QSC 20

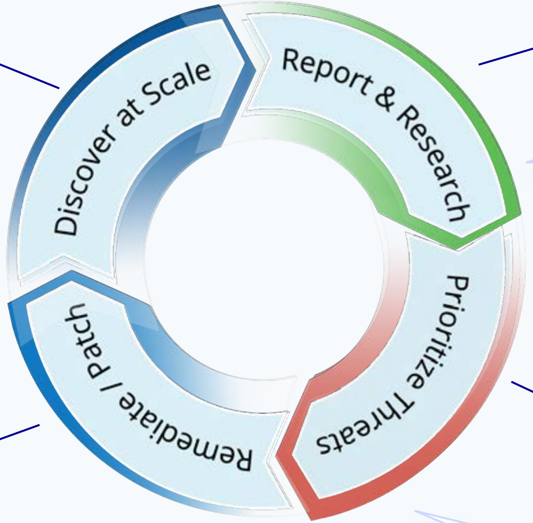
QUALYS SECURITY CONFERENCE 2020

Vulnerability Management Detection & Response (VMDR)

Chris Carlson

VP Product & Technology, Qualys, Inc.

Vulnerability Management Lifecycle



Asset Inventory

Do you know what all your assets are and where they are?

Vulnerability Management

Do you know the type and amount of open vulnerabilities?

Threat Risk and Prioritization

Can you prioritize remediation based on threat intelligence?

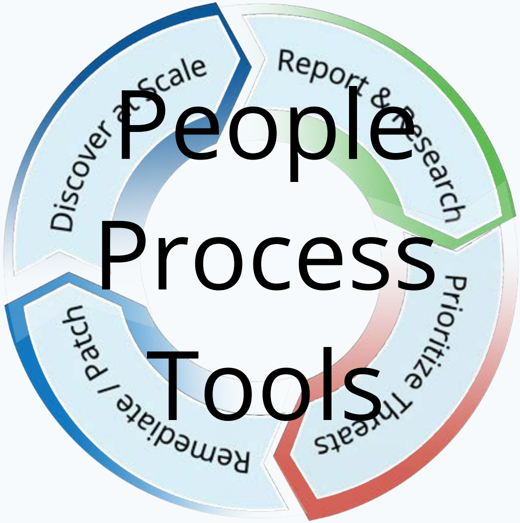
Patch Management

How can you deploy patches to close high-impact vulnerabilities?

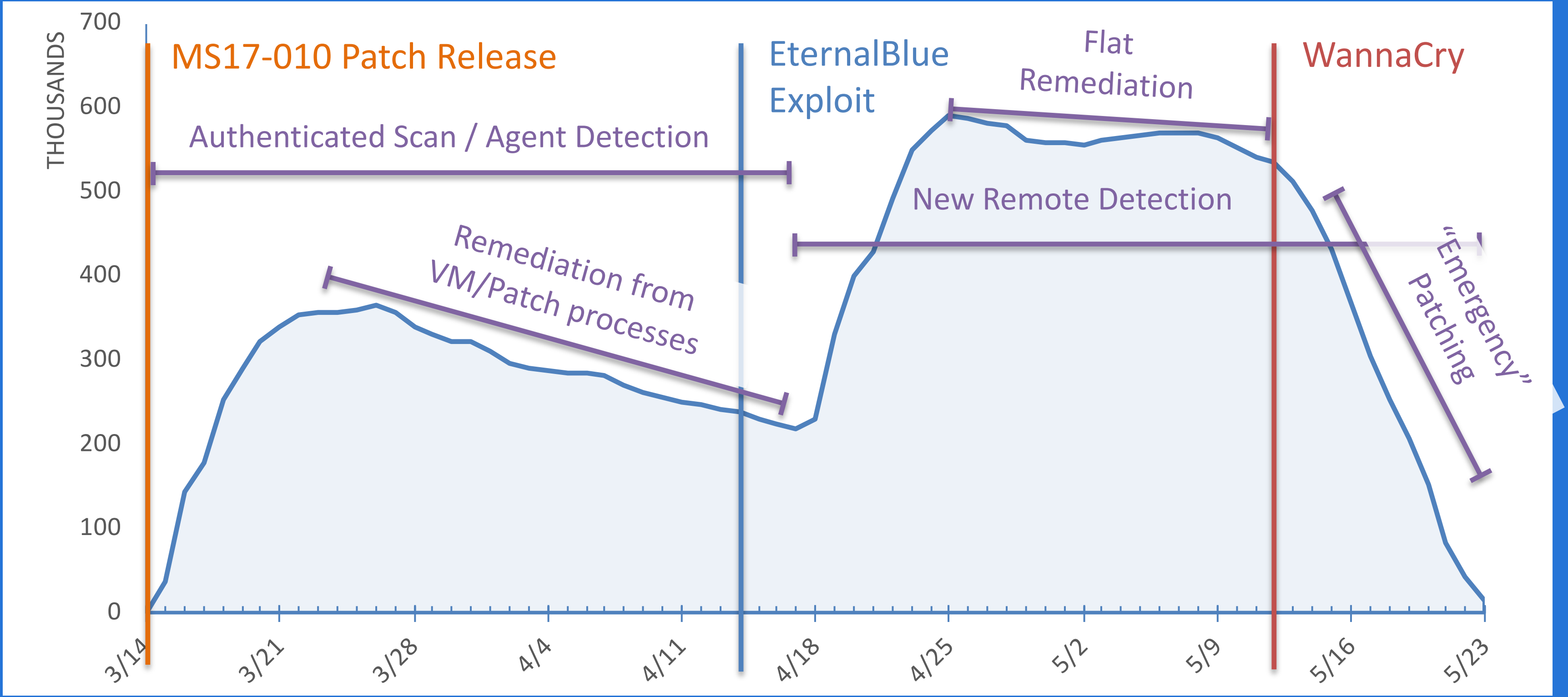
People

Process

Tools



WannaCry Timeline and Remediation



Qualys.

One solution to Discover, Assess, Prioritize and Patch critical vulnerabilities

Asset Discovery

Detect known and unknown assets

Workflow to add an unmanaged asset as a managed asset

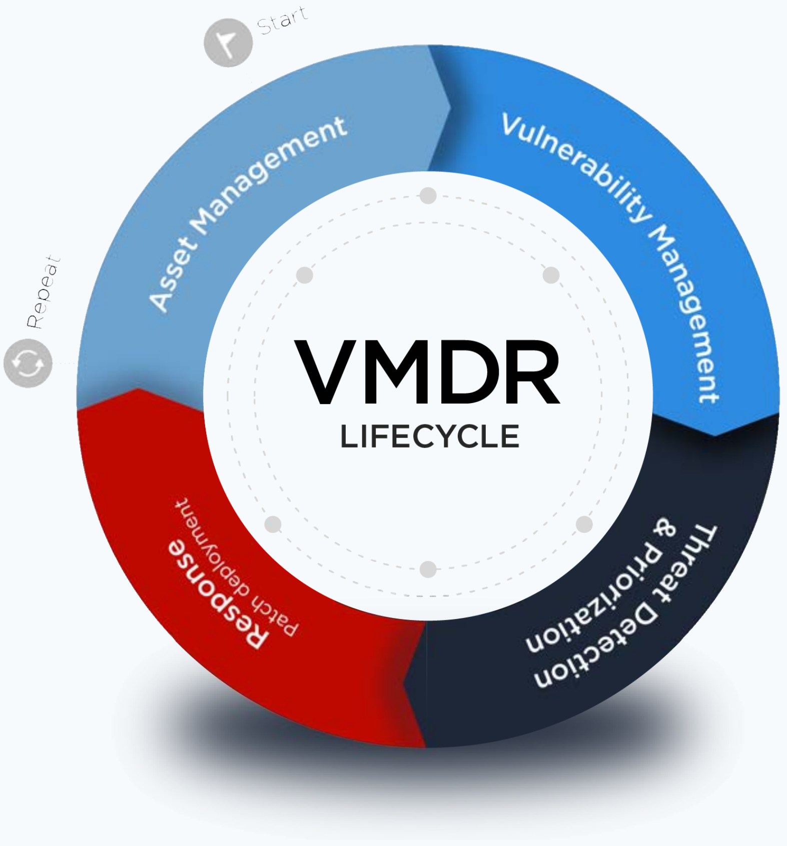
Asset Inventory

Hardware, operating system, and application inventory for all assets

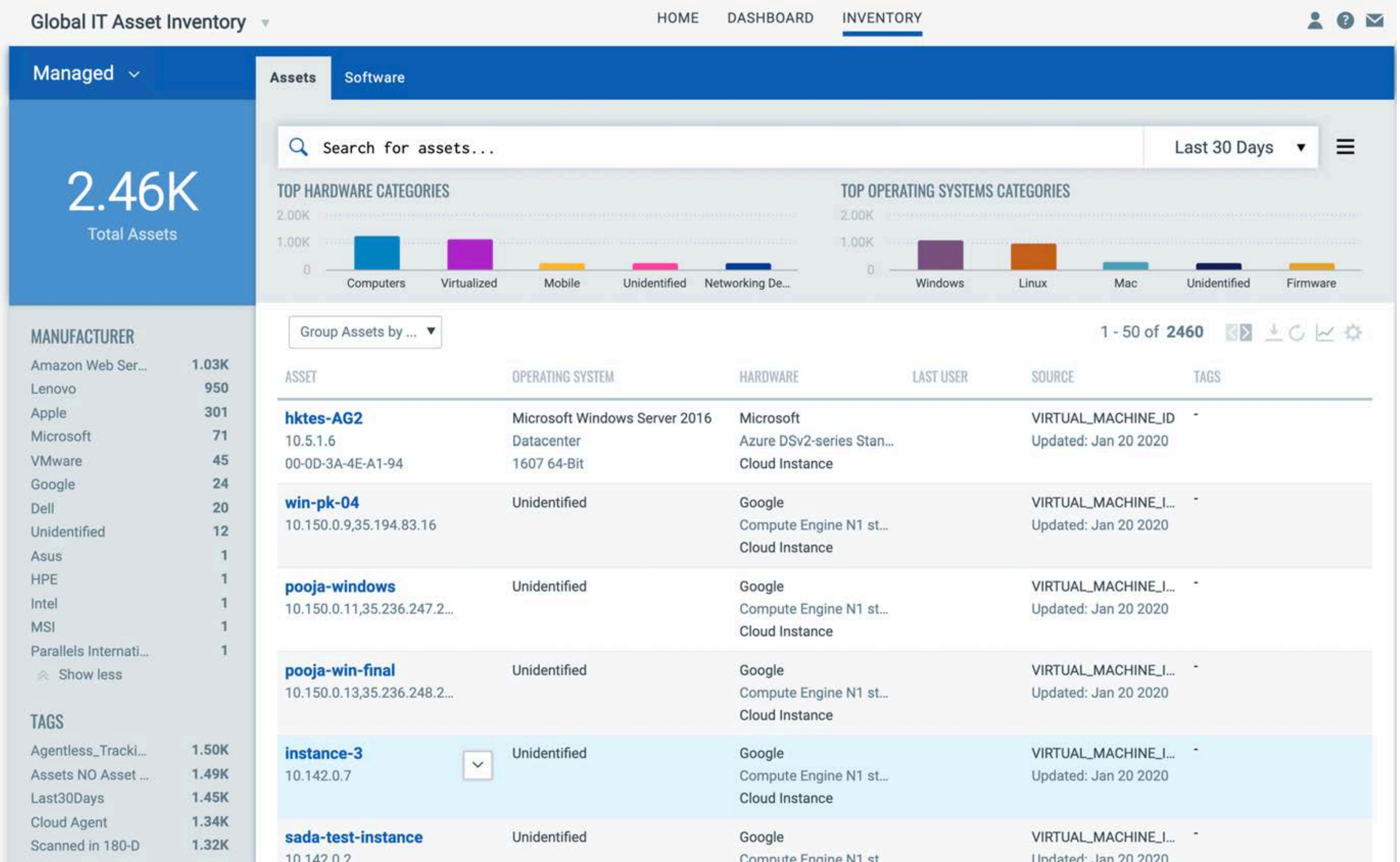
Asset Normalization and Categorization

Normalize Inventory data by common attributes

Categorize by vendor, version, type



Qualys.



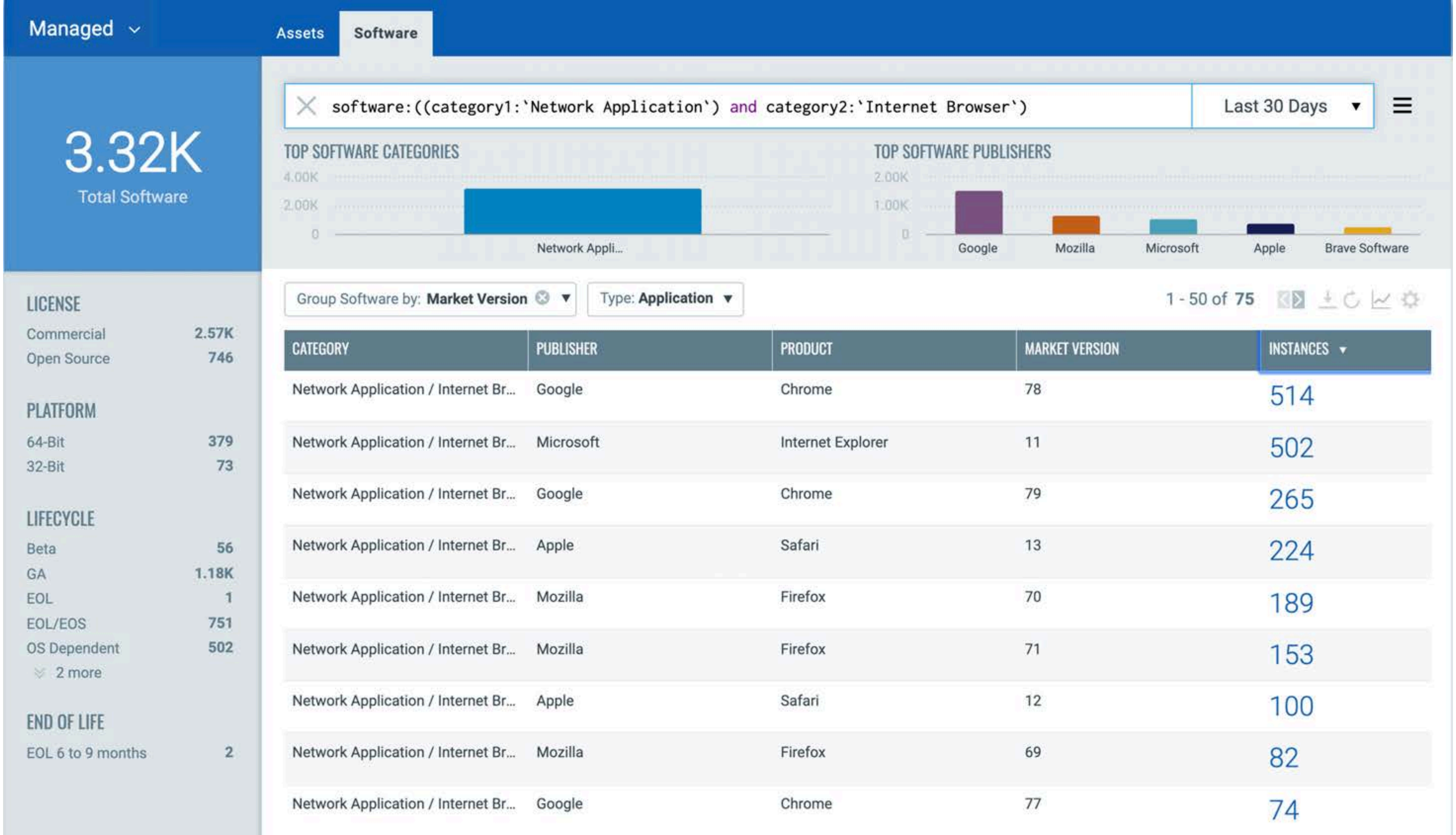
2.46K
Total Assets

MANUFACTURER	
Amazon Web Ser...	1.03K
Lenovo	950
Apple	301
Microsoft	71
VMware	45
Google	24
Dell	20
Unidentified	12
Asus	1
HPE	1
Intel	1
MSI	1
Parallels Internati...	1

TAGS	
Agentless_Tracki...	1.50K
Assets NO Asset ...	1.49K
Last30Days	1.45K
Cloud Agent	1.34K
Scanned in 180-D	1.32K

1 - 50 of 2460

ASSET	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCE	TAGS
hktes-AG2 10.5.1.6 00-0D-3A-4E-A1-94	Microsoft Windows Server 2016 Datacenter 1607 64-Bit	Microsoft Azure DSv2-series Stan... Cloud Instance		VIRTUAL_MACHINE_ID Updated: Jan 20 2020	-
win-pk-04 10.150.0.9,35.194.83.16	Unidentified	Google Compute Engine N1 st... Cloud Instance		VIRTUAL_MACHINE_I... Updated: Jan 20 2020	-
pooja-windows 10.150.0.11,35.236.247.2...	Unidentified	Google Compute Engine N1 st... Cloud Instance		VIRTUAL_MACHINE_I... Updated: Jan 20 2020	-
pooja-win-final 10.150.0.13,35.236.248.2...	Unidentified	Google Compute Engine N1 st... Cloud Instance		VIRTUAL_MACHINE_I... Updated: Jan 20 2020	-
instance-3 10.142.0.7	Unidentified	Google Compute Engine N1 st... Cloud Instance		VIRTUAL_MACHINE_I... Updated: Jan 20 2020	-
sada-test-instance 10.142.0.2	Unidentified	Google Compute Engine N1 st		VIRTUAL_MACHINE_I... Updated: Jan 20 2020	-



```
software:((category1:`Network Application`) and category2:`Internet Browser`)
```

Last 30 Days

3.32K
Total Software

TOP SOFTWARE CATEGORIES

TOP SOFTWARE PUBLISHERS

LICENSE

Commercial	2.57K
Open Source	746

PLATFORM

64-Bit	379
32-Bit	73

LIFECYCLE

Beta	56
GA	1.18K
EOL	1
EOL/EOS	751
OS Dependent	502

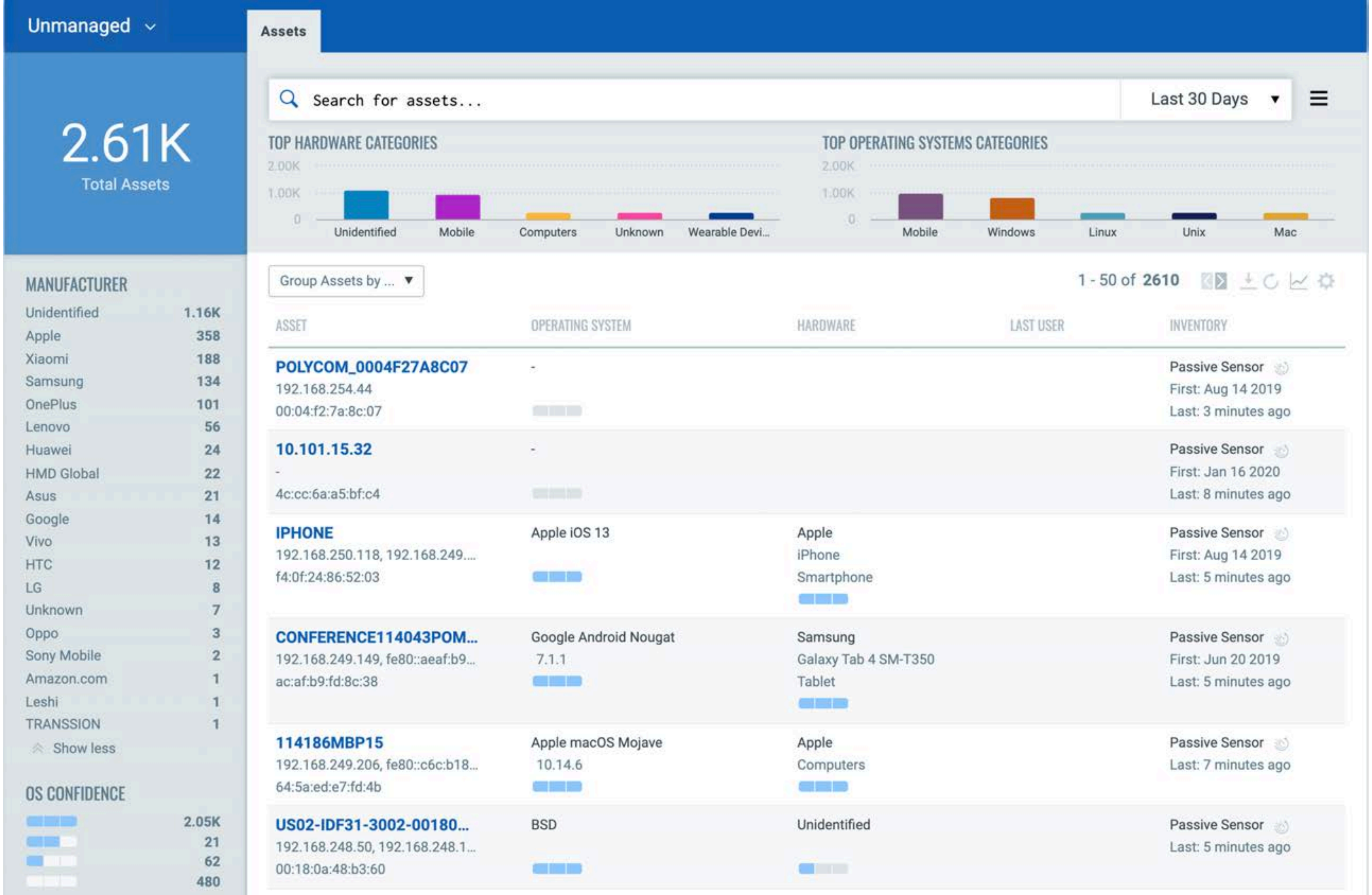
2 more

END OF LIFE

EOL 6 to 9 months	2

Group Software by: **Market Version**   Type: **Application**   1 - 50 of **75**

CATEGORY	PUBLISHER	PRODUCT	MARKET VERSION	INSTANCES ▼
Network Application / Internet Br...	Google	Chrome	78	514
Network Application / Internet Br...	Microsoft	Internet Explorer	11	502
Network Application / Internet Br...	Google	Chrome	79	265
Network Application / Internet Br...	Apple	Safari	13	224
Network Application / Internet Br...	Mozilla	Firefox	70	189
Network Application / Internet Br...	Mozilla	Firefox	71	153
Network Application / Internet Br...	Apple	Safari	12	100
Network Application / Internet Br...	Mozilla	Firefox	69	82
Network Application / Internet Br...	Google	Chrome	77	74



2.61K
Total Assets

TOP HARDWARE CATEGORIES

TOP OPERATING SYSTEMS CATEGORIES

MANUFACTURER

Unidentified	1.16K
Apple	358
Xiaomi	188
Samsung	134
OnePlus	101
Lenovo	56
Huawei	24
HMD Global	22
Asus	21
Google	14
Vivo	13
HTC	12
LG	8
Unknown	7
Oppo	3
Sony Mobile	2
Amazon.com	1
Leshi	1
TRANSSION	1

OS CONFIDENCE

■■■	2.05K
■■□	21
■□□	62
□□□	480

1 - 50 of 2610

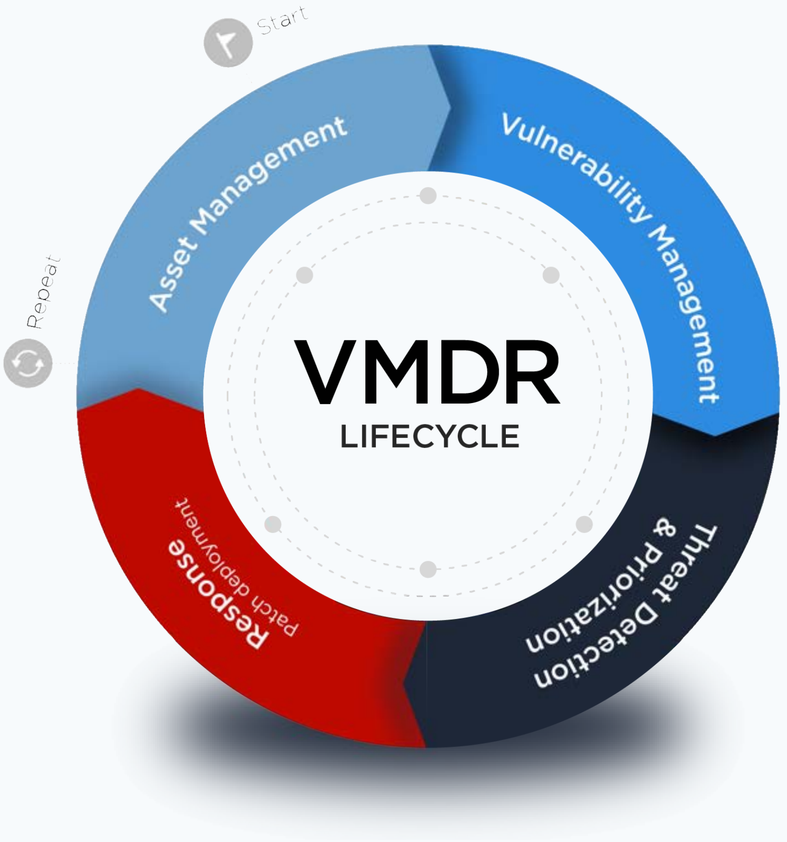
ASSET	OPERATING SYSTEM	HARDWARE	LAST USER	INVENTORY
POLYCOM_0004F27A8C07 192.168.254.44 00:04:f2:7a:8c:07	- □□□			Passive Sensor First: Aug 14 2019 Last: 3 minutes ago
10.101.15.32 - 4c:cc:6a:a5:bf:c4	- □□□			Passive Sensor First: Jan 16 2020 Last: 8 minutes ago
IPHONE 192.168.250.118, 192.168.249.... f4:0f:24:86:52:03	Apple iOS 13 ■■■	Apple iPhone Smartphone ■■■		Passive Sensor First: Aug 14 2019 Last: 5 minutes ago
CONFERENCE114043POM... 192.168.249.149, fe80::aeaf:b9... ac:af:b9:fd:8c:38	Google Android Nougat 7.1.1 ■■■	Samsung Galaxy Tab 4 SM-T350 Tablet ■■■		Passive Sensor First: Jun 20 2019 Last: 5 minutes ago
114186MBP15 192.168.249.206, fe80::c6c:b18... 64:5a:ed:e7:fd:4b	Apple macOS Mojave 10.14.6 ■■■	Apple Computers ■■■		Passive Sensor Last: 7 minutes ago
US02-IDF31-3002-00180... 192.168.248.50, 192.168.248.1... 00:18:0a:48:b3:60	BSD ■■■	Unidentified ■□□		Passive Sensor Last: 5 minutes ago

Vulnerability Management

- Detect vulnerabilities by QID
- CVE-to-QID mapping
- CVSSv2 and CVSSv3 base scores

Security Configuration Assessment

- CIS Benchmarks
- Security-related misconfigurations



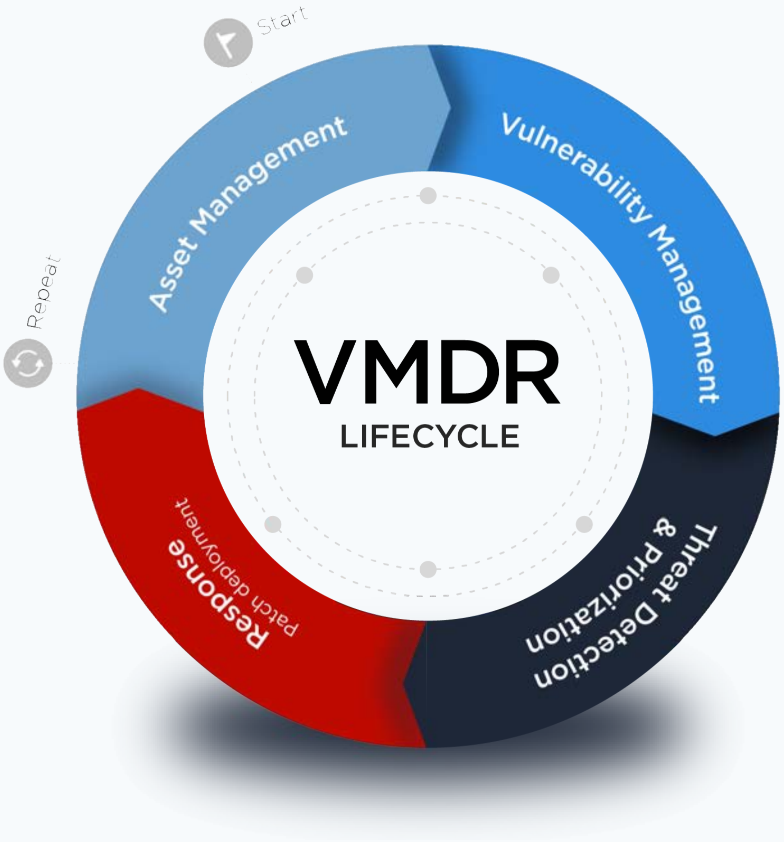
Qualys.

Prioritization

- Using real-time threat context
- Real-world exploits
- Proof of Concepts
- Exploit categorization
- Exploit severity

Machine Learning

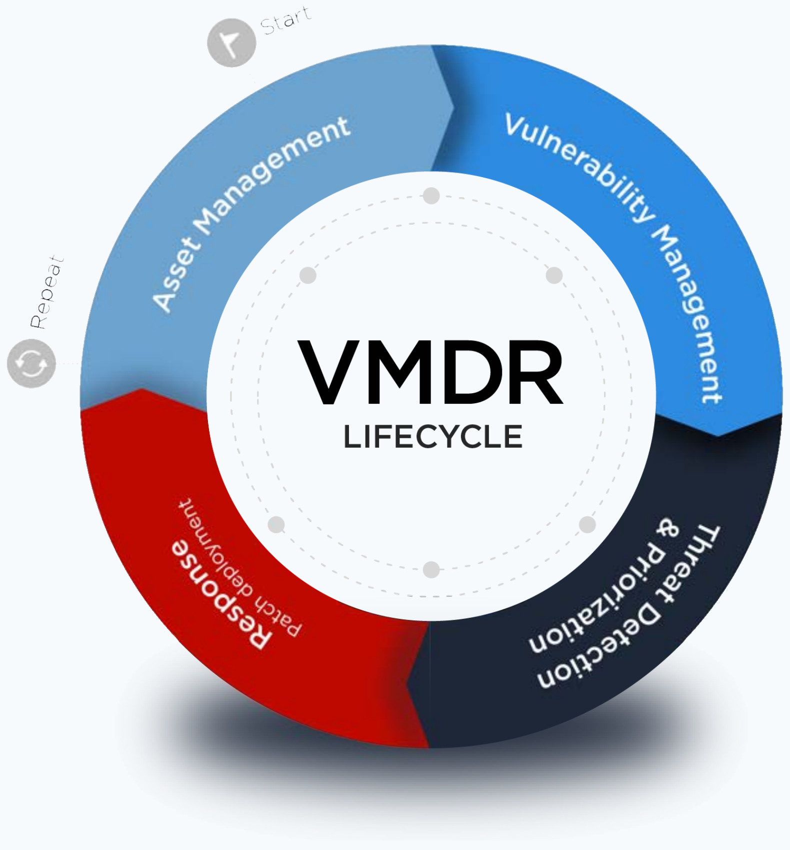
Contextual Awareness



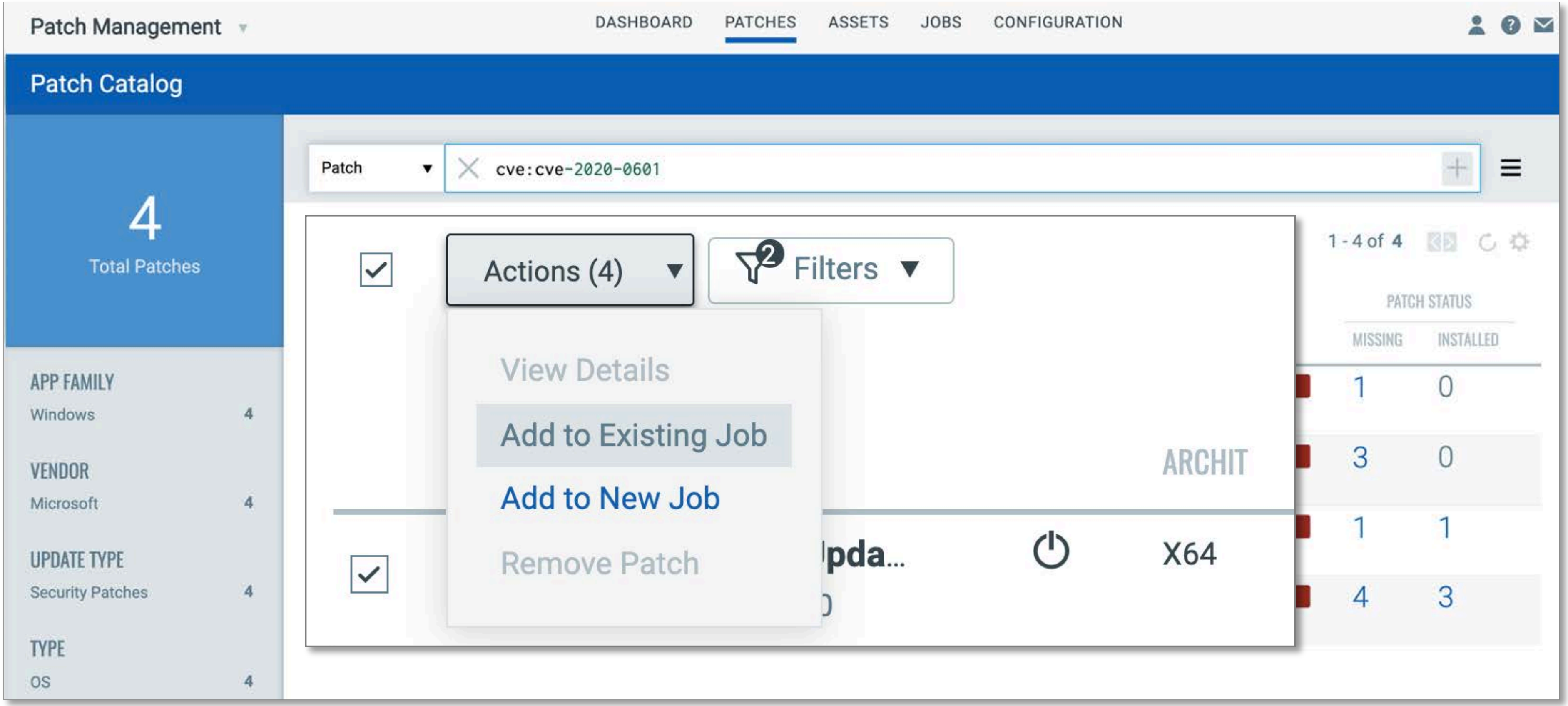
Qualys.

Remediation

- Automatically correlate vulnerabilities to patches
- End-to-end User Interface workflows
- Fit-for-purpose visualizations and recommendations
- Orchestration for remediation



Qualys.



Patch ▾ cve:cve-2020-0601

4
Total Patches

APP FAMILY

Windows	4

VENDOR

Microsoft	4

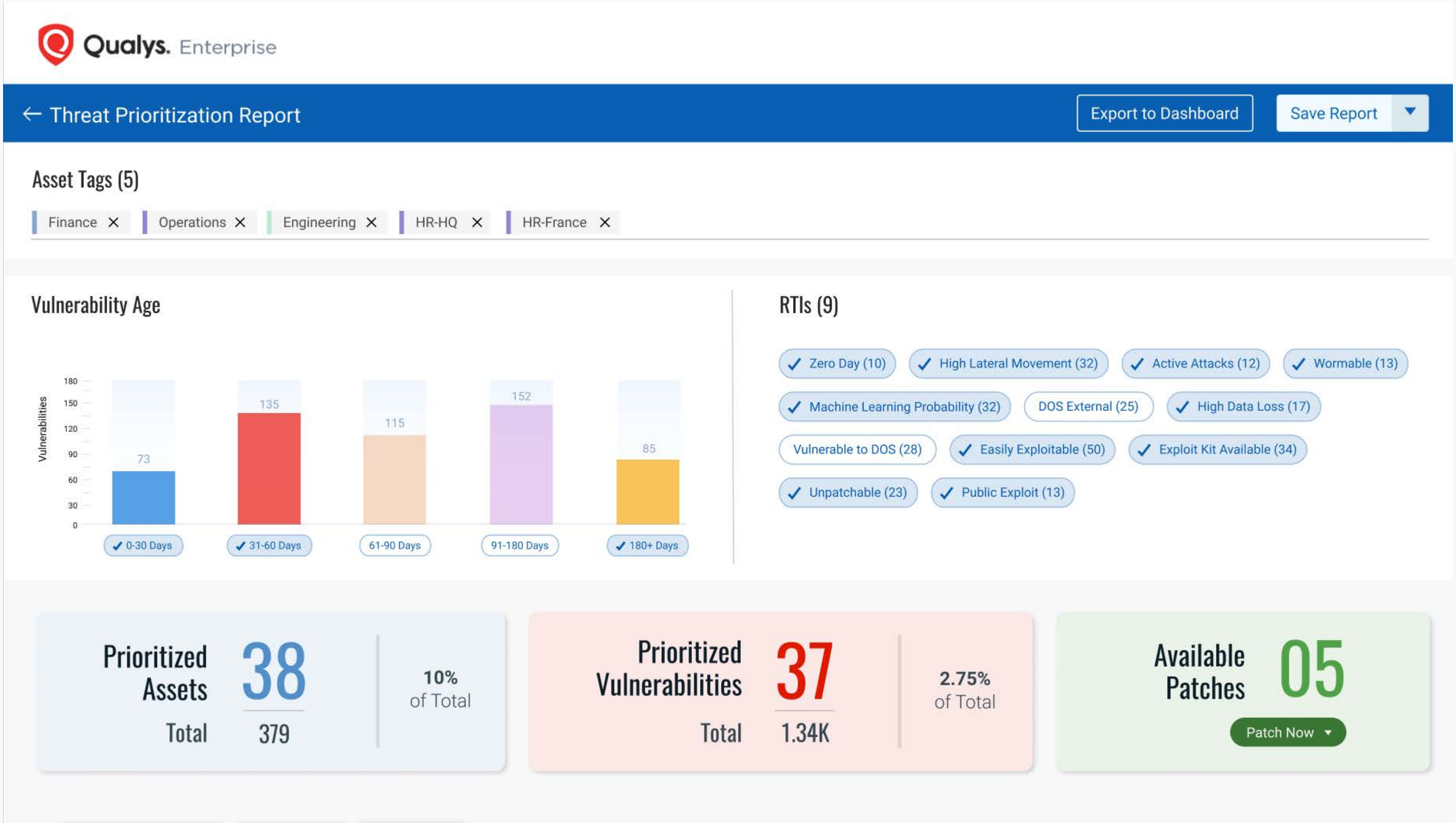
UPDATE TYPE

Security Patches	4

TYPE

OS	4

PATCH STATUS	
MISSING	INSTALLED
1	0
3	0
1	1
4	3



Asset Tags (5)

Finance ✕ | Operations ✕ | Engineering ✕ | HR-HQ ✕ | HR-France ✕

Vulnerability Age

RTIs (9)

- ✓ Zero Day (10)
- ✓ High Lateral Movement (32)
- ✓ Active Attacks (12)
- ✓ Wormable (13)
- ✓ Machine Learning Probability (32)
- DOS External (25)
- ✓ High Data Loss (17)
- Vulnerable to DOS (28)
- ✓ Easily Exploitable (50)
- ✓ Exploit Kit Available (34)
- ✓ Unpatchable (23)
- ✓ Public Exploit (13)

Prioritized Assets 38
Total 379
10% of Total

Prioritized Vulnerabilities 37
Total 1.34K
2.75% of Total

Available Patches 05

Prioritization Engine – Machine Learning

Written in Python and TensorFlow

Dataset of 120,000+ Vulnerabilities

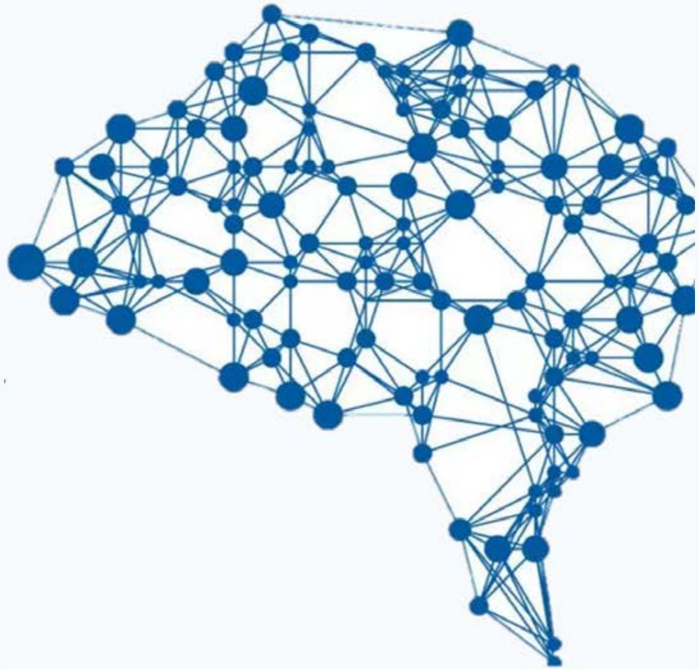
132 Vulnerability Features

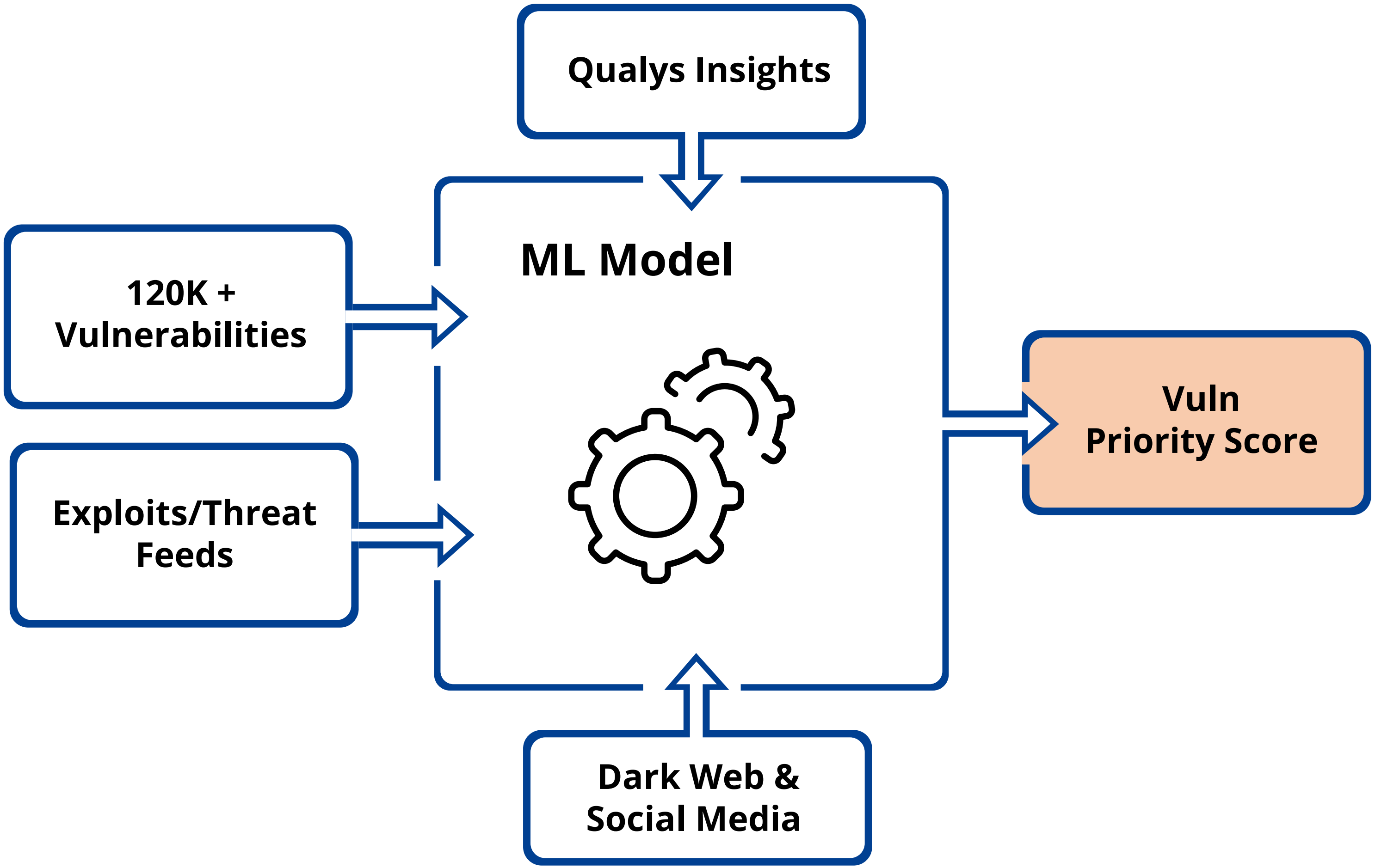
Live Exploits / Proof Of Concepts

Historical Threat Patterns

Historical Vulnerable Software/Vendor

Dark Web and Social Media References




Qualys Insights
ML Model
120K +
Vulnerabilities
Exploits/Threat
Feeds
Vuln
Priority Score
Dark Web &
Social Media

Contextual Awareness

Your Network is Unique to You

External Facing Assets

Business / Customer Applications

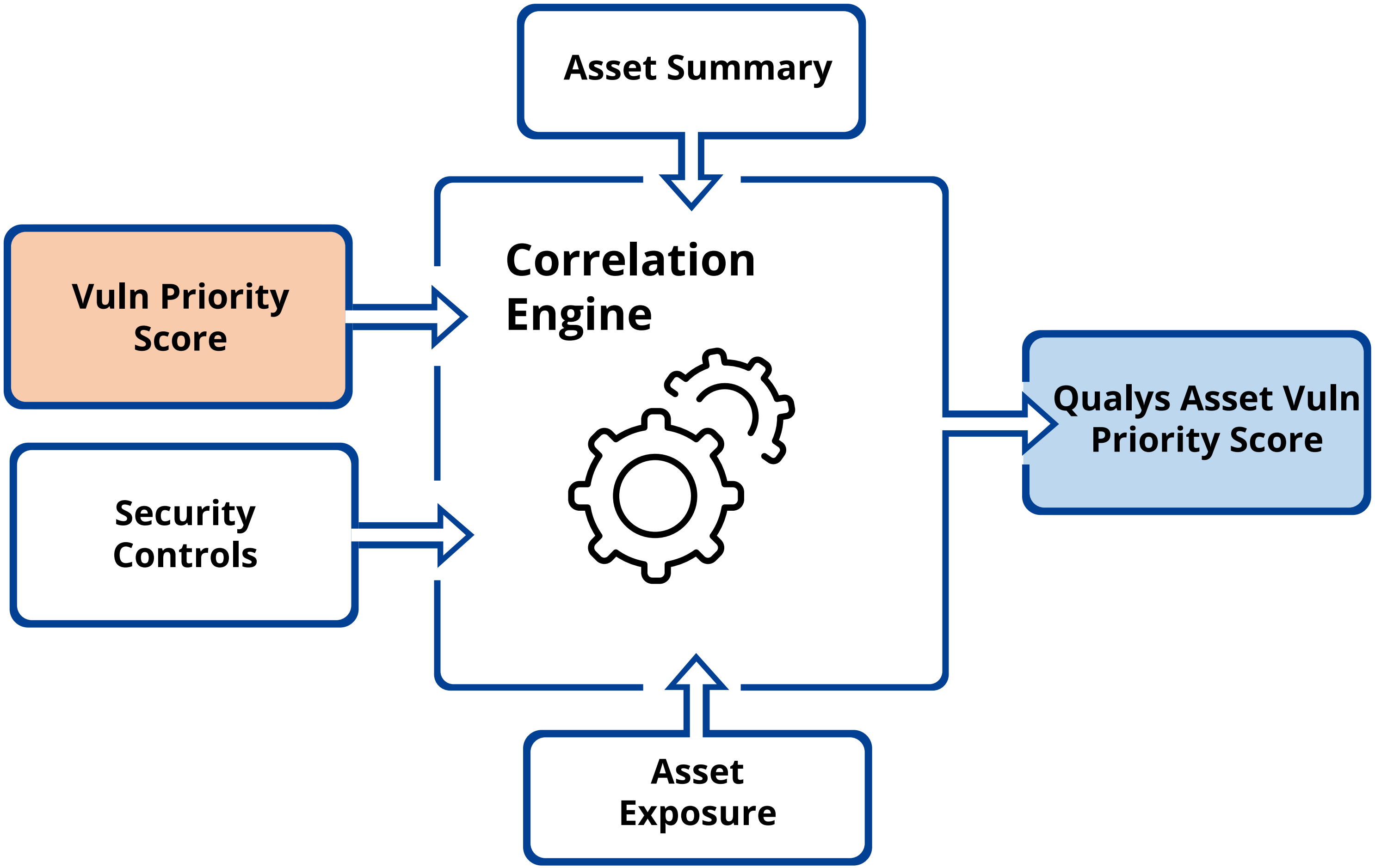
Network Reachability / Cloud Security Groups

Zero-Trust Networking / Micro-Segmentation

Data Sensitivity and Data Access Governance

Asset System Configuration

Security Control Validation


Asset Summary
Vuln Priority Score
Security Controls
Correlation Engine
Qualys Asset Vuln Priority Score
Asset Exposure

VMDR
Concept Demo

VMDR comes with much more

Unlimited Cloud Agents

Unlimited Virtual Scanners

Unlimited Passive Sensors

Certificate Inventory

Cloud Inventory

Container Inventory

Mobile Device Inventory

Asset Categorization

Asset Normalization

Configuration Assessment

CIS Benchmarks

Continuous Monitoring

Vulnerability Management

Patch Detection and CVE Correlation

Available February 2020

Thank You

Chris Carlson

ccarlson@qualys.com