QUALYS SECURITY CONFERENCE 2018

# Real-Time Vulnerability Management

## Operationalizing the VM process from detection to remediation

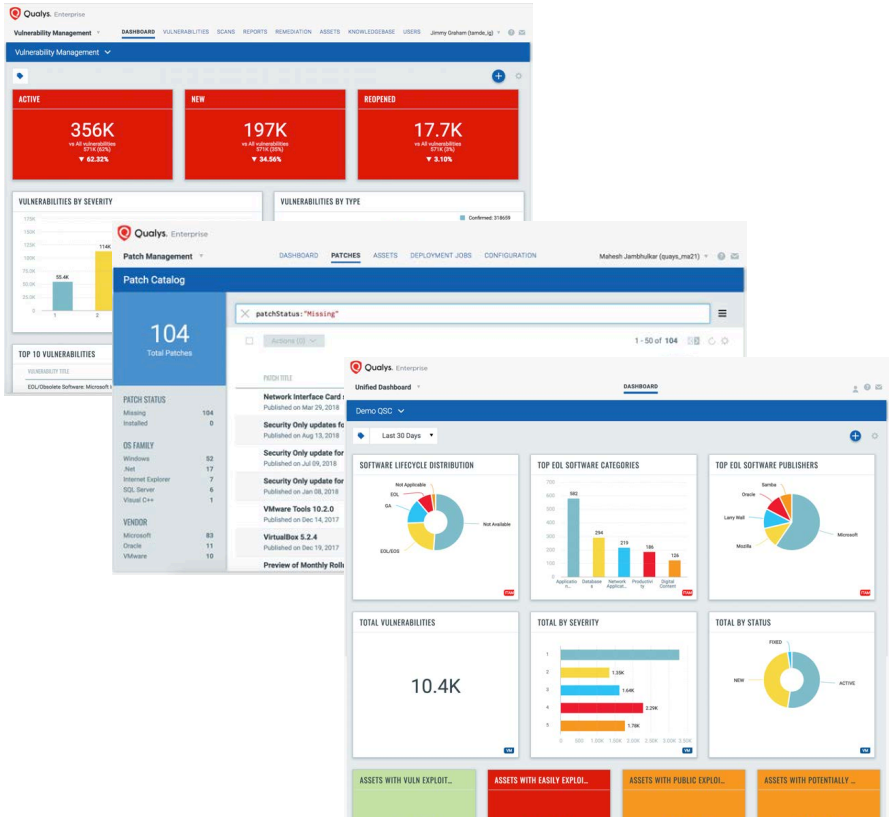
**Jimmy Graham**
Senior Director, Product Management, Qualys, Inc.

# Agenda

Expanding Vulnerability Management

Introducing Qualys Patch Management

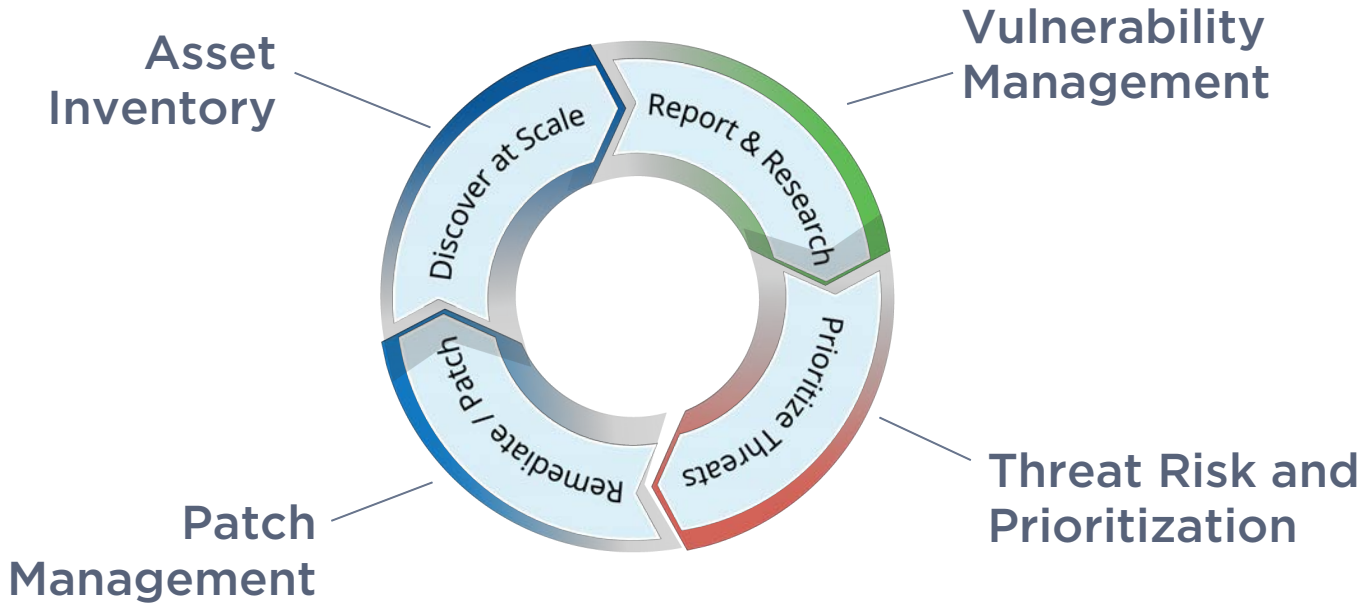
Unified Dashboard






Qualys.

# Vulnerability Management Lifecycle






Qualys.

# Expanding Vulnerability Management




Qualys.

# 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

Qualys.

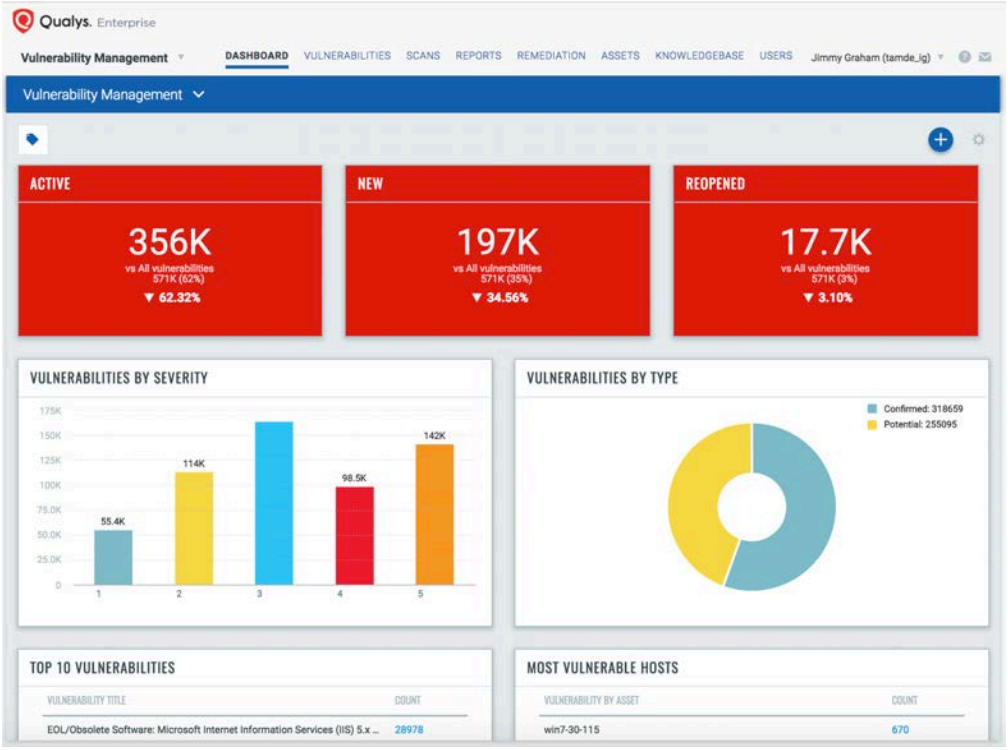
# Elastic VM Dashboard

Merges AssetView technology into Qualys VM

Build widgets with vulnerability counts

Search filters for quickly building queries

Replace long-running reports with live widgets






Qualys.

# Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface (QRDI)

Create your own or share on Qualys Community

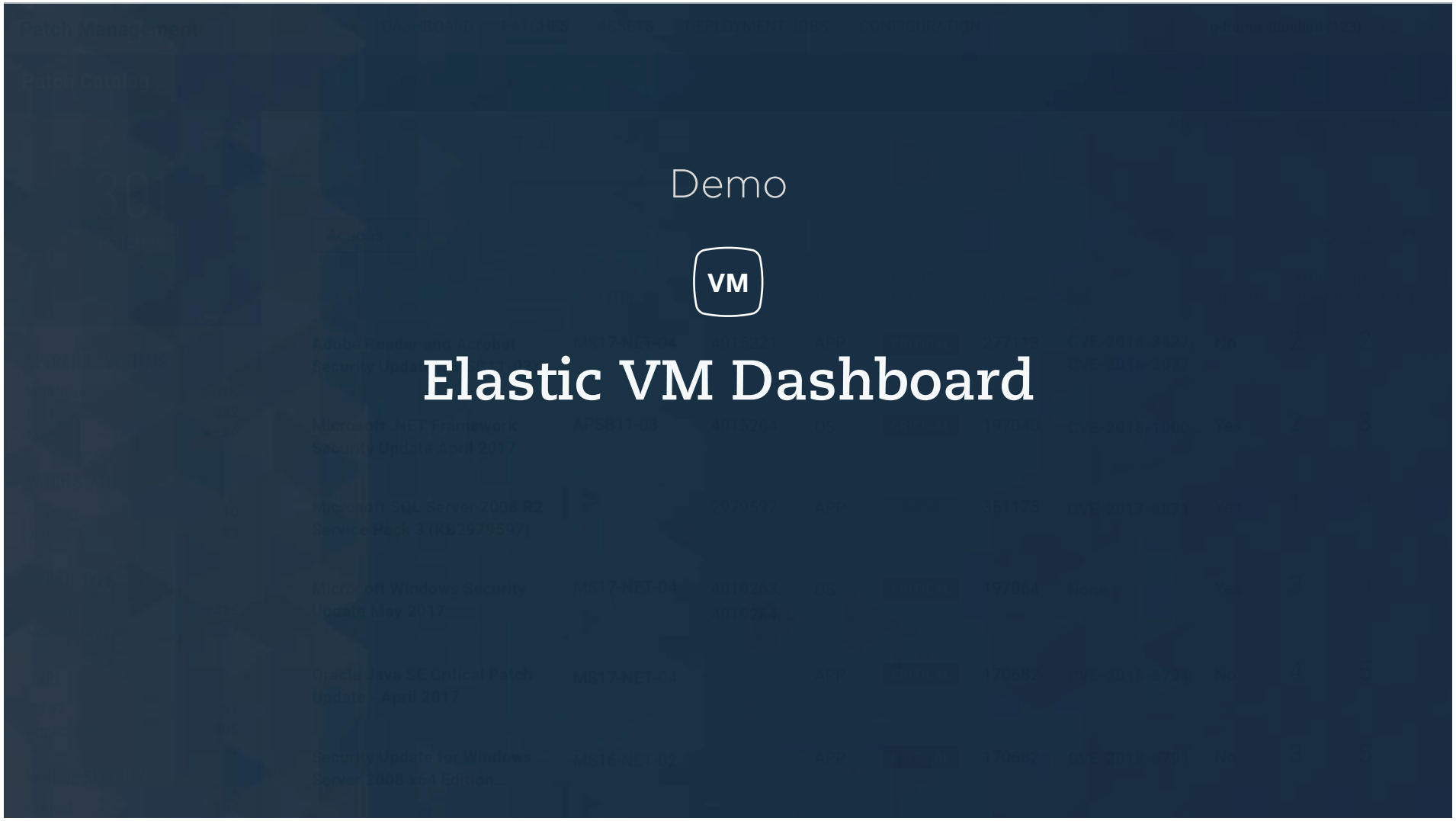
Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic




Qualys.


Demo
VM
Elastic VM Dashboard

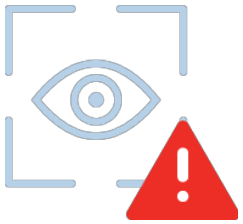
# Qualys Patch Management

## Overview

Qualys.

# 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

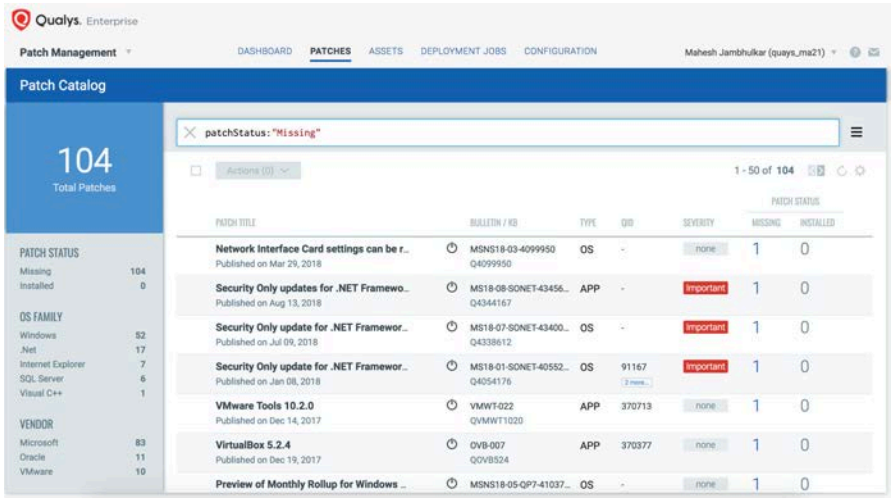
Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing

# Qualys Patch Management




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

Qualys


Demo
PM
Patch Management
Beta

# 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



Qualys.

# 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



Qualys.

# Unified Dashboards

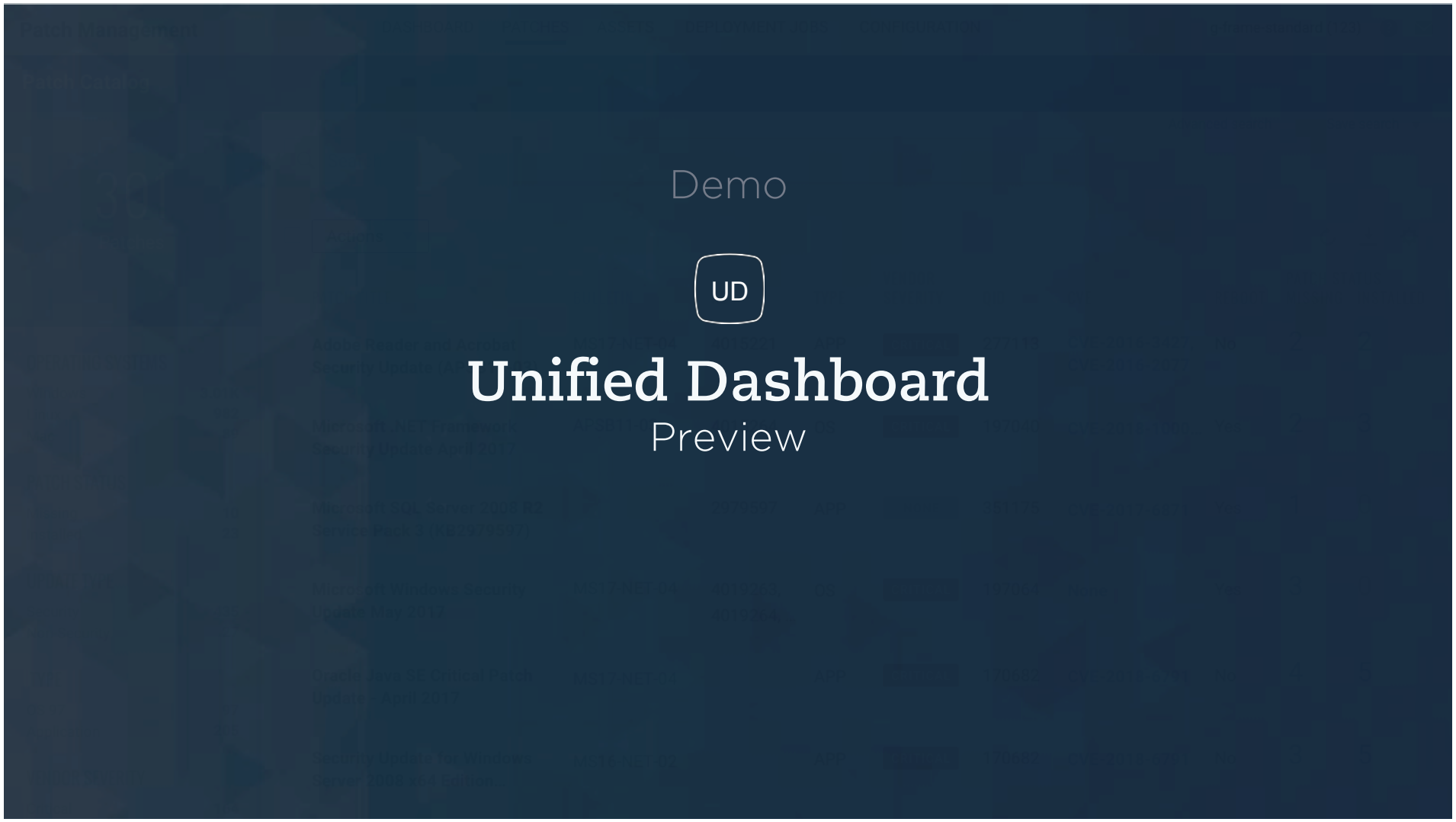
## Overview

Qualys.

# Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

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


Demo
UD
Unified Dashboard
Preview

# Unified Dashboard Rollout

## Phase 1

Unified Dashboard App

Global dashboard filters

Support for:

VM PC FIM IOC

AI PM CRI TP

## Phase 2

Unified widget builder

Upgrade existing Cloud App Dashboards

Support for:

WAS WAF SAQ

CS CV

# Thank You

**Jimmy Graham**
jgraham@qualys.com