Qualys. | MAKING THE WORLD SAFER – ONE APP AT A TIME

# Security at a Crossroads

## A significant opportunity for Qualys

Melissa Fisher, CFO
Philippe Courtot, Chairman & CEO
Sumedh Thakar, Chief Product Officer
Dilip Bachwani, SVP Cloud Platform

INVESTOR & ANALYST PRODUCT LUNCHEON - BLACK HAT - AUG 7th 2019

# Agenda

Security at a Crossroads

What makes Qualys Unique

Ubiquity Play

Cloud Platform Expansion

Blending Data Lake, SOAR, SIEMs, EDR and EPP into our Cloud Platform

Summary

Everything visible. Everything secure.

A single cloud platform for IT, security and compliance across all your global IT assets.

Designed from the Ground Up
for the Digital Transformation

# Security at a Crossroads

Fueled by cloud technologies, the security industry is on the verge of a massive and accelerated consolidation. We believe the market will coalesce into four distinct segments

Large Enterprises
Public Cloud Providers
New Generation of MSSPs
OT/IoT environments

*Qualys, thanks to its scalable and extensible Cloud Security and Compliance Platform and highly scalable and profitable business model is, we believe, uniquely positioned to address these four market segments and become a major actor in the consolidation of the industry.*

The digital transformation has created an explosion of new technology and opportunities.

It has left chaos and many gaping security holes in its wake.

Today's plethora of current IT, security and compliance tools create more problems than they solve – delivering diminishing returns.

# Going Back to our Origins – 1999

## Our Original Mission and Vision

Apply nascent Internet Technologies (called now SaaS or Cloud) to automate Vulnerability Assessment making it accurate, continuous and scalable.

72% F50, 61% F100,

46% F500 and 25% Global 2000

ADP
Agilent Technologies
ally
accenture
AVAYA
Boston Scientific
GM
CATERPILLAR
kpn
cisco
DAIMLER
DU PONT
Deloitte.
DOWJONES
ERNST & YOUNG
gsk
Goldman Sachs
THE HOME DEPOT
hp
KPMG
Lilly
Man Group plc
NISSAN
PRICEWATERHOUSECOOPERS
PURDUE
SYBASE
bp
STARWOOD
HOTELS & RESORTS WORLDWIDE, INC.
Ogilvy
ORACLE
Russell Investments
Symantec.
STAPLES
STARZ!
VIACOM
intuit
MORNINGSTAR
THOMSON
TOSHIBA
VeriSign
Walgreens
WB
WILLIAMS-SONOMA

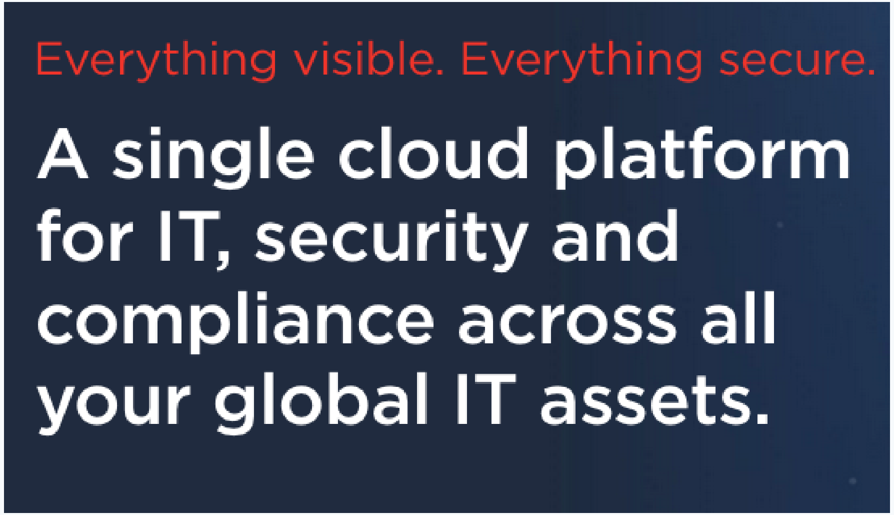
12,200+ customers and active users in 130+ countries

Qualys.

# Where Are We Now?

## Today's Mission and Vision

Unifying IT, Security and Compliance in a single-pane-of-glass-view with 2-second visibility across on-premises, endpoints, cloud(s), containers, web apps, API, mobile and OT/IoT environments



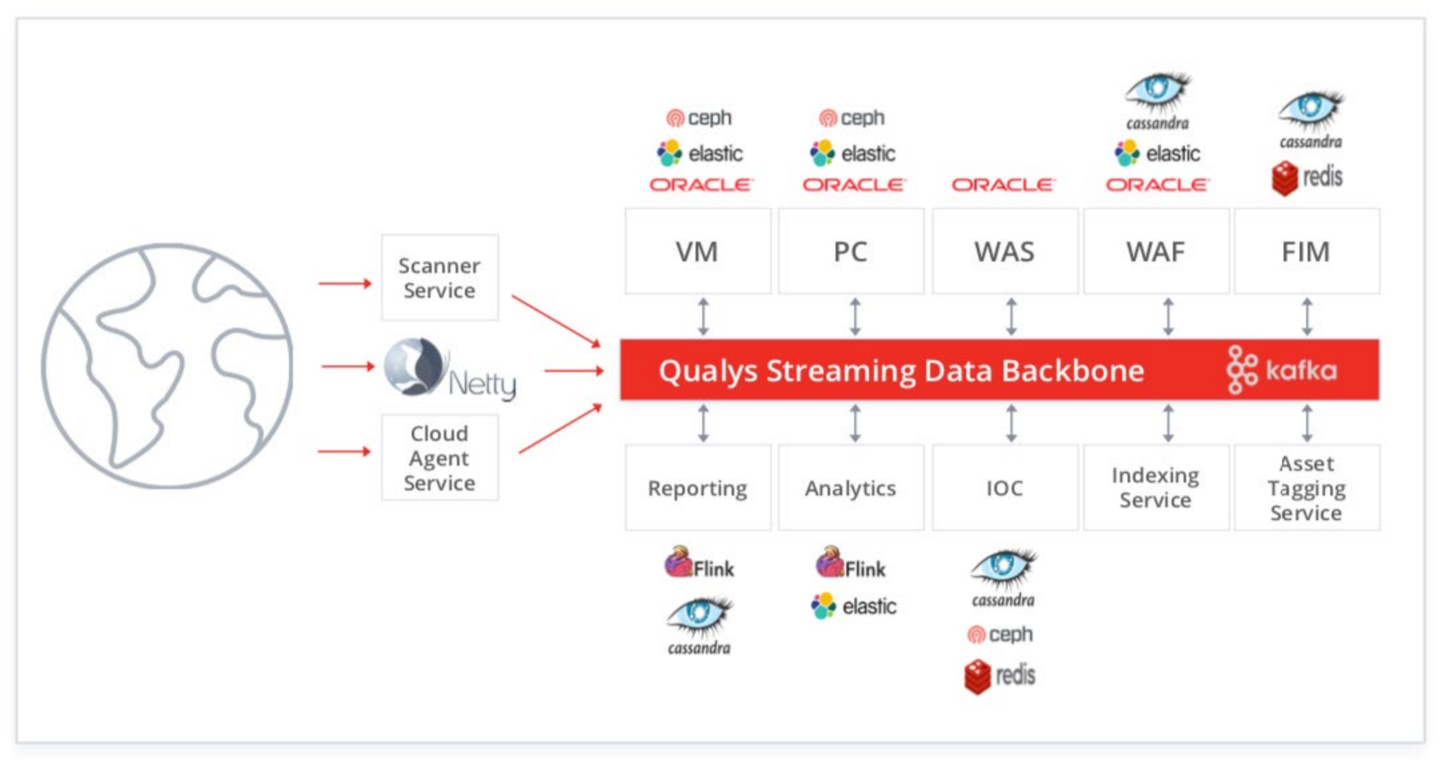
Everything visible. Everything secure.

A single cloud platform for IT, security and compliance across all your global IT assets.

Designed from the Ground Up for the Digital Transformation

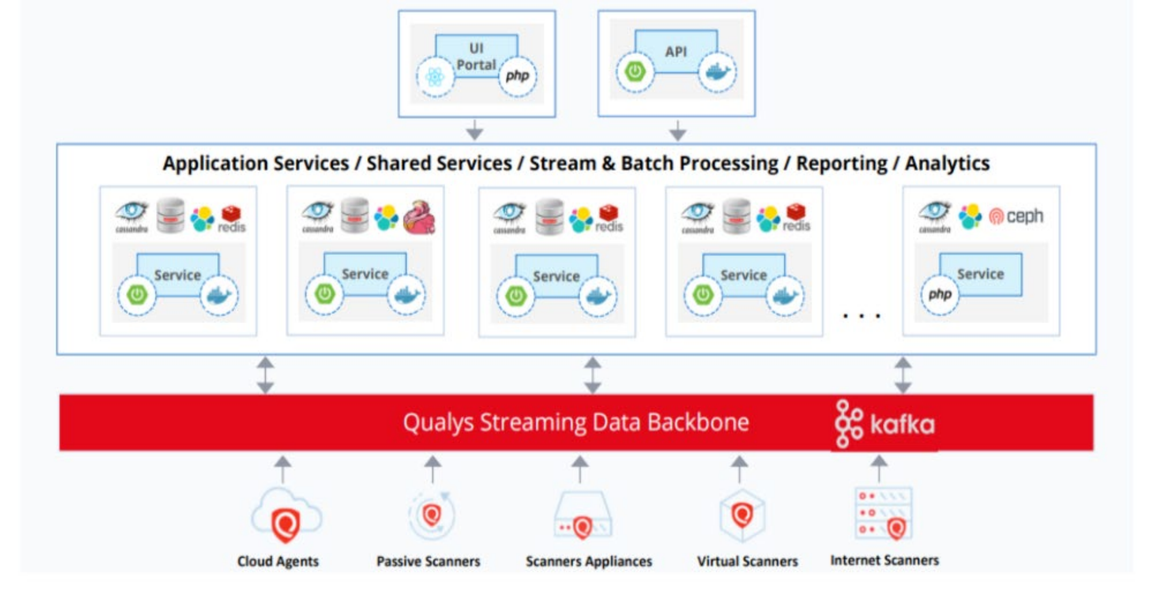
# Extensible Cloud Platform

## Serves as a Scalable and Cost-Effective Distribution Channel



# State-of-the-Art Microservices Architecture

## Sensors, Data Platform, Microservices, DevOps



UI Portal

php

API

Application Services / Shared Services / Stream & Batch Processing / Reporting / Analytics

Qualys Streaming Data Backbone

Cloud Agents

Passive Scanners

Scanners Appliances

Virtual Scanners

Internet Scanners

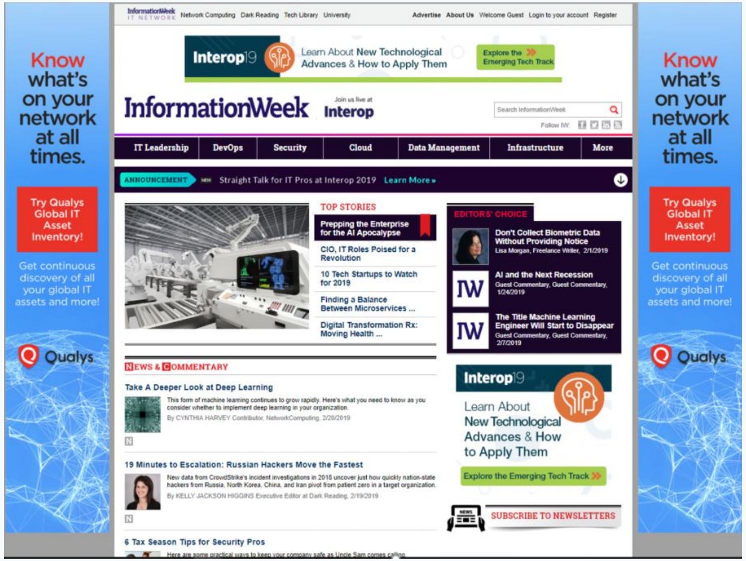
3+ Billion scans/year

3+ Trillion data points indexed on our Elasticsearch clusters

3+ Billion messages per day on our Kafka bus

# Scalable Go-to-market Strategy

## The Platform is the Distribution Channel



Know what's on your network at all times.

Try Qualys Global IT Asset Inventory!

Get continuous discovery of all your global IT assets and more!

Qualys

InformationWeek IT NETWORK Network Computing Dark Reading Tech Library University Advertise About Us Welcome Guest Login to your account Register

Interop19 Learn About New Technological Advances & How to Apply Them Explore the Emerging Tech Track

InformationWeek Join us live at Interop

Search InformationWeek

Follow IW:

IT Leadership | DevOps | Security | Cloud | Data Management | Infrastructure | More

ANNOUNCEMENT NEW Straight Talk for IT Pros at Interop 2019 Learn More »

TOP STORIES

- Prepping the Enterprise for the AI Apocalypse
- CIO, IT Roles Poised for a Revolution
- 10 Tech Startups to Watch for 2019
- Finding a Balance Between Microservices ...
- Digital Transformation Rx: Moving Health ...

EDITORS' CHOICE

- Don't Collect Biometric Data Without Providing Notice  
  Lisa Morgan, Freelance Writer, 2/1/2019
- AI and the Next Recession  
  Guest Commentary, Guest Commentary, 1/24/2019
- The Title Machine Learning Engineer Will Start to Disappear  
  Guest Commentary, Guest Commentary, 2/7/2019

NEWS & COMMENTARY

Take A Deeper Look at Deep Learning

This form of machine learning continues to grow rapidly. Here's what you need to know as you consider whether to implement deep learning in your organization.

By CYNTHIA HARVEY Contributor, NetworkComputing, 2/20/2019

19 Minutes to Escalation: Russian Hackers Move the Fastest

New data from CrowdStrike's incident investigations in 2018 uncover just how quickly nation-state hackers from Russia, North Korea, China, and Iran pivot from patient zero in a target organization.

By KELLY JACKSON HIGGINS Executive Editor at Dark Reading, 2/19/2019

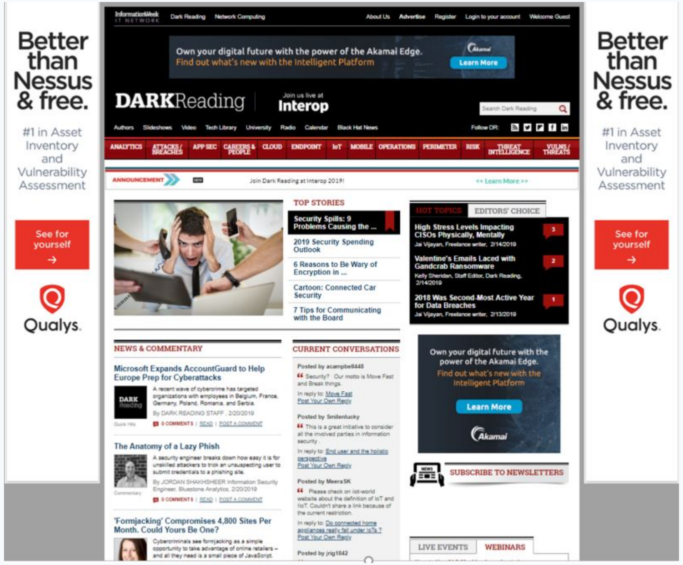
6 Tax Season Tips for Security Pros

Here are some practical ways to keep your company safe as Uncle Sam comes calling.

Interop19 Learn About New Technological Advances & How to Apply Them

Explore the Emerging Tech Track

SUBSCRIBE TO NEWSLETTERS



Better than Nessus & free.

#1 in Asset Inventory and Vulnerability Assessment

See for yourself →

Qualys.

InformationWeek IT NETWORK Dark Reading Network Computing About Us Advertise Register Login to your account Welcome Guest

Own your digital future with the power of the Akamai Edge. Find out what's new with the Intelligent Platform Akamai Learn More

DARKReading Join us live at Interop

Search Dark Reading

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News Follow DR:

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERATIONS | PERIMETER | RISK | THREAT INTELLIGENCE | VULNS / THREATS

ANNOUNCEMENT NEW Join Dark Reading at Interop 2019! << Learn More >>

TOP STORIES

- Security Spills: 9 Problems Causing the ...
- 2019 Security Spending Outlook
- 6 Reasons to Be Wary of Encryption in ...
- Cartoon: Connected Car Security
- 7 Tips for Communicating with the Board

HOT TOPICS EDITORS' CHOICE

- High Stress Levels Impacting CISOs Physically, Mentally 3  
  Jai Vijayan, Freelance writer, 2/14/2019
- Valentine's Emails Laced with Gandcrab Ransomware 2  
  Kelly Sheridan, Staff Editor, Dark Reading, 2/14/2019
- 2018 Was Second-Most Active Year for Data Breaches 1  
  Jai Vijayan, Freelance writer, 2/13/2019

NEWS & COMMENTARY

Microsoft Expands AccountGuard to Help Europe Prep for Cyberattacks

A recent wave of cybercrime has targeted organizations with employees in Belgium, France, Germany, Poland, Romania, and Serbia.

By DARK READING STAFF, 2/20/2019

Quick Hits 0 COMMENTS | READ | POST A COMMENT

The Anatomy of a Lazy Phish

A security engineer breaks down how easy it is for unskilled attackers to trick an unsuspecting user to submit credentials to a phishing site.

By JORDAN SHAKHSHEER Information Security Engineer, Bluestone Analytics, 2/20/2019

Commentary 0 COMMENTS | READ | POST A COMMENT

'Formjacking' Compromises 4,800 Sites Per Month. Could Yours Be One?

Cybercriminals see formjacking as a simple opportunity to take advantage of online retailers – and all they need is a small piece of JavaScript.

CURRENT CONVERSATIONS

Posted by acampbell448

Security? Our motto is Move Fast and Break things.

In reply to: Move Fast

Post Your Own Reply

Posted by Smilenlucky

This is a great initiative to consider all the involved parties in information security .

In reply to: End user and the holistic perspective

Post Your Own Reply

Posted by MeeraSK

Please check on iiot-world website about the definition of IoT and IIoT. Couldn't share a link because of the current restriction.

In reply to: Do connected home appliances really fall under IoTs ?

Post Your Own Reply

Posted by jrig1842

Own your digital future with the power of the Akamai Edge. Find out what's new with the Intelligent Platform Learn More Akamai

SUBSCRIBE TO NEWSLETTERS

LIVE EVENTS WEBINARS

Try & Buy Model - Fully Automated Lead-Gen Campaigns

# Ubiquity Play

## Launch at Black Hat of our Groundbreaking Global IT Discovery and Asset Inventory Apps

Our Global IT Asset Discovery and Inventory are two of the many apps we have running native on our Cloud Platform.

It will come in two versions: free and paid.

**What makes it unique:**

- Our Cloud Agents span across on-premises, endpoints, cloud(s), containers and mobile.
- The Asset Inventory App automatically normalizes and categorizes assets.
- Natively integrated with the Discovery App (passive scanning) provides a continuous view of “known and unknown assets” connecting to corporate networks giving **100%** visibility.

Qualys.

# Highly Leveraged Business Model

We currently have **almost 24 million** Cloud Agents installed across on-premises, endpoints, cloud(s), containers and mobile.

Our lightweight Cloud Agents (3Mb) currently spawn **seven services** with more to come.

Once the Cloud Agent is deployed, all the additional services are already available (nothing to install or maintain) and customers can **automatically provision** new services themselves.

As organizations download our Cloud Agent for implementing global IT asset inventory, **we make it frictionless to subscribe** to our paid apps because no additional infrastructure is required.

# Ubiquity Play

## Early Results – Early Success

**1307 SIGN-UPS**
**IN 3 DAYS**

1159 SIGN-UPS
New Users

148 SIGN-UPS
Existing Users

# 2020 New Services and Platform Expansion

Launch of Global IT Asset Inventory, Passive Scanning and IOC 2.0 at Black Hat

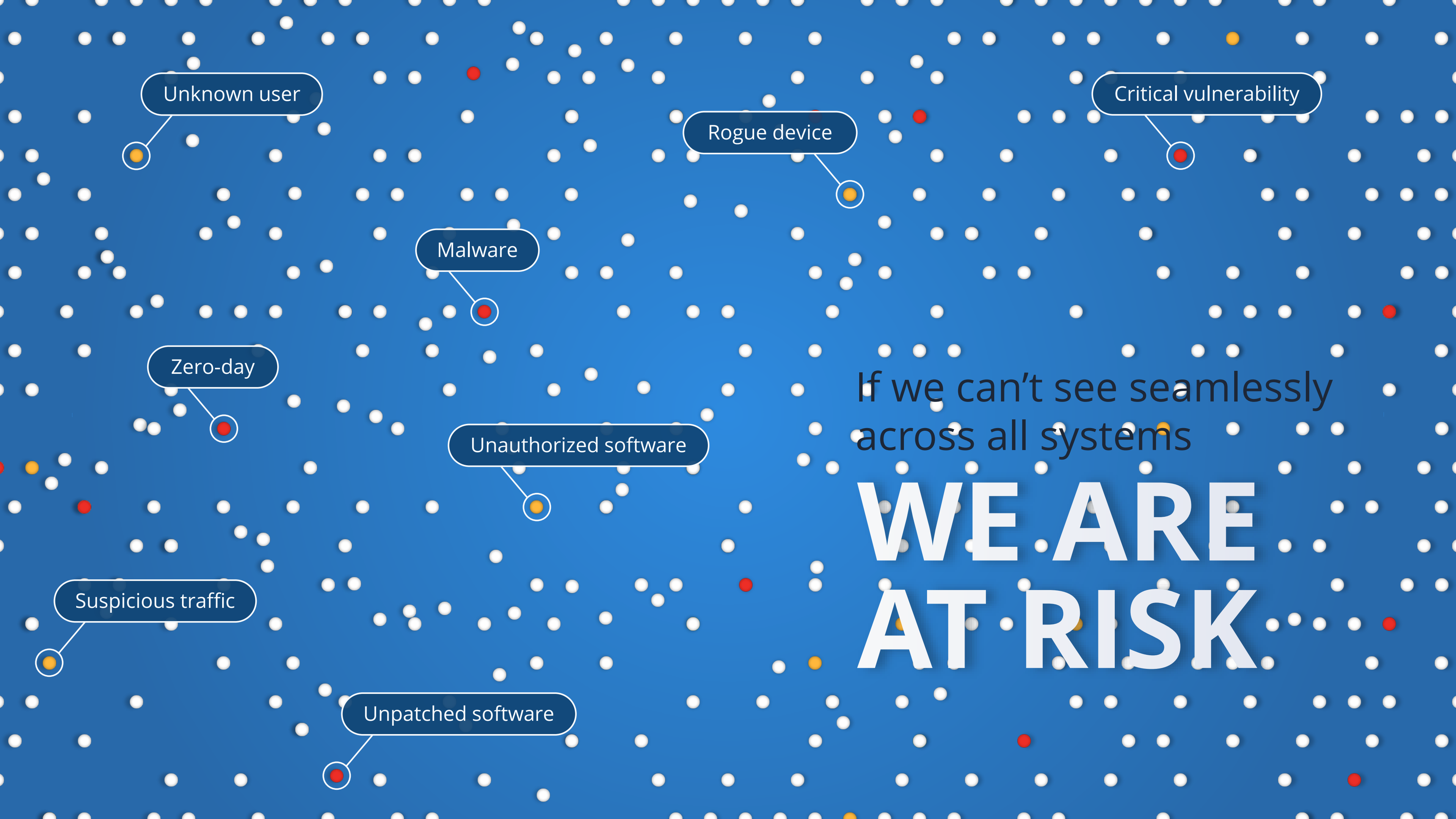
Uniquely positioned to **blend** Data Lake, SIEMs, EDR and **EPP on the top of our Cloud Platform** - Q1/Q2 2020 (Beta)

Qualys.

# A New Prescription for Cyber Security

## Qualys Global IT Asset Inventory

**Black Hat Conference**
August 2019



Unknown user

Critical vulnerability

Rogue device

Malware

Zero-day

Unauthorized software

Suspicious traffic

Unpatched software

If we can’t see seamlessly across all systems

# WE ARE AT RISK

We made a promise to
the world of security...

# MAKE EVERYTHING VISIBLE

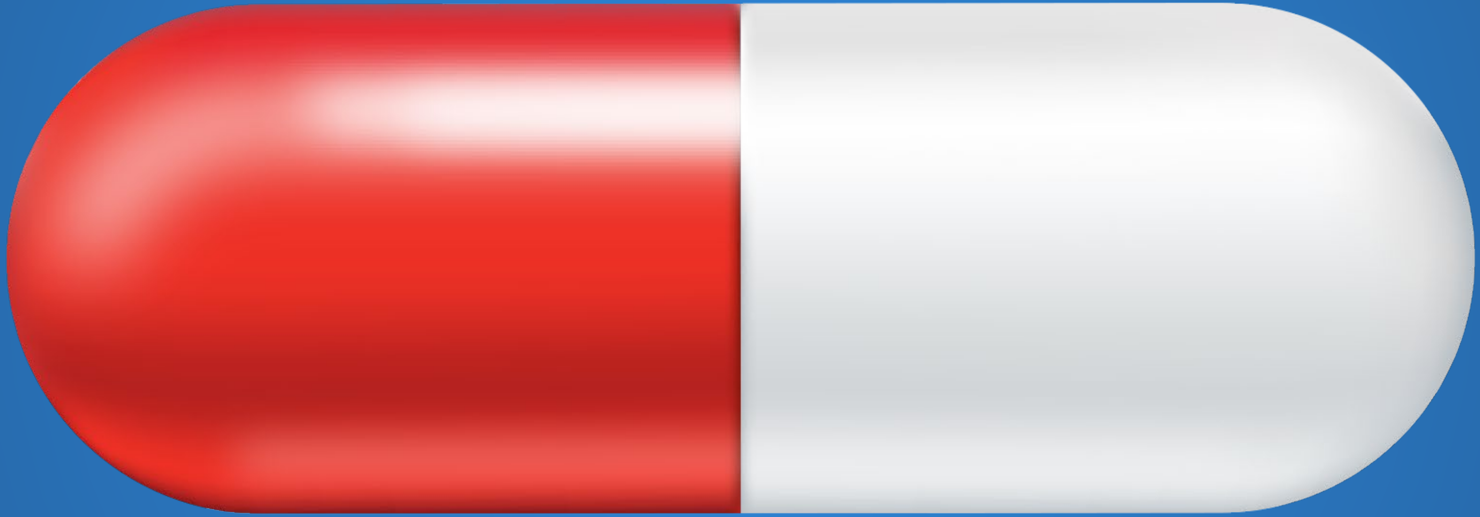
We made a promise to
the world of security...

# MAKE EVERYTHING
# VISIBLE

Today’s dynamic environment calls for a

# NEW PRESCRIPTION

IT’S NOT FOR EVERYONE.



# Side Effects May Include

Knowing what’s on your global hybrid-IT environment

Providing a single source of truth for all your teams

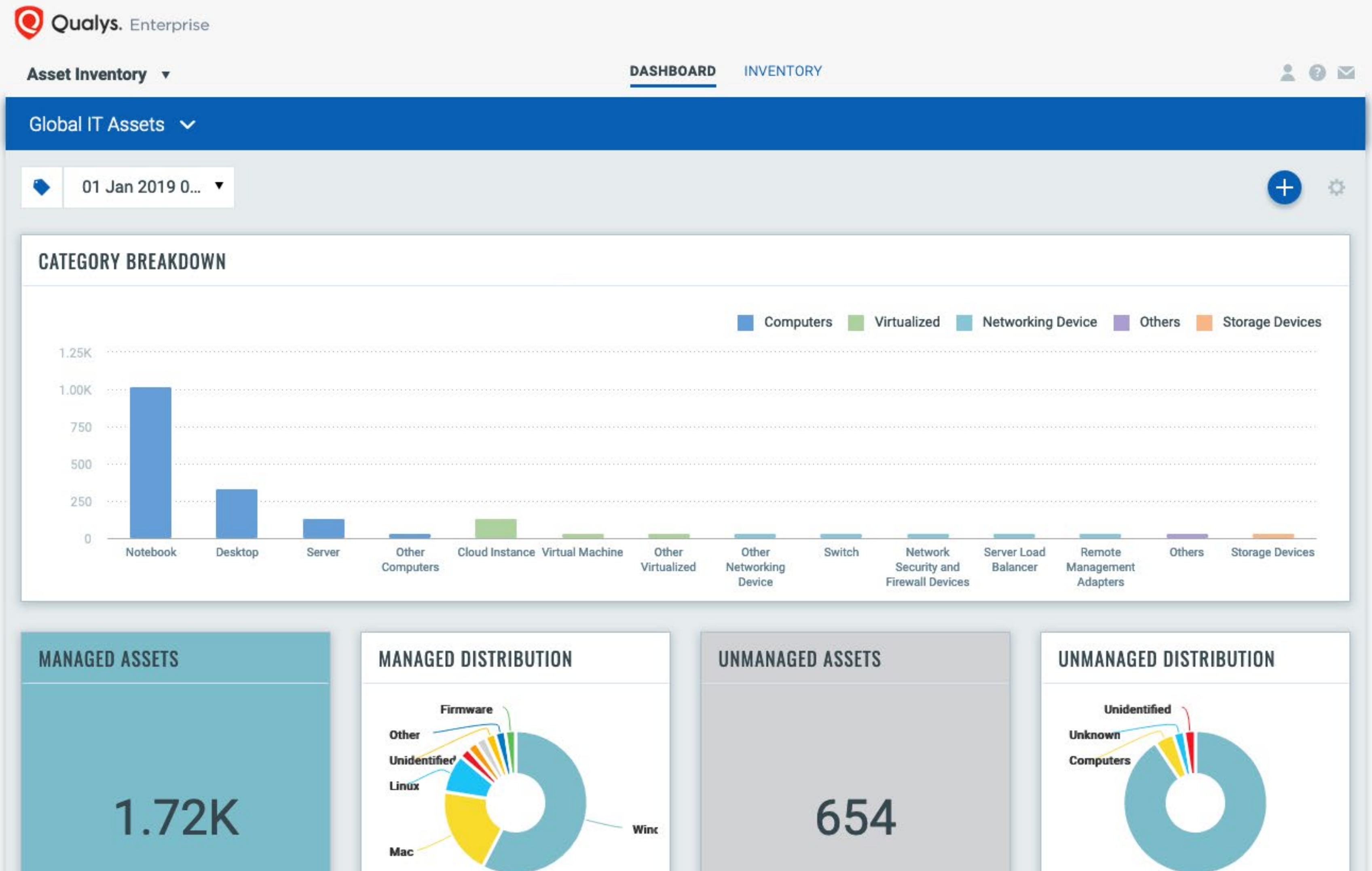
Better decision making using enriched data

Improving your security and compliance posture

Getting that promotion you always wanted

# DEMO

Global IT Asset Inventory



CATEGORY BREAKDOWN

MANAGED ASSETS

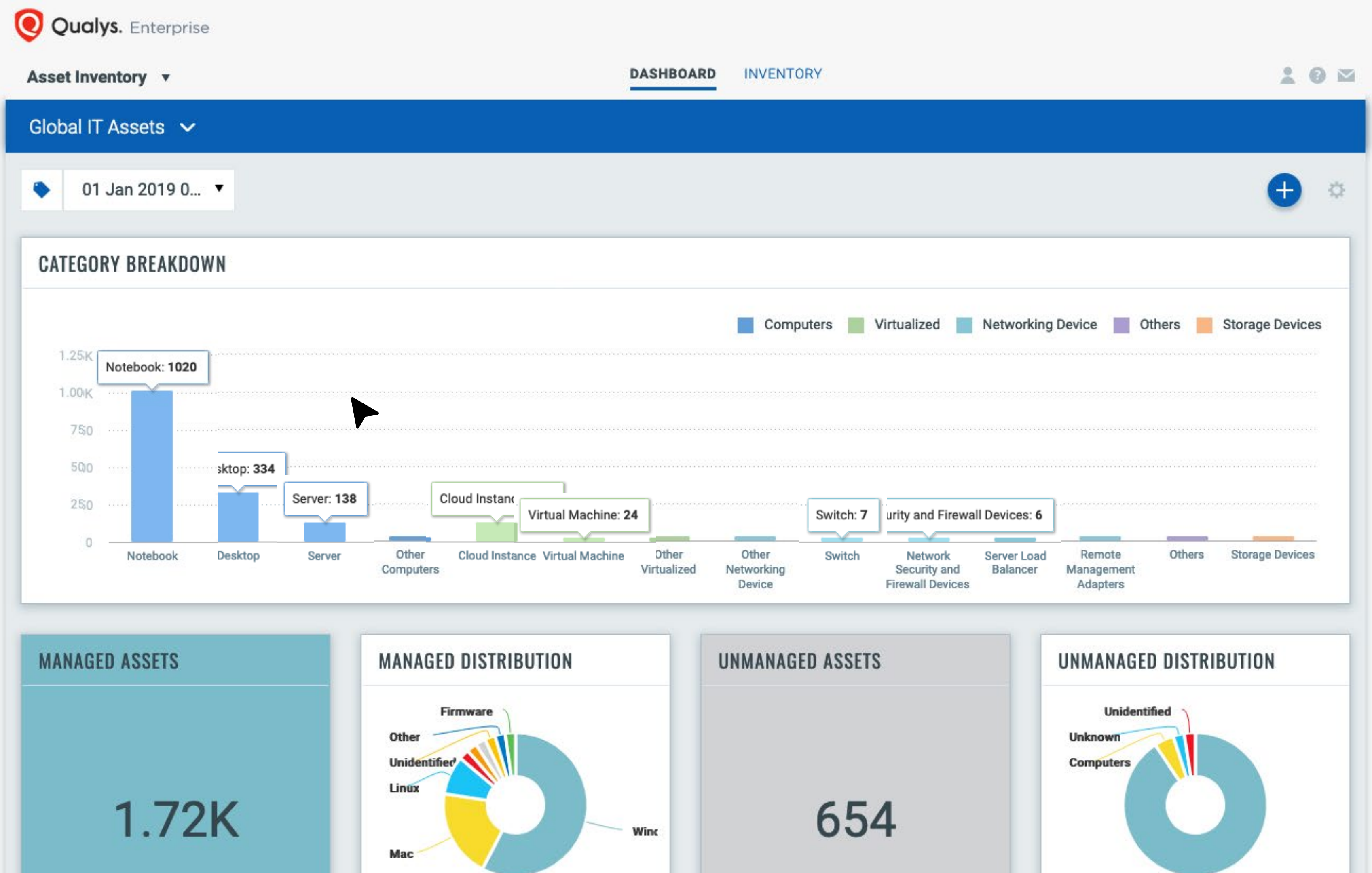
1.72K

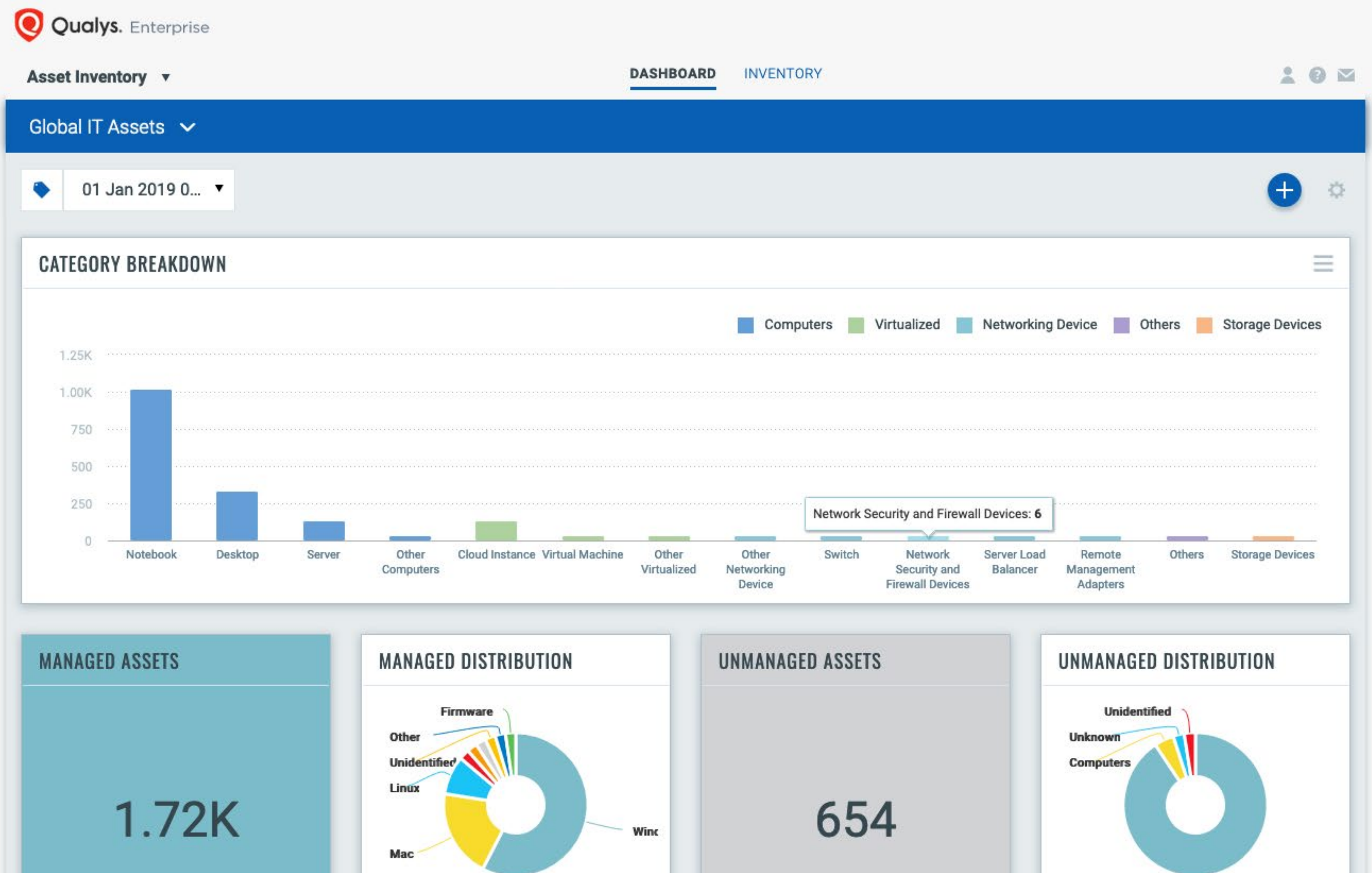
MANAGED DISTRIBUTION

UNMANAGED ASSETS

654

UNMANAGED DISTRIBUTION


Qualys. Enterprise
Asset Inventory ▼
DASHBOARD
INVENTORY
Global IT Assets
01 Jan 2019 0... ▼
CATEGORY BREAKDOWN
Computers
Virtualized
Networking Device
Others
Storage Devices
1.25K
1.00K
750
500
250
0
Notebook: 1020
sktop: 334
Server: 138
Cloud Instanc
Virtual Machine: 24
Switch: 7
urity and Firewall Devices: 6
Notebook
Desktop
Server
Other Computers
Cloud Instance
Virtual Machine
Other Virtualized
Other Networking Device
Switch
Network Security and Firewall Devices
Server Load Balancer
Remote Management Adapters
Others
Storage Devices
MANAGED ASSETS
1.72K
MANAGED DISTRIBUTION
Firmware
Other
Unidentified
Linux
Mac
Winc
UNMANAGED ASSETS
654
UNMANAGED DISTRIBUTION
Unidentified
Unknown
Computers



CATEGORY BREAKDOWN

Network Security and Firewall Devices: **6**

MANAGED ASSETS

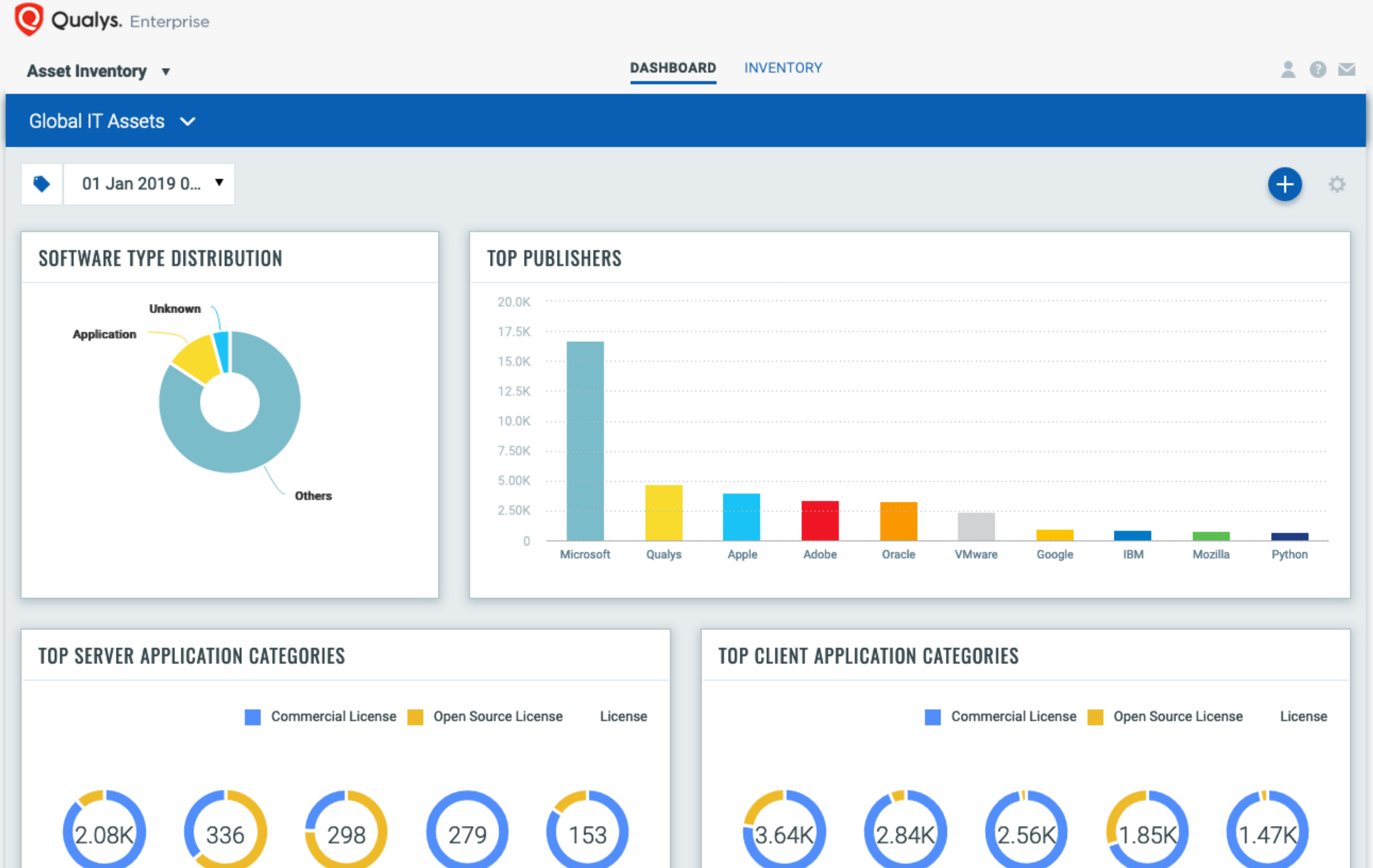
1.72K

MANAGED DISTRIBUTION

UNMANAGED ASSETS

654

UNMANAGED DISTRIBUTION



Qualys. Enterprise

Asset Inventory ▾

DASHBOARD INVENTORY

Global IT Assets

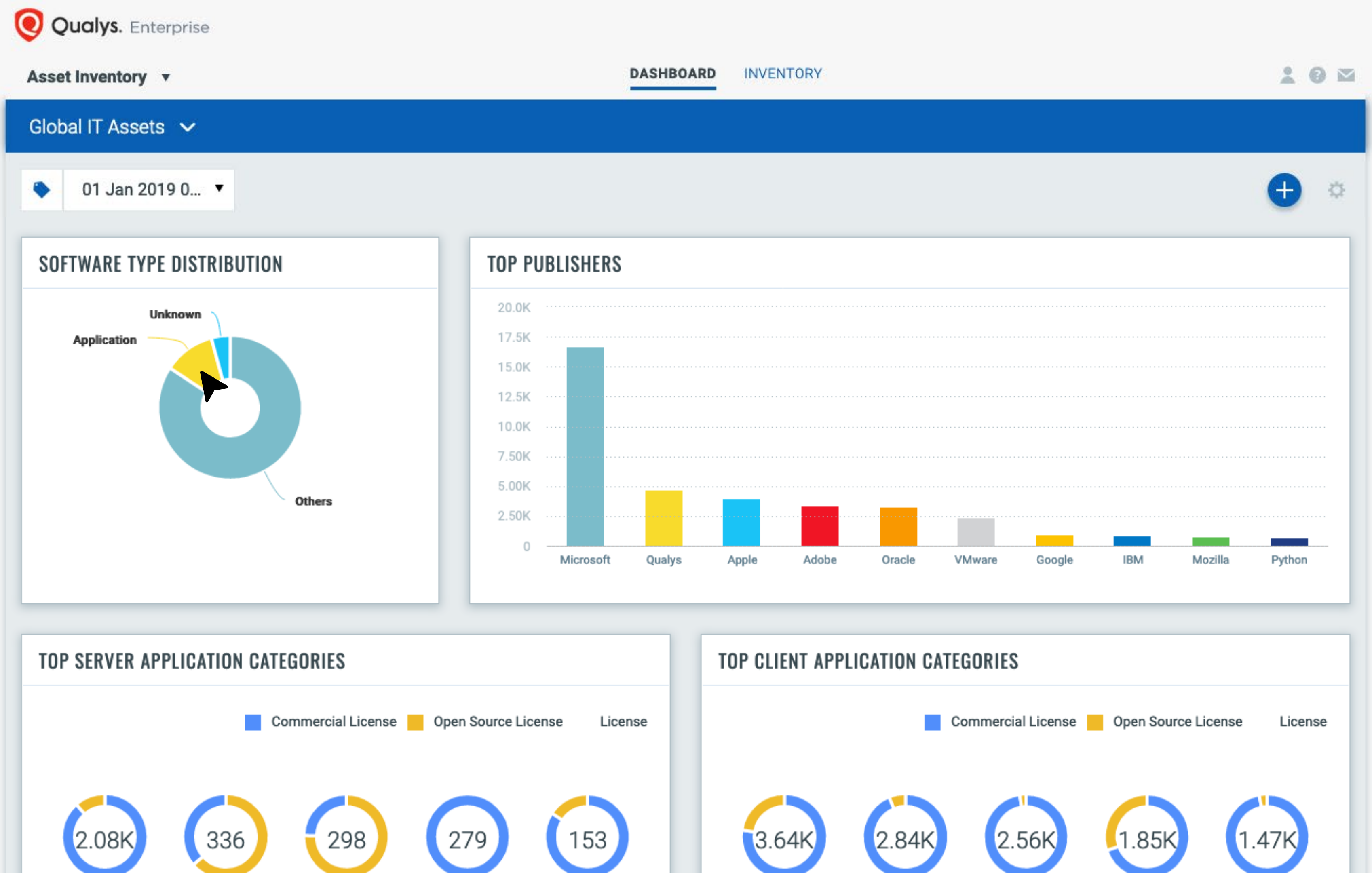
01 Jan 2019 0... ▾

SOFTWARE TYPE DISTRIBUTION

TOP PUBLISHERS

TOP SERVER APPLICATION CATEGORIES

TOP CLIENT APPLICATION CATEGORIES

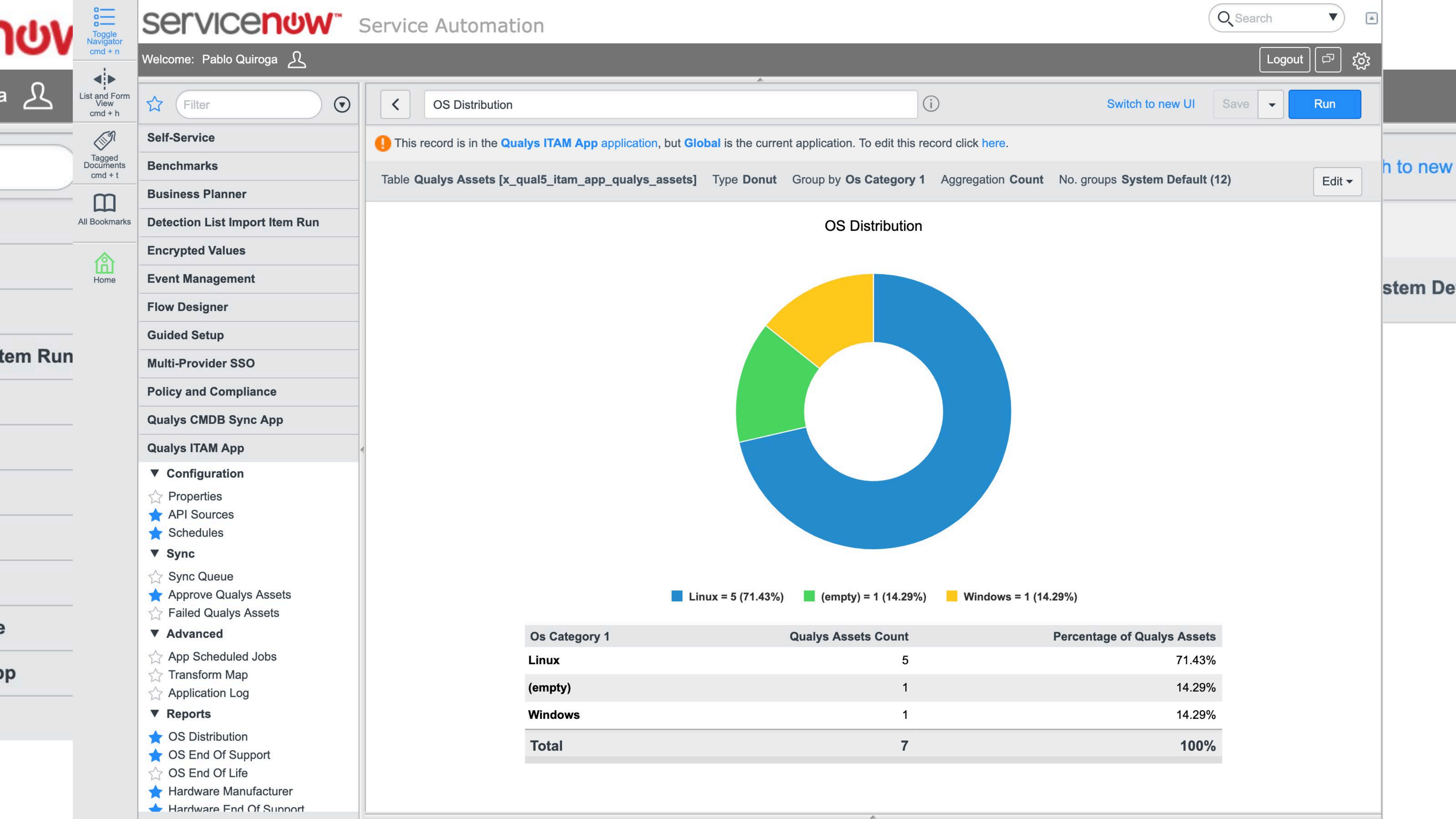


SOFTWARE TYPE DISTRIBUTION

TOP PUBLISHERS

TOP SERVER APPLICATION CATEGORIES

TOP CLIENT APPLICATION CATEGORIES

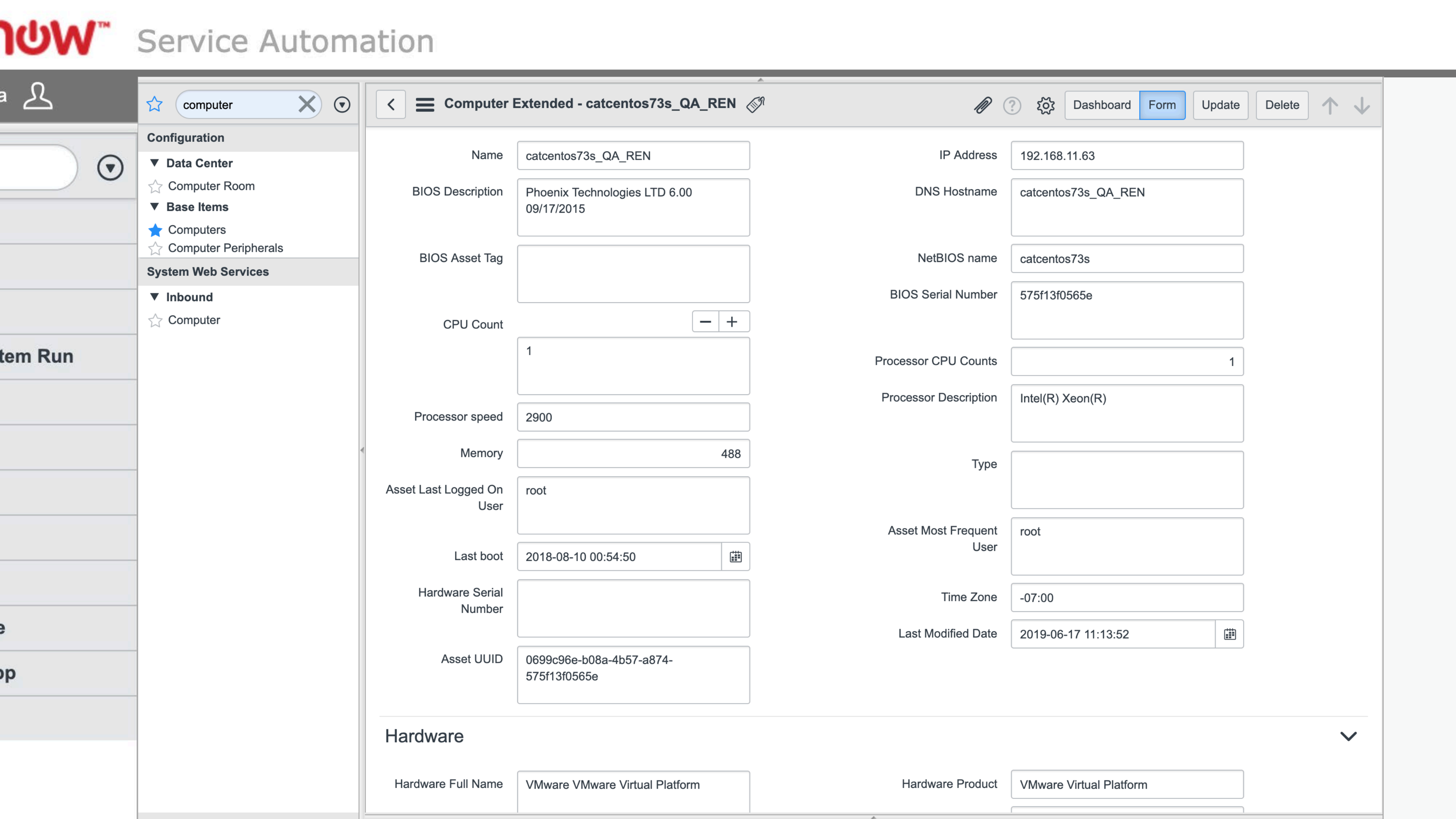


This record is in the **Qualys ITAM App** application, but **Global** is the current application. To edit this record click here.

Table **Qualys Assets [x_qual5_itam_app_qualys_assets]** Type **Donut** Group by **Os Category 1** Aggregation **Count** No. groups **System Default (12)**

OS Distribution

| Os Category 1 | Qualys Assets Count | Percentage of Qualys Assets |
|---|---|---|
| Linux | 5 | 71.43% |
| (empty) | 1 | 14.29% |
| Windows | 1 | 14.29% |
| Total | 7 | 100% |



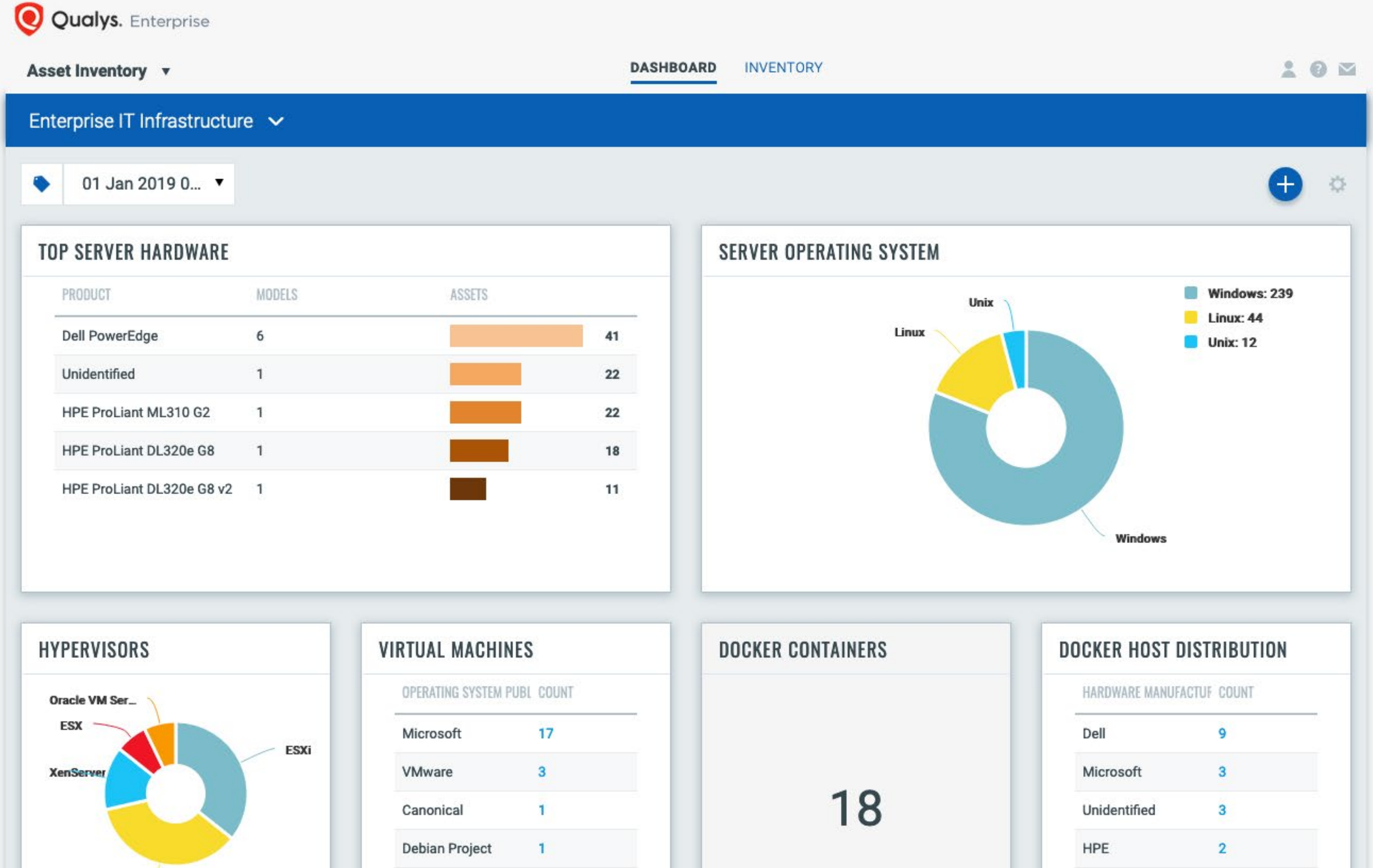
Computer Extended - catcentos73s_QA_REN

| | | | |
|---|---|---|---|
| Name | catcentos73s_QA_REN | IP Address | 192.168.11.63 |
| BIOS Description | Phoenix Technologies LTD 6.00 09/17/2015 | DNS Hostname | catcentos73s_QA_REN |
| BIOS Asset Tag | | NetBIOS name | catcentos73s |
| | | BIOS Serial Number | 575f13f0565e |
| CPU Count | 1 | Processor CPU Counts | 1 |
| | | Processor Description | Intel(R) Xeon(R) |
| Processor speed | 2900 | | |
| Memory | 488 | Type | |
| Asset Last Logged On User | root | Asset Most Frequent User | root |
| Last boot | 2018-08-10 00:54:50 | Time Zone | -07:00 |
| Hardware Serial Number | | Last Modified Date | 2019-06-17 11:13:52 |
| Asset UUID | 0699c96e-b08a-4b57-a874-575f13f0565e | | |

Hardware

| | | | |
|---|---|---|---|
| Hardware Full Name | VMware VMware Virtual Platform | Hardware Product | VMware Virtual Platform |

# Obtain in-depth visibility of your assets



TOP SERVER HARDWARE

| PRODUCT | MODELS | ASSETS |
|---|---|---|
| Dell PowerEdge | 6 | 41 |
| Unidentified | 1 | 22 |
| HPE ProLiant ML310 G2 | 1 | 22 |
| HPE ProLiant DL320e G8 | 1 | 18 |
| HPE ProLiant DL320e G8 v2 | 1 | 11 |

SERVER OPERATING SYSTEM

HYPERVISORS

VIRTUAL MACHINES

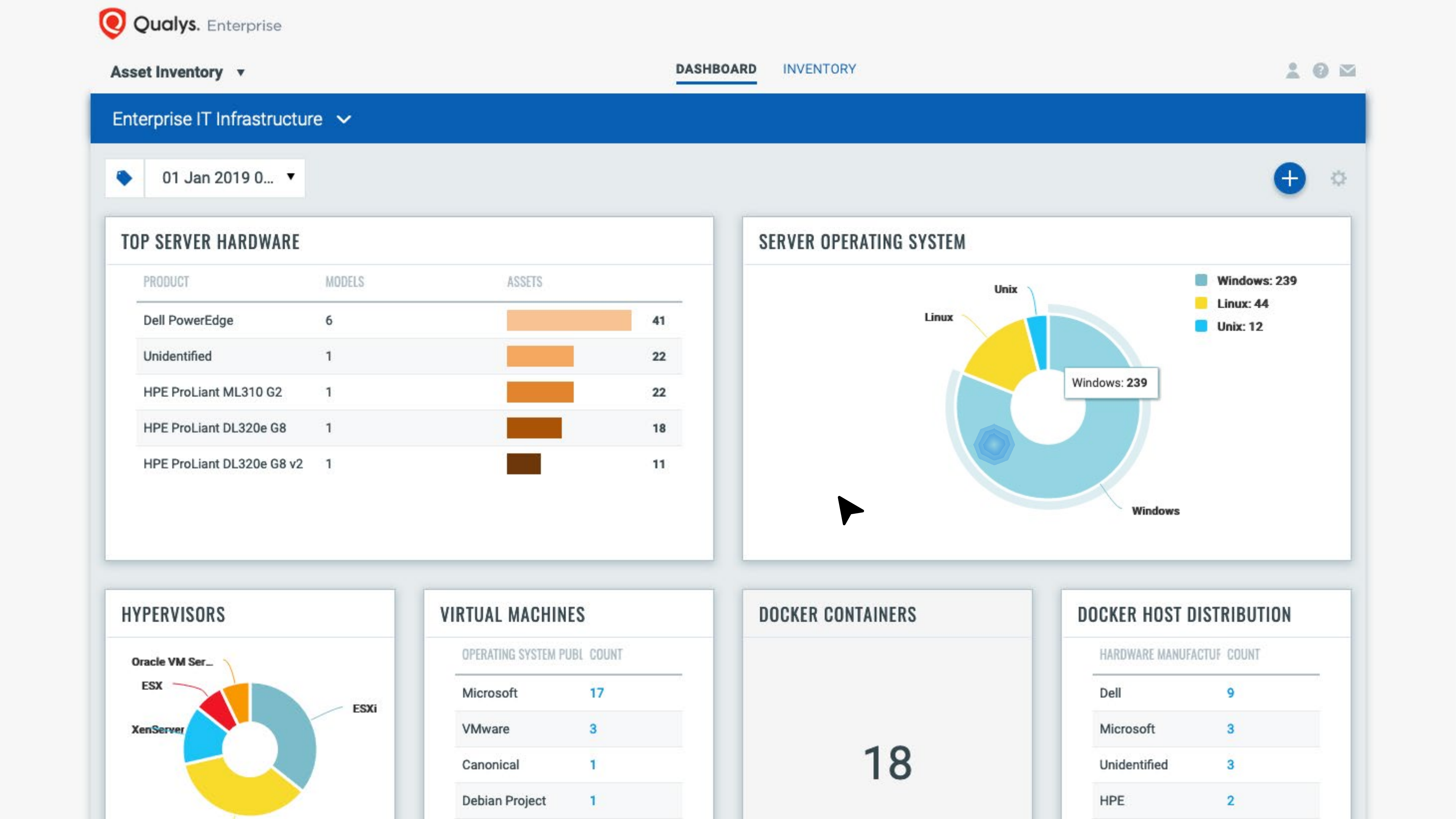
| OPERATING SYSTEM PUBL | COUNT |
|---|---|
| Microsoft | 17 |
| VMware | 3 |
| Canonical | 1 |
| Debian Project | 1 |

DOCKER CONTAINERS

18

DOCKER HOST DISTRIBUTION

| HARDWARE MANUFACTUF | COUNT |
|---|---|
| Dell | 9 |
| Microsoft | 3 |
| Unidentified | 3 |
| HPE | 2 |



Qualys. Enterprise

Asset Inventory ▾

DASHBOARD INVENTORY

Enterprise IT Infrastructure

01 Jan 2019 0... ▾

## TOP SERVER HARDWARE

| PRODUCT | MODELS | ASSETS |
|---|---|---|
| Dell PowerEdge | 6 | 41 |
| Unidentified | 1 | 22 |
| HPE ProLiant ML310 G2 | 1 | 22 |
| HPE ProLiant DL320e G8 | 1 | 18 |
| HPE ProLiant DL320e G8 v2 | 1 | 11 |

## SERVER OPERATING SYSTEM

## HYPERVISORS

## VIRTUAL MACHINES

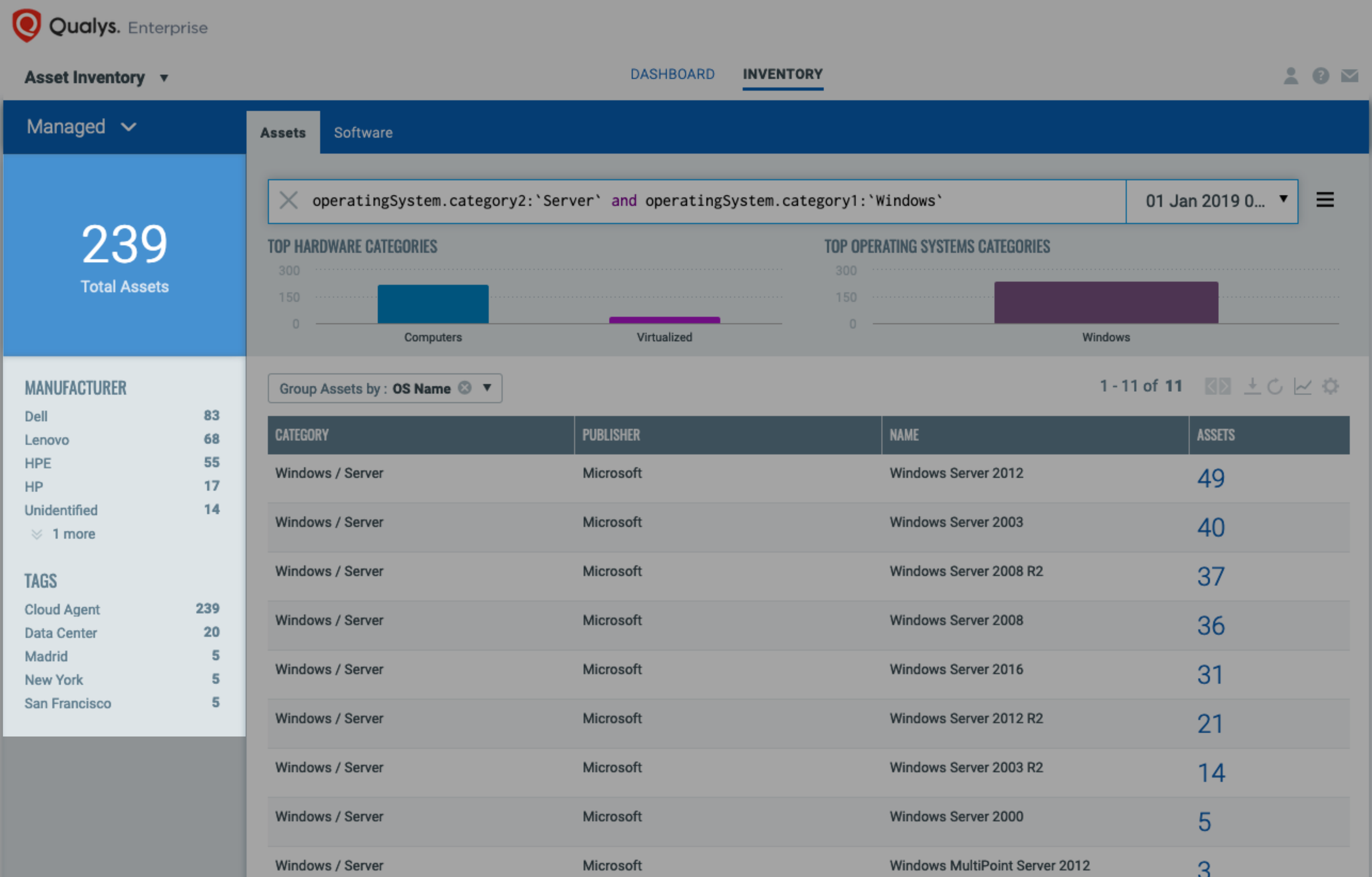
| OPERATING SYSTEM PUBL | COUNT |
|---|---|
| Microsoft | 17 |
| VMware | 3 |
| Canonical | 1 |
| Debian Project | 1 |

## DOCKER CONTAINERS

18

## DOCKER HOST DISTRIBUTION

| HARDWARE MANUFACTUF | COUNT |
|---|---|
| Dell | 9 |
| Microsoft | 3 |
| Unidentified | 3 |
| HPE | 2 |



```
operatingSystem.category2:`Server` and operatingSystem.category1:`Windows`
```

239
Total Assets

MANUFACTURER

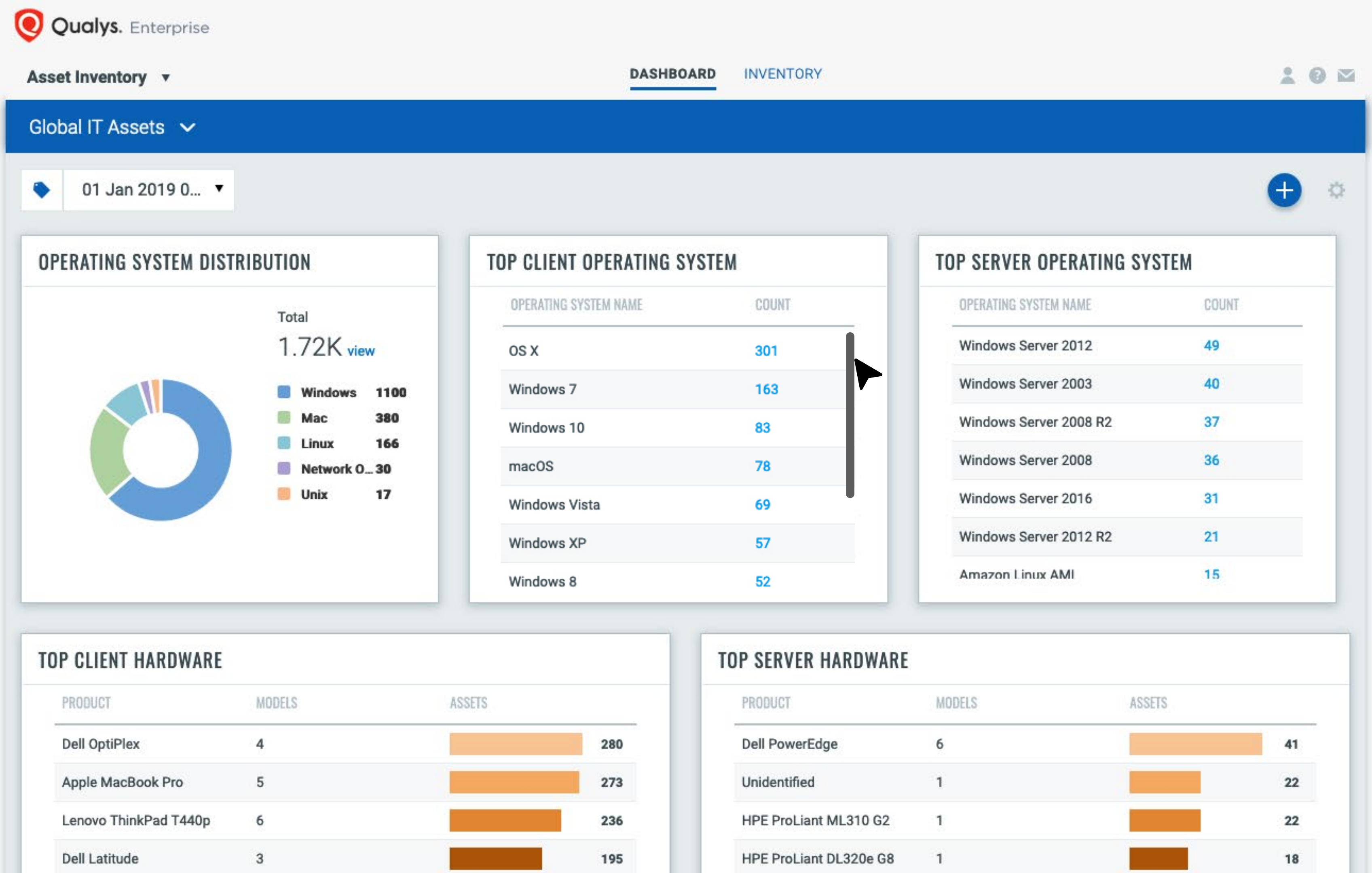
| | |
|---|---|
| Dell | 83 |
| Lenovo | 68 |
| HPE | 55 |
| HP | 17 |
| Unidentified | 14 |
| 1 more | |

TAGS

| | |
|---|---|
| Cloud Agent | 239 |
| Data Center | 20 |
| Madrid | 5 |
| New York | 5 |
| San Francisco | 5 |

Group Assets by : OS Name

| CATEGORY | PUBLISHER | NAME | ASSETS |
|---|---|---|---|
| Windows / Server | Microsoft | Windows Server 2012 | 49 |
| Windows / Server | Microsoft | Windows Server 2003 | 40 |
| Windows / Server | Microsoft | Windows Server 2008 R2 | 37 |
| Windows / Server | Microsoft | Windows Server 2008 | 36 |
| Windows / Server | Microsoft | Windows Server 2016 | 31 |
| Windows / Server | Microsoft | Windows Server 2012 R2 | 21 |
| Windows / Server | Microsoft | Windows Server 2003 R2 | 14 |
| Windows / Server | Microsoft | Windows Server 2000 | 5 |
| Windows / Server | Microsoft | Windows MultiPoint Server 2012 | 3 |



Qualys. Enterprise

Asset Inventory ▼ | DASHBOARD | INVENTORY

Global IT Assets

01 Jan 2019 0... ▼

## OPERATING SYSTEM DISTRIBUTION

Total
1.72K view

| | | |
|---|---|---|
| 🟦 | Windows | 1100 |
| 🟩 | Mac | 380 |
| 🟦 | Linux | 166 |
| 🟪 | Network O... | 30 |
| 🟧 | Unix | 17 |

## TOP CLIENT OPERATING SYSTEM

| OPERATING SYSTEM NAME | COUNT |
|---|---|
| OS X | 301 |
| Windows 7 | 163 |
| Windows 10 | 83 |
| macOS | 78 |
| Windows Vista | 69 |
| Windows XP | 57 |
| Windows 8 | 52 |

## TOP SERVER OPERATING SYSTEM

| OPERATING SYSTEM NAME | COUNT |
|---|---|
| Windows Server 2012 | 49 |
| Windows Server 2003 | 40 |
| Windows Server 2008 R2 | 37 |
| Windows Server 2008 | 36 |
| Windows Server 2016 | 31 |
| Windows Server 2012 R2 | 21 |
| Amazon Linux AMI | 15 |

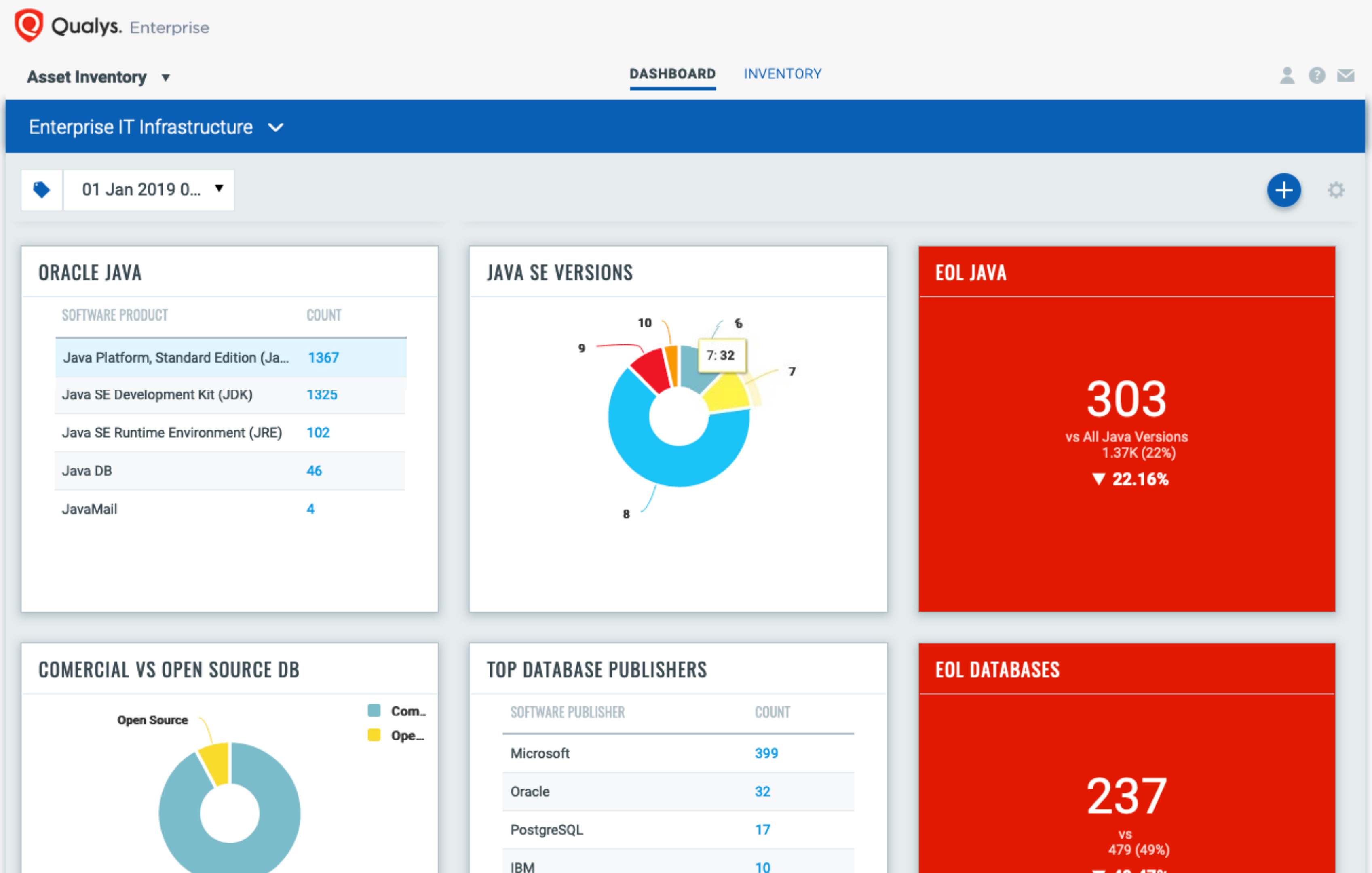
## TOP CLIENT HARDWARE

| PRODUCT | MODELS | ASSETS |
|---|---|---|
| Dell OptiPlex | 4 | 280 |
| Apple MacBook Pro | 5 | 273 |
| Lenovo ThinkPad T440p | 6 | 236 |
| Dell Latitude | 3 | 195 |

## TOP SERVER HARDWARE

| PRODUCT | MODELS | ASSETS |
|---|---|---|
| Dell PowerEdge | 6 | 41 |
| Unidentified | 1 | 22 |
| HPE ProLiant ML310 G2 | 1 | 22 |
| HPE ProLiant DL320e G8 | 1 | 18 |

# Solve important business problems



Enterprise IT Infrastructure

01 Jan 2019 0... ▼

## ORACLE JAVA

| SOFTWARE PRODUCT | COUNT |
|---|---|
| Java Platform, Standard Edition (Ja... | 1367 |
| Java SE Development Kit (JDK) | 1325 |
| Java SE Runtime Environment (JRE) | 102 |
| Java DB | 46 |
| JavaMail | 4 |

## JAVA SE VERSIONS

## EOL JAVA

303

vs All Java Versions
1.37K (22%)

▼ 22.16%

## COMERCIAL VS OPEN SOURCE DB

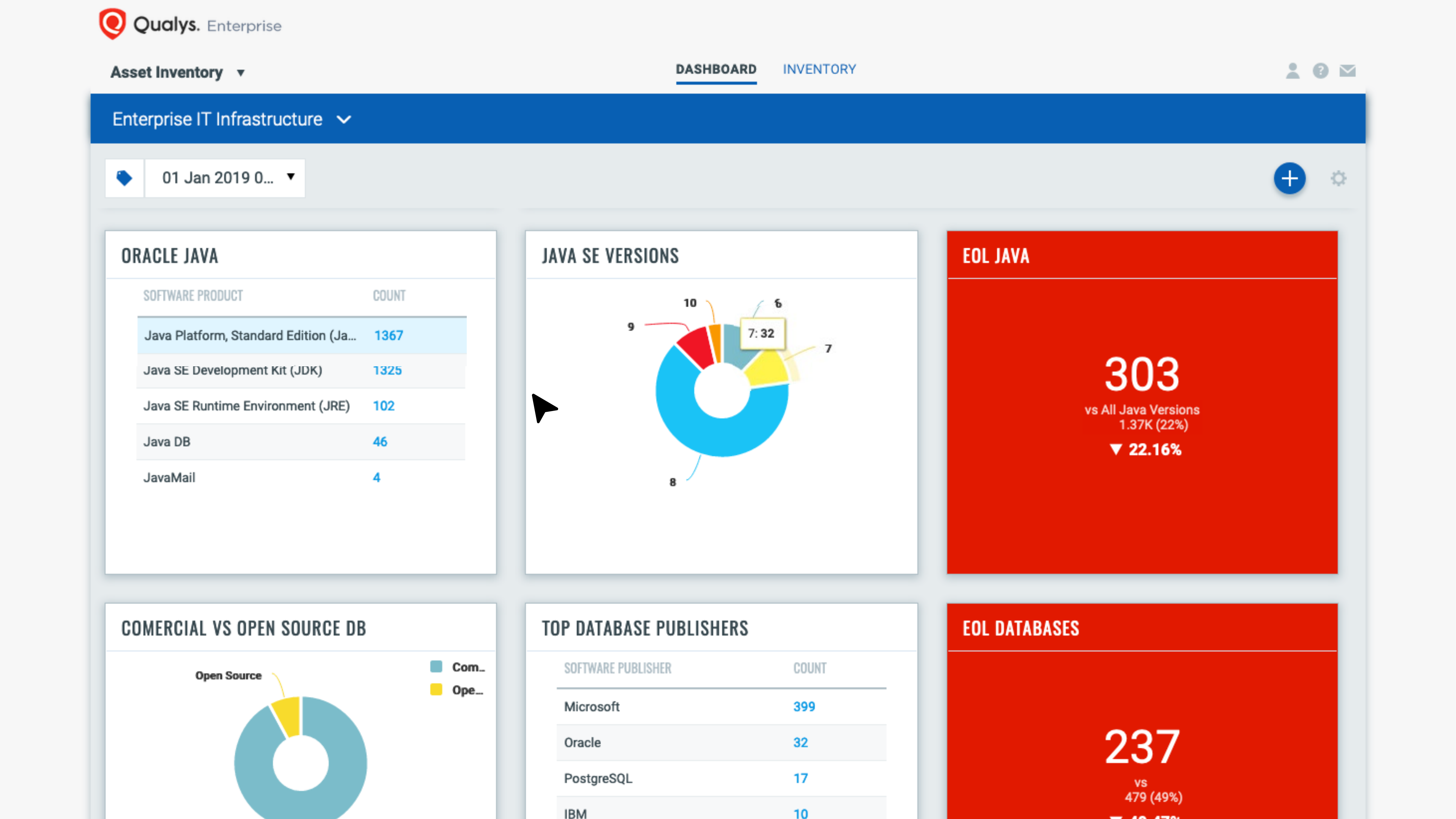
## TOP DATABASE PUBLISHERS

| SOFTWARE PUBLISHER | COUNT |
|---|---|
| Microsoft | 399 |
| Oracle | 32 |
| PostgreSQL | 17 |
| IBM | 10 |

## EOL DATABASES

237

vs
479 (49%)



## ORACLE JAVA

| SOFTWARE PRODUCT | COUNT |
|---|---|
| Java Platform, Standard Edition (Ja... | 1367 |
| Java SE Development Kit (JDK) | 1325 |
| Java SE Runtime Environment (JRE) | 102 |
| Java DB | 46 |
| JavaMail | 4 |

## JAVA SE VERSIONS

## EOL JAVA

303

vs All Java Versions
1.37K (22%)

▼ 22.16%

## COMERCIAL VS OPEN SOURCE DB

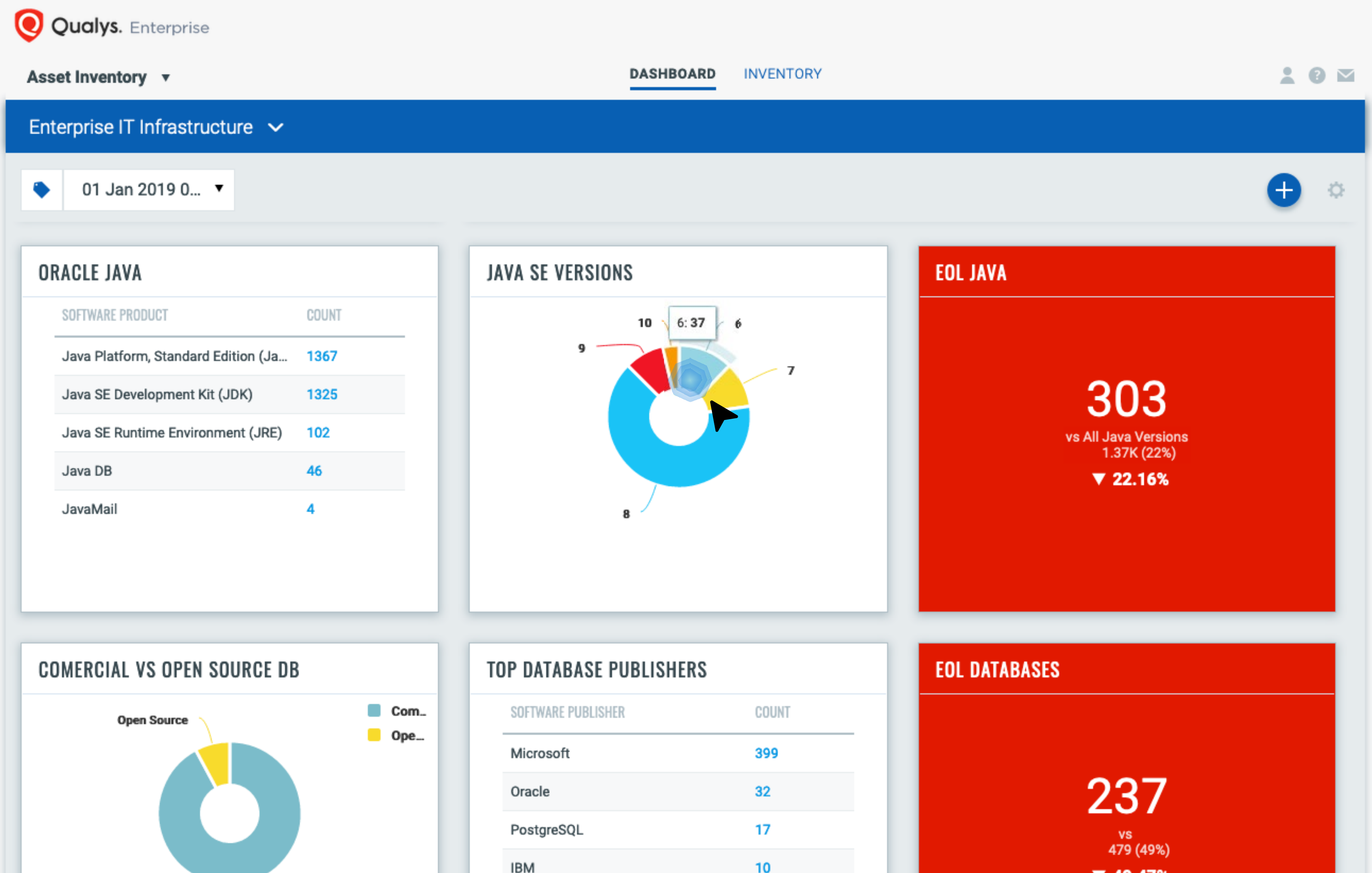
## TOP DATABASE PUBLISHERS

| SOFTWARE PUBLISHER | COUNT |
|---|---|
| Microsoft | 399 |
| Oracle | 32 |
| PostgreSQL | 17 |
| IBM | 10 |

## EOL DATABASES

237

vs
479 (49%)



Qualys. Enterprise

Asset Inventory ▼

DASHBOARD INVENTORY

Enterprise IT Infrastructure

01 Jan 2019 0... ▼

## ORACLE JAVA

| SOFTWARE PRODUCT | COUNT |
|---|---|
| Java Platform, Standard Edition (Ja... | 1367 |
| Java SE Development Kit (JDK) | 1325 |
| Java SE Runtime Environment (JRE) | 102 |
| Java DB | 46 |
| JavaMail | 4 |

## JAVA SE VERSIONS

## EOL JAVA

303

vs All Java Versions
1.37K (22%)

▼ 22.16%

## COMERCIAL VS OPEN SOURCE DB

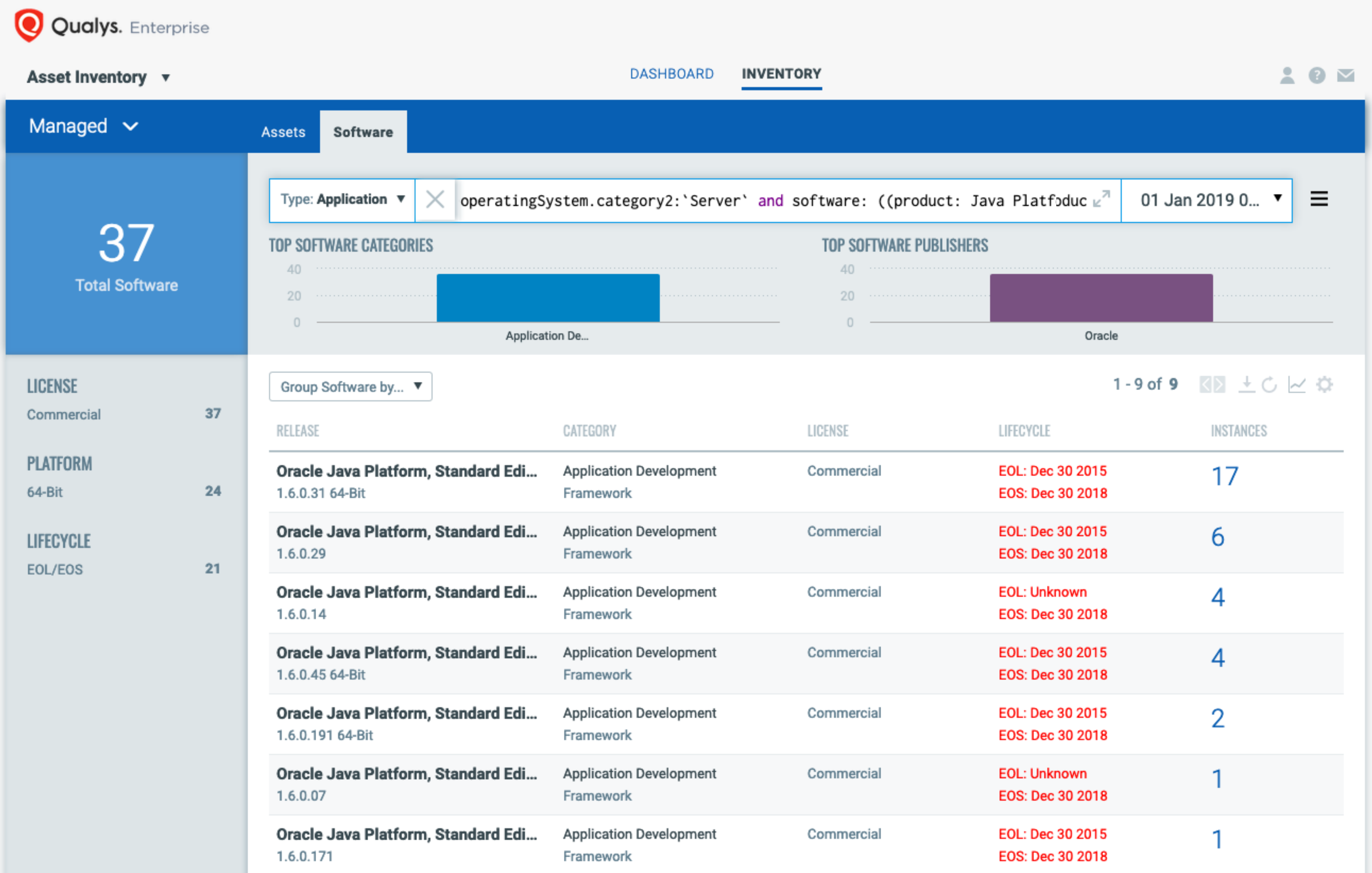
## TOP DATABASE PUBLISHERS

| SOFTWARE PUBLISHER | COUNT |
|---|---|
| Microsoft | 399 |
| Oracle | 32 |
| PostgreSQL | 17 |
| IBM | 10 |

## EOL DATABASES

237

vs
479 (49%)



Type: Application ▼

operatingSystem.category2:`Server` and software: ((product: Java Platfɔduc

01 Jan 2019 0... ▼

37

Total Software

| LICENSE | |
|---|---|
| Commercial | 37 |

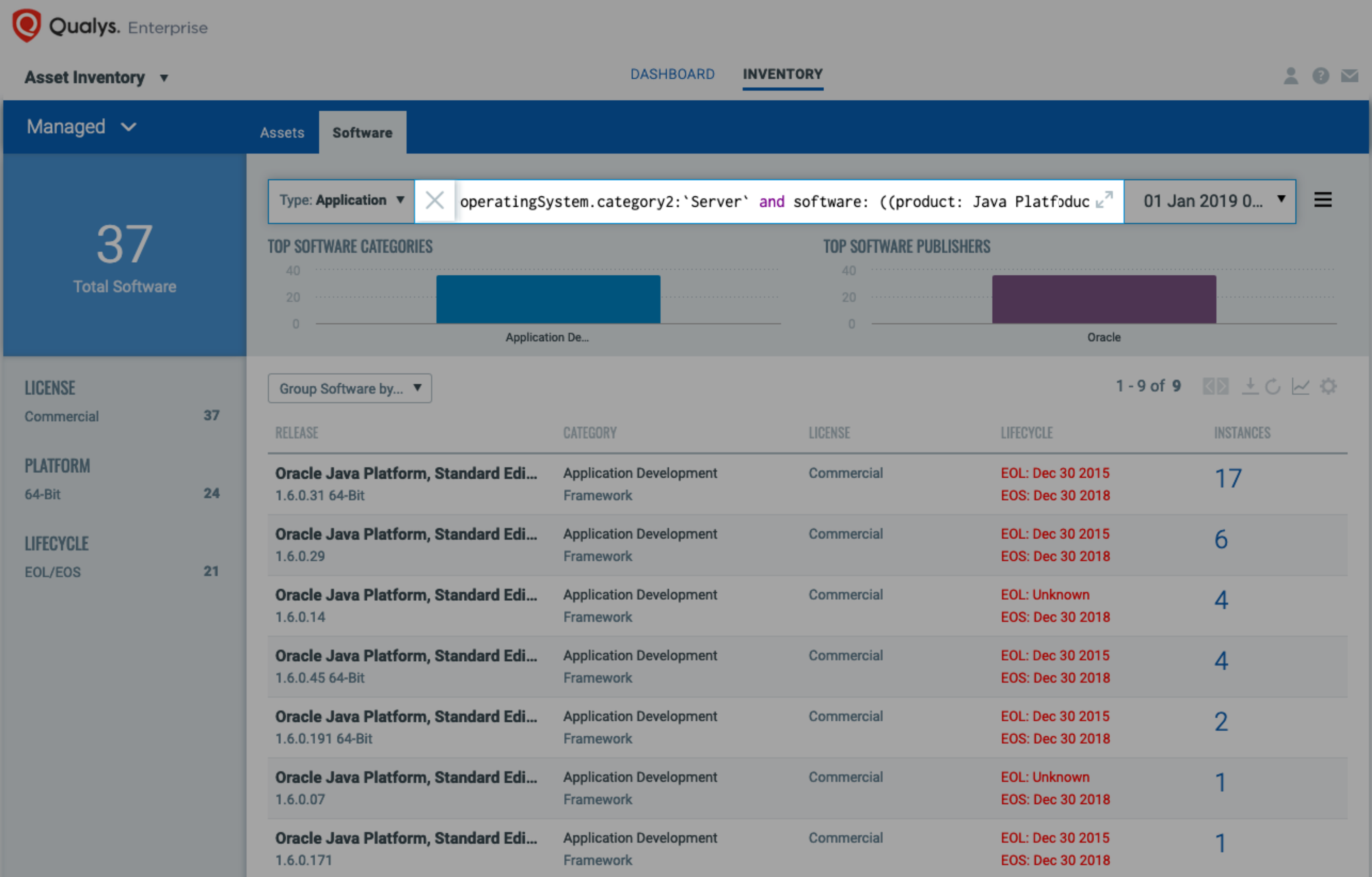
| PLATFORM | |
|---|---|
| 64-Bit | 24 |

| LIFECYCLE | |
|---|---|
| EOL/EOS | 21 |

Group Software by... ▼

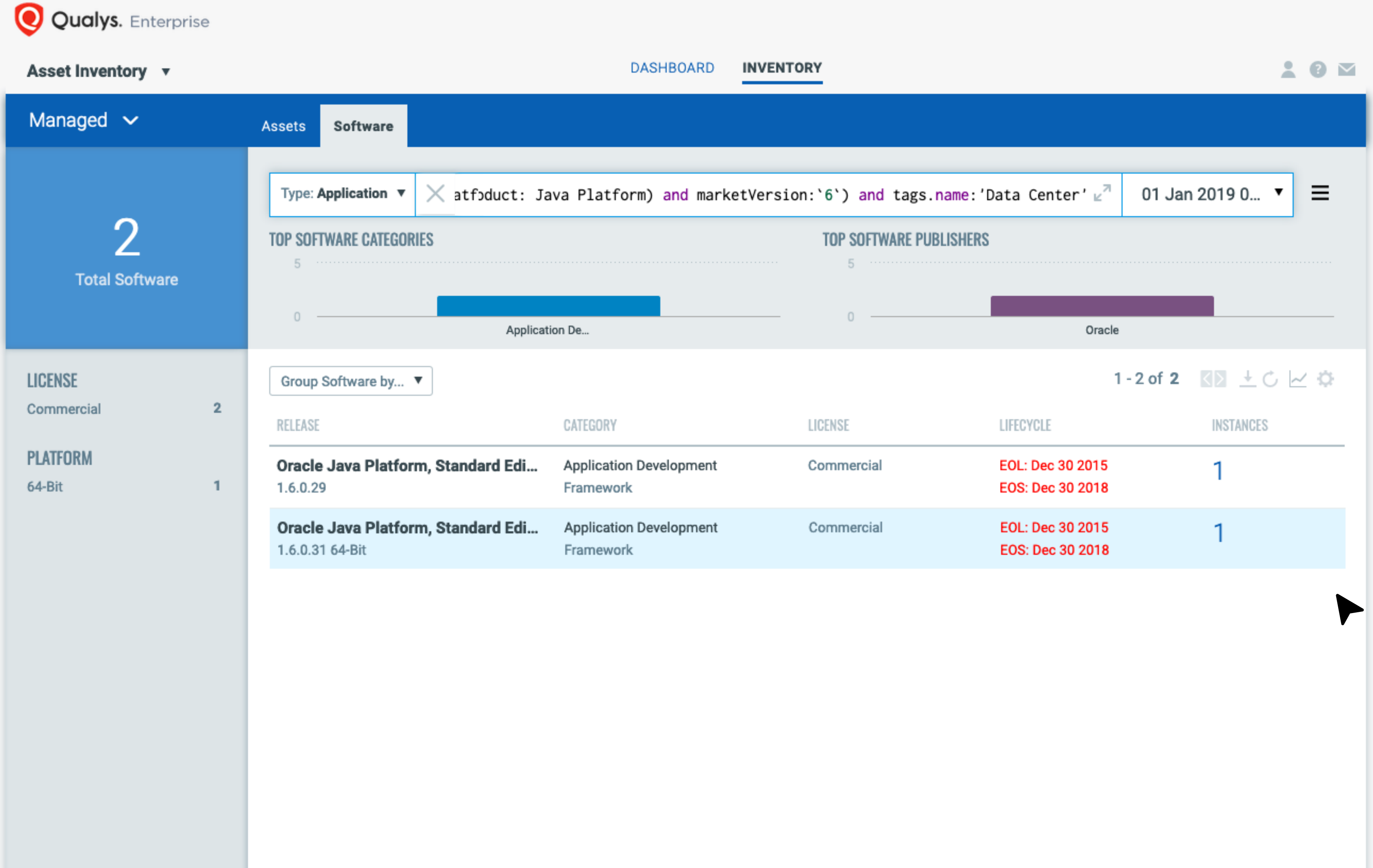
1 - 9 of 9

| RELEASE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|---|---|---|---|---|
| Oracle Java Platform, Standard Edi...<br>1.6.0.31 64-Bit | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 17 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.29 | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 6 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.14 | Application Development Framework | Commercial | EOL: Unknown<br>EOS: Dec 30 2018 | 4 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.45 64-Bit | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 4 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.191 64-Bit | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 2 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.07 | Application Development Framework | Commercial | EOL: Unknown<br>EOS: Dec 30 2018 | 1 |
| Oracle Java Platform, Standard Edi...<br>1.6.0.171 | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 1 |



```
operatingSystem.category2:`Server` and software: ((product: Java Platfɔduc
```

| RELEASE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|---|---|---|---|---|
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.31 64-Bit | Application Development<br>Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 17 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.29 | Application Development<br>Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 6 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.14 | Application Development<br>Framework | Commercial | EOL: Unknown<br>EOS: Dec 30 2018 | 4 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.45 64-Bit | Application Development<br>Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 4 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.191 64-Bit | Application Development<br>Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 2 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.07 | Application Development<br>Framework | Commercial | EOL: Unknown<br>EOS: Dec 30 2018 | 1 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.171 | Application Development<br>Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 1 |



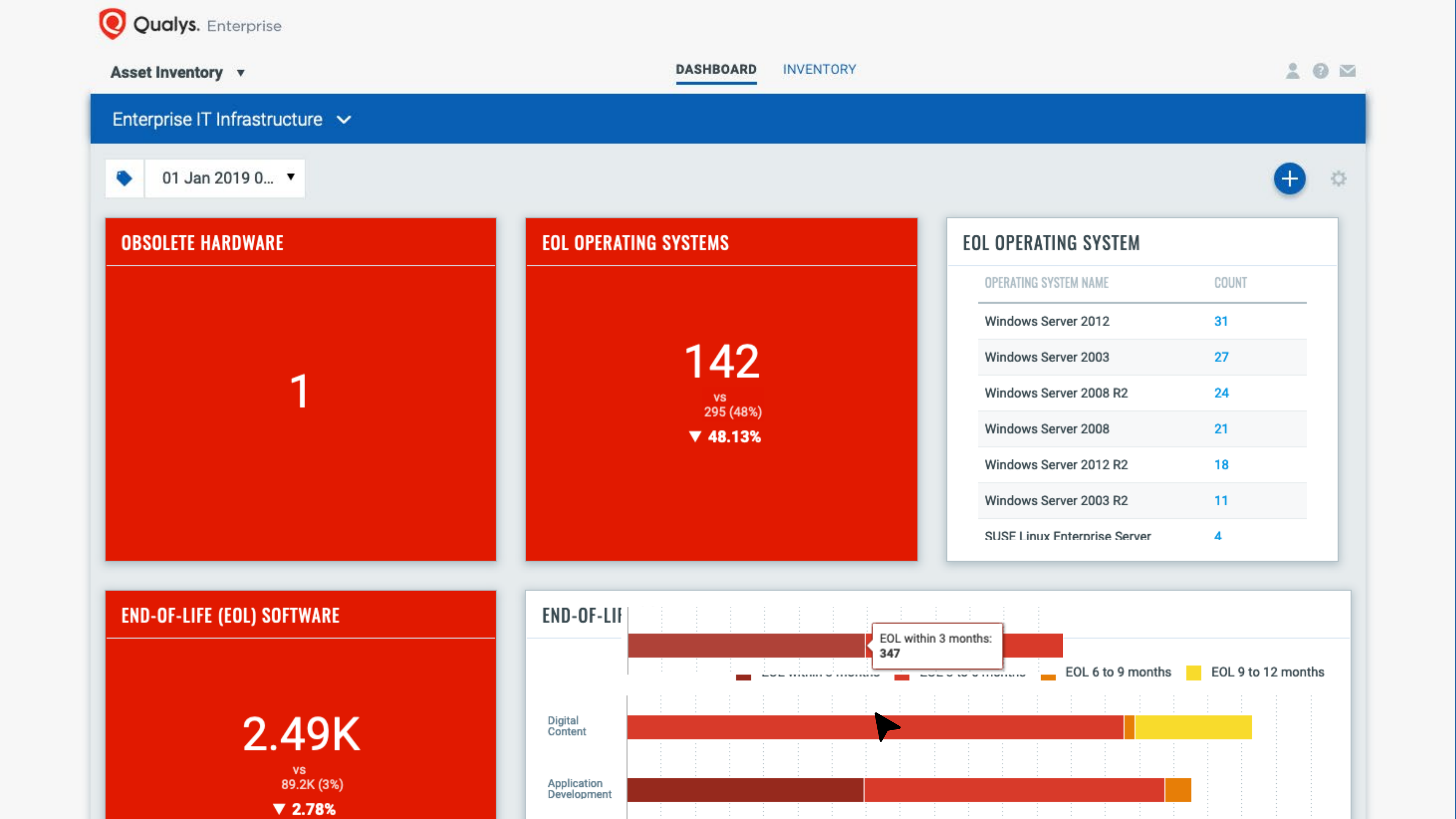
Type: Application

atfɔduct: Java Platform) and marketVersion:`6`) and tags.name:'Data Center'

01 Jan 2019 0...

| RELEASE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|---|---|---|---|---|
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.29 | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 1 |
| **Oracle Java Platform, Standard Edi...**<br>1.6.0.31 64-Bit | Application Development Framework | Commercial | EOL: Dec 30 2015<br>EOS: Dec 30 2018 | 1 |

# Track hardware and software lifecycles and licenses



Qualys. Enterprise

Asset Inventory ▾

DASHBOARD INVENTORY

Enterprise IT Infrastructure ⌄

01 Jan 2019 0... ▾

**OBSOLETE HARDWARE**

1

**EOL OPERATING SYSTEMS**

142

vs
295 (48%)

▼ 48.13%

**EOL OPERATING SYSTEM**

| OPERATING SYSTEM NAME | COUNT |
|---|---|
| Windows Server 2012 | 31 |
| Windows Server 2003 | 27 |
| Windows Server 2008 R2 | 24 |
| Windows Server 2008 | 21 |
| Windows Server 2012 R2 | 18 |
| Windows Server 2003 R2 | 11 |
| SUSE Linux Enterprise Server | 4 |

**END-OF-LIFE (EOL) SOFTWARE**

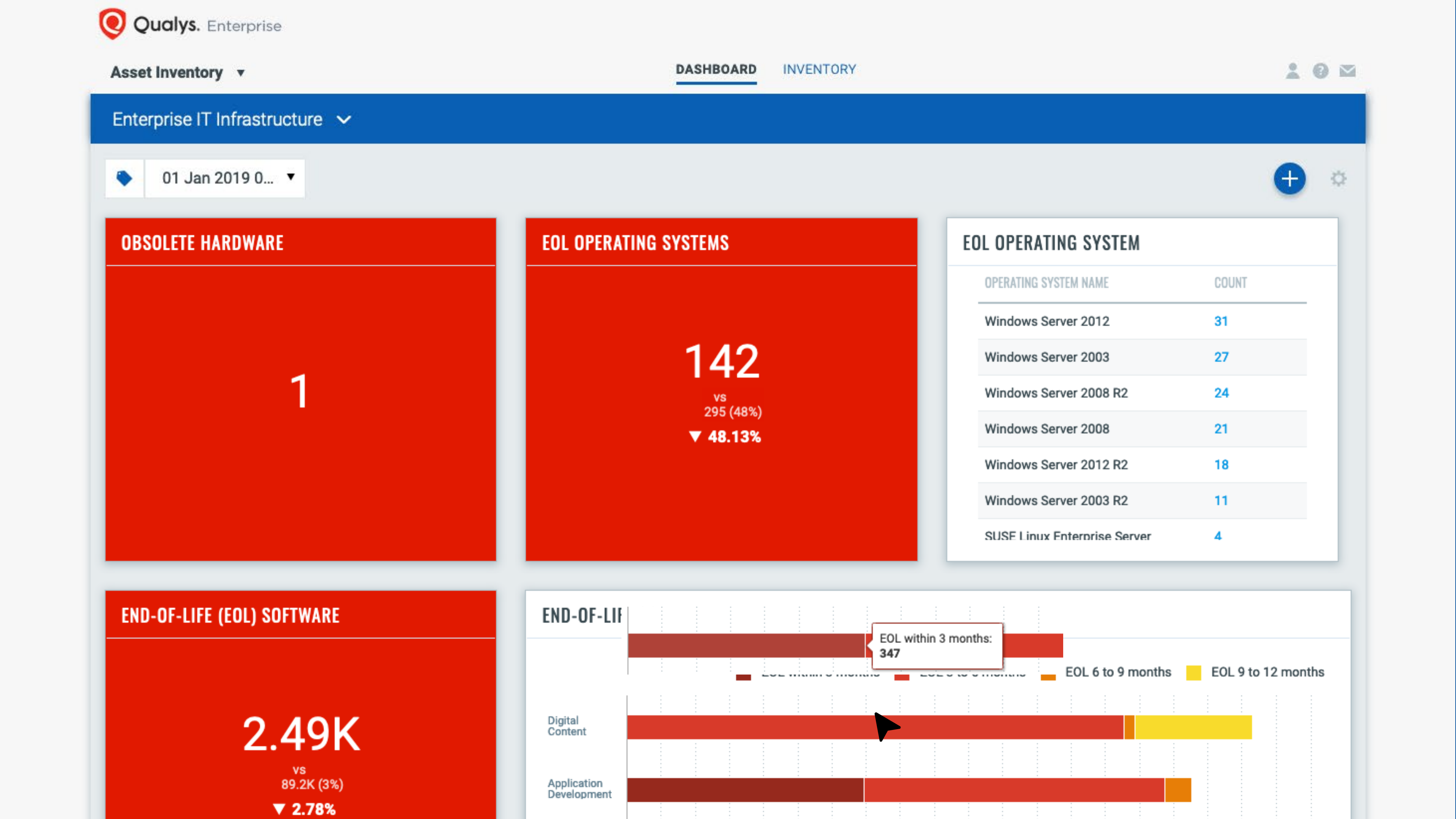
2.49K

vs
89.2K (3%)

▼ 2.78%

**END-OF-LIF**

EOL within 3 months:
**347**



OBSOLETE HARDWARE

1

EOL OPERATING SYSTEMS

142
vs
295 (48%)
▼ 48.13%

EOL OPERATING SYSTEM

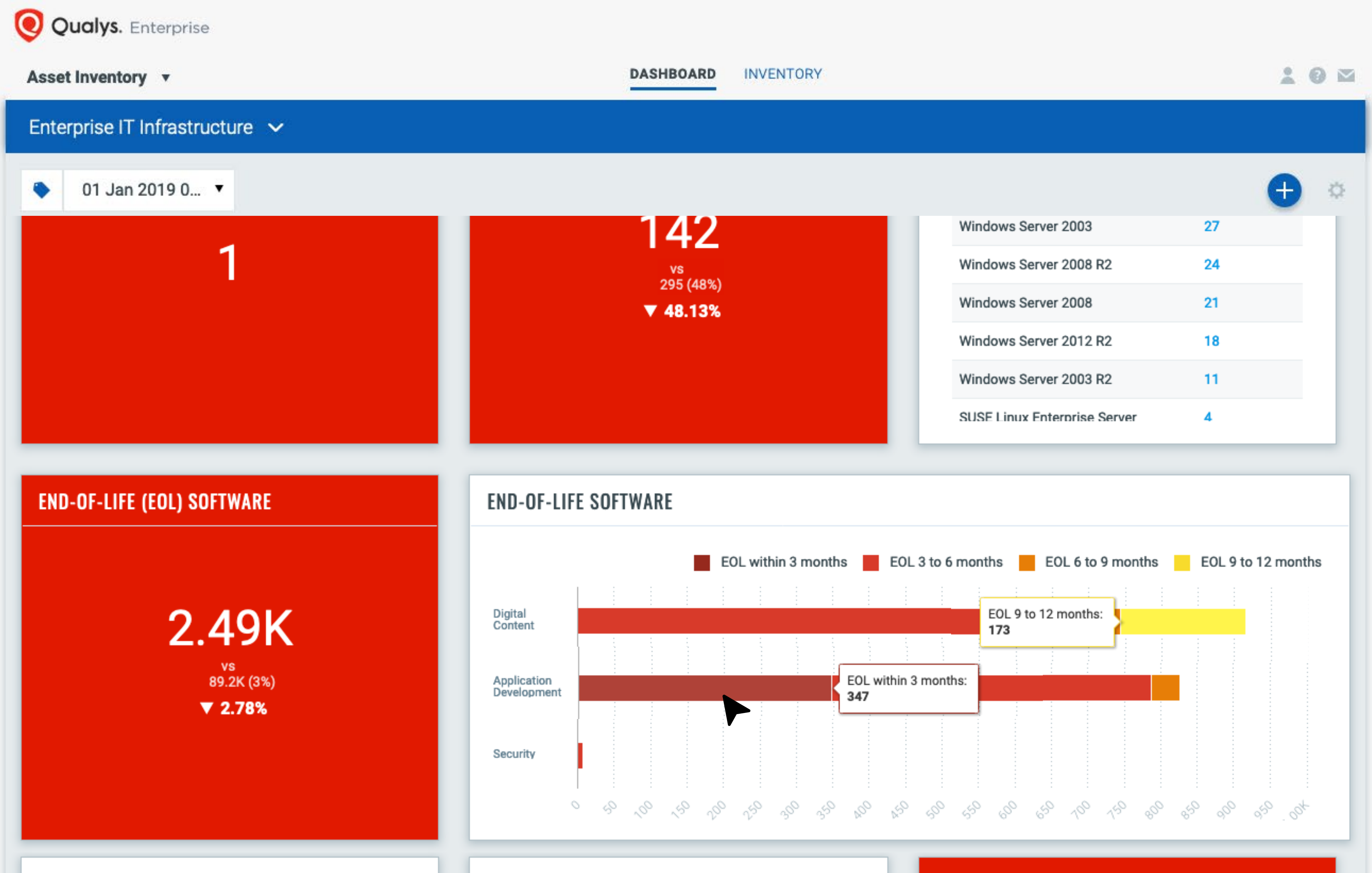
| OPERATING SYSTEM NAME | COUNT |
|---|---|
| Windows Server 2012 | 31 |
| Windows Server 2003 | 27 |
| Windows Server 2008 R2 | 24 |
| Windows Server 2008 | 21 |
| Windows Server 2012 R2 | 18 |
| Windows Server 2003 R2 | 11 |
| SUSE Linux Enterprise Server | 4 |

END-OF-LIFE (EOL) SOFTWARE

2.49K
vs
89.2K (3%)
▼ 2.78%

END-OF-LIF

EOL within 3 months: 347



1

142
vs
295 (48%)
▼ 48.13%

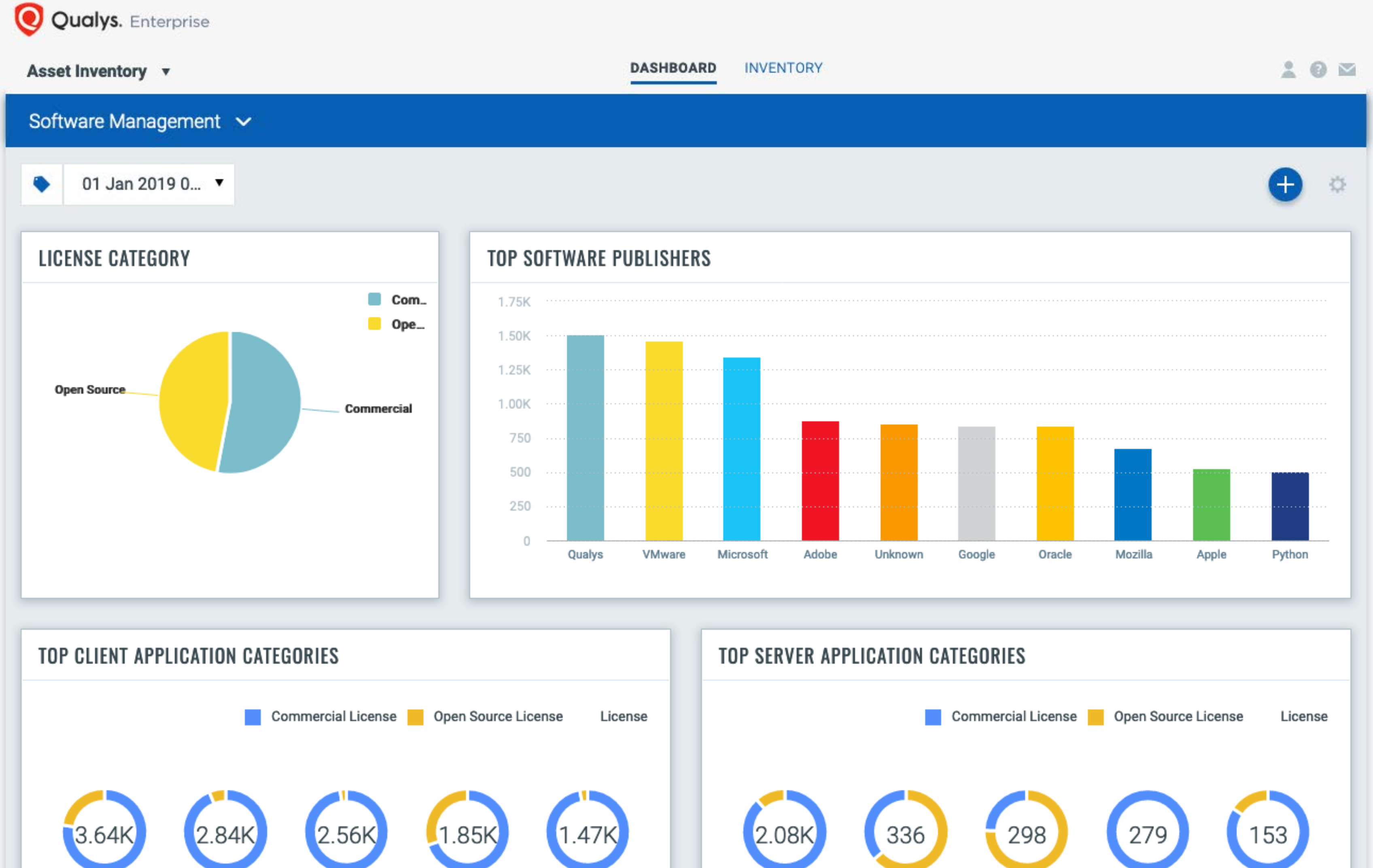
| | |
|---|---|
| Windows Server 2003 | 27 |
| Windows Server 2008 R2 | 24 |
| Windows Server 2008 | 21 |
| Windows Server 2012 R2 | 18 |
| Windows Server 2003 R2 | 11 |
| SUSE Linux Enterprise Server | 4 |

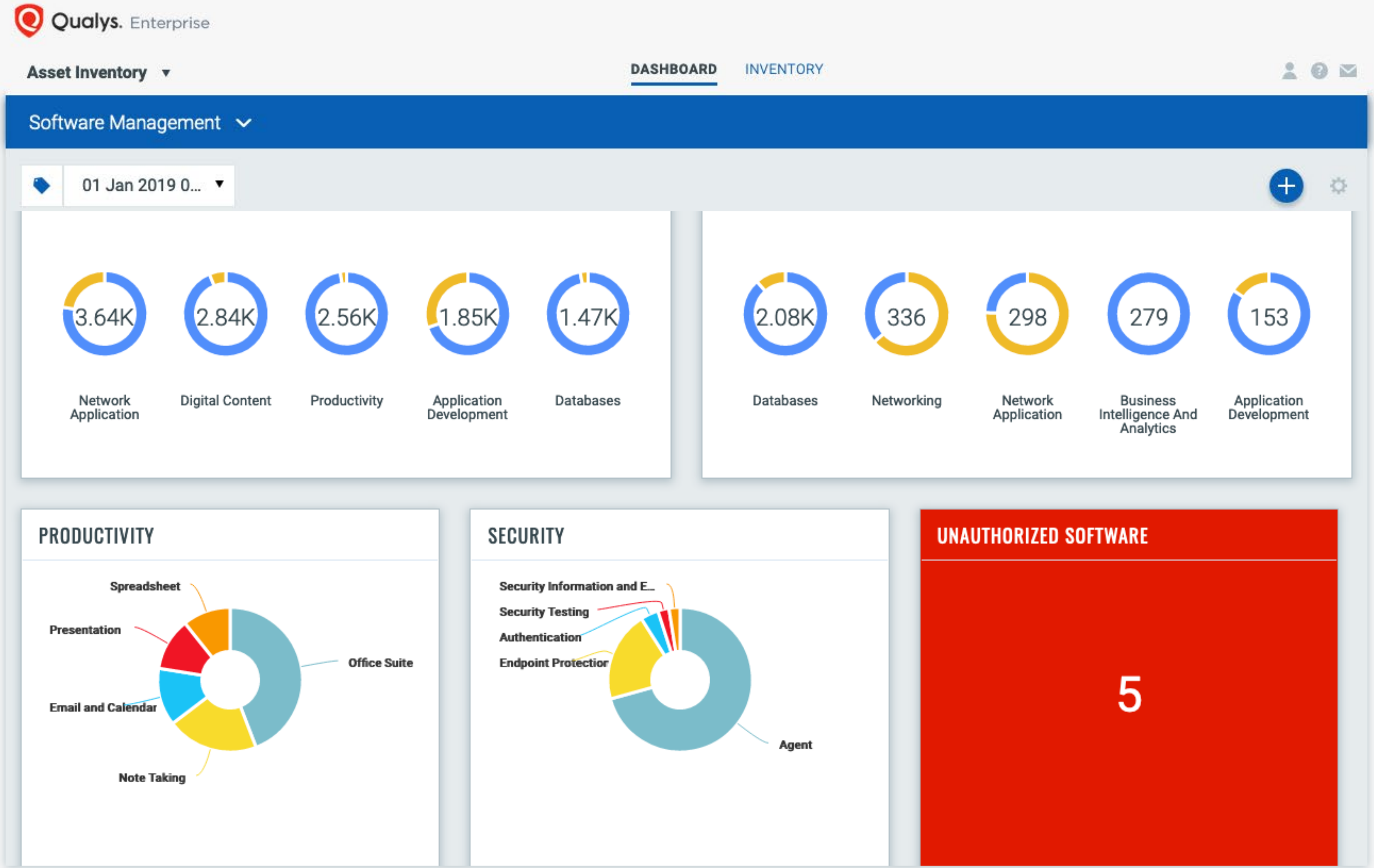
END-OF-LIFE (EOL) SOFTWARE

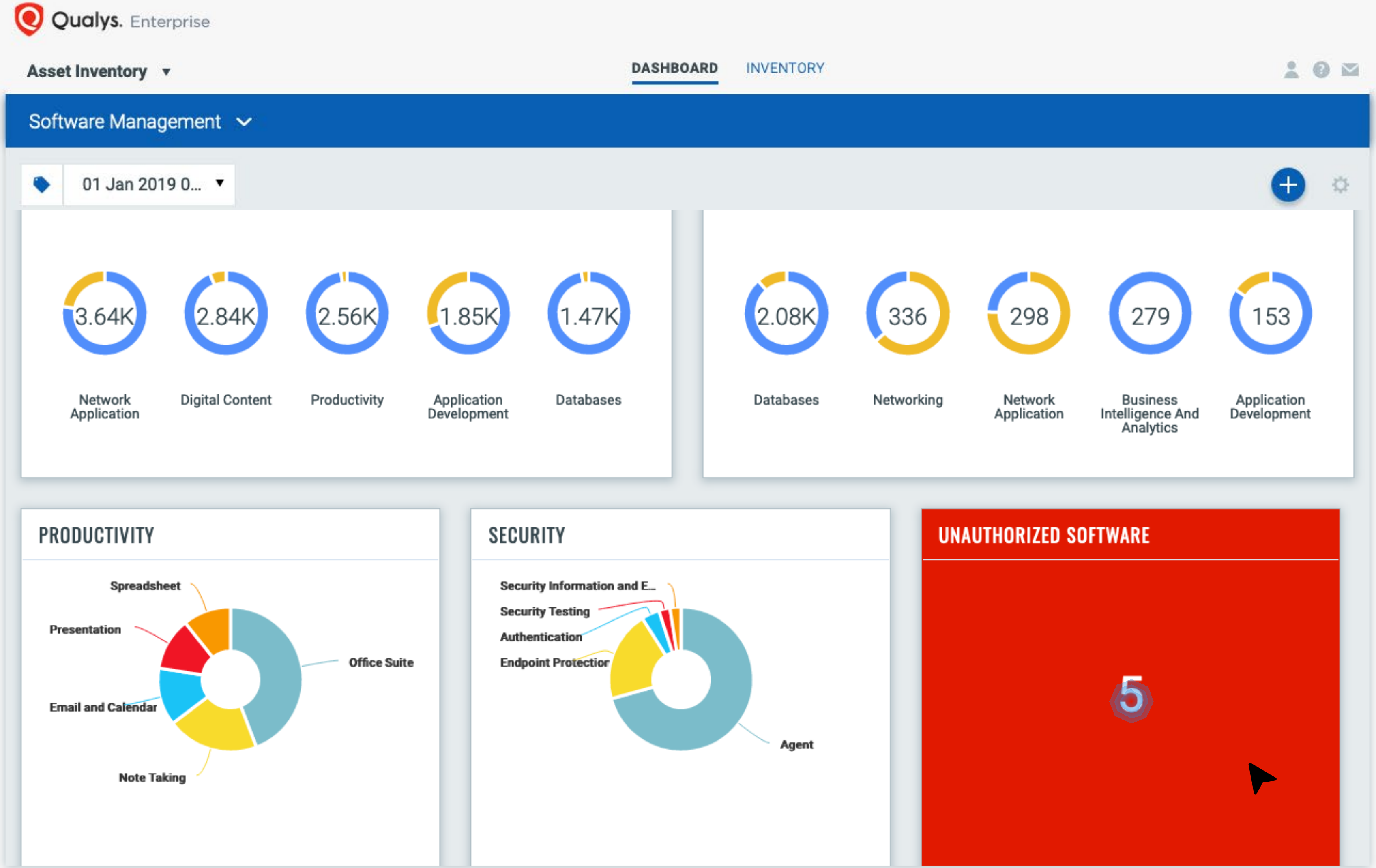
2.49K
vs
89.2K (3%)
▼ 2.78%

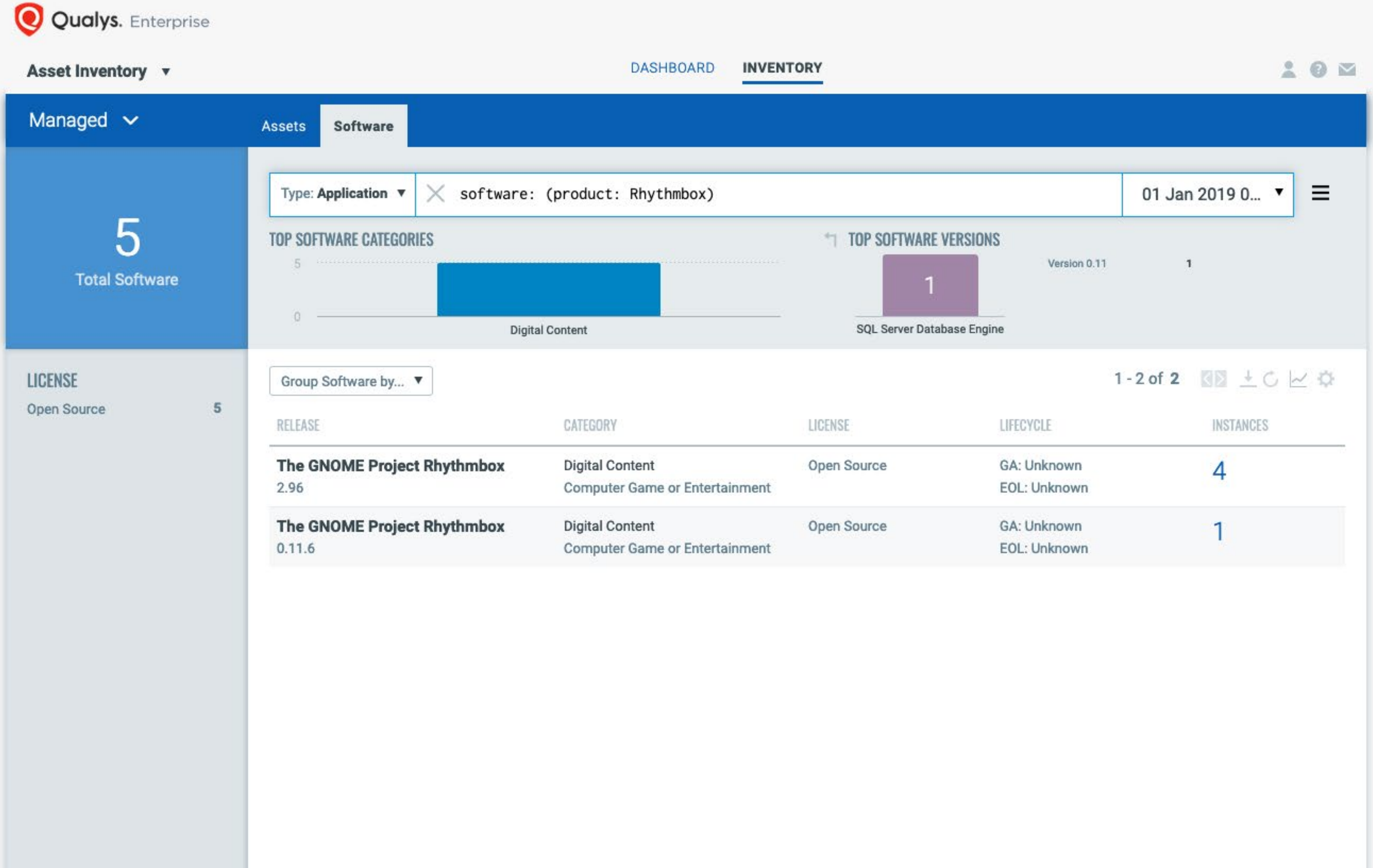
END-OF-LIFE SOFTWARE

# Find unauthorized software


Qualys. Enterprise
Asset Inventory ▾
DASHBOARD
INVENTORY
Software Management
01 Jan 2019 0...
LICENSE CATEGORY
Com...
Ope...
Open Source
Commercial
TOP SOFTWARE PUBLISHERS
1.75K
1.50K
1.25K
1.00K
750
500
250
0
Qualys
VMware
Microsoft
Adobe
Unknown
Google
Oracle
Mozilla
Apple
Python
TOP CLIENT APPLICATION CATEGORIES
Commercial License
Open Source License
License
3.64K
2.84K
2.56K
1.85K
1.47K
TOP SERVER APPLICATION CATEGORIES
Commercial License
Open Source License
License
2.08K
336
298
279
153


Qualys. Enterprise
Asset Inventory ▼
DASHBOARD
INVENTORY
Software Management
01 Jan 2019 0... ▼
+
3.64K
Network Application
2.84K
Digital Content
2.56K
Productivity
1.85K
Application Development
1.47K
Databases
2.08K
Databases
336
Networking
298
Network Application
279
Business Intelligence And Analytics
153
Application Development
PRODUCTIVITY
Spreadsheet
Presentation
Office Suite
Email and Calendar
Note Taking
SECURITY
Security Information and E...
Security Testing
Authentication
Endpoint Protectior
Agent
UNAUTHORIZED SOFTWARE
5


Qualys. Enterprise
Asset Inventory ▼
DASHBOARD
INVENTORY
Software Management
01 Jan 2019 0... ▼
3.64K
Network Application
2.84K
Digital Content
2.56K
Productivity
1.85K
Application Development
1.47K
Databases
2.08K
Databases
336
Networking
298
Network Application
279
Business Intelligence And Analytics
153
Application Development
PRODUCTIVITY
Spreadsheet
Presentation
Office Suite
Email and Calendar
Note Taking
SECURITY
Security Information and E...
Security Testing
Authentication
Endpoint Protection
Agent
UNAUTHORIZED SOFTWARE
5



Type: Application ▼

```
software: (product: Rhythmbox)
```

01 Jan 2019 0... ▼

5

Total Software

TOP SOFTWARE CATEGORIES

TOP SOFTWARE VERSIONS

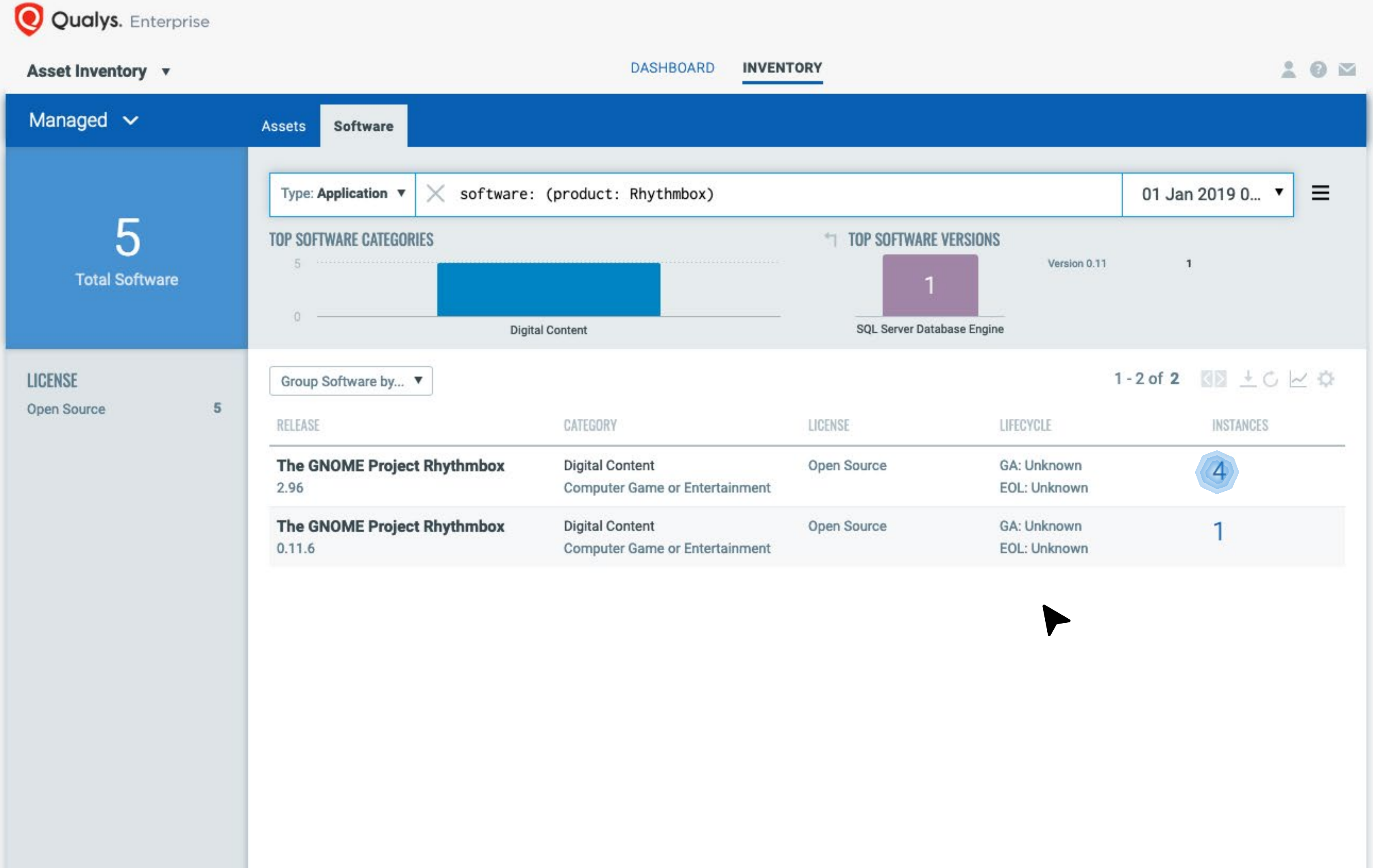
LICENSE

| | |
|---|---|
| Open Source | 5 |

Group Software by... ▼

1 - 2 of 2

| RELEASE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|---|---|---|---|---|
| The GNOME Project Rhythmbox<br>2.96 | Digital Content<br>Computer Game or Entertainment | Open Source | GA: Unknown<br>EOL: Unknown | 4 |
| The GNOME Project Rhythmbox<br>0.11.6 | Digital Content<br>Computer Game or Entertainment | Open Source | GA: Unknown<br>EOL: Unknown | 1 |



software: (product: Rhythmbox)

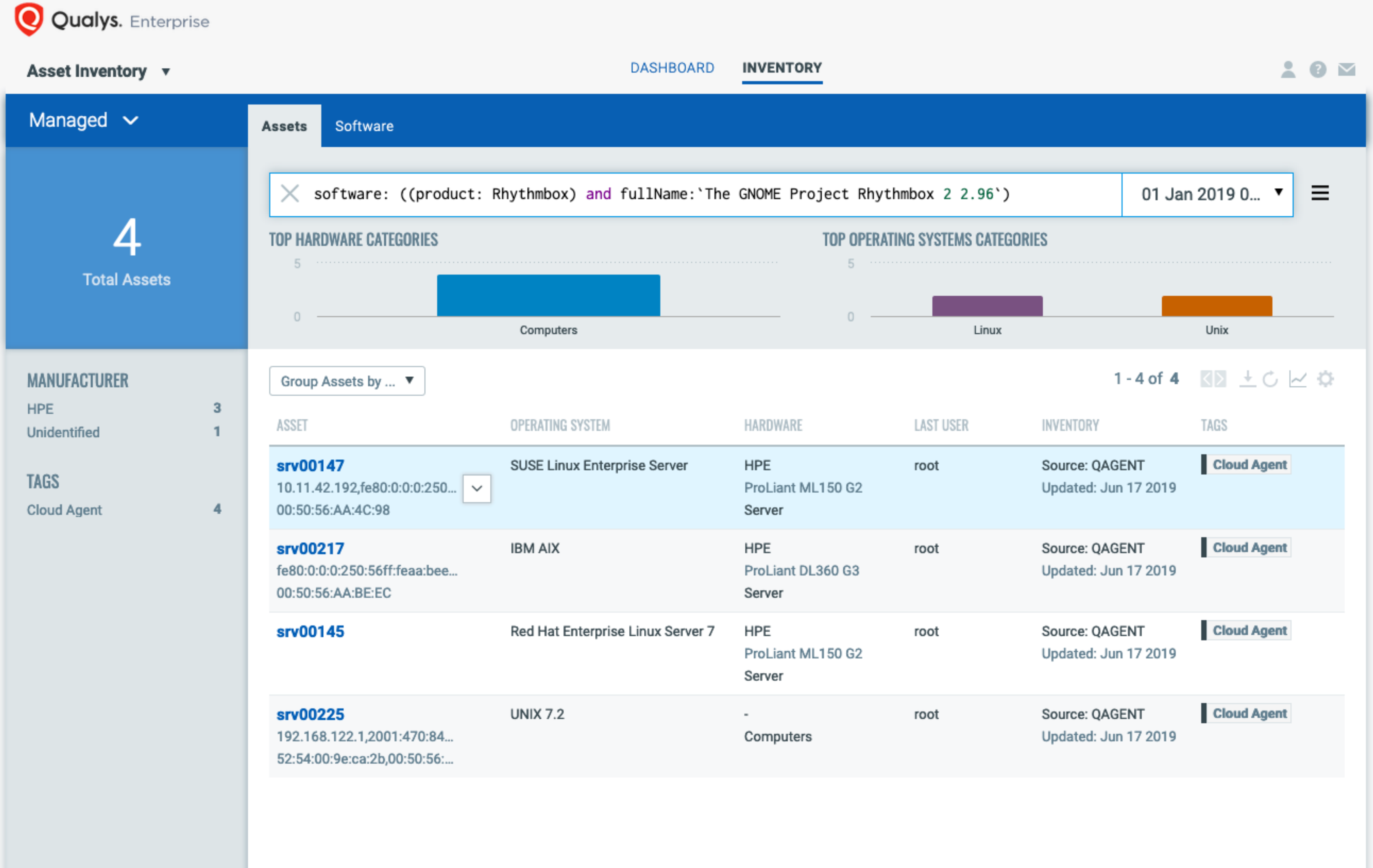
01 Jan 2019 0...

5 Total Software

LICENSE

Open Source 5

| RELEASE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|---|---|---|---|---|
| **The GNOME Project Rhythmbox**<br>2.96 | Digital Content<br>Computer Game or Entertainment | Open Source | GA: Unknown<br>EOL: Unknown | 4 |
| **The GNOME Project Rhythmbox**<br>0.11.6 | Digital Content<br>Computer Game or Entertainment | Open Source | GA: Unknown<br>EOL: Unknown | 1 |



```
software: ((product: Rhythmbox) and fullName:`The GNOME Project Rhythmbox 2 2.96`)
```

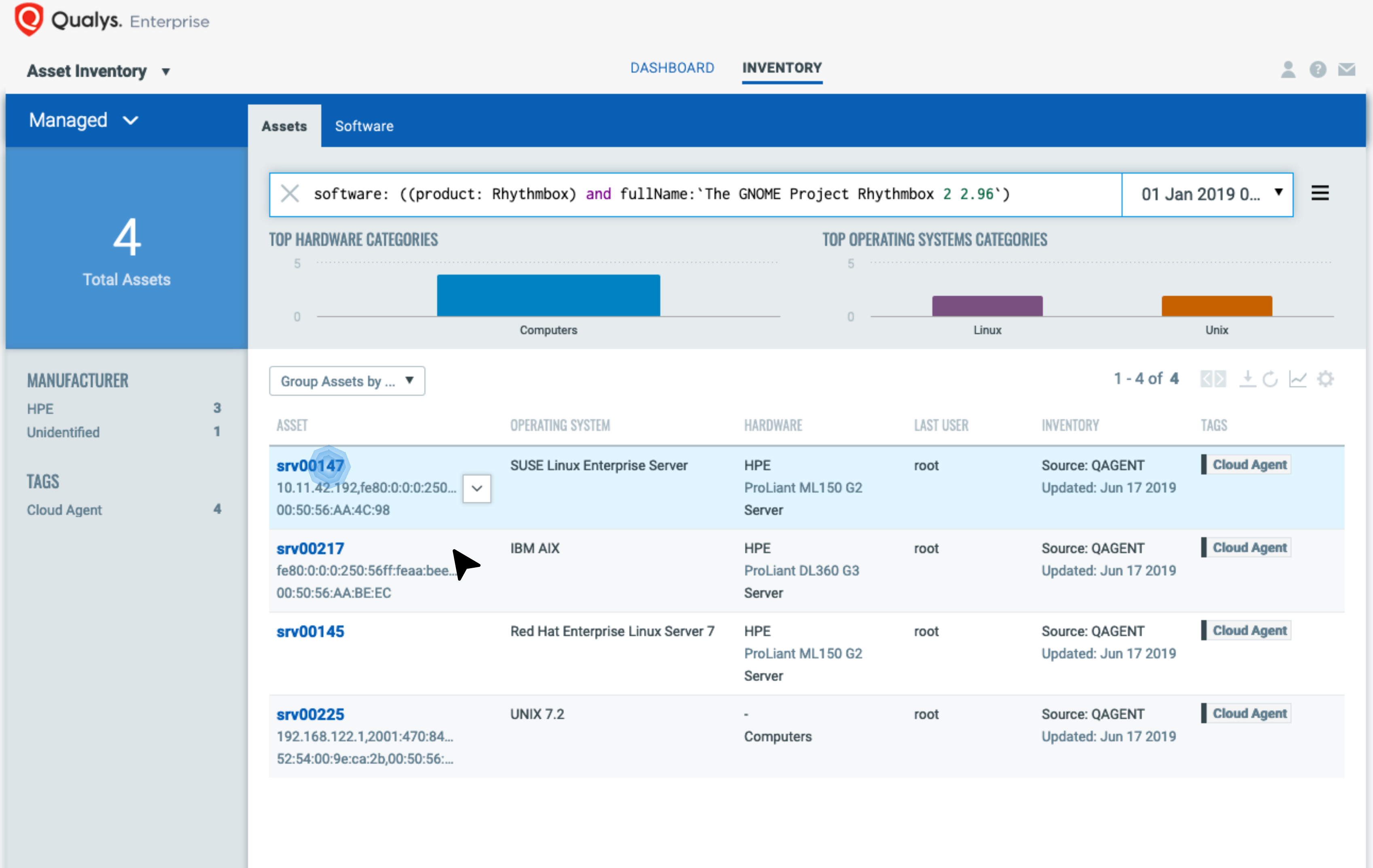
MANUFACTURER

| | |
|---|---|
| HPE | 3 |
| Unidentified | 1 |

TAGS

| | |
|---|---|
| Cloud Agent | 4 |

| ASSET | OPERATING SYSTEM | HARDWARE | LAST USER | INVENTORY | TAGS |
|---|---|---|---|---|---|
| srv00147<br>10.11.42.192,fe80:0:0:0:250...<br>00:50:56:AA:4C:98 | SUSE Linux Enterprise Server | HPE<br>ProLiant ML150 G2<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00217<br>fe80:0:0:0:250:56ff:feaa:bee...<br>00:50:56:AA:BE:EC | IBM AIX | HPE<br>ProLiant DL360 G3<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00145 | Red Hat Enterprise Linux Server 7 | HPE<br>ProLiant ML150 G2<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00225<br>192.168.122.1,2001:470:84...<br>52:54:00:9e:ca:2b,00:50:56:... | UNIX 7.2 | -<br>Computers | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |



```
software: ((product: Rhythmbox) and fullName:`The GNOME Project Rhythmbox 2 2.96`)
```

01 Jan 2019 0... ▾

4 Total Assets

MANUFACTURER

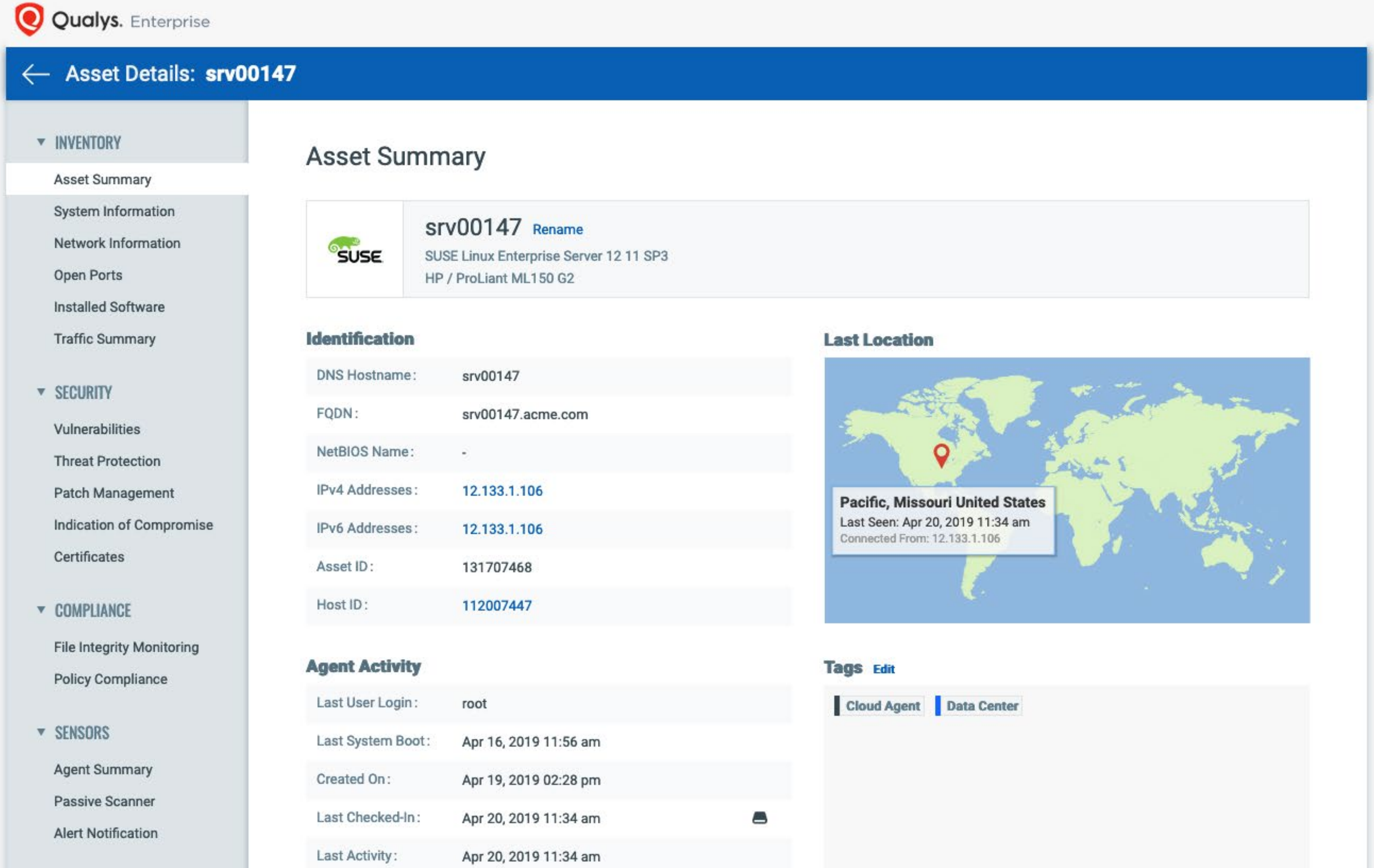
| | |
|---|---|
| HPE | 3 |
| Unidentified | 1 |

TAGS

| | |
|---|---|
| Cloud Agent | 4 |

1 - 4 of 4

| ASSET | OPERATING SYSTEM | HARDWARE | LAST USER | INVENTORY | TAGS |
|---|---|---|---|---|---|
| srv00147<br>10.11.42.192,fe80:0:0:0:250...<br>00:50:56:AA:4C:98 | SUSE Linux Enterprise Server | HPE<br>ProLiant ML150 G2<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00217<br>fe80:0:0:0:250:56ff:feaa:bee...<br>00:50:56:AA:BE:EC | IBM AIX | HPE<br>ProLiant DL360 G3<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00145 | Red Hat Enterprise Linux Server 7 | HPE<br>ProLiant ML150 G2<br>Server | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |
| srv00225<br>192.168.122.1,2001:470:84...<br>52:54:00:9e:ca:2b,00:50:56:... | UNIX 7.2 | -<br>Computers | root | Source: QAGENT<br>Updated: Jun 17 2019 | Cloud Agent |



Asset Details: srv00147

## Asset Summary

SUSE

srv00147

SUSE Linux Enterprise Server 12 11 SP3

HP / ProLiant ML150 G2

### Identification

DNS Hostname: srv00147

FQDN: srv00147.acme.com

NetBIOS Name: -

IPv4 Addresses: 12.133.1.106

IPv6 Addresses: 12.133.1.106

Asset ID: 131707468

Host ID: 112007447

### Last Location

Pacific, Missouri United States

Last Seen: Apr 20, 2019 11:34 am

Connected From: 12.133.1.106

### Agent Activity

Last User Login: root

Last System Boot: Apr 16, 2019 11:56 am

Created On: Apr 19, 2019 02:28 pm

Last Checked-In: Apr 20, 2019 11:34 am

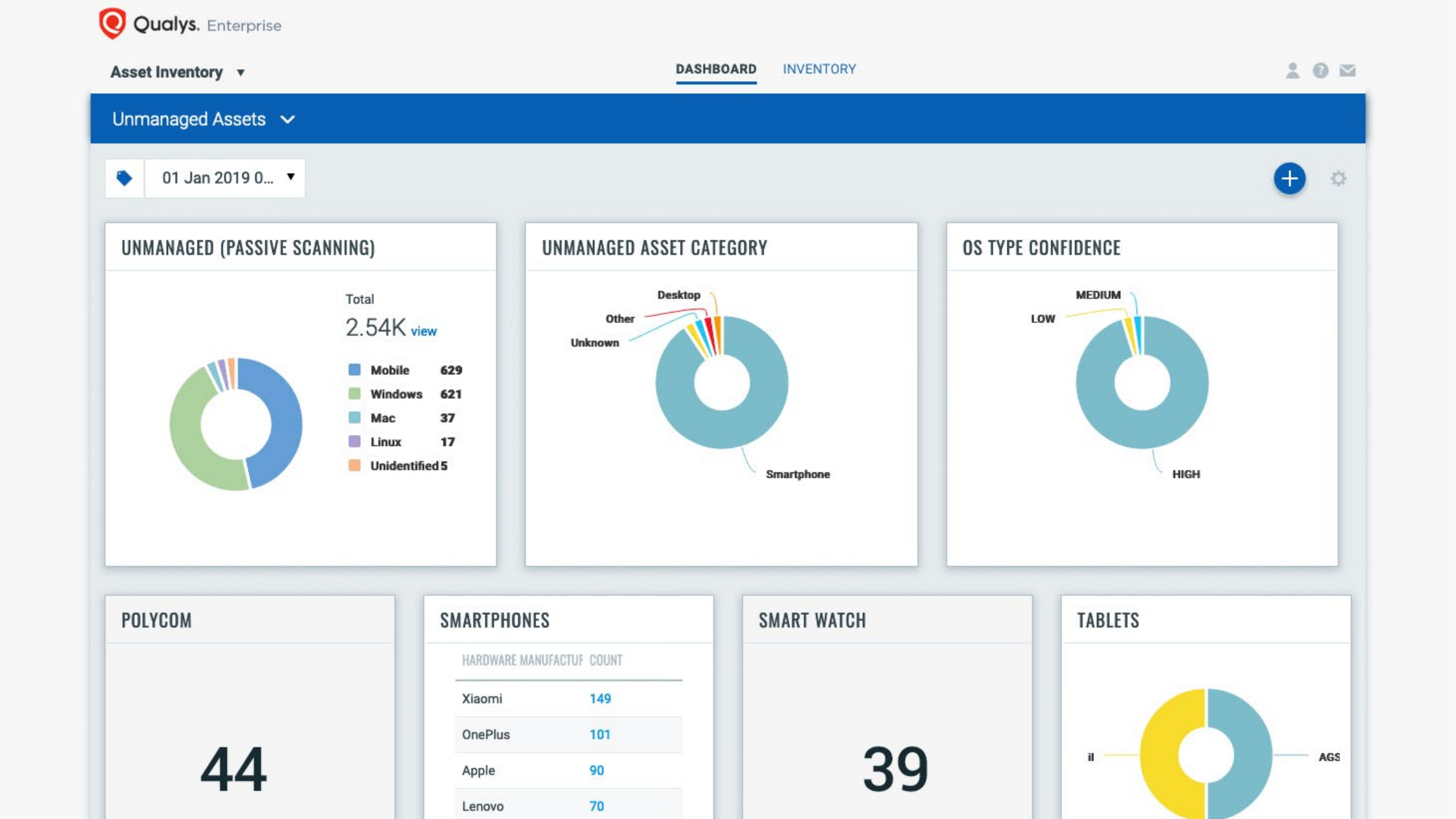
Last Activity: Apr 20, 2019 11:34 am

### Tags

Cloud Agent

Data Center

Identify unknown assets
that connect to the network



Qualys. Enterprise

Asset Inventory ▼

DASHBOARD INVENTORY

Unmanaged Assets

01 Jan 2019 0... ▼

## UNMANAGED (PASSIVE SCANNING)

Total

2.54K view

| | | |
|---|---|---|
| 🟦 | Mobile | 629 |
| 🟩 | Windows | 621 |
| 🟦 | Mac | 37 |
| 🟪 | Linux | 17 |
| 🟧 | Unidentified | 5 |

## UNMANAGED ASSET CATEGORY

## OS TYPE CONFIDENCE

## POLYCOM

44

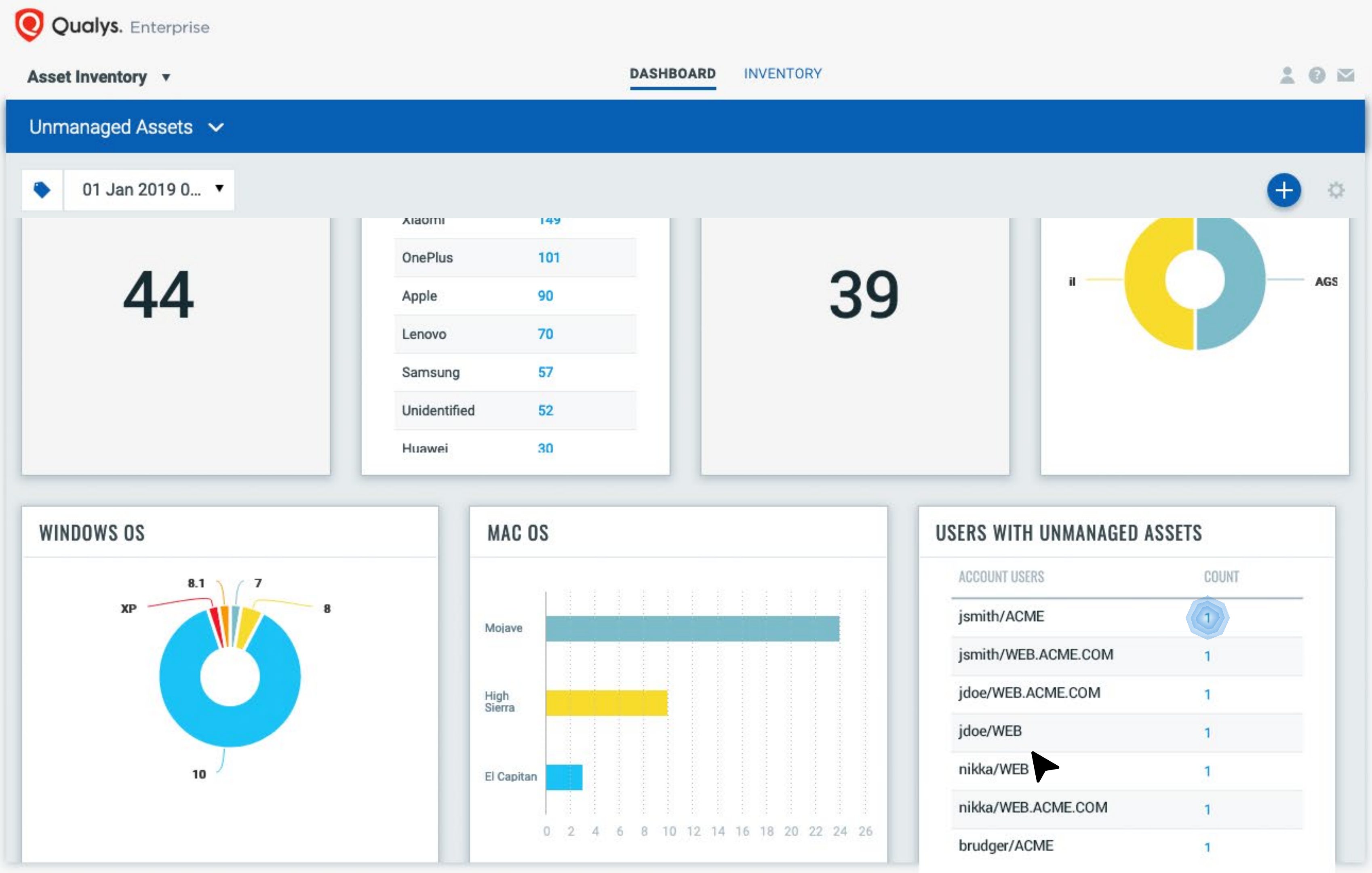
## SMARTPHONES

| HARDWARE MANUFACTUF | COUNT |
|---|---|
| Xiaomi | 149 |
| OnePlus | 101 |
| Apple | 90 |
| Lenovo | 70 |

## SMART WATCH

39

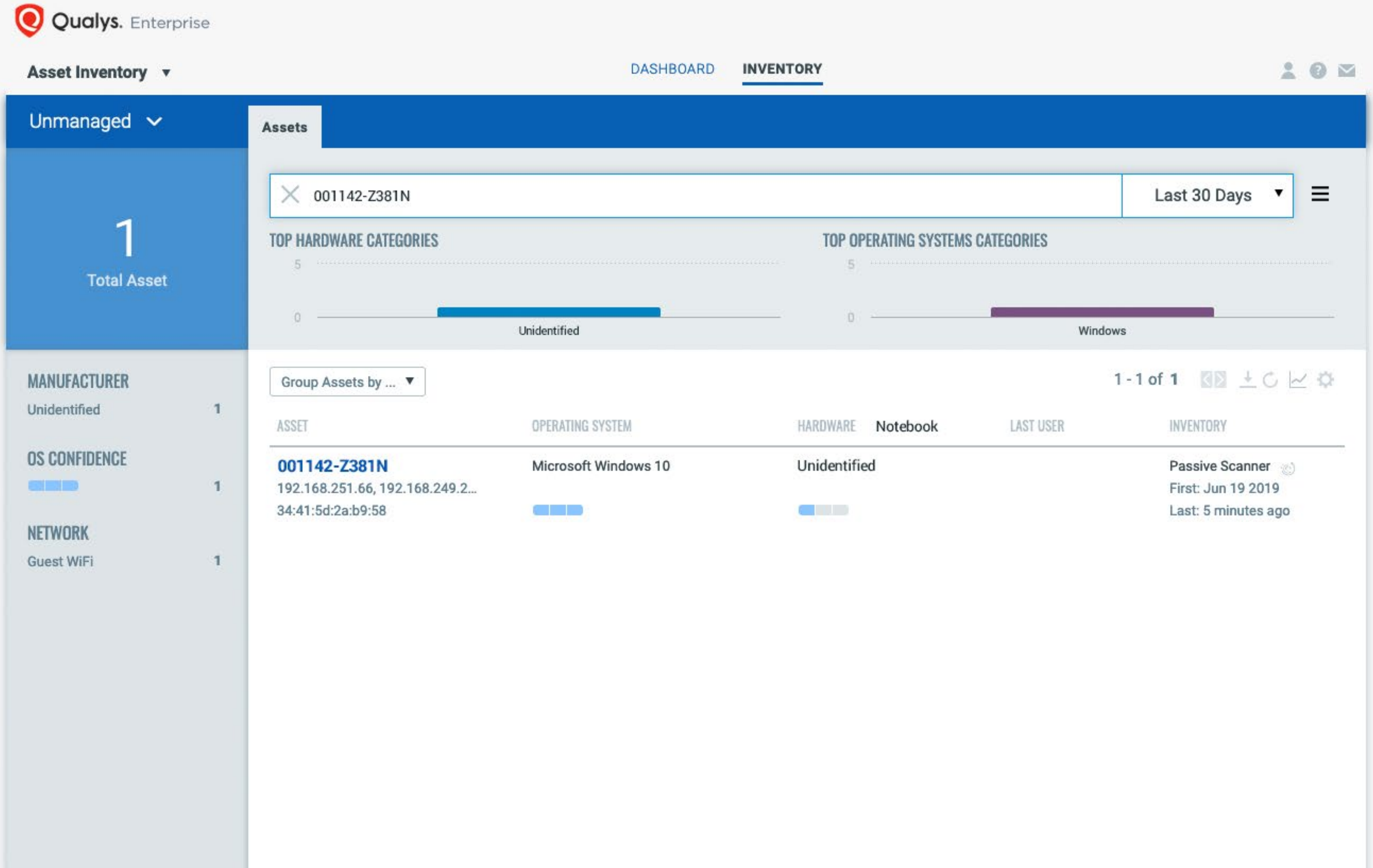
## TABLETS



| | |
|---|---|
| Xiaomi | 149 |
| OnePlus | 101 |
| Apple | 90 |
| Lenovo | 70 |
| Samsung | 57 |
| Unidentified | 52 |
| Huawei | 30 |

USERS WITH UNMANAGED ASSETS

| ACCOUNT USERS | COUNT |
|---|---|
| jsmith/ACME | 1 |
| jsmith/WEB.ACME.COM | 1 |
| jdoe/WEB.ACME.COM | 1 |
| jdoe/WEB | 1 |
| nikka/WEB | 1 |
| nikka/WEB.ACME.COM | 1 |
| brudger/ACME | 1 |



1 Total Asset

Search: 001142-Z381N

Last 30 Days ▼

MANUFACTURER

| | |
|---|---|
| Unidentified | 1 |

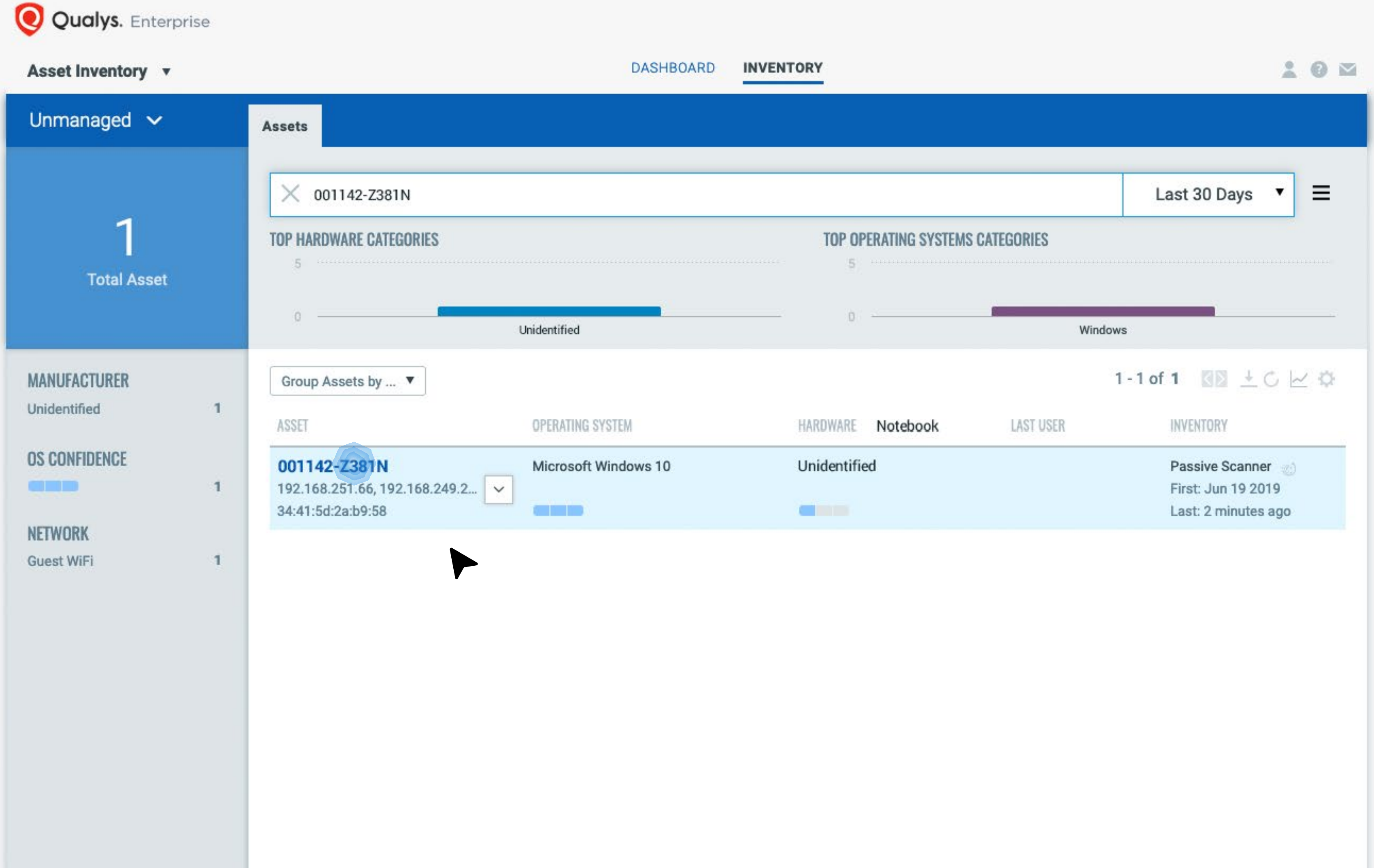
OS CONFIDENCE

| | |
|---|---|
| ▬▬▬ | 1 |

NETWORK

| | |
|---|---|
| Guest WiFi | 1 |

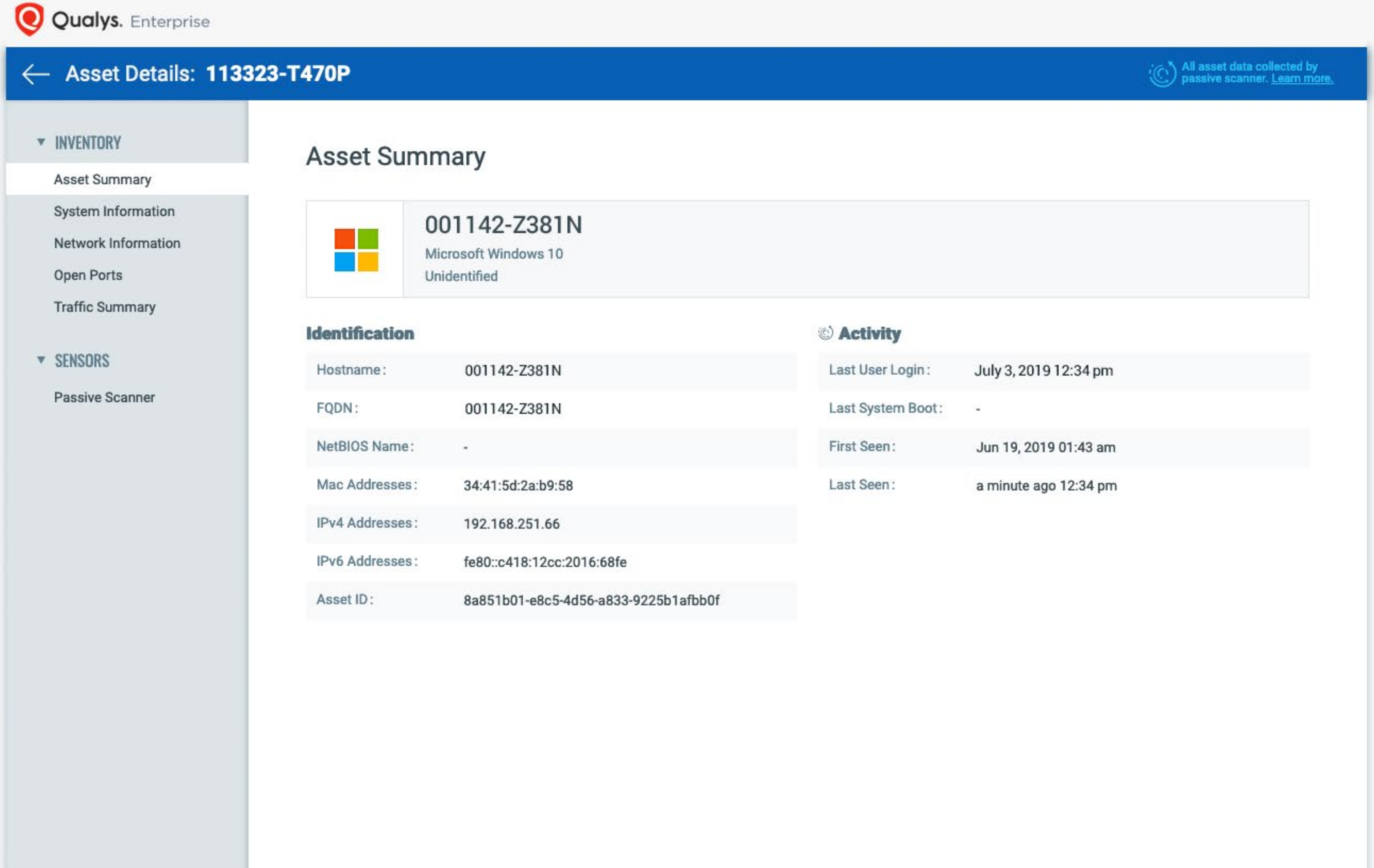
| ASSET | OPERATING SYSTEM | HARDWARE Notebook | LAST USER | INVENTORY |
|---|---|---|---|---|
| 001142-Z381N<br>192.168.251.66, 192.168.249.2...<br>34:41:5d:2a:b9:58 | Microsoft Windows 10<br>▬▬▬ | Unidentified<br>▬ | | Passive Scanner<br>First: Jun 19 2019<br>Last: 5 minutes ago |



Search: 001142-Z381N

Last 30 Days

| ASSET | OPERATING SYSTEM | HARDWARE | Notebook | LAST USER | INVENTORY |
|---|---|---|---|---|---|
| 001142-Z381N<br>192.168.251.66, 192.168.249.2...<br>34:41:5d:2a:b9:58 | Microsoft Windows 10 | Unidentified | | | Passive Scanner<br>First: Jun 19 2019<br>Last: 2 minutes ago |



Asset Details: 113323-T470P

## Asset Summary

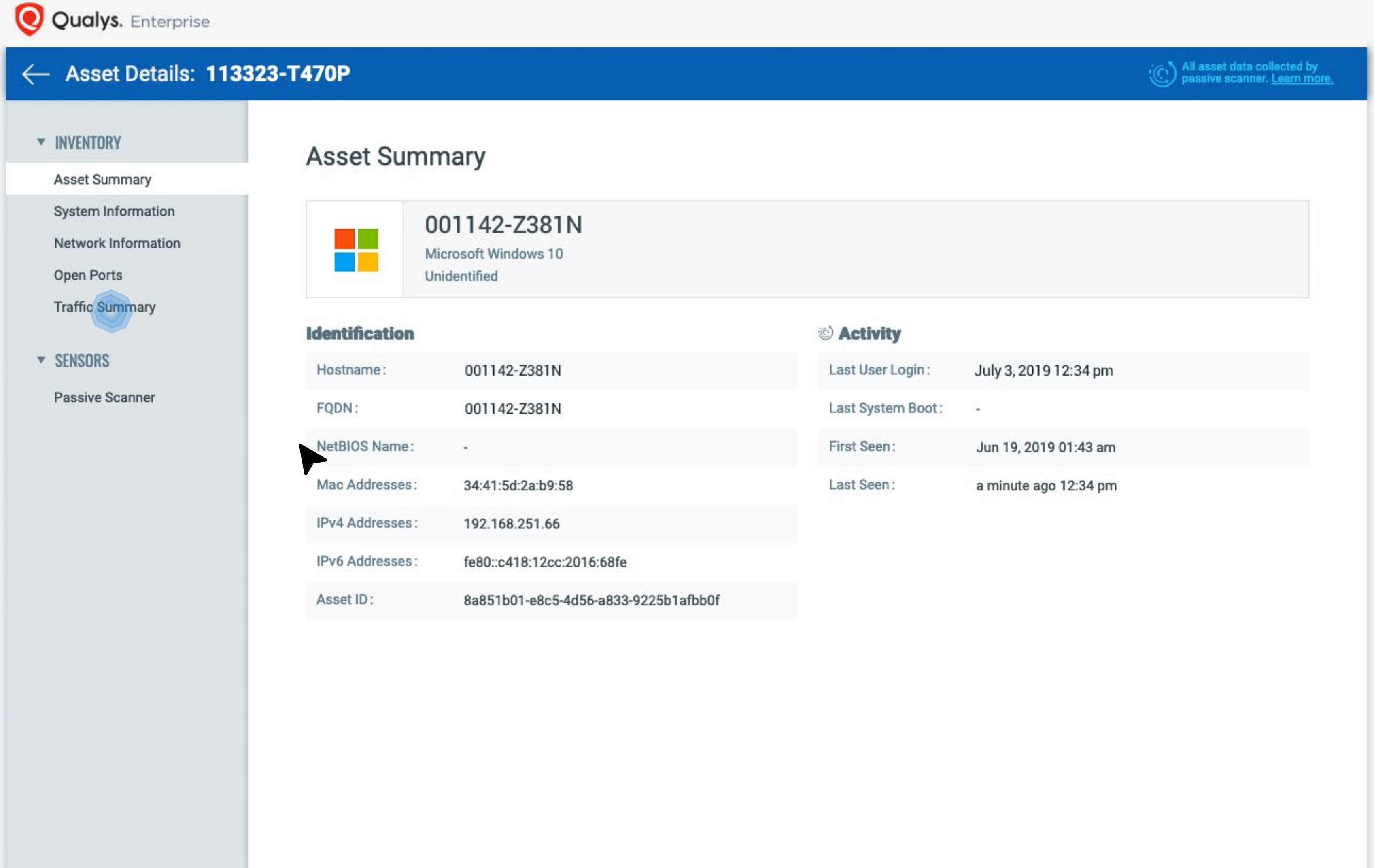
001142-Z381N
Microsoft Windows 10
Unidentified

### Identification

| | |
|---|---|
| Hostname : | 001142-Z381N |
| FQDN : | 001142-Z381N |
| NetBIOS Name : | - |
| Mac Addresses : | 34:41:5d:2a:b9:58 |
| IPv4 Addresses : | 192.168.251.66 |
| IPv6 Addresses : | fe80::c418:12cc:2016:68fe |
| Asset ID : | 8a851b01-e8c5-4d56-a833-9225b1afbb0f |

### Activity

| | |
|---|---|
| Last User Login : | July 3, 2019 12:34 pm |
| Last System Boot : | - |
| First Seen : | Jun 19, 2019 01:43 am |
| Last Seen : | a minute ago 12:34 pm |



Qualys. Enterprise

Asset Details: 113323-T470P

All asset data collected by passive scanner. Learn more.

## Asset Summary

001142-Z381N

Microsoft Windows 10

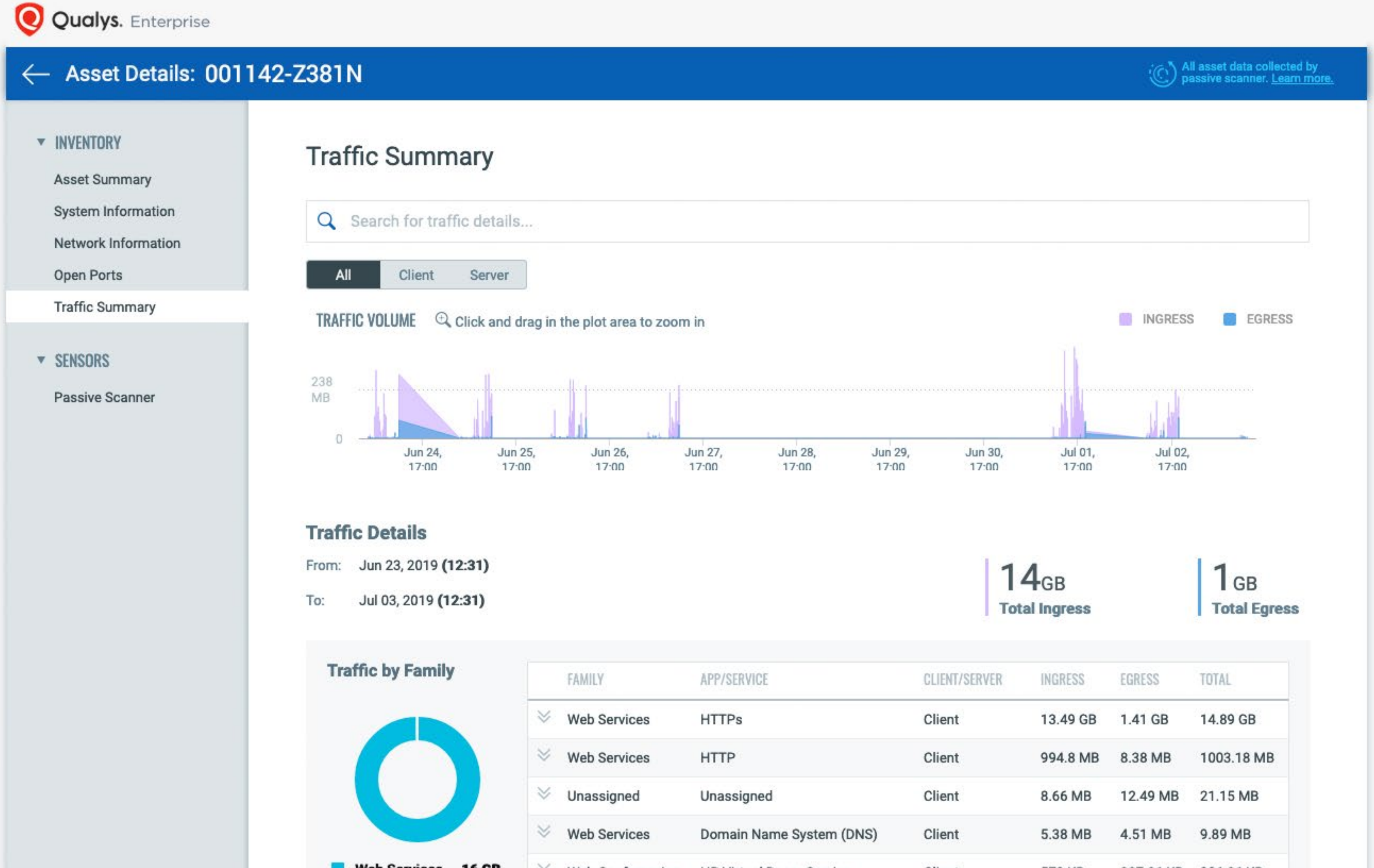
Unidentified

**Identification**

| | |
|---|---|
| Hostname : | 001142-Z381N |
| FQDN : | 001142-Z381N |
| NetBIOS Name : | - |
| Mac Addresses : | 34:41:5d:2a:b9:58 |
| IPv4 Addresses : | 192.168.251.66 |
| IPv6 Addresses : | fe80::c418:12cc:2016:68fe |
| Asset ID : | 8a851b01-e8c5-4d56-a833-9225b1afbb0f |

**Activity**

| | |
|---|---|
| Last User Login : | July 3, 2019 12:34 pm |
| Last System Boot : | - |
| First Seen : | Jun 19, 2019 01:43 am |
| Last Seen : | a minute ago 12:34 pm |



Asset Details: 001142-Z381N

## Traffic Summary

### Traffic Details

From: Jun 23, 2019 **(12:31)**

To: Jul 03, 2019 **(12:31)**

14GB **Total Ingress**

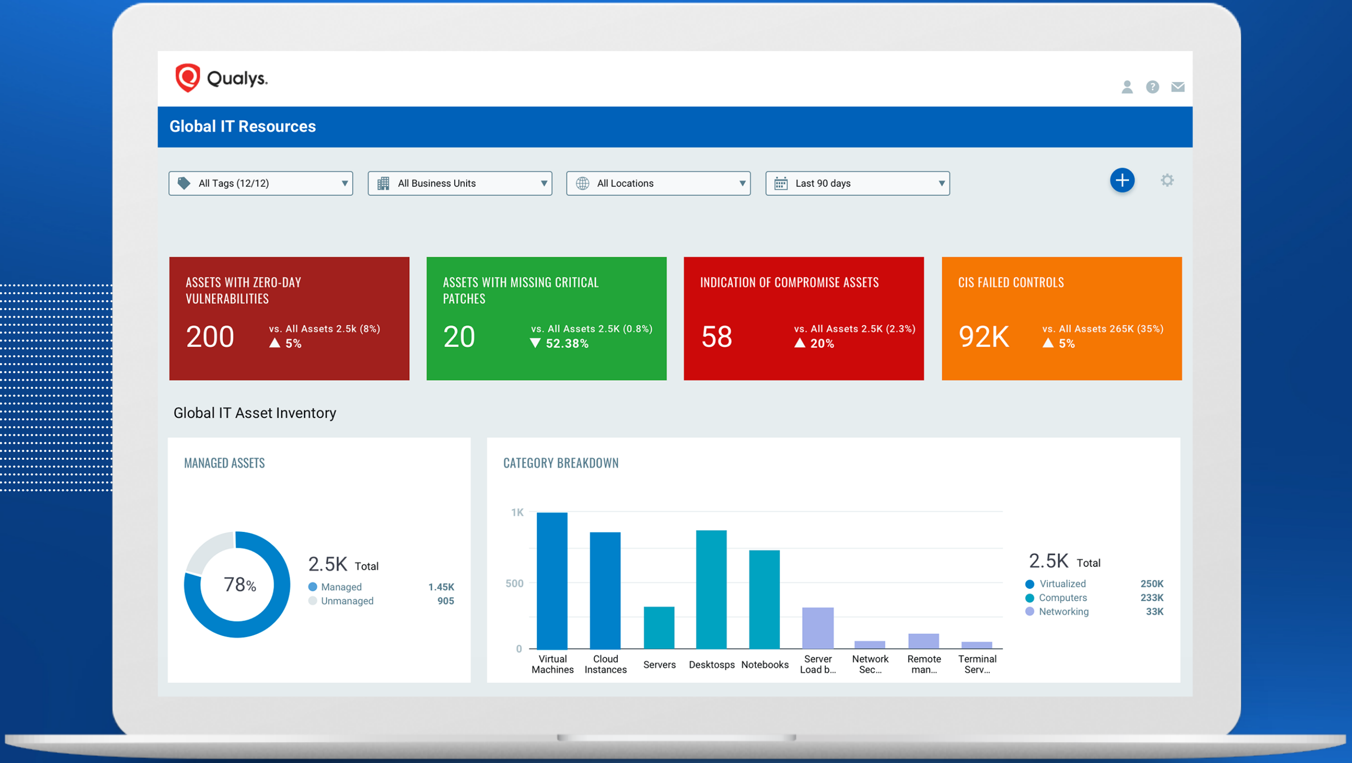
1GB **Total Egress**

**Traffic by Family**

| FAMILY | APP/SERVICE | CLIENT/SERVER | INGRESS | EGRESS | TOTAL |
|---|---|---|---|---|---|
| Web Services | HTTPs | Client | 13.49 GB | 1.41 GB | 14.89 GB |
| Web Services | HTTP | Client | 994.8 MB | 8.38 MB | 1003.18 MB |
| Unassigned | Unassigned | Client | 8.66 MB | 12.49 MB | 21.15 MB |
| Web Services | Domain Name System (DNS) | Client | 5.38 MB | 4.51 MB | 9.89 MB |

How is this possible?

# CLOUD-BASED ARCHITECTURE



Qualys.

## Global IT Resources

All Tags (12/12) ▾ | All Business Units ▾ | All Locations ▾ | Last 90 days ▾

**ASSETS WITH ZERO-DAY VULNERABILITIES**
200 vs. All Assets 2.5k (8%) ▲ 5%

**ASSETS WITH MISSING CRITICAL PATCHES**
20 vs. All Assets 2.5K (0.8%) ▼ 52.38%

**INDICATION OF COMPROMISE ASSETS**
58 vs. All Assets 2.5K (2.3%) ▲ 20%

**CIS FAILED CONTROLS**
92K vs. All Assets 265K (35%) ▲ 5%

### Global IT Asset Inventory

MANAGED ASSETS

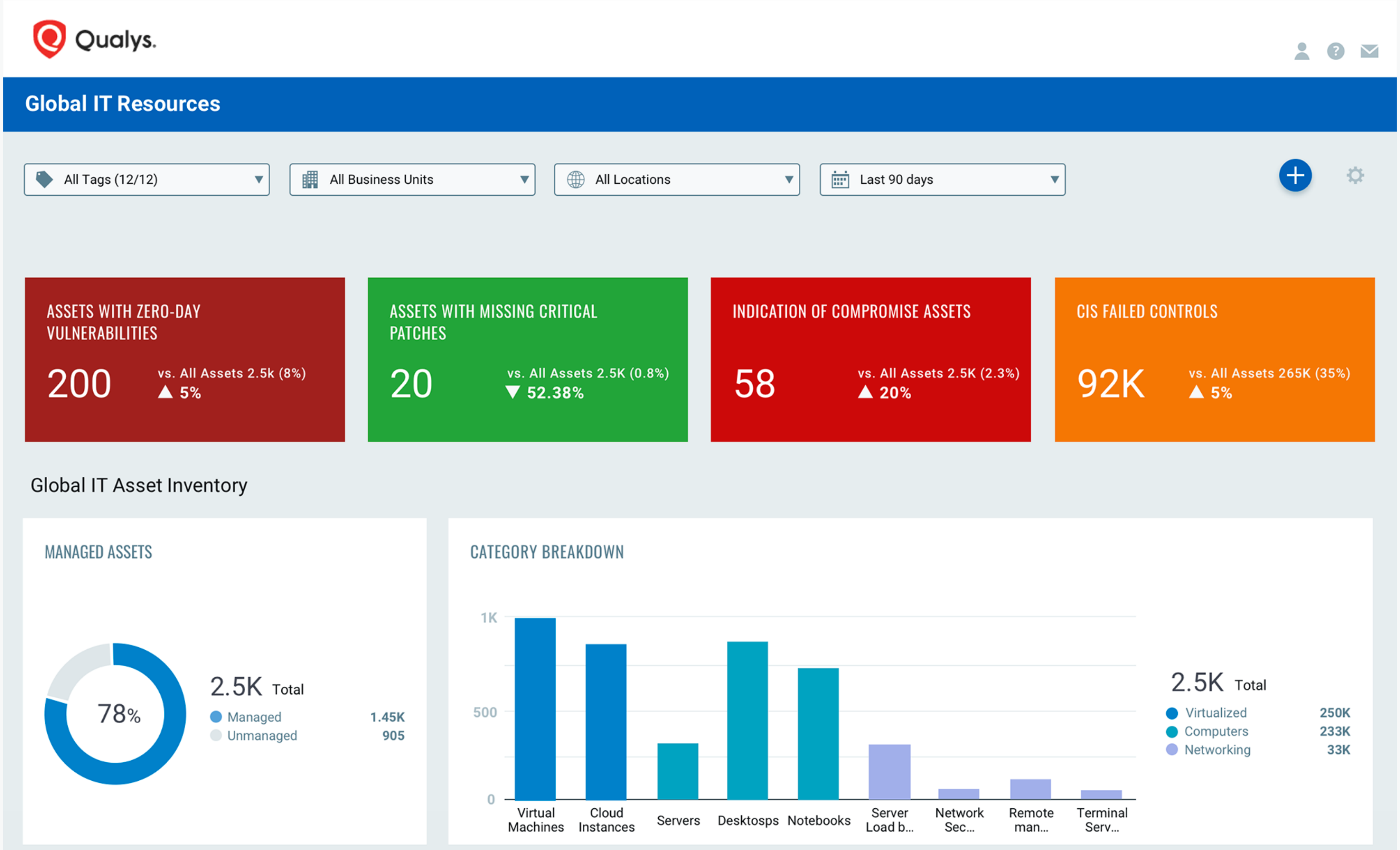
2.5K Total

| | |
|---|---|
| ● Managed | 1.45K |
| ● Unmanaged | 905 |

CATEGORY BREAKDOWN

2.5K Total

| | |
|---|---|
| ● Virtualized | 250K |
| ● Computers | 233K |
| ● Networking | 33K |



Qualys.

Global IT Resources

All Tags (12/12) ▾ | All Business Units ▾ | All Locations ▾ | Last 90 days ▾

ASSETS WITH ZERO-DAY VULNERABILITIES

200 vs. All Assets 2.5k (8%) ▲ 5%

ASSETS WITH MISSING CRITICAL PATCHES

20 vs. All Assets 2.5K (0.8%) ▼ 52.38%

INDICATION OF COMPROMISE ASSETS

58 vs. All Assets 2.5K (2.3%) ▲ 20%

CIS FAILED CONTROLS

92K vs. All Assets 265K (35%) ▲ 5%

Global IT Asset Inventory

MANAGED ASSETS

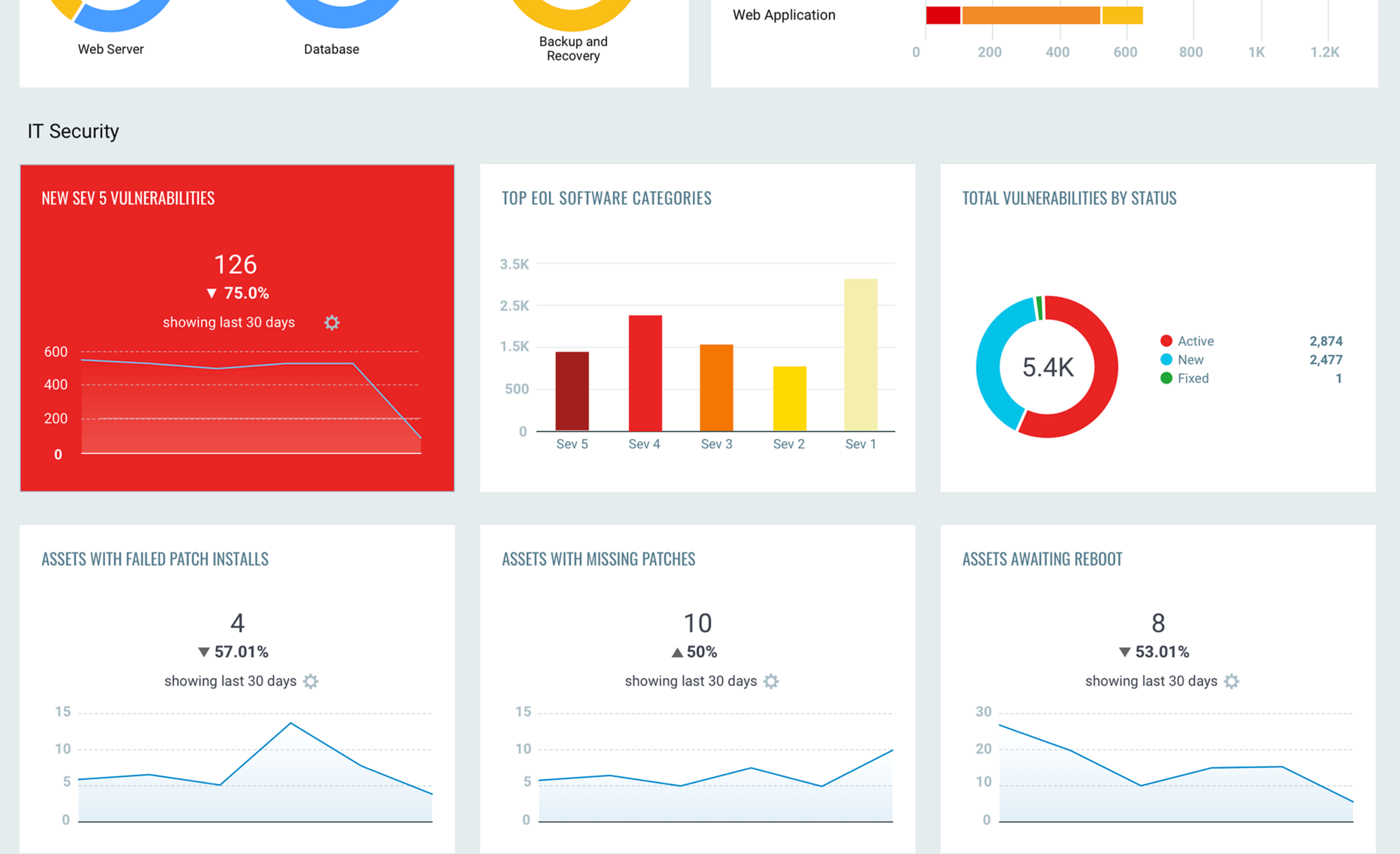
2.5K Total

| | |
|---|---|
| ● Managed | 1.45K |
| ● Unmanaged | 905 |

CATEGORY BREAKDOWN

2.5K Total

| | |
|---|---|
| ● Virtualized | 250K |
| ● Computers | 233K |
| ● Networking | 33K |



IT Security

NEW SEV 5 VULNERABILITIES

126
▼ 75.0%
showing last 30 days

TOP EOL SOFTWARE CATEGORIES

TOTAL VULNERABILITIES BY STATUS

| | |
|---|---|
| ● Active | 2,874 |
| ● New | 2,477 |
| ● Fixed | 1 |

ASSETS WITH FAILED PATCH INSTALLS

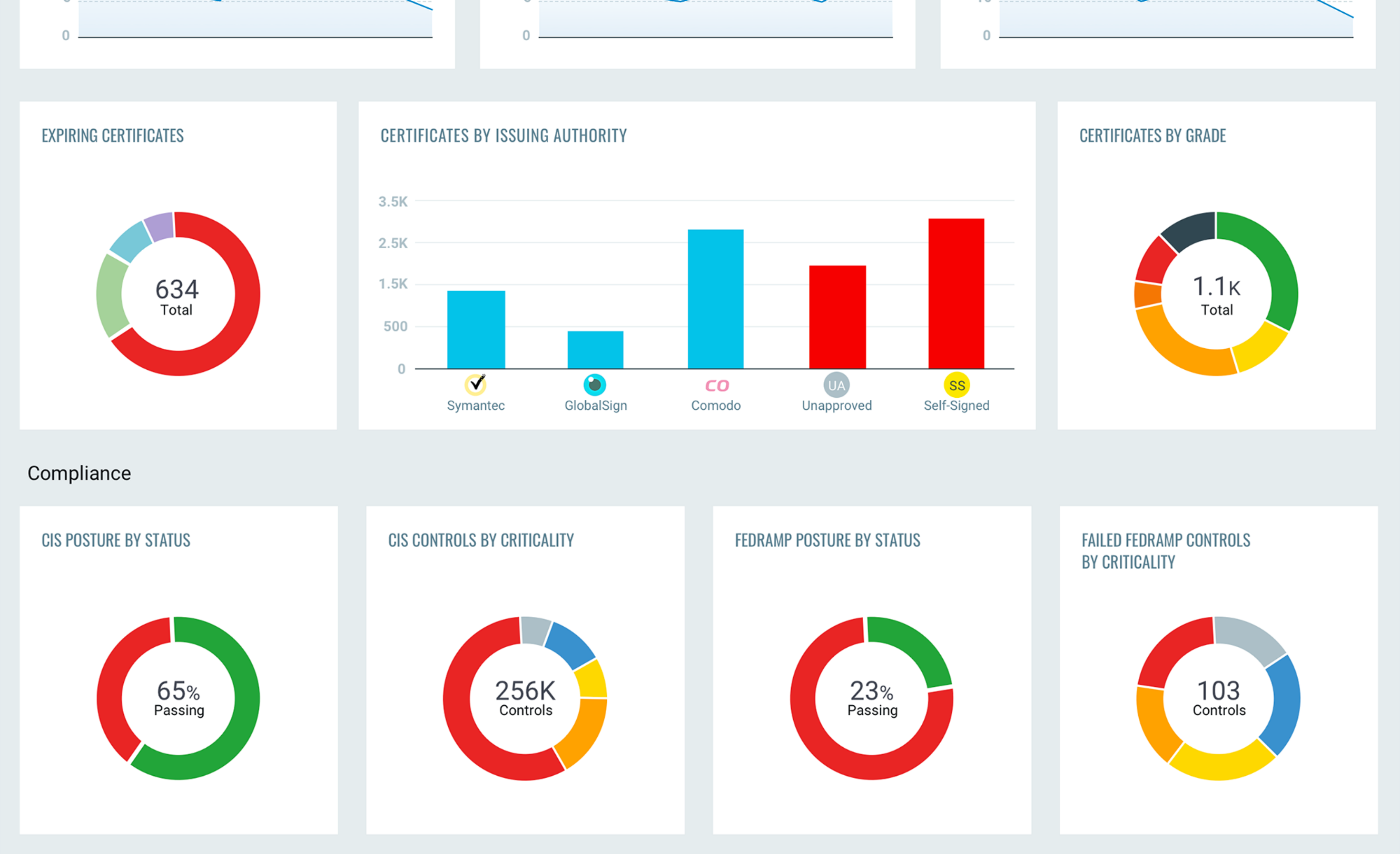
4
▼ 57.01%
showing last 30 days

ASSETS WITH MISSING PATCHES

10
▲ 50%
showing last 30 days

ASSETS AWAITING REBOOT

8
▼ 53.01%
showing last 30 days



EXPIRING CERTIFICATES

CERTIFICATES BY ISSUING AUTHORITY

CERTIFICATES BY GRADE

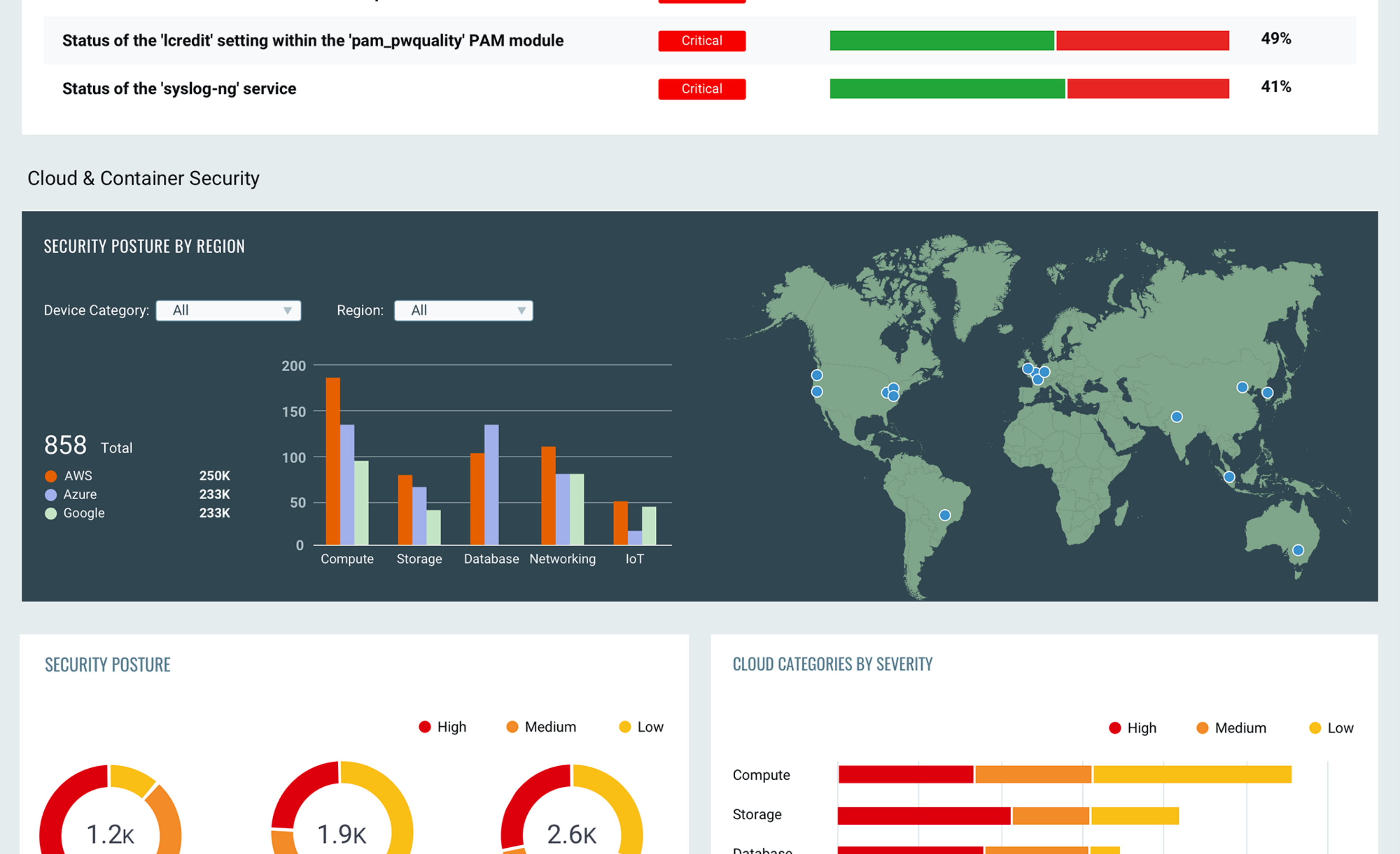
Compliance

CIS POSTURE BY STATUS

CIS CONTROLS BY CRITICALITY

FEDRAMP POSTURE BY STATUS

FAILED FEDRAMP CONTROLS BY CRITICALITY



| | | | |
|---|---|---|---|
| Status of the 'lcredit' setting within the 'pam_pwquality' PAM module | Critical | 🟩🟥 | 49% |
| Status of the 'syslog-ng' service | Critical | 🟩🟥 | 41% |

## Cloud & Container Security

### SECURITY POSTURE BY REGION

Device Category: All

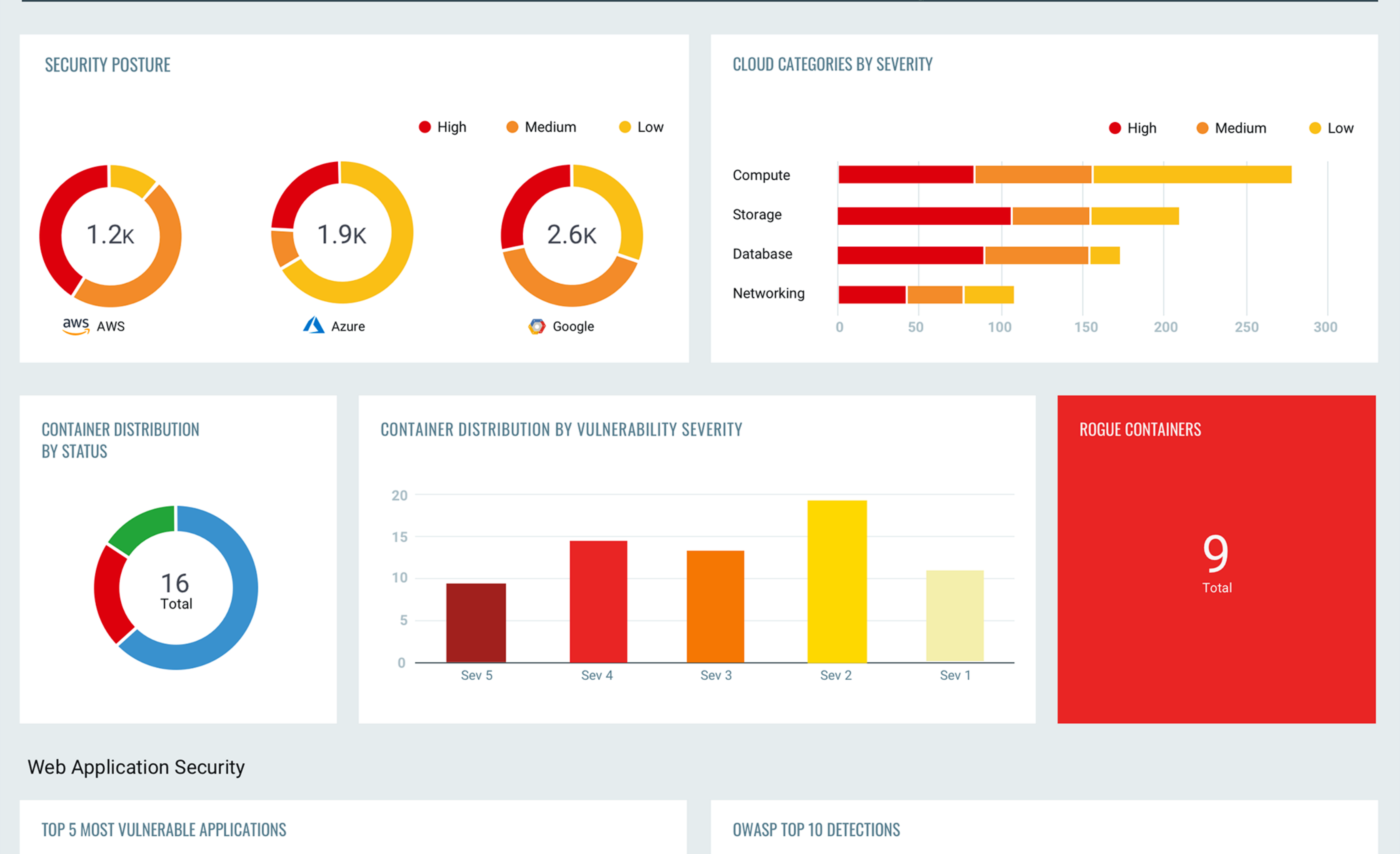
Region: All

858 Total

| | |
|---|---|
| ● AWS | 250K |
| ● Azure | 233K |
| ● Google | 233K |

### SECURITY POSTURE

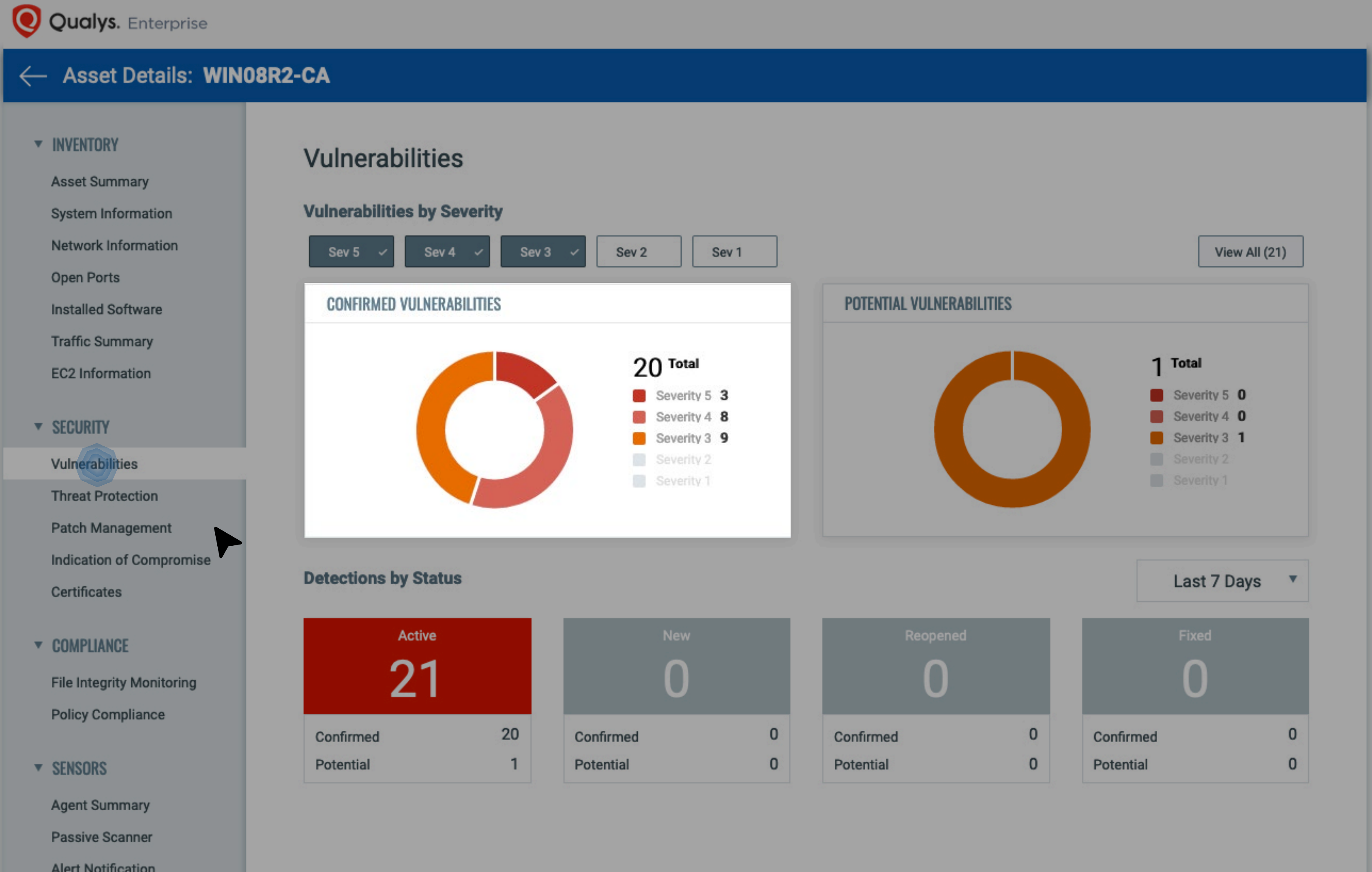
### CLOUD CATEGORIES BY SEVERITY


SECURITY POSTURE
● High
● Medium
● Low
1.2K
aws AWS
1.9K
Azure
2.6K
Google
CLOUD CATEGORIES BY SEVERITY
● High
● Medium
● Low
Compute
Storage
Database
Networking
0
50
100
150
200
250
300
CONTAINER DISTRIBUTION BY STATUS
16
Total
CONTAINER DISTRIBUTION BY VULNERABILITY SEVERITY
20
15
10
5
0
Sev 5
Sev 4
Sev 3
Sev 2
Sev 1
ROGUE CONTAINERS
9
Total
Web Application Security
TOP 5 MOST VULNERABLE APPLICATIONS
OWASP TOP 10 DETECTIONS

# DEMO

Responding to a suspicious device

11:04



Asset Details: WIN08R2-CA

Vulnerabilities

Vulnerabilities by Severity

CONFIRMED VULNERABILITIES

20 Total

| | | |
|---|---|---|
| 🟥 | Severity 5 | 3 |
| 🟥 | Severity 4 | 8 |
| 🟧 | Severity 3 | 9 |
| □ | Severity 2 | |
| □ | Severity 1 | |

POTENTIAL VULNERABILITIES

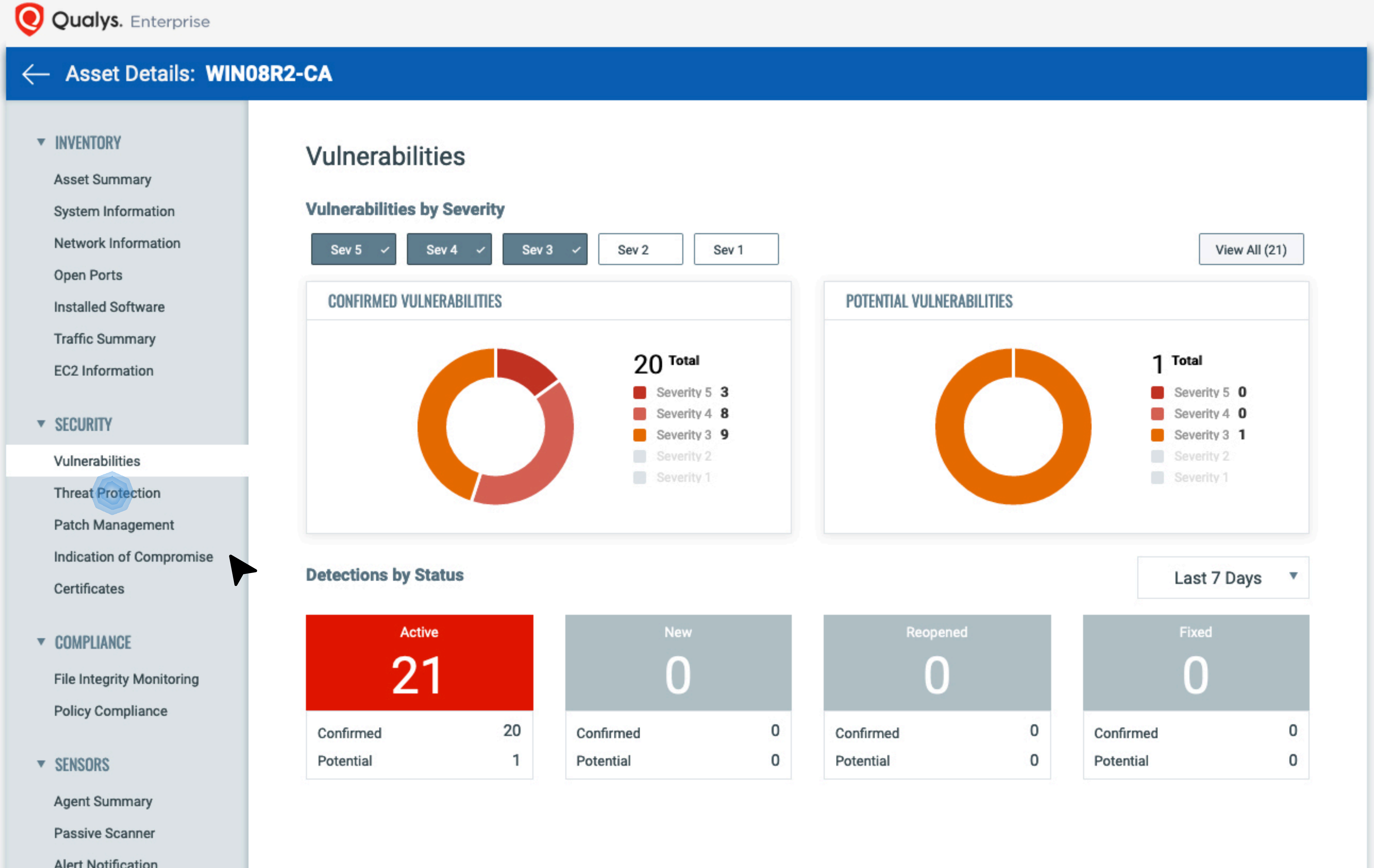
1 Total

| | | |
|---|---|---|
| 🟥 | Severity 5 | 0 |
| 🟥 | Severity 4 | 0 |
| 🟧 | Severity 3 | 1 |
| □ | Severity 2 | |
| □ | Severity 1 | |

Detections by Status

Last 7 Days ▾

| Active | New | Reopened | Fixed |
|---|---|---|---|
| 21 | 0 | 0 | 0 |
| Confirmed 20 | Confirmed 0 | Confirmed 0 | Confirmed 0 |
| Potential 1 | Potential 0 | Potential 0 | Potential 0 |



Qualys. Enterprise

← Asset Details: WIN08R2-CA

▼ INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Traffic Summary
- EC2 Information

▼ SECURITY
- Vulnerabilities
- Threat Protection
- Patch Management
- Indication of Compromise
- Certificates

▼ COMPLIANCE
- File Integrity Monitoring
- Policy Compliance

▼ SENSORS
- Agent Summary
- Passive Scanner
- Alert Notification

Vulnerabilities

Vulnerabilities by Severity

Sev 5 ✓ | Sev 4 ✓ | Sev 3 ✓ | Sev 2 | Sev 1 | View All (21)

CONFIRMED VULNERABILITIES

20 Total

| | | |
|---|---|---|
| 🟥 | Severity 5 | 3 |
| 🟥 | Severity 4 | 8 |
| 🟧 | Severity 3 | 9 |
| ⬜ | Severity 2 | |
| ⬜ | Severity 1 | |

POTENTIAL VULNERABILITIES

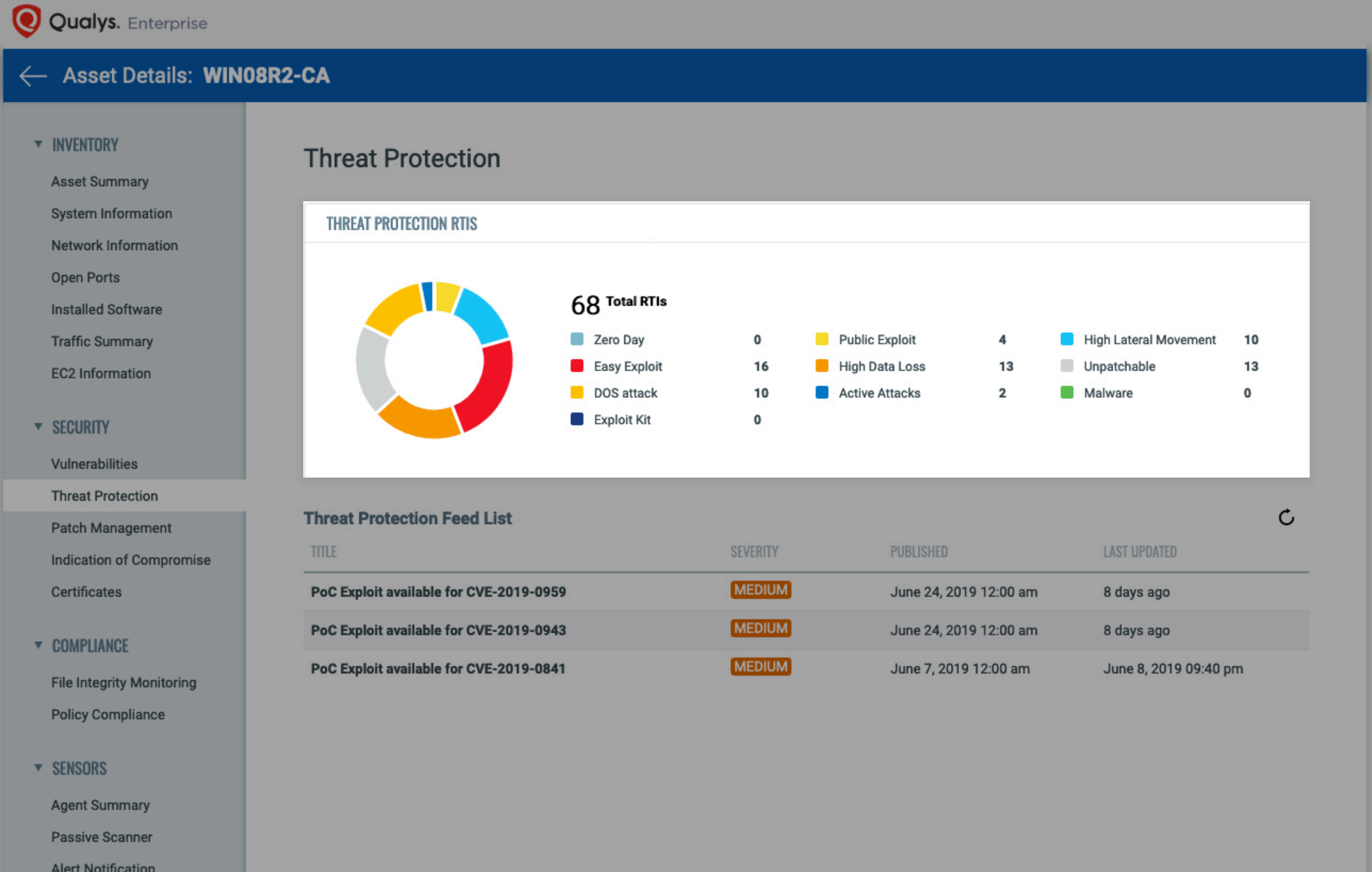
1 Total

| | | |
|---|---|---|
| 🟥 | Severity 5 | 0 |
| 🟥 | Severity 4 | 0 |
| 🟧 | Severity 3 | 1 |
| ⬜ | Severity 2 | |
| ⬜ | Severity 1 | |

Detections by Status

Last 7 Days ▼

| | Active | New | Reopened | Fixed |
|---|---|---|---|---|
| | 21 | 0 | 0 | 0 |
| Confirmed | 20 | 0 | 0 | 0 |
| Potential | 1 | 0 | 0 | 0 |



Asset Details: WIN08R2-CA

## Threat Protection

THREAT PROTECTION RTIS

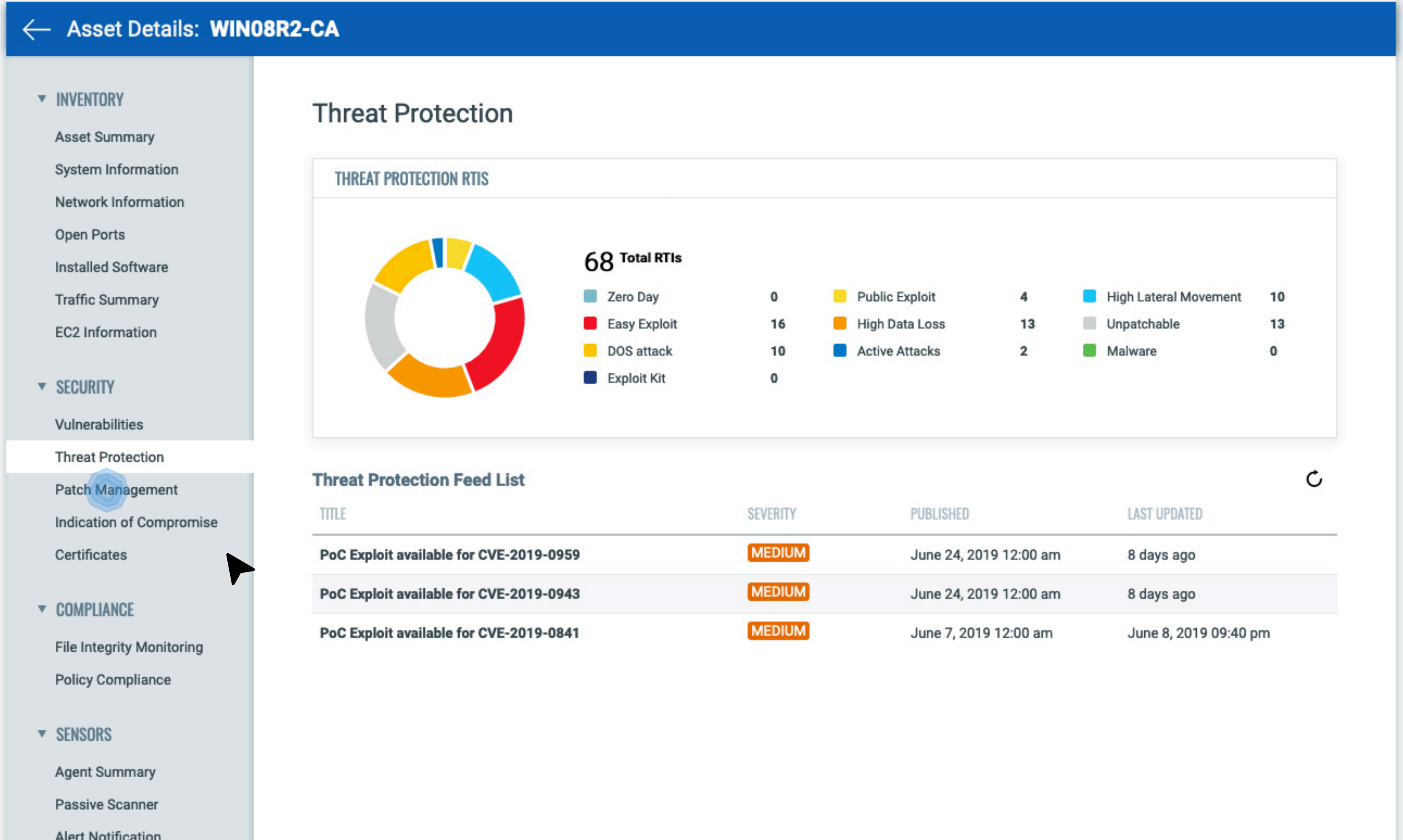
68 Total RTIs

| | | | | | |
|---|---|---|---|---|---|
| Zero Day | 0 | Public Exploit | 4 | High Lateral Movement | 10 |
| Easy Exploit | 16 | High Data Loss | 13 | Unpatchable | 13 |
| DOS attack | 10 | Active Attacks | 2 | Malware | 0 |
| Exploit Kit | 0 | | | | |

### Threat Protection Feed List

| TITLE | SEVERITY | PUBLISHED | LAST UPDATED |
|---|---|---|---|
| PoC Exploit available for CVE-2019-0959 | MEDIUM | June 24, 2019 12:00 am | 8 days ago |
| PoC Exploit available for CVE-2019-0943 | MEDIUM | June 24, 2019 12:00 am | 8 days ago |
| PoC Exploit available for CVE-2019-0841 | MEDIUM | June 7, 2019 12:00 am | June 8, 2019 09:40 pm |

Qualys. Enterprise



## Threat Protection

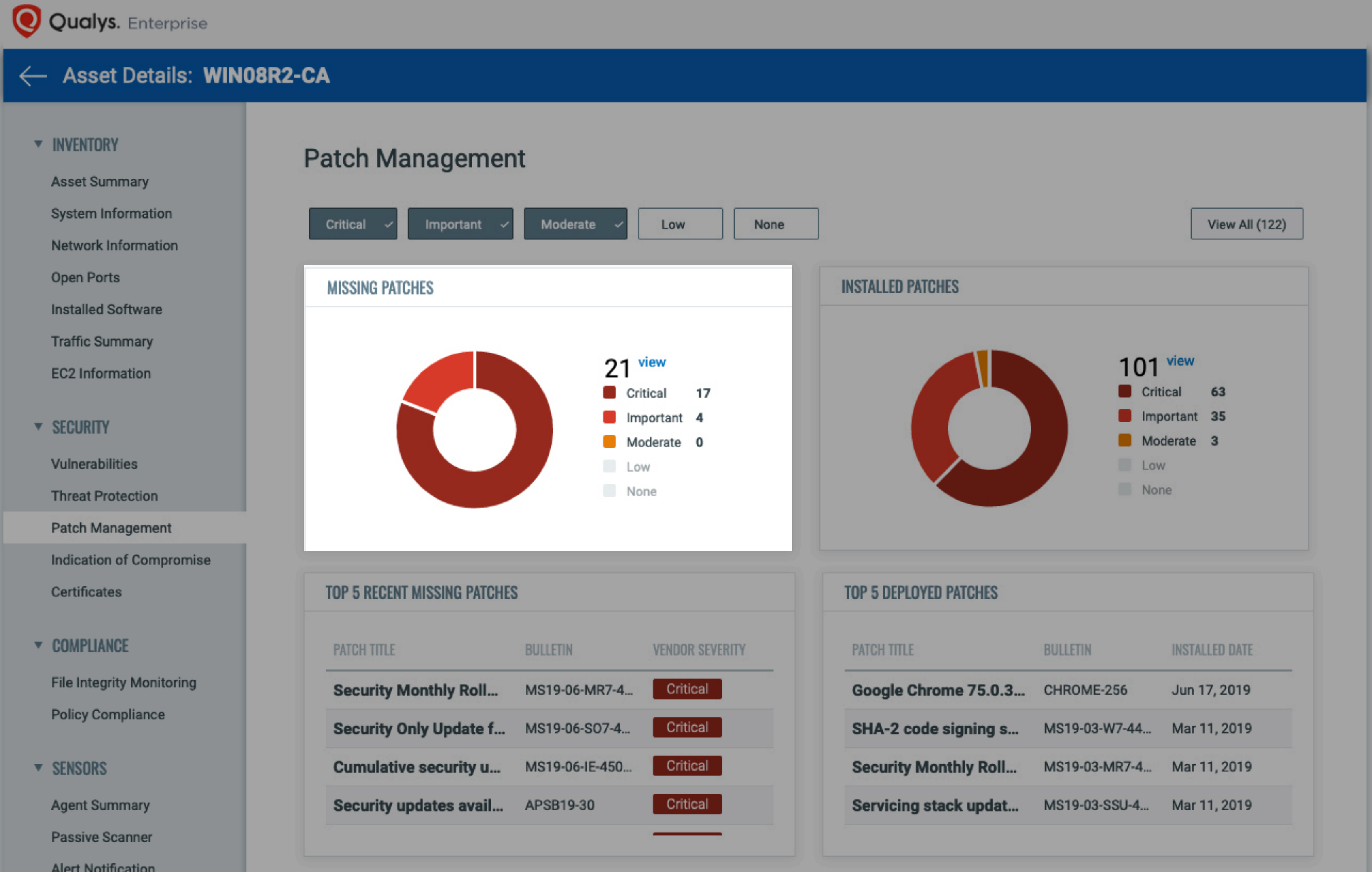
THREAT PROTECTION RTIS

68 Total RTIs

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 🟦 | Zero Day | 0 | 🟨 | Public Exploit | 4 | 🟦 | High Lateral Movement | 10 |
| 🟥 | Easy Exploit | 16 | 🟧 | High Data Loss | 13 | ⬜ | Unpatchable | 13 |
| 🟨 | DOS attack | 10 | 🟦 | Active Attacks | 2 | 🟩 | Malware | 0 |
| 🟦 | Exploit Kit | 0 | | | | | | |

Threat Protection Feed List

| TITLE | SEVERITY | PUBLISHED | LAST UPDATED |
|---|---|---|---|
| PoC Exploit available for CVE-2019-0959 | MEDIUM | June 24, 2019 12:00 am | 8 days ago |
| PoC Exploit available for CVE-2019-0943 | MEDIUM | June 24, 2019 12:00 am | 8 days ago |
| PoC Exploit available for CVE-2019-0841 | MEDIUM | June 7, 2019 12:00 am | June 8, 2019 09:40 pm |



Qualys. Enterprise

## Asset Details: WIN08R2-CA

▾ INVENTORY

- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Traffic Summary
- EC2 Information

▾ SECURITY

- Vulnerabilities
- Threat Protection
- Patch Management
- Indication of Compromise
- Certificates

▾ COMPLIANCE

- File Integrity Monitoring
- Policy Compliance

▾ SENSORS

- Agent Summary
- Passive Scanner
- Alert Notification

## Patch Management

Critical ✓ Important ✓ Moderate ✓ Low None View All (122)

### MISSING PATCHES

21 view

| | | |
|---|---|---|
| ■ | Critical | 17 |
| ■ | Important | 4 |
| ■ | Moderate | 0 |
| □ | Low | |
| □ | None | |

### INSTALLED PATCHES

101 view

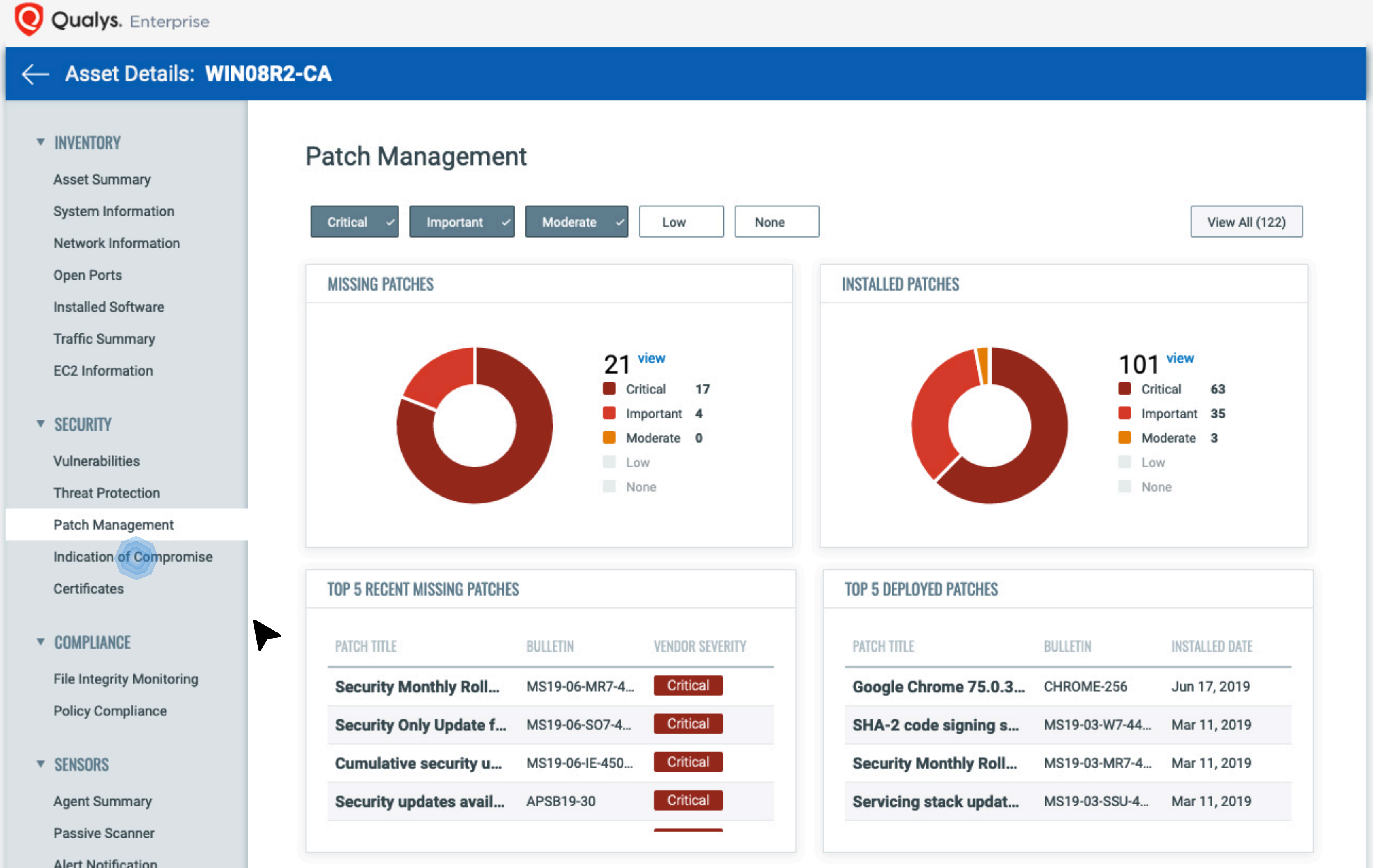
| | | |
|---|---|---|
| ■ | Critical | 63 |
| ■ | Important | 35 |
| ■ | Moderate | 3 |
| □ | Low | |
| □ | None | |

### TOP 5 RECENT MISSING PATCHES

| PATCH TITLE | BULLETIN | VENDOR SEVERITY |
|---|---|---|
| Security Monthly Roll... | MS19-06-MR7-4... | Critical |
| Security Only Update f... | MS19-06-SO7-4... | Critical |
| Cumulative security u... | MS19-06-IE-450... | Critical |
| Security updates avail... | APSB19-30 | Critical |

### TOP 5 DEPLOYED PATCHES

| PATCH TITLE | BULLETIN | INSTALLED DATE |
|---|---|---|
| Google Chrome 75.0.3... | CHROME-256 | Jun 17, 2019 |
| SHA-2 code signing s... | MS19-03-W7-44... | Mar 11, 2019 |
| Security Monthly Roll... | MS19-03-MR7-4... | Mar 11, 2019 |
| Servicing stack updat... | MS19-03-SSU-4... | Mar 11, 2019 |



Qualys. Enterprise

← Asset Details: **WIN08R2-CA**

## Patch Management

Critical ✓ | Important ✓ | Moderate ✓ | Low | None | View All (122)

### MISSING PATCHES

21 view

| | | |
|---|---|---|
| 🟥 | Critical | 17 |
| 🟥 | Important | 4 |
| 🟧 | Moderate | 0 |
| □ | Low | |
| □ | None | |

### INSTALLED PATCHES

101 view

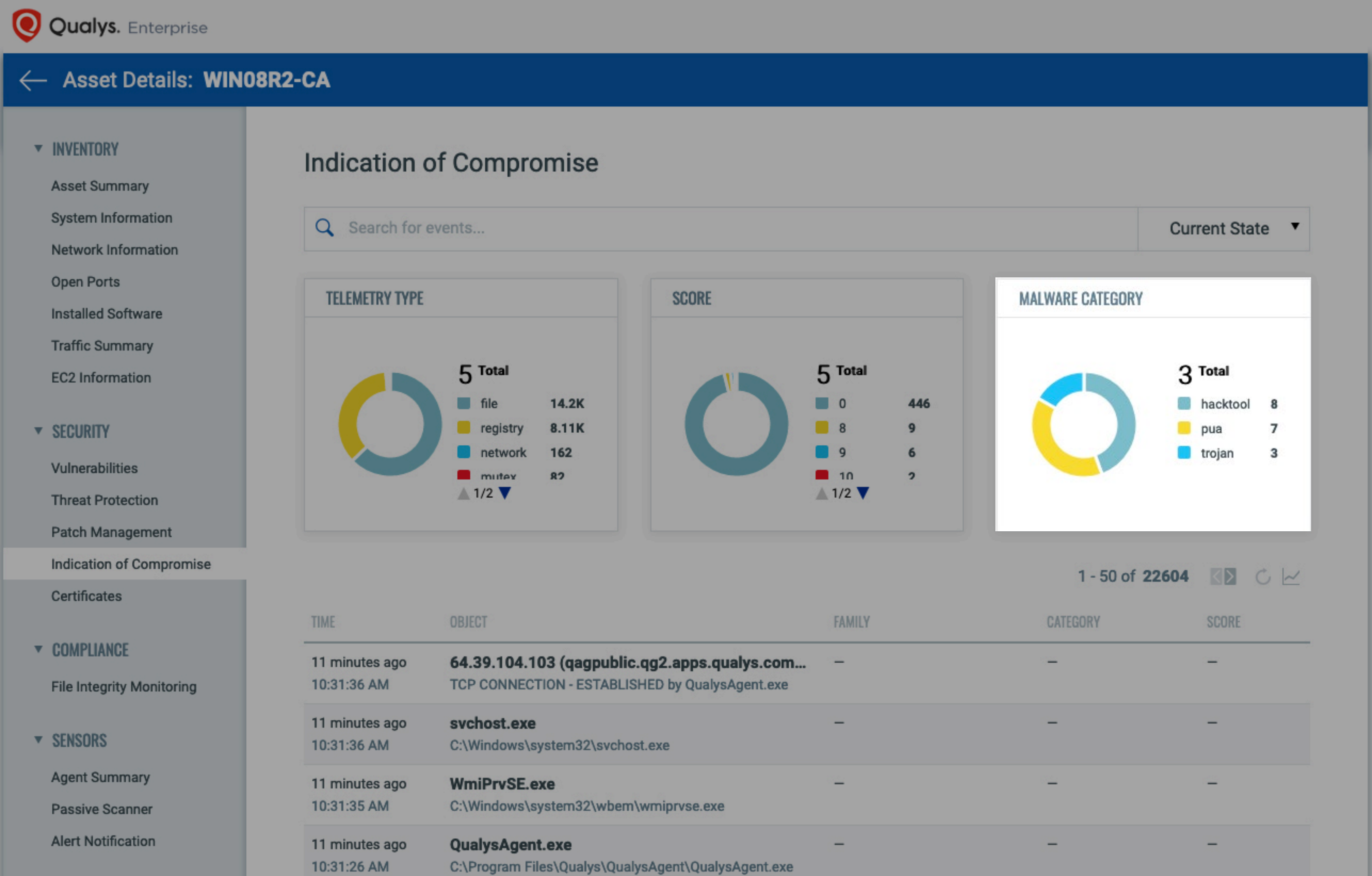
| | | |
|---|---|---|
| 🟥 | Critical | 63 |
| 🟥 | Important | 35 |
| 🟧 | Moderate | 3 |
| □ | Low | |
| □ | None | |

### TOP 5 RECENT MISSING PATCHES

| PATCH TITLE | BULLETIN | VENDOR SEVERITY |
|---|---|---|
| **Security Monthly Roll...** | MS19-06-MR7-4... | Critical |
| **Security Only Update f...** | MS19-06-SO7-4... | Critical |
| **Cumulative security u...** | MS19-06-IE-450... | Critical |
| **Security updates avail...** | APSB19-30 | Critical |

### TOP 5 DEPLOYED PATCHES

| PATCH TITLE | BULLETIN | INSTALLED DATE |
|---|---|---|
| **Google Chrome 75.0.3...** | CHROME-256 | Jun 17, 2019 |
| **SHA-2 code signing s...** | MS19-03-W7-44... | Mar 11, 2019 |
| **Security Monthly Roll...** | MS19-03-MR7-4... | Mar 11, 2019 |
| **Servicing stack updat...** | MS19-03-SSU-4... | Mar 11, 2019 |



Qualys. Enterprise

Asset Details: WIN08R2-CA

▾ INVENTORY
- Asset Summary
- System Information
- Network Information
- Open Ports
- Installed Software
- Traffic Summary
- EC2 Information

▾ SECURITY
- Vulnerabilities
- Threat Protection
- Patch Management
- Indication of Compromise
- Certificates

▾ COMPLIANCE
- File Integrity Monitoring

▾ SENSORS
- Agent Summary
- Passive Scanner
- Alert Notification

## Indication of Compromise

Search for events... | Current State ▾

**TELEMETRY TYPE** — 5 Total

| | | |
|---|---|---|
| 🟦 | file | 14.2K |
| 🟨 | registry | 8.11K |
| 🟦 | network | 162 |
| 🟥 | mutex | 82 |

▲ 1/2 ▼

**SCORE** — 5 Total

| | | |
|---|---|---|
| 🟦 | 0 | 446 |
| 🟨 | 8 | 9 |
| 🟦 | 9 | 6 |
| 🟥 | 10 | 2 |

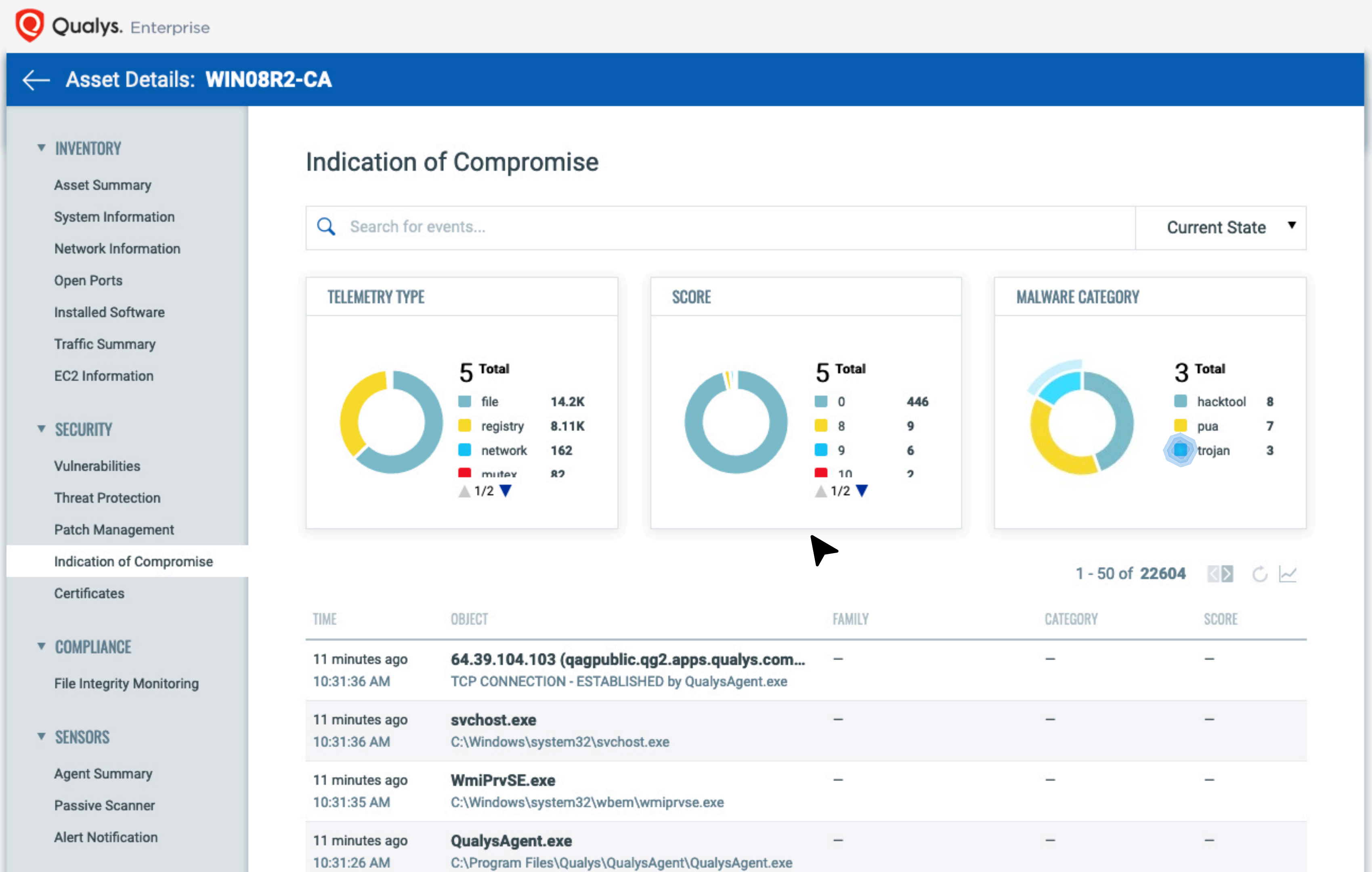
▲ 1/2 ▼

**MALWARE CATEGORY** — 3 Total

| | | |
|---|---|---|
| 🟦 | hacktool | 8 |
| 🟨 | pua | 7 |
| 🟦 | trojan | 3 |

1 - 50 of 22604

| TIME | OBJECT | FAMILY | CATEGORY | SCORE |
|---|---|---|---|---|
| 11 minutes ago<br>10:31:36 AM | **64.39.104.103 (qagpublic.qg2.apps.qualys.com...**<br>TCP CONNECTION - ESTABLISHED by QualysAgent.exe | – | – | – |
| 11 minutes ago<br>10:31:36 AM | **svchost.exe**<br>C:\Windows\system32\svchost.exe | – | – | – |
| 11 minutes ago<br>10:31:35 AM | **WmiPrvSE.exe**<br>C:\Windows\system32\wbem\wmiprvse.exe | – | – | – |
| 11 minutes ago<br>10:31:26 AM | **QualysAgent.exe**<br>C:\Program Files\Qualys\QualysAgent\QualysAgent.exe | – | – | – |



Qualys. Enterprise

Asset Details: WIN08R2-CA

## Indication of Compromise

Search for events...

Current State ▼

**TELEMETRY TYPE**

5 Total

| | | |
|---|---|---|
| 🟦 | file | 14.2K |
| 🟨 | registry | 8.11K |
| 🟦 | network | 162 |
| 🟥 | mutex | 82 |

▲ 1/2 ▼

**SCORE**

5 Total

| | | |
|---|---|---|
| 🟦 | 0 | 446 |
| 🟨 | 8 | 9 |
| 🟦 | 9 | 6 |
| 🟥 | 10 | 2 |

▲ 1/2 ▼

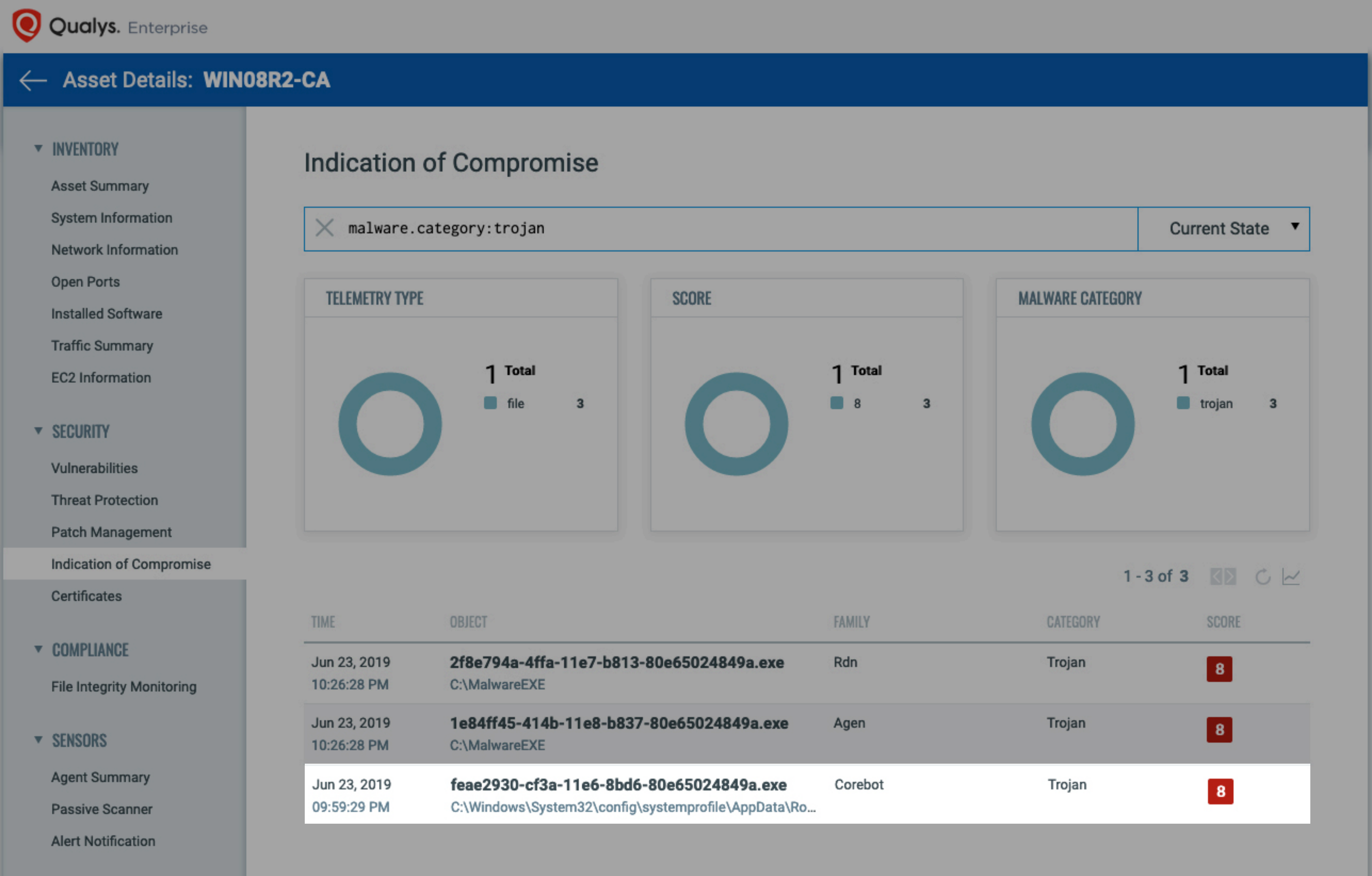
**MALWARE CATEGORY**

3 Total

| | | |
|---|---|---|
| 🟦 | hacktool | 8 |
| 🟨 | pua | 7 |
| 🟦 | trojan | 3 |

1 - 50 of 22604

| TIME | OBJECT | FAMILY | CATEGORY | SCORE |
|---|---|---|---|---|
| 11 minutes ago<br>10:31:36 AM | **64.39.104.103 (qagpublic.qg2.apps.qualys.com...**<br>TCP CONNECTION - ESTABLISHED by QualysAgent.exe | – | – | – |
| 11 minutes ago<br>10:31:36 AM | **svchost.exe**<br>C:\Windows\system32\svchost.exe | – | – | – |
| 11 minutes ago<br>10:31:35 AM | **WmiPrvSE.exe**<br>C:\Windows\system32\wbem\wmiprvse.exe | – | – | – |
| 11 minutes ago<br>10:31:26 AM | **QualysAgent.exe**<br>C:\Program Files\Qualys\QualysAgent\QualysAgent.exe | – | – | – |

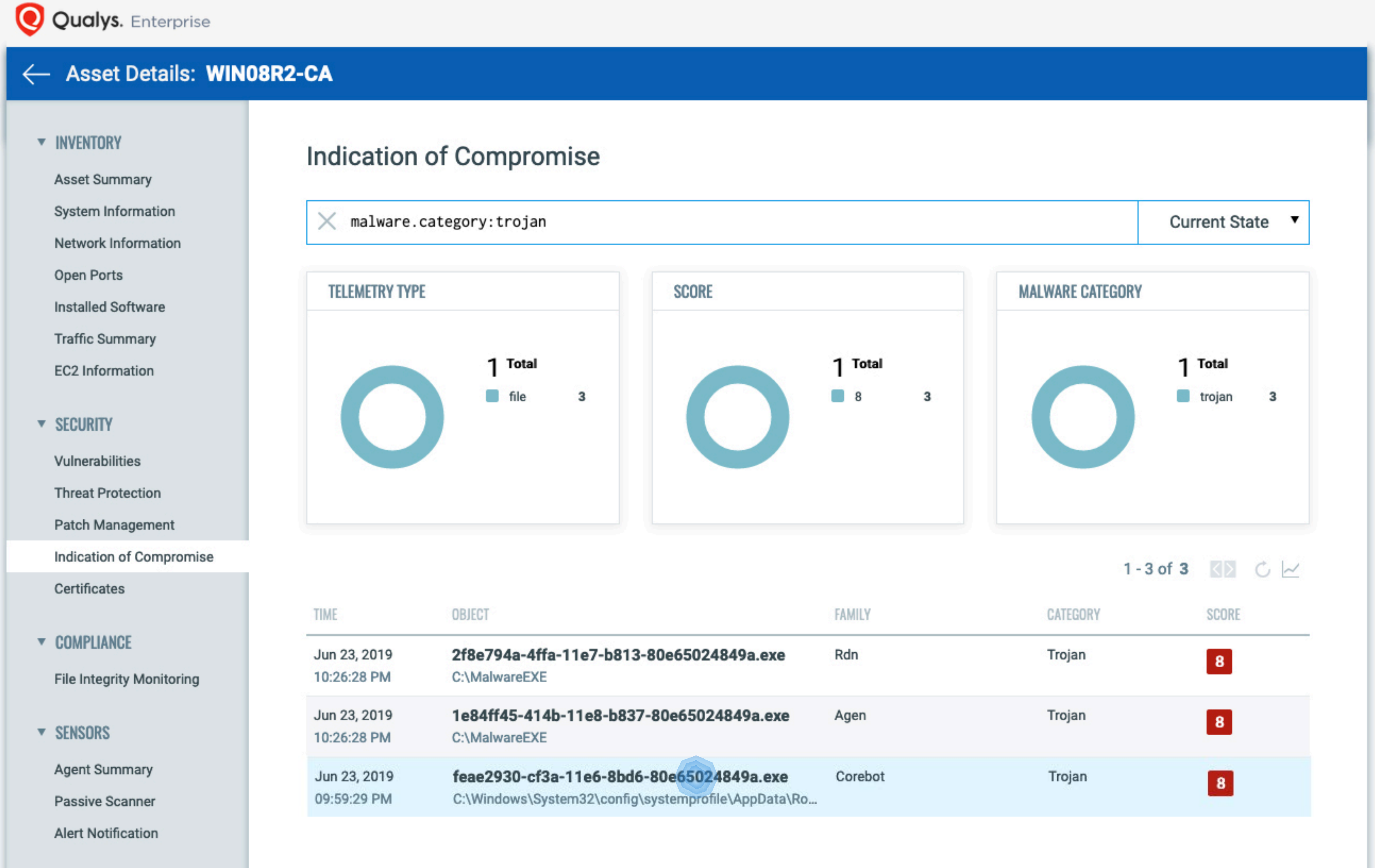


## Indication of Compromise

```
malware.category:trojan
```

Current State ▾

| TIME | OBJECT | FAMILY | CATEGORY | SCORE |
|---|---|---|---|---|
| Jun 23, 2019<br>10:26:28 PM | **2f8e794a-4ffa-11e7-b813-80e65024849a.exe**<br>C:\MalwareEXE | Rdn | Trojan | 8 |
| Jun 23, 2019<br>10:26:28 PM | **1e84ff45-414b-11e8-b837-80e65024849a.exe**<br>C:\MalwareEXE | Agen | Trojan | 8 |
| Jun 23, 2019<br>09:59:29 PM | **feae2930-cf3a-11e6-8bd6-80e65024849a.exe**<br>C:\Windows\System32\config\systemprofile\AppData\Ro... | Corebot | Trojan | 8 |



## Indication of Compromise

`malware.category:trojan`

Current State

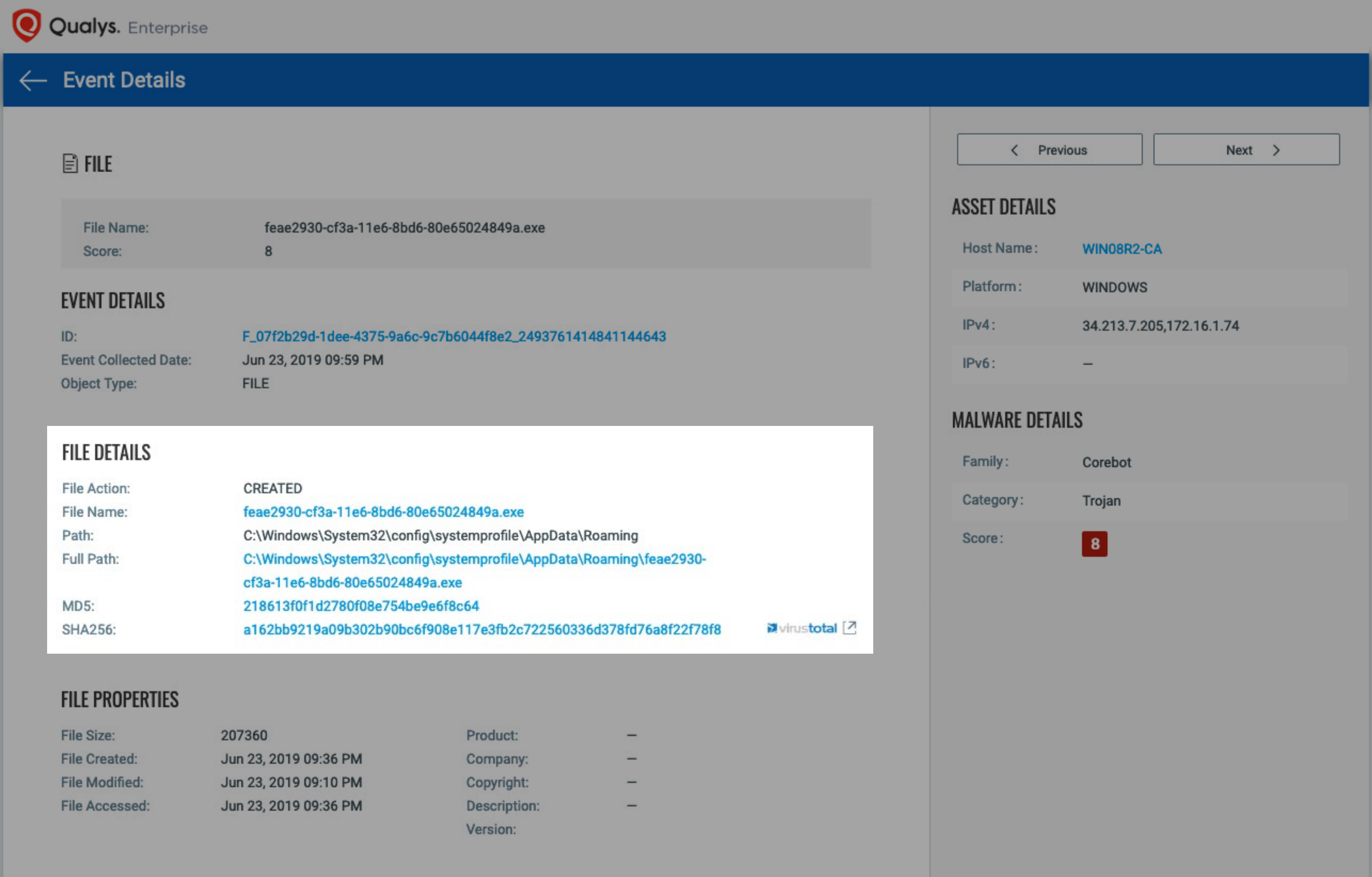
TELEMETRY TYPE
1 Total
🟦 file 3

SCORE
1 Total
🟦 8 3

MALWARE CATEGORY
1 Total
🟦 trojan 3

1 - 3 of 3

| TIME | OBJECT | FAMILY | CATEGORY | SCORE |
|---|---|---|---|---|
| Jun 23, 2019<br>10:26:28 PM | **2f8e794a-4ffa-11e7-b813-80e65024849a.exe**<br>C:\MalwareEXE | Rdn | Trojan | 8 |
| Jun 23, 2019<br>10:26:28 PM | **1e84ff45-414b-11e8-b837-80e65024849a.exe**<br>C:\MalwareEXE | Agen | Trojan | 8 |
| Jun 23, 2019<br>09:59:29 PM | **feae2930-cf3a-11e6-8bd6-80e65024849a.exe**<br>C:\Windows\System32\config\systemprofile\AppData\Ro... | Corebot | Trojan | 8 |



Qualys. Enterprise

## Event Details

### FILE

| | |
|---|---|
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Score: | 8 |

### EVENT DETAILS

| | |
|---|---|
| ID: | F_07f2b29d-1dee-4375-9a6c-9c7b6044f8e2_2493761414841144643 |
| Event Collected Date: | Jun 23, 2019 09:59 PM |
| Object Type: | FILE |

### FILE DETAILS

| | |
|---|---|
| File Action: | CREATED |
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming |
| Full Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming\feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| MD5: | 218613f0f1d2780f08e754be9e6f8c64 |
| SHA256: | a162bb9219a09b302b90bc6f908e117e3fb2c722560336d378fd76a8f22f78f8 |

### FILE PROPERTIES

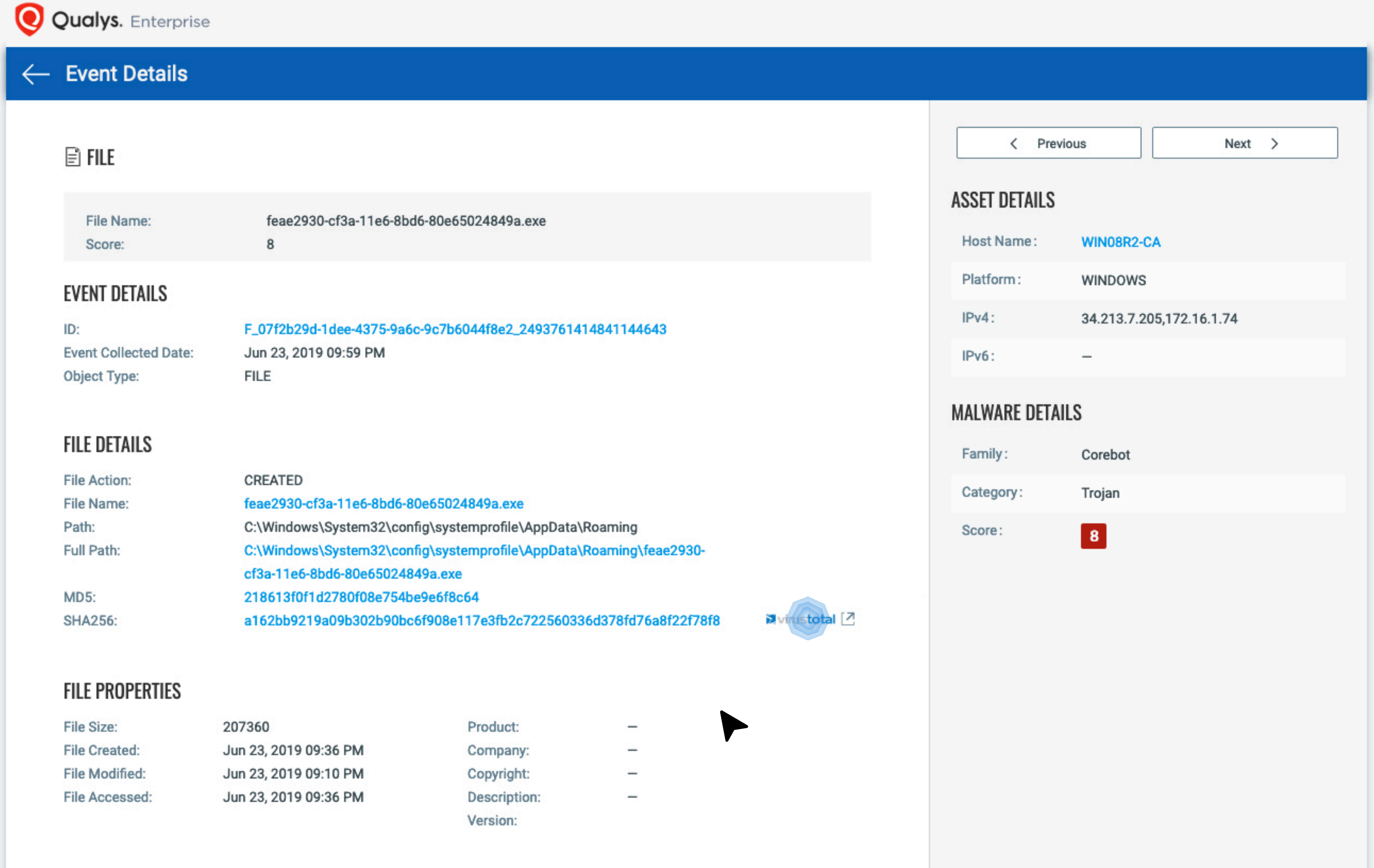
| | | | |
|---|---|---|---|
| File Size: | 207360 | Product: | – |
| File Created: | Jun 23, 2019 09:36 PM | Company: | – |
| File Modified: | Jun 23, 2019 09:10 PM | Copyright: | – |
| File Accessed: | Jun 23, 2019 09:36 PM | Description: | – |
| | | Version: | |

### ASSET DETAILS

| | |
|---|---|
| Host Name: | WIN08R2-CA |
| Platform: | WINDOWS |
| IPv4: | 34.213.7.205,172.16.1.74 |
| IPv6: | – |

### MALWARE DETAILS

| | |
|---|---|
| Family: | Corebot |
| Category: | Trojan |
| Score: | 8 |



Qualys. Enterprise

## Event Details

### FILE

| | |
|---|---|
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Score: | 8 |

### EVENT DETAILS

| | |
|---|---|
| ID: | F_07f2b29d-1dee-4375-9a6c-9c7b6044f8e2_2493761414841144643 |
| Event Collected Date: | Jun 23, 2019 09:59 PM |
| Object Type: | FILE |

### FILE DETAILS

| | |
|---|---|
| File Action: | CREATED |
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming |
| Full Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming\feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| MD5: | 218613f0f1d2780f08e754be9e6f8c64 |
| SHA256: | a162bb9219a09b302b90bc6f908e117e3fb2c722560336d378fd76a8f22f78f8 |

### FILE PROPERTIES

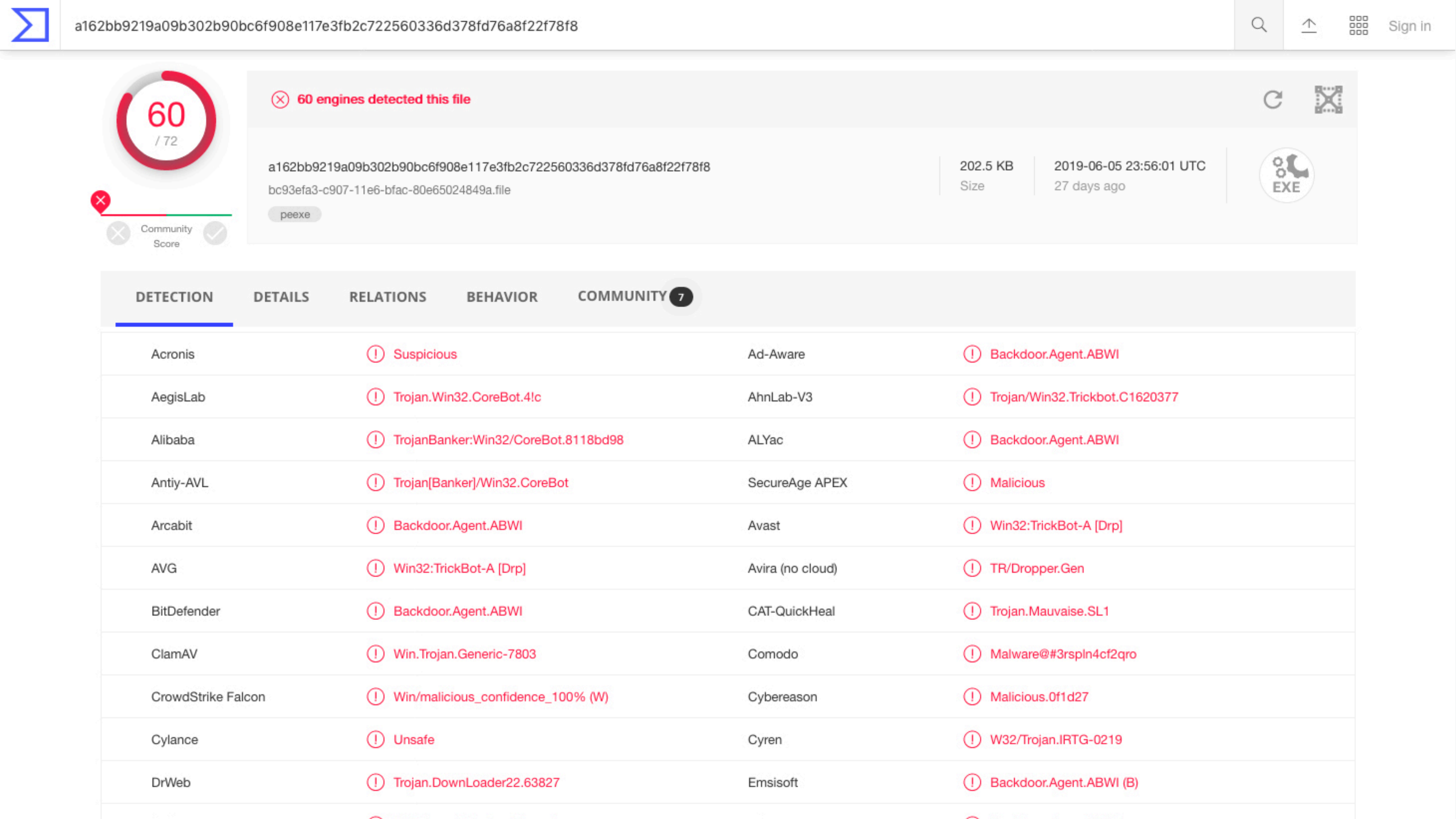
| | | | |
|---|---|---|---|
| File Size: | 207360 | Product: | – |
| File Created: | Jun 23, 2019 09:36 PM | Company: | – |
| File Modified: | Jun 23, 2019 09:10 PM | Copyright: | – |
| File Accessed: | Jun 23, 2019 09:36 PM | Description: | – |
| | | Version: | |

### ASSET DETAILS

| | |
|---|---|
| Host Name: | WIN08R2-CA |
| Platform: | WINDOWS |
| IPv4: | 34.213.7.205,172.16.1.74 |
| IPv6: | – |

### MALWARE DETAILS

| | |
|---|---|
| Family: | Corebot |
| Category: | Trojan |
| Score: | 8 |



a162bb9219a09b302b90bc6f908e117e3fb2c722560336d378fd76a8f22f78f8

60 / 72

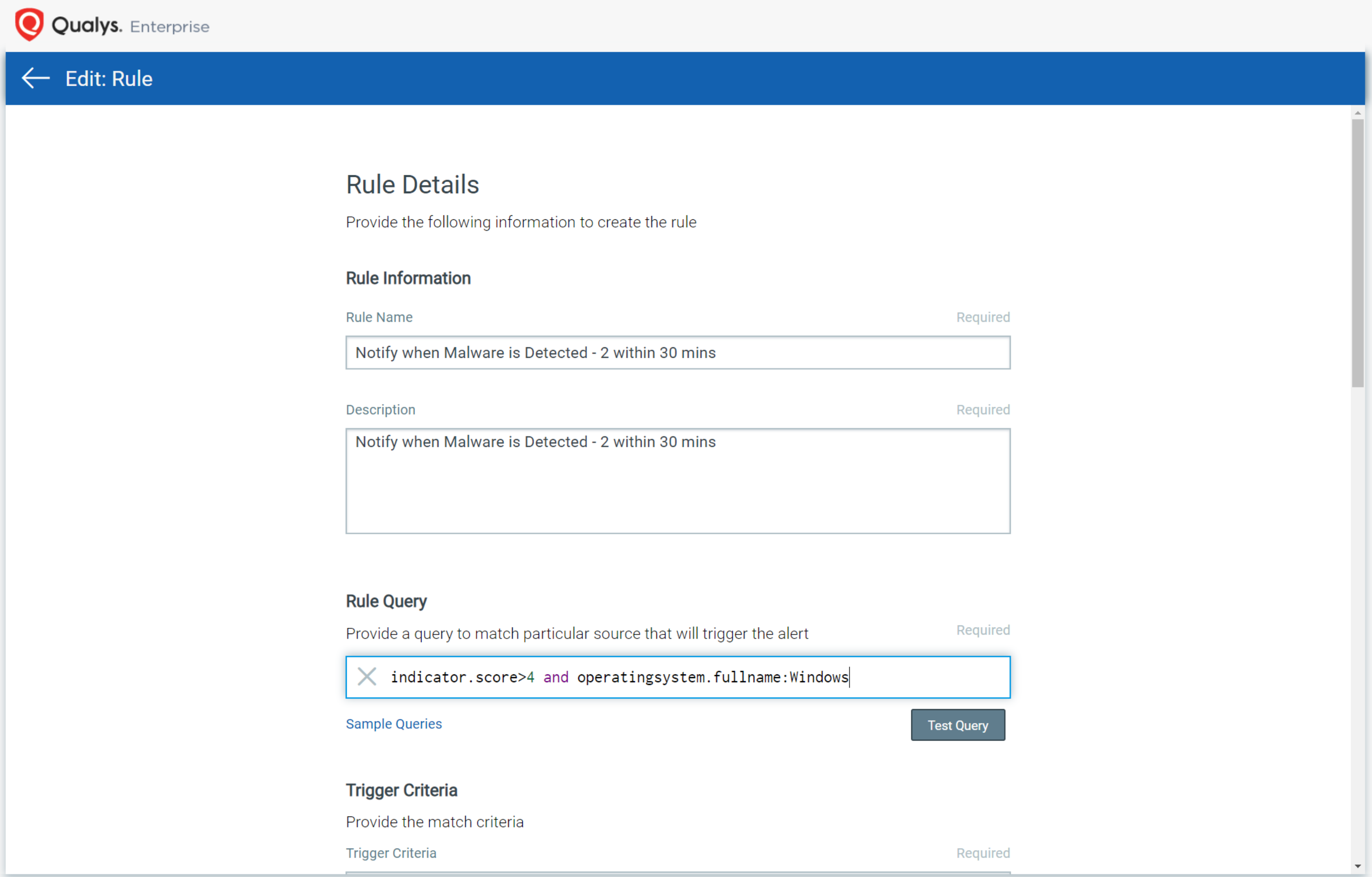
60 engines detected this file

a162bb9219a09b302b90bc6f908e117e3fb2c722560336d378fd76a8f22f78f8
bc93efa3-c907-11e6-bfac-80e65024849a.file
peexe

202.5 KB
Size

2019-06-05 23:56:01 UTC
27 days ago

| | | | |
|---|---|---|---|
| Acronis | Suspicious | Ad-Aware | Backdoor.Agent.ABWI |
| AegisLab | Trojan.Win32.CoreBot.4!c | AhnLab-V3 | Trojan/Win32.Trickbot.C1620377 |
| Alibaba | TrojanBanker:Win32/CoreBot.8118bd98 | ALYac | Backdoor.Agent.ABWI |
| Antiy-AVL | Trojan[Banker]/Win32.CoreBot | SecureAge APEX | Malicious |
| Arcabit | Backdoor.Agent.ABWI | Avast | Win32:TrickBot-A [Drp] |
| AVG | Win32:TrickBot-A [Drp] | Avira (no cloud) | TR/Dropper.Gen |
| BitDefender | Backdoor.Agent.ABWI | CAT-QuickHeal | Trojan.Mauvaise.SL1 |
| ClamAV | Win.Trojan.Generic-7803 | Comodo | Malware@#3rspln4cf2qro |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Cybereason | Malicious.0f1d27 |
| Cylance | Unsafe | Cyren | W32/Trojan.IRTG-0219 |
| DrWeb | Trojan.DownLoader22.63827 | Emsisoft | Backdoor.Agent.ABWI (B) |



## Rule Details

Provide the following information to create the rule

### Rule Information

Rule Name — Required

Notify when Malware is Detected - 2 within 30 mins

Description — Required

Notify when Malware is Detected - 2 within 30 mins

### Rule Query

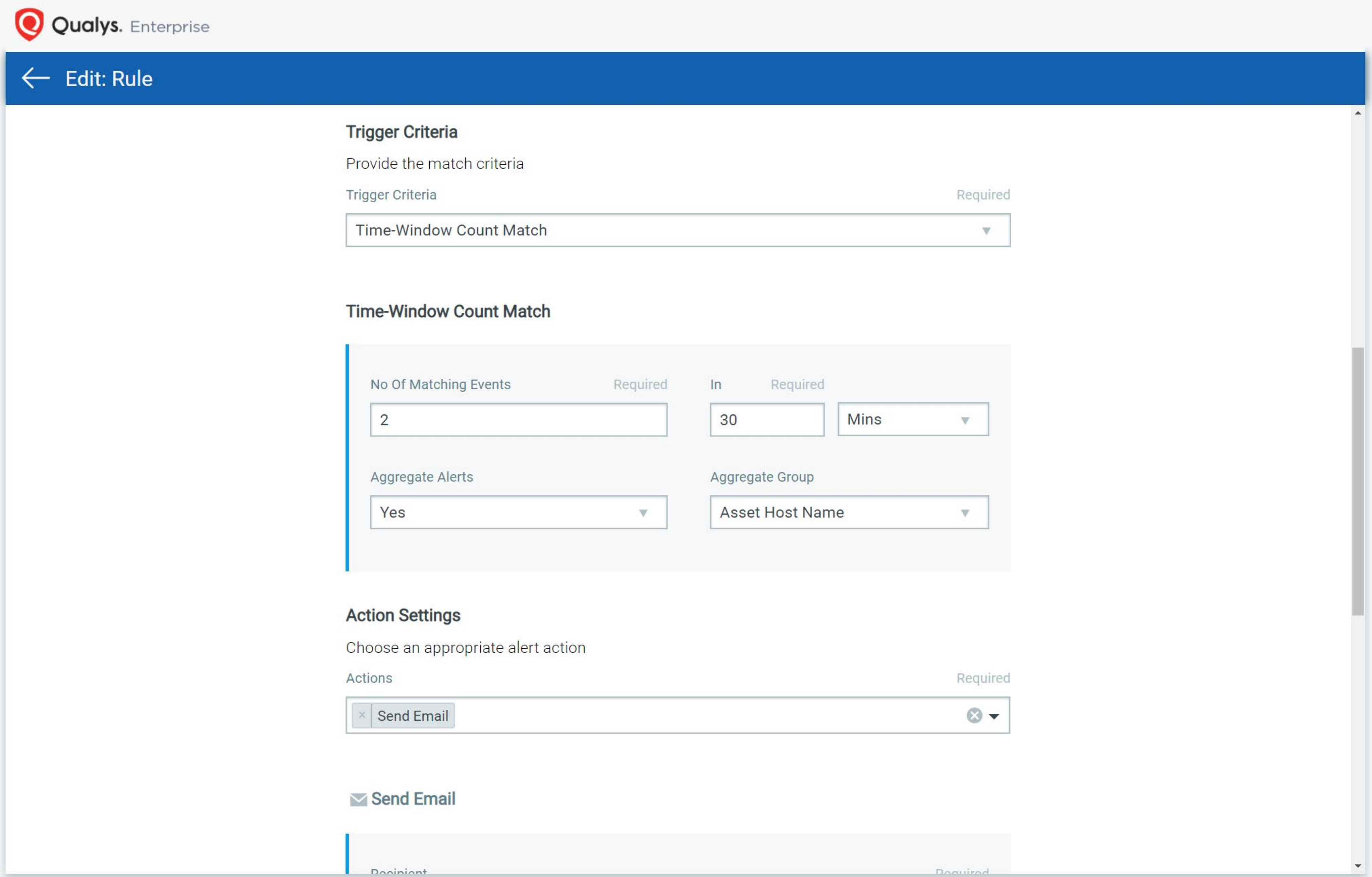
Provide a query to match particular source that will trigger the alert — Required

```
indicator.score>4 and operatingsystem.fullname:Windows
```

### Trigger Criteria

Provide the match criteria

Trigger Criteria — Required



Edit: Rule

Trigger Criteria

Provide the match criteria

Trigger Criteria — Required: Time-Window Count Match ▼

Time-Window Count Match

No Of Matching Events — Required: 2

In — Required: 30 Mins ▼

Aggregate Alerts: Yes ▼

Aggregate Group: Asset Host Name ▼

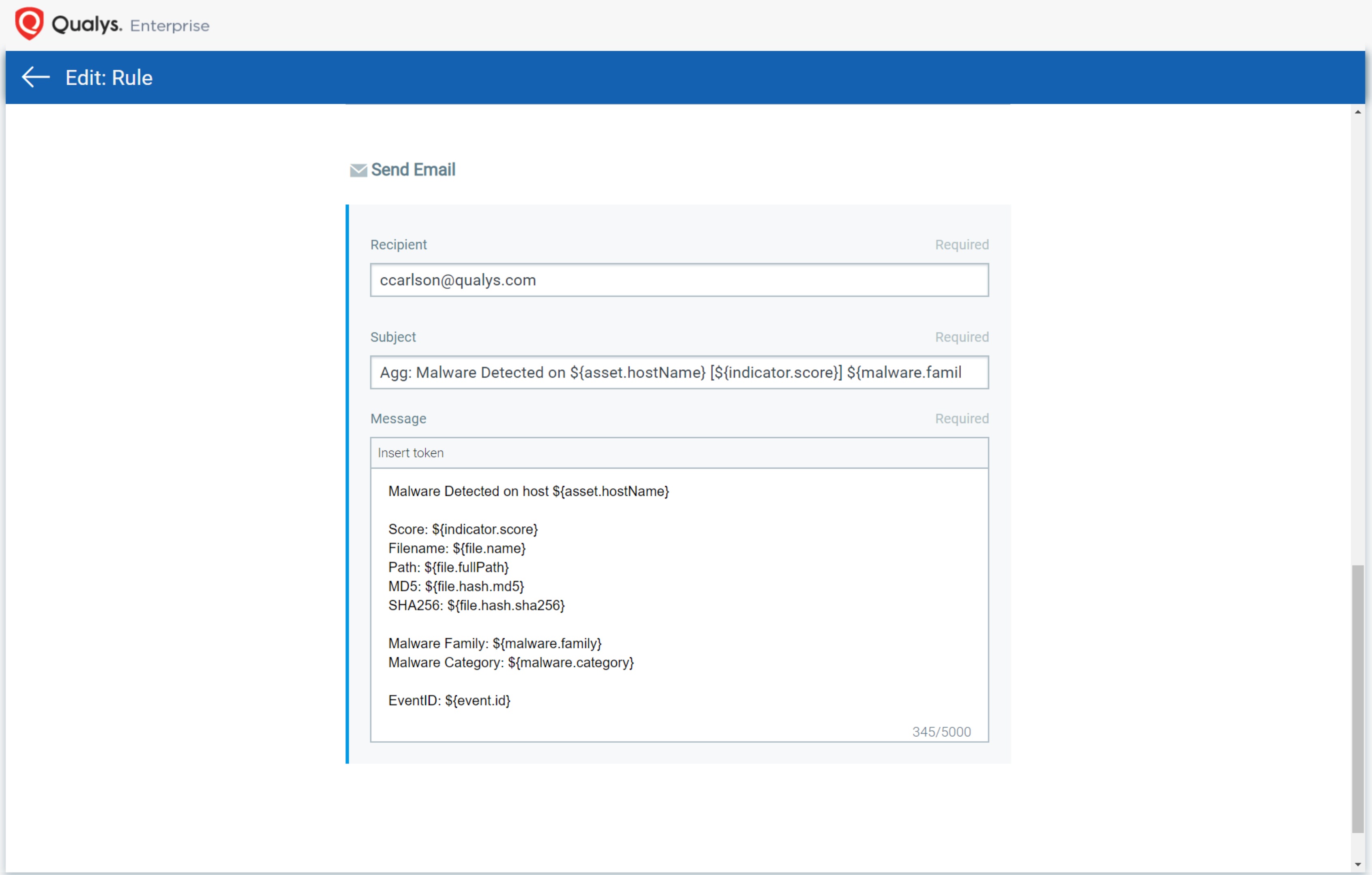
Action Settings

Choose an appropriate alert action

Actions — Required: × Send Email ⊗ ▼

Send Email

Recipient — Required



Send Email

Recipient Required

ccarlson@qualys.com

Subject Required

Agg: Malware Detected on ${asset.hostName} [${indicator.score}] ${malware.famil

Message Required

Insert token

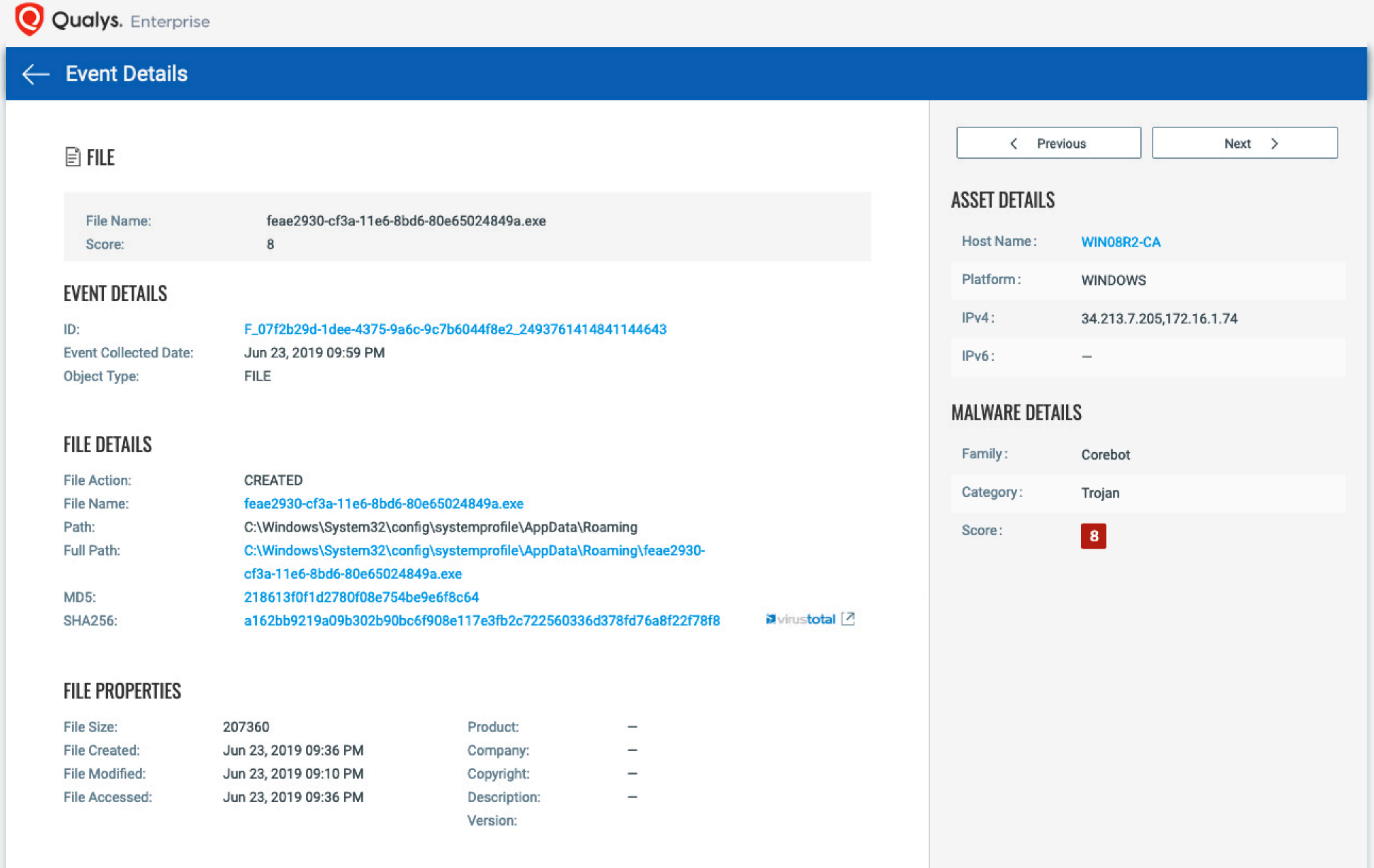
Malware Detected on host ${asset.hostName}

Score: ${indicator.score}
Filename: ${file.name}
Path: ${file.fullPath}
MD5: ${file.hash.md5}
SHA256: ${file.hash.sha256}

Malware Family: ${malware.family}
Malware Category: ${malware.category}

EventID: ${event.id}

345/5000



## Event Details

### FILE

| | |
|---|---|
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Score: | 8 |

### EVENT DETAILS

| | |
|---|---|
| ID: | F_07f2b29d-1dee-4375-9a6c-9c7b6044f8e2_2493761414841144643 |
| Event Collected Date: | Jun 23, 2019 09:59 PM |
| Object Type: | FILE |

### FILE DETAILS

| | |
|---|---|
| File Action: | CREATED |
| File Name: | feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming |
| Full Path: | C:\Windows\System32\config\systemprofile\AppData\Roaming\feae2930-cf3a-11e6-8bd6-80e65024849a.exe |
| MD5: | 218613f0f1d2780f08e754be9e6f8c64 |
| SHA256: | a162bb9219a09b302b90bc6f908e117e3fb2c722560336d378fd76a8f22f78f8 |

### FILE PROPERTIES

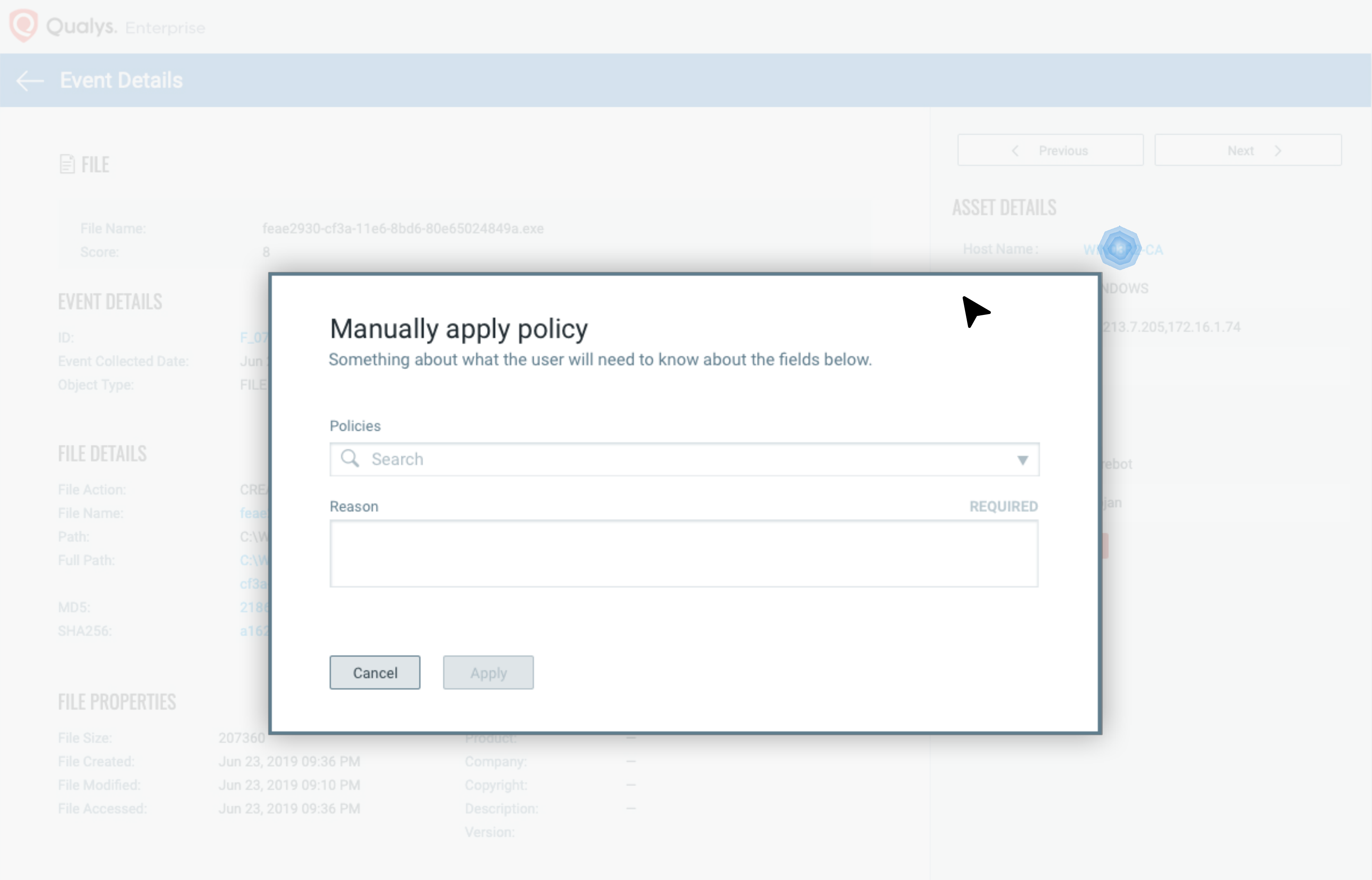
| | | | |
|---|---|---|---|
| File Size: | 207360 | Product: | – |
| File Created: | Jun 23, 2019 09:36 PM | Company: | – |
| File Modified: | Jun 23, 2019 09:10 PM | Copyright: | – |
| File Accessed: | Jun 23, 2019 09:36 PM | Description: | – |
| | | Version: | |

### ASSET DETAILS

| | |
|---|---|
| Host Name : | WIN08R2-CA |
| Platform : | WINDOWS |
| IPv4 : | 34.213.7.205,172.16.1.74 |
| IPv6 : | – |

### MALWARE DETAILS

| | |
|---|---|
| Family : | Corebot |
| Category : | Trojan |
| Score : | 8 |



File Name: feae2930-cf3a-11e6-8bd6-80e65024849a.exe
Score: 8

ID: F_07
Event Collected Date: Jun
Object Type: FILE

File Action: CRE
File Name: feae
Path: C:\W
Full Path: C:\W cf3a
MD5: 218
SHA256: a16

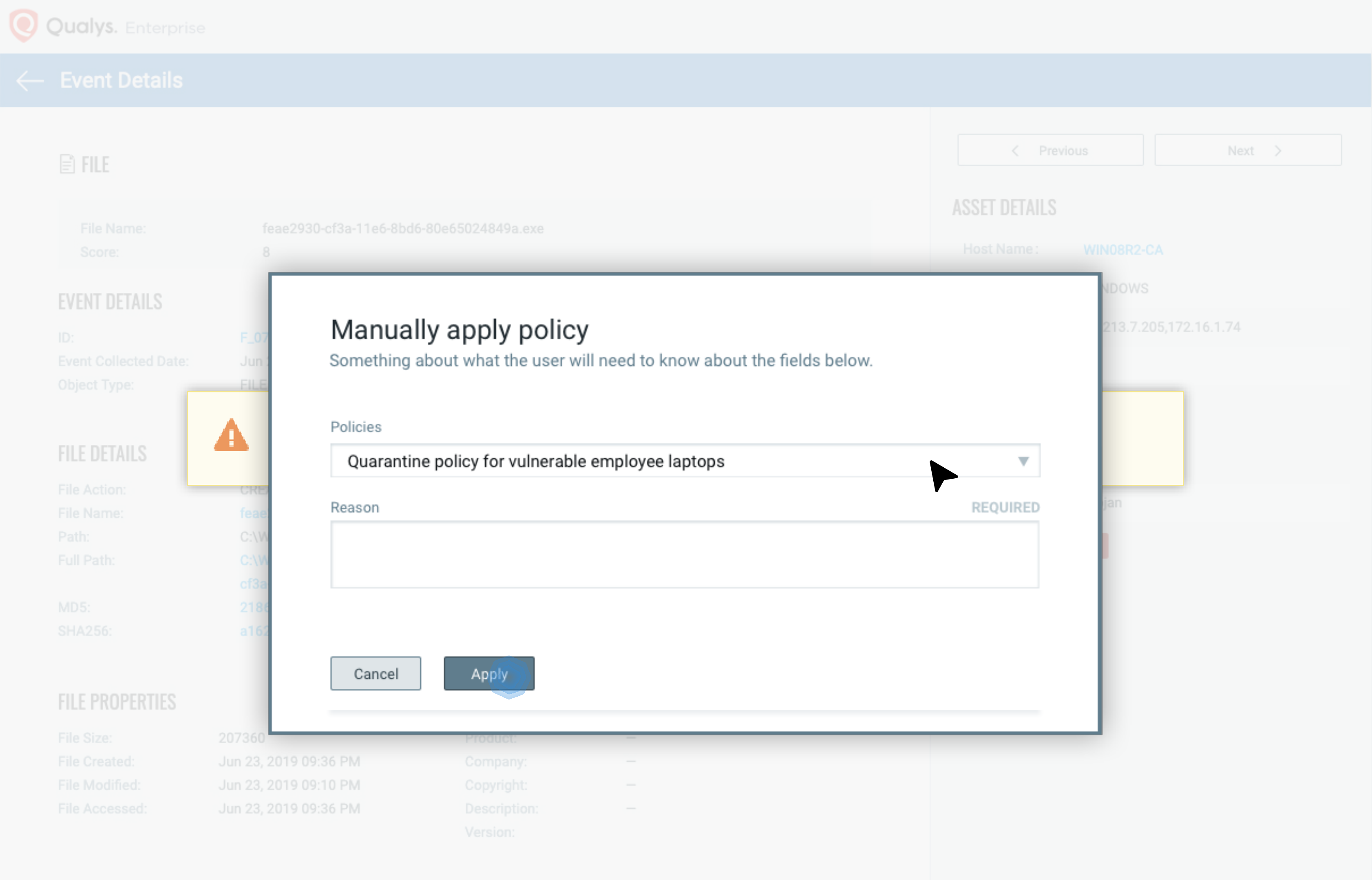
File Size: 207360
File Created: Jun 23, 2019 09:36 PM
File Modified: Jun 23, 2019 09:10 PM
File Accessed: Jun 23, 2019 09:36 PM

Product: –
Company: –
Copyright: –
Description: –
Version:

NDOWS
213.7.205,172.16.1.74
rebot
jan

## Manually apply policy

Something about what the user will need to know about the fields below.



FILE

File Name: feae2930-cf3a-11e6-8bd6-80e65024849a.exe
Score: 8

EVENT DETAILS

ID: F_07
Event Collected Date: Jun
Object Type: FILE

FILE DETAILS

File Action: CRE
File Name: feae
Path: C:\W
Full Path: C:\W cf3a
MD5: 2186
SHA256: a162

FILE PROPERTIES

File Size: 207360
File Created: Jun 23, 2019 09:36 PM
File Modified: Jun 23, 2019 09:10 PM
File Accessed: Jun 23, 2019 09:36 PM
Product: –
Company: –
Copyright: –
Description: –
Version:

ASSET DETAILS

Host Name: WIN08R2-CA
NDOWS
213.7.205,172.16.1.74
jan

## Manually apply policy

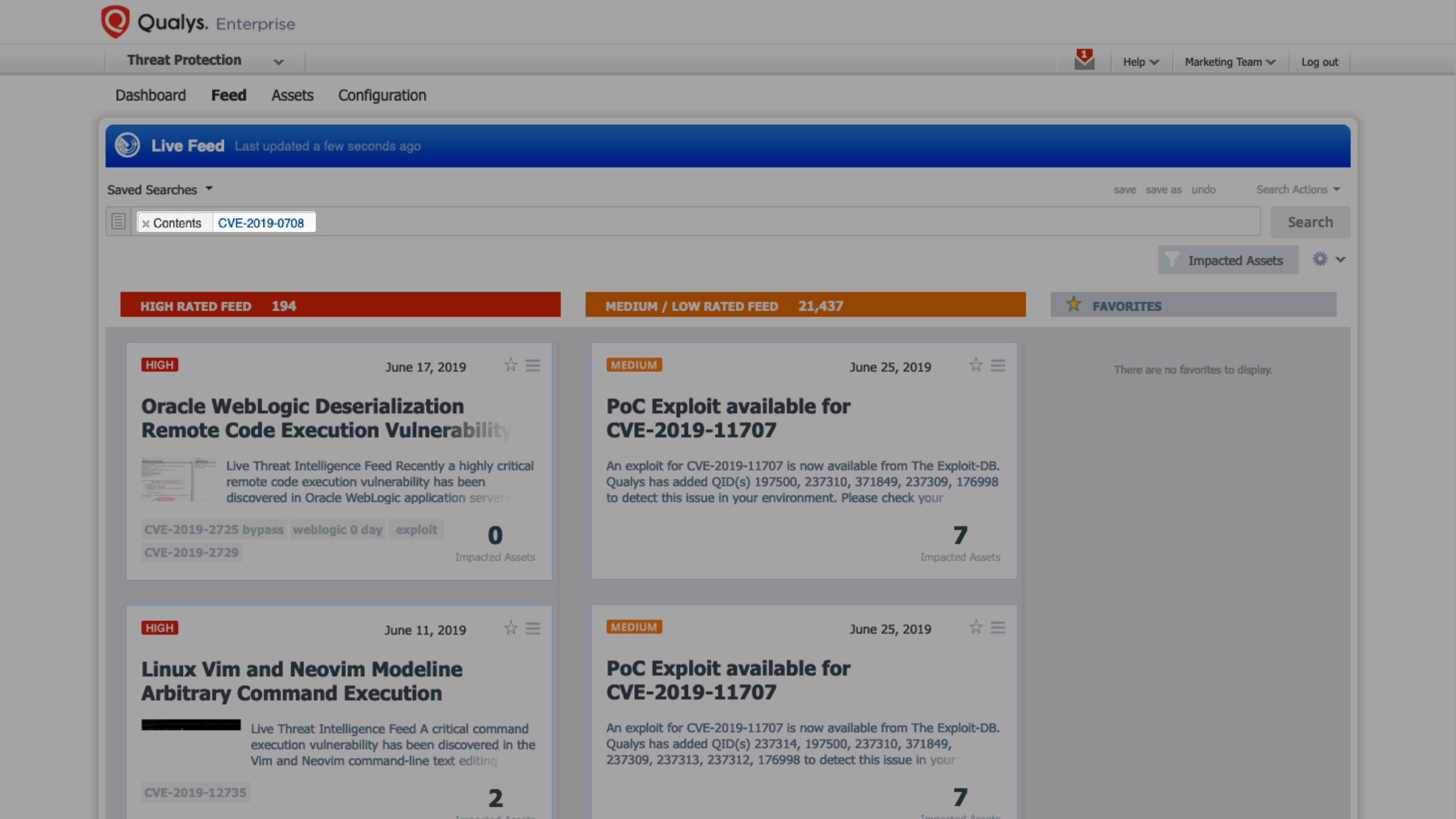
Something about what the user will need to know about the fields below.

Policies: Quarantine policy for vulnerable employee laptops

Reason REQUIRED

# DEMO

Searching for a critical exploit



There are no favorites to display.

HIGH June 17, 2019

**Oracle WebLogic Deserialization Remote Code Execution Vulnerability**

Live Threat Intelligence Feed Recently a highly critical remote code execution vulnerability has been discovered in Oracle WebLogic application server

CVE-2019-2725 bypass weblogic 0 day exploit CVE-2019-2729

0 Impacted Assets

MEDIUM June 25, 2019

**PoC Exploit available for CVE-2019-11707**

An exploit for CVE-2019-11707 is now available from The Exploit-DB. Qualys has added QID(s) 197500, 237310, 371849, 237309, 176998 to detect this issue in your environment. Please check your

7 Impacted Assets

HIGH June 11, 2019

**Linux Vim and Neovim Modeline Arbitrary Command Execution**

Live Threat Intelligence Feed A critical command execution vulnerability has been discovered in the Vim and Neovim command-line text editing

CVE-2019-12735

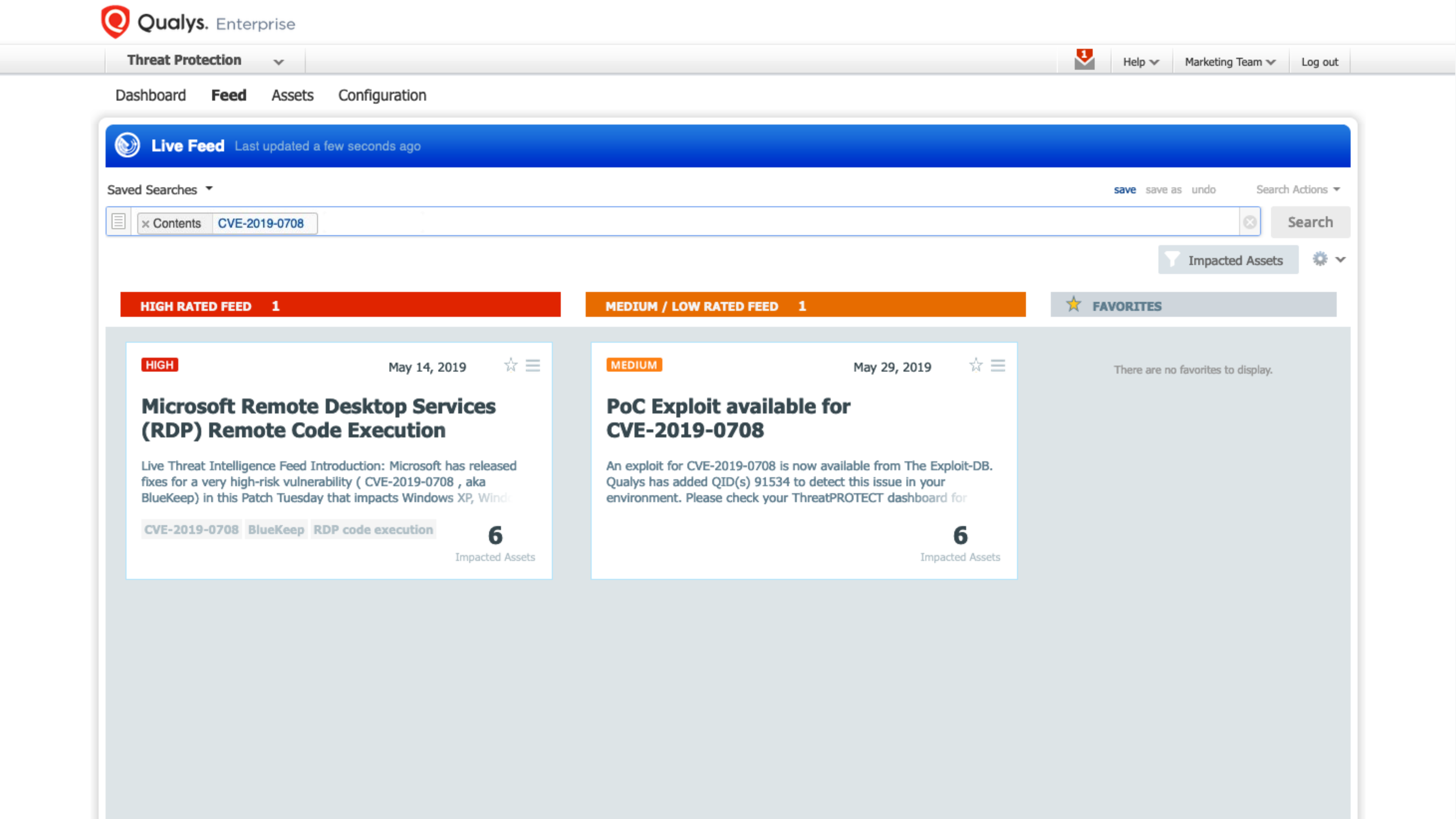
2

MEDIUM June 25, 2019

**PoC Exploit available for CVE-2019-11707**

An exploit for CVE-2019-11707 is now available from The Exploit-DB. Qualys has added QID(s) 237314, 197500, 237310, 371849, 237309, 237313, 237312, 176998 to detect this issue in your

7



HIGH

May 14, 2019

**Microsoft Remote Desktop Services (RDP) Remote Code Execution**

Live Threat Intelligence Feed Introduction: Microsoft has released fixes for a very high-risk vulnerability ( CVE-2019-0708 , aka BlueKeep) in this Patch Tuesday that impacts Windows XP, Wind

CVE-2019-0708 BlueKeep RDP code execution

6 Impacted Assets

MEDIUM

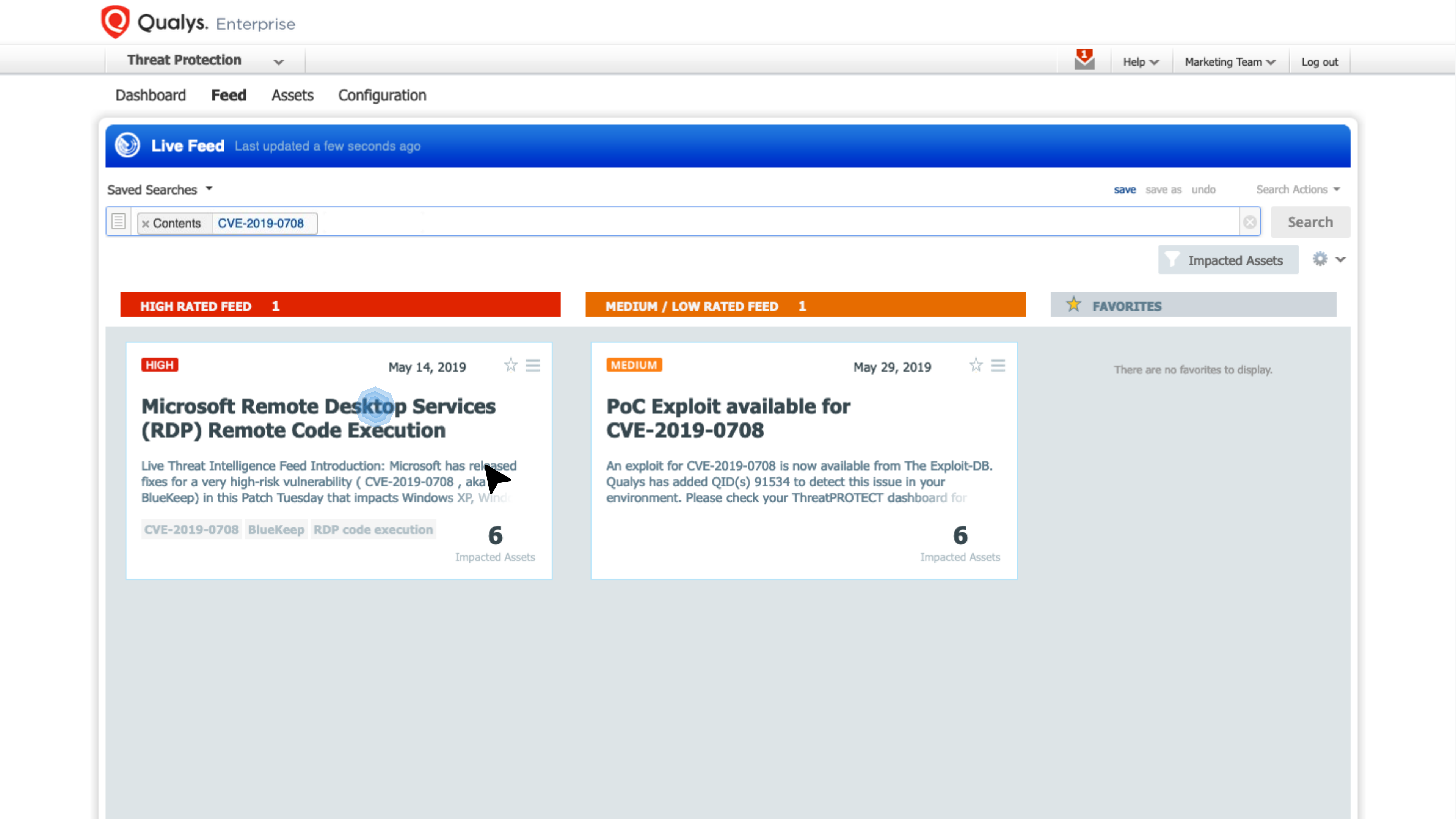
May 29, 2019

**PoC Exploit available for CVE-2019-0708**

An exploit for CVE-2019-0708 is now available from The Exploit-DB. Qualys has added QID(s) 91534 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for

6 Impacted Assets

There are no favorites to display.



× Contents CVE-2019-0708

HIGH May 14, 2019

**Microsoft Remote Desktop Services (RDP) Remote Code Execution**

Live Threat Intelligence Feed Introduction: Microsoft has released fixes for a very high-risk vulnerability ( CVE-2019-0708 , aka BlueKeep) in this Patch Tuesday that impacts Windows XP, Wind

CVE-2019-0708 BlueKeep RDP code execution

6 Impacted Assets

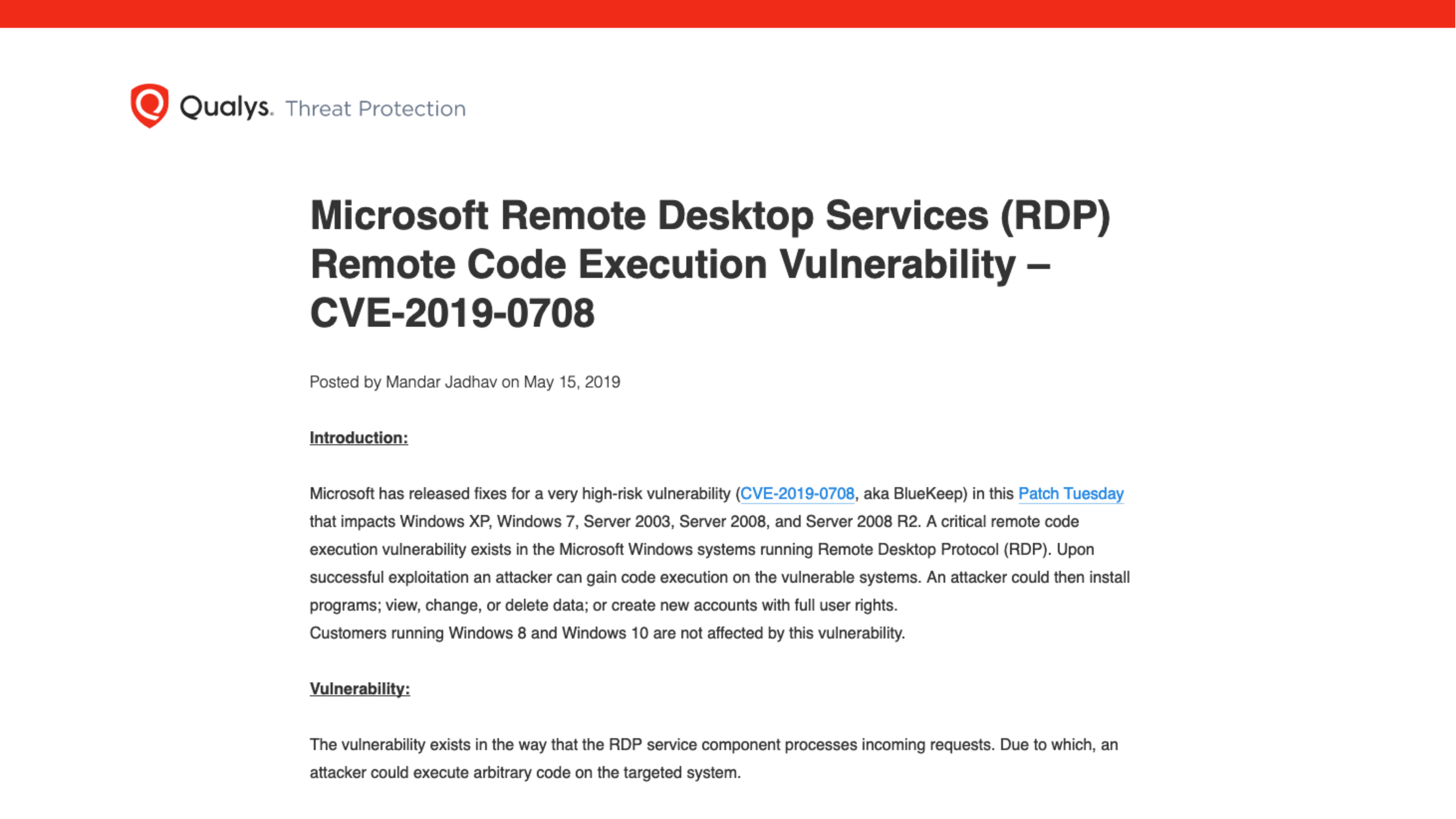
MEDIUM May 29, 2019

**PoC Exploit available for CVE-2019-0708**

An exploit for CVE-2019-0708 is now available from The Exploit-DB. Qualys has added QID(s) 91534 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for

6 Impacted Assets

There are no favorites to display.



Qualys. Threat Protection

# Microsoft Remote Desktop Services (RDP) Remote Code Execution Vulnerability – CVE-2019-0708

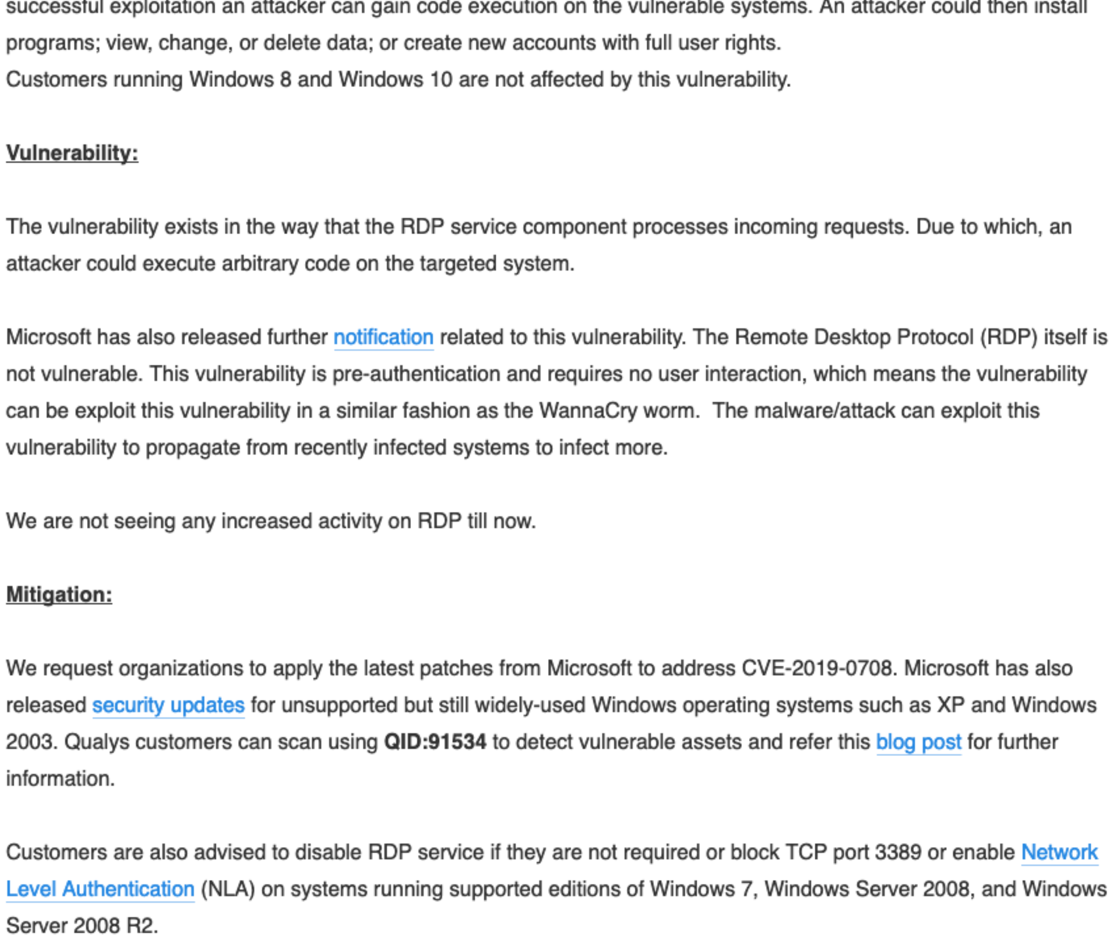
Posted by Mandar Jadhav on May 15, 2019

**Introduction:**

Microsoft has released fixes for a very high-risk vulnerability (CVE-2019-0708, aka BlueKeep) in this Patch Tuesday that impacts Windows XP, Windows 7, Server 2003, Server 2008, and Server 2008 R2. A critical remote code execution vulnerability exists in the Microsoft Windows systems running Remote Desktop Protocol (RDP). Upon successful exploitation an attacker can gain code execution on the vulnerable systems. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
Customers running Windows 8 and Windows 10 are not affected by this vulnerability.

**Vulnerability:**

The vulnerability exists in the way that the RDP service component processes incoming requests. Due to which, an attacker could execute arbitrary code on the targeted system.



successful exploitation an attacker can gain code execution on the vulnerable systems. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
Customers running Windows 8 and Windows 10 are not affected by this vulnerability.

**Vulnerability:**

The vulnerability exists in the way that the RDP service component processes incoming requests. Due to which, an attacker could execute arbitrary code on the targeted system.

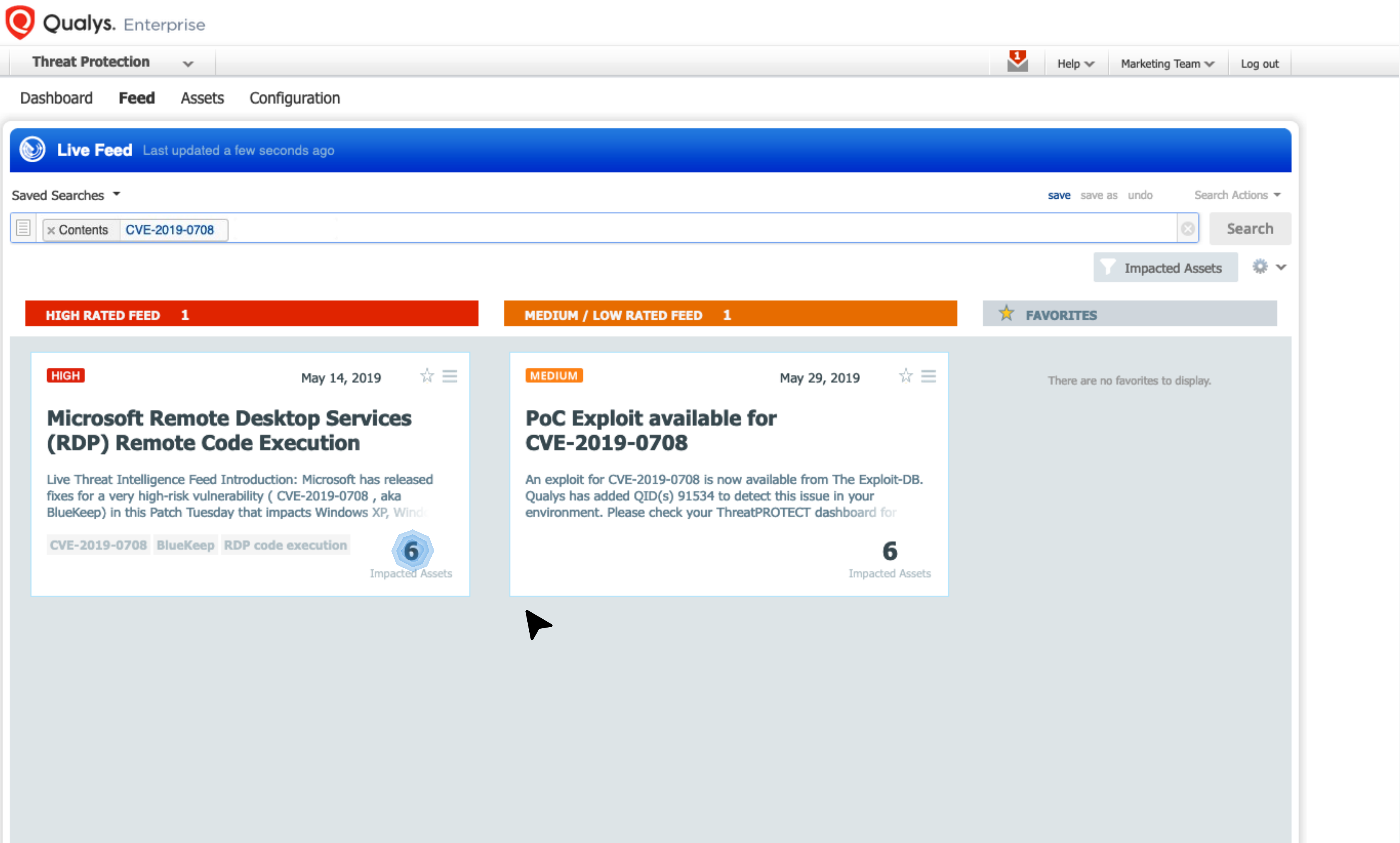
Microsoft has also released further notification related to this vulnerability. The Remote Desktop Protocol (RDP) itself is not vulnerable. This vulnerability is pre-authentication and requires no user interaction, which means the vulnerability can be exploit this vulnerability in a similar fashion as the WannaCry worm.  The malware/attack can exploit this vulnerability to propagate from recently infected systems to infect more.

We are not seeing any increased activity on RDP till now.

**Mitigation:**

We request organizations to apply the latest patches from Microsoft to address CVE-2019-0708. Microsoft has also released security updates for unsupported but still widely-used Windows operating systems such as XP and Windows 2003. Qualys customers can scan using **QID:91534** to detect vulnerable assets and refer this blog post for further information.

Customers are also advised to disable RDP service if they are not required or block TCP port 3389 or enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.



HIGH May 14, 2019

**Microsoft Remote Desktop Services (RDP) Remote Code Execution**

Live Threat Intelligence Feed Introduction: Microsoft has released fixes for a very high-risk vulnerability ( CVE-2019-0708 , aka BlueKeep) in this Patch Tuesday that impacts Windows XP, Wind

CVE-2019-0708 BlueKeep RDP code execution

6 Impacted Assets

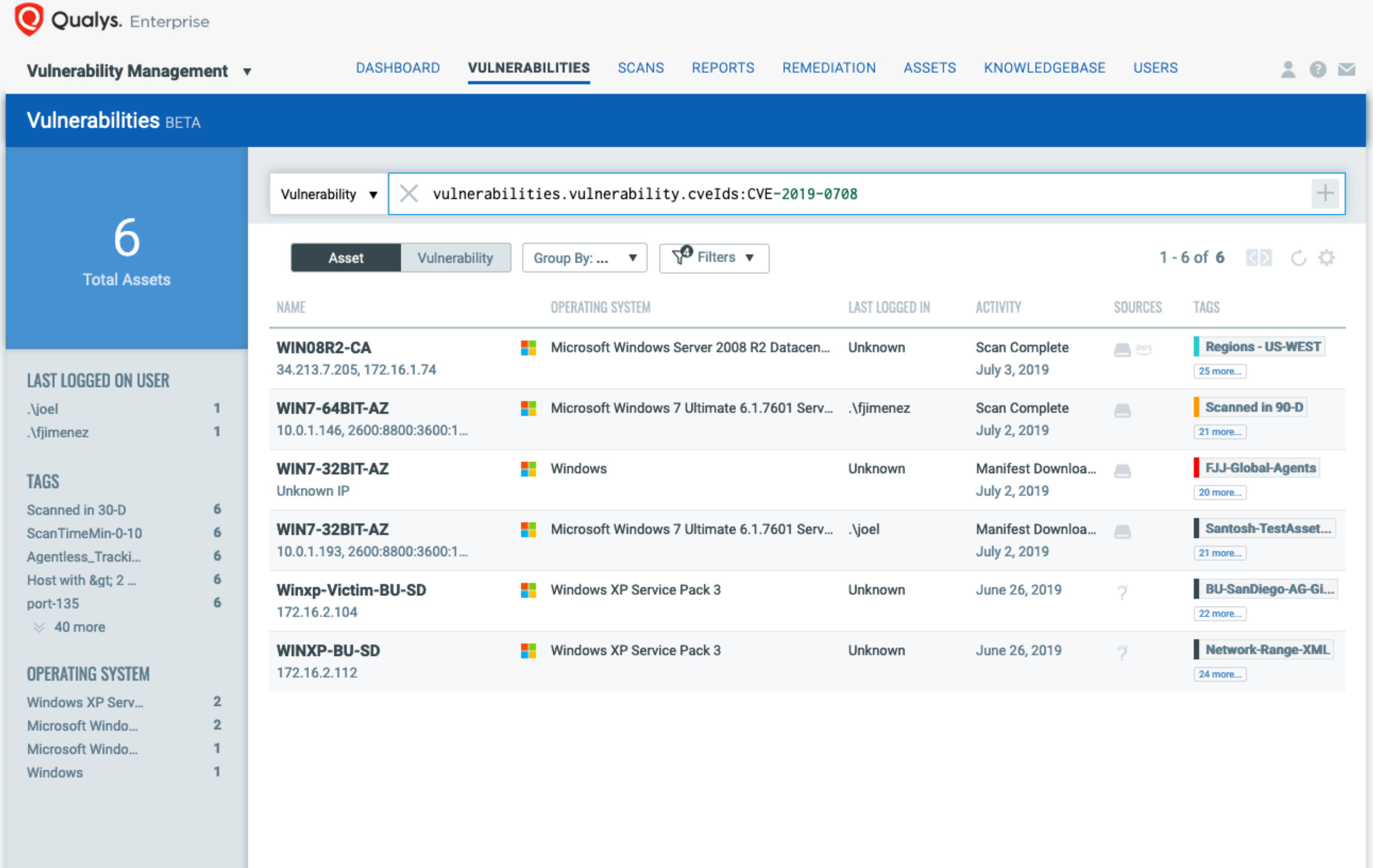
MEDIUM May 29, 2019

**PoC Exploit available for CVE-2019-0708**

An exploit for CVE-2019-0708 is now available from The Exploit-DB. Qualys has added QID(s) 91534 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for

6 Impacted Assets

There are no favorites to display.



Vulnerabilities BETA

Vulnerability `vulnerabilities.vulnerability.cveIds:CVE-2019-0708`

6
Total Assets

LAST LOGGED ON USER

| | |
|---|---|
| .\joel | 1 |
| .\fjimenez | 1 |

TAGS

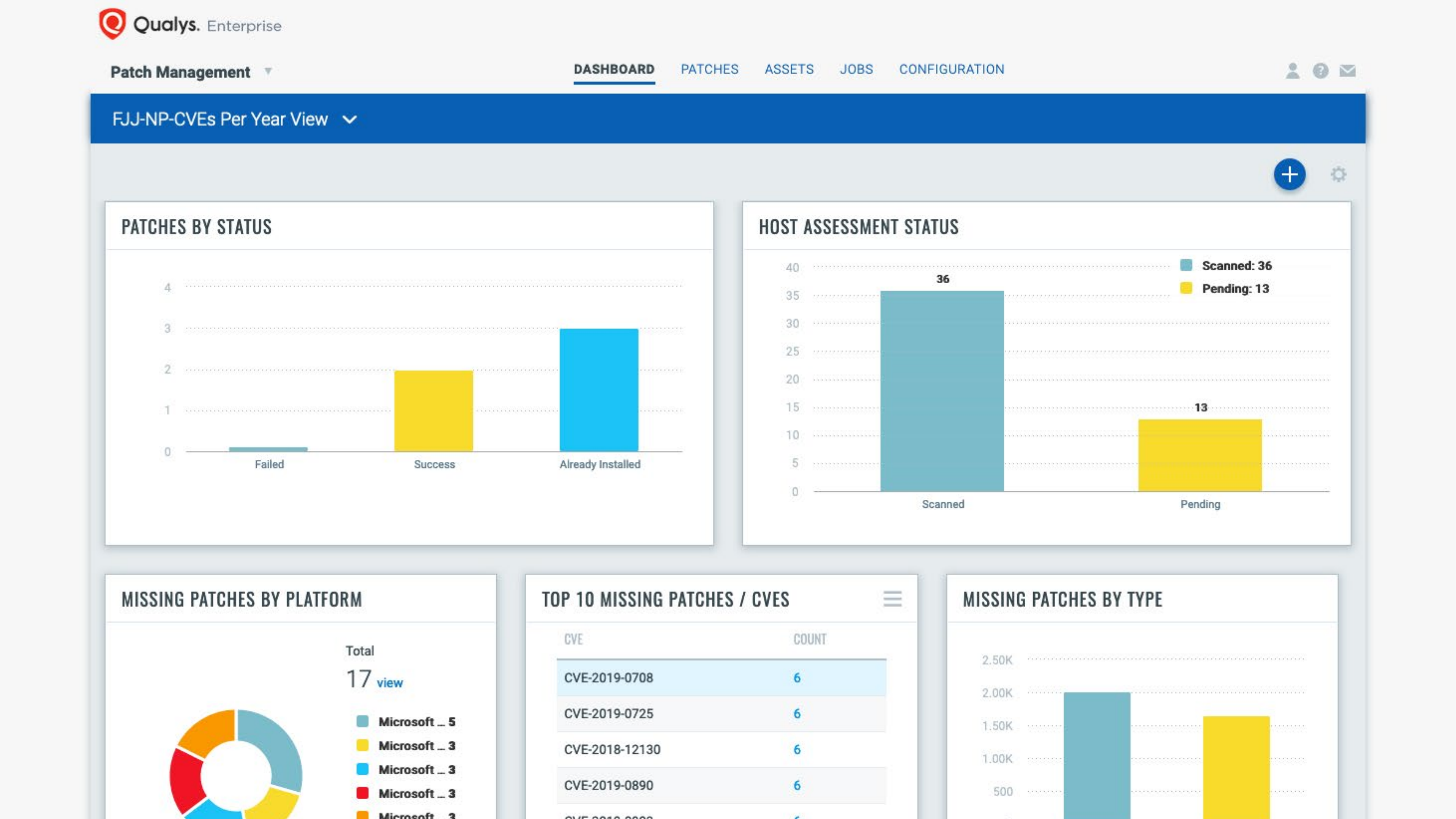
| | |
|---|---|
| Scanned in 30-D | 6 |
| ScanTimeMin-0-10 | 6 |
| Agentless_Tracki... | 6 |
| Host with &gt; 2 ... | 6 |
| port-135 | 6 |

40 more

OPERATING SYSTEM

| | |
|---|---|
| Windows XP Serv... | 2 |
| Microsoft Windo... | 2 |
| Microsoft Windo... | 1 |
| Windows | 1 |

| NAME | OPERATING SYSTEM | LAST LOGGED IN | ACTIVITY | SOURCES | TAGS |
|---|---|---|---|---|---|
| WIN08R2-CA<br>34.213.7.205, 172.16.1.74 | Microsoft Windows Server 2008 R2 Datacen... | Unknown | Scan Complete<br>July 3, 2019 | aws | Regions - US-WEST<br>25 more... |
| WIN7-64BIT-AZ<br>10.0.1.146, 2600:8800:3600:1... | Microsoft Windows 7 Ultimate 6.1.7601 Serv... | .\fjimenez | Scan Complete<br>July 2, 2019 | | Scanned in 90-D<br>21 more... |
| WIN7-32BIT-AZ<br>Unknown IP | Windows | Unknown | Manifest Downloa...<br>July 2, 2019 | | FJJ-Global-Agents<br>20 more... |
| WIN7-32BIT-AZ<br>10.0.1.193, 2600:8800:3600:1... | Microsoft Windows 7 Ultimate 6.1.7601 Serv... | .\joel | Manifest Downloa...<br>July 2, 2019 | | Santosh-TestAsset...<br>21 more... |
| Winxp-Victim-BU-SD<br>172.16.2.104 | Windows XP Service Pack 3 | Unknown | June 26, 2019 | ? | BU-SanDiego-AG-Gi...<br>22 more... |
| WINXP-BU-SD<br>172.16.2.112 | Windows XP Service Pack 3 | Unknown | June 26, 2019 | ? | Network-Range-XML<br>24 more... |



FJJ-NP-CVEs Per Year View

PATCHES BY STATUS

HOST ASSESSMENT STATUS

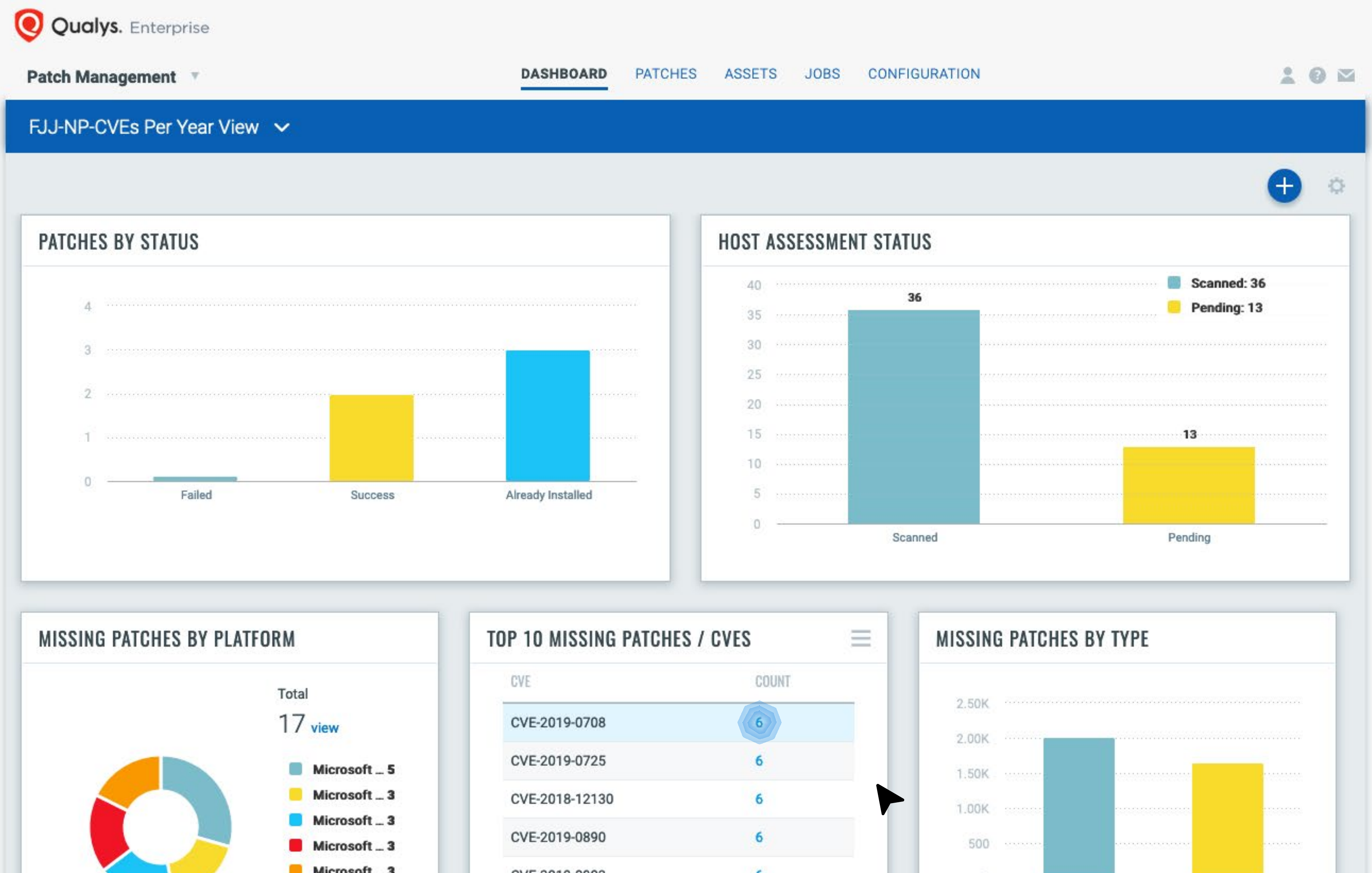
MISSING PATCHES BY PLATFORM

Total
17 view

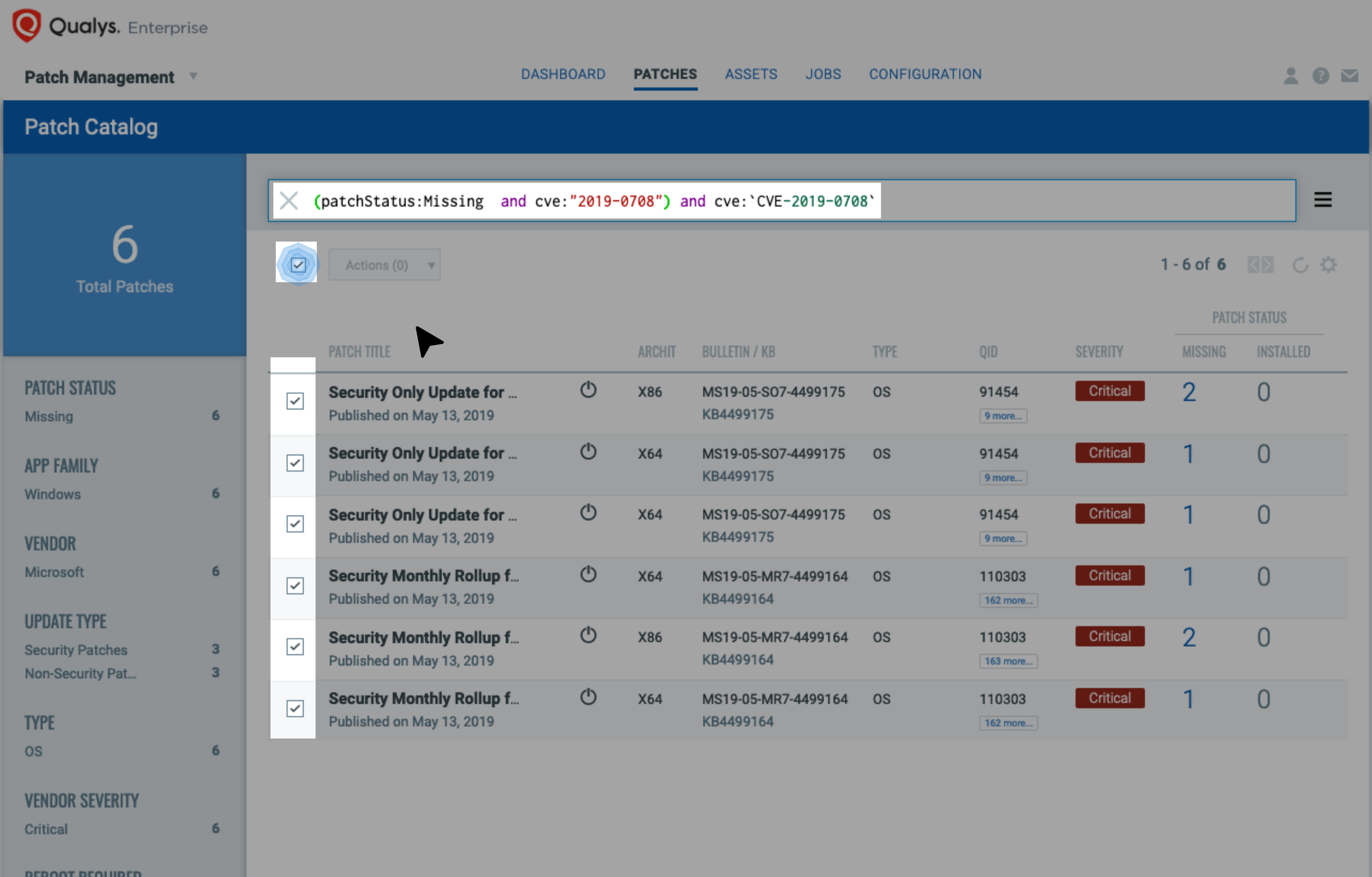
TOP 10 MISSING PATCHES / CVES

| CVE | COUNT |
|---|---|
| CVE-2019-0708 | 6 |
| CVE-2019-0725 | 6 |
| CVE-2018-12130 | 6 |
| CVE-2019-0890 | 6 |

MISSING PATCHES BY TYPE



| CVE | COUNT |
|---|---|
| CVE-2019-0708 | 6 |
| CVE-2019-0725 | 6 |
| CVE-2018-12130 | 6 |
| CVE-2019-0890 | 6 |



Patch Catalog

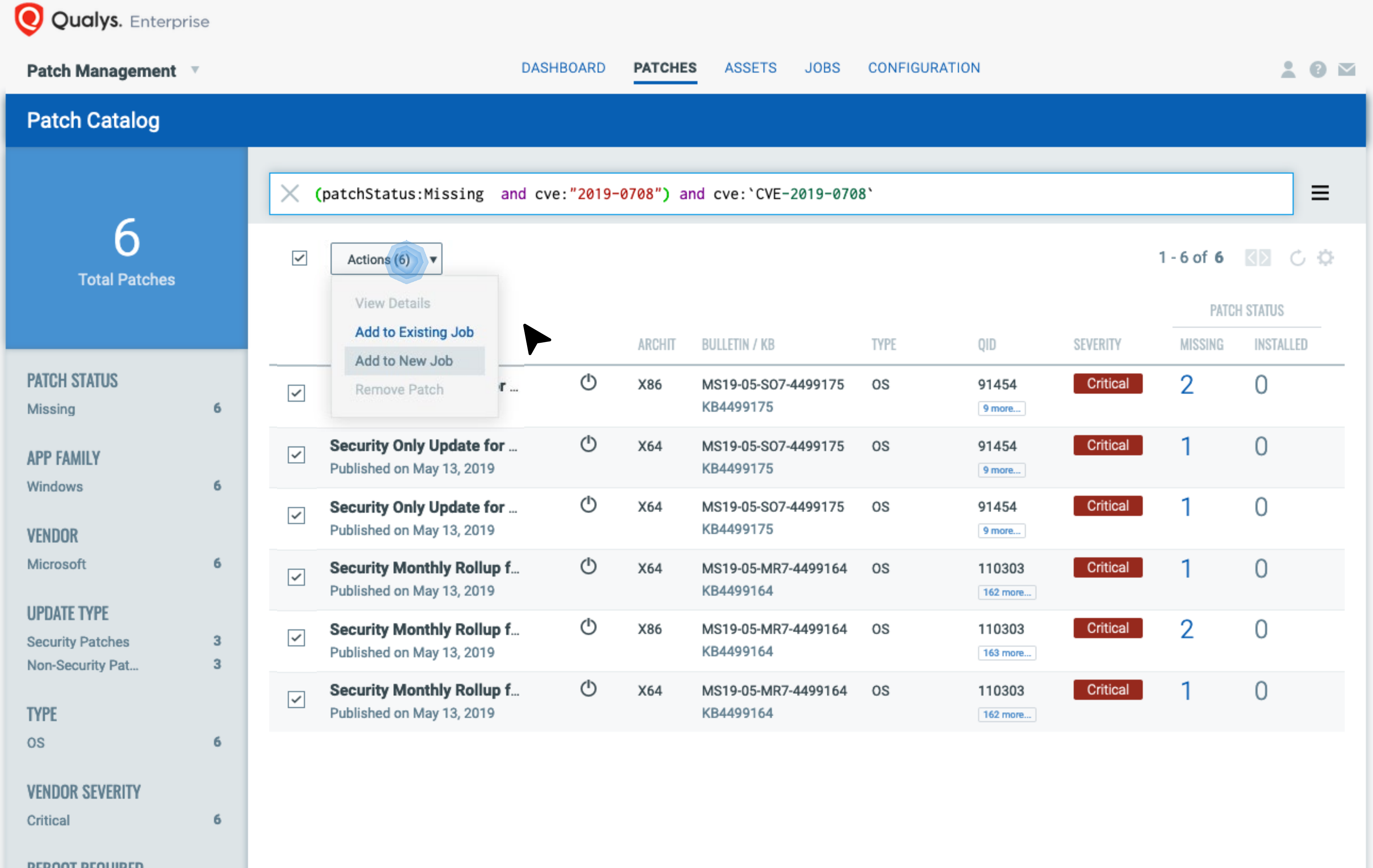
```
(patchStatus:Missing  and cve:"2019-0708") and cve:`CVE-2019-0708`
```

6
Total Patches

| | |
|---|---|
| **PATCH STATUS** | |
| Missing | 6 |
| **APP FAMILY** | |
| Windows | 6 |
| **VENDOR** | |
| Microsoft | 6 |
| **UPDATE TYPE** | |
| Security Patches | 3 |
| Non-Security Pat... | 3 |
| **TYPE** | |
| OS | 6 |
| **VENDOR SEVERITY** | |
| Critical | 6 |
| **REBOOT REQUIRED** | |

1 - 6 of 6

| | PATCH TITLE | | ARCHIT | BULLETIN / KB | TYPE | QID | SEVERITY | PATCH STATUS | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | MISSING | INSTALLED |
| ☑ | **Security Only Update for ...**<br>Published on May 13, 2019 | ⏻ | X86 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 2 | 0 |
| ☑ | **Security Only Update for ...**<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | **Security Only Update for ...**<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | **Security Monthly Rollup f...**<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |
| ☑ | **Security Monthly Rollup f...**<br>Published on May 13, 2019 | ⏻ | X86 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>163 more... | Critical | 2 | 0 |
| ☑ | **Security Monthly Rollup f...**<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |

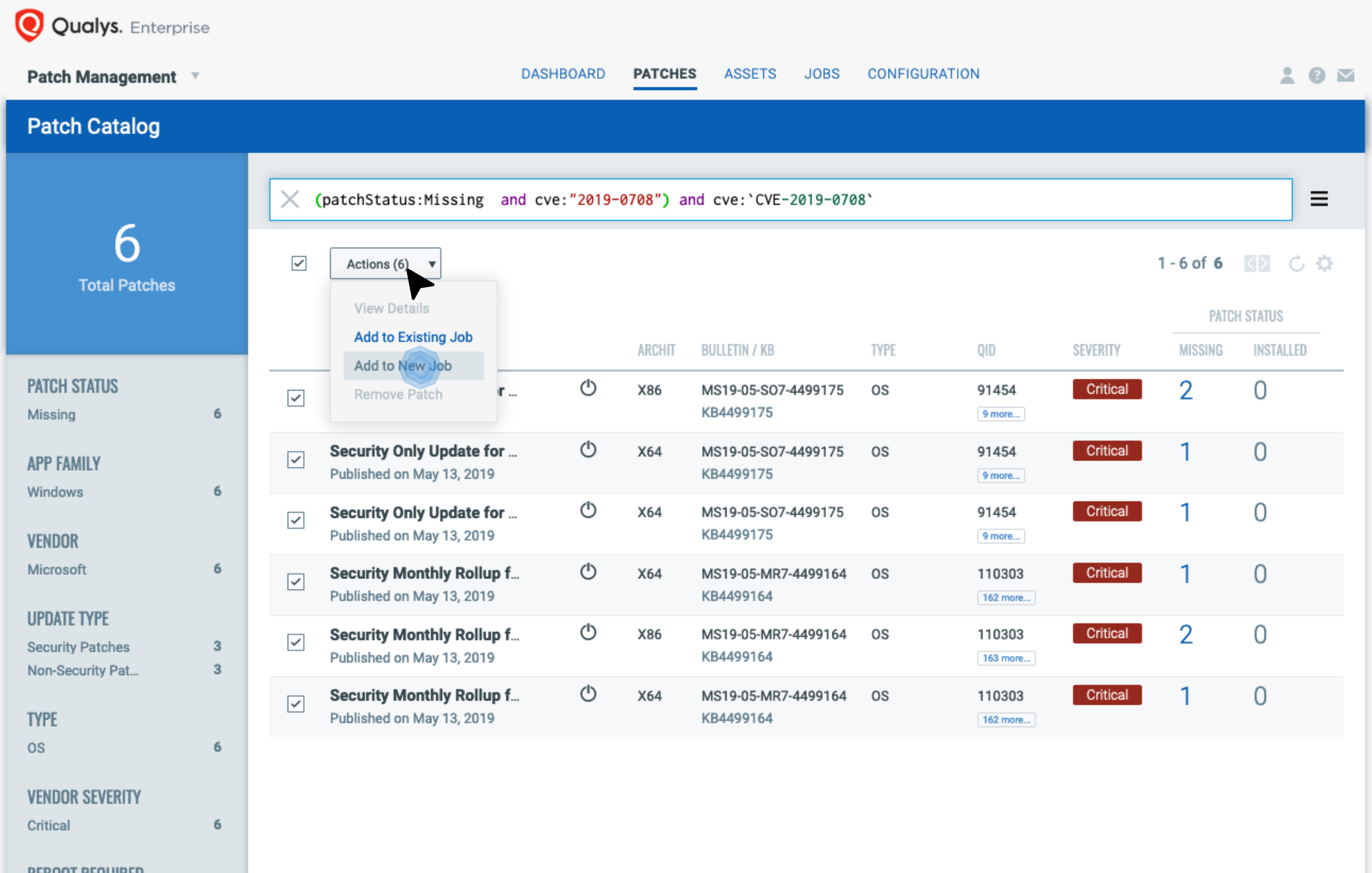


```
(patchStatus:Missing  and cve:"2019-0708") and cve:`CVE-2019-0708`
```

6
Total Patches

| | |
|---|---|
| **PATCH STATUS** | |
| Missing | 6 |
| **APP FAMILY** | |
| Windows | 6 |
| **VENDOR** | |
| Microsoft | 6 |
| **UPDATE TYPE** | |
| Security Patches | 3 |
| Non-Security Pat... | 3 |
| **TYPE** | |
| OS | 6 |
| **VENDOR SEVERITY** | |
| Critical | 6 |
| **REBOOT REQUIRED** | |

| | | | ARCHIT | BULLETIN / KB | TYPE | QID | SEVERITY | PATCH STATUS<br>MISSING | <br>INSTALLED |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | r ... | ⏻ | X86 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 2 | 0 |
| ☑ | Security Only Update for ...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | Security Only Update for ...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X86 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>163 more... | Critical | 2 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |



Patch Catalog

```
(patchStatus:Missing  and cve:"2019-0708") and cve:`CVE-2019-0708`
```

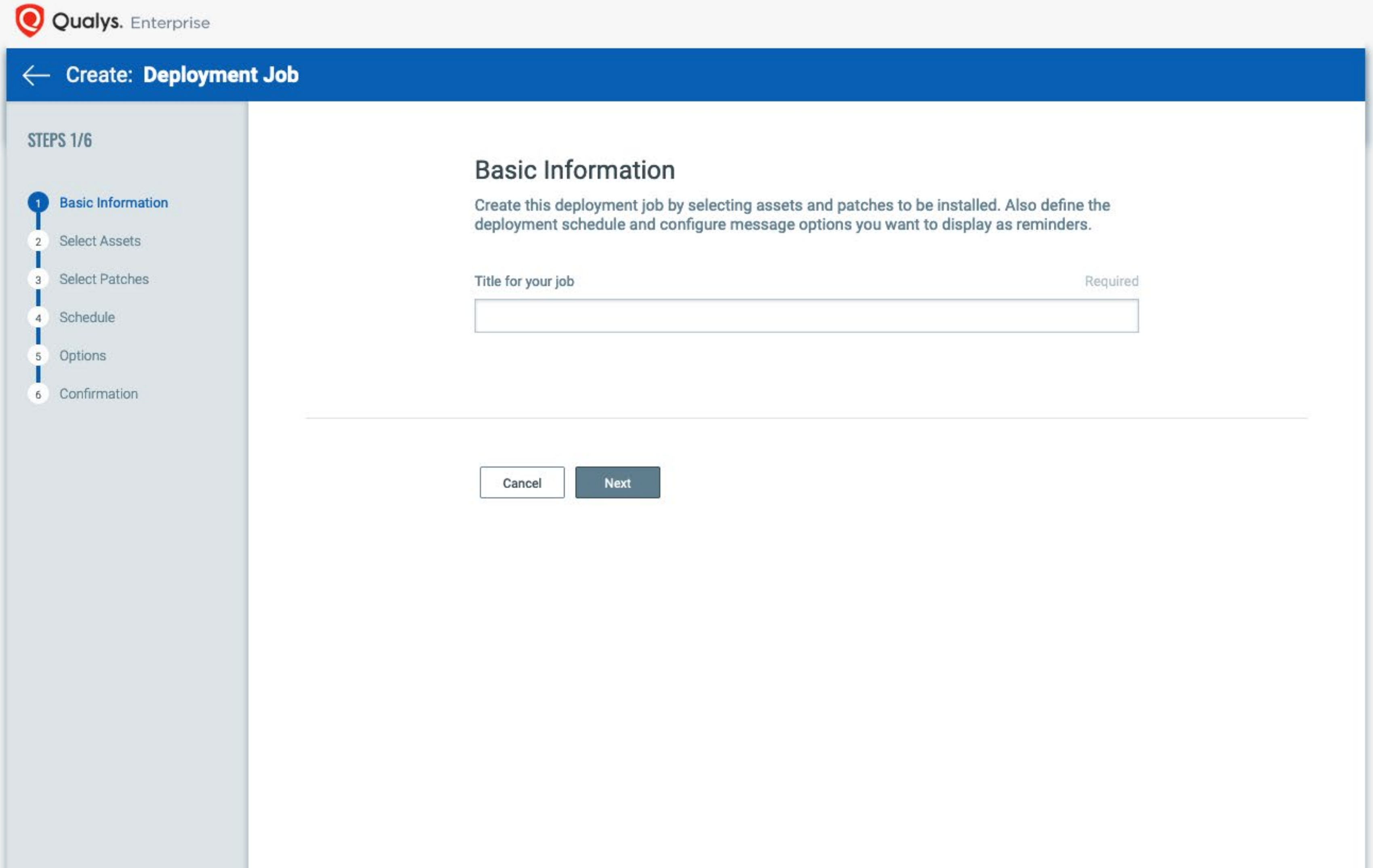
6 Total Patches

| | |
|---|---|
| **PATCH STATUS** | |
| Missing | 6 |
| **APP FAMILY** | |
| Windows | 6 |
| **VENDOR** | |
| Microsoft | 6 |
| **UPDATE TYPE** | |
| Security Patches | 3 |
| Non-Security Pat... | 3 |
| **TYPE** | |
| OS | 6 |
| **VENDOR SEVERITY** | |
| Critical | 6 |
| **REBOOT REQUIRED** | |

☑ Actions (6) ▾

1 - 6 of 6

| | | | ARCHIT | BULLETIN / KB | TYPE | QID | SEVERITY | PATCH STATUS MISSING | PATCH STATUS INSTALLED |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | r ... | ⏻ | X86 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 2 | 0 |
| ☑ | Security Only Update for ...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | Security Only Update for ...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-SO7-4499175<br>KB4499175 | OS | 91454<br>9 more... | Critical | 1 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X86 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>163 more... | Critical | 2 | 0 |
| ☑ | Security Monthly Rollup f...<br>Published on May 13, 2019 | ⏻ | X64 | MS19-05-MR7-4499164<br>KB4499164 | OS | 110303<br>162 more... | Critical | 1 | 0 |

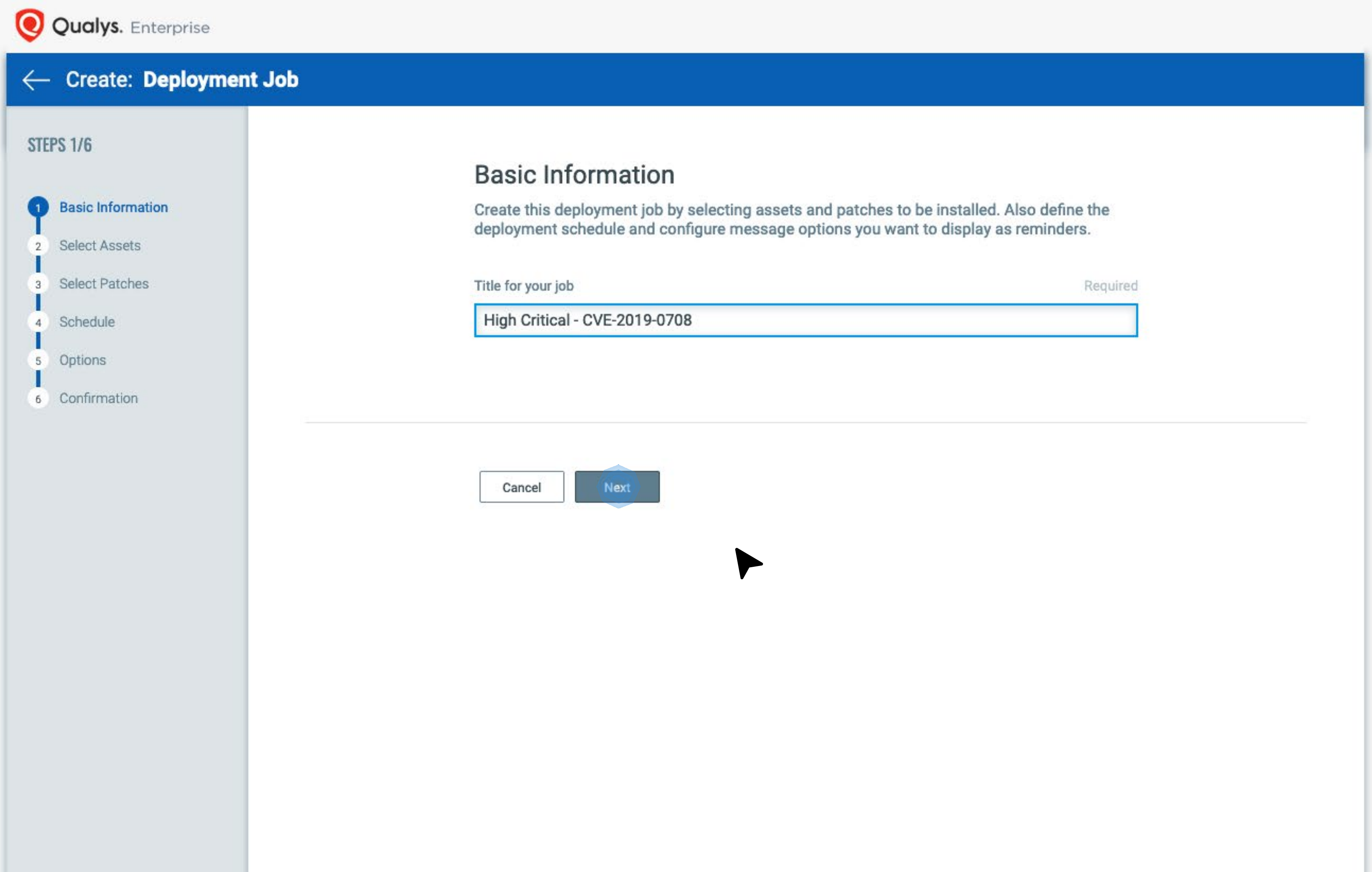


Create: **Deployment Job**

## Basic Information

Create this deployment job by selecting assets and patches to be installed. Also define the deployment schedule and configure message options you want to display as reminders.

Title for your job Required



Qualys. Enterprise

Create: **Deployment Job**

STEPS 1/6

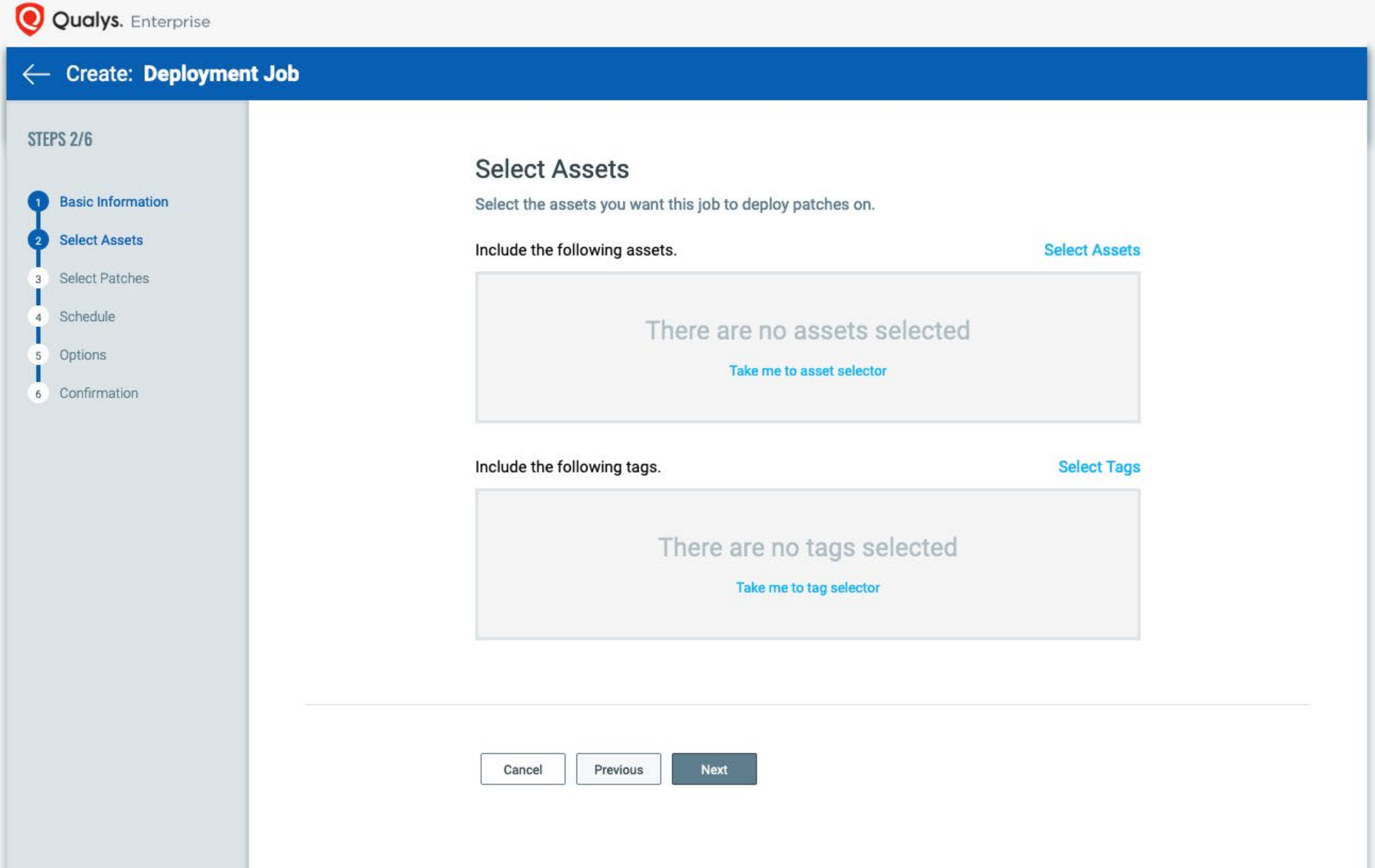
1. Basic Information
2. Select Assets
3. Select Patches
4. Schedule
5. Options
6. Confirmation

## Basic Information

Create this deployment job by selecting assets and patches to be installed. Also define the deployment schedule and configure message options you want to display as reminders.

Title for your job — Required

High Critical - CVE-2019-0708



Qualys. Enterprise

Create: Deployment Job

STEPS 2/6

1 Basic Information

2 Select Assets

3 Select Patches

4 Schedule

5 Options

6 Confirmation

## Select Assets

Select the assets you want this job to deploy patches on.

Include the following assets. Select Assets

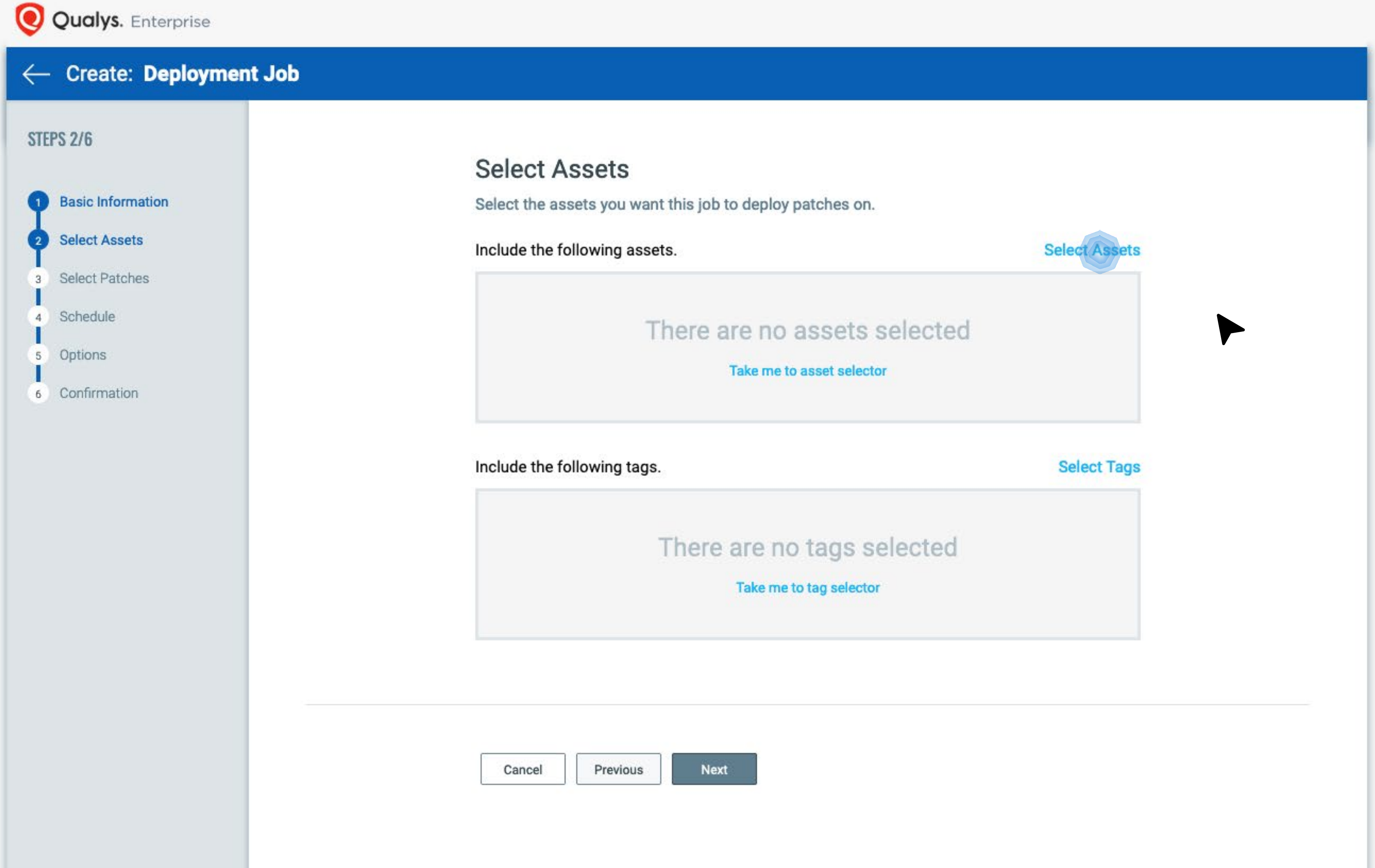
There are no assets selected

Take me to asset selector

Include the following tags. Select Tags

There are no tags selected

Take me to tag selector



## Select Assets

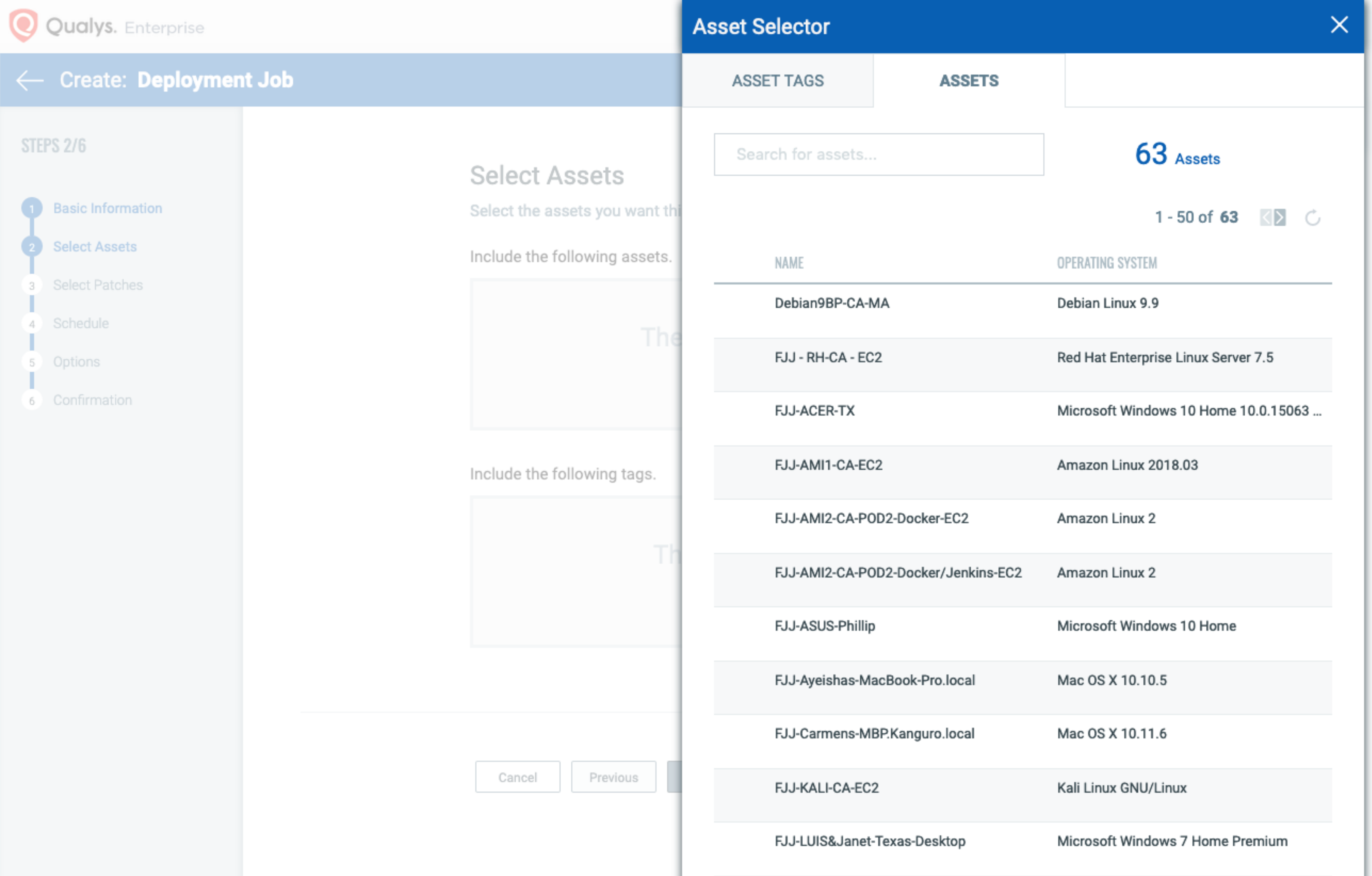
Select the assets you want this job to deploy patches on.

Include the following assets.

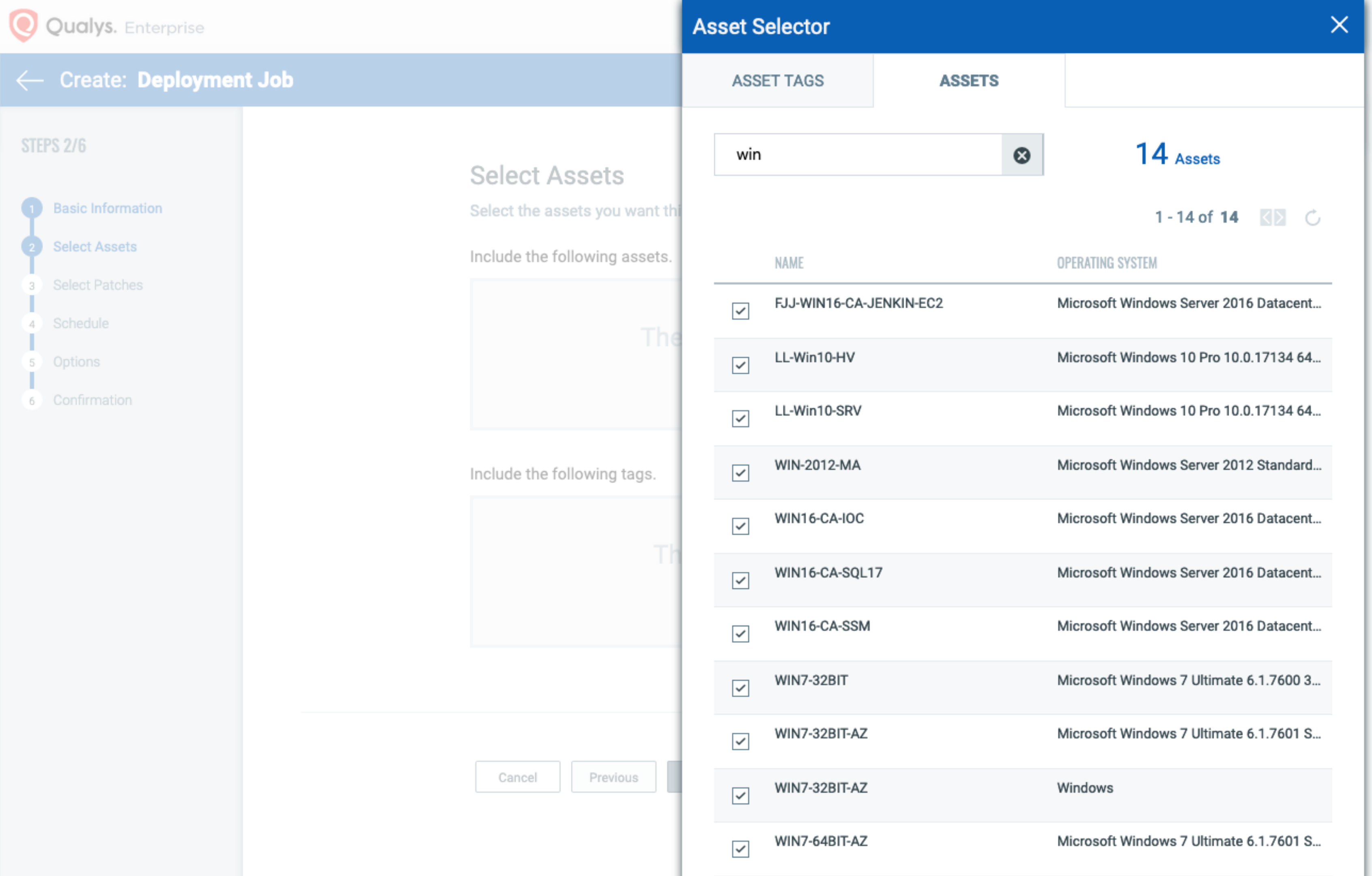
There are no assets selected

Include the following tags.

There are no tags selected



| NAME | OPERATING SYSTEM |
|---|---|
| Debian9BP-CA-MA | Debian Linux 9.9 |
| FJJ - RH-CA - EC2 | Red Hat Enterprise Linux Server 7.5 |
| FJJ-ACER-TX | Microsoft Windows 10 Home 10.0.15063 ... |
| FJJ-AMI1-CA-EC2 | Amazon Linux 2018.03 |
| FJJ-AMI2-CA-POD2-Docker-EC2 | Amazon Linux 2 |
| FJJ-AMI2-CA-POD2-Docker/Jenkins-EC2 | Amazon Linux 2 |
| FJJ-ASUS-Phillip | Microsoft Windows 10 Home |
| FJJ-Ayeishas-MacBook-Pro.local | Mac OS X 10.10.5 |
| FJJ-Carmens-MBP.Kanguro.local | Mac OS X 10.11.6 |
| FJJ-KALI-CA-EC2 | Kali Linux GNU/Linux |
| FJJ-LUIS&Janet-Texas-Desktop | Microsoft Windows 7 Home Premium |



Select Assets

Select the assets you want thi

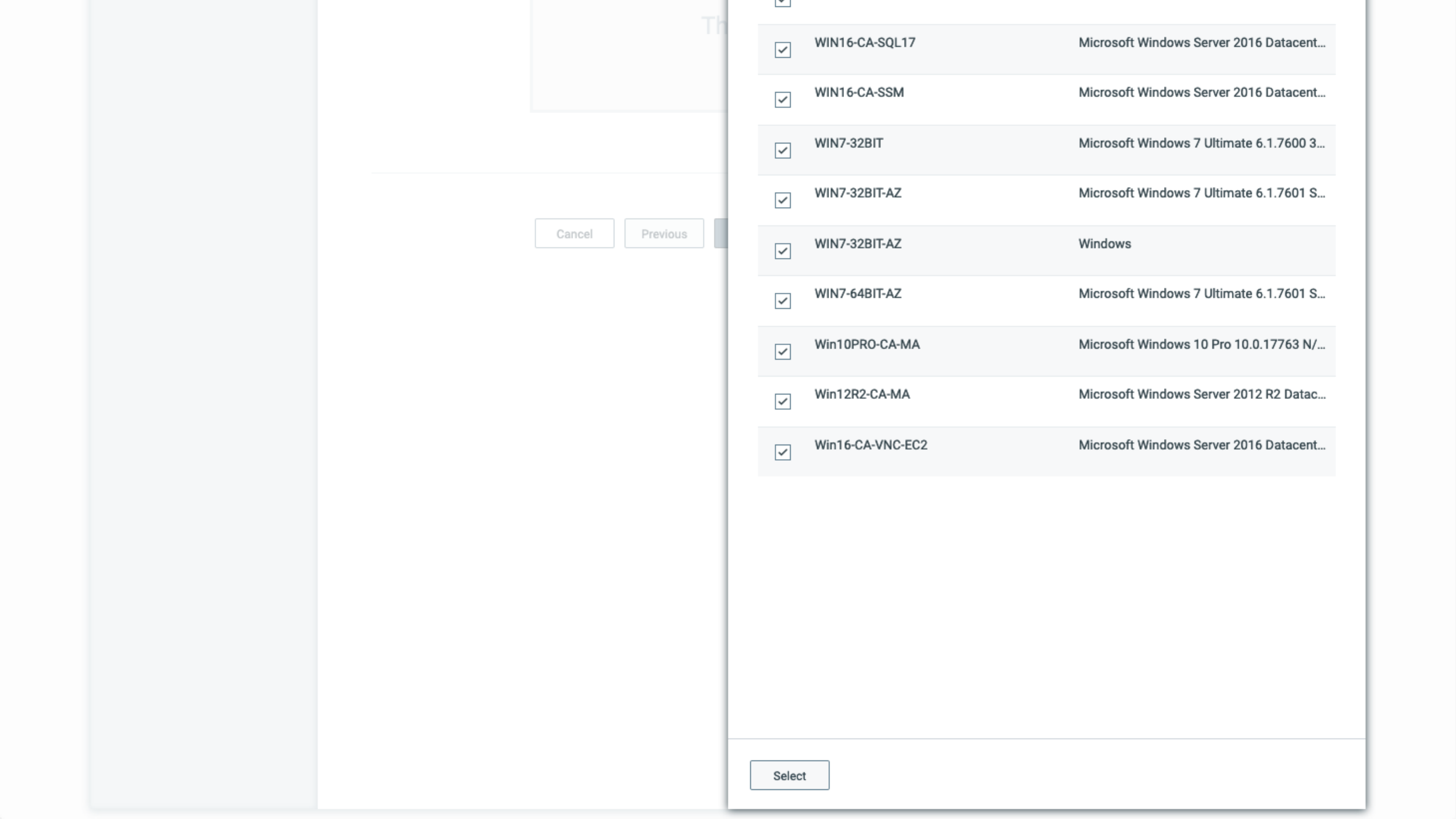
Include the following assets.

The

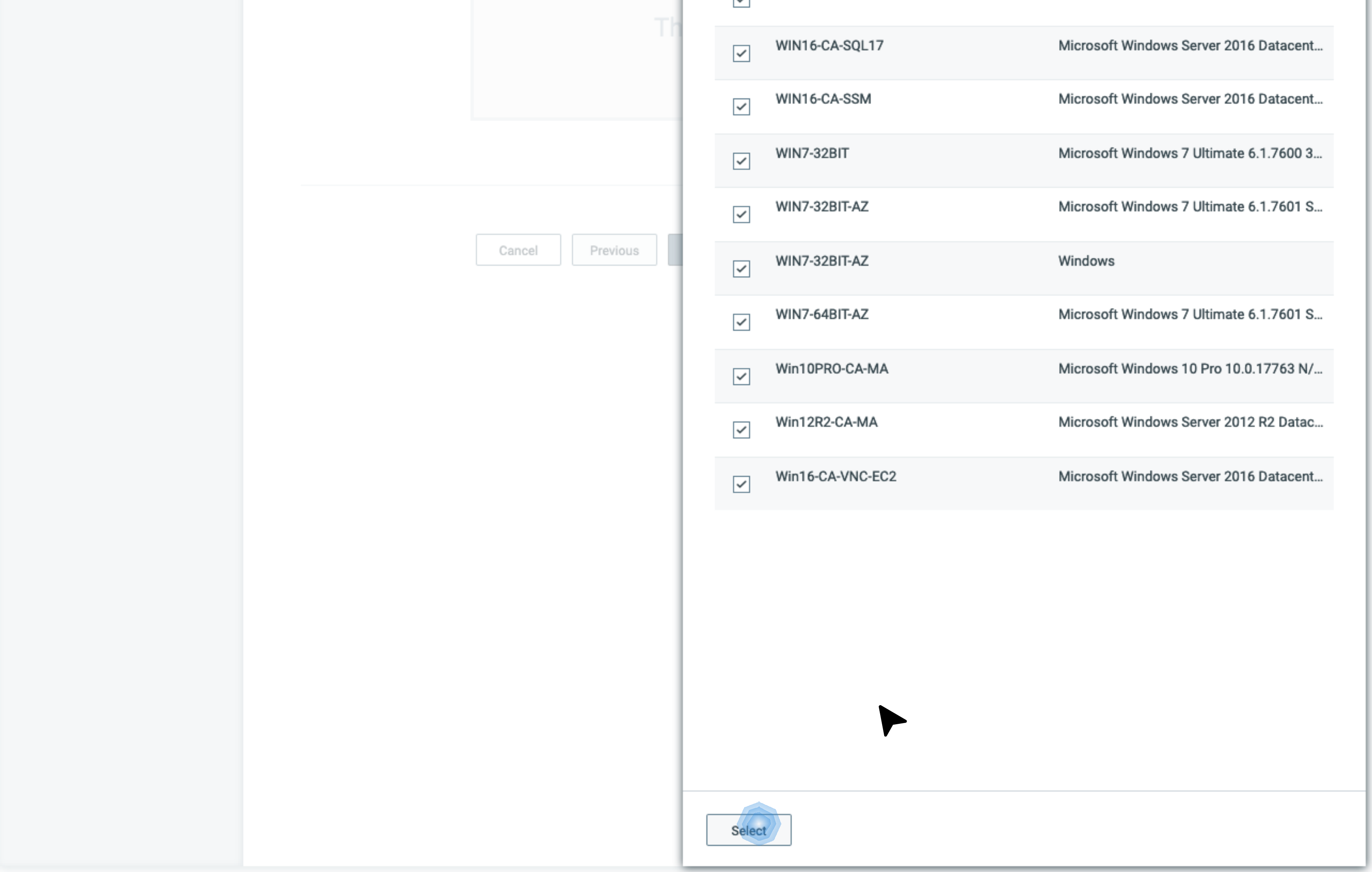
Include the following tags.

Th

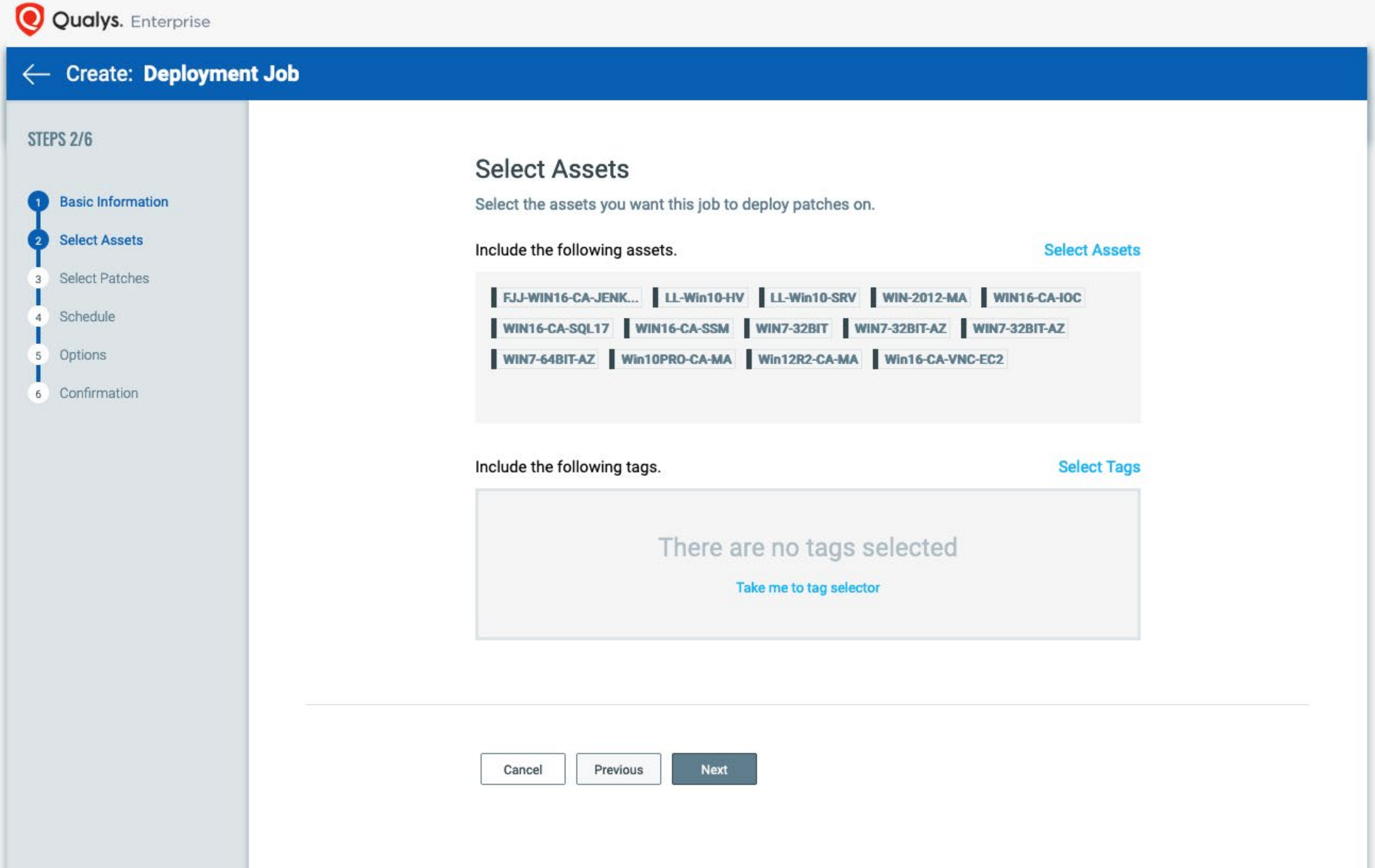
| | NAME | OPERATING SYSTEM |
|---|---|---|
| ☑ | FJJ-WIN16-CA-JENKIN-EC2 | Microsoft Windows Server 2016 Datacent... |
| ☑ | LL-Win10-HV | Microsoft Windows 10 Pro 10.0.17134 64... |
| ☑ | LL-Win10-SRV | Microsoft Windows 10 Pro 10.0.17134 64... |
| ☑ | WIN-2012-MA | Microsoft Windows Server 2012 Standard... |
| ☑ | WIN16-CA-IOC | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN16-CA-SQL17 | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN16-CA-SSM | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN7-32BIT | Microsoft Windows 7 Ultimate 6.1.7600 3... |
| ☑ | WIN7-32BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |
| ☑ | WIN7-32BIT-AZ | Windows |
| ☑ | WIN7-64BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |



| | | |
|---|---|---|
| ☑ | | |
| ☑ | WIN16-CA-SQL17 | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN16-CA-SSM | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN7-32BIT | Microsoft Windows 7 Ultimate 6.1.7600 3... |
| ☑ | WIN7-32BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |
| ☑ | WIN7-32BIT-AZ | Windows |
| ☑ | WIN7-64BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |
| ☑ | Win10PRO-CA-MA | Microsoft Windows 10 Pro 10.0.17763 N/... |
| ☑ | Win12R2-CA-MA | Microsoft Windows Server 2012 R2 Datac... |
| ☑ | Win16-CA-VNC-EC2 | Microsoft Windows Server 2016 Datacent... |



| | | |
|---|---|---|
| ☑ | WIN16-CA-SQL17 | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN16-CA-SSM | Microsoft Windows Server 2016 Datacent... |
| ☑ | WIN7-32BIT | Microsoft Windows 7 Ultimate 6.1.7600 3... |
| ☑ | WIN7-32BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |
| ☑ | WIN7-32BIT-AZ | Windows |
| ☑ | WIN7-64BIT-AZ | Microsoft Windows 7 Ultimate 6.1.7601 S... |
| ☑ | Win10PRO-CA-MA | Microsoft Windows 10 Pro 10.0.17763 N/... |
| ☑ | Win12R2-CA-MA | Microsoft Windows Server 2012 R2 Datac... |
| ☑ | Win16-CA-VNC-EC2 | Microsoft Windows Server 2016 Datacent... |



Qualys. Enterprise

Create: **Deployment Job**

STEPS 2/6

1 Basic Information
2 Select Assets
3 Select Patches
4 Schedule
5 Options
6 Confirmation

## Select Assets

Select the assets you want this job to deploy patches on.

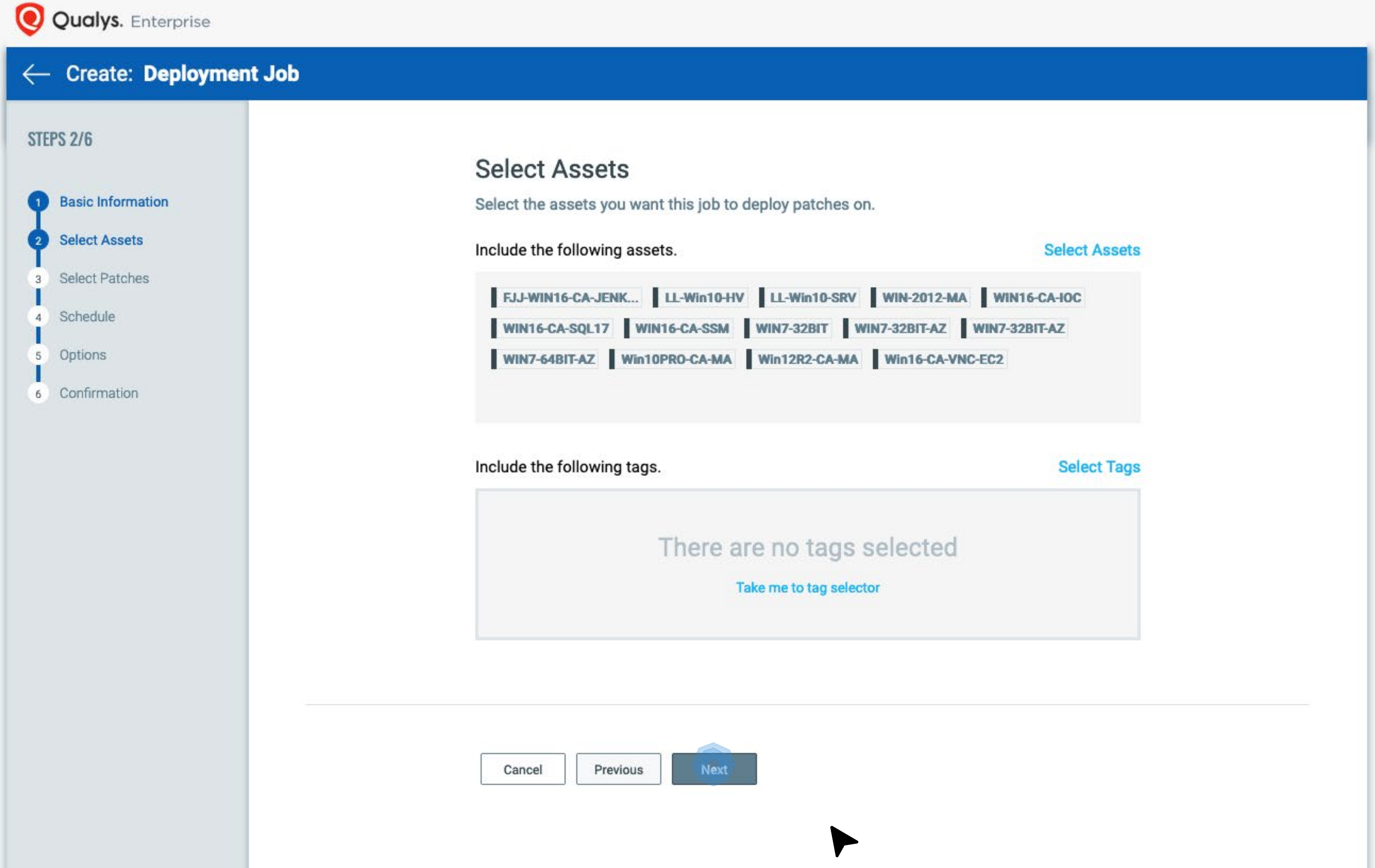
Include the following assets. Select Assets

FJJ-WIN16-CA-JENK... | LL-Win10-HV | LL-Win10-SRV | WIN-2012-MA | WIN16-CA-IOC | WIN16-CA-SQL17 | WIN16-CA-SSM | WIN7-32BIT | WIN7-32BIT-AZ | WIN7-32BIT-AZ | WIN7-64BIT-AZ | Win10PRO-CA-MA | Win12R2-CA-MA | Win16-CA-VNC-EC2

Include the following tags. Select Tags

There are no tags selected

Take me to tag selector



Qualys. Enterprise

Create: **Deployment Job**

STEPS 2/6

1 Basic Information
2 Select Assets
3 Select Patches
4 Schedule
5 Options
6 Confirmation

## Select Assets

Select the assets you want this job to deploy patches on.

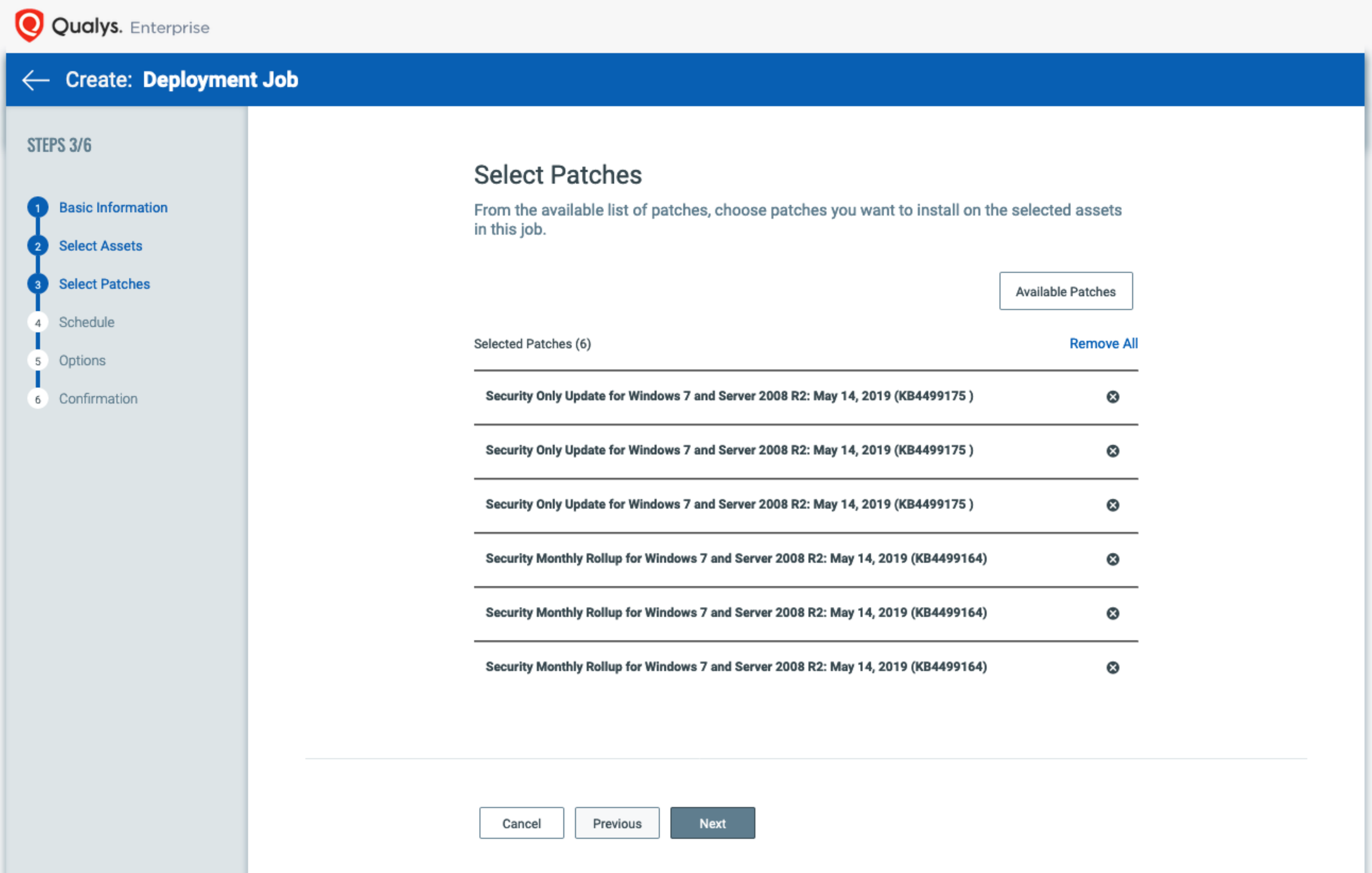
Include the following assets. Select Assets

FJJ-WIN16-CA-JENK... LL-Win10-HV LL-Win10-SRV WIN-2012-MA WIN16-CA-IOC
WIN16-CA-SQL17 WIN16-CA-SSM WIN7-32BIT WIN7-32BIT-AZ WIN7-32BIT-AZ
WIN7-64BIT-AZ Win10PRO-CA-MA Win12R2-CA-MA Win16-CA-VNC-EC2

Include the following tags. Select Tags

There are no tags selected

Take me to tag selector



## Select Patches

From the available list of patches, choose patches you want to install on the selected assets in this job.

Selected Patches (6)

**Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )**

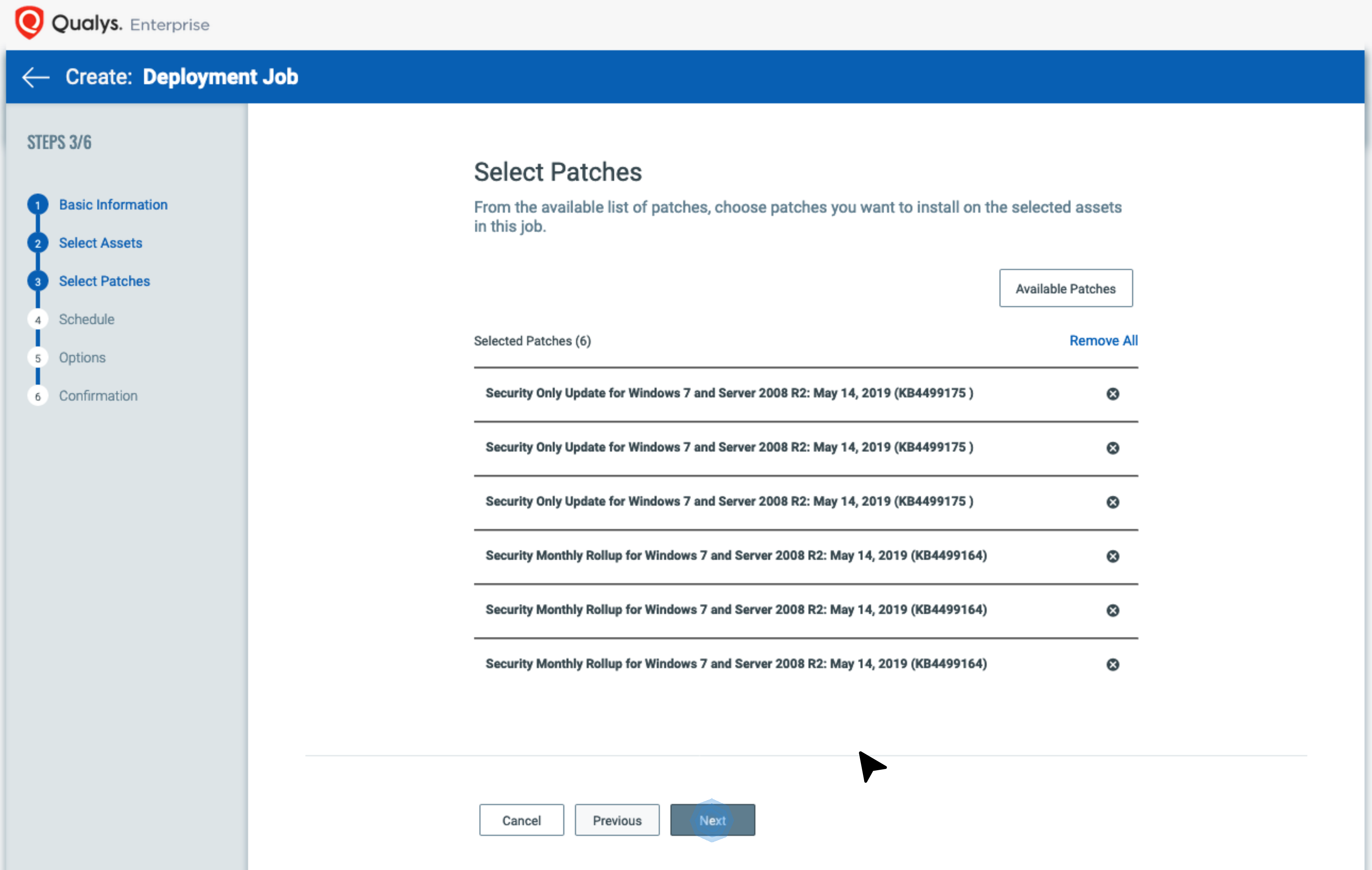
**Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )**

**Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )**

**Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)**

**Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)**

**Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)**

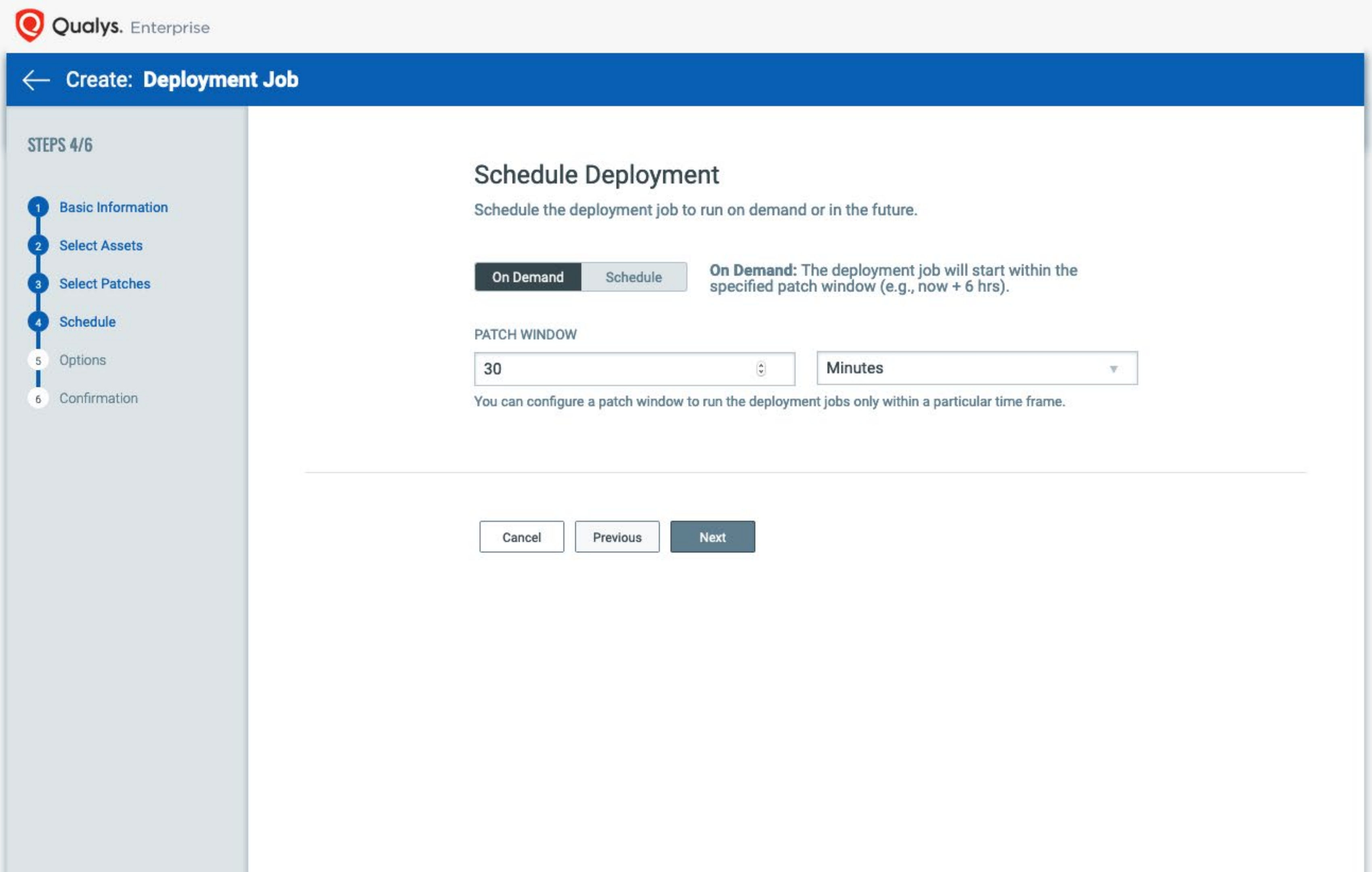


## Select Patches

From the available list of patches, choose patches you want to install on the selected assets in this job.

Selected Patches (6)

- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)



## Create: Deployment Job

STEPS 4/6

1 Basic Information
2 Select Assets
3 Select Patches
4 Schedule
5 Options
6 Confirmation

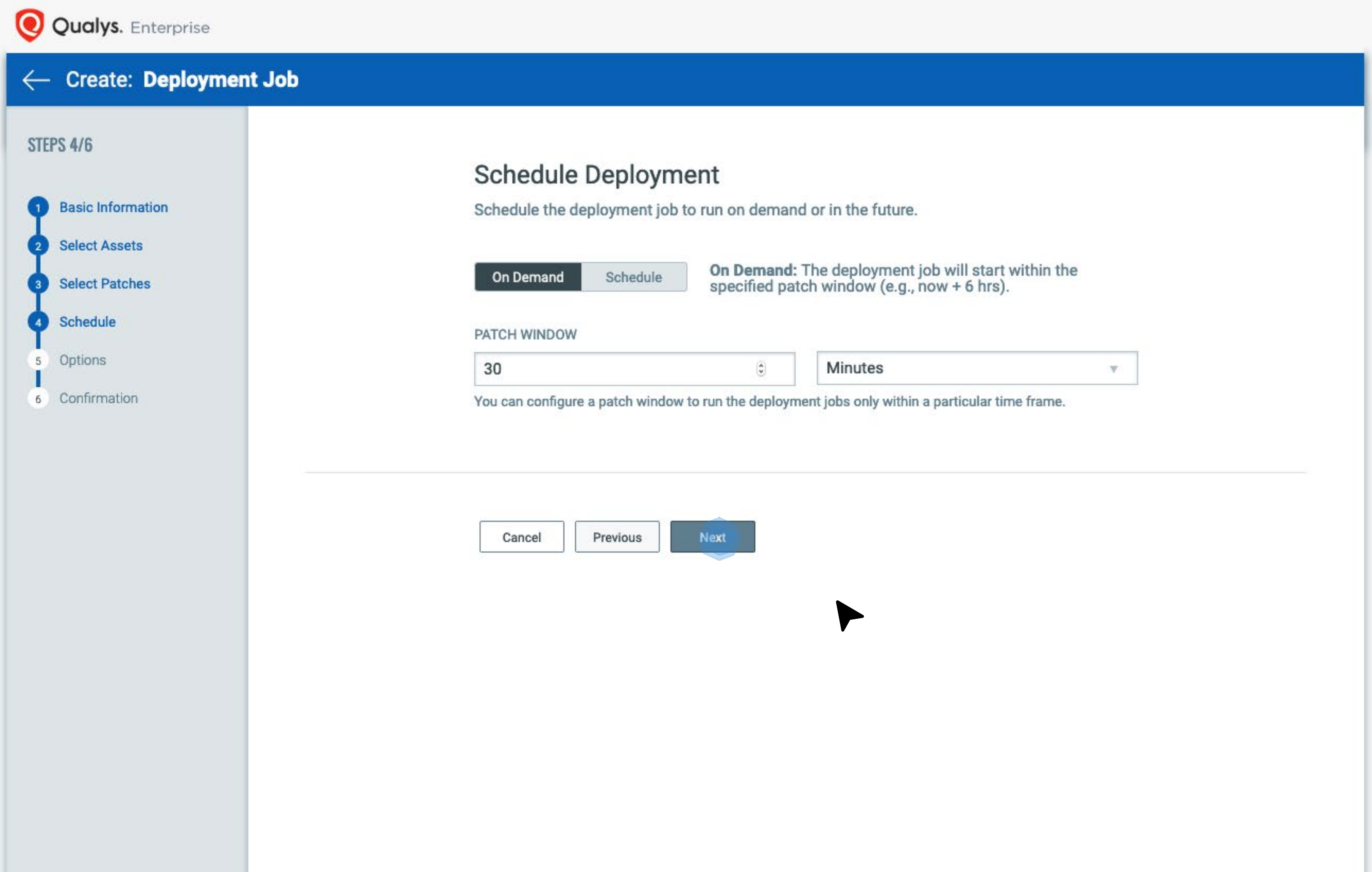
### Schedule Deployment

Schedule the deployment job to run on demand or in the future.

**On Demand:** The deployment job will start within the specified patch window (e.g., now + 6 hrs).

PATCH WINDOW: 30 Minutes

You can configure a patch window to run the deployment jobs only within a particular time frame.



Create: **Deployment Job**

## Schedule Deployment

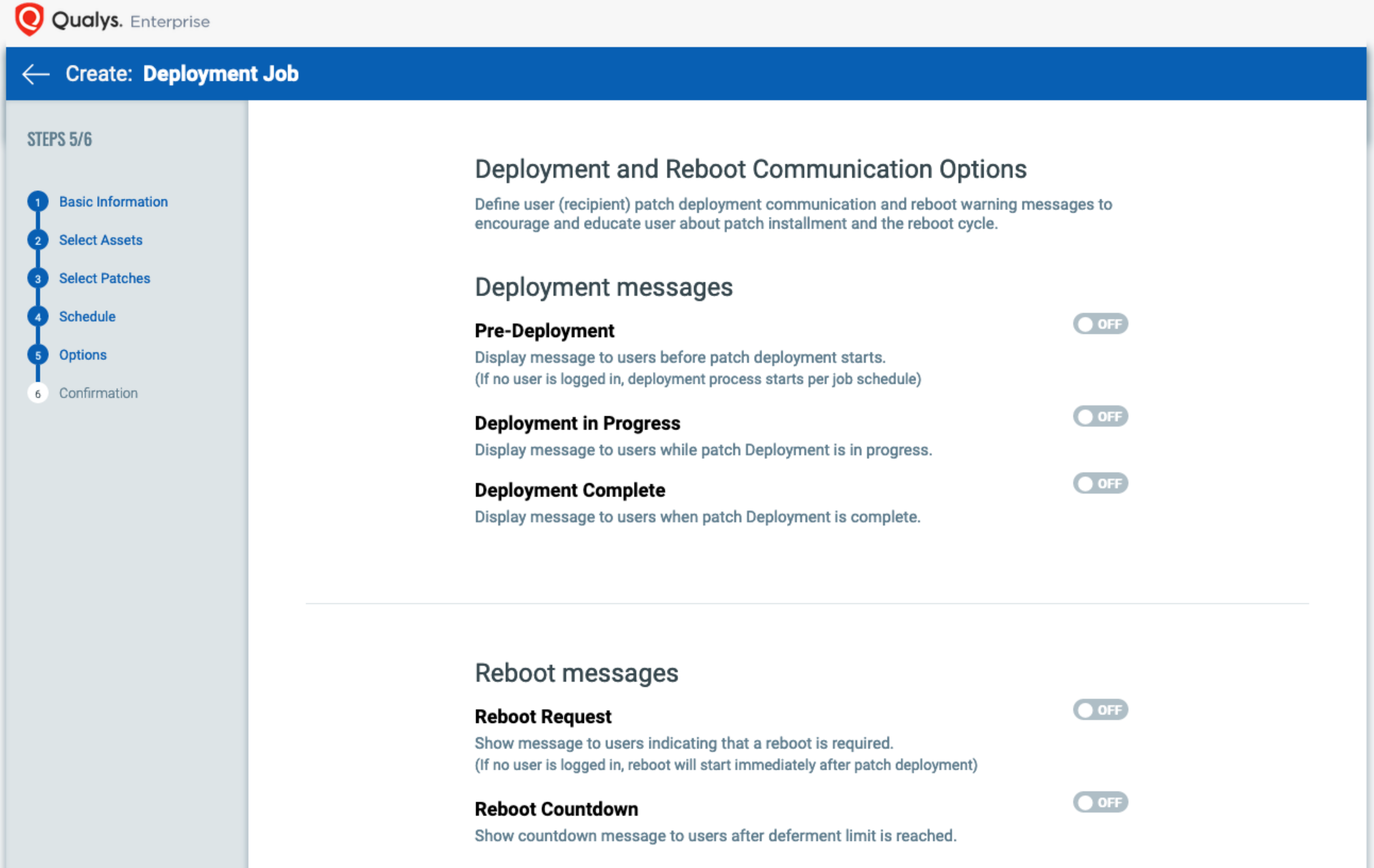
Schedule the deployment job to run on demand or in the future.

**On Demand:** The deployment job will start within the specified patch window (e.g., now + 6 hrs).

PATCH WINDOW

30 Minutes

You can configure a patch window to run the deployment jobs only within a particular time frame.



Create: **Deployment Job**

STEPS 5/6

1. Basic Information
2. Select Assets
3. Select Patches
4. Schedule
5. Options
6. Confirmation

## Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate user about patch installment and the reboot cycle.

### Deployment messages

**Pre-Deployment** OFF

Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

**Deployment in Progress** OFF

Display message to users while patch Deployment is in progress.

**Deployment Complete** OFF

Display message to users when patch Deployment is complete.

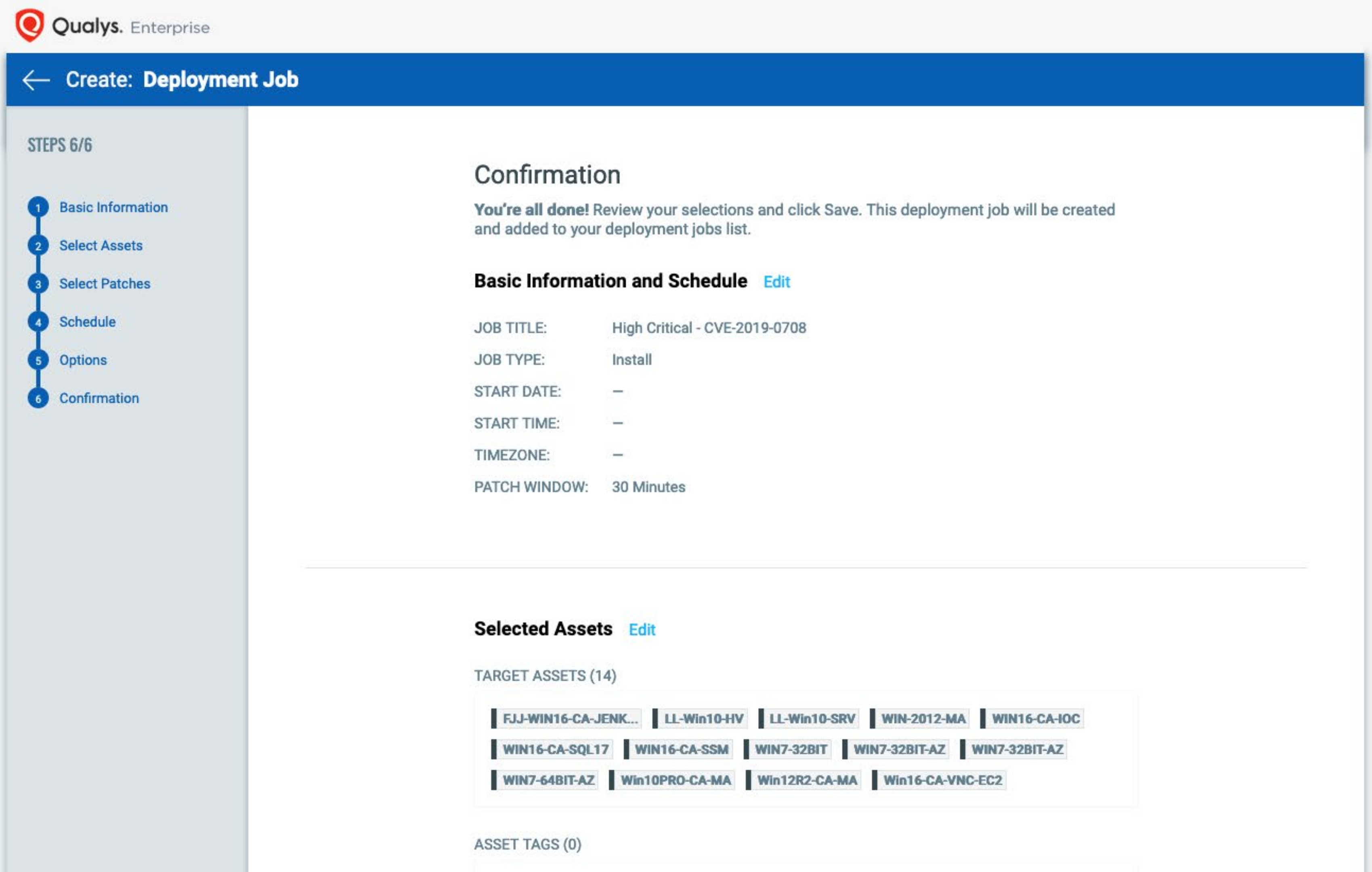
### Reboot messages

**Reboot Request** OFF

Show message to users indicating that a reboot is required.
(If no user is logged in, reboot will start immediately after patch deployment)

**Reboot Countdown** OFF

Show countdown message to users after deferment limit is reached.



## Create: Deployment Job

STEPS 6/6

1 Basic Information
2 Select Assets
3 Select Patches
4 Schedule
5 Options
6 Confirmation

### Confirmation

**You're all done!** Review your selections and click Save. This deployment job will be created and added to your deployment jobs list.

**Basic Information and Schedule** Edit

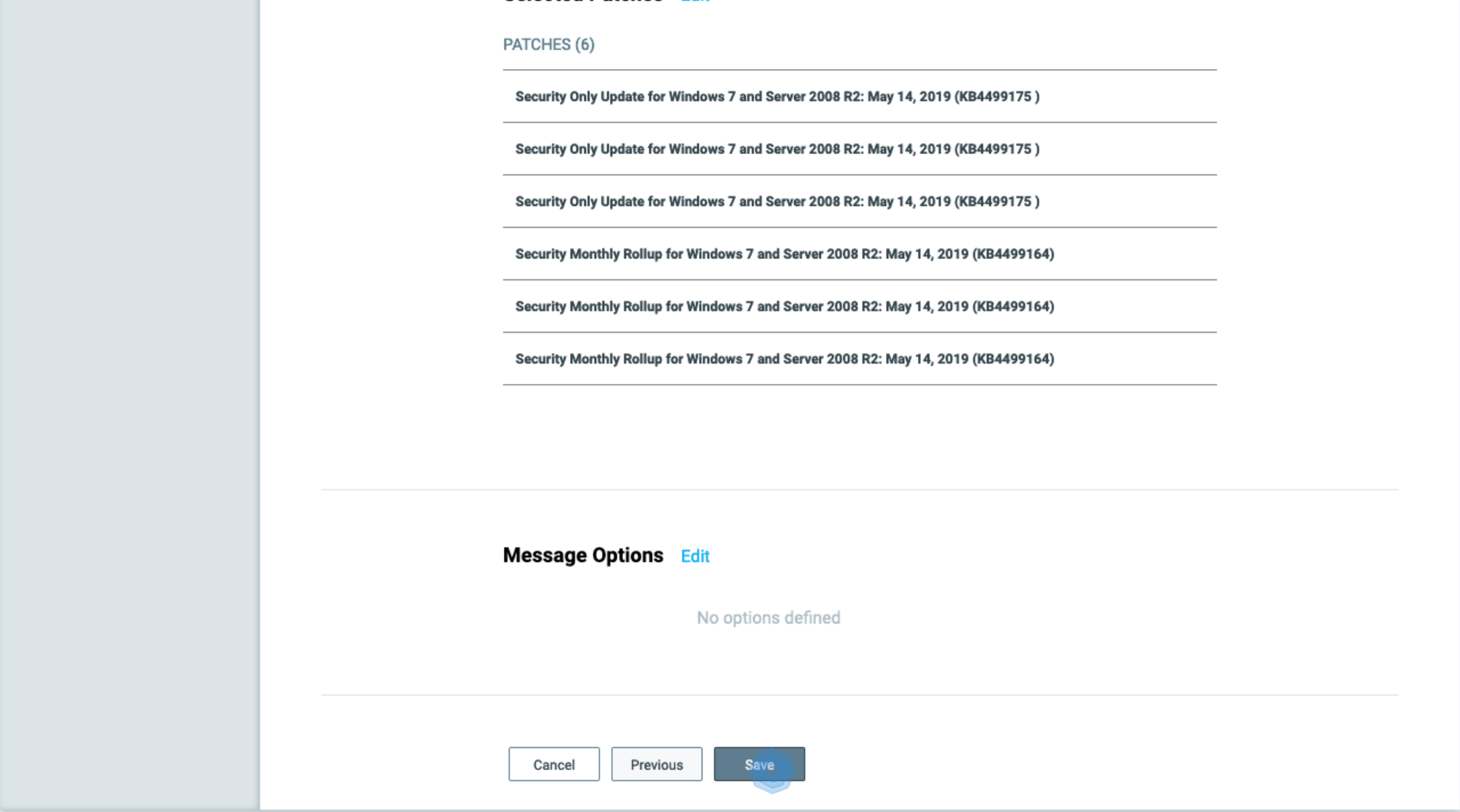
| | |
|---|---|
| JOB TITLE: | High Critical - CVE-2019-0708 |
| JOB TYPE: | Install |
| START DATE: | – |
| START TIME: | – |
| TIMEZONE: | – |
| PATCH WINDOW: | 30 Minutes |

**Selected Assets** Edit

TARGET ASSETS (14)

FJJ-WIN16-CA-JENK... LL-Win10-HV LL-Win10-SRV WIN-2012-MA WIN16-CA-IOC
WIN16-CA-SQL17 WIN16-CA-SSM WIN7-32BIT WIN7-32BIT-AZ WIN7-32BIT-AZ
WIN7-64BIT-AZ Win10PRO-CA-MA Win12R2-CA-MA Win16-CA-VNC-EC2

ASSET TAGS (0)



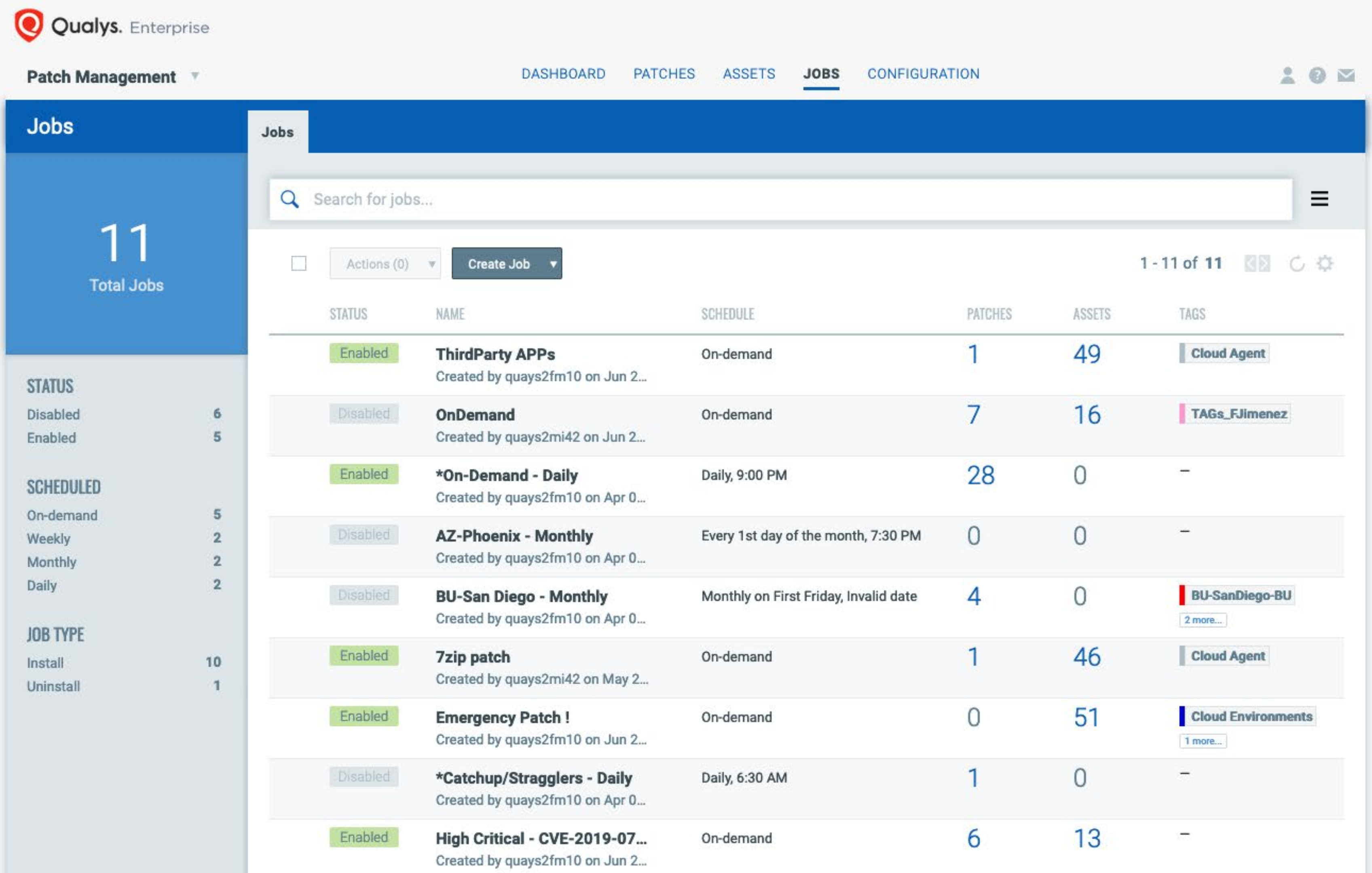
Selected Patches Edit

PATCHES (6)

- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Only Update for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499175 )
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)
- Security Monthly Rollup for Windows 7 and Server 2008 R2: May 14, 2019 (KB4499164)

Message Options Edit

No options defined



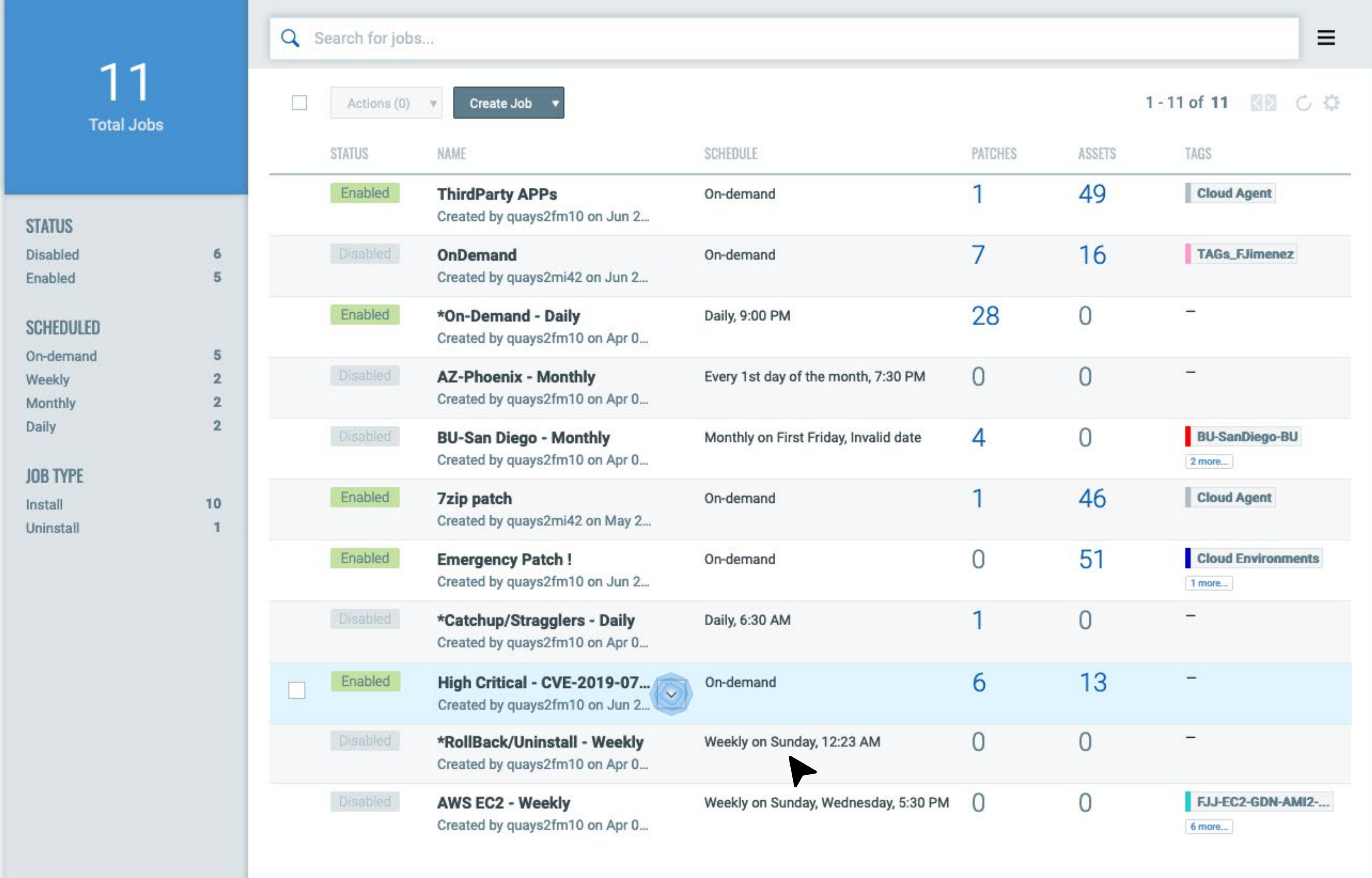
11
Total Jobs

| STATUS | |
|---|---|
| Disabled | 6 |
| Enabled | 5 |

| SCHEDULED | |
|---|---|
| On-demand | 5 |
| Weekly | 2 |
| Monthly | 2 |
| Daily | 2 |

| JOB TYPE | |
|---|---|
| Install | 10 |
| Uninstall | 1 |

| STATUS | NAME | SCHEDULE | PATCHES | ASSETS | TAGS |
|---|---|---|---|---|---|
| Enabled | ThirdParty APPs<br>Created by quays2fm10 on Jun 2... | On-demand | 1 | 49 | Cloud Agent |
| Disabled | OnDemand<br>Created by quays2mi42 on Jun 2... | On-demand | 7 | 16 | TAGs_FJimenez |
| Enabled | *On-Demand - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 9:00 PM | 28 | 0 | – |
| Disabled | AZ-Phoenix - Monthly<br>Created by quays2fm10 on Apr 0... | Every 1st day of the month, 7:30 PM | 0 | 0 | – |
| Disabled | BU-San Diego - Monthly<br>Created by quays2fm10 on Apr 0... | Monthly on First Friday, Invalid date | 4 | 0 | BU-SanDiego-BU<br>2 more... |
| Enabled | 7zip patch<br>Created by quays2mi42 on May 2... | On-demand | 1 | 46 | Cloud Agent |
| Enabled | Emergency Patch !<br>Created by quays2fm10 on Jun 2... | On-demand | 0 | 51 | Cloud Environments<br>1 more... |
| Disabled | *Catchup/Stragglers - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 6:30 AM | 1 | 0 | – |
| Enabled | High Critical - CVE-2019-07...<br>Created by quays2fm10 on Jun 2... | On-demand | 6 | 13 | – |



11
Total Jobs

STATUS

| | |
|---|---|
| Disabled | 6 |
| Enabled | 5 |

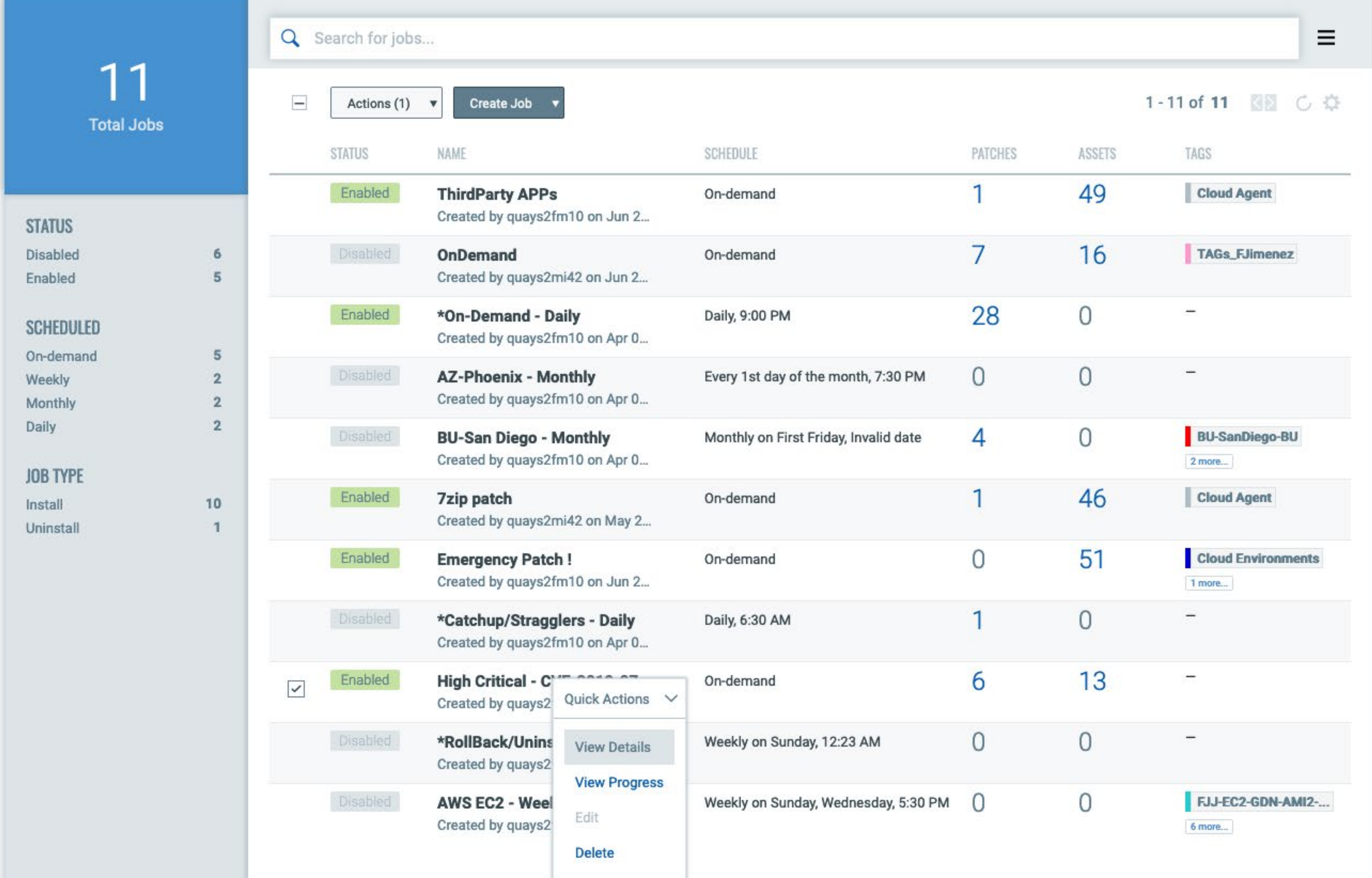
SCHEDULED

| | |
|---|---|
| On-demand | 5 |
| Weekly | 2 |
| Monthly | 2 |
| Daily | 2 |

JOB TYPE

| | |
|---|---|
| Install | 10 |
| Uninstall | 1 |

| STATUS | NAME | SCHEDULE | PATCHES | ASSETS | TAGS |
|---|---|---|---|---|---|
| Enabled | ThirdParty APPs<br>Created by quays2fm10 on Jun 2... | On-demand | 1 | 49 | Cloud Agent |
| Disabled | OnDemand<br>Created by quays2mi42 on Jun 2... | On-demand | 7 | 16 | TAGs_FJimenez |
| Enabled | *On-Demand - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 9:00 PM | 28 | 0 | – |
| Disabled | AZ-Phoenix - Monthly<br>Created by quays2fm10 on Apr 0... | Every 1st day of the month, 7:30 PM | 0 | 0 | – |
| Disabled | BU-San Diego - Monthly<br>Created by quays2fm10 on Apr 0... | Monthly on First Friday, Invalid date | 4 | 0 | BU-SanDiego-BU<br>2 more... |
| Enabled | 7zip patch<br>Created by quays2mi42 on May 2... | On-demand | 1 | 46 | Cloud Agent |
| Enabled | Emergency Patch !<br>Created by quays2fm10 on Jun 2... | On-demand | 0 | 51 | Cloud Environments<br>1 more... |
| Disabled | *Catchup/Stragglers - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 6:30 AM | 1 | 0 | – |
| Enabled | High Critical - CVE-2019-07...<br>Created by quays2fm10 on Jun 2... | On-demand | 6 | 13 | – |
| Disabled | *RollBack/Uninstall - Weekly<br>Created by quays2fm10 on Apr 0... | Weekly on Sunday, 12:23 AM | 0 | 0 | – |
| Disabled | AWS EC2 - Weekly<br>Created by quays2fm10 on Apr 0... | Weekly on Sunday, Wednesday, 5:30 PM | 0 | 0 | FJJ-EC2-GDN-AMI2-...<br>6 more... |



11
Total Jobs

**STATUS**

| | |
|---|---|
| Disabled | 6 |
| Enabled | 5 |

**SCHEDULED**

| | |
|---|---|
| On-demand | 5 |
| Weekly | 2 |
| Monthly | 2 |
| Daily | 2 |

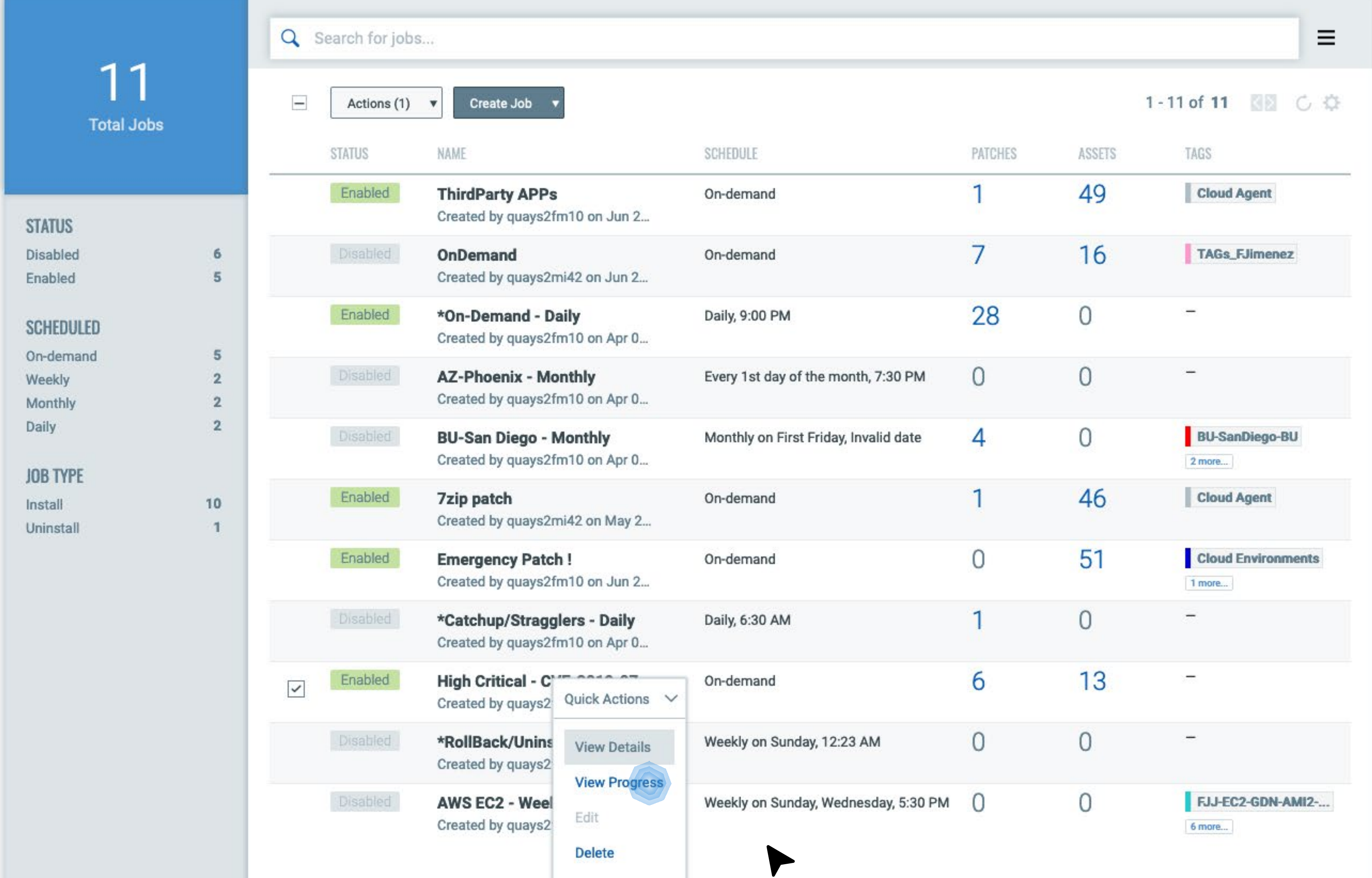
**JOB TYPE**

| | |
|---|---|
| Install | 10 |
| Uninstall | 1 |

Search for jobs...

Actions (1) ▾ | Create Job ▾ | 1 - 11 of 11

| | STATUS | NAME | SCHEDULE | PATCHES | ASSETS | TAGS |
|---|---|---|---|---|---|---|
| | Enabled | **ThirdParty APPs**<br>Created by quays2fm10 on Jun 2... | On-demand | 1 | 49 | Cloud Agent |
| | Disabled | **OnDemand**<br>Created by quays2mi42 on Jun 2... | On-demand | 7 | 16 | TAGs_FJimenez |
| | Enabled | ***On-Demand - Daily**<br>Created by quays2fm10 on Apr 0... | Daily, 9:00 PM | 28 | 0 | – |
| | Disabled | **AZ-Phoenix - Monthly**<br>Created by quays2fm10 on Apr 0... | Every 1st day of the month, 7:30 PM | 0 | 0 | – |
| | Disabled | **BU-San Diego - Monthly**<br>Created by quays2fm10 on Apr 0... | Monthly on First Friday, Invalid date | 4 | 0 | BU-SanDiego-BU<br>2 more... |
| | Enabled | **7zip patch**<br>Created by quays2mi42 on May 2... | On-demand | 1 | 46 | Cloud Agent |
| | Enabled | **Emergency Patch !**<br>Created by quays2fm10 on Jun 2... | On-demand | 0 | 51 | Cloud Environments<br>1 more... |
| | Disabled | ***Catchup/Stragglers - Daily**<br>Created by quays2fm10 on Apr 0... | Daily, 6:30 AM | 1 | 0 | – |
| ☑ | Enabled | **High Critical - C**<br>Created by quays2 | On-demand | 6 | 13 | – |
| | Disabled | ***RollBack/Unins**<br>Created by quays2 | Weekly on Sunday, 12:23 AM | 0 | 0 | – |
| | Disabled | **AWS EC2 - Weel**<br>Created by quays2 | Weekly on Sunday, Wednesday, 5:30 PM | 0 | 0 | FJJ-EC2-GDN-AMI2-...<br>6 more... |



11
Total Jobs

STATUS

| | |
|---|---|
| Disabled | 6 |
| Enabled | 5 |

SCHEDULED

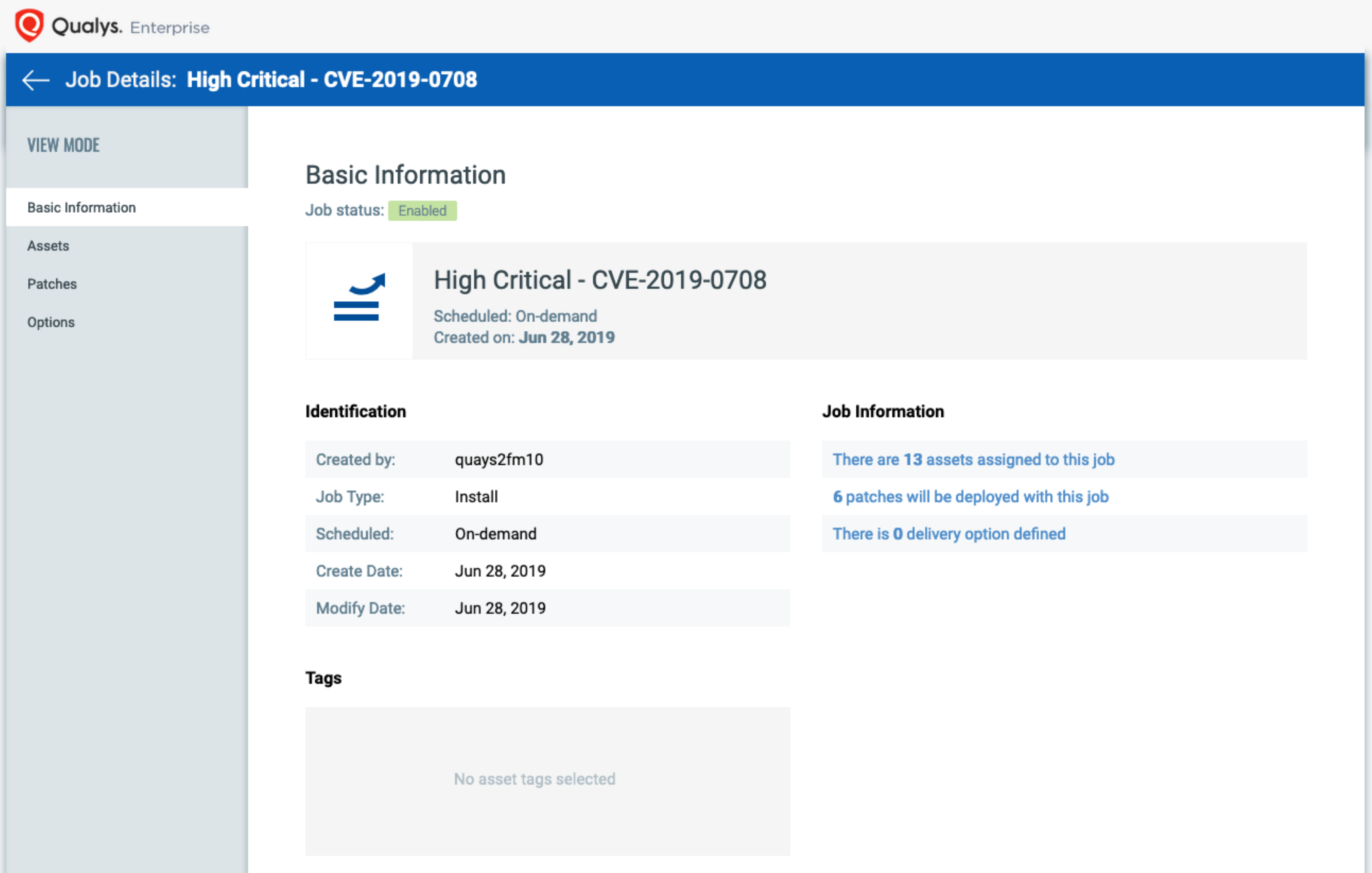
| | |
|---|---|
| On-demand | 5 |
| Weekly | 2 |
| Monthly | 2 |
| Daily | 2 |

JOB TYPE

| | |
|---|---|
| Install | 10 |
| Uninstall | 1 |

1 - 11 of 11

| | STATUS | NAME | SCHEDULE | PATCHES | ASSETS | TAGS |
|---|---|---|---|---|---|---|
| | Enabled | ThirdParty APPs<br>Created by quays2fm10 on Jun 2... | On-demand | 1 | 49 | Cloud Agent |
| | Disabled | OnDemand<br>Created by quays2mi42 on Jun 2... | On-demand | 7 | 16 | TAGs_FJimenez |
| | Enabled | *On-Demand - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 9:00 PM | 28 | 0 | – |
| | Disabled | AZ-Phoenix - Monthly<br>Created by quays2fm10 on Apr 0... | Every 1st day of the month, 7:30 PM | 0 | 0 | – |
| | Disabled | BU-San Diego - Monthly<br>Created by quays2fm10 on Apr 0... | Monthly on First Friday, Invalid date | 4 | 0 | BU-SanDiego-BU<br>2 more... |
| | Enabled | 7zip patch<br>Created by quays2mi42 on May 2... | On-demand | 1 | 46 | Cloud Agent |
| | Enabled | Emergency Patch !<br>Created by quays2fm10 on Jun 2... | On-demand | 0 | 51 | Cloud Environments<br>1 more... |
| | Disabled | *Catchup/Stragglers - Daily<br>Created by quays2fm10 on Apr 0... | Daily, 6:30 AM | 1 | 0 | – |
| ☑ | Enabled | High Critical - C<br>Created by quays2 | On-demand | 6 | 13 | – |
| | Disabled | *RollBack/Unins<br>Created by quays2 | Weekly on Sunday, 12:23 AM | 0 | 0 | – |
| | Disabled | AWS EC2 - Weel<br>Created by quays2 | Weekly on Sunday, Wednesday, 5:30 PM | 0 | 0 | FJJ-EC2-GDN-AMI2-...<br>6 more... |



Job Details: **High Critical - CVE-2019-0708**

## Basic Information

Job status: Enabled

### High Critical - CVE-2019-0708

Scheduled: On-demand
Created on: **Jun 28, 2019**

**Identification**

| | |
|---|---|
| Created by: | quays2fm10 |
| Job Type: | Install |
| Scheduled: | On-demand |
| Create Date: | Jun 28, 2019 |
| Modify Date: | Jun 28, 2019 |

**Job Information**

There are **13** assets assigned to this job

**6** patches will be deployed with this job

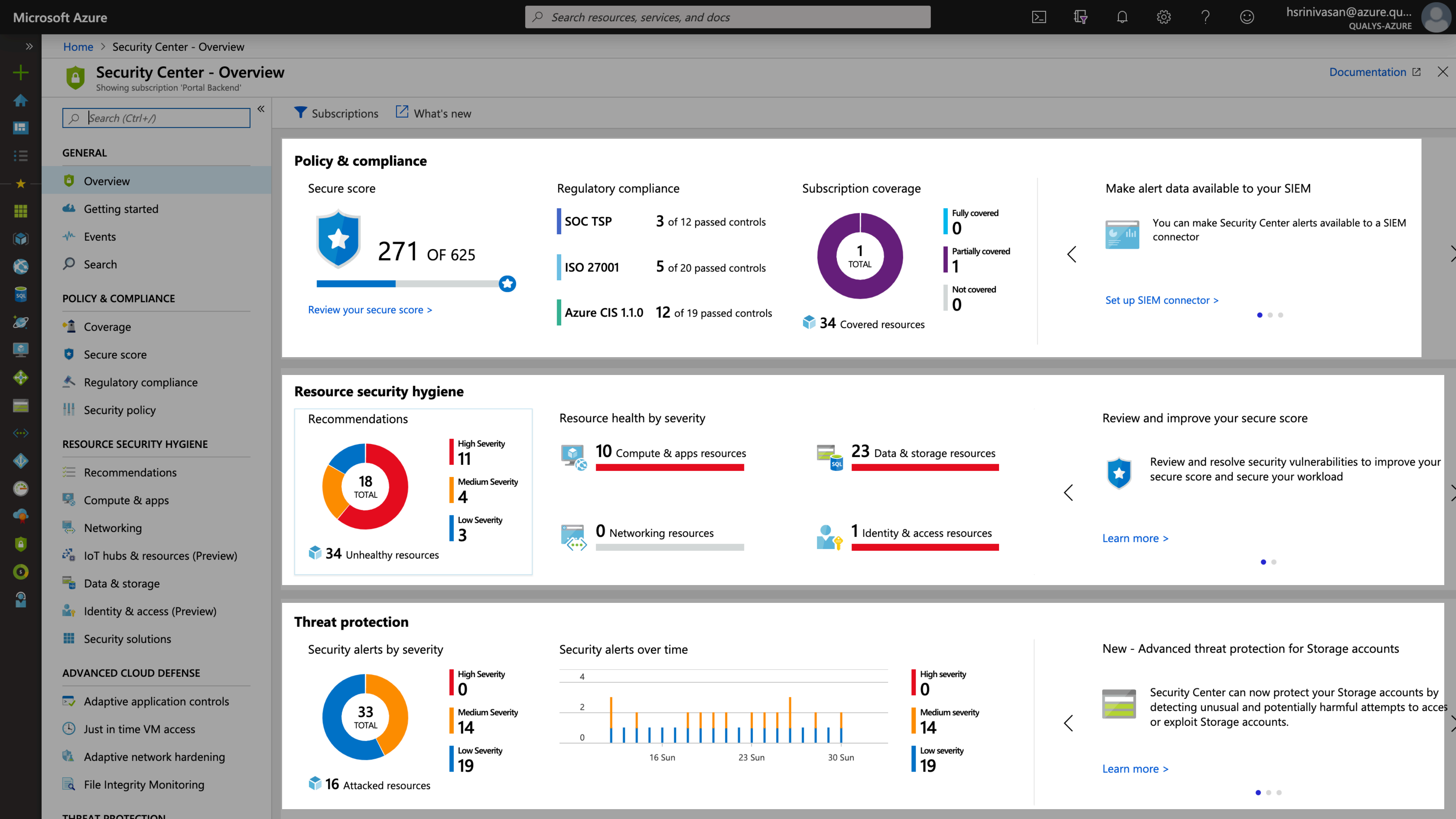
There is **0** delivery option defined

**Tags**

No asset tags selected

# DEMO

Security built in Azure – not bolted on



## Security Center - Overview

Showing subscription 'Portal Backend'

### Policy & compliance

**Secure score**

271 OF 625

Review your secure score >

**Regulatory compliance**

| | |
|---|---|
| SOC TSP | 3 of 12 passed controls |
| ISO 27001 | 5 of 20 passed controls |
| Azure CIS 1.1.0 | 12 of 19 passed controls |

**Subscription coverage**

1 TOTAL

Fully covered 0

Partially covered 1

Not covered 0

34 Covered resources

**Make alert data available to your SIEM**

You can make Security Center alerts available to a SIEM connector

Set up SIEM connector >

### Resource security hygiene

**Recommendations**

18 TOTAL

High Severity 11

Medium Severity 4

Low Severity 3

34 Unhealthy resources

**Resource health by severity**

10 Compute & apps resources

23 Data & storage resources

0 Networking resources

1 Identity & access resources

**Review and improve your secure score**

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

### Threat protection

**Security alerts by severity**

33 TOTAL

High Severity 0

Medium Severity 14

Low Severity 19

16 Attacked resources

**Security alerts over time**

High severity 0

Medium severity 14

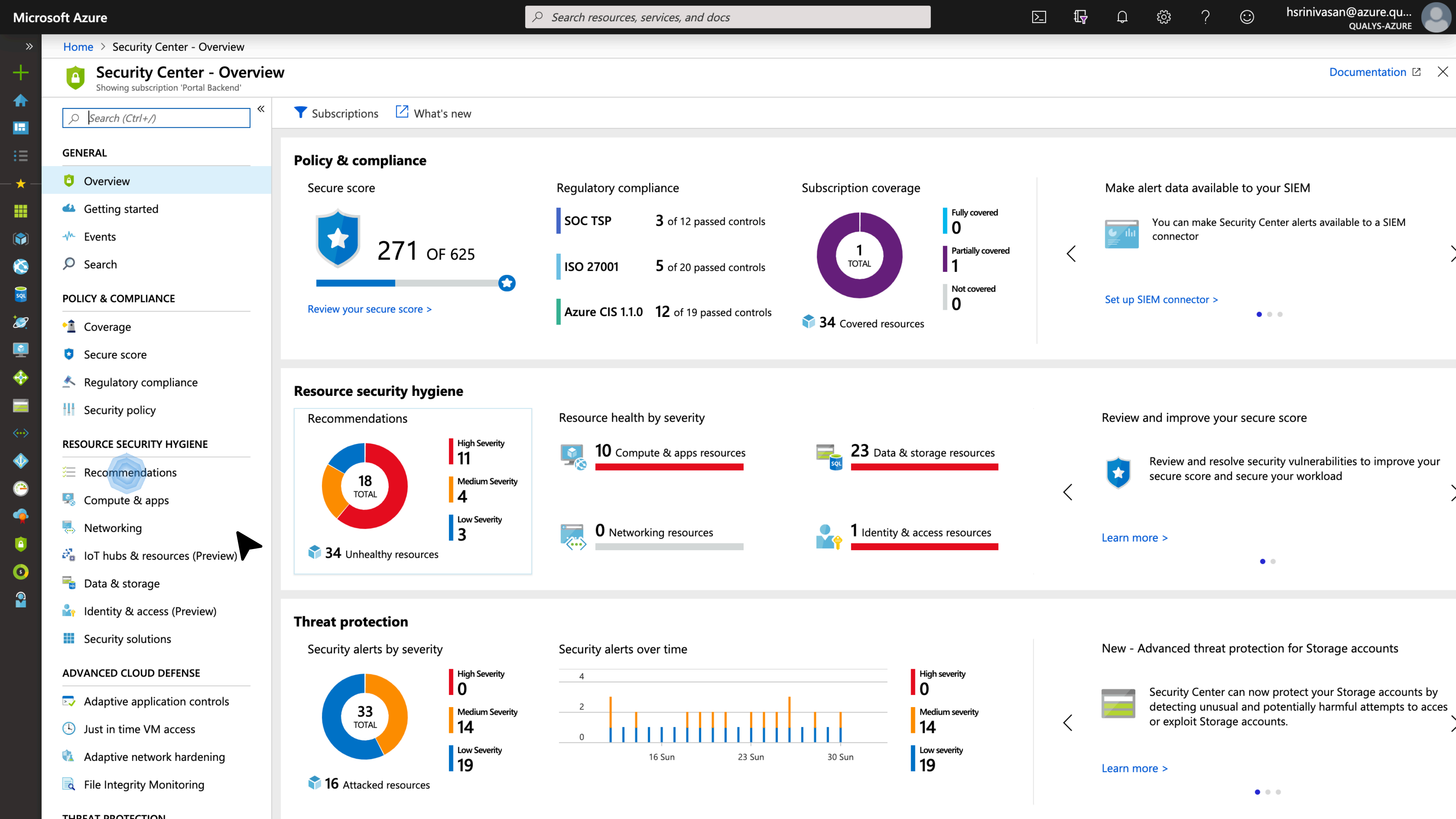
Low severity 19

**New - Advanced threat protection for Storage accounts**

Security Center can now protect your Storage accounts by detecting unusual and potentially harmful attempts to acces

or exploit Storage accounts.

Learn more >



Microsoft Azure

Search resources, services, and docs

hsrinivasan@azure.qu...
QUALYS-AZURE

Home > Security Center - Overview

# Security Center - Overview

Showing subscription 'Portal Backend'

Documentation

Search (Ctrl+/)

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Secure score
- Regulatory compliance
- Security policy

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- IoT hubs & resources (Preview)
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

THREAT PROTECTION

Subscriptions    What's new

## Policy & compliance

### Secure score

271 OF 625

Review your secure score >

### Regulatory compliance

| | |
|---|---|
| SOC TSP | 3 of 12 passed controls |
| ISO 27001 | 5 of 20 passed controls |
| Azure CIS 1.1.0 | 12 of 19 passed controls |

### Subscription coverage

1 TOTAL

| | |
|---|---|
| Fully covered | 0 |
| Partially covered | 1 |
| Not covered | 0 |

34 Covered resources

### Make alert data available to your SIEM

You can make Security Center alerts available to a SIEM connector

Set up SIEM connector >

## Resource security hygiene

### Recommendations

18 TOTAL

| | |
|---|---|
| High Severity | 11 |
| Medium Severity | 4 |
| Low Severity | 3 |

34 Unhealthy resources

### Resource health by severity

10 Compute & apps resources

23 Data & storage resources

0 Networking resources

1 Identity & access resources

### Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

## Threat protection

### Security alerts by severity

33 TOTAL

| | |
|---|---|
| High Severity | 0 |
| Medium Severity | 14 |
| Low Severity | 19 |

16 Attacked resources

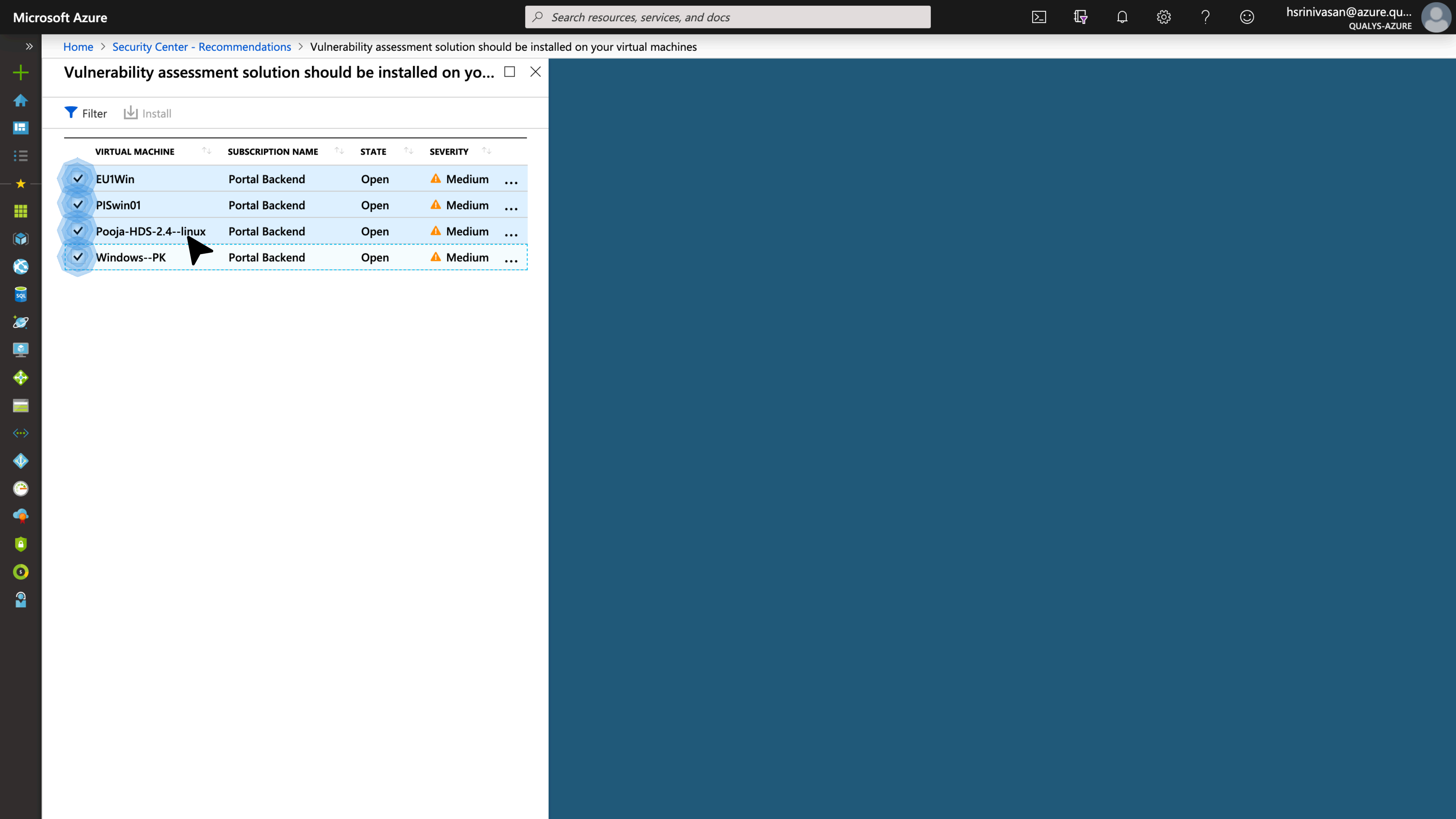
### Security alerts over time

| | |
|---|---|
| High severity | 0 |
| Medium severity | 14 |
| Low severity | 19 |

### New - Advanced threat protection for Storage accounts

Security Center can now protect your Storage accounts by detecting unusual and potentially harmful attempts to acces or exploit Storage accounts.

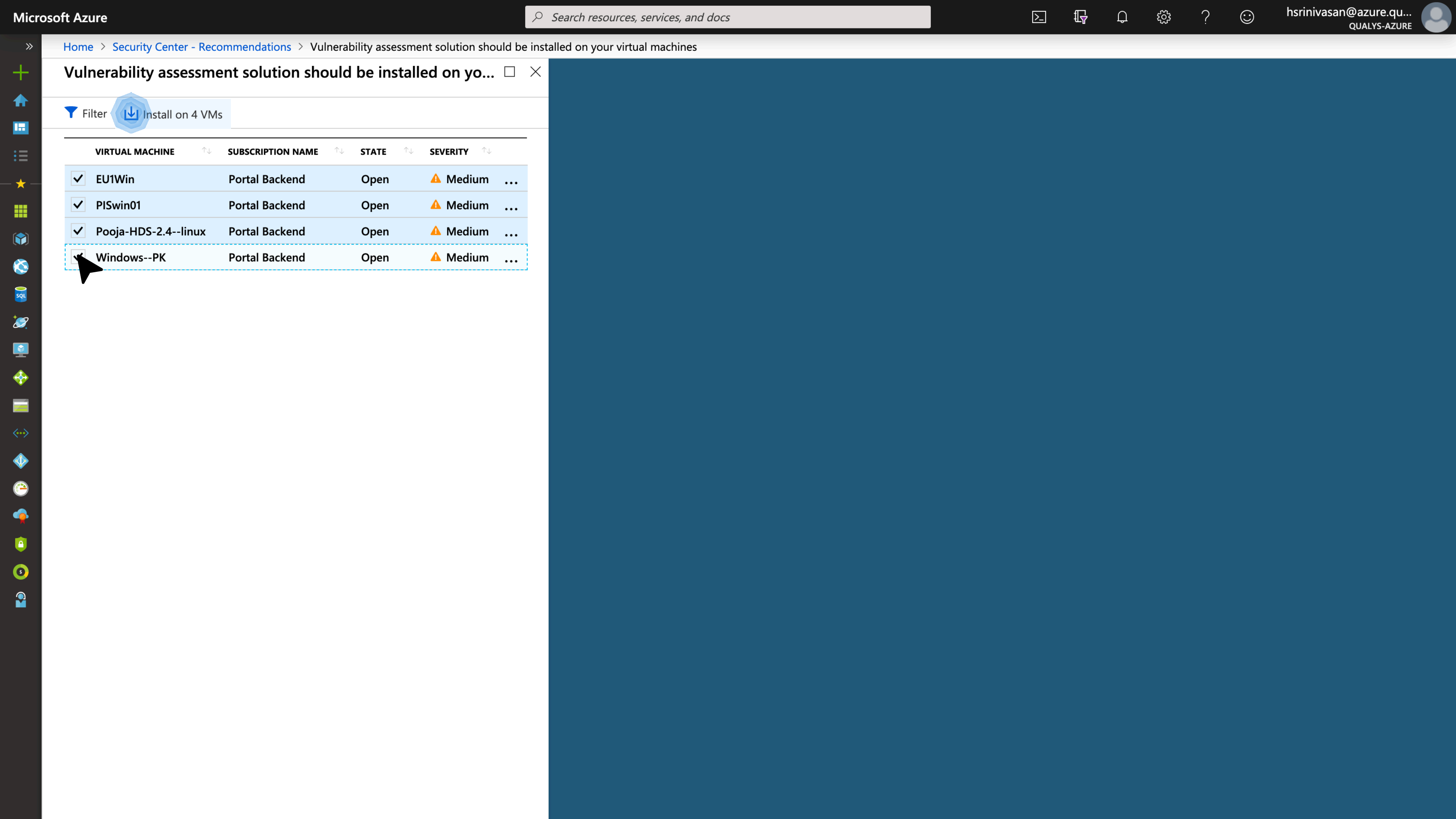
Learn more >



Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > Security Center - Recommendations > Vulnerability assessment solution should be installed on your virtual machines

Vulnerability assessment solution should be installed on yo...

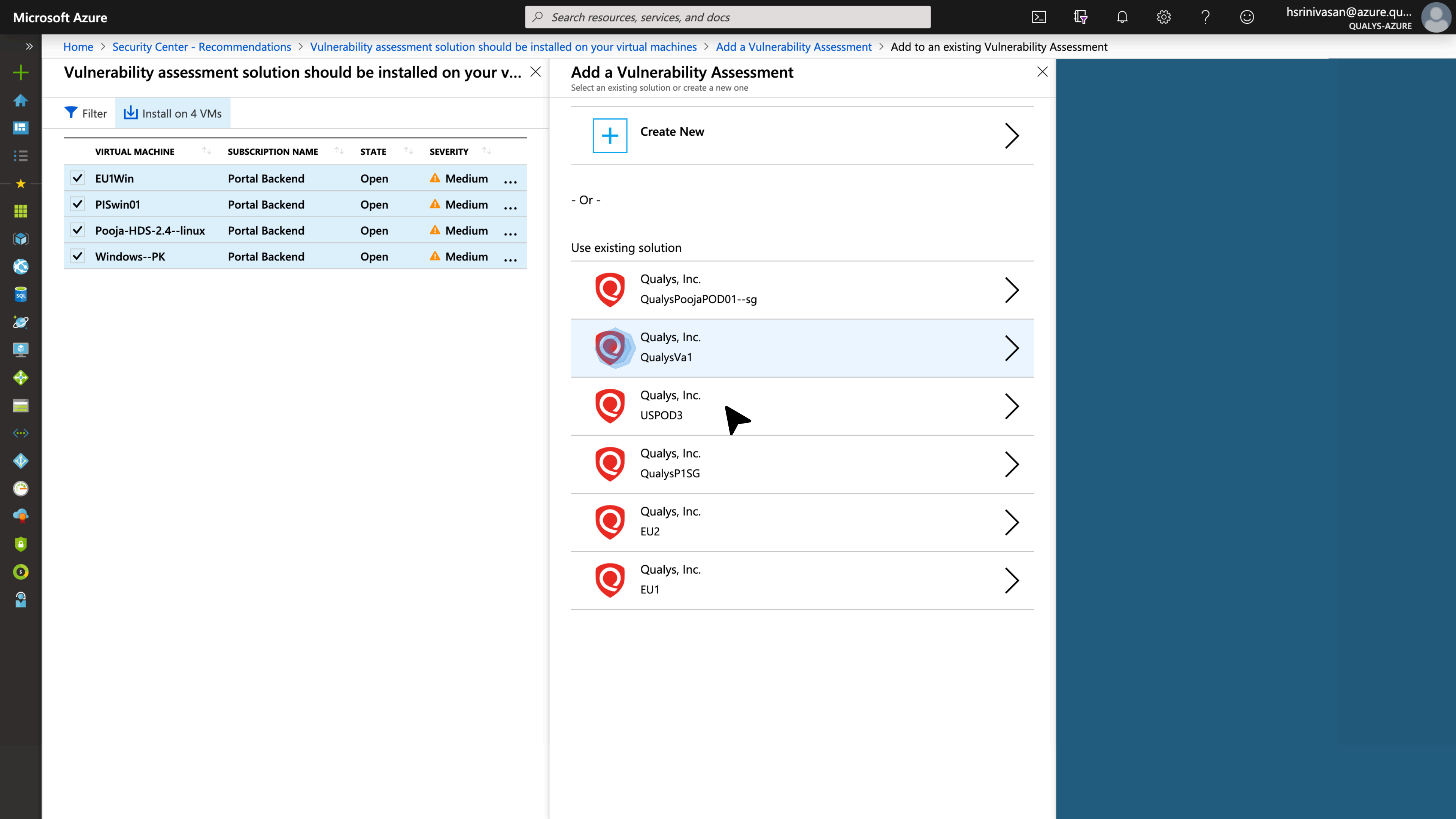
| | VIRTUAL MACHINE | SUBSCRIPTION NAME | STATE | SEVERITY | |
|---|---|---|---|---|---|
| ✓ | EU1Win | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | PISwin01 | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Pooja-HDS-2.4--linux | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Windows--PK | Portal Backend | Open | ⚠ Medium | ... |



Home > Security Center - Recommendations > Vulnerability assessment solution should be installed on your virtual machines

Vulnerability assessment solution should be installed on yo...

| | VIRTUAL MACHINE | SUBSCRIPTION NAME | STATE | SEVERITY | |
|---|---|---|---|---|---|
| ☑ | EU1Win | Portal Backend | Open | ⚠ Medium | ... |
| ☑ | PISwin01 | Portal Backend | Open | ⚠ Medium | ... |
| ☑ | Pooja-HDS-2.4--linux | Portal Backend | Open | ⚠ Medium | ... |
| ☑ | Windows--PK | Portal Backend | Open | ⚠ Medium | ... |



Home > Security Center - Recommendations > Vulnerability assessment solution should be installed on your virtual machines > Add a Vulnerability Assessment > Add to an existing Vulnerability Assessment

Vulnerability assessment solution should be installed on your v...

| | VIRTUAL MACHINE | SUBSCRIPTION NAME | STATE | SEVERITY | |
|---|---|---|---|---|---|
| ✓ | EU1Win | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | PISwin01 | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Pooja-HDS-2.4--linux | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Windows--PK | Portal Backend | Open | ⚠ Medium | ... |

Add a Vulnerability Assessment

Select an existing solution or create a new one

- Or -

Use existing solution

Qualys, Inc.
QualysPoojaPOD01--sg

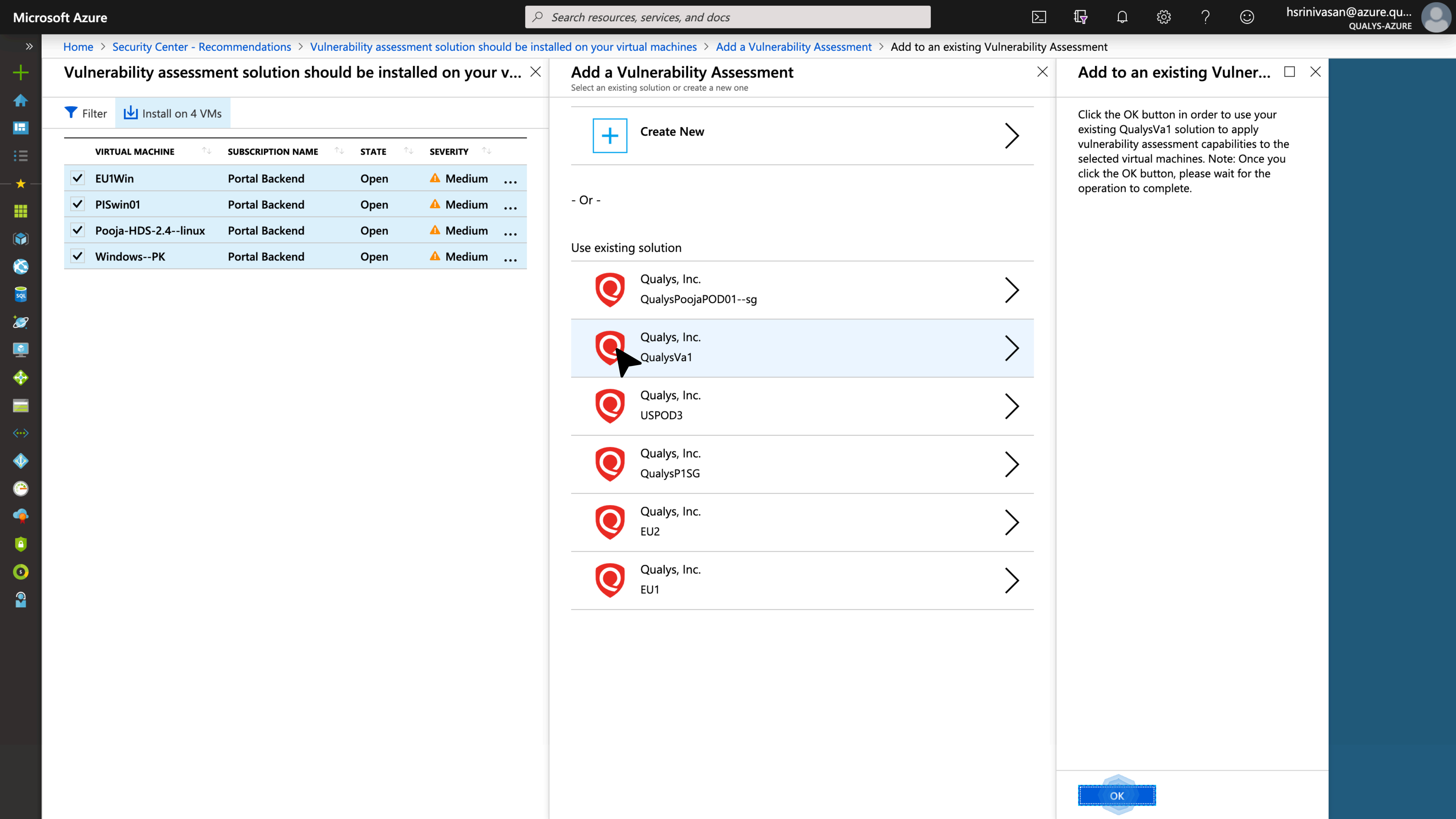
Qualys, Inc.
QualysVa1

Qualys, Inc.
USPOD3

Qualys, Inc.
QualysP1SG

Qualys, Inc.
EU2

Qualys, Inc.
EU1



Home > Security Center - Recommendations > Vulnerability assessment solution should be installed on your virtual machines > Add a Vulnerability Assessment > Add to an existing Vulnerability Assessment

## Vulnerability assessment solution should be installed on your v...

| | VIRTUAL MACHINE | SUBSCRIPTION NAME | STATE | SEVERITY | |
|---|---|---|---|---|---|
| ✓ | EU1Win | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | PISwin01 | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Pooja-HDS-2.4--linux | Portal Backend | Open | ⚠ Medium | ... |
| ✓ | Windows--PK | Portal Backend | Open | ⚠ Medium | ... |

## Add a Vulnerability Assessment

Select an existing solution or create a new one

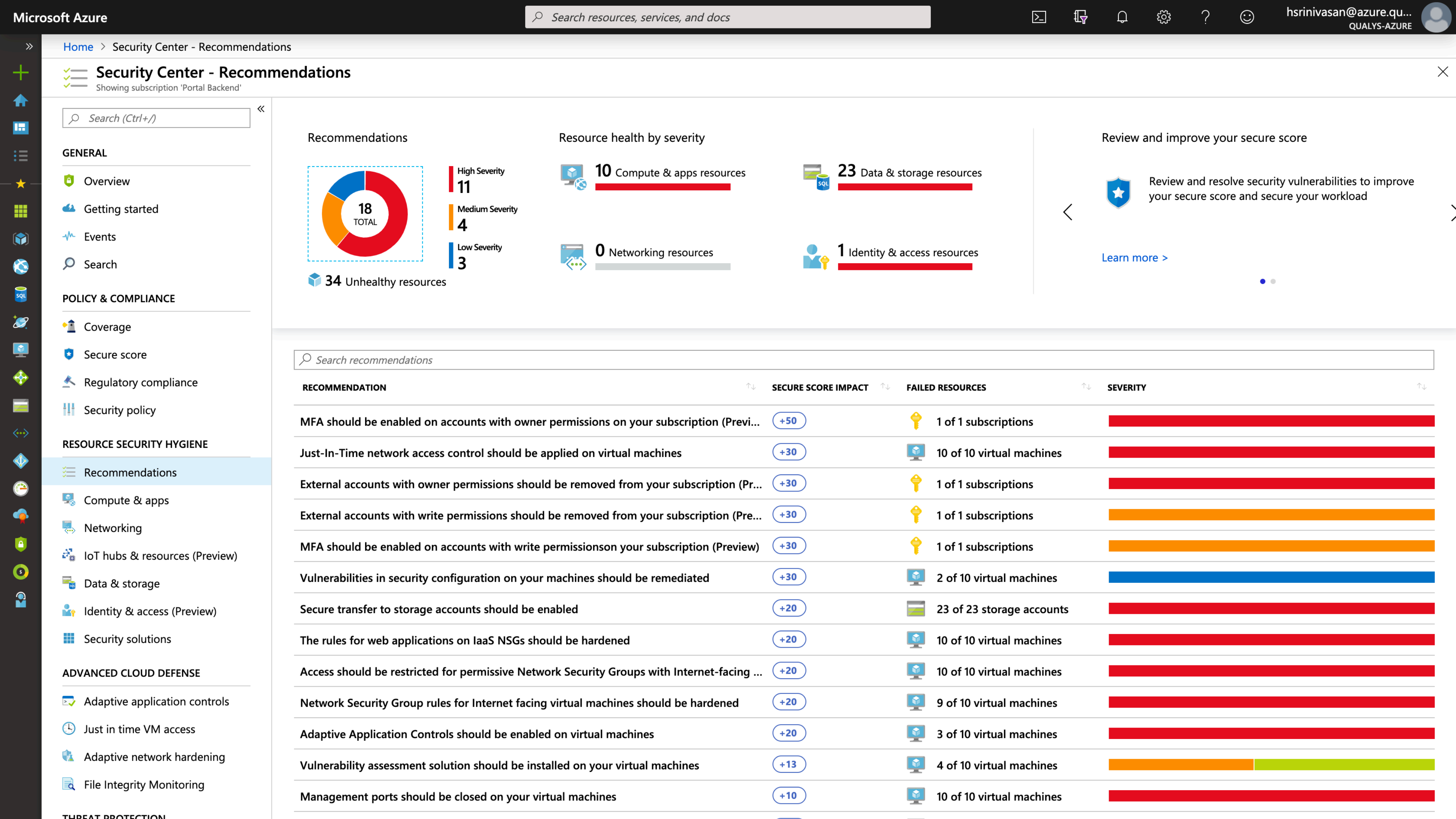
- Or -

Use existing solution

- Qualys, Inc.
  QualysPoojaPOD01--sg
- Qualys, Inc.
  QualysVa1
- Qualys, Inc.
  USPOD3
- Qualys, Inc.
  QualysP1SG
- Qualys, Inc.
  EU2
- Qualys, Inc.
  EU1

## Add to an existing Vulner...

Click the OK button in order to use your existing QualysVa1 solution to apply vulnerability assessment capabilities to the selected virtual machines. Note: Once you click the OK button, please wait for the operation to complete.



Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > Security Center - Recommendations

## Security Center - Recommendations

Showing subscription 'Portal Backend'

Recommendations

34 Unhealthy resources

Resource health by severity

10 Compute & apps resources

23 Data & storage resources

0 Networking resources

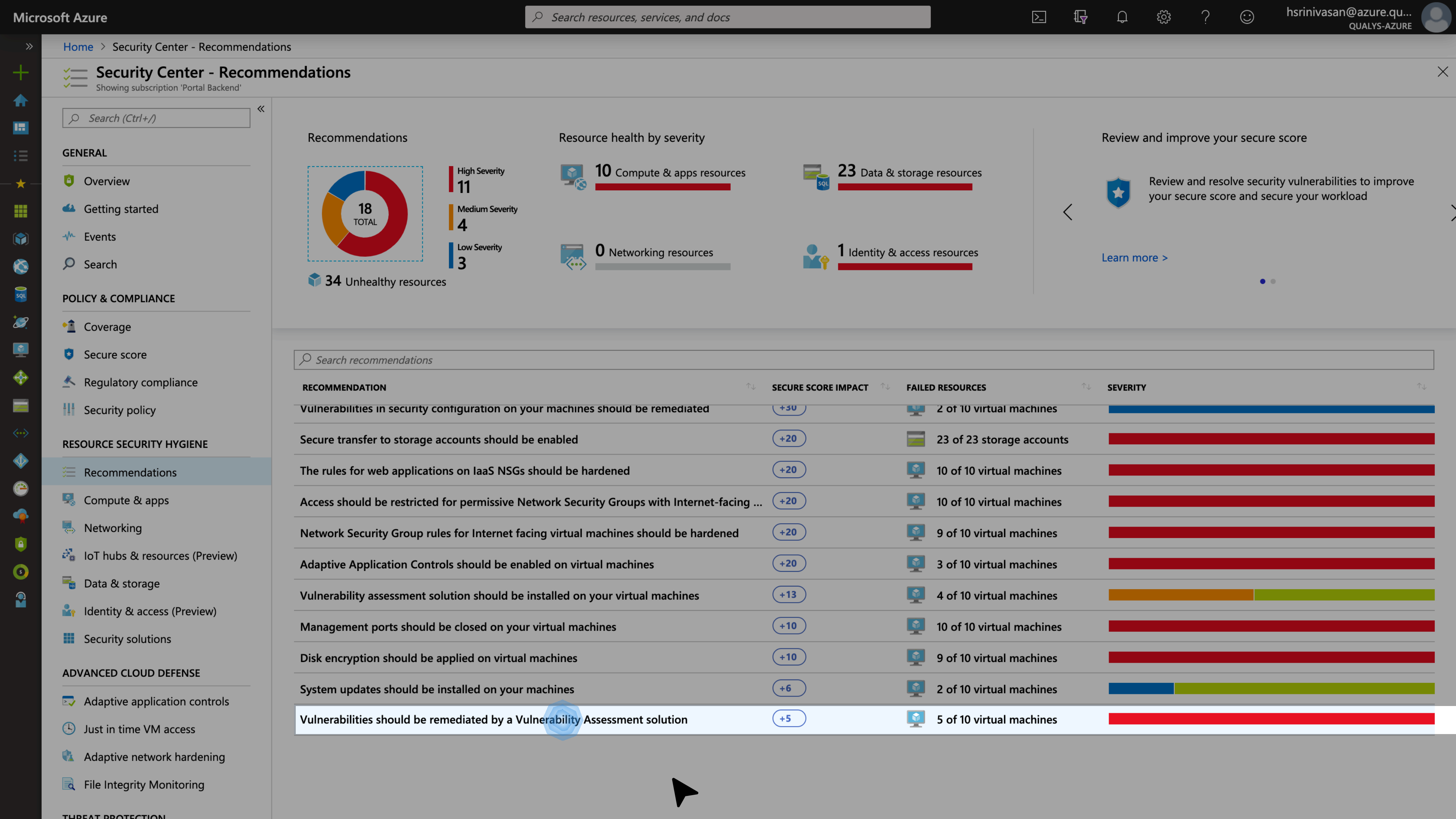
1 Identity & access resources

Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

| RECOMMENDATION | SECURE SCORE IMPACT | FAILED RESOURCES | SEVERITY |
|---|---|---|---|
| MFA should be enabled on accounts with owner permissions on your subscription (Previ... | +50 | 1 of 1 subscriptions | 🟥 |
| Just-In-Time network access control should be applied on virtual machines | +30 | 10 of 10 virtual machines | 🟥 |
| External accounts with owner permissions should be removed from your subscription (Pr... | +30 | 1 of 1 subscriptions | 🟥 |
| External accounts with write permissions should be removed from your subscription (Pre... | +30 | 1 of 1 subscriptions | 🟧 |
| MFA should be enabled on accounts with write permissionson your subscription (Preview) | +30 | 1 of 1 subscriptions | 🟧 |
| Vulnerabilities in security configuration on your machines should be remediated | +30 | 2 of 10 virtual machines | 🟦 |
| Secure transfer to storage accounts should be enabled | +20 | 23 of 23 storage accounts | 🟥 |
| The rules for web applications on IaaS NSGs should be hardened | +20 | 10 of 10 virtual machines | 🟥 |
| Access should be restricted for permissive Network Security Groups with Internet-facing ... | +20 | 10 of 10 virtual machines | 🟥 |
| Network Security Group rules for Internet facing virtual machines should be hardened | +20 | 9 of 10 virtual machines | 🟥 |
| Adaptive Application Controls should be enabled on virtual machines | +20 | 3 of 10 virtual machines | 🟥 |
| Vulnerability assessment solution should be installed on your virtual machines | +13 | 4 of 10 virtual machines | 🟧🟩 |
| Management ports should be closed on your virtual machines | +10 | 10 of 10 virtual machines | 🟥 |



Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > Security Center - Recommendations

# Security Center - Recommendations

Showing subscription 'Portal Backend'

Recommendations

18 TOTAL

High Severity 11
Medium Severity 4
Low Severity 3

34 Unhealthy resources

Resource health by severity

10 Compute & apps resources
23 Data & storage resources
0 Networking resources
1 Identity & access resources

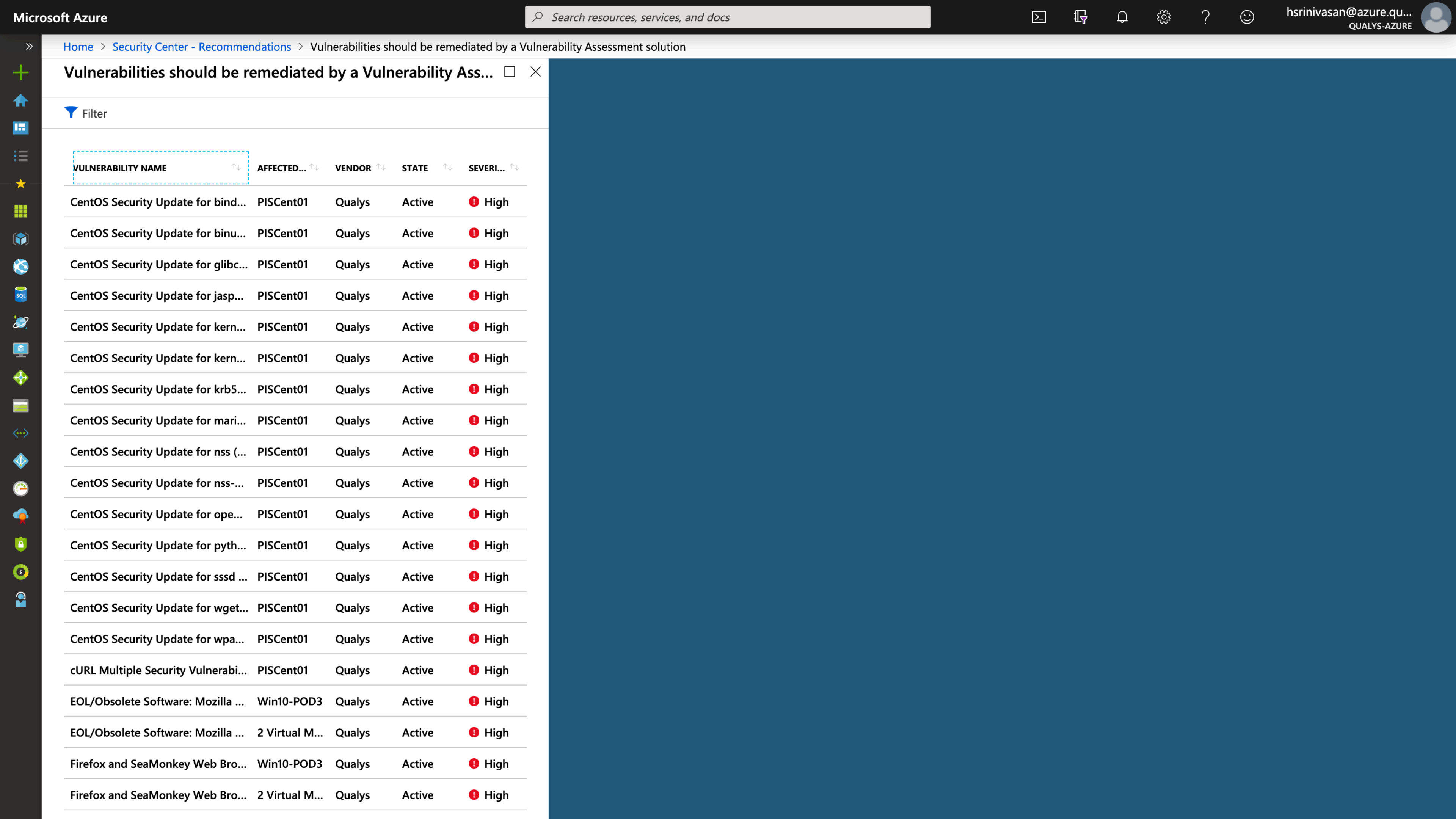
Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

Search recommendations

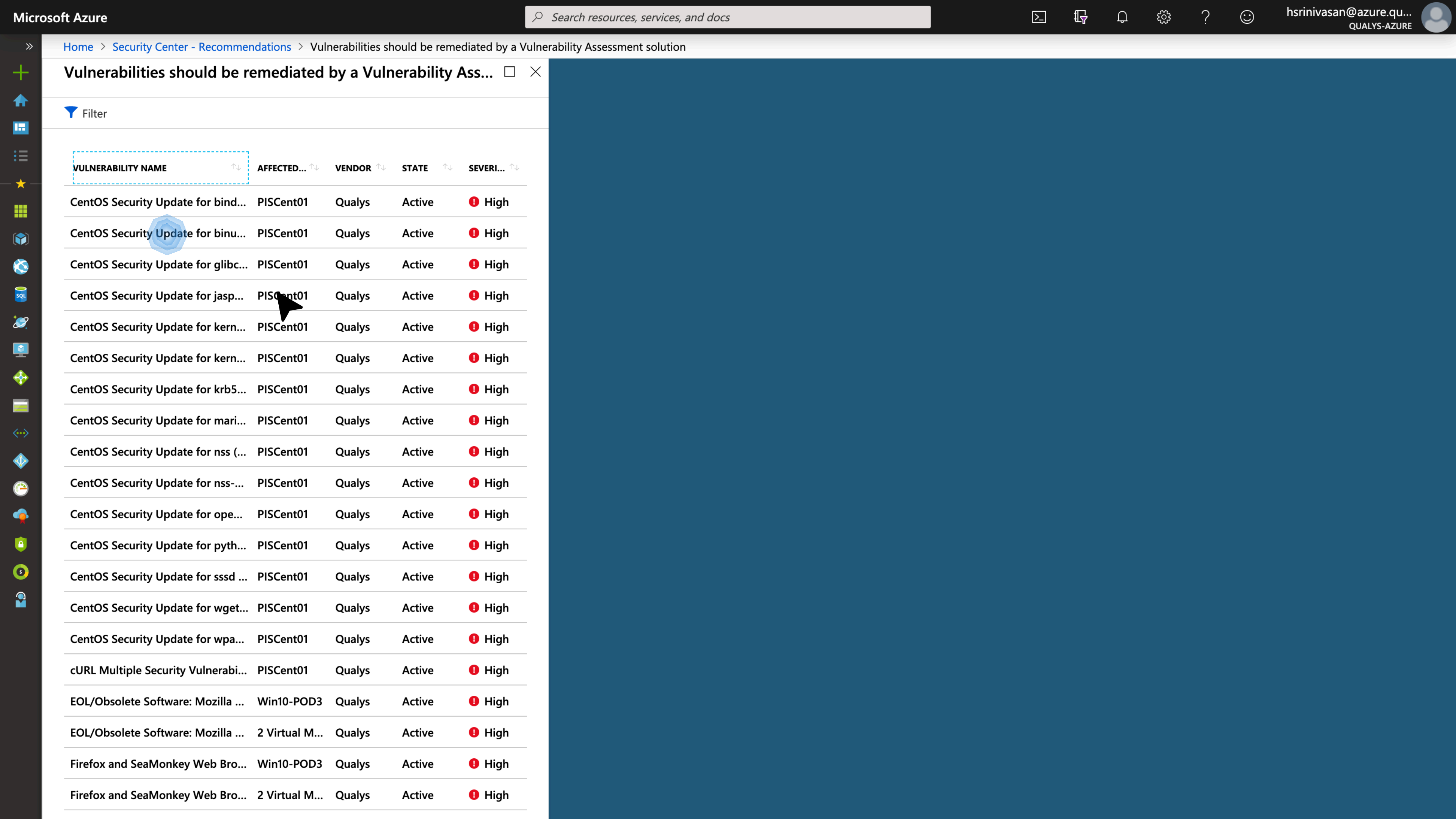
| RECOMMENDATION | SECURE SCORE IMPACT | FAILED RESOURCES | SEVERITY |
|---|---|---|---|
| Vulnerabilities in security configuration on your machines should be remediated | +30 | 2 of 10 virtual machines | 🟦 |
| Secure transfer to storage accounts should be enabled | +20 | 23 of 23 storage accounts | 🟥 |
| The rules for web applications on IaaS NSGs should be hardened | +20 | 10 of 10 virtual machines | 🟥 |
| Access should be restricted for permissive Network Security Groups with Internet-facing ... | +20 | 10 of 10 virtual machines | 🟥 |
| Network Security Group rules for Internet facing virtual machines should be hardened | +20 | 9 of 10 virtual machines | 🟥 |
| Adaptive Application Controls should be enabled on virtual machines | +20 | 3 of 10 virtual machines | 🟥 |
| Vulnerability assessment solution should be installed on your virtual machines | +13 | 4 of 10 virtual machines | 🟧🟩 |
| Management ports should be closed on your virtual machines | +10 | 10 of 10 virtual machines | 🟥 |
| Disk encryption should be applied on virtual machines | +10 | 9 of 10 virtual machines | 🟥 |
| System updates should be installed on your machines | +6 | 2 of 10 virtual machines | 🟦🟩 |
| Vulnerabilities should be remediated by a Vulnerability Assessment solution | +5 | 5 of 10 virtual machines | 🟥 |



Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > Security Center - Recommendations > Vulnerabilities should be remediated by a Vulnerability Assessment solution
Filter

Vulnerabilities should be remediated by a Vulnerability Ass...

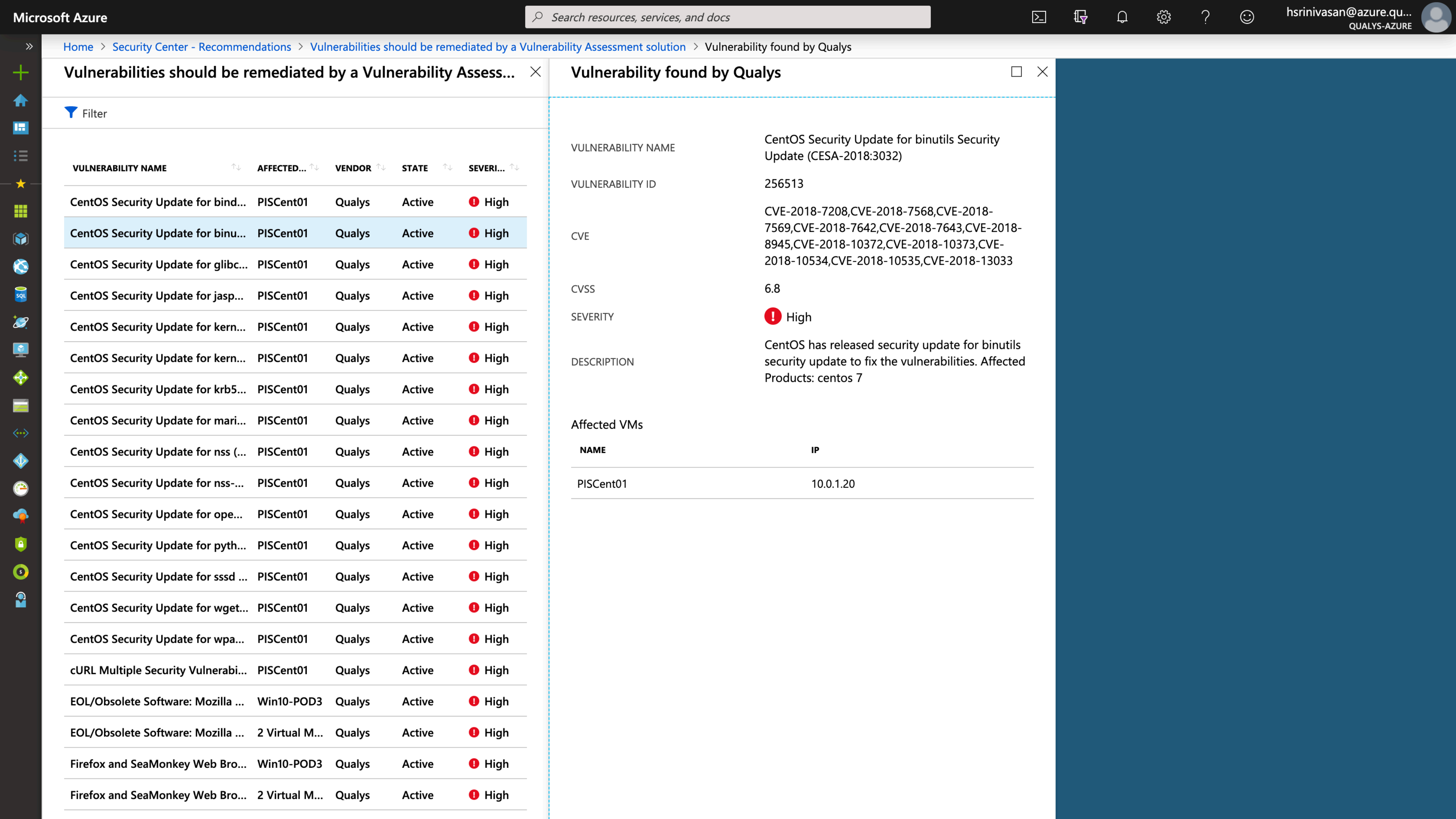
| VULNERABILITY NAME | AFFECTED... | VENDOR | STATE | SEVERI... |
|---|---|---|---|---|
| CentOS Security Update for bind... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for binu... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for glibc... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for jasp... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for krb5... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for mari... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for nss (... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for nss-... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for ope... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for pyth... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for sssd ... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for wget... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for wpa... | PISCent01 | Qualys | Active | ❗ High |
| cURL Multiple Security Vulnerabi... | PISCent01 | Qualys | Active | ❗ High |
| EOL/Obsolete Software: Mozilla ... | Win10-POD3 | Qualys | Active | ❗ High |
| EOL/Obsolete Software: Mozilla ... | 2 Virtual M... | Qualys | Active | ❗ High |
| Firefox and SeaMonkey Web Bro... | Win10-POD3 | Qualys | Active | ❗ High |
| Firefox and SeaMonkey Web Bro... | 2 Virtual M... | Qualys | Active | ❗ High |



Home > Security Center - Recommendations > Vulnerabilities should be remediated by a Vulnerability Assessment solution

Vulnerabilities should be remediated by a Vulnerability Ass...

| VULNERABILITY NAME | AFFECTED... | VENDOR | STATE | SEVERI... |
|---|---|---|---|---|
| CentOS Security Update for bind... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for binu... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for glibc... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for jasp... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for krb5... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for mari... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for nss (... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for nss-... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for ope... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for pyth... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for sssd ... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for wget... | PISCent01 | Qualys | Active | High |
| CentOS Security Update for wpa... | PISCent01 | Qualys | Active | High |
| cURL Multiple Security Vulnerabi... | PISCent01 | Qualys | Active | High |
| EOL/Obsolete Software: Mozilla ... | Win10-POD3 | Qualys | Active | High |
| EOL/Obsolete Software: Mozilla ... | 2 Virtual M... | Qualys | Active | High |
| Firefox and SeaMonkey Web Bro... | Win10-POD3 | Qualys | Active | High |
| Firefox and SeaMonkey Web Bro... | 2 Virtual M... | Qualys | Active | High |


Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > Security Center - Recommendations > Vulnerabilities should be remediated by a Vulnerability Assessment solution > Vulnerability found by Qualys
Filter

## Vulnerabilities should be remediated by a Vulnerability Assess...

| VULNERABILITY NAME | AFFECTED... | VENDOR | STATE | SEVERI... |
|---|---|---|---|---|
| CentOS Security Update for bind... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for binu... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for glibc... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for jasp... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for kern... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for krb5... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for mari... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for nss (... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for nss-... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for ope... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for pyth... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for sssd ... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for wget... | PISCent01 | Qualys | Active | ❗ High |
| CentOS Security Update for wpa... | PISCent01 | Qualys | Active | ❗ High |
| cURL Multiple Security Vulnerabi... | PISCent01 | Qualys | Active | ❗ High |
| EOL/Obsolete Software: Mozilla ... | Win10-POD3 | Qualys | Active | ❗ High |
| EOL/Obsolete Software: Mozilla ... | 2 Virtual M... | Qualys | Active | ❗ High |
| Firefox and SeaMonkey Web Bro... | Win10-POD3 | Qualys | Active | ❗ High |
| Firefox and SeaMonkey Web Bro... | 2 Virtual M... | Qualys | Active | ❗ High |

## Vulnerability found by Qualys

VULNERABILITY NAME: CentOS Security Update for binutils Security Update (CESA-2018:3032)

VULNERABILITY ID: 256513

CVE: CVE-2018-7208,CVE-2018-7568,CVE-2018-7569,CVE-2018-7642,CVE-2018-7643,CVE-2018-8945,CVE-2018-10372,CVE-2018-10373,CVE-2018-10534,CVE-2018-10535,CVE-2018-13033

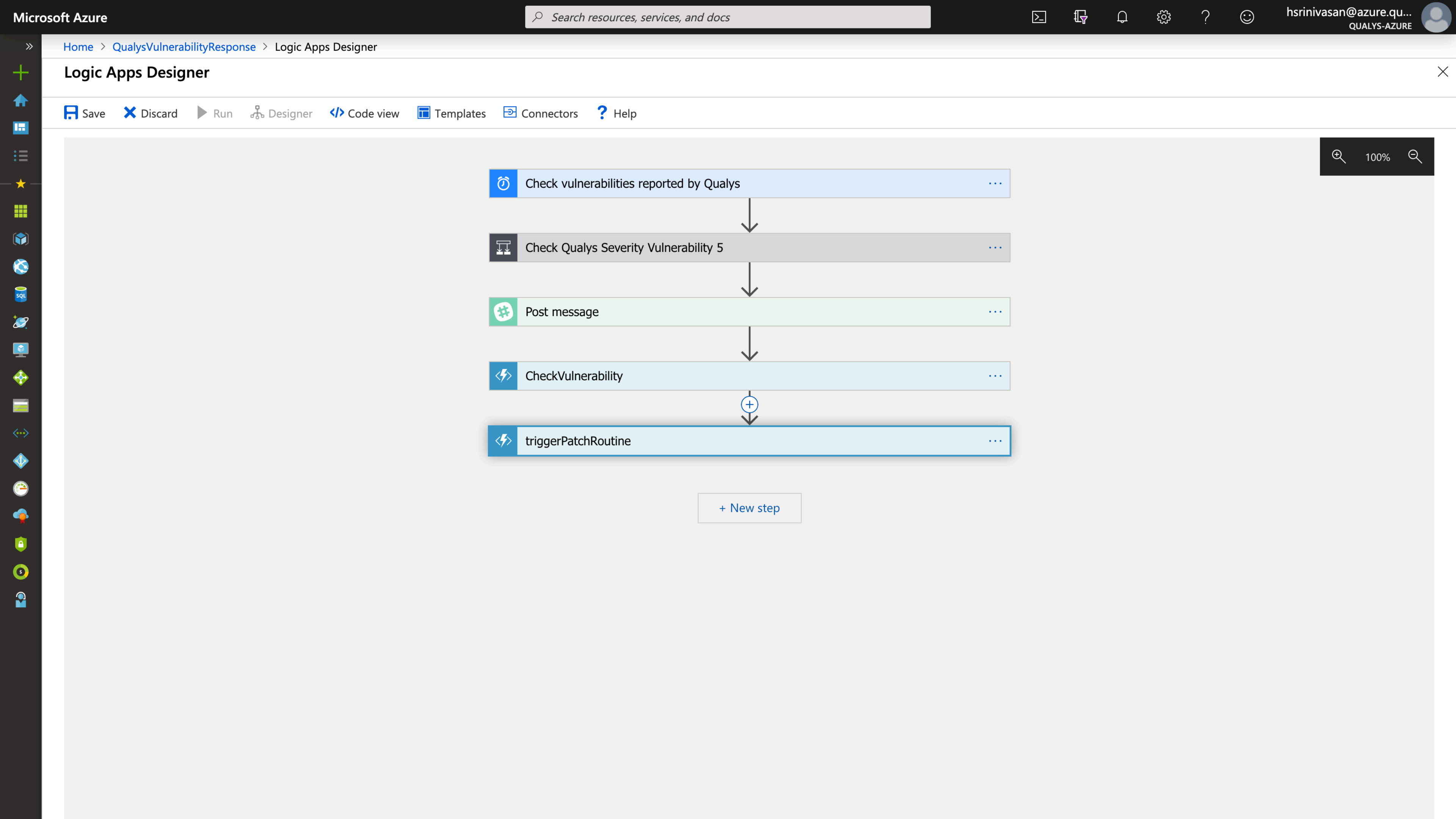
CVSS: 6.8

SEVERITY: ❗ High

DESCRIPTION: CentOS has released security update for binutils security update to fix the vulnerabilities. Affected Products: centos 7

Affected VMs

| NAME | IP |
|---|---|
| PISCent01 | 10.0.1.20 |



Microsoft Azure
Search resources, services, and docs
hsrinivasan@azure.qu...
QUALYS-AZURE
Home > QualysVulnerabilityResponse > Logic Apps Designer

Logic Apps Designer

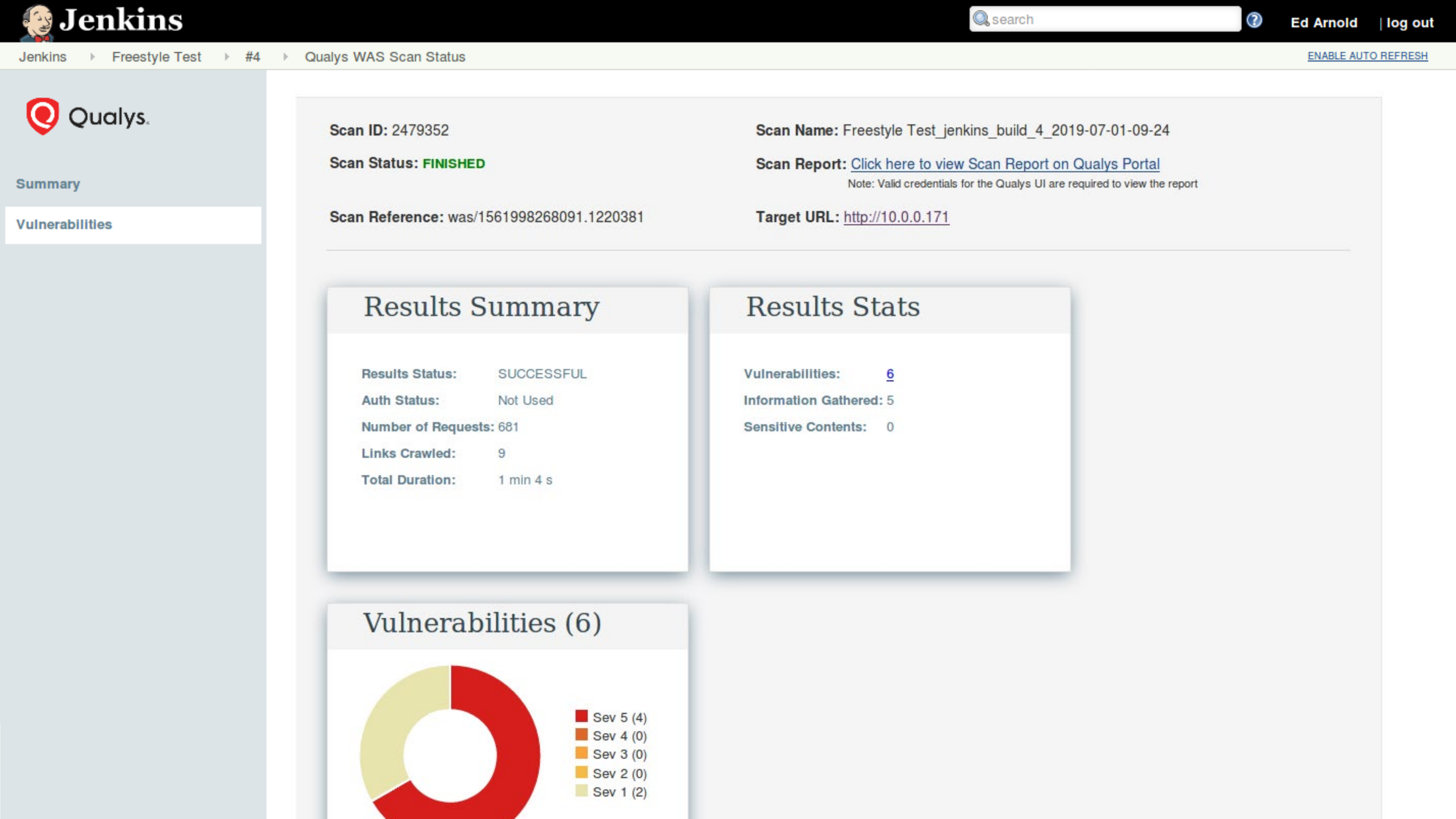
Check vulnerabilities reported by Qualys

Check Qualys Severity Vulnerability 5

Post message

CheckVulnerability

triggerPatchRoutine



**Scan ID:** 2479352

**Scan Name:** Freestyle Test_jenkins_build_4_2019-07-01-09-24

**Scan Status:** FINISHED

**Scan Report:** Click here to view Scan Report on Qualys Portal

Note: Valid credentials for the Qualys UI are required to view the report

**Scan Reference:** was/1561998268091.1220381

**Target URL:** http://10.0.0.171

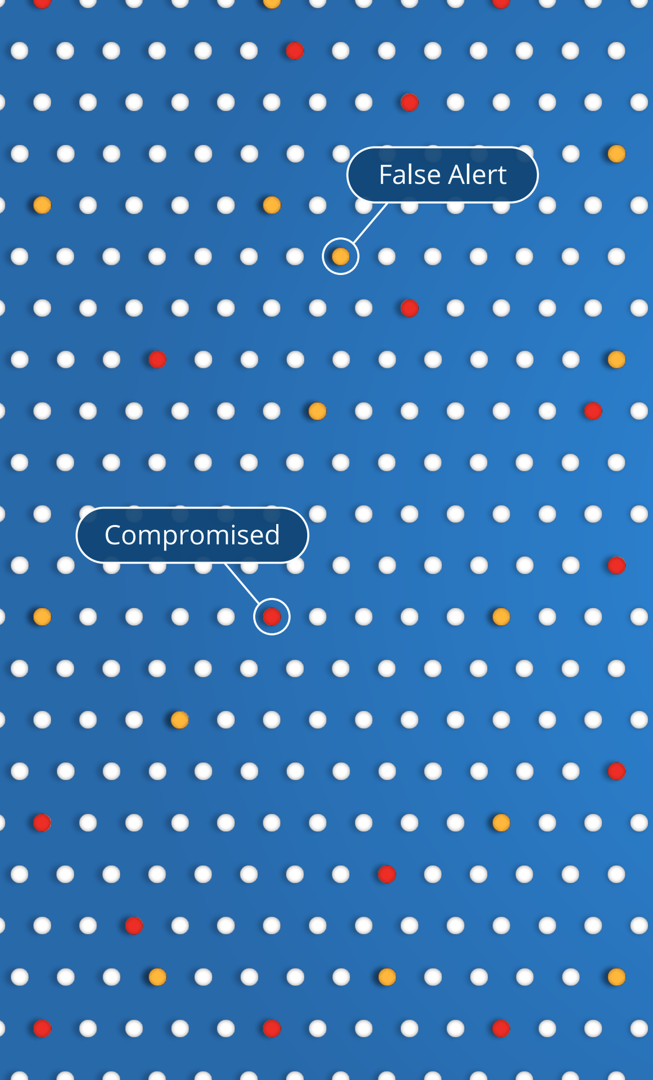
## Results Summary

| | |
|---|---|
| Results Status: | SUCCESSFUL |
| Auth Status: | Not Used |
| Number of Requests: | 681 |
| Links Crawled: | 9 |
| Total Duration: | 1 min 4 s |

## Results Stats

| | |
|---|---|
| Vulnerabilities: | 6 |
| Information Gathered: | 5 |
| Sensitive Contents: | 0 |

## Vulnerabilities (6)

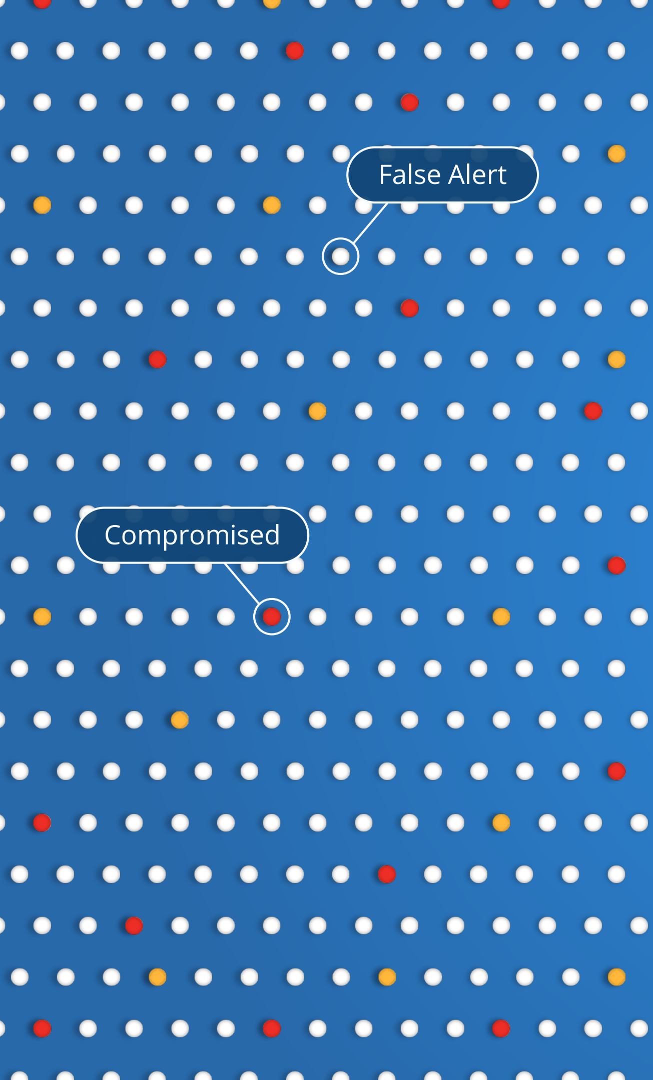


Drastically reducing

# FALSE ALERTS

The ability to respond in

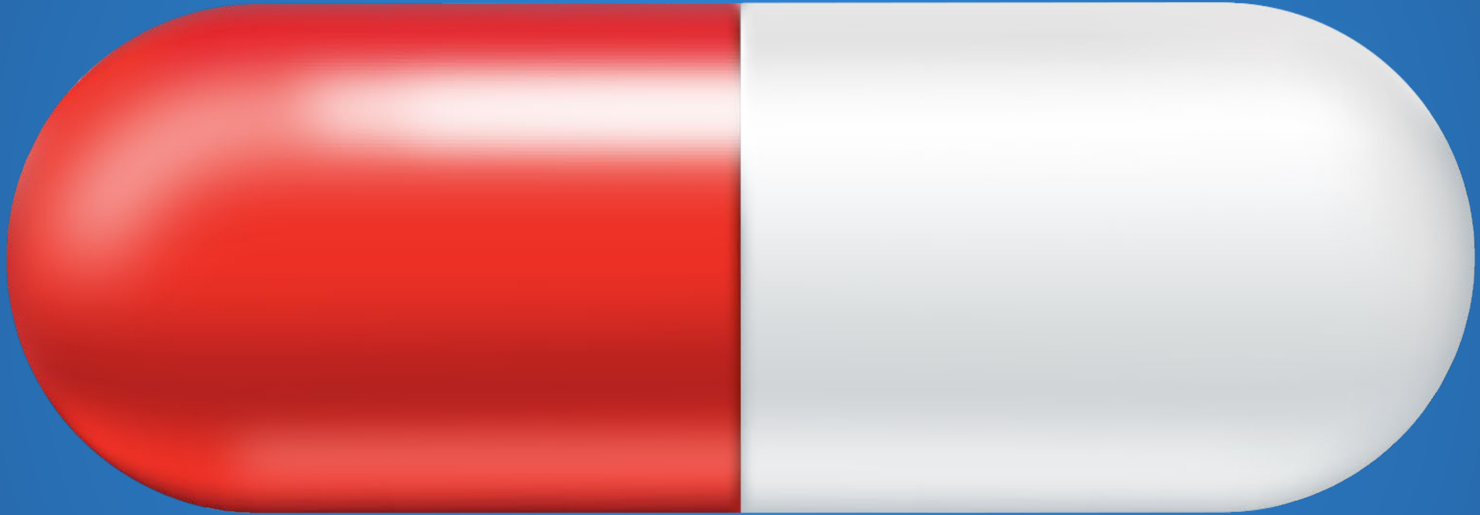
# REAL TIME



We cannot secure

# WHAT WE CAN'T SEE OR DON'T KNOW EXISTS.

Qualys Global IT
Asset Inventory



# Data Lake and Security Analytics

# Data Lake and Security Analytics - Goals

Provide a coherent and actionable view of your security posture by breaking down security data silos

Coalesce all data into a centralized highly scalable security data lake

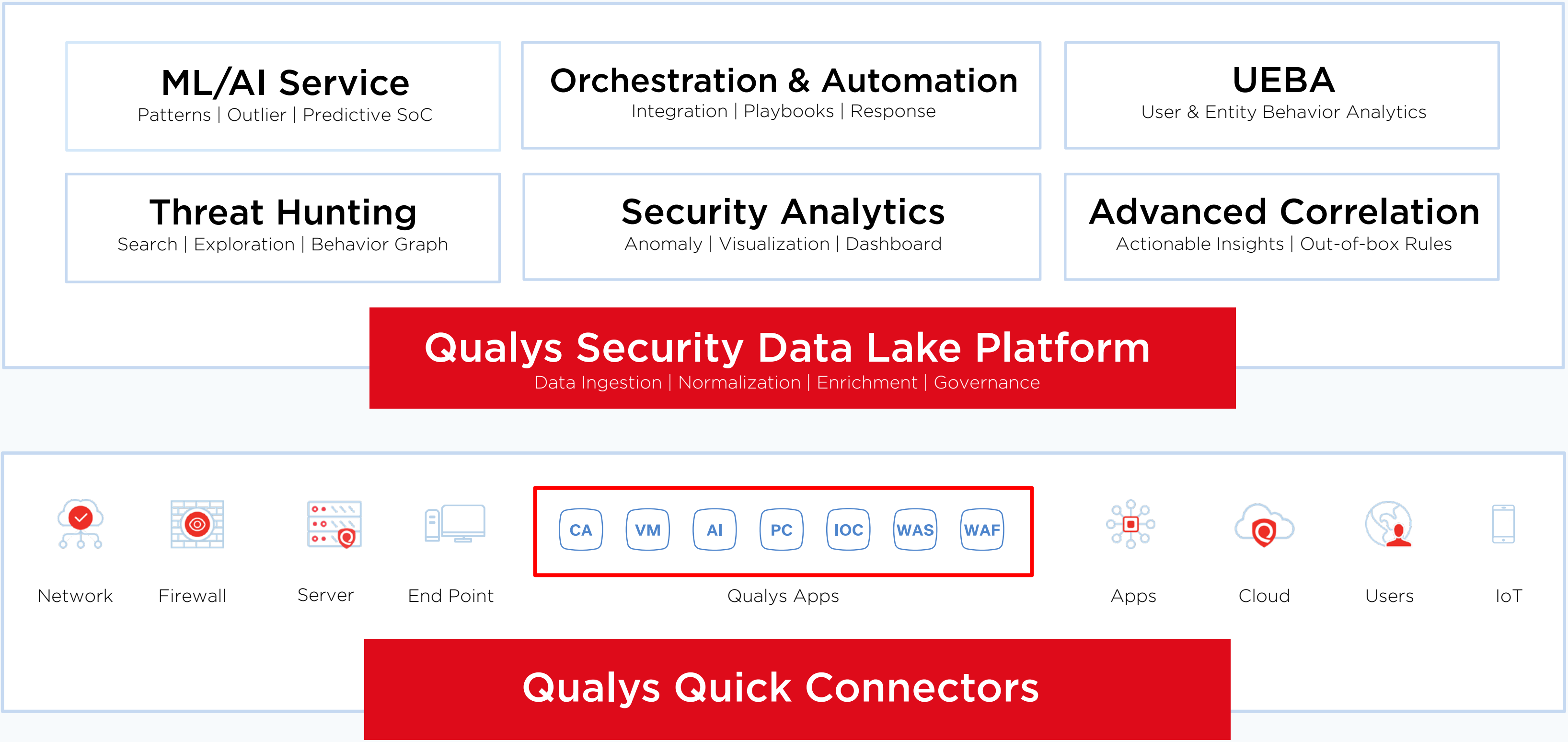
Leverage the strength of Qualys Cloud Platform, Cloud Agent and Apps to build a comprehensive security analytics platform

# Data Lake and Security Analytics - Objectives

Combine and enrich Qualys generated findings and telemetry with third-party signals (firewall logs, IDS, IPS, user data, threat feeds, etc.) to provide:

- Real-time streaming correlation and analytics solution
- Out-of-band batch analytics to generate unique insights
- Ad-hoc querying and threat hunting on enriched and security aware data sets
- Advanced analytics use cases using machine learning
- Risk based orchestration
- Response and endpoint protection

# Advanced Correlation and Analytics



**ML/AI Service**
Patterns | Outlier | Predictive SoC

**Orchestration & Automation**
Integration | Playbooks | Response

**UEBA**
User & Entity Behavior Analytics

**Threat Hunting**
Search | Exploration | Behavior Graph

**Security Analytics**
Anomaly | Visualization | Dashboard

**Advanced Correlation**
Actionable Insights | Out-of-box Rules

**Qualys Security Data Lake Platform**
Data Ingestion | Normalization | Enrichment | Governance

Network

Firewall

Server

End Point

CA VM AI PC IOC WAS WAF
Qualys Apps

Apps

Cloud

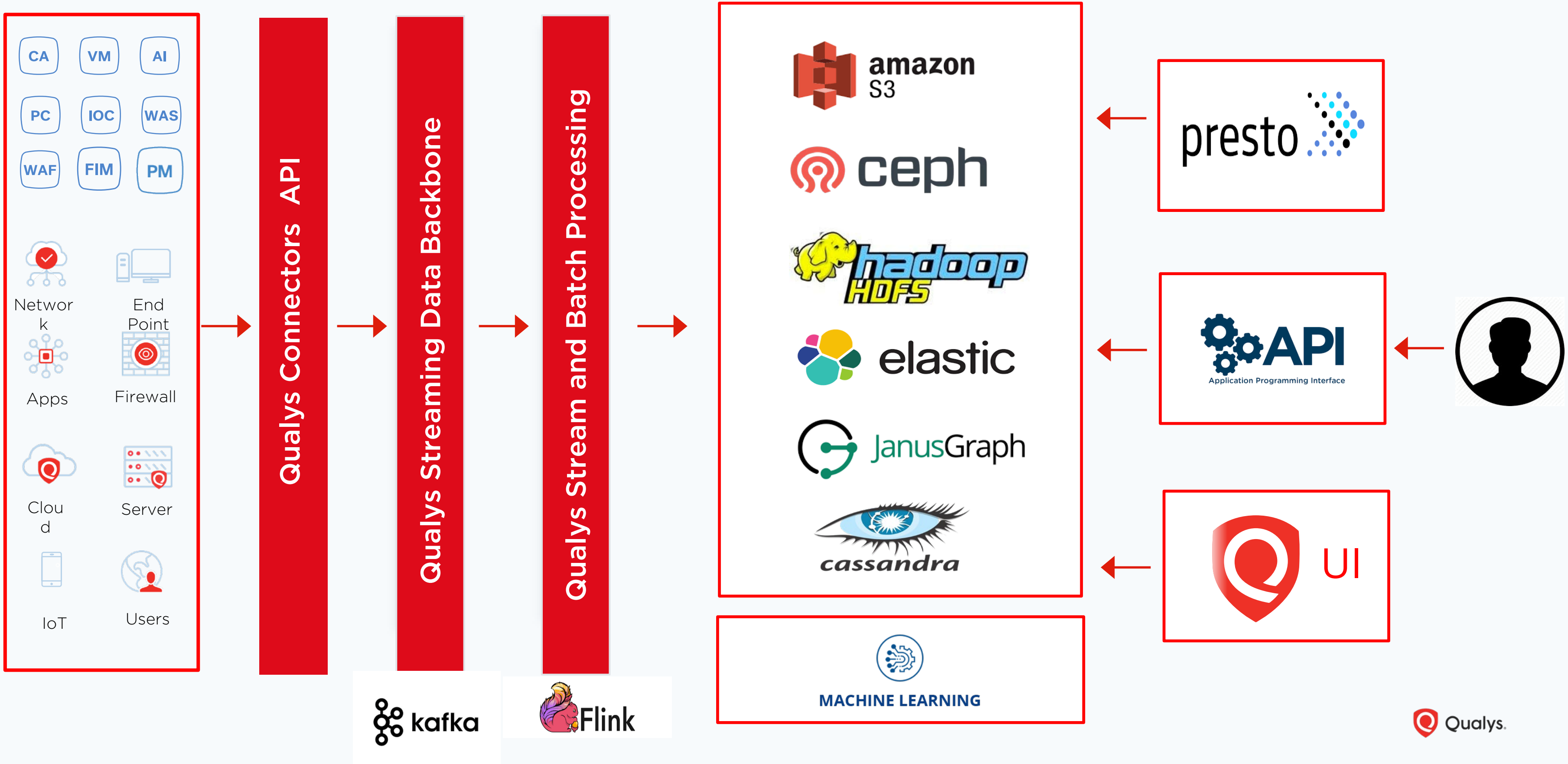
Users

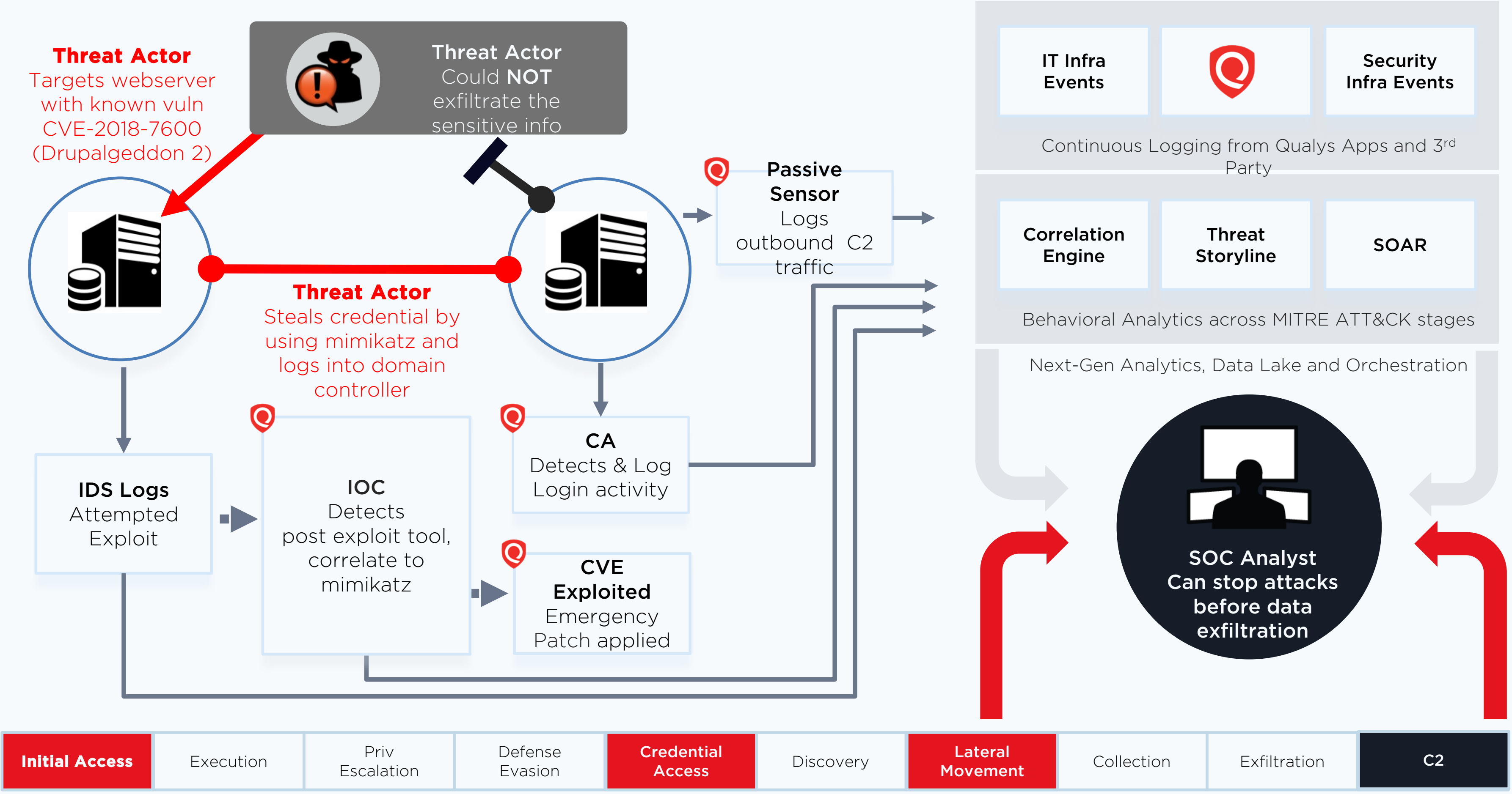
IoT

**Qualys Quick Connectors**

Qualys.

# Correlation and Data Platform Architecture





**Threat Actor**
Targets webserver with known vuln CVE-2018-7600 (Drupalgeddon 2)

**Threat Actor**
Could **NOT** exfiltrate the sensitive info

**Threat Actor**
Steals credential by using mimikatz and logs into domain controller

**IDS Logs**
Attempted Exploit

**IOC**
Detects post exploit tool, correlate to mimikatz

**CA**
Detects & Log Login activity

**CVE Exploited**
Emergency Patch applied

**Passive Sensor**
Logs outbound C2 traffic

**IT Infra Events**

**Security Infra Events**

Continuous Logging from Qualys Apps and 3rd Party

**Correlation Engine**

**Threat Storyline**

**SOAR**

Behavioral Analytics across MITRE ATT&CK stages

Next-Gen Analytics, Data Lake and Orchestration

**SOC Analyst Can stop attacks before data exfiltration**

| **Initial Access** | Execution | Priv Escalation | Defense Evasion | **Credential Access** | Discovery | **Lateral Movement** | Collection | Exfiltration | C2 |
|---|---|---|---|---|---|---|---|---|---|

**MITRE ATT&CK Stages**

Qualys.

# Accelerated Security Analytics Practice

- Robust security incident detection and management
- Centralized auditing for compliance
- Comprehensive orchestration
- Detection, protection and response
- Out-of-box and real-time threat hunting and forensic capabilities

… all built on top of a very robust and highly scalable techology platform.

# Summary

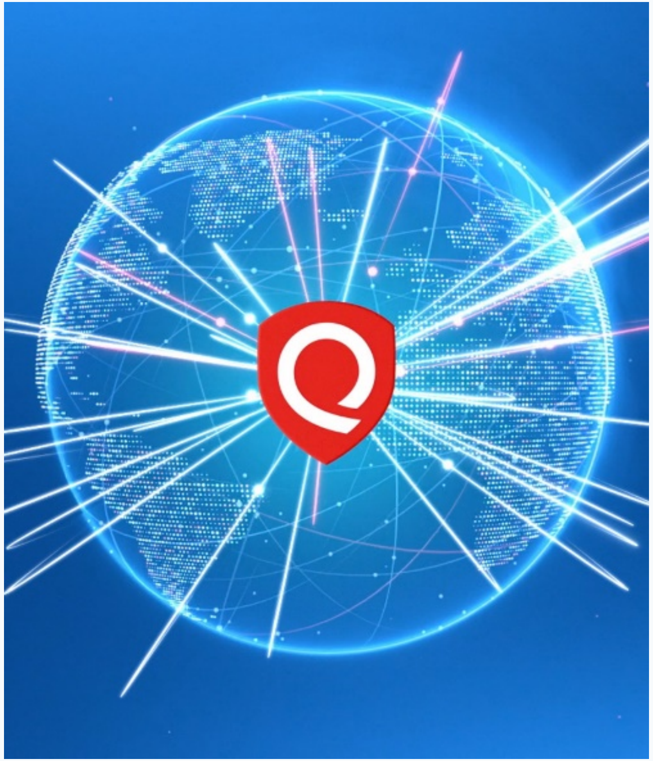
## Bringing a Unique Value Proposition to our Customers and Investors

Global IT Asset Discovery and Inventory as a free service for all

Enabling stack consolidation with 19 apps native on the Qualys Cloud Platform providing a single pane of glass view

Helping build security into their Digital Transformation

**A Company Highly Profitable and Built to Last**



# Thank You

pcourtot@qualys.com
sthakar@qualys.com