



QUALYS SECURITY CONFERENCE 2018

# Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

**Jimmy Graham**

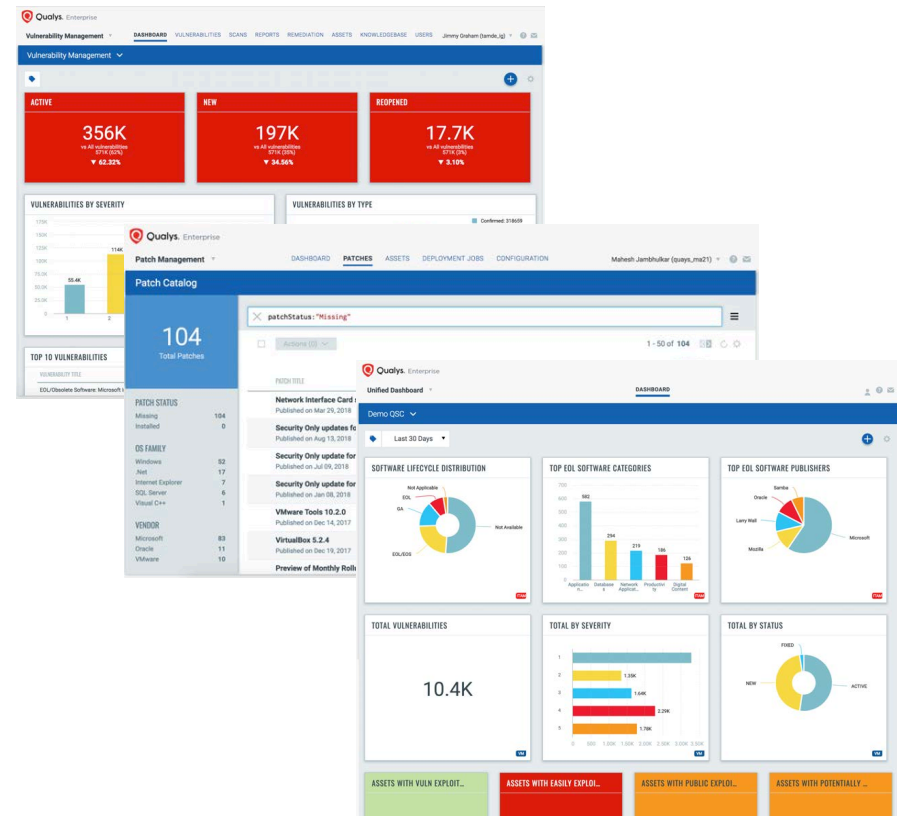
Senior Director, Product Management, Qualys, Inc.

# Agenda

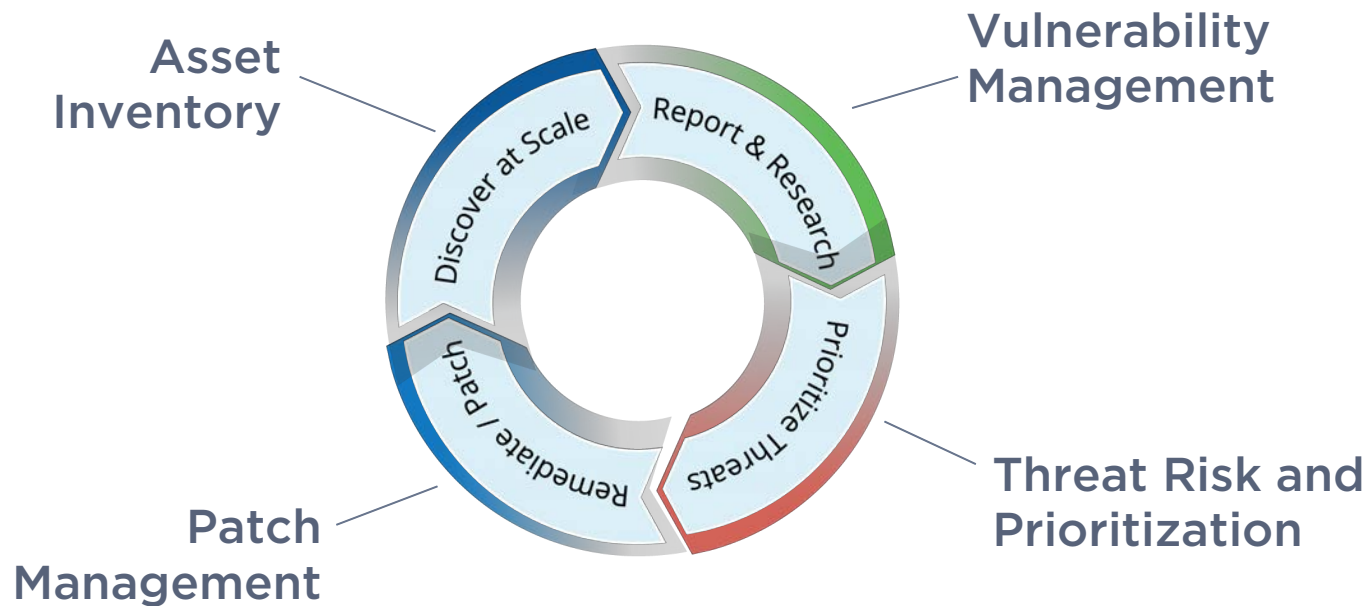
Expanding Vulnerability Management

Introducing Qualys Patch Management

Unified Dashboard



# Vulnerability Management Lifecycle



# Expanding Vulnerability Management



# Case Study: Large US 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

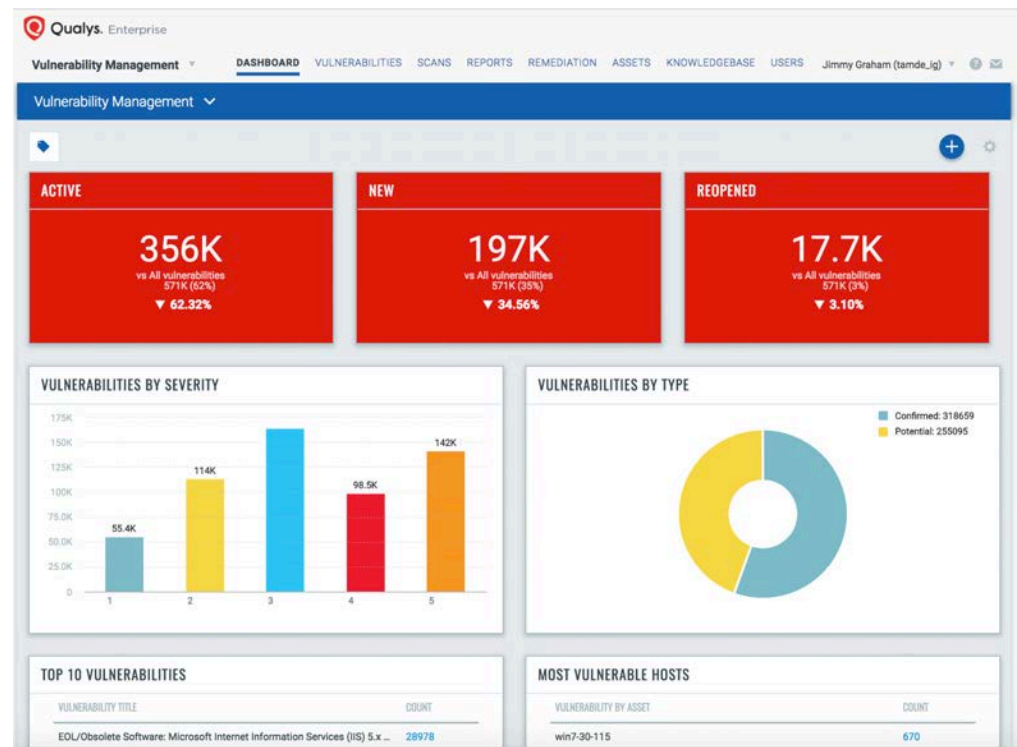
# Elastic VM Dashboard

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": "regex",
12       "match": "<firmwareVer>(.*?)</firmwareVer>",
13       "extract": [{"var": "wholeMatch"}, {"var": "firmwareVersion"
14     },
15     {
16       "transaction": "report", "result": {"concat": ["Foscam Firr
17     }
18   ]
19 }
20
```



Patch Management

DASHBOARD

PATCHES

ASSETS

DEPLOYMENT JOBS

CONFIGURATION

gFrameStandard11231

Patch Control

Demo



# Elastic VM Dashboard

Adobe Reader 2017.00804  
Security Update April 2017

MS17-010

4013264

OS

100%

197040

CS-2017-0001

No

4

5

Microsoft .NET Framework  
Security Update April 2017

MS17-008

4013264

OS

100%

197040

CS-2017-0001

No

4

5

Microsoft SQL Server 2008 R2  
Service Pack 3 (KB2979597)

MS17-007

2979597

APP

100%

351175

CS-2017-0001

No

1

5

Microsoft Windows Security  
Update May 2017

MS17-004

4013263

4013264

OS

100%

197064

None

Yes

3

5

Oracle Java SE Critical Patch  
Update - April 2017

MS17-004

APP

100%

170682

CS-2017-0001

No

4

5

Security Updates for Windows  
Server 2008 x64 Edition...

MS16-002

APP

100%

170682

CS-2017-0001

No

3

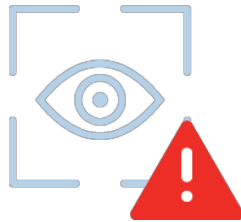
5

# 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 the patch has fixed the vulnerability

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

Qualys Enterprise

Patch Management

DASHBOARD PATCHES ASSETS DEPLOYMENT JOBS CONFIGURATION

Mahesh Jambhulkar (qualys\_ma21)

Patch Catalog

104 Total Patches

patchStatus: "Missing"

Actions (0)

1 - 50 of 104

PATCH TITLE	BULLETIN / KB	TYPE	OS	SEVERITY	PATCH STATUS	
					MISSING	INSTALLED
Network Interface Card settings can be r... Published on Mar 29, 2018	MSNS18-03-4099950 Q4099950	OS	-	none	1	0
Security Only updates for .NET Framewo... Published on Aug 13, 2018	MS18-08-SONET-43456... Q4344167	APP	-	Important	1	0
Security Only update for .NET Framewor... Published on Jul 09, 2018	MS18-07-SONET-43400... Q4338612	OS	-	Important	1	0
Security Only update for .NET Framewor... Published on Jan 08, 2018	MS18-01-SONET-40552... Q4054176	OS	91167	Important	1	0
VMware Tools 10.2.0 Published on Dec 14, 2017	VMWTF022 QVMWTF1020	APP	370713	none	1	0
VirtualBox 5.2.4 Published on Dec 19, 2017	OVB-007 QOVB524	APP	370377	none	1	0
Preview of Monthly Rollup for Windows ...	MSNS18-05-QP7-41037...	OS	-	none	1	0

PATCH STATUS

Missing 104  
Installed 0

OS FAMILY

Windows 52  
.Net 17  
Internet Explorer 7  
SQL Server 6  
Visual C++ 1

VENDOR

Microsoft 83  
Oracle 11  
VMware 10

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

Simple dashboarding for  
tracking patch deployments

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

## Beta

Adobe Reader and Acrobat  
Security Update 10

MS17-NET-04

4019261

APP

777119

CVE-2016-3121  
CVE-2016-3122

No

2

2

Microsoft .NET Framework  
Security Update April 2017

APSB1704

4019262

OS

107040

CVE-2016-0054  
CVE-2016-0055

Yes

4

4

Microsoft SQL Server 2008 R2  
Service Pack 3 (KB2979597)

MS17-NET-04

2979597

APP

381175

CVE-2017-0871

Yes

1

1

Microsoft Windows Security  
Update May 2017

MS17-NET-04

4019263  
4019264

OS

197064

None

Yes

3

3

Oracle Java SE Critical Patch  
Update - April 2017

MS17-NET-04

4019261

APP

170682

CVE-2016-0755

No

4

5

Security Updates for Windows  
Server 2008 x64 Edition...

MS16-NET-02

4019261

APP

170682

CVE-2016-0755

No

3

5

# Platform Support



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



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

\* Beta will focus on Windows- other operating systems will follow later

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

# Roadmap

**Beta:** Q4 2018 – Windows patch deployment  
**General Availability:** Early 2019

## Beta 1

Windows patching  
(desktops and servers)

Qualys serves patches

Third party Windows  
applications



## Beta 2

On-prem Caching of  
patches (QGS)

Direct download from  
vendors for off-prem

Additional tokens for  
dashboarding



## Upcoming

Mac patching

Linux patching

Repository integration

Automation Rules &  
Approval workflows



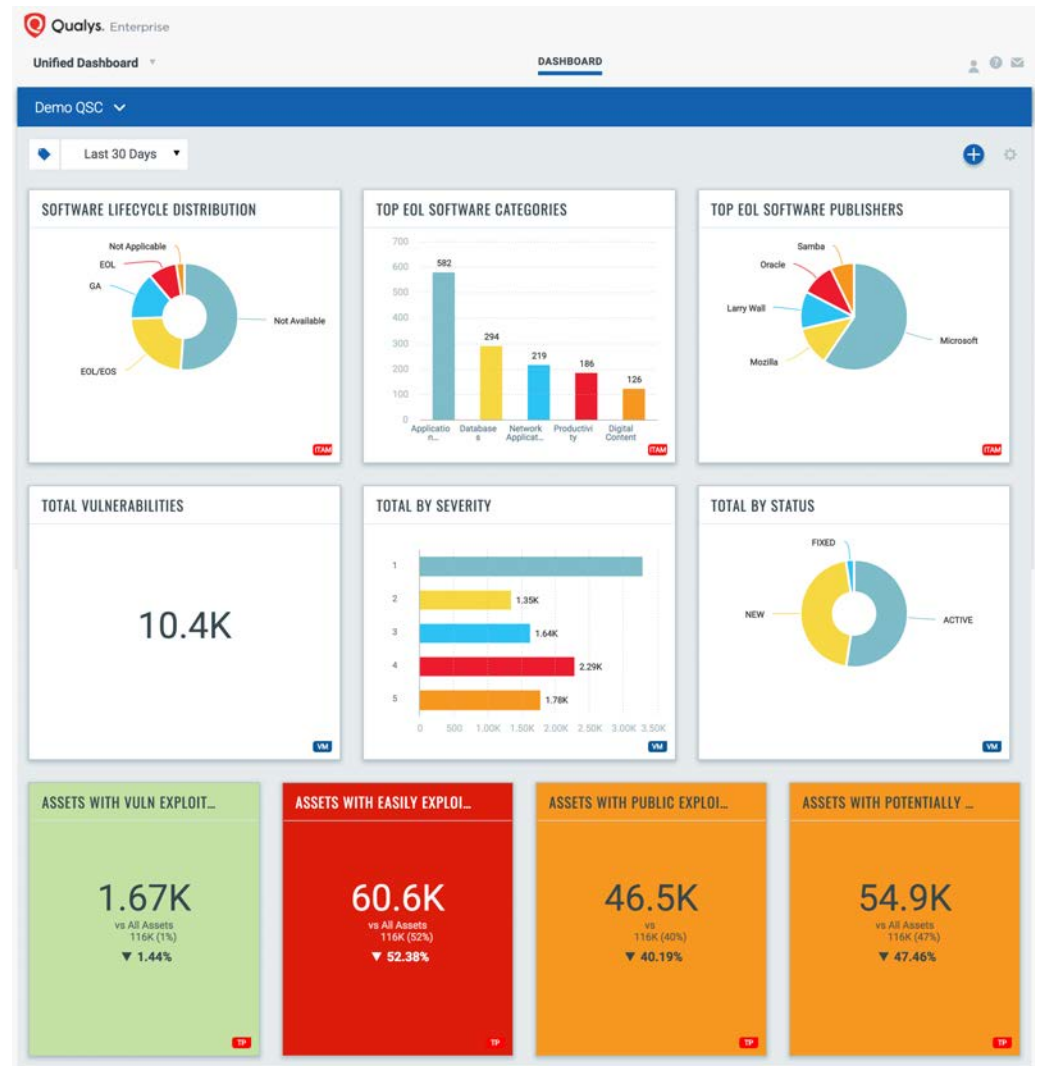
# Unified Dashboards

## Overview

# Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

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



Patch Management

DASHBOARD

PATCHES

ASSETS

DEPLOYMENT JOBS

CONFIGURATION

g frame standard (1/23)

Patch Categories

Demo



# Unified Dashboard

## Preview

ADDITIONAL INFO

Adobe Reader and Acrobat  
Security Update (KB2869272)

MS17-004

357718

APP

357718

1/16/2016

Yes

3

5

ADDITIONAL INFO

Microsoft .NET Framework  
Security Update April 2017

MS17-004

357718

APP

357718

1/16/2016

Yes

3

5

ADDITIONAL INFO

Microsoft SQL Server 2008 R2  
Service Pack 3 (KB2979597)

MS17-004

357718

APP

357718

1/16/2016

Yes

3

5

ADDITIONAL INFO

Microsoft Windows Security  
Update May 2017

MS17-004

357718

OS

357718

1/16/2016

Yes

3

5

ADDITIONAL INFO

Oracle Java SE Critical Patch  
Update - April 2017

MS17-004

357718

APP

357718

1/16/2016

Yes

3

5

ADDITIONAL INFO

Security Updates for Windows  
Server 2008 x64 Edition...

MS17-004

357718

APP

357718

1/16/2016

Yes

3

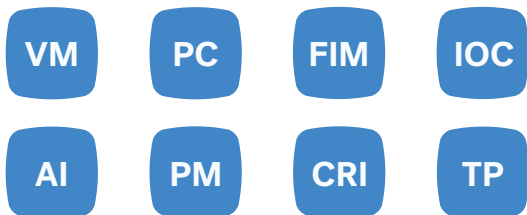
5

# Unified Dashboard Rollout

## Phase 1

Unified Dashboard App  
Global dashboard filters

Support for:



## Phase 2

Unified widget builder  
Upgrade existing Cloud  
App Dashboards

Support for:





QUALYS SECURITY CONFERENCE 2018

# Thank You

**Jimmy Graham**  
jgraham@qualys.com