

# Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

Jimmy Graham

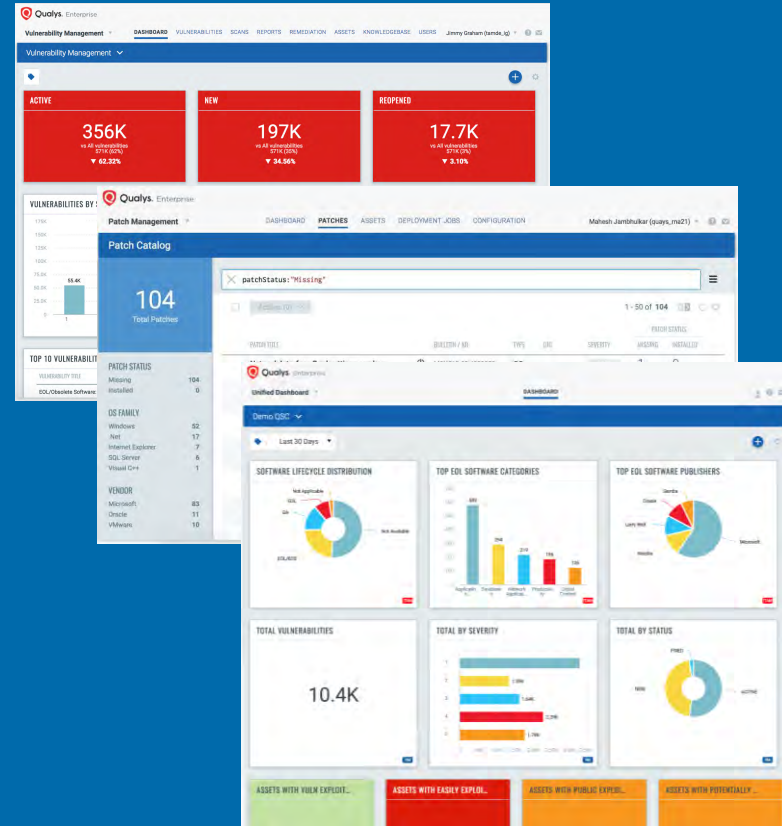
*Senior Director, Product Management, Qualys, Inc.*

# Agenda

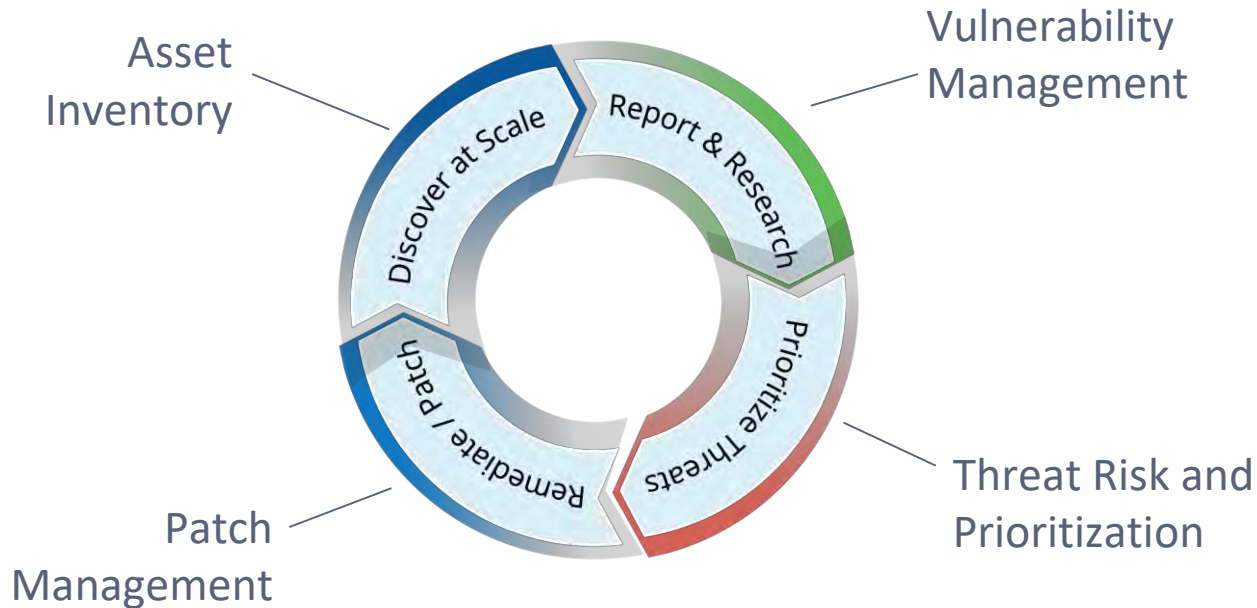
Expanding Vulnerability Management

Vulnerability Management Platform Evolution

Introducing Qualys Patch Management



# Vulnerability Management Lifecycle



# Expanding Vulnerability Management



# Case Study: Large Bank

## Challenge

Difficult to prioritize vulnerabilities across 100,000 endpoints

Manual correlation of external threat data

No active alerting on high-threat vulnerabilities

Low visibility into workstations

## Solution

Threat Protection RTIs automates prioritization

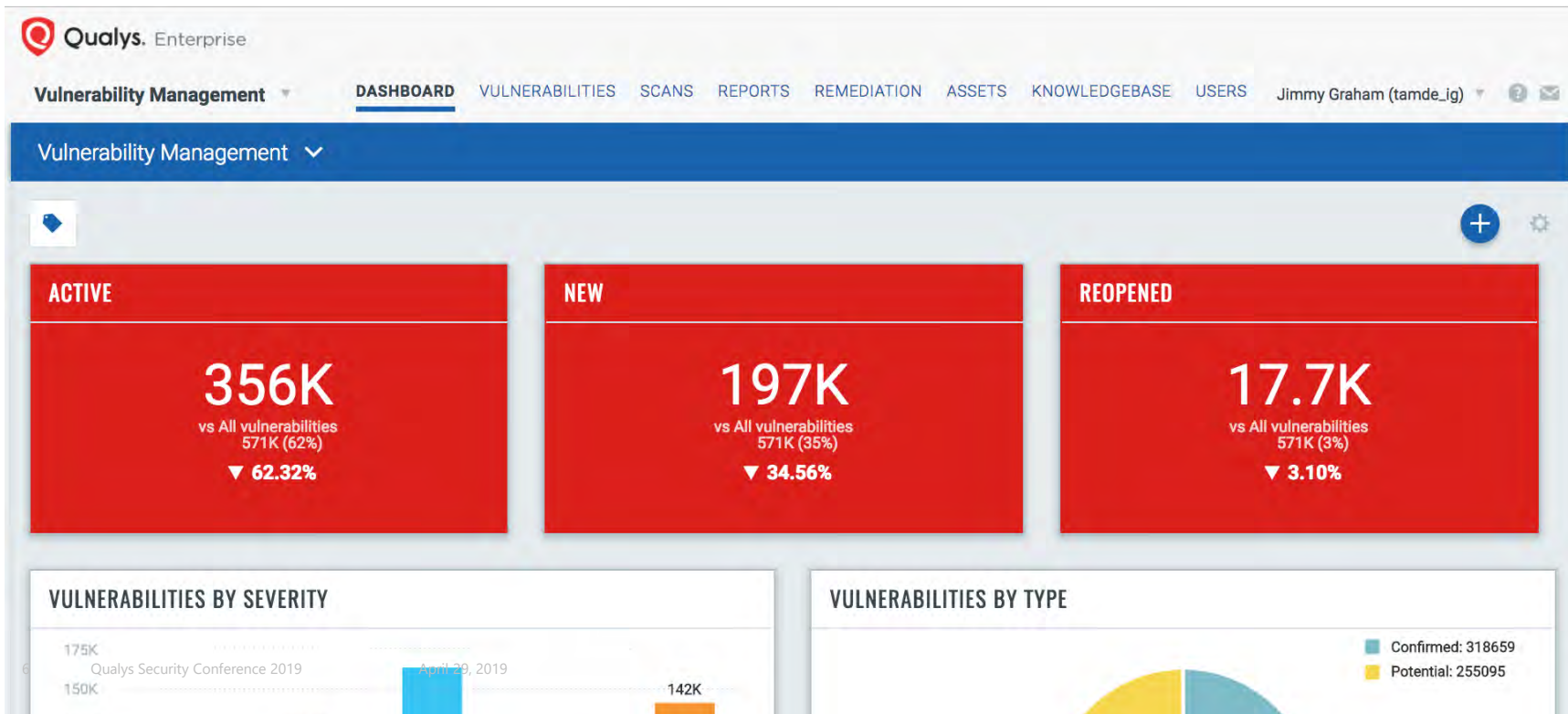
Threat Protection Live Feed provides one-click access to impacted assets

Continuous Monitoring combined with RTIs

Qualys Cloud Agent for continuous and complete visibility

# Vulnerability Management

## Platform Evolution



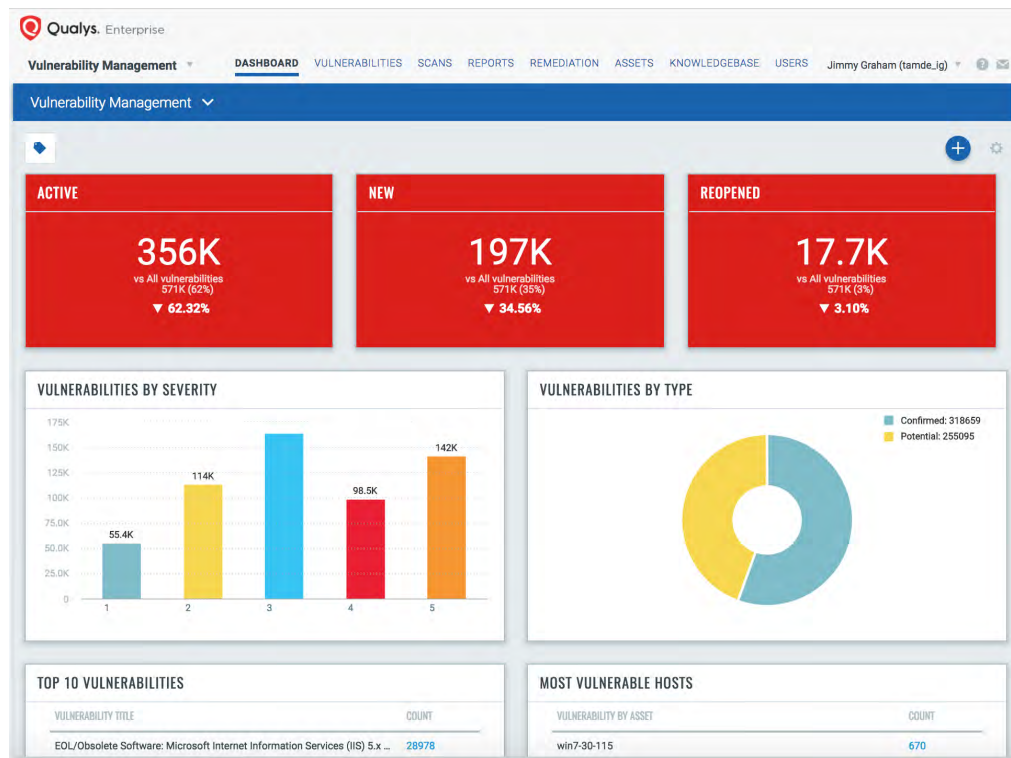
# Dynamic VM Dashboard

Merges AssetView  
technology into Qualys VM

Build widgets with  
vulnerability counts

Search filters for quickly  
building queries

Replace long-running reports  
with live widgets



# Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface  
(QRDI)

Create your own or share on Qualys  
Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

```
{ } IPcam_QRDI.json ●
1  {
2  "detection_type": "http_dialog", "api_version": 1, "trigger_type": "
3  "dialog": [
4      {
5          "transaction": "http_get",
6          "object": "/cgi-bin/CGIPProxy.fcgi?usr=visitor&pwd=testingq
7          "on_error": "stop" |
8      },
9      {
10         "transaction": "process",
11         "mode": "regexp",
12         "match": "<firmwareVer>(.*?)</firmwareVer>",
13         "extract": [{"var": "wholeMatch"}, {"var": "firmwareVersion"}
14     ],
15     {
16         "transaction": "report", "result": {"concat": ["Foscam Firm
17     }
18 ]
19 }
20
```





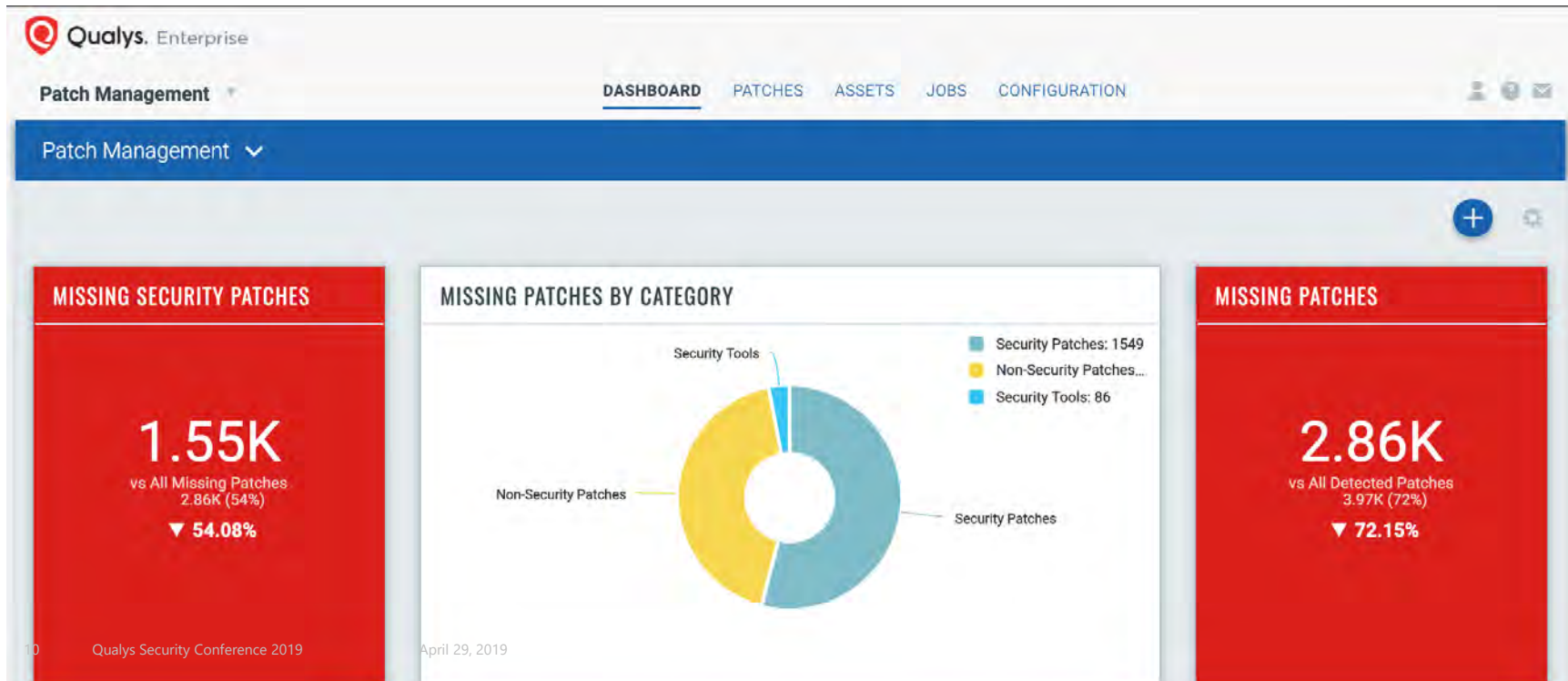
DEMO

# Vulnerability Management

## Dynamic Dashboard

# Qualys Patch Management

## Overview



# Current Patch Management Tools

## Challenges and Impact



Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

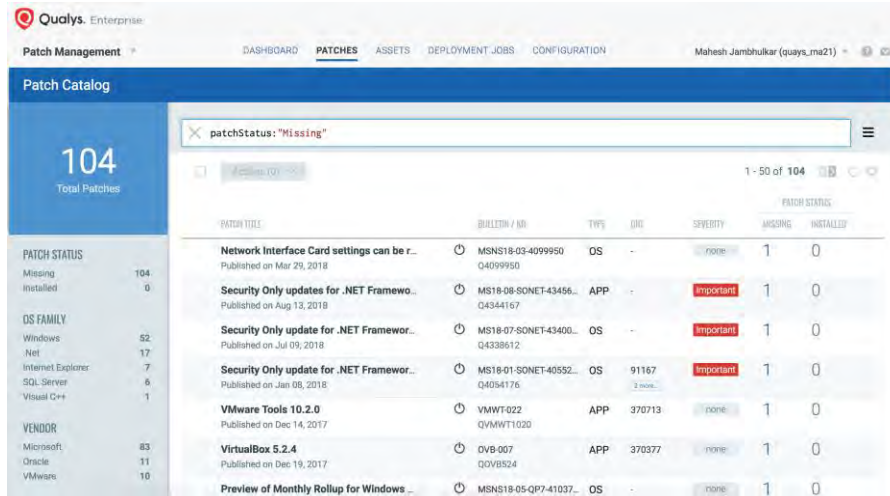
Waiting for vulnerability reports to confirm remediation

Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

# Introducing Qualys Patch Management



The screenshot shows the Qualys Enterprise Patch Management interface. The top navigation bar includes 'DASHBOARD', 'PATCHES', 'ASSETS', 'DEPLOYMENT JOBS', and 'CONFIGURATION'. The user is logged in as 'Maresh Jambhulkar (qualys\_ma21)'. The main area is titled 'Patch Catalog' and shows a search filter for 'patchStatus: "Missing"'. A summary box on the left indicates '104 Total Patches'. Below this is a table of patches with columns for Patch Title, Bulletin / ID, Type, Urgency, Severity, Actions, and Install. The table lists several missing patches, including updates for .NET Framework, VMware Tools, and VirtualBox.

PATCH STATUS	MISSING	INSTALLED
Missing	104	0
Installed	0	0

PATCH TITLE	BULLETIN / ID	TYPE	URGENCY	SEVERITY	ACTIONS	INSTALL
Network Interface Card settings can be r...	MSNS18-03-4099950 Q4099950	OS	-	none	1	0
Security Only updates for .NET Framewo...	MS18-08-SONET-43456... Q4344167	APP	-	Important	1	0
Security Only update for .NET Framewor...	MS18-07-SONET-43400... Q4338612	OS	-	Important	1	0
Security Only update for .NET Framewor...	MS18-01-SONET-40552... Q4054176	OS	91167 2 week...	Important	1	0
VMware Tools 10.0.2.0	VMWTF022 QVMWTF020	APP	370713	none	1	0
VirtualBox 5.2.4	DVB-007 QDVBS24	APP	370377	none	1	0
Preview of Monthly Rollup for Windows ...	MSNS18-05-QP7-41037... OS	-	-	none	1	0

Automated correlation of  
vulnerability and patch data  
– Which patch fixes the CVE?

Simple dashboarding for  
tracking missing patches

Patch using the Qualys  
Cloud Agent, anywhere

Patch OS and third-party  
applications

Single solution for Windows,  
macOS, and Linux

# Shift From Reaction Mode to Operational Security



Always up-to-date on  
missing patches

Security and IT teams can “speak the same language”

Collaboration – key to successful digital transformation

Unify discovery, prioritization, and remediation into one platform

Rapid remediation of high-profile vulnerabilities in days vs. weeks

Regularly scheduled deployments are repeatable and reported on



DEMO

# Patch Management

# Platform Support



XP SP3+  
Vista  
Windows 7  
Windows 8/8.1  
Windows 10  
Server 2003 SP2+  
Server 2008/R2  
Server 2012/R2  
Server 2016  
Server 2019



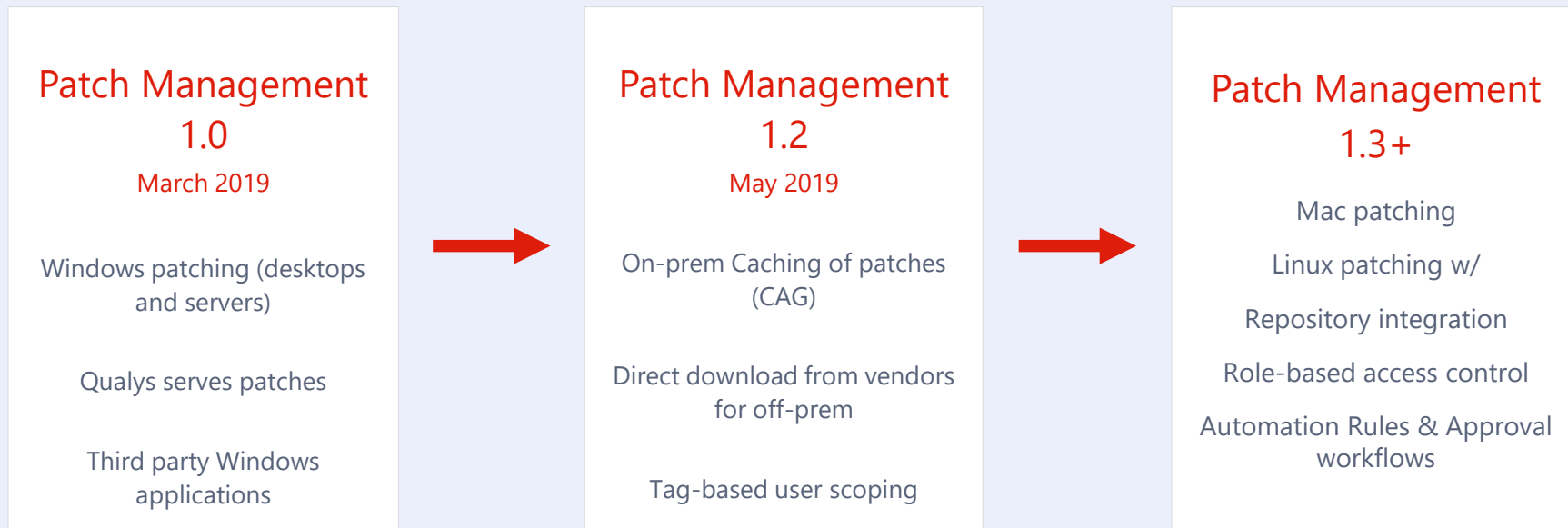
OS X 10.10  
Yosemite  
OS X 10.11  
El Capitan  
macOS 10.12  
Sierra  
macOS 10.13  
High Sierra  
macOS 10.14  
Mojave



RHEL 6,7  
CentOS 5.4+,6,7  
SUSE Linux Enterprise  
Server/ Desktop  
11,12,15  
Oracle Ent Linux  
6,7(Server)  
Ubuntu  
14.x,15.x,16.x,18.x

\* Roadmap items are future-looking; timing and specifications may change

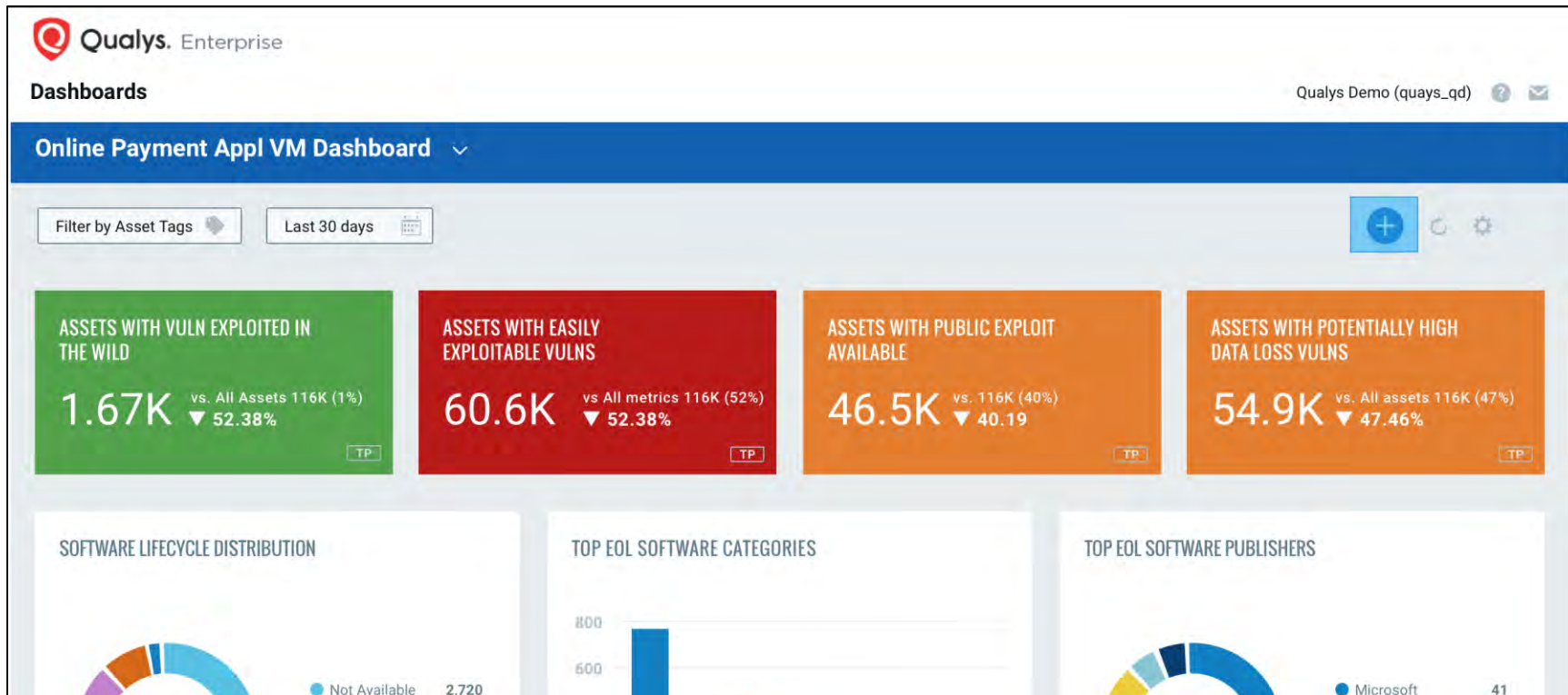
# Patch Management Roadmap





# Qualys Unified Dashboard

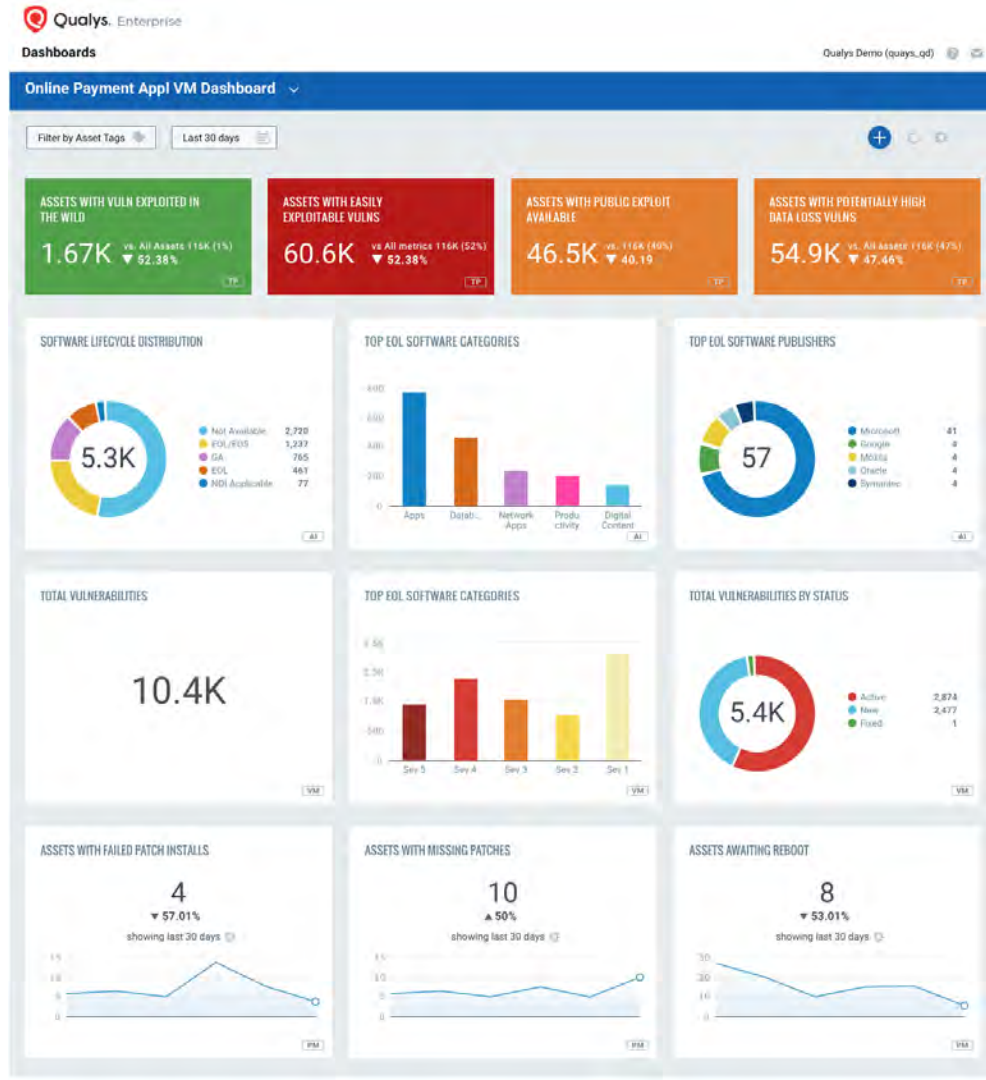
Preview



# Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags





PREVIEW

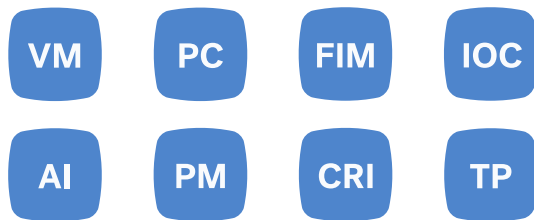
# Unified Dashboard

# Unified Dashboard Rollout

## Phase 1 – Q3 2019

Unified Dashboard App  
Global dashboard filters

Support for:



## Phase 2 – Q1 2020

Unified widget builder  
Upgrade existing Cloud App  
Dashboards

Support for:





# Thank You

**Jimmy Graham**

[jgraham@qualys.com](mailto:jgraham@qualys.com)