QSC23

Unified Attack Surface Management

with an Attacker's and Defender's View

Kunal Modasiya
Vice President, Product Management
Attack Surface Management – CSAM & EASM
Web App & API Security - WAS

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

Measure Cyber Risk

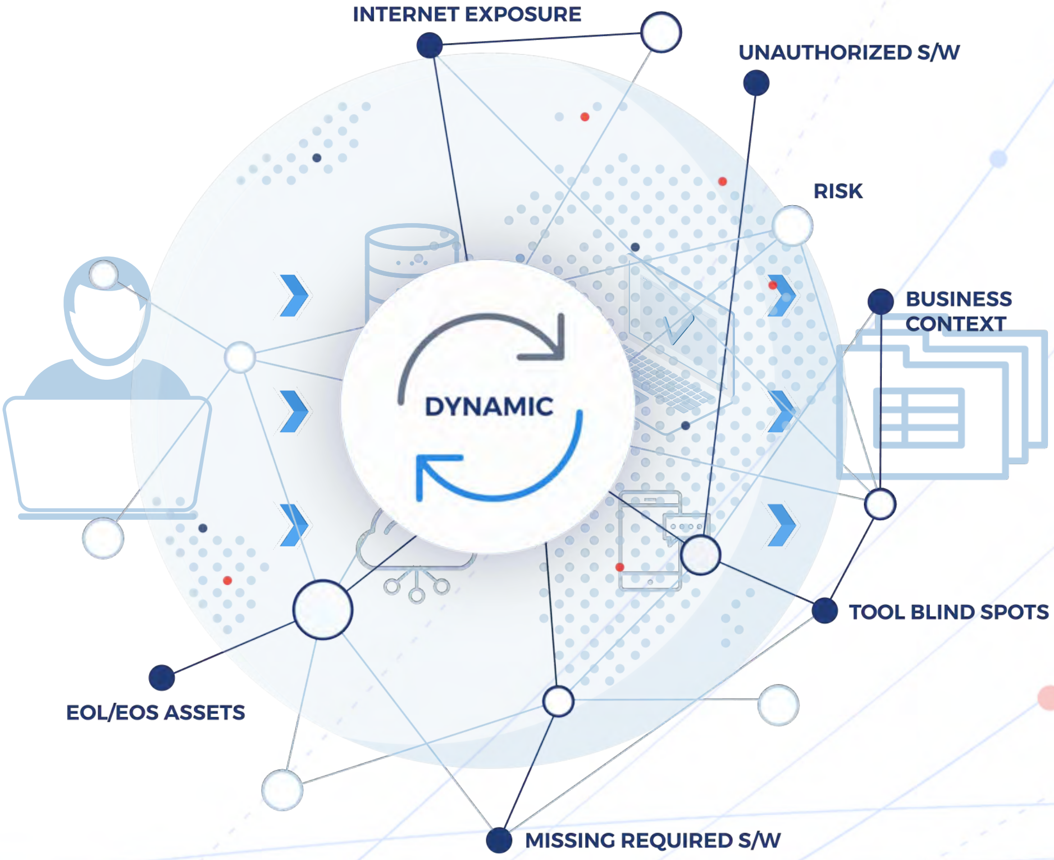
First Step in measuring your Cyber Risk begins with Effective Attack Surface Management Program and discover all the Assets

Qualys.

Challenges with IT-Centric Asset Inventory

Outdated and Lacks Cyber Risk Context

- ☒ Laborious, time-consuming task to create & maintain spreadsheets
- ☒ Outdated CMDB lacks real-time context of IT Estate
- ☒ Lack of visibility into all environments (e.g., PCI, OT, Internet-facing) creates blind-spots
- ☒ Unauthorized software, ports, and services
- ☒ Risk of End-of-Support/End-of-Life Software
- ☒ Lacks Cyber Risk Context in the Asset Inventory



How do you perform Inventory Risk Assessment with Inaccurate Inventory ?

The Attack Surface is Constantly Evolving

IT Assets

Digital Certificates

Office 365

SaaS Apps

Servers

Open Source Software

Databases

IP Cameras

Endpoints

Cloud Assets

aws

Cloud Apps

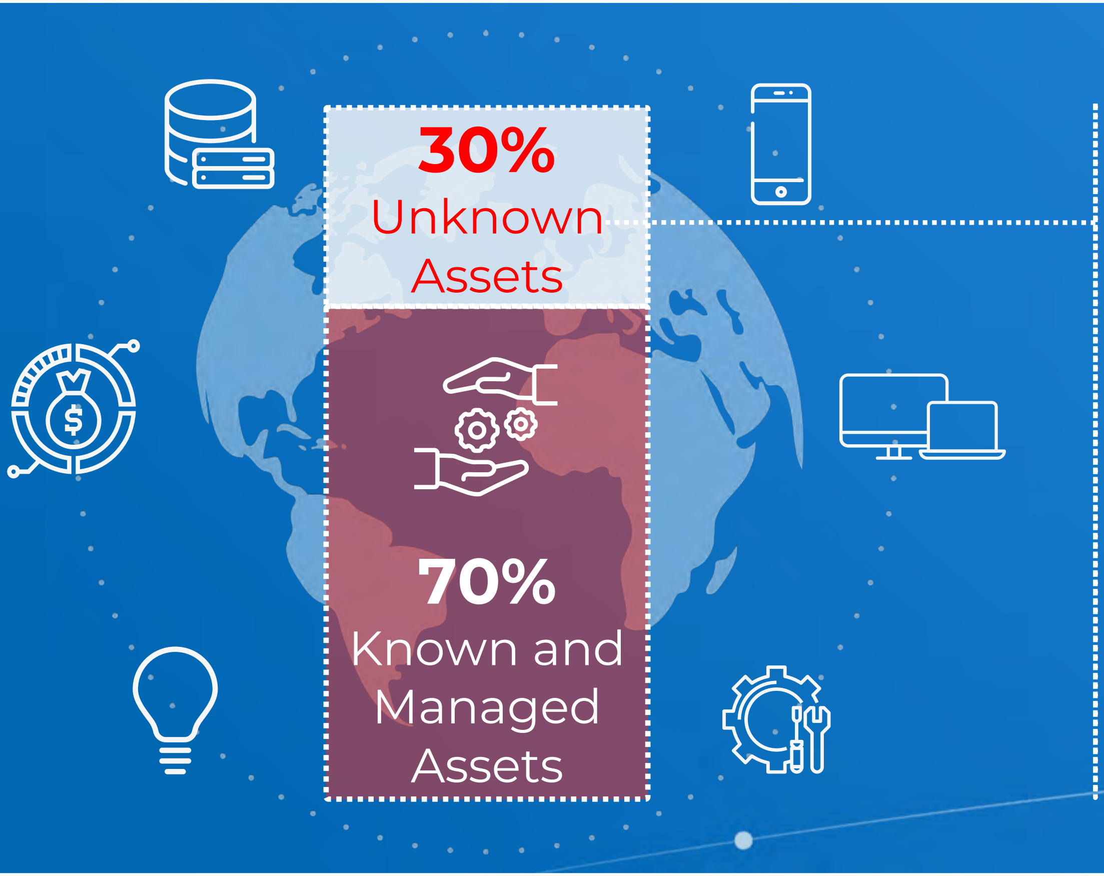
Azure

First-party Apps

Qualys.

Impact of Unknown Assets

Not Known to Your VM, But Known to Attackers



30%
Unknown Assets

70%
Known and Managed Assets

- **Only 9%** of orgs believe they actively **monitor 100% of their attack surface**
- **43%** of orgs spend more than **80 hours discovering assets**
- **69%** or orgs experience an attack **targeting 'unknown' assets**

Introducing Qualys' Approach to Manage Dynamic Attack Surface

Qualys.

CyberSecurity Asset Management (CSAM)

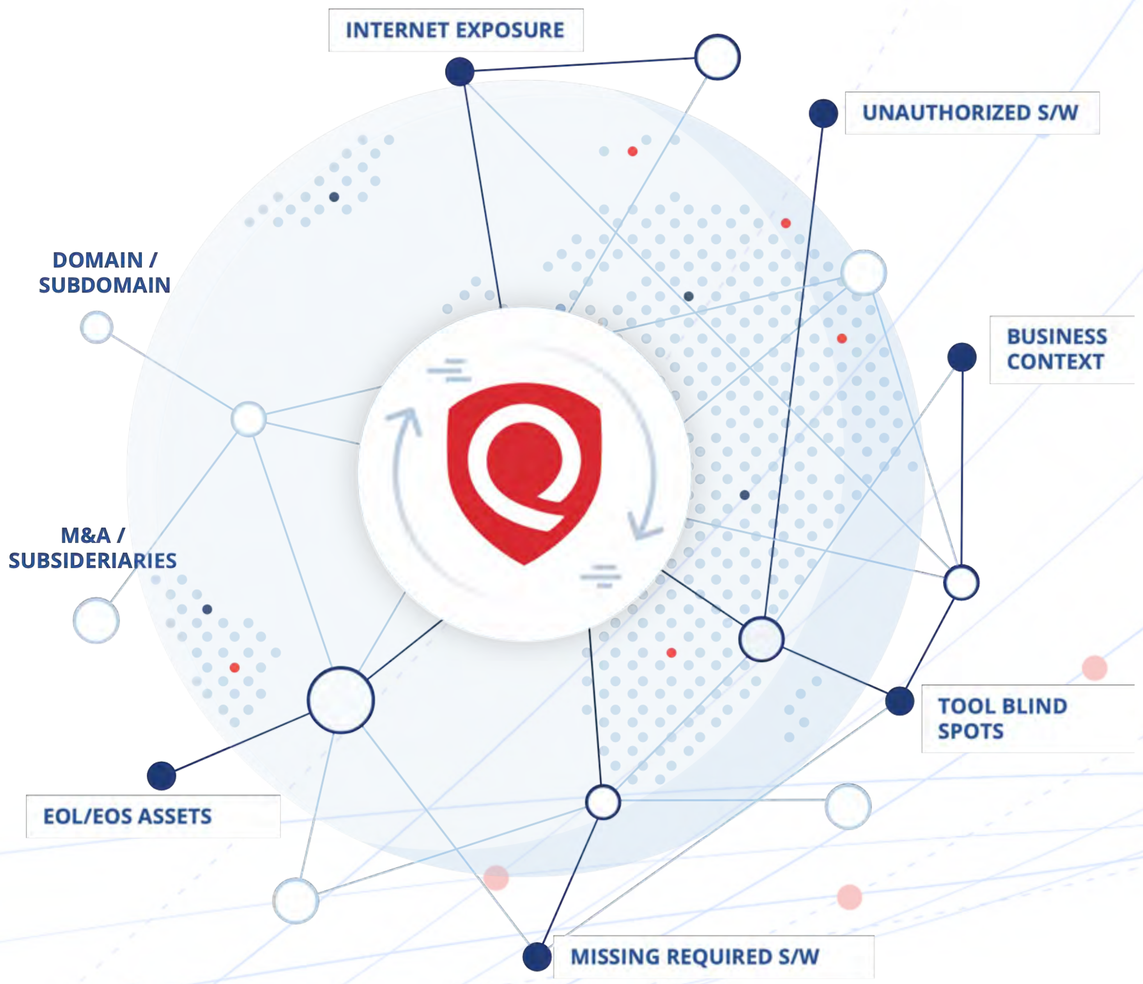
Internal + External View = Entire Attack Surface

1 **Unified Inventory with Cyber Risk & Business Context**

Simplify and improve Risk-based **vulnerability management**, **AppSec, Patch management & SOC** programs

2 **External Attack Surface Management**

Continuous discovery, risk assessment, prioritization, and remediation of the entire attack surface



Qualys.

CSAM - Attack Surface Discovery

Use Case Based Flexible and Incremental Discovery Methods

Internal assets

Agent, Scanner, Sensors

IOT/OT assets

Passive Network Sensor

Internal +
External
Known and
Unknown
Asset

Assets from 3rd parties

API-Based Connectors

Active Directory · servicenow · bmc helix · vmware

External assets

Open-source Tech &
Qualys Internet canner

SHODAN · Scanner · Whois Identity for everyone · DNS

Qualys.

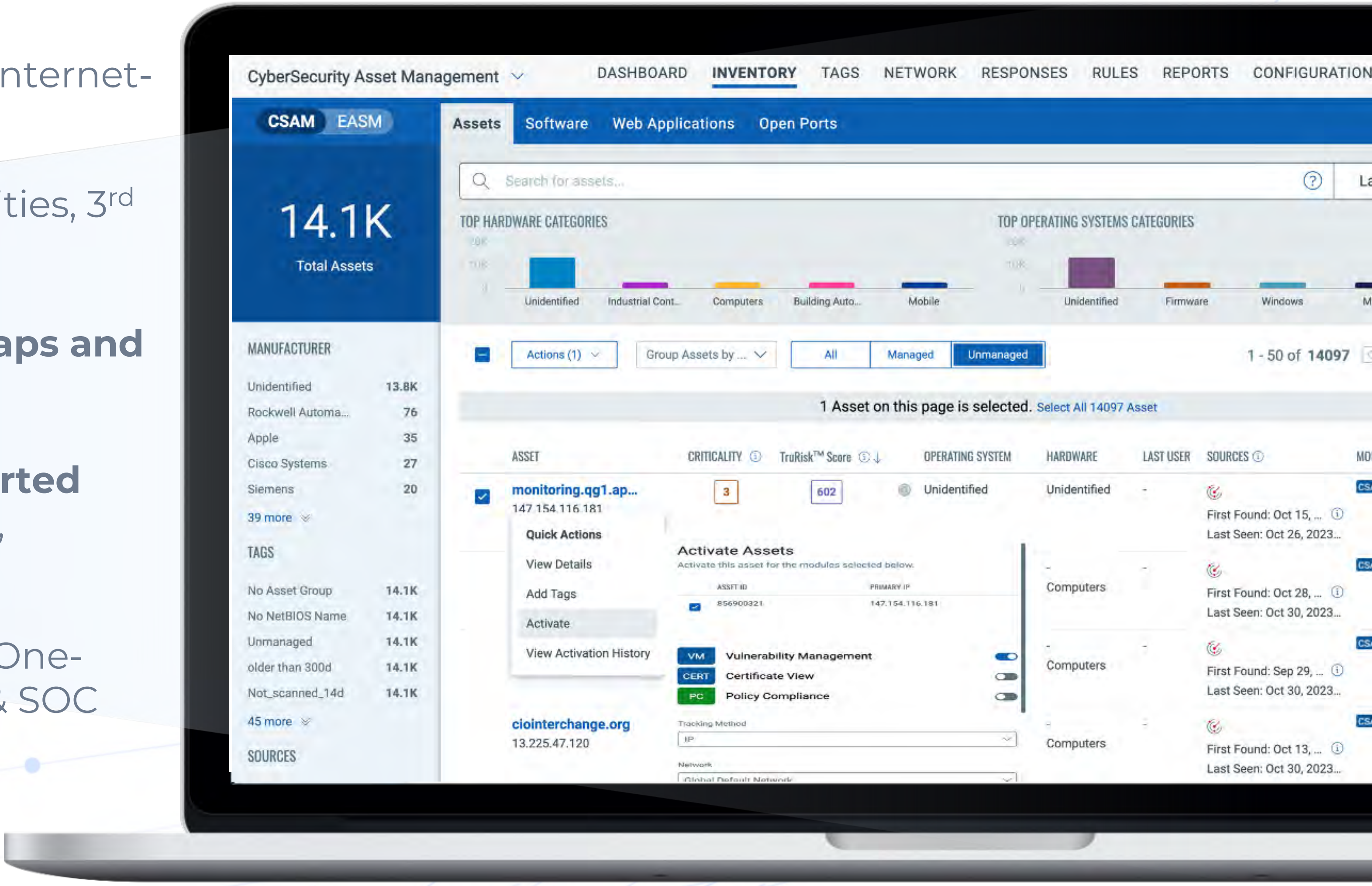
External Attack Surface Discovery & Monitoring

Qualys.

External Attack Surface Management (EASM)

Attackers' View – Outside-in perspective

1. Discover '**Previously Unknown**' internet-facing assets
2. **Monitor Cyber Risk** for M&A Entities, 3rd party vendors, subsidiaries
3. **Identify** & **remediate security gaps and misconfiguration** issues
4. **Continuous monitoring - Be alerted** when unknown assets, domains, subdomains are found
5. **Operationalize asset data** with One-click into VM, WAS, Patch, ITSM & SOC



MANUFACTURER	
Unidentified	13.8K
Rockwell Automa...	76
Apple	35
Cisco Systems	27
Siemens	20
39 more	

TAGS	
No Asset Group	14.1K
No NetBIOS Name	14.1K
Unmanaged	14.1K
older than 300d	14.1K
Not_scanned_14d	14.1K
45 more	

SOURCES

1 Asset on this page is selected. Select All 14097 Asset

ASSET	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCES
monitoring.qg1.ap... 147.154.116.181	3	602	Unidentified	Unidentified	-	First Found: Oct 15, ... Last Seen: Oct 26, 2023...
				Computers	-	First Found: Oct 28, ... Last Seen: Oct 30, 2023...
				Computers	-	First Found: Sep 29, ... Last Seen: Oct 30, 2023...
ciointerchange.org 13.225.47.120				Computers	-	First Found: Oct 13, ... Last Seen: Oct 30, 2023...

Activate Assets

Activate this asset for the modules selected below.

	ASSET ID	PRIMARY IP
☑	856900321	147.154.116.181

- VM Vulnerability Management ●
- CERT Certificate View ○
- PC Policy Compliance ○

Tracking Method: IP

Network: Global Default Network

Qualys.

EASM KPI Dashboard – Measuring Risk

~2K
# of Customers

~200K (3%)
# of Assets w/ DB Open Ports(mssql, mysql, cassandra…)

2.9M+
# of Sub Domain Discovered

~7M
# of EASM Discovered Asset

330K+
Avg # of External Assets of Top 10 customers

6000+
# of Subsidiaries

~500K(7%)
# of Vulnerable EASM Asset

10+
Avg # of Related Entities Discovered

~1.5M (21%)
# of Assets w/ Risky Open Ports(RDP, SSH, SFTP…)

105K+
# of Domain Discovered

Avg % of External **UNKNOWN** Asset to Total Asset is

~30-36%

Qualys.

Internal Attack Surface Discovery & Monitoring

Introducing Qualys Cloud Agent Passive Sensor

For detecting 100% of devices' communication in the network

Continuously Monitor and Reduce Internal Attack Surface

✓ **Single, Lightweight, extensible, self-updating & centrally managed Agent**

Customizable Qualys Agent for various systems, filters data from public or home networks

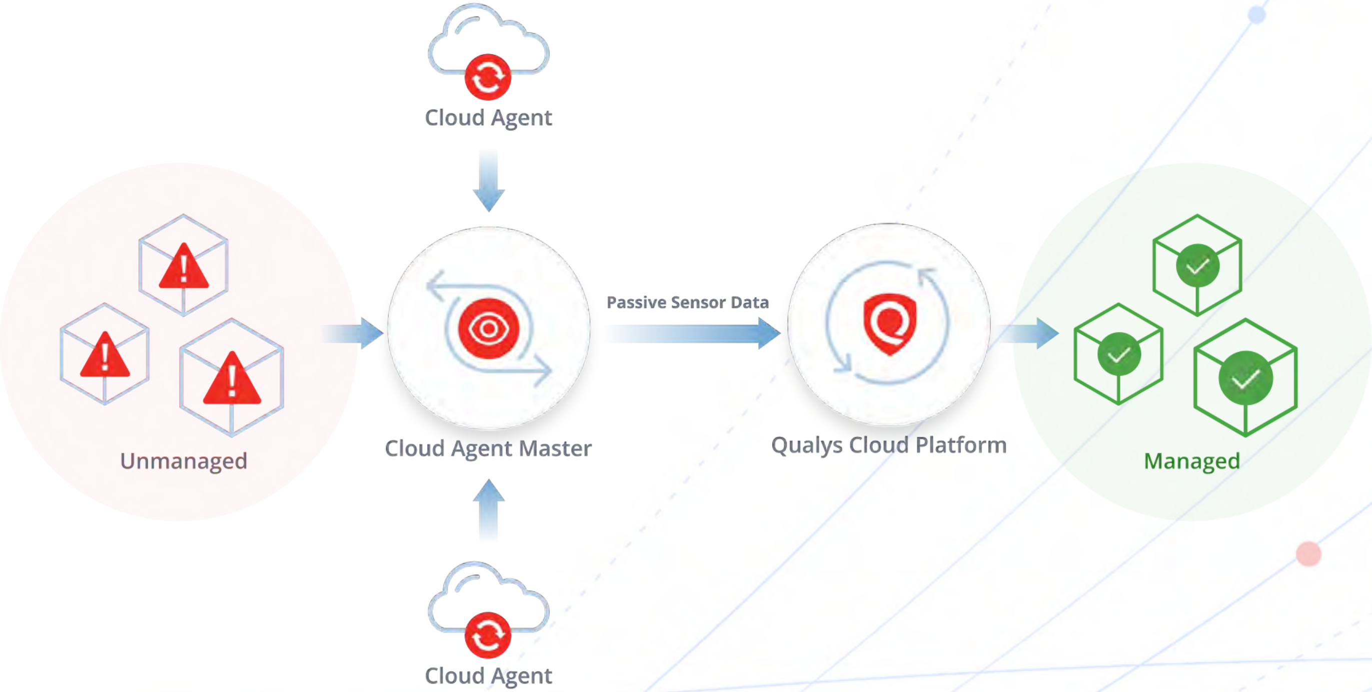
✓ **Get away from the limitation of network taps**

Non-intrusive network reporting with auto-elected Master Reporter per domain, showing managed/unmanaged assets in Qualys platform

✓ **Passive sensing**

Data will be sniffed passively in the subnet by listening to broadcasts and multicasts

- Collect rich asset metadata using ARP, DHCP, SSDP, NetBios, mDNS, CDP/LLDP, LLMNR, WSD and more.



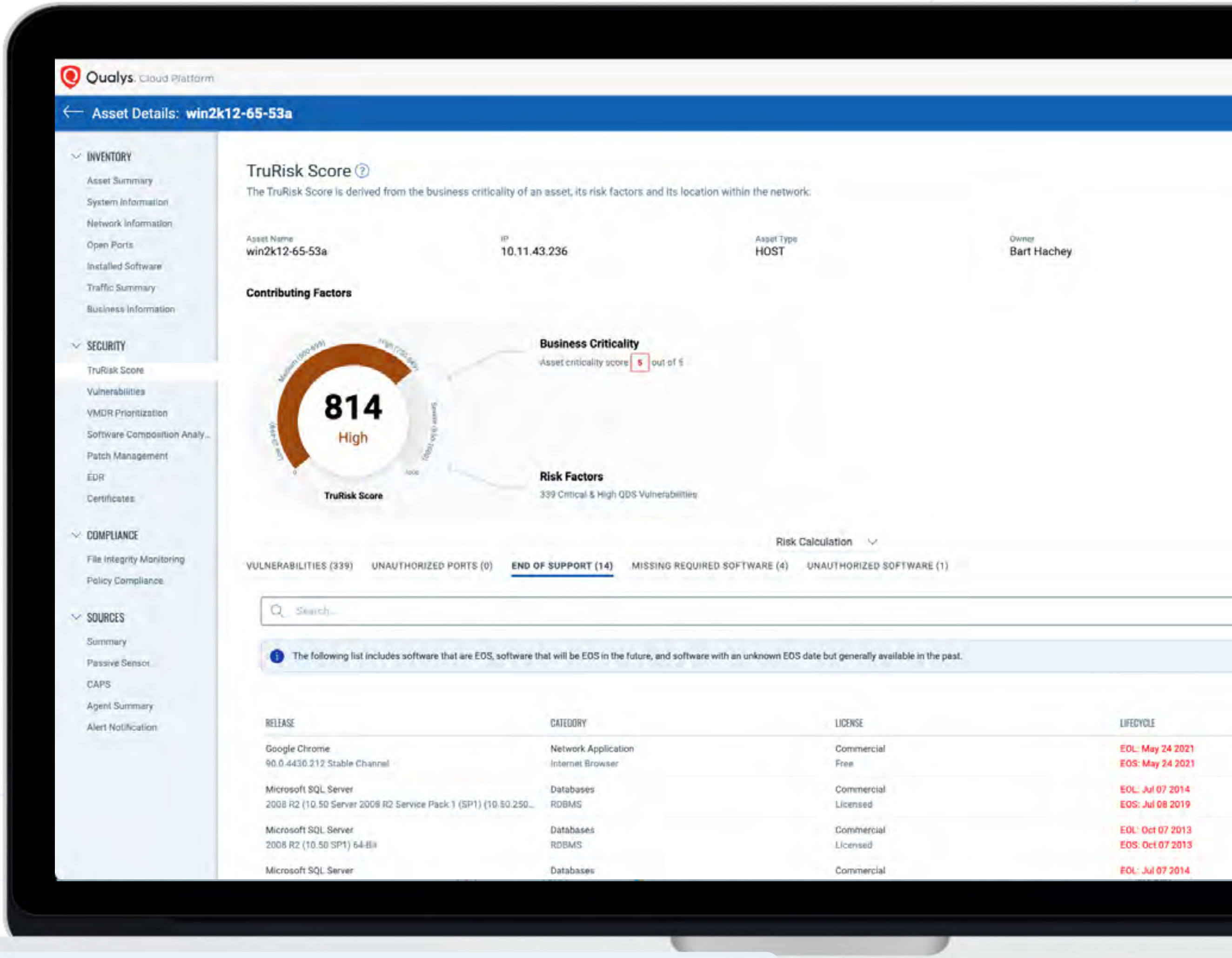
Identify Rogue Devices even in IOT environment without a massive investment in sensors and new systems

Qualys.

CyberSecurity Asset Management - CSAM

Defenders’ View – Inside-out Perspective

1. Comprehensive **Asset discovery & Inventory** – Cloud, On-prem, IoT/OT, Internet-facing
2. **Third-party integrations** for asset aggregation and intelligence
3. **Bi-Dir CMDB Sync** for enriching inventory with **business context**
4. **Cyber Risk Assessment of Inventory**
   - Unauthorized Software, Ports
   - Find Security Agent Coverage
   - Manage EoL/EoS (Tech-Debt)
5. **Risk-based prioritization** and remediation workflows **with Qualys TruRisk**



TruRisk Score

The TruRisk Score is derived from the business criticality of an asset, its risk factors and its location within the network.

Asset Name	IP	Asset Type	Owner
win2k12-65-53a	10.11.43.236	HOST	Bart Hachey

Contributing Factors

Business Criticality
Asset criticality score 5 out of 5

Risk Factors
339 Critical & High QDS Vulnerabilities

The following list includes software that are EOS, software that will be EOS in the future, and software with an unknown EOS date but generally available in the past.

RELEASE	CATEGORY	LICENSE	LIFECYCLE
Google Chrome 90.0.4430.212 Stable Channel	Network Application Internet Browser	Commercial Free	EOL: May 24 2021 EOS: May 24 2021
Microsoft SQL Server 2008 R2 (10.50 Server 2008 R2 Service Pack 1 (SP1) (10.50.250...	Databases RDBMS	Commercial Licensed	EOL: Jul 07 2014 EOS: Jul 08 2019
Microsoft SQL Server 2008 R2 (10.50 SP1) 64-Bit	Databases RDBMS	Commercial Licensed	EOL: Oct 07 2013 EOS: Oct 07 2013
Microsoft SQL Server	Databases	Commercial	EOL: Jul 07 2014

Purpose-built Inventory for Cyber Security Team

Bringing Together External + Internal Attack Surface

Purpose-built for Cybersecurity and VM/Risk teams

1 External Attack Surface Management

Attacker outside-in perspective.

- Discover and continuously **monitor outside-in digital footprint internet-facing assets**
- **Natively integrate with VMDR** (or other) for vuln analysis and prioritization
- Continuously improve and implement **attack surface management (ASM)** strategies

Internal Attack Surface Management 2

Defender inside-out perspective

- Discover **Cloud, On-prem, Data center, IT, OT/IoT** and **Rogue Assets**
- Security, **compliance**, and **Risk-based** prioritization
- Orchestrate and Automate Workflow across IT and Security

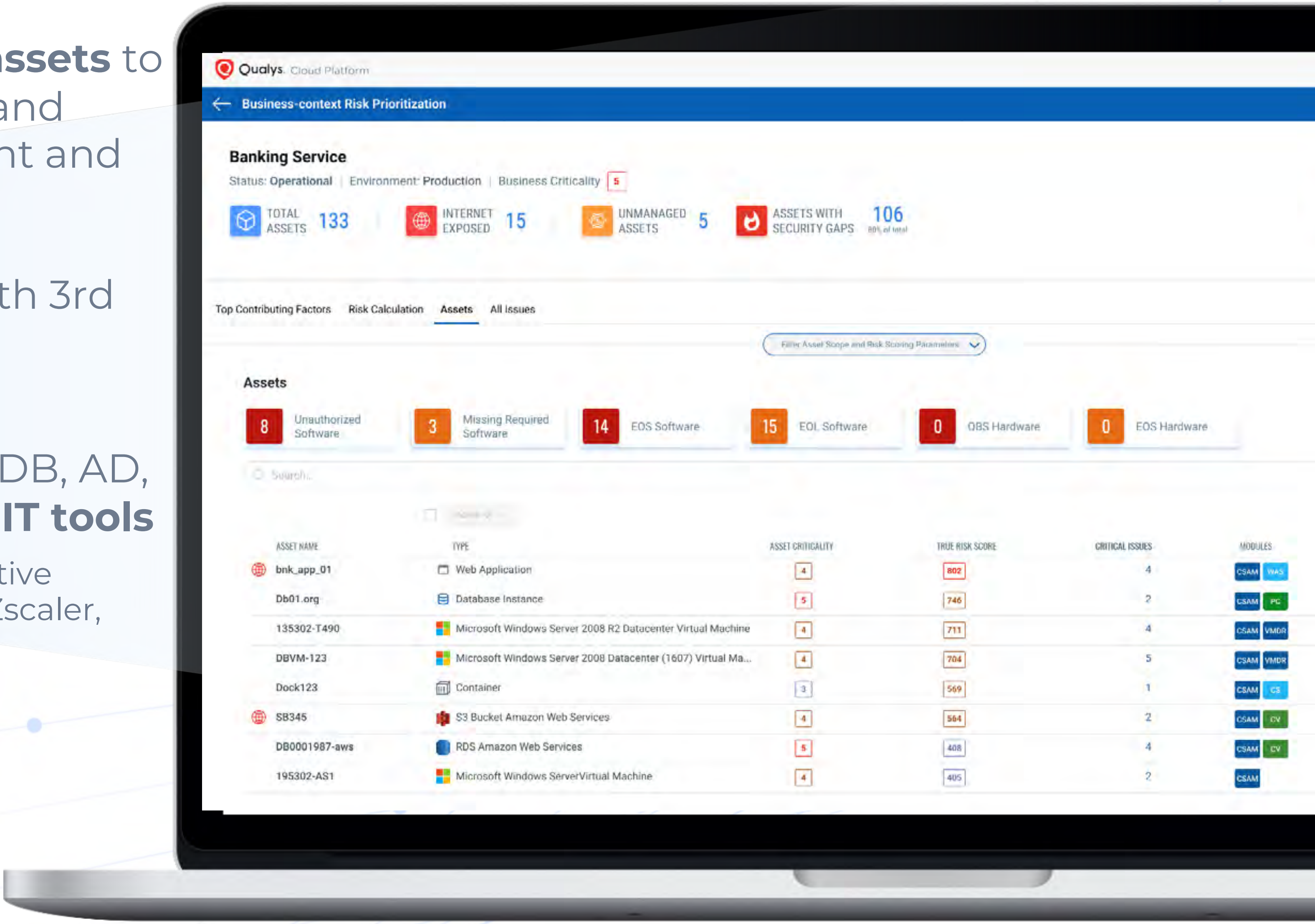
Risk-Based Prioritization

… Must Include 3rd-Party (Non-Qualys) Environment

1. **Bring in missing 3rd party assets** to Qualys for unified inventory and attack surface risk assessment and monitoring

2. **Risk-Based prioritization** with 3rd party business context

3. **3rd Party Connectors** for CMDB, AD, Webhook, and **Security and IT tools**
    - ServiceNow CMDB, BMC Helix, Active Directory**,** VMware, CrowdStrike, Zscaler, Splunk, Jira, etc.



Qualys. Cloud Platform

Business-context Risk Prioritization

Banking Service

Status: **Operational** | Environment: **Production** | Business Criticality 5

TOTAL ASSETS 133 | INTERNET EXPOSED 15 | UNMANAGED ASSETS 5 | ASSETS WITH SECURITY GAPS 106 80% of total

Top Contributing Factors | Risk Calculation | **Assets** | All Issues

Filter Asset Scope and Risk Scoring Parameters

Assets

8 Unauthorized Software | 3 Missing Required Software | 14 EOS Software | 15 EOL Software | 0 OBS Hardware | 0 EOS Hardware

Search...

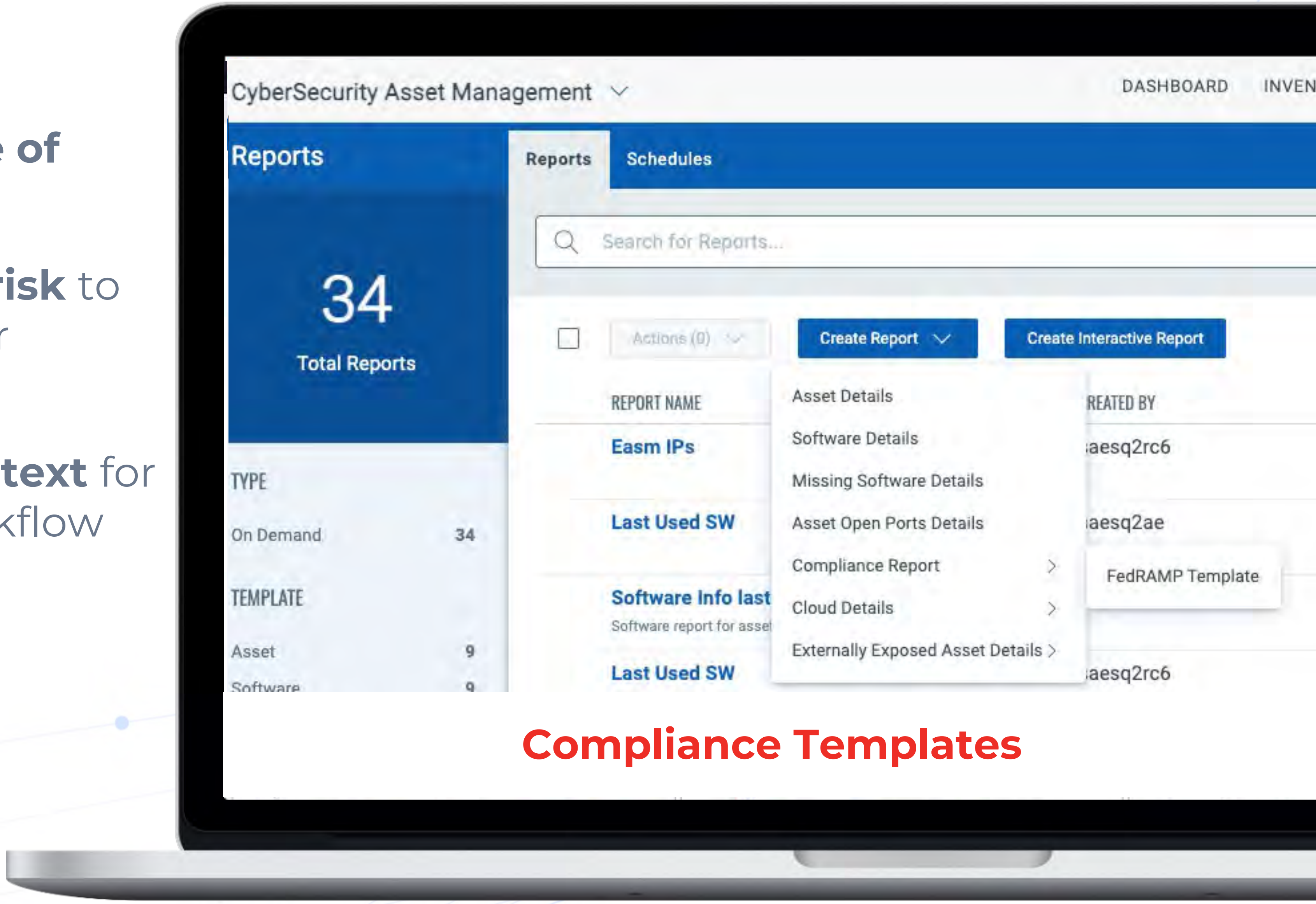
ASSET NAME	TYPE	ASSET CRITICALITY	TRUE RISK SCORE	CRITICAL ISSUES	MODULES
bnk_app_01	Web Application	4	802	4	CSAM WAS
Db01.org	Database Instance	5	746	2	CSAM PC
135302-T490	Microsoft Windows Server 2008 R2 Datacenter Virtual Machine	4	711	4	CSAM VMDR
DBVM-123	Microsoft Windows Server 2008 Datacenter (1607) Virtual Ma...	4	704	5	CSAM VMDR
Dock123	Container	3	569	1	CSAM CS
SB345	S3 Bucket Amazon Web Services	4	564	2	CSAM CV
DB0001987-aws	RDS Amazon Web Services	5	408	4	CSAM CV
195302-AS1	Microsoft Windows ServerVirtual Machine	4	405	2	CSAM

Qualys.

Communicate Cyber Risk

To Drive Business Outcomes

- Create a **single source of truth**
- **Communicate cyber risk** to all stakeholders in your organization
- Provide **complete context** for every stage of the workflow



REPORT NAME	REATED BY
Easm IPs	aesq2rc6
Last Used SW	aesq2ae
Software Info last Software report for asse	
Last Used SW	aesq2rc6

Compliance Templates

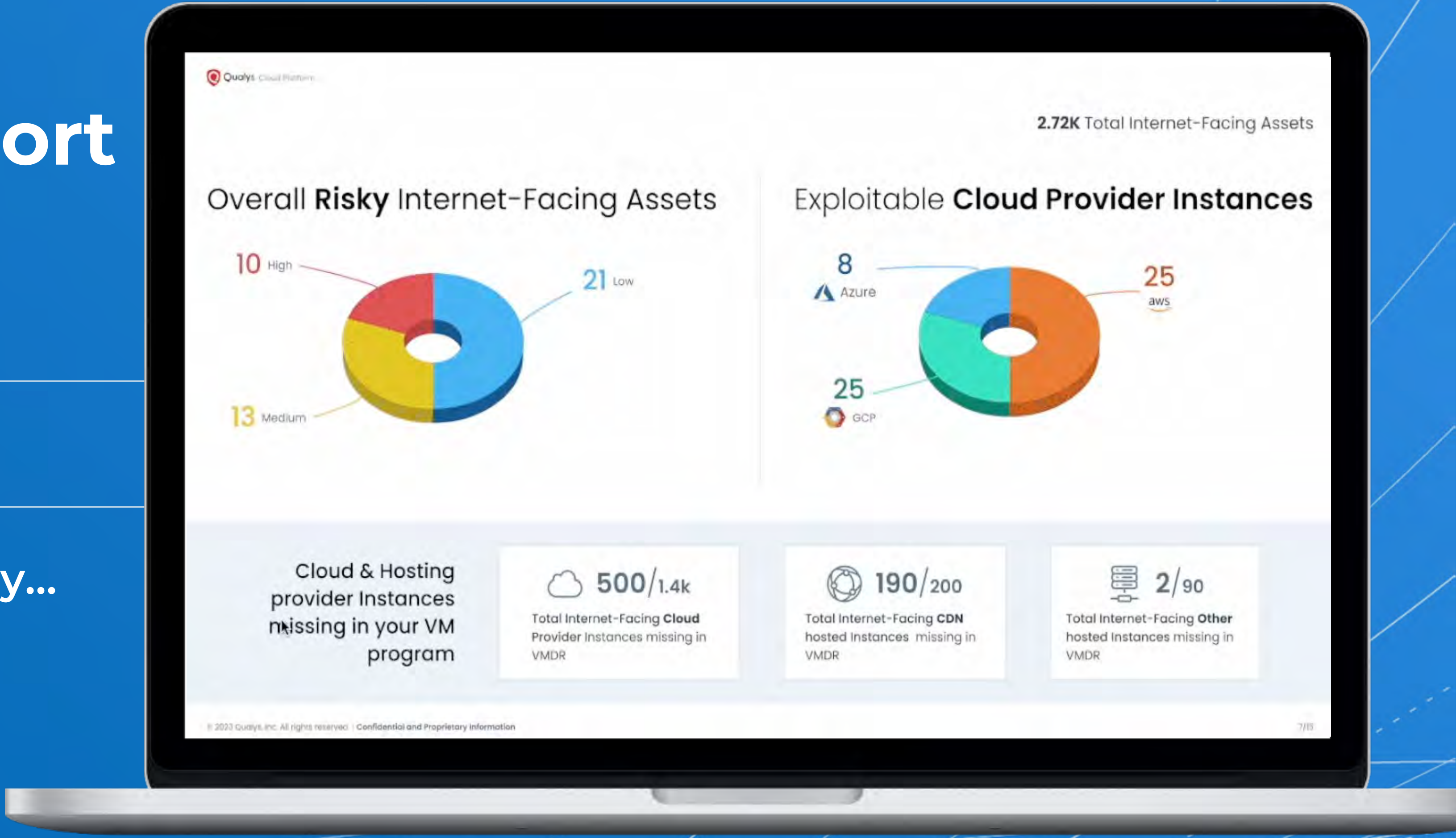
Qualys.

External Attack Surface Risk Report

Know your Risk on Internet-facing Assets

View Your Attack Surface

Prioritize Your Risk Accordingly...



Qualys Cloud Platform

2.72K Total Internet-Facing Assets

Overall **Risky** Internet-Facing Assets

Exploitable **Cloud Provider Instances**

Cloud & Hosting provider Instances missing in your VM program

500/1.4k Total Internet-Facing **Cloud** Provider Instances missing in VMDR

190/200 Total Internet-Facing **CDN** hosted Instances missing in VMDR

2/90 Total Internet-Facing **Other** hosted Instances missing in VMDR

© 2023 Qualys, Inc. All rights reserved | **Confidential and Proprietary Information** 7/15

Powered by:

Stop by the **Q&A Bar** to receive your EASM report and speak with a Qualys expert!

Qualys.

Powered by:

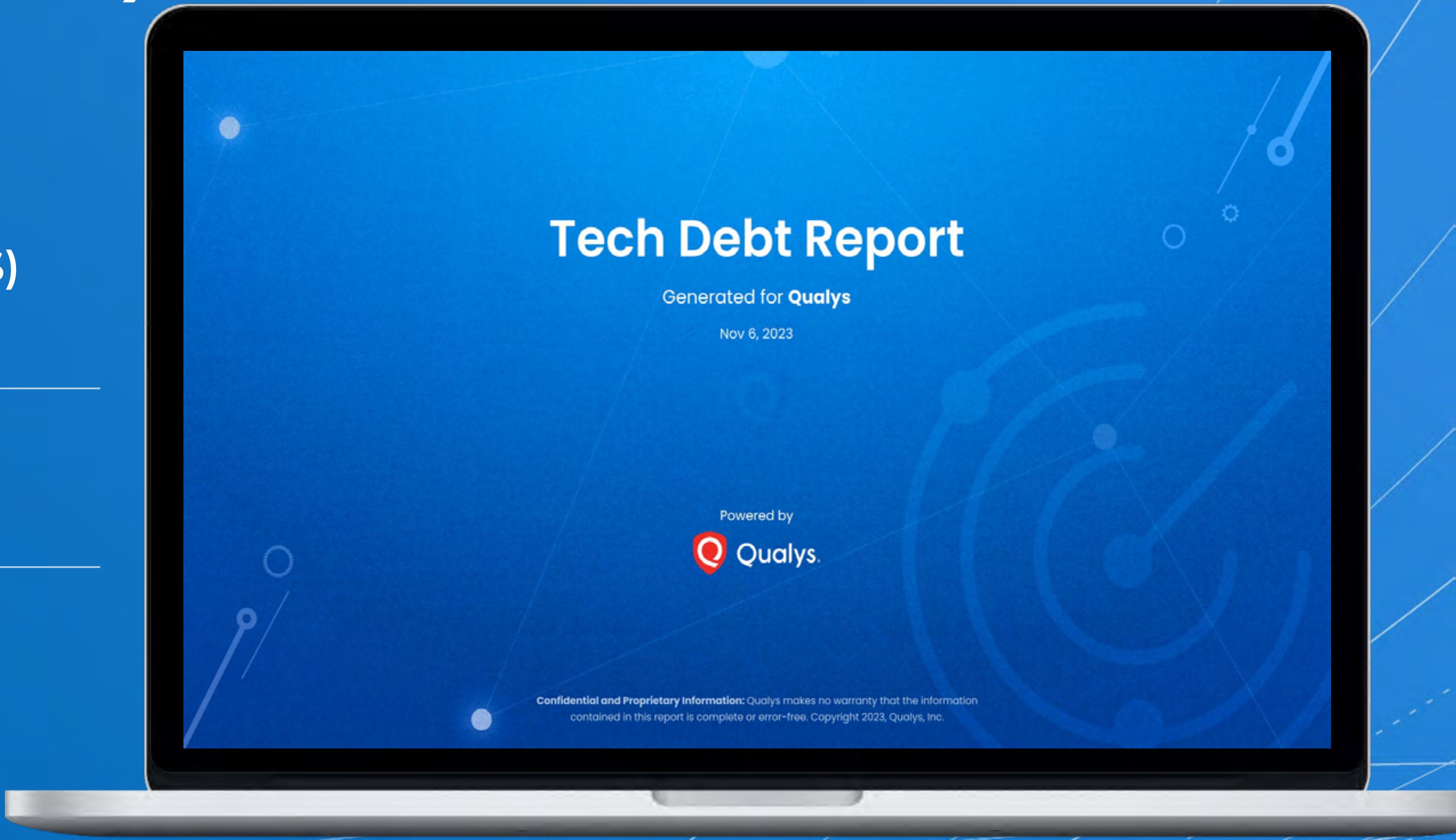
Tech-Debt (EoL/EoS) Risk Report

View Your Tech-Debt (EoL/EoS) across hybrid environment

Proactively plan of upgrade of upcoming EoL/EoS

TruRisk Based Prioritization

Coming Soon



Tech Debt Report

Generated for **Qualys**

Nov 6, 2023

Powered by

Qualys.

Confidential and Proprietary Information: Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2023, Qualys, Inc.

Powered by:

Solving CISO Challenges

Simplified & Optimized Cybersecurity with Unified Platform

No More Siloed Tools

- External Attack Surface Management
- IT Asset Inventory for On-Prem
- IT Asset Inventory for Cloud
- IT Asset Inventory for OT/IOT
- Vulnerability Management
- CMDB/ITSM Ticketing

SecOps & IT Ops Optimization

- Removes manual stitching of data across VM, ITSM, CMDB, Patch Mgmt, SOC & GRC tools
- Discover entire attack surface and add business context with Bi-directional CMDB sync

Reduced TCO

- Reduced TCO with centralized platform
- Consolidate siloed point products into Unified One-platform-one-agent

Eliminate Cyber Risk

Qualys.

Eliminate Cyber Risk

With a Continuous, Actionable Inventory

Discovery internal rogue and external unknown unmanaged assets and bring them to VM, WAS, PC Scan

Proactively find and plan upgrade the EoL/EoS Software and associated vulnerabilities

One-click Uninstall workflow for unauthorized, open source software

Accelerate the incident triage and response

ROI: Delivering Business Outcomes

Reduce the Attack Surface with a Unified Approach

Mean-Time-to-Discovery	30 Days	→	2 Days
Asset Coverage	~50-70%	→	~100%
Tech Debt Mitigation	Reactive	→	Planned up to 12 months
Mean-Time-to-Remediation	30+ Days	→	1-2 Days

CyberSecurity Asset Management

with **External Attack Surface Management (EASM)**

Turn on CSAM + EASM for your Environment:

- **30-day trial**
- **Joint review after 10 days**
- **Go to:** qualys.com/apps/cybersecurity-asset-management/

Qualys.

Beatrice Sirchis

Vice President, Application Security

Background includes:

- ✓ Network Engineer
- ✓ Security Engineer
- ✓ Security Architect and Project Manager
- ✓ CISO of Affiliate Subsidiaries at Discount Bank

Qualys. IDB BANK®

> *Enabling factor for business success.*

IDB Bank

More than 70 years of personal service and sophisticated financial solutions.

IDB Bank offers personalized and comprehensive solutions for protecting and preserving your wealth.

- ✓ Company Founded: **1935**
- ✓ Headquarters: **New York, NY**
- ✓ **Company Scope: International**

United States, Latin America, Israel

Driving the Bank's Rapid Business Growth

Cyber Security as a Business Enabler and Competitive Advantage for Bank

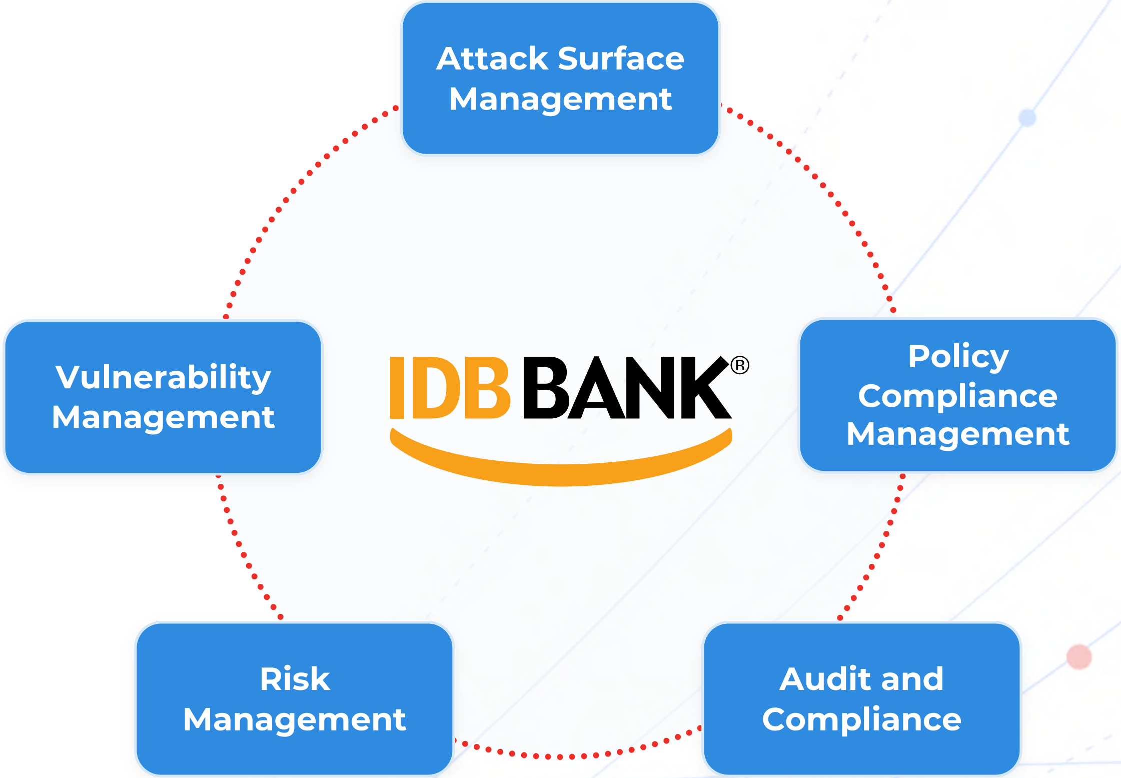
IT assets and resources of all types exist in on-prem and multi-cloud environment

Integrate business and IT systems/resources

- Highly regulated environment
- Real-time threat detection and remediation with integrated platform

Growing number of hardware and software providers – extension of corporate network means stringent security standards be met

Measure and improve efficiency within the security program – KRIs



Zero Trust Security Architecture

Critical Requirements We Were Looking For

Dynamic visibility of previously unknown/rogue assets in real-time to stay prepared for audits and regulations

Identify **external, internet-facing** exposure and bring to VM, PC scan

Identify gaps: EoL/EoS (and scope of impact), unauthorized software, missing agents, etc.

Automated CMDB sync to streamline remediation through ticket assignment and SLA enforcement

Reporting with unified dashboard including KRIs, vulns with critical risk, and defined risk thresholds to prioritize most important work

Qualys. IDB BANK®

IDB BANK®

Shared platform across IT, Security, Internal Audit, and Risk Management Teams.

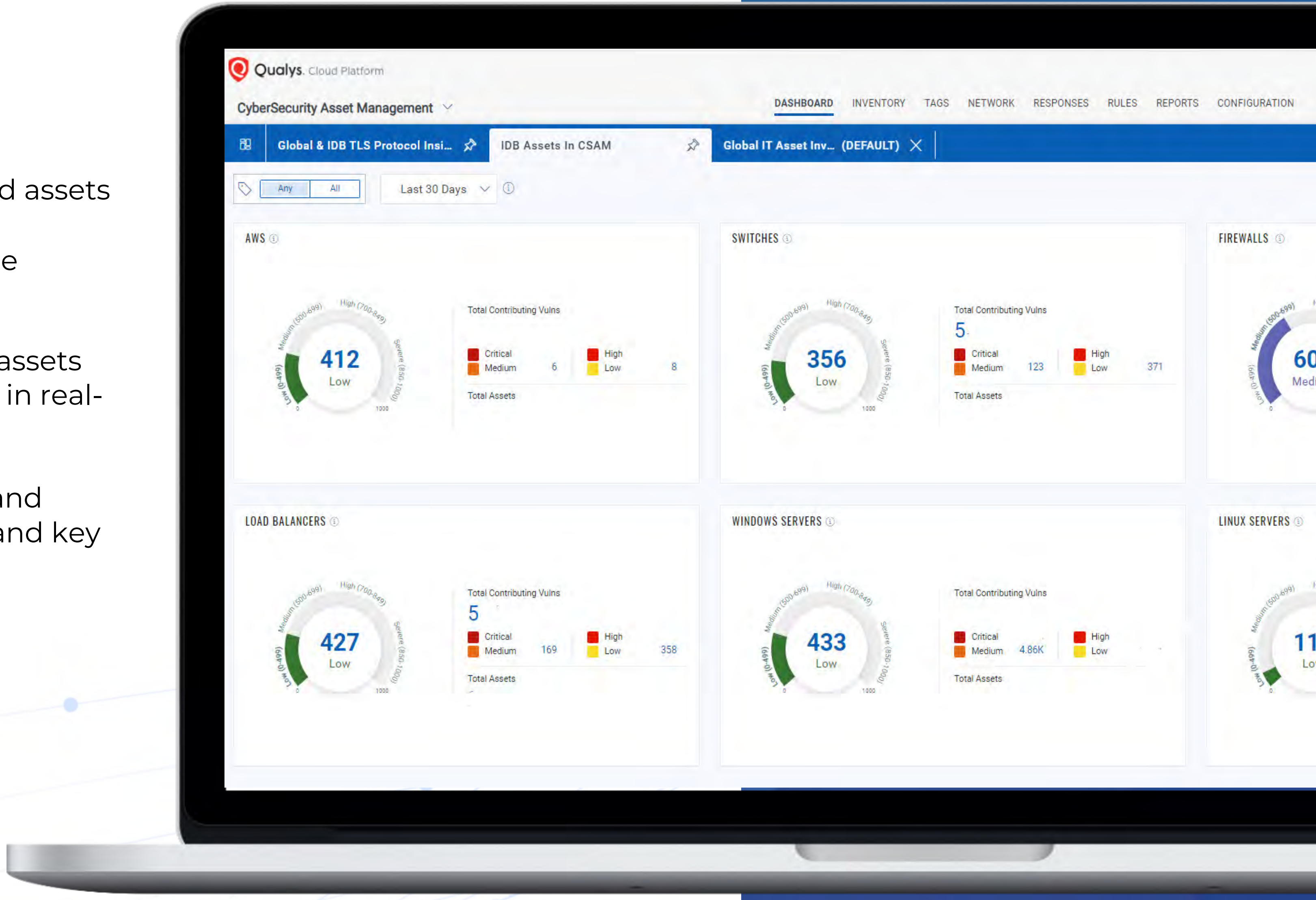
How We Use CSAM

Continuous Visibility Across the Hybrid Environment

Complete asset and software visibility across all our environments (categorization of assets)

- ✓ Including on-prem and multiple cloud assets
- ✓ Cloud agent deployment for complete software visibility
- ✓ Network passive sensor detects new assets connecting to our corporate network in real-time, to add them to VM & PC
- ✓ Using the Traffic Analyzer to understand asset communication, relationships, and key services (e.g., databases)

Effective purge rules to maintain inventory up-to-date



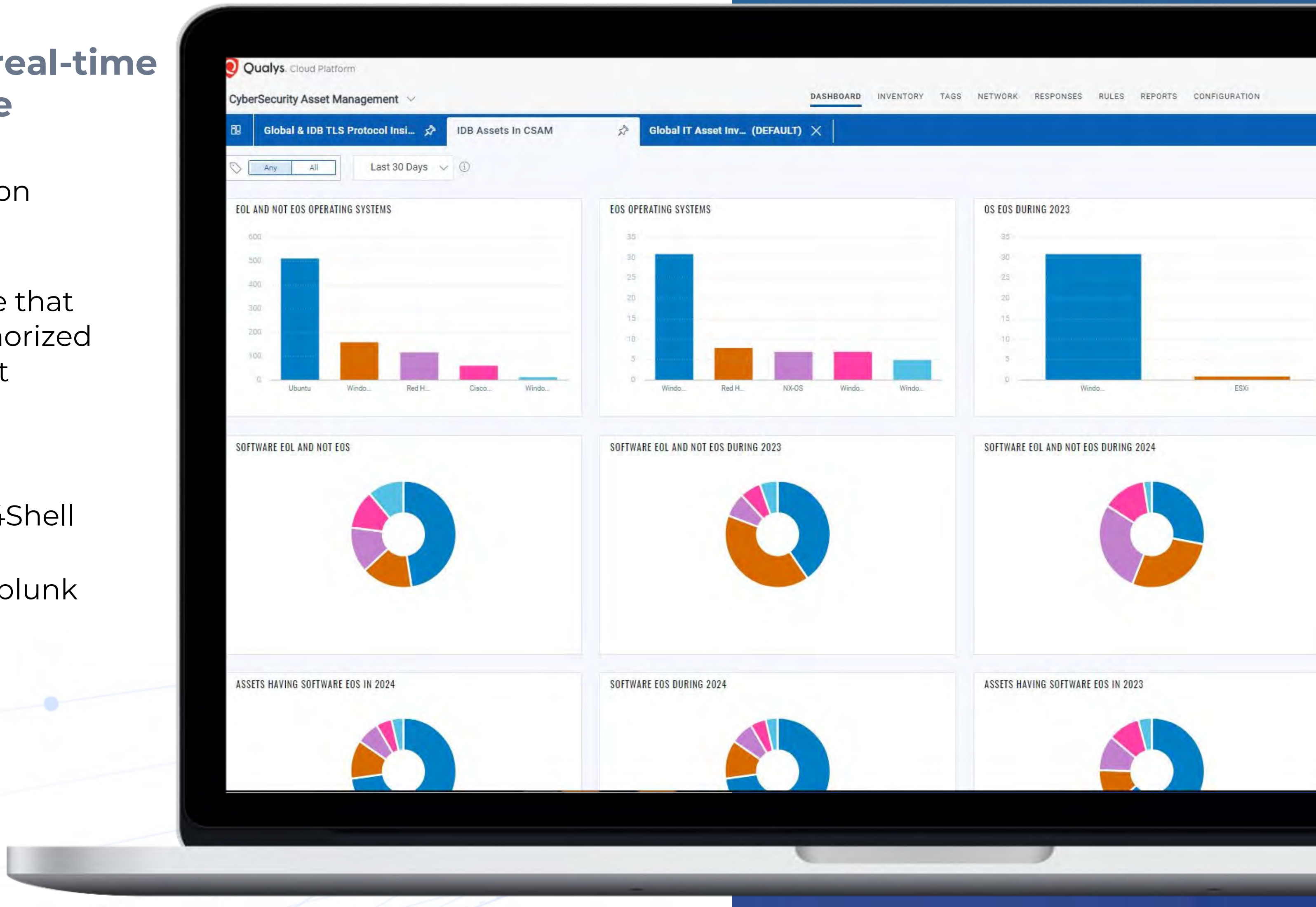
Qualys. IDB BANK®

How We Use CSAM

Continuous Cyber Risk Assessment Across the Hybrid Environment

Proactively reduce tech debt with real-time EoL/EoS and unauthorized software

- ✓ Plan ahead based on defined widgets on EOL/EOS due dates – Java, .NET
- ✓ Automatically identify & notify software that is elevating cybersecurity risk – Unauthorized Software – File sharing (Samba), Packet Inspection (Sniffer), Paranoia
- ✓ Automatically identify new vulnerable applications – such as to Log4j/Spring4Shell
- ✓ Detect missing agents (CrowdStrike, Splunk Collector, etc.)

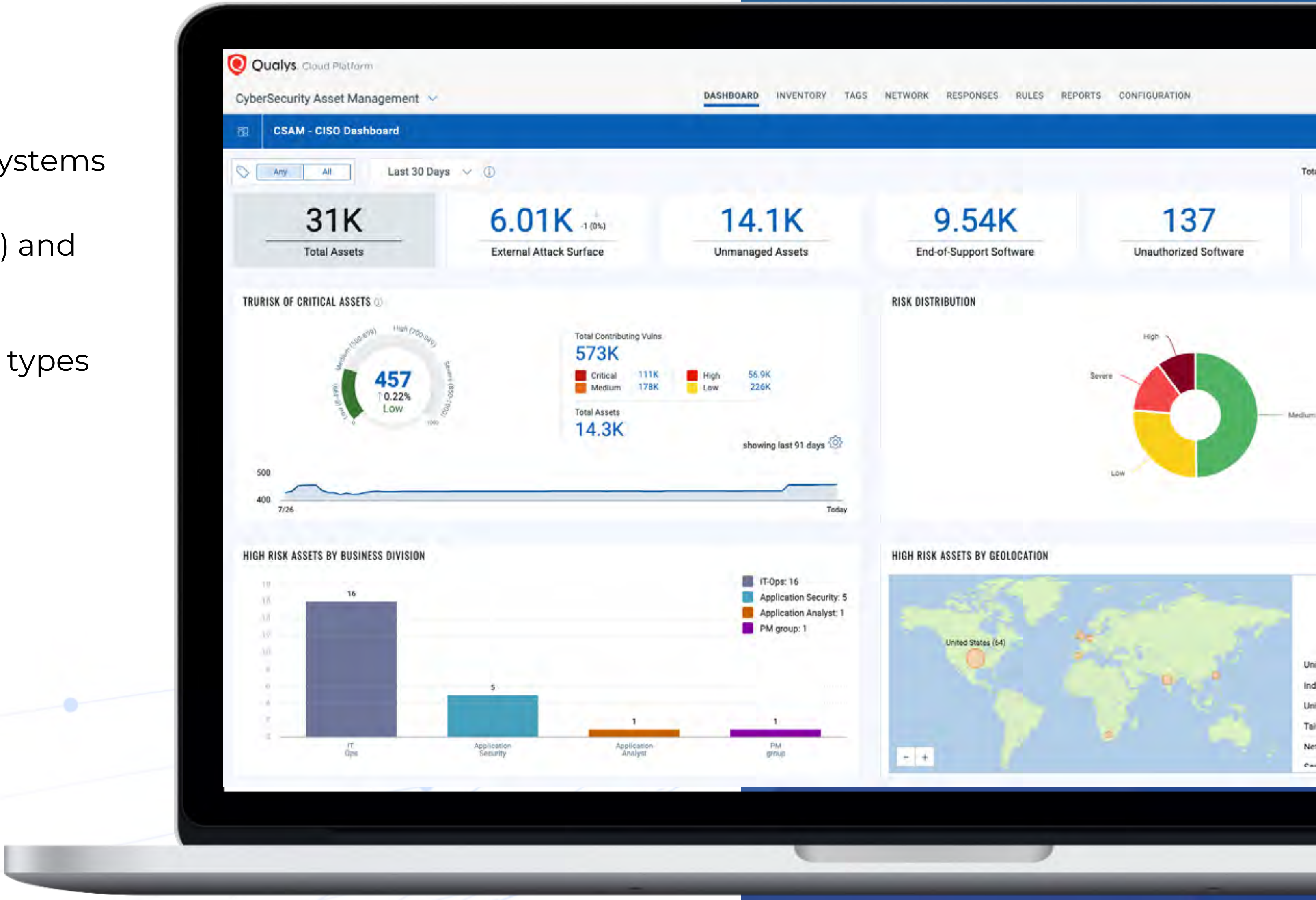


How We Use CSAM

Business Context with Tagging to drive effective prioritization

Business and IT oriented tagging

- ✓ Business, IT and Cybersec critical systems
- ✓ Environments (prod, test, dev, UAT) and locations
- ✓ Operating systems types, software types
- ✓ Functional and performance



Qualys. Cloud Platform

CyberSecurity Asset Management

CSAM - CISO Dashboard

31K	6.01K -1 (0%)	14.1K	9.54K	137
Total Assets	External Attack Surface	Unmanaged Assets	End-of-Support Software	Unauthorized Software

TRURISK OF CRITICAL ASSETS

Total Contributing Vulns
573K

Critical	111K	High	56.9K
Medium	178K	Low	226K

Total Assets
14.3K

showing last 91 days

RISK DISTRIBUTION

HIGH RISK ASSETS BY BUSINESS DIVISION

- IT-Ops: 16
- Application Security: 5
- Application Analyst: 1
- PM group: 1

HIGH RISK ASSETS BY GEOLOCATION

Qualys.

IDB BANK®

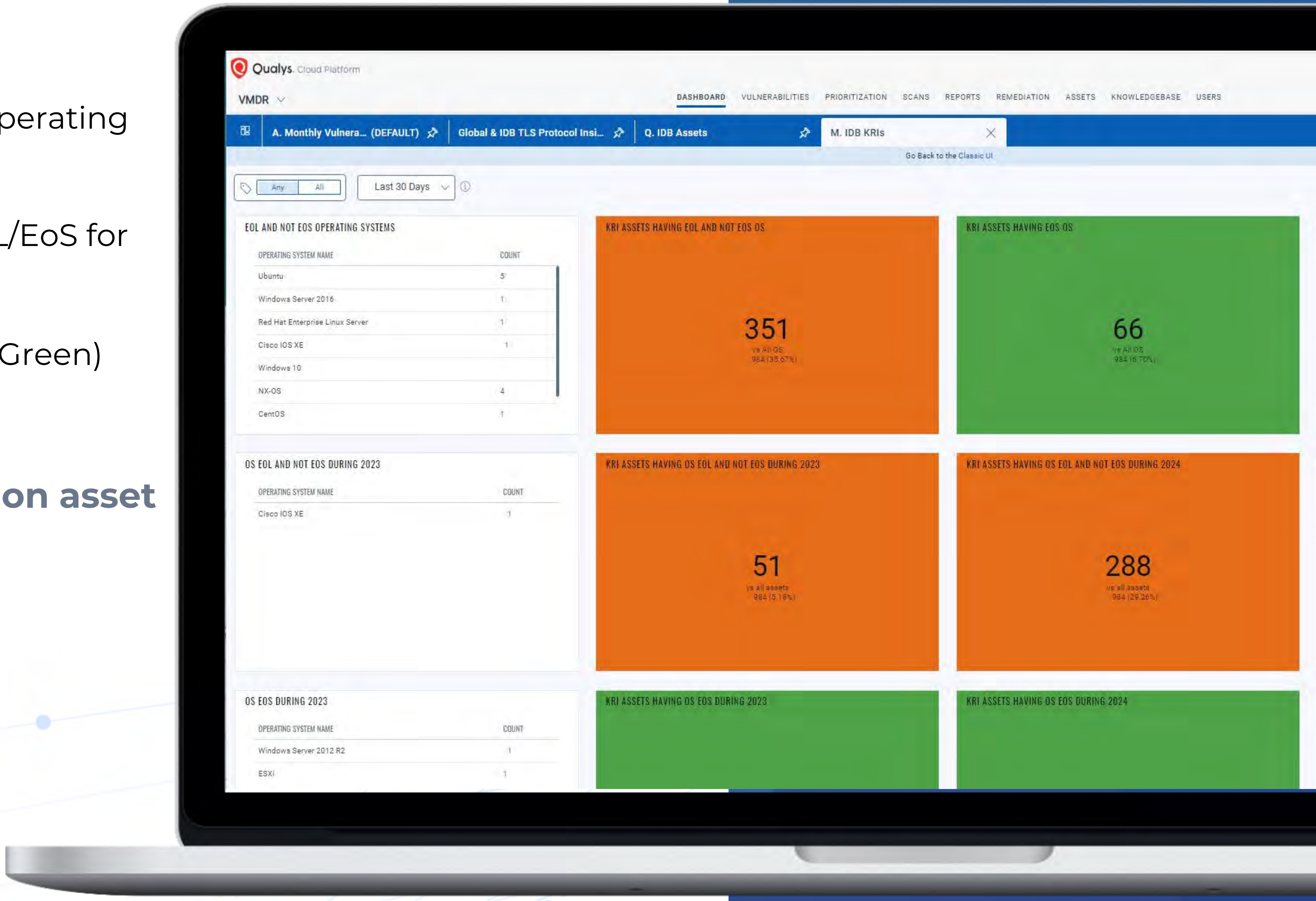
How We Use CSAM

Measure, Communicate and Eliminate the Risk

Monitoring cybersecurity KRIs

- ✓ Number of Assets having EoL/EoS Operating Systems & Software
- ✓ Plan budget for fixing upcoming EoL/EoS for next year
- ✓ Threshold based reporting (Orange, Green) for mitigation planning

Prioritize and remediate risk based on asset criticality and TruRisk ratings



EOL AND NOT EOS OPERATING SYSTEMS

OPERATING SYSTEM NAME	COUNT
Ubuntu	5
Windows Server 2016	1
Red Hat Enterprise Linux Server	1
Cisco IOS XE	1
Windows 10	
NX-OS	4
CentOS	1

KRI ASSETS HAVING EOL AND NOT EOS OS

351
vs All OS
984 (35.67%)

KRI ASSETS HAVING EOS OS

66
vs All OS
984 (6.70%)

OS EOL AND NOT EOS DURING 2023

OPERATING SYSTEM NAME	COUNT
Cisco IOS XE	1

KRI ASSETS HAVING OS EOL AND NOT EOS DURING 2023

51
vs all assets
984 (5.18%)

KRI ASSETS HAVING OS EOL AND NOT EOS DURING 2024

288
vs all assets
984 (29.26%)

OS EOS DURING 2023

OPERATING SYSTEM NAME	COUNT
Windows Server 2012 R2	1
ESXi	1

KRI ASSETS HAVING OS EOS DURING 2023

KRI ASSETS HAVING OS EOS DURING 2024

Qualys. IDBBANK®

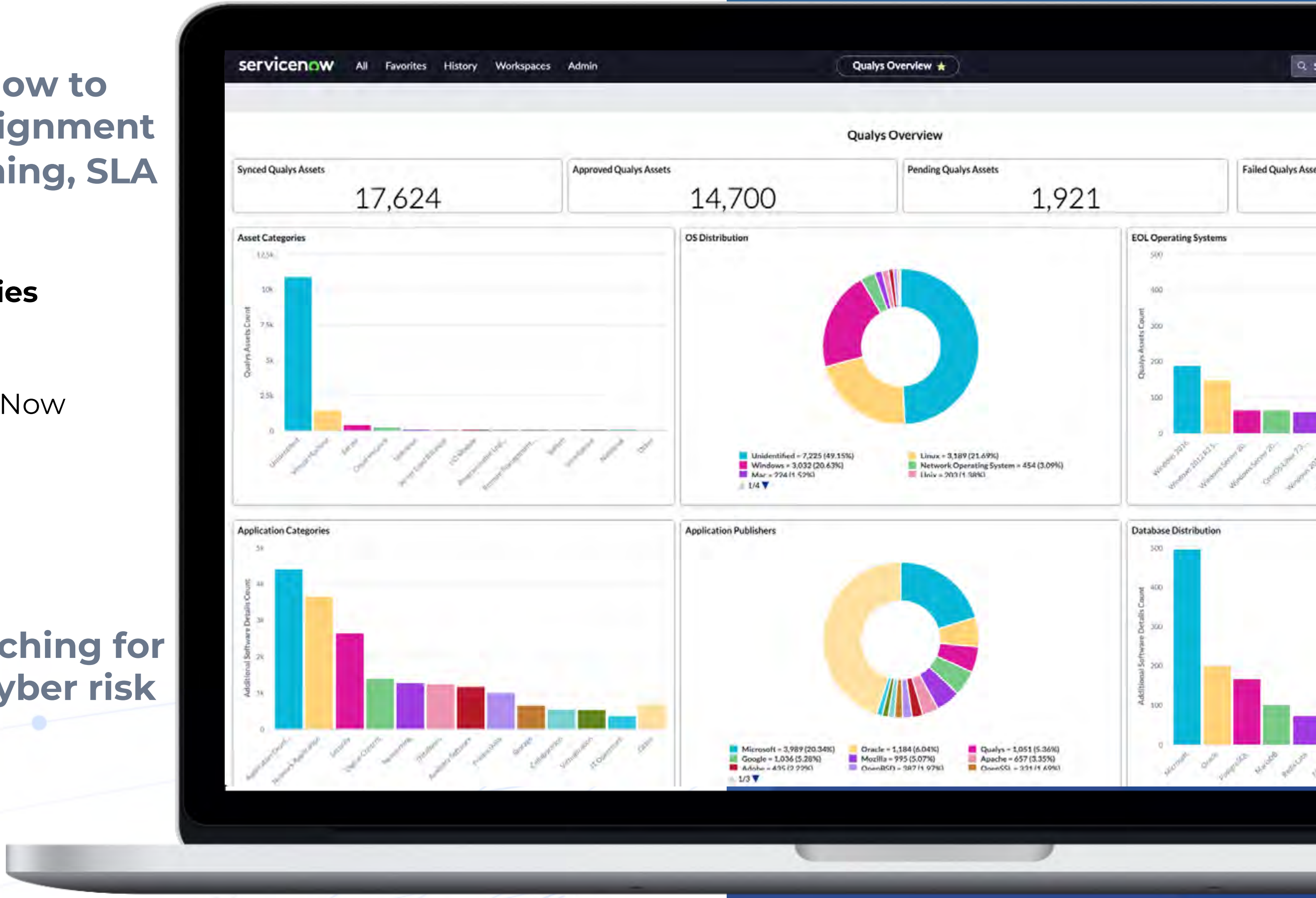
How We Use CSAM

Turbocharge CMDB with Assets and Cyber Risk Context and Reduce MTTR

Leveraging CMDB sync for ServiceNow to operationalize role-based ticket assignment (owner, department), monitor patching, SLA and more

- ✓ Daily, automatic **asset and vulnerabilities** export to ServiceNow
- ✓ **Automatic assignment** rules in ServiceNow based on Qualys tags
- ✓ **SLA defined** and follow up procedures according to Qualys tags

Accelerate the remediation and patching for IT team with enriched CMDB with cyber risk context



Qualys Overview

Synced Qualys Assets 17,624

Approved Qualys Assets 14,700

Pending Qualys Assets 1,921

Failed Qualys Asse

Qualys. IDBBANK®

Qualys CSAM Outcomes for IDBNY

Measure, Communicate and Eliminate the Risk

MTTD: more than 200% faster
Security team resource time savings with automated asset discovery and management.

Instantly comply to meet SLA expectations and compliance requirements for inventory, EoL/EoS, unauthorized software, and more.

Proactively plan for end-of-support operating systems and software **3-12 months in advance**, reducing exposure significantly.

Close tickets faster with automated ticket assignment with **up to 95% accuracy.**

Qualys. IDB BANK®

What’s Next?

Expand Attack Surface Management Journey with Qualys

Augment the vulnerability management program with insights from an **external attacker’s point of view**

Internal Attack Surface with Cloud Agent Passive Sensor - Identify rogue devices (even in IoT environment) without a massive investment in sensors and new systems

Bring in missing Assets from non-Qualys environment with **Active Directory** Connector

Monitor and Reduce Attack Surface Risk

IDB BANK®

Demo

Challenges IT-Centric Inventory with Disjoint View

IT Team

Laborious, time-consuming task to create & maintain spreadsheets/CMDB

Asset inventory is typically **updated manually** or through infrequent uploads

Lack of visibility into the ephemeral external internet-facing assets

Lack of visibility into all environments (e.g., PCI, OT) **creates blind-spots**

Cyber Security Team

Manual effort in mapping vulnerabilities to asset records, creating, assigning tickets, and tracking progress.

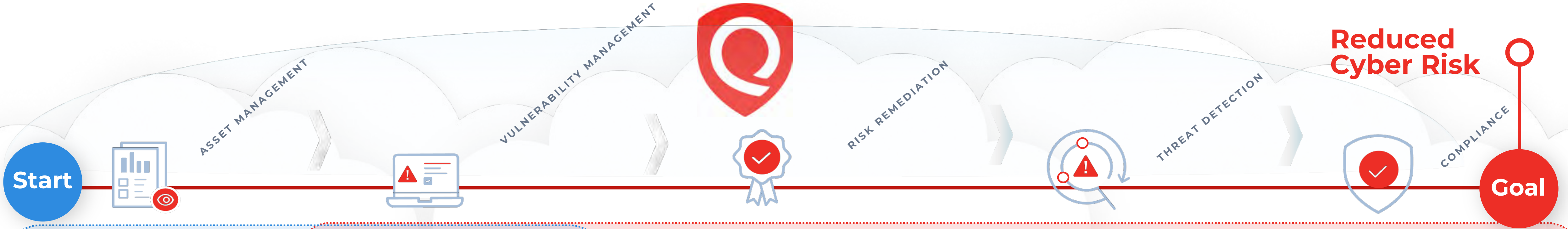
Time-consuming task to find & correlate asset context with Incident investigation & triage

Lack of correlated asset, vulnerabilities, **applications and business context**, creates gaps in risk-based prioritization program.

Inaccurate CMDB and ITSM with severely impacted MTTR

Landing & Expanding with Qualys

Manage Risk to your organization, no matter where it is.



See Everything with Business Context

CSAM

- **EASM**
- **CMDB Sync**

Risk-Based Vulnerability Management (RBVM)

VMDR with TruRisk

WAS

TotalCloud CWPP with...

- Container Security (CS)
- Infrastructure as Code (IaC)

Integrated Remediation & Patch Mgmt.

Patch Management

Custom Remediation and Assessment (CAR)

Extended Detection and Response

Endpoint Security (EDR/XDR)

TotalCloud CWPP with...

- Cloud Detection and Response

PCI 4.0 and Beyond

Policy Management (PM

Security Assessment Questionnaire (SAQ)

File Integrity Management (FIM)

TotalCloud CWPP with...

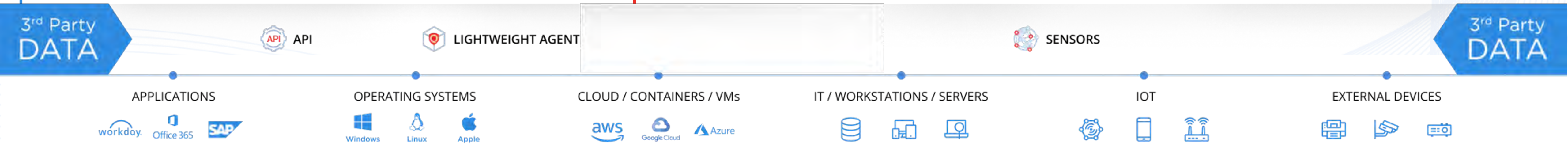
- Cloud Security Posture Management (CSPM)

Unifying Asset and Attack Surface Management

- Extend Risk-Based Vulnerability Management **across all assets using one dashboard with VMDR + CSAM.**

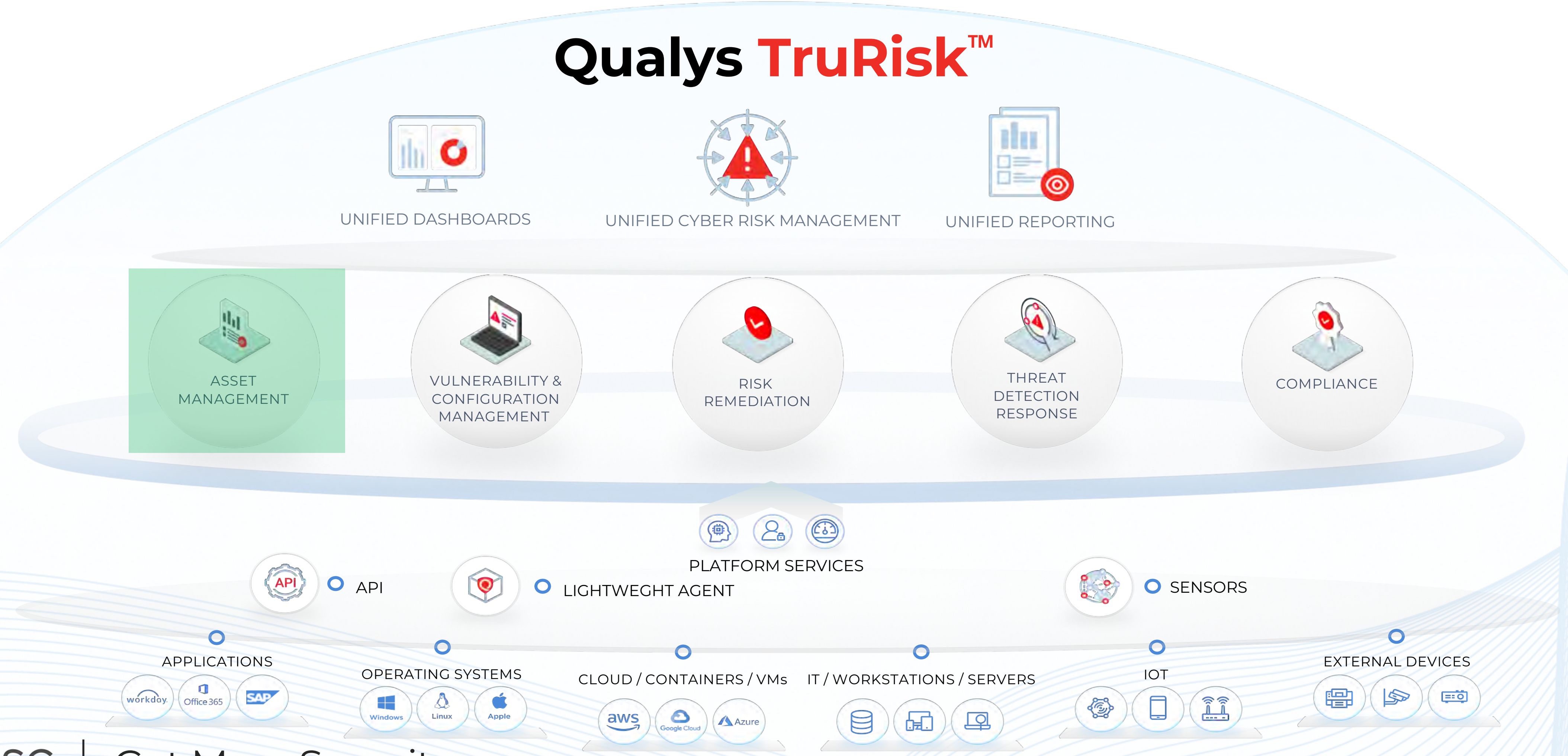
Operationalizing and Consolidating Cybersecurity Stack with VM

- **Reduce MTTR and improve IT-Security workflows** with extended anti-malware/ransomware, ITSM, and CMDB integrations, as well as PCI compliance.



The Qualys Enterprise TruRisk Platform

Reducing Cybersecurity Risk Effectively Across the Enterprise



Qualys TruRisk™

UNIFIED DASHBOARDS

UNIFIED CYBER RISK MANAGEMENT

UNIFIED REPORTING

ASSET MANAGEMENT

VULNERABILITY & CONFIGURATION MANAGEMENT

RISK REMEDIATION

THREAT DETECTION RESPONSE

COMPLIANCE

PLATFORM SERVICES

API

LIGHTWEGHT AGENT

SENSORS

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

The Qualys Platform

Qualys Products and the Problems They Solve

Cyber Asset Attack Surface Management (CSAM)

Continuous Integration (CI)

External Attack Surface Management (EASM)

Vulnerability Management, Detection and Response (VMDR)

Container Security (CS)

Cloud Workload Protection Platform (CWPP)

Web App Scanning (WAS)

Infrastructure as Code Security (IaC)

Custom Assessment and Remediation (CAR)

Patch Management (PM)

First-Party Software Risk Management

Cloud Detection and Response (CDR)

Extended Detection and Response (XDR)

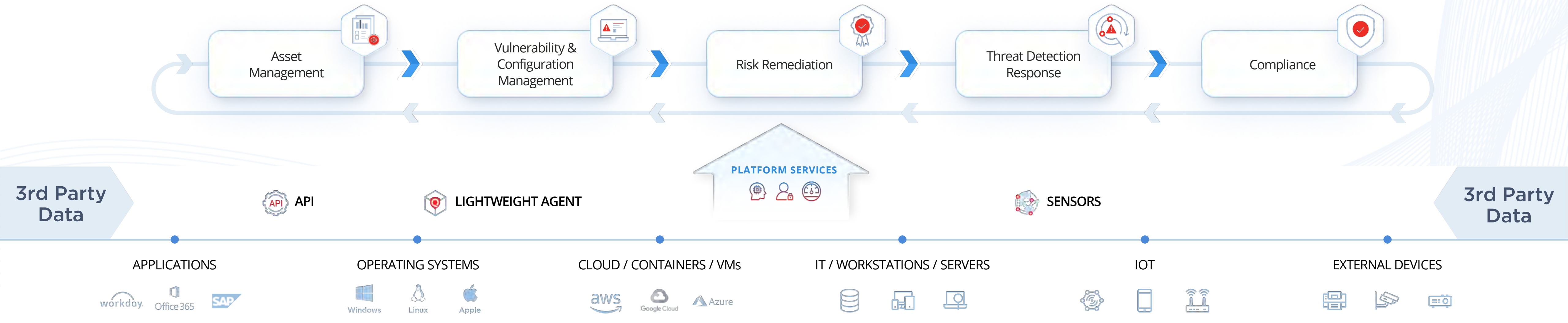
Endpoint Detection and Response (EDR)

Policy Compliance (PC)

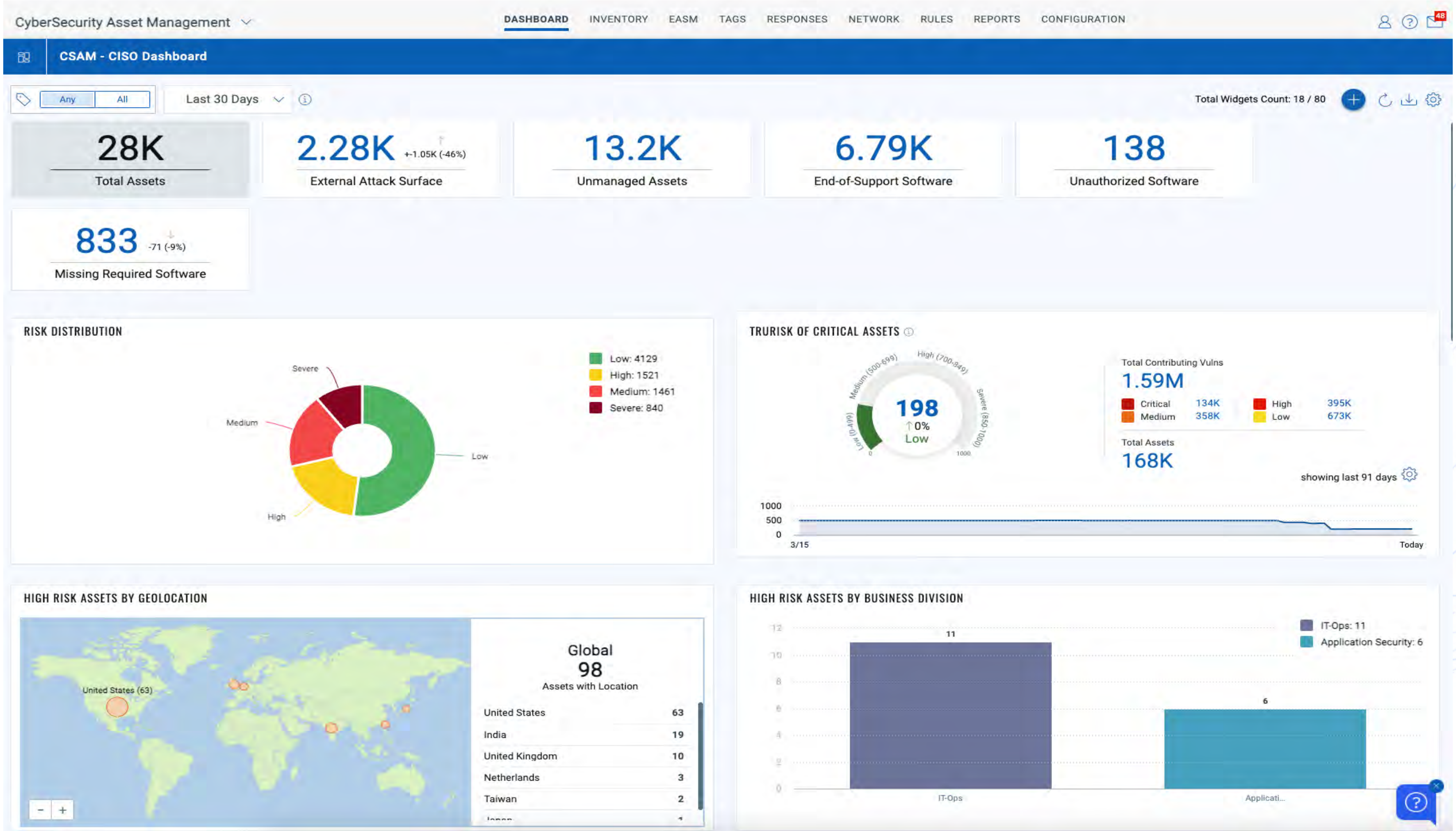
Security Assessment Questionnaire (SAQ)

Cloud Security Posture Management (CSPM)

File Integrity Monitoring (FIM)



Global CISO Dashboard – Inventory Breakdown



28K
Total Assets

2.28K +1.05K (-46%)
External Attack Surface

13.2K
Unmanaged Assets

6.79K
End-of-Support Software

138
Unauthorized Software

833 -71 (-9%)
Missing Required Software

RISK DISTRIBUTION

TRURISK OF CRITICAL ASSETS

Total Contributing Vulns
1.59M

🟥 Critical	134K	🟥 High	395K
🟧 Medium	358K	🟨 Low	673K

Total Assets
168K

showing last 91 days

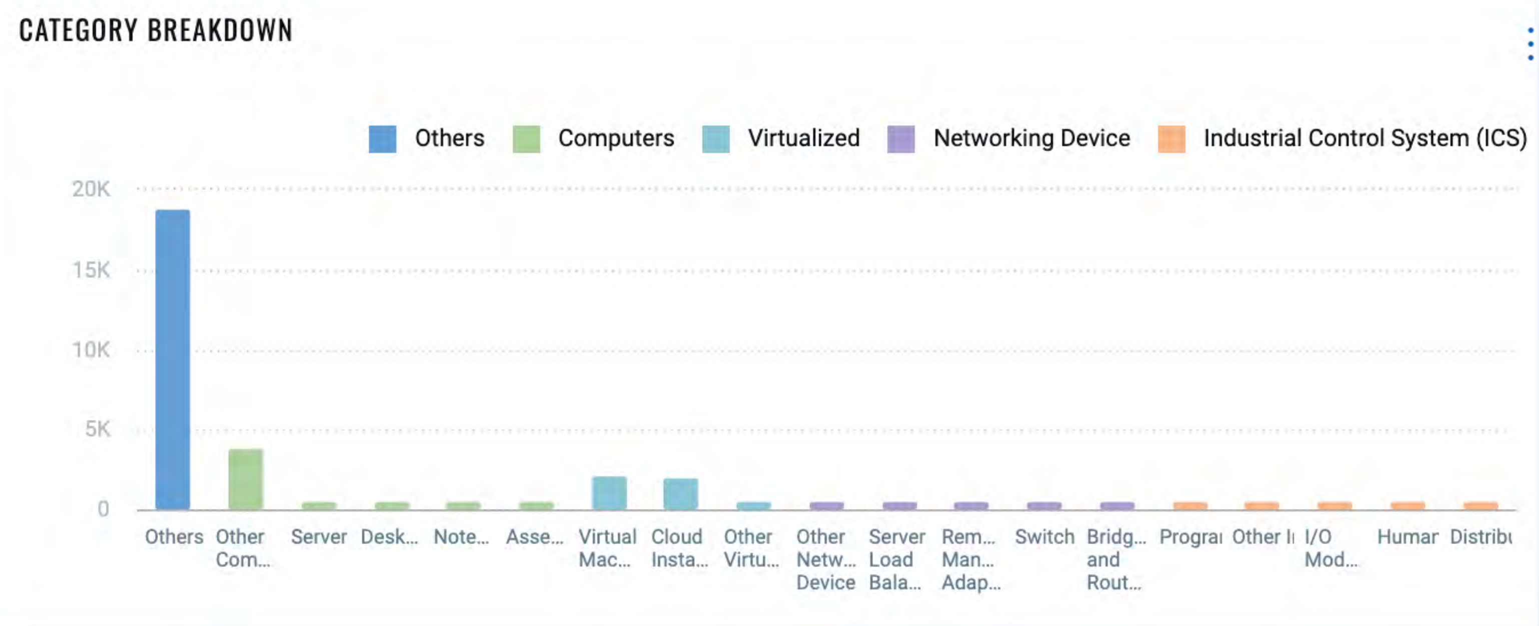
HIGH RISK ASSETS BY GEOLOCATION

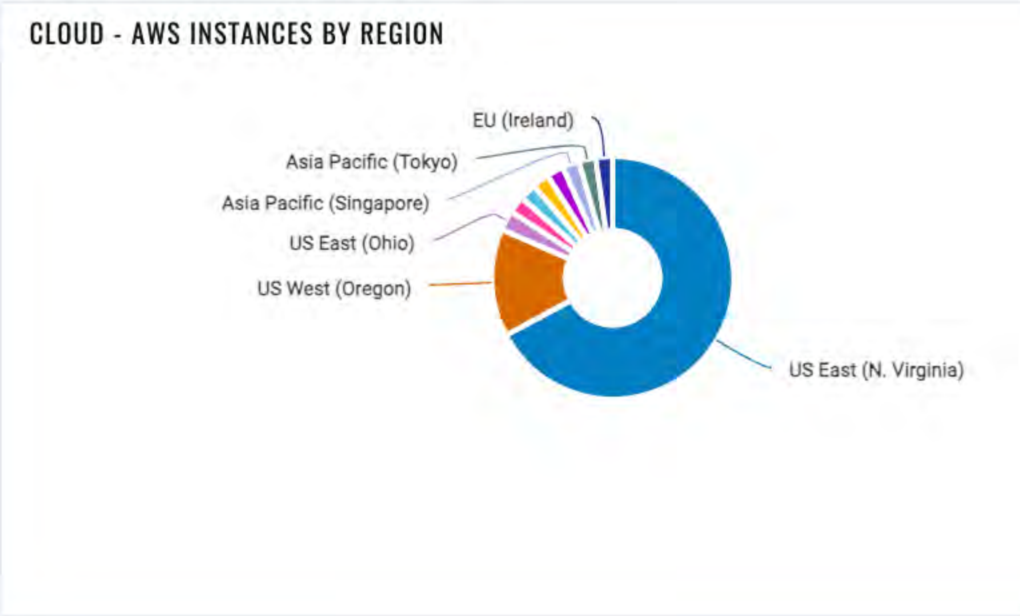
Global
98
Assets with Location

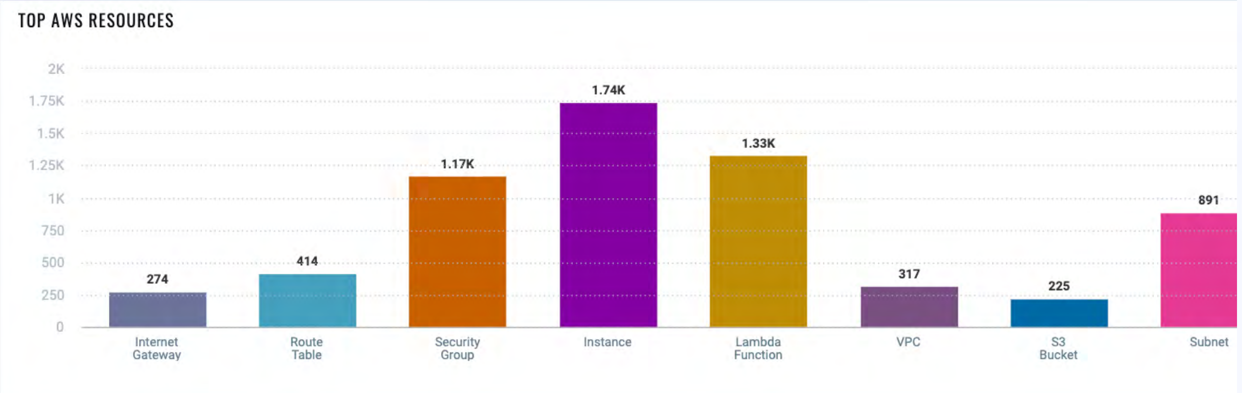
United States	63
India	19
United Kingdom	10
Netherlands	3
Taiwan	2
Japan	1

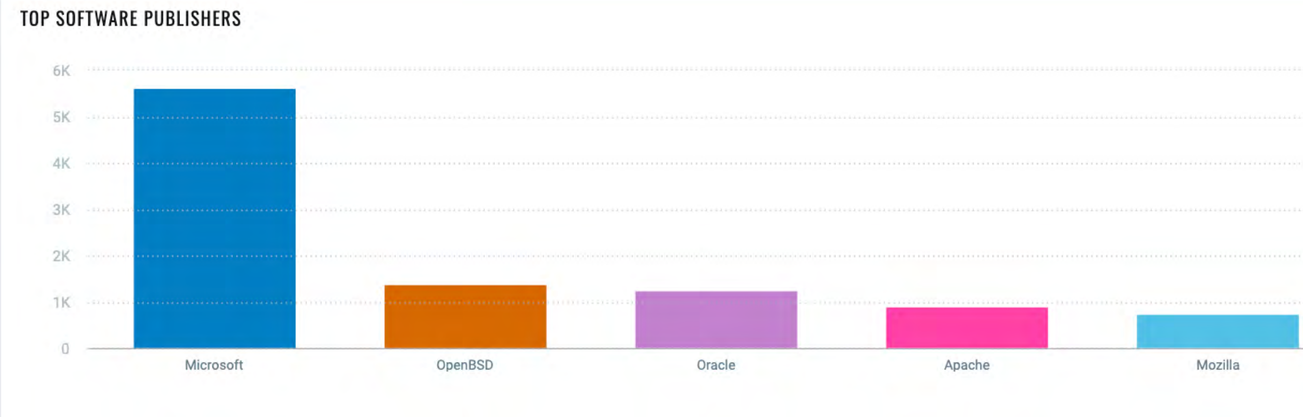
HIGH RISK ASSETS BY BUSINESS DIVISION

Global CISO Dashboard – Inventory Breakdown

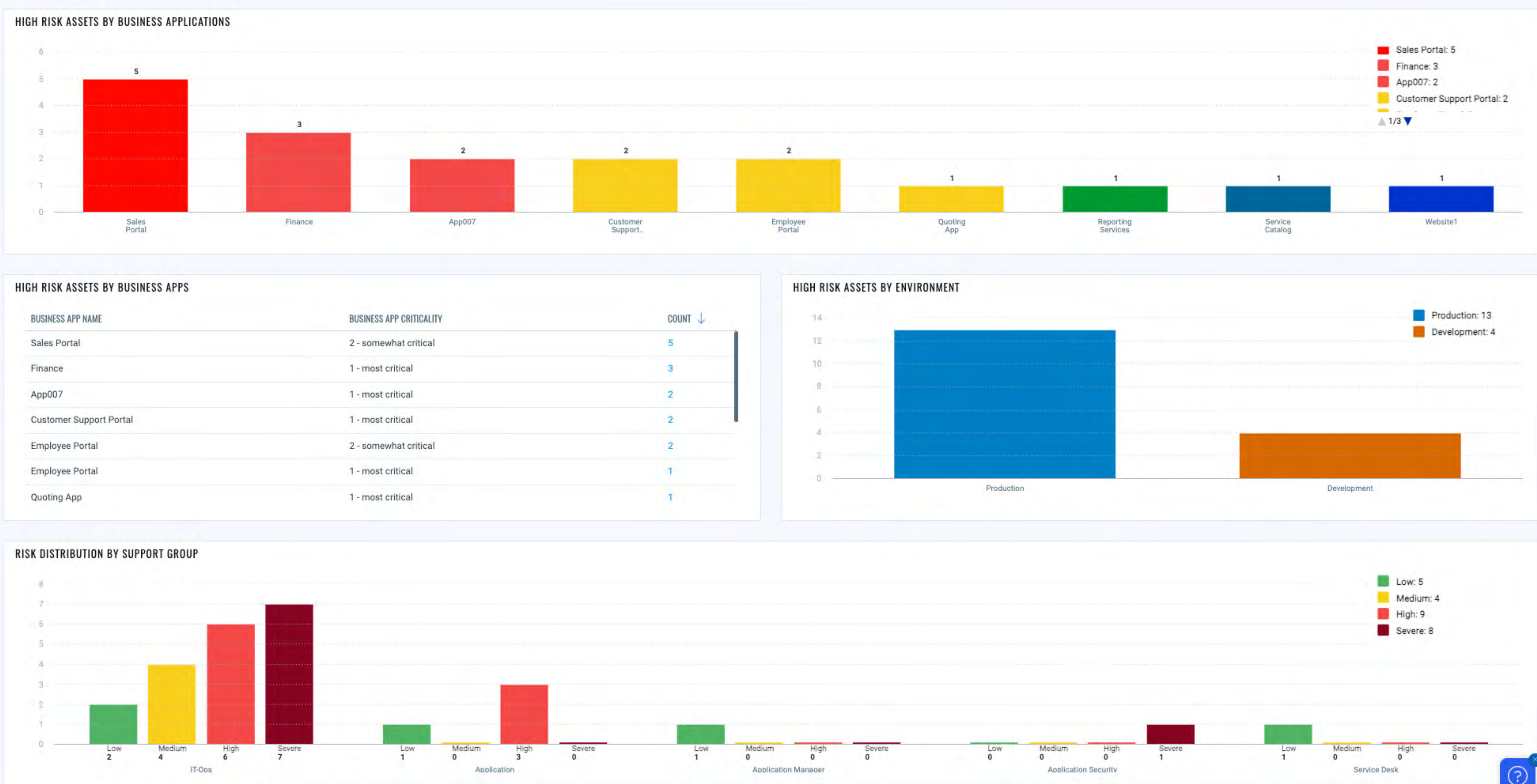








Risk-Based Prioritization View of Attack Surface



HIGH RISK ASSETS BY BUSINESS APPLICATIONS

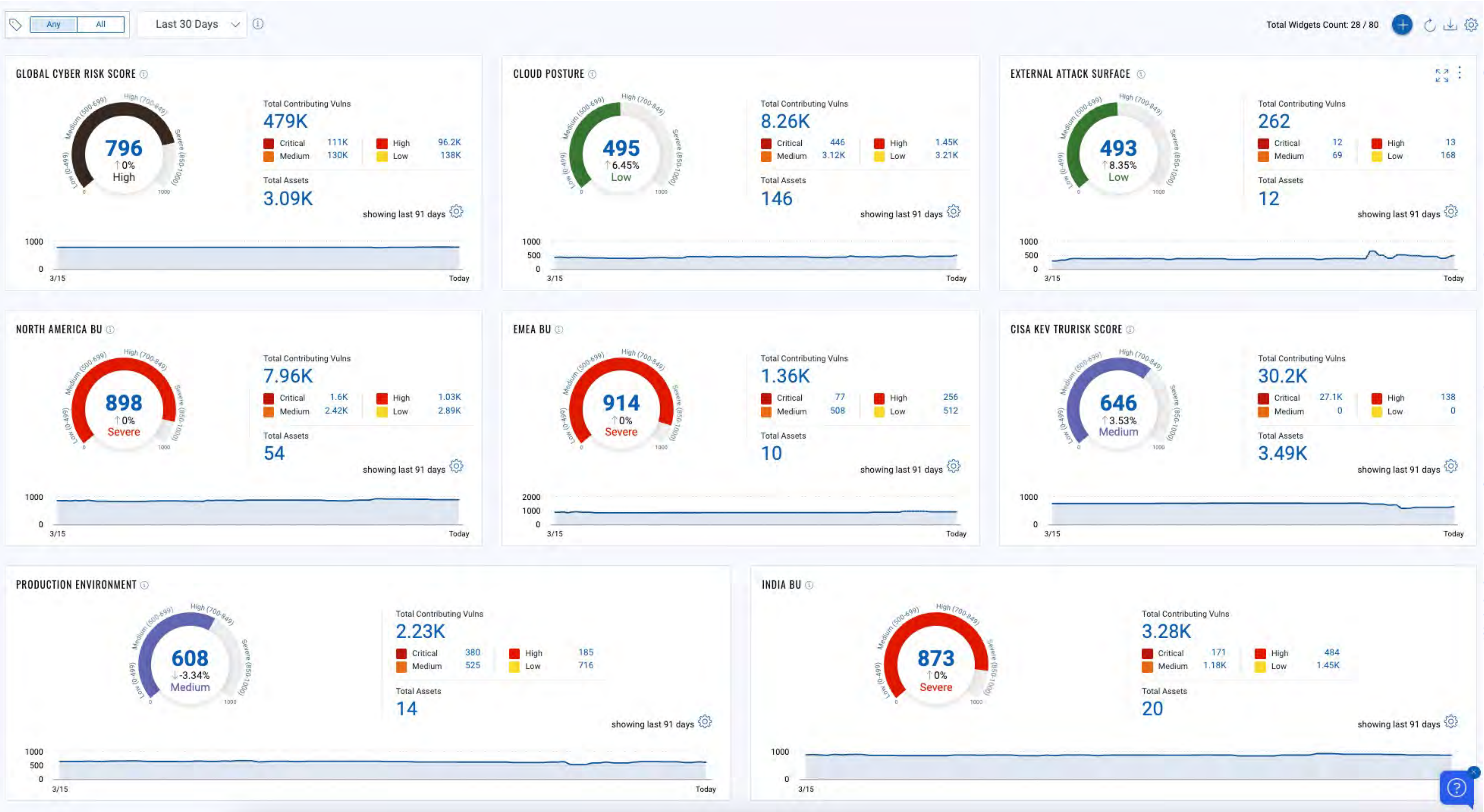
HIGH RISK ASSETS BY BUSINESS APPS

BUSINESS APP NAME	BUSINESS APP CRITICALITY	COUNT ↓
Sales Portal	2 - somewhat critical	5
Finance	1 - most critical	3
App007	1 - most critical	2
Customer Support Portal	1 - most critical	2
Employee Portal	2 - somewhat critical	2
Employee Portal	1 - most critical	1
Quoting App	1 - most critical	1

HIGH RISK ASSETS BY ENVIRONMENT

RISK DISTRIBUTION BY SUPPORT GROUP

Risk-Based Prioritization View of Attack Surface



Any | All

Last 30 Days

Total Widgets Count: 28 / 80

GLOBAL CYBER RISK SCORE

796 ↑0% High

Total Contributing Vulns 479K

🟥 Critical	111K	🟥 High	96.2K
🟧 Medium	130K	🟨 Low	138K

Total Assets 3.09K

showing last 91 days

CLOUD POSTURE

495 ↑6.45% Low

Total Contributing Vulns 8.26K

🟥 Critical	446	🟥 High	1.45K
🟧 Medium	3.12K	🟨 Low	3.21K

Total Assets 146

showing last 91 days

EXTERNAL ATTACK SURFACE

493 ↑8.35% Low

Total Contributing Vulns 262

🟥 Critical	12	🟥 High	13
🟧 Medium	69	🟨 Low	168

Total Assets 12

showing last 91 days

NORTH AMERICA BU

898 ↑0% Severe

Total Contributing Vulns 7.96K

🟥 Critical	1.6K	🟥 High	1.03K
🟧 Medium	2.42K	🟨 Low	2.89K

Total Assets 54

showing last 91 days

EMEA BU

914 ↑0% Severe

Total Contributing Vulns 1.36K

🟥 Critical	77	🟥 High	256
🟧 Medium	508	🟨 Low	512

Total Assets 10

showing last 91 days

CISA KEV TRURISK SCORE

646 ↑3.53% Medium

Total Contributing Vulns 30.2K

🟥 Critical	27.1K	🟥 High	138
🟧 Medium	0	🟨 Low	0

Total Assets 3.49K

showing last 91 days

PRODUCTION ENVIRONMENT

608 ↓-3.34% Medium

Total Contributing Vulns 2.23K

🟥 Critical	380	🟥 High	185
🟧 Medium	525	🟨 Low	716

Total Assets 14

showing last 91 days

INDIA BU

873 ↑0% Severe

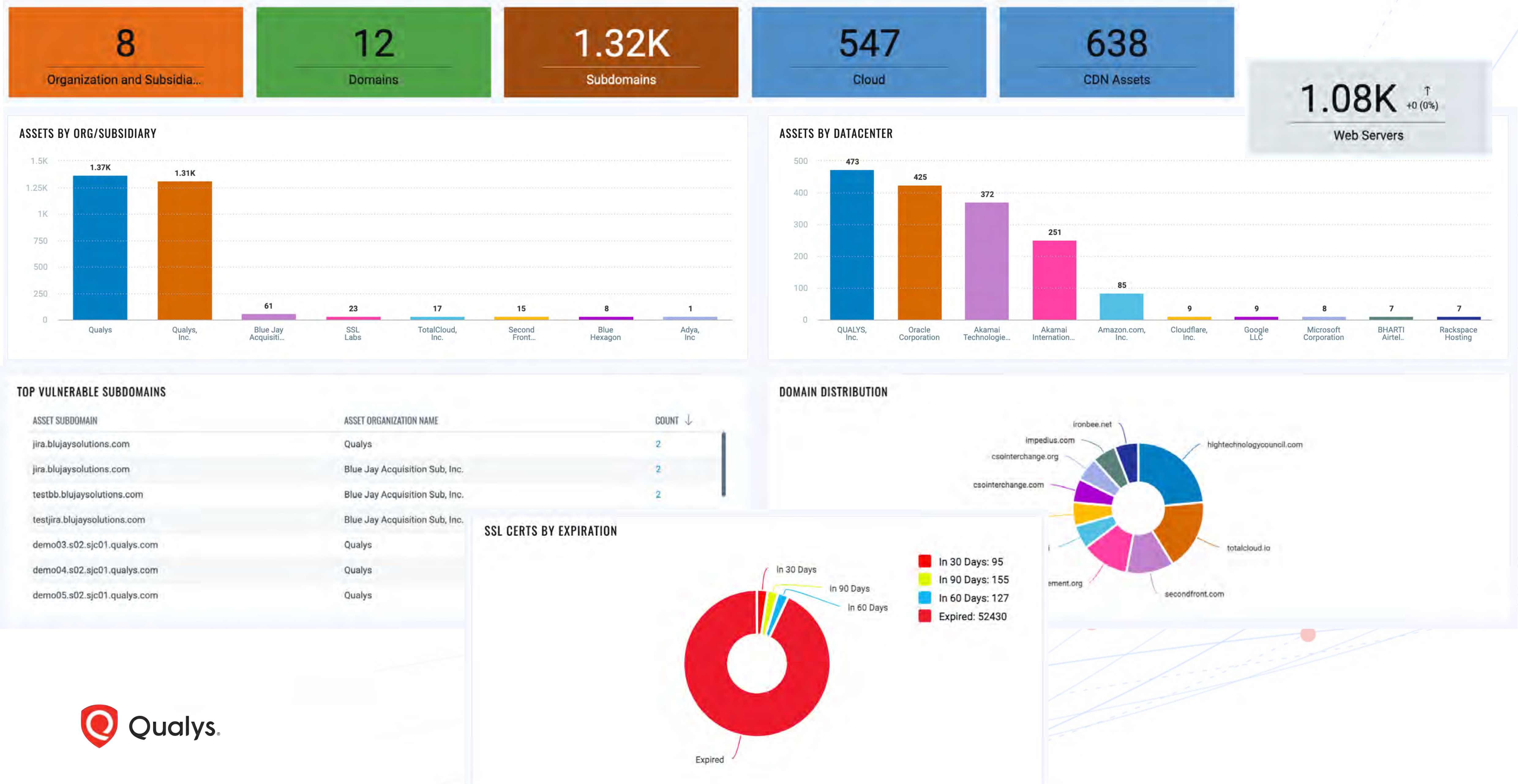
Total Contributing Vulns 3.28K

🟥 Critical	171	🟥 High	484
🟧 Medium	1.18K	🟨 Low	1.45K

Total Assets 20

showing last 91 days

Insights from the EASM



8 Organization and Subsidia...

12 Domains

1.32K Subdomains

547 Cloud

638 CDN Assets

1.08K ↑ +0 (0%) Web Servers

ASSETS BY ORG/SUBSIDIARY

ASSETS BY DATACENTER

TOP VULNERABLE SUBDOMAINS

ASSET SUBDOMAIN	ASSET ORGANIZATION NAME	COUNT ↓
jira.blujaysolutions.com	Qualys	2
jira.blujaysolutions.com	Blue Jay Acquisition Sub, Inc.	2
testbb.blujaysolutions.com	Blue Jay Acquisition Sub, Inc.	2
testjira.blujaysolutions.com	Blue Jay Acquisition Sub, Inc.	
demo03.s02.sjc01.qualys.com	Qualys	
demo04.s02.sjc01.qualys.com	Qualys	
demo05.s02.sjc01.qualys.com	Qualys	

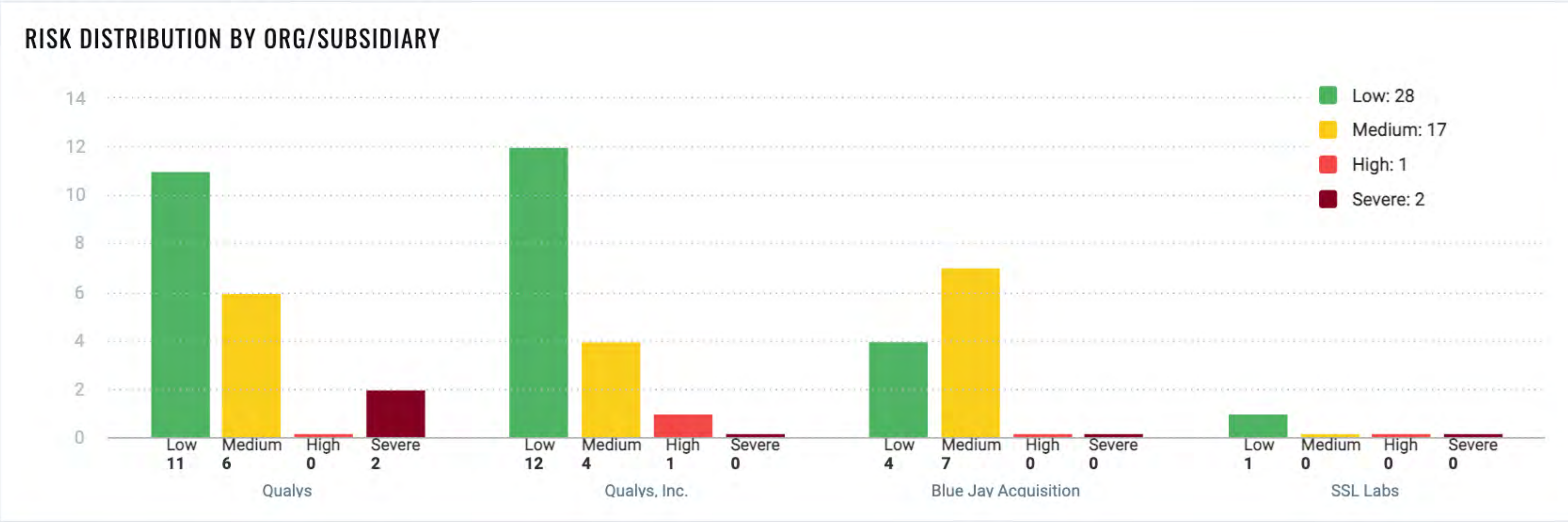
DOMAIN DISTRIBUTION

SSL CERTS BY EXPIRATION

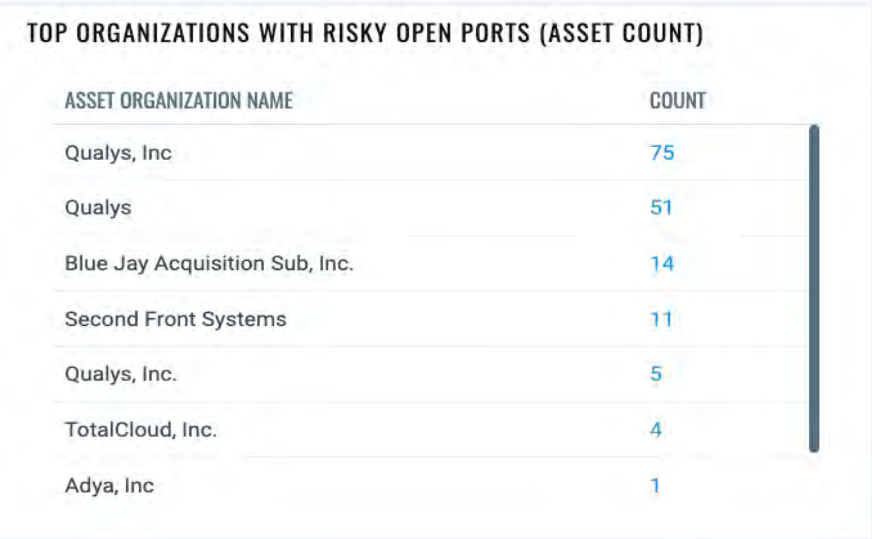
🟥 In 30 Days: 95
🟨 In 90 Days: 155
🟦 In 60 Days: 127
🟥 Expired: 52430

Qualys.

Insights from the EASM - Risk Distribution

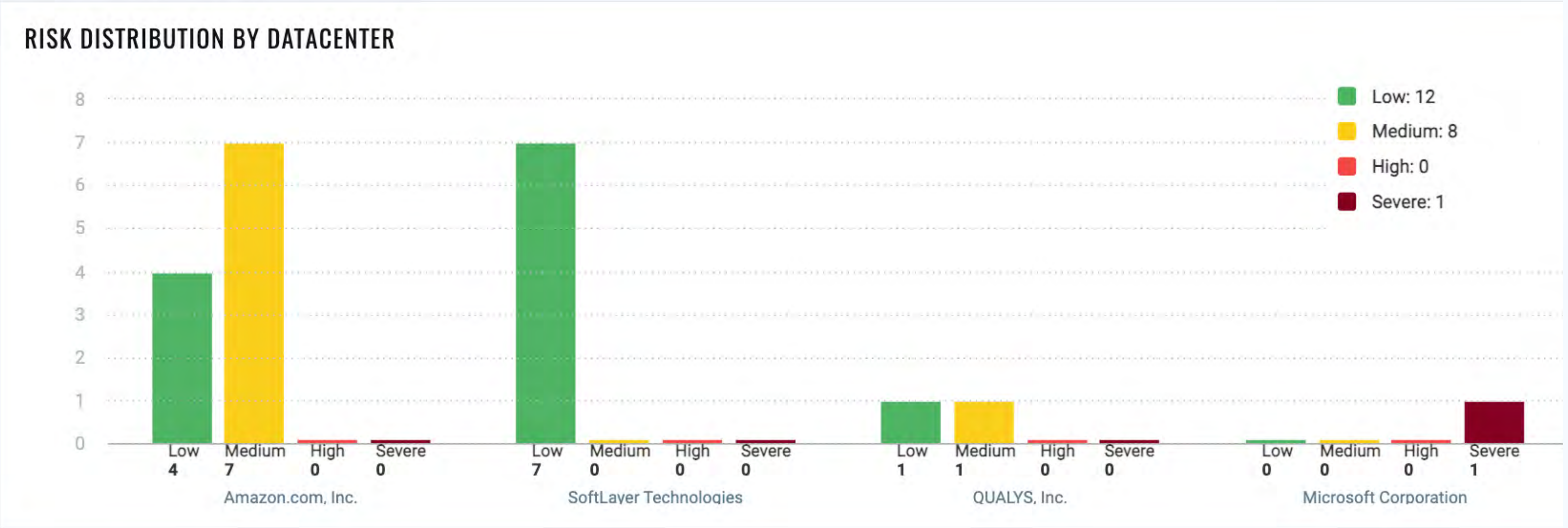


RISK DISTRIBUTION BY ORG/SUBSIDIARY

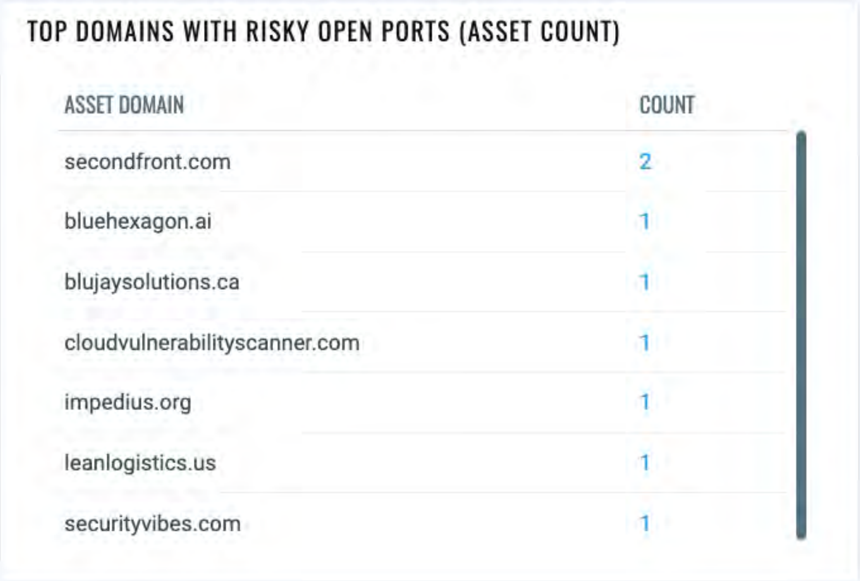


TOP ORGANIZATIONS WITH RISKY OPEN PORTS (ASSET COUNT)

ASSET ORGANIZATION NAME	COUNT
Qualys, Inc	75
Qualys	51
Blue Jay Acquisition Sub, Inc.	14
Second Front Systems	11
Qualys, Inc.	5
TotalCloud, Inc.	4
Adya, Inc	1



RISK DISTRIBUTION BY DATACENTER



TOP DOMAINS WITH RISKY OPEN PORTS (ASSET COUNT)

ASSET DOMAIN	COUNT
secondfront.com	2
bluehexagon.ai	1
blujaysolutions.ca	1
cloudvulnerabilityscanner.com	1
impedius.org	1
leanlogistics.us	1
securityvibes.com	1

QSC23