to easily push Burp scanner findings to the Web Application Scanning (WAS) module within the Qualys Cloud Platform. As a Qualys WAS customer, you can then view and report Burp issues alongside WAS findings for a more complete picture of your web application's security posture.

To learn more about Qualys WAS, its integration with Burp, and the additional security and compliance solutions available in the Qualys Cloud Platform, please visit <https://qualys.com/was-burp>.

Requirements:

- Burp Suite Professional 1.7 or later
- Qualys WAS subscription, including API

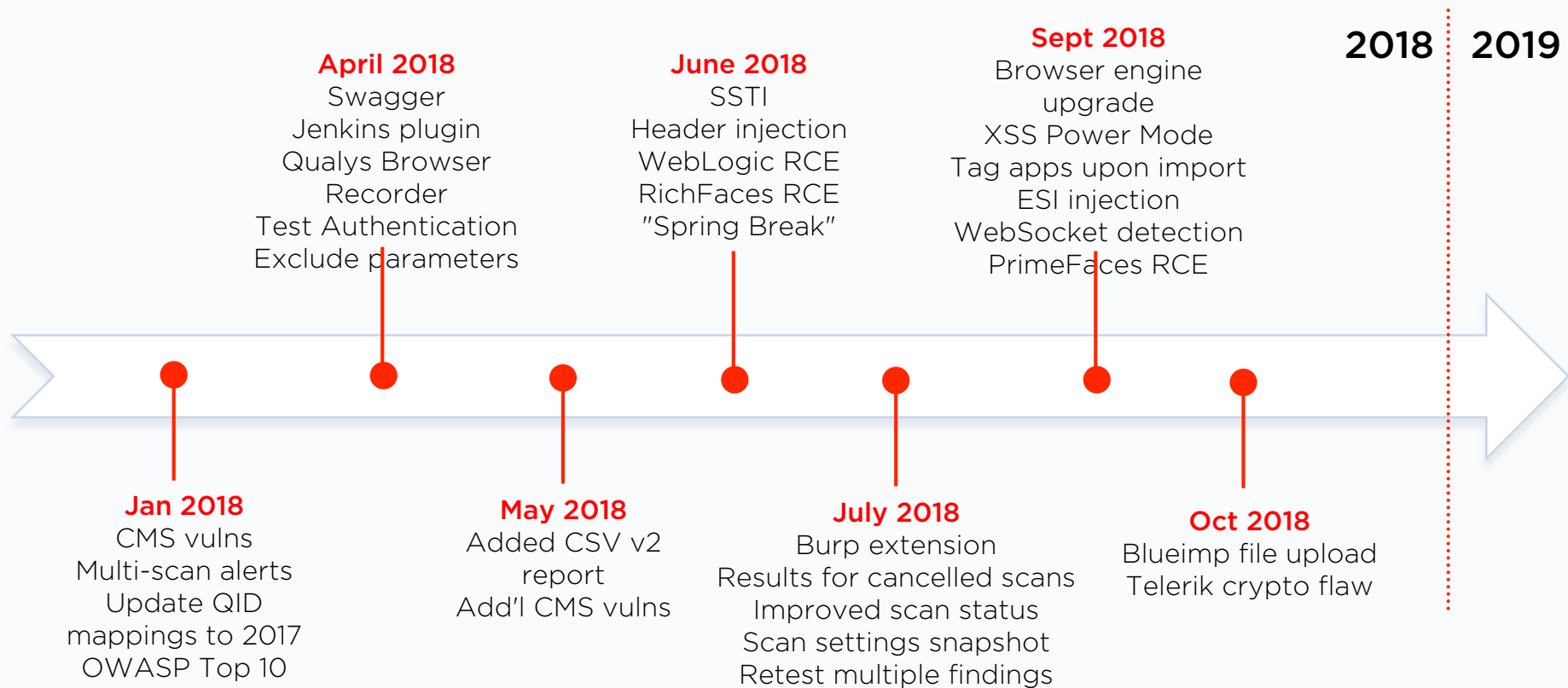
Features:

- Straightforward setup and usage
- Supports all Qualys shared platforms as well as private cloud platforms
- Selected Burp scanner finding(s) exported to Qualys WAS via context menu
- Upstream proxy server settings in Burp are honored automatically
- Option to purge or close existing Burp issues in WAS
- Written in Java

Usage:

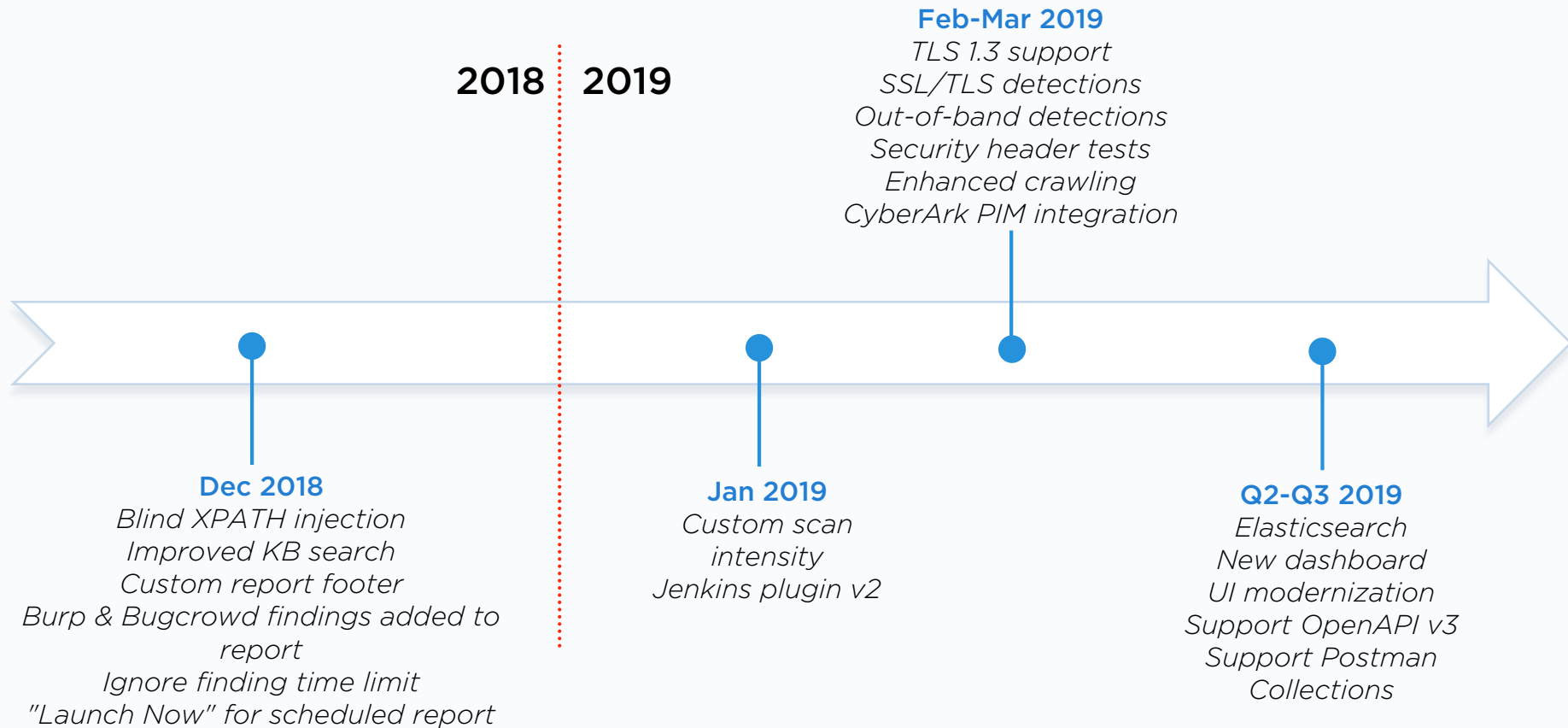
1. Add the extension to your instance of Burp Suite Professional by installing directly from the "BApp Store" tab within Burp or by loading the jar file from the Extensions tab.
2. In the "Qualys WAS" tab, select the appropriate Qualys platform for your subscription and enter your Qualys username & password.

WAS Enhancements, YTD

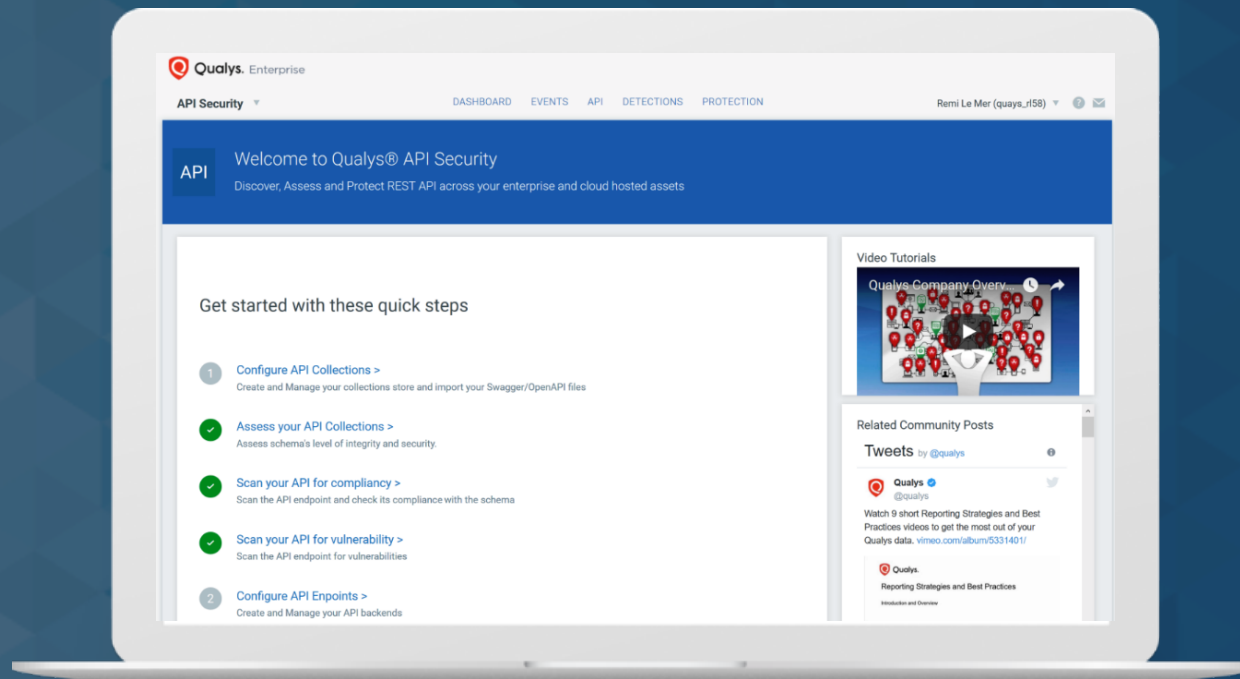


Qualys WAS Roadmap

WAS Roadmap



And Coming in 2019

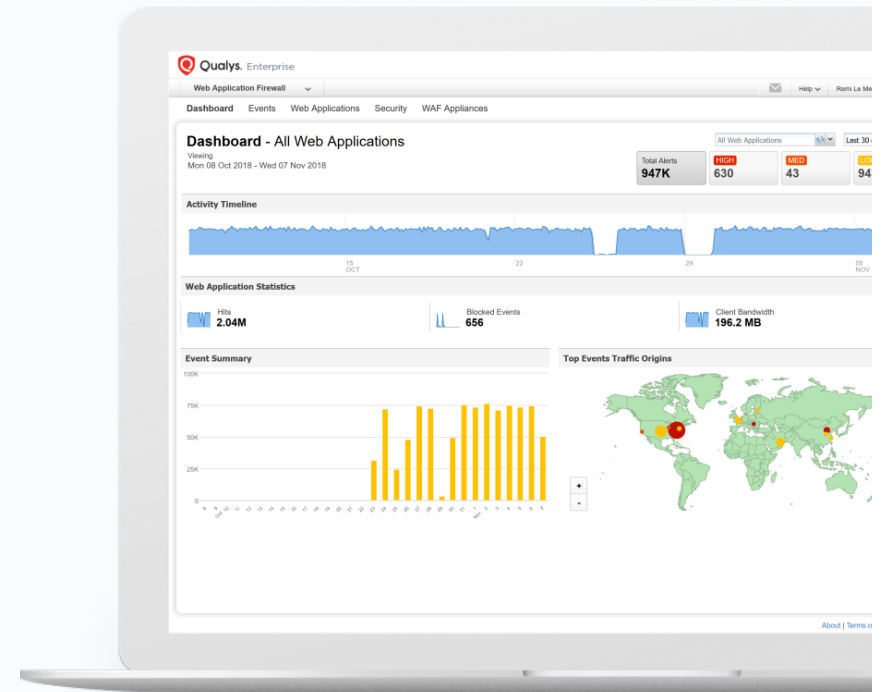


Web Application Firewall

Review

Qualys WAF

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



WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection
Assess both the application and the policy that protects it

The screenshot displays the ScanTrust Detection Management interface. The top navigation bar includes 'Detection Management', 'Detection List', 'Burp', and 'Bugcrowd'. The main content area shows a table of search results for '-demo.qualys.com'. The table has columns for Status, QID, Name, Group, Last Detected, Age, Patch, and Severity. The vulnerabilities listed include Blind SQL Injection (Protected), Reflected Cross-Site Scripting (XSS) Vulnerabilities (Protected), and Browser-Specific Cross-Site Scripting Vulnerabilities (Protected). A 'New' vulnerability is highlighted in yellow, with a 'Quick Actions' menu open, showing options like 'View', 'Ignore', 'Activate', 'Install Patch', 'Remove Patch', 'Edit Severity', 'Restore Standard Severity', and 'External References'. On the left, there are filters for 'Confirmed Vulnerability Level', 'Potential Vulnerability Level', 'Sensitive Content Level', 'Information Gathered Level', 'Status', and 'Group'.

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		
Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		
Protected	150013	Browser-Specific Cross-Site Scripting Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		
Fixed	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS	27 Oct 2016	512		
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS		716		

WAS / WAF Integration: Virtual Patch

Virtual Patch : One-click mitigation tool for CISO teams

Run from within WAS to address confirmed threats

Web Application Scanning

Dashboard Web Applications Sc

Detection Management

Search Results

150173 Search

Filter Results Clear All

Confirmed Vulnerability Level

Potential Vulnerability Level

Sensitive Content Level

Information Gathered Level

Install Virtual Patch

You are about to install a virtual patch

We'll automatically add a virtual patch rule to your WAF to block exploitation of the selected vulnerability on your web application. You can easily remove the virtual patch (and rule) at any time either here or from the WAF management interface.

Patch Details

When request.header.content-type MATCH `"^.*\\%.*\\{.*multipart/form-data$"` Add

- 1 request path MATCH `^[a-zA-Z0-9\\|\\-_%]...`
- 2 request header content-type MATCH `^.*\\%.*\\{.*multipart...`
- 3 request header Content-Type DETECT 150173
- 4 request query-string parameter p MATCH `^.*admin.*$`

1 - 10 of 10

id	Patch	Severity
1		High
2		High
3		High
4		High

Qualys

What's New in Qualys WAF

Supported Platforms

Shared and Private
Qualys Cloud Platforms

Add New WAF Appliance

Select Virtual Appliance Image

Choose the virtualization platform you want to use to run your WAF appliance on.

Platform	Details
<input checked="" type="radio"/> VMware Standard	VMware virtualization platform
<input type="radio"/> Hyper-V	Microsoft Hyper-V 5.1 virtualization platform
<input type="radio"/> Amazon EC2	Amazon EC2-Classic, Amazon EC2-VPC
<input type="radio"/> Microsoft Azure	Microsoft Azure platform
<input type="radio"/> Google Cloud	Google Cloud platform
<input type="radio"/> Docker	Docker platform

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

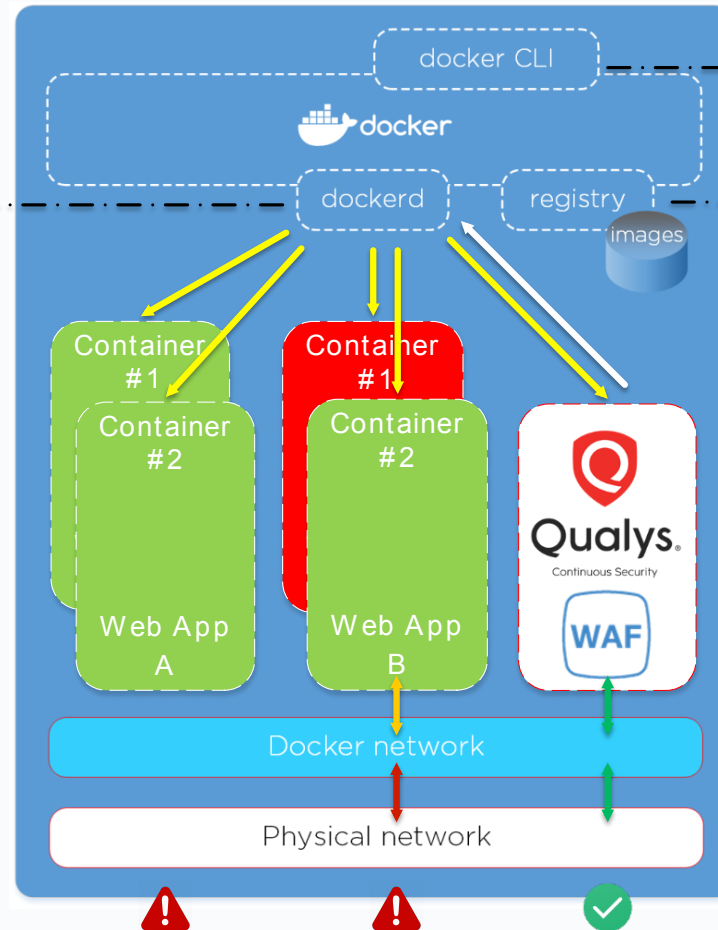
Orchestration via Qualys API



Docker

Single Host

- Controls :
- containers (start | stop | delete | inspect)
 - networks
 - images (pull | push | delete)



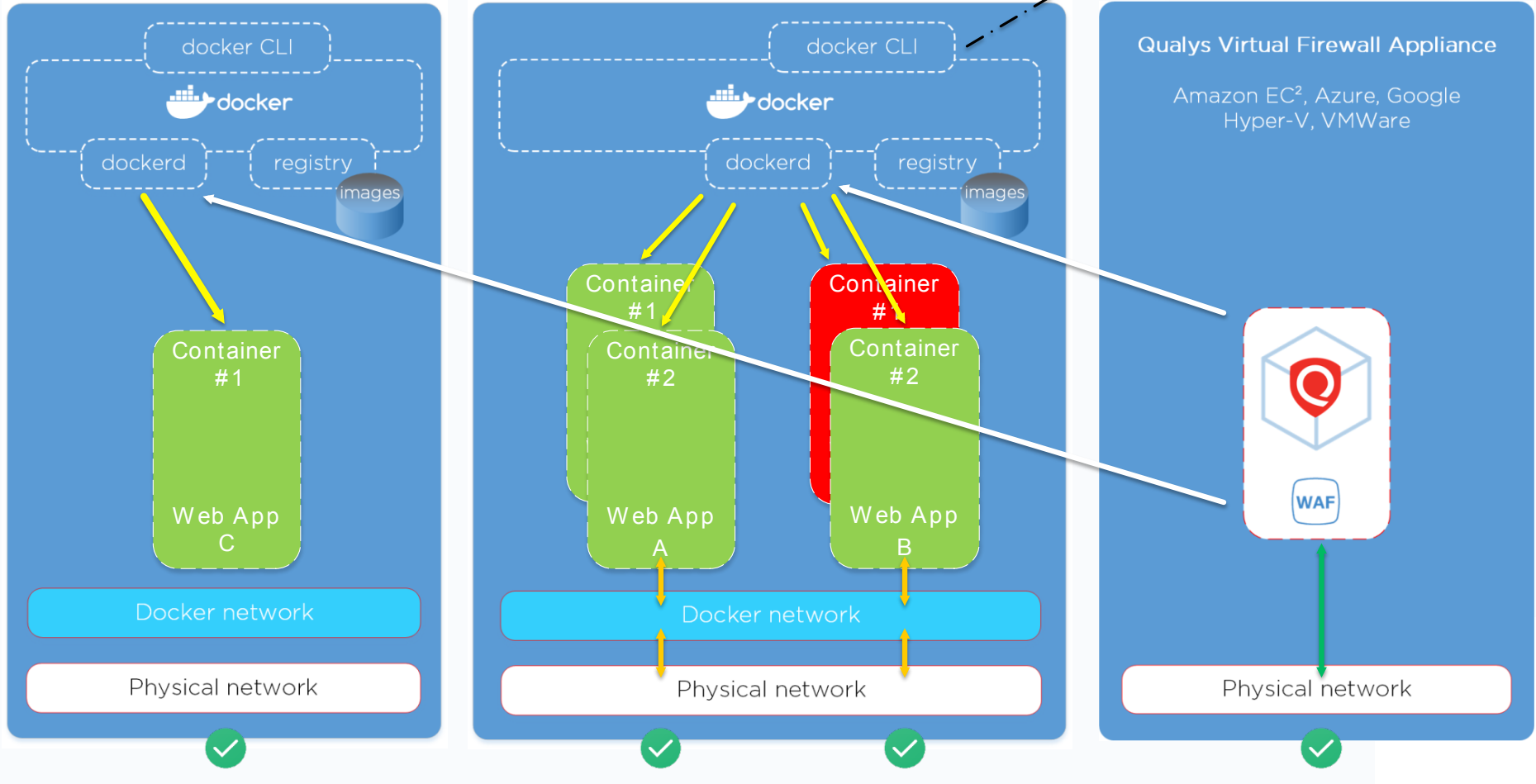
Access to docker services via unix sockets

Stores images

Docker

Multiple Hosts

Access to docker services via network sockets



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

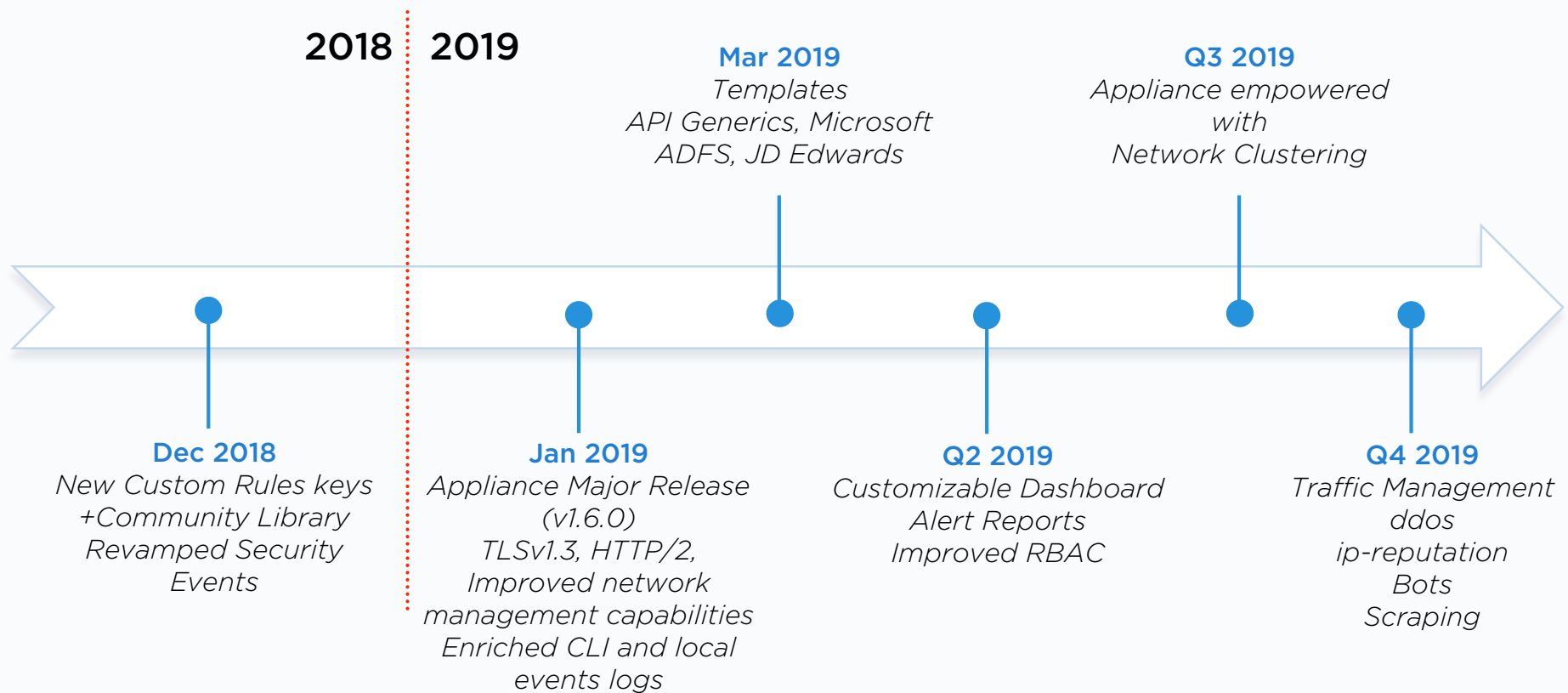
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x

- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x

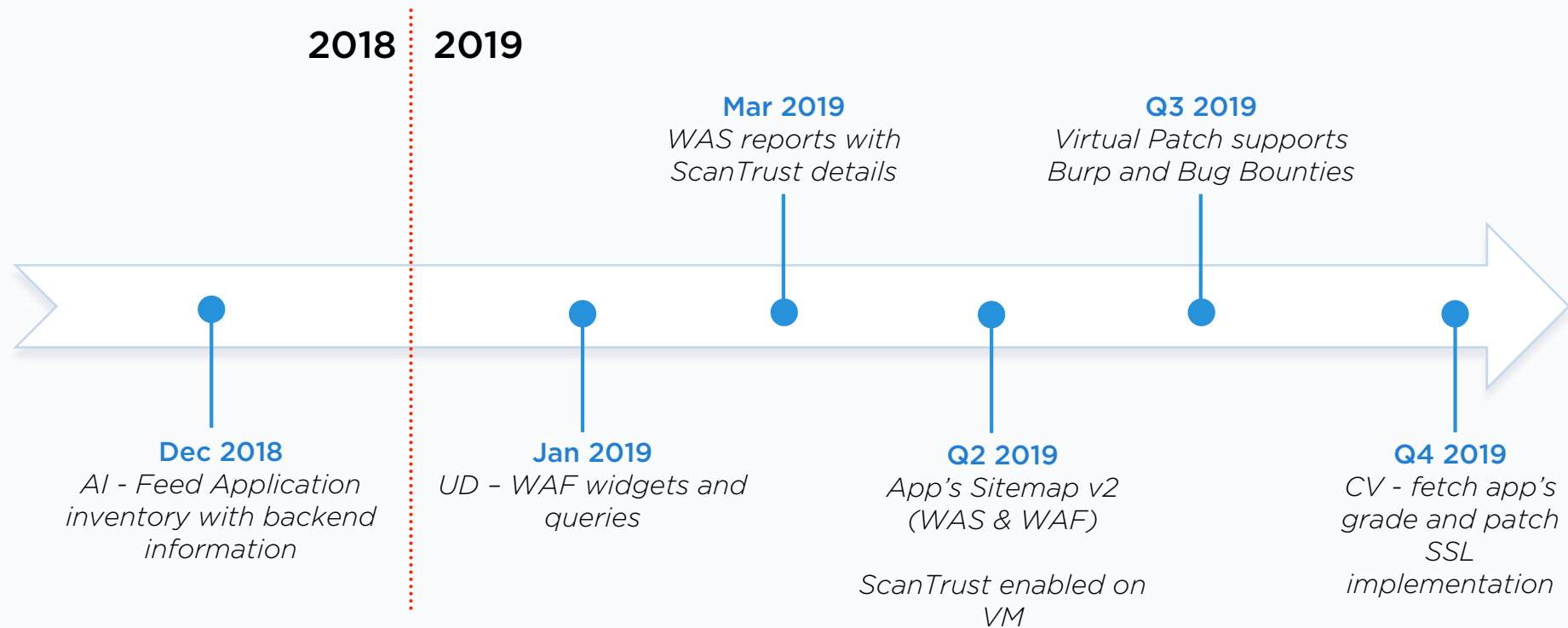
- Qualys Generics for unknown apps

Qualys WAF Roadmap

WAF Roadmap - Standalone



WAF Roadmap – Integrated Suite





QUALYS SECURITY CONFERENCE 2018

Thank You

Dave Ferguson - dferguson@qualys.com

Remi Le Mer - rlemer@qualys.com