Unified Attack Surface Management with an Attackers' and Defenders' View

Kunal Modasiya

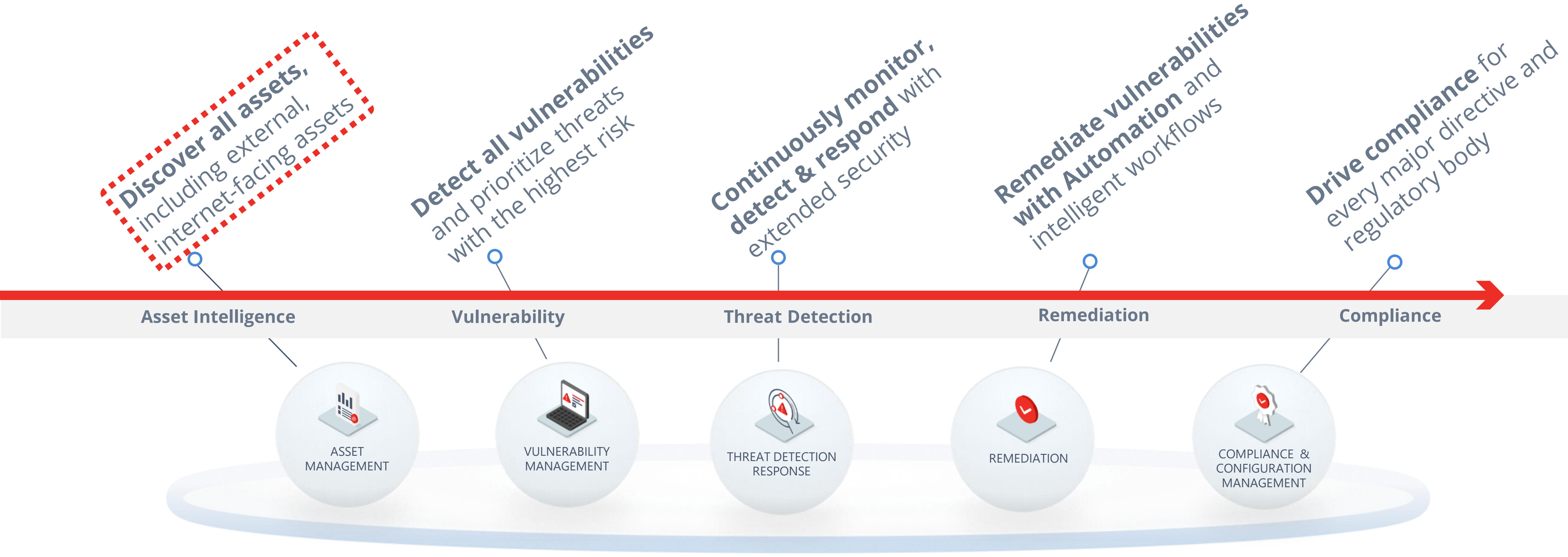
VP of Product Management

Attack Surface Management & AppSec

Qualys Security Conference

A Risk-based Approach to Cybersecurity

All Security Journey Begin with Asset Discovery & Intelligence



Discover all assets, including external, internet-facing assets

Detect all vulnerabilities and prioritize threats with the highest risk

Continuously monitor, detect & respond with extended security

Remediate vulnerabilities with Automation and intelligent workflows

Drive compliance for every major directive and regulatory body

CyberSecurity Asset Management (CSAM)

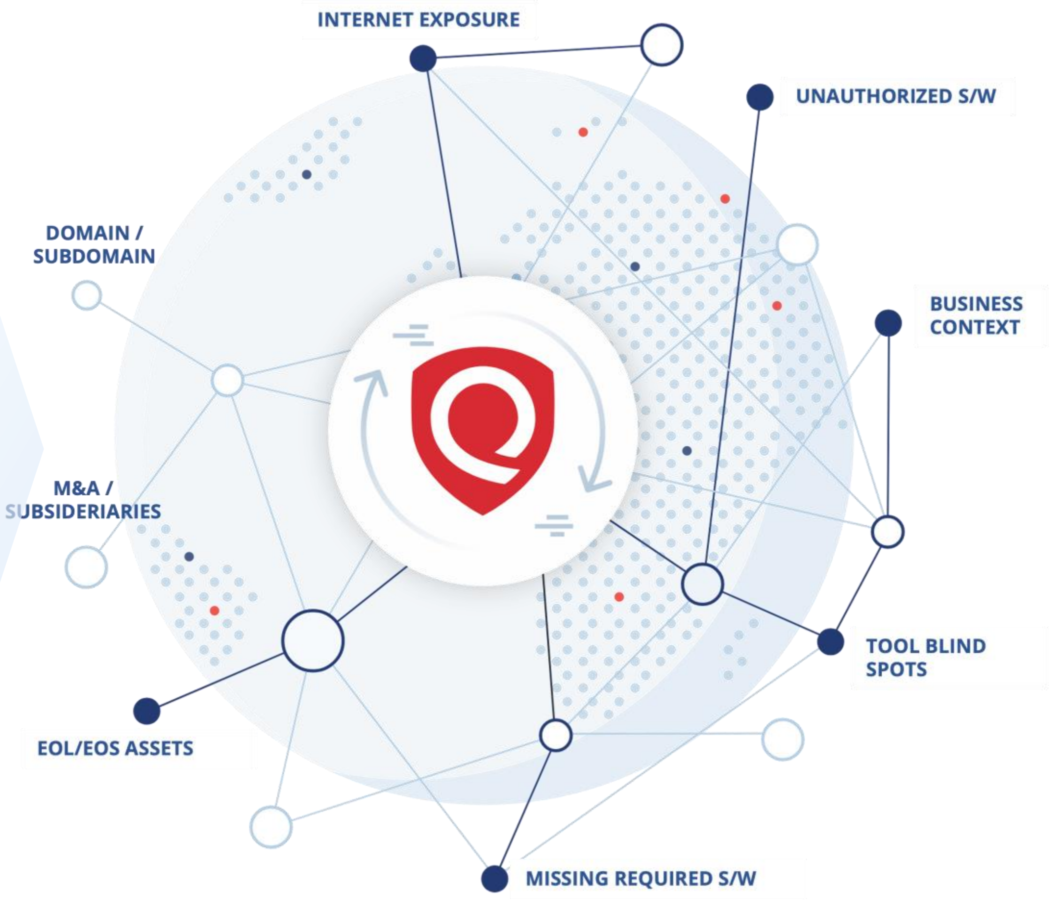
Internal + External View = Entire Attack Surface

1 Unified Inventory with Cyber Risk & Business Context

- ✓ Simplify and improve **vulnerability management**, **AppSec** and **Patch management** programs

2 External Attack Surface Management

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



Qualys.

CyberSecurity Asset Management - CSAM

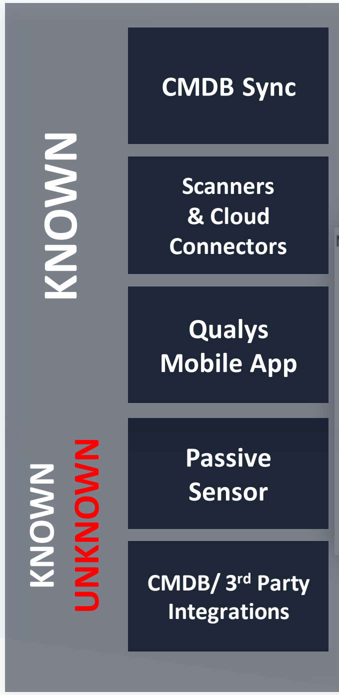
Defenders’ View – Inside-out perspective

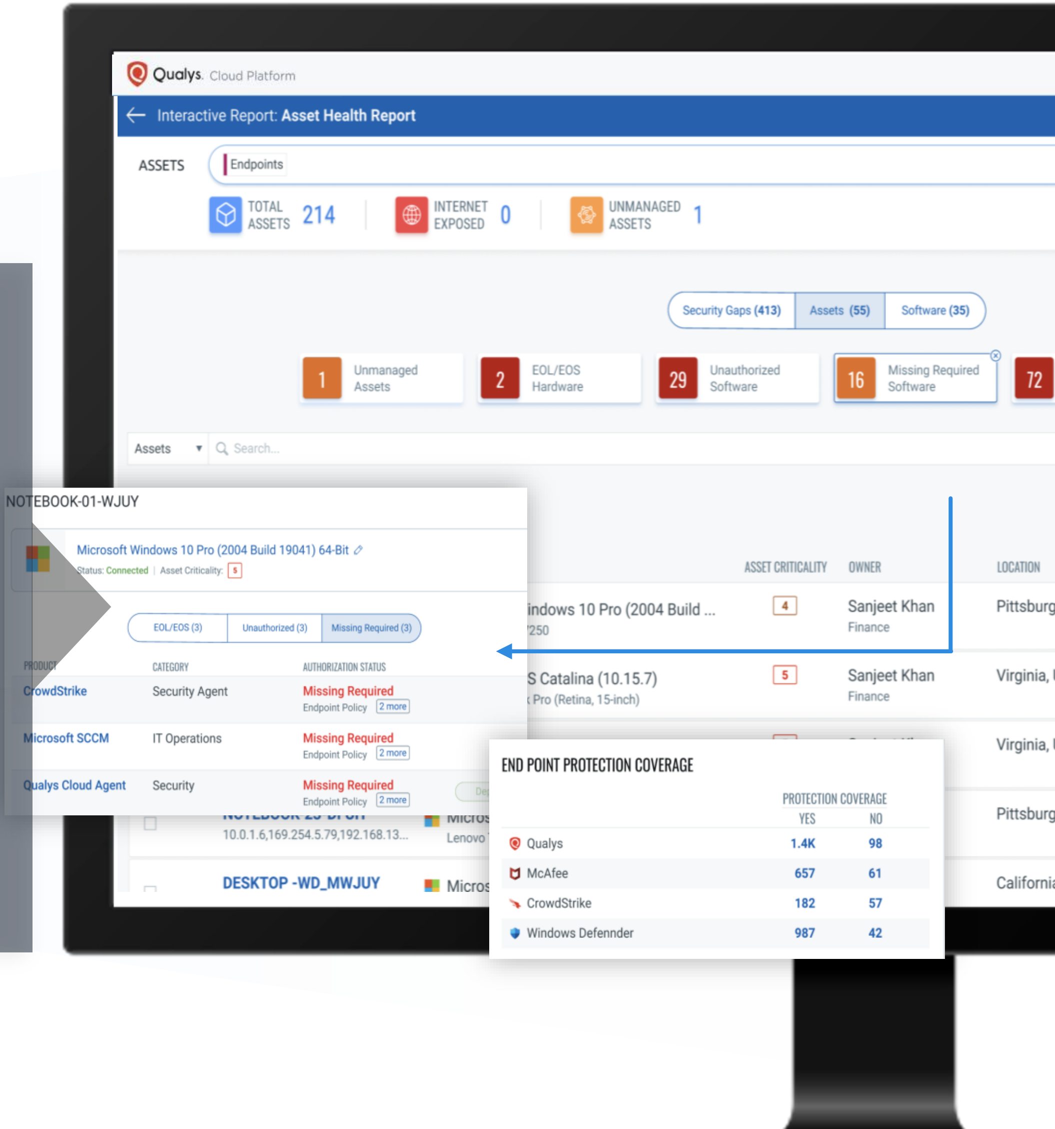
1. Asset discovery & **inventory w/ business context**

2. **Third-party integrations** for asset aggregation and intelligence

3. **Expose security** gaps & monitor asset health
   - Manage EoL/EoS
   - Find Agent Coverage
   - Unauthorized Software

4. **Risk-based prioritization** and remediation workflows **with Qualys TruRisk**





TOTAL ASSETS 214 | INTERNET EXPOSED 0 | UNMANAGED ASSETS 1

Security Gaps (413) | Assets (55) | Software (35)

1 Unmanaged Assets | 2 EOL/EOS Hardware | 29 Unauthorized Software | 16 Missing Required Software | 72

NOTEBOOK-01-WJUY

Microsoft Windows 10 Pro (2004 Build 19041) 64-Bit

Status: Connected | Asset Criticality: 5

EOL/EOS (3) | Unauthorized (3) | Missing Required (3)

PRODUCT	CATEGORY	AUTHORIZATION STATUS
CrowdStrike	Security Agent	Missing Required Endpoint Policy 2 more
Microsoft SCCM	IT Operations	Missing Required Endpoint Policy 2 more
Qualys Cloud Agent	Security	Missing Required Endpoint Policy 2 more

	ASSET CRITICALITY	OWNER	LOCATION
indows 10 Pro (2004 Build ... '250	4	Sanjeet Khan Finance	Pittsburg
S Catalina (10.15.7) Pro (Retina, 15-inch)	5	Sanjeet Khan Finance	Virginia,
			Virginia,
NOTEBOOK-23-DFUH 10.0.1.6,169.254.5.79,192.168.13... Micros Lenovo			Pittsburg
DESKTOP -WD_MWJUY Micros			California

END POINT PROTECTION COVERAGE

	PROTECTION COVERAGE	
	YES	NO
Qualys	1.4K	98
McAfee	657	61
CrowdStrike	182	57
Windows Defennder	987	42

External Attack Surface Management (EASM)

Attackers’ View – Outside-in perspective

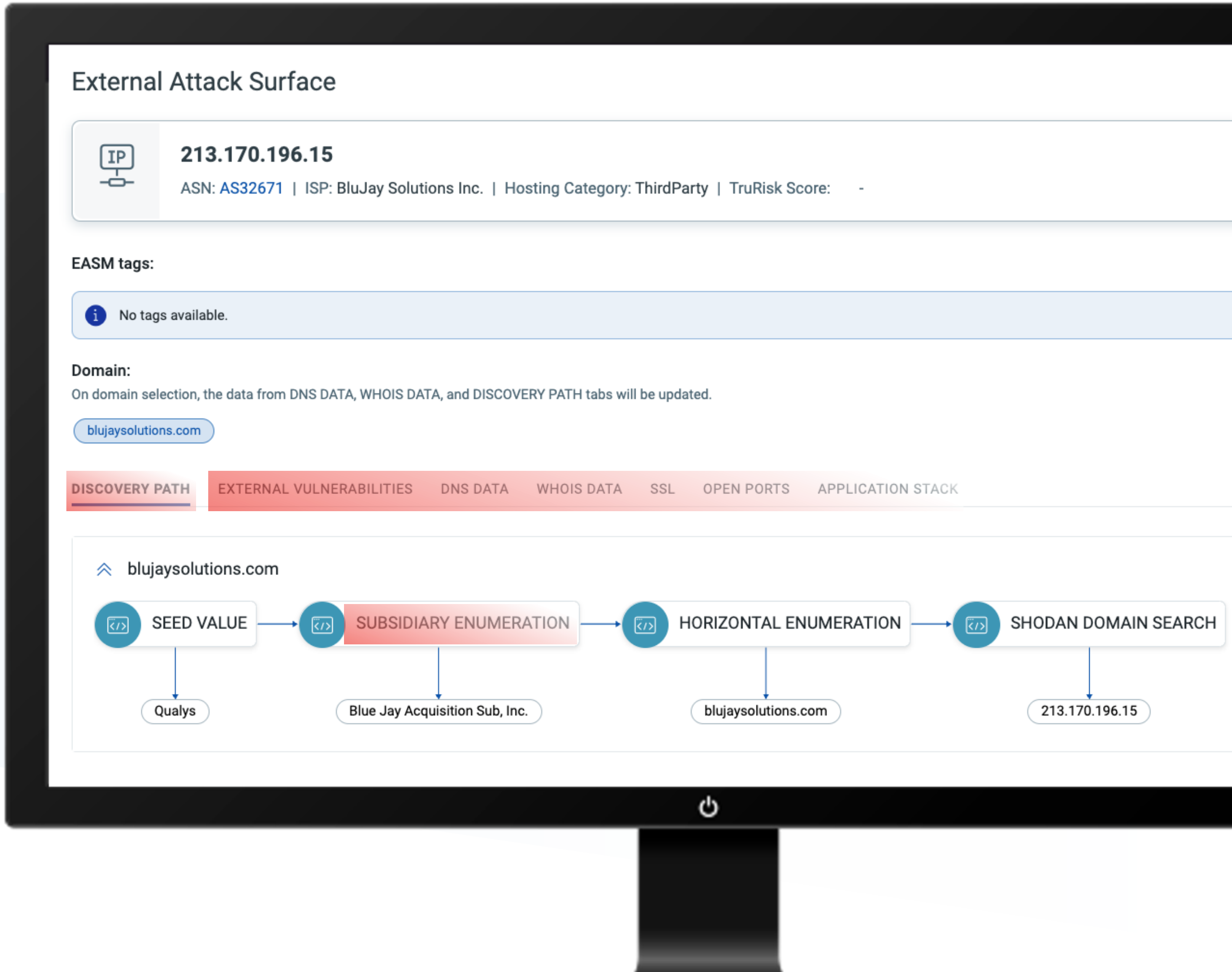
1 Discover ‘**Previously Unknown**’ internet-facing assets

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



External Attack Surface

213.170.196.15

ASN: AS32671 | ISP: BluJay Solutions Inc. | Hosting Category: ThirdParty | TruRisk Score: -

EASM tags:

No tags available.

Domain:

On domain selection, the data from DNS DATA, WHOIS DATA, and DISCOVERY PATH tabs will be updated.

blujaysolutions.com

Bringing Together EASM and CSAM

Purpose-built for Cybersecurity and VM/Risk teams

1 External Attack Surface Management (EASM)

CyberSecurity Asset Management (CSAM) 2

Attack surface from an **attacker outside-in** perspective.

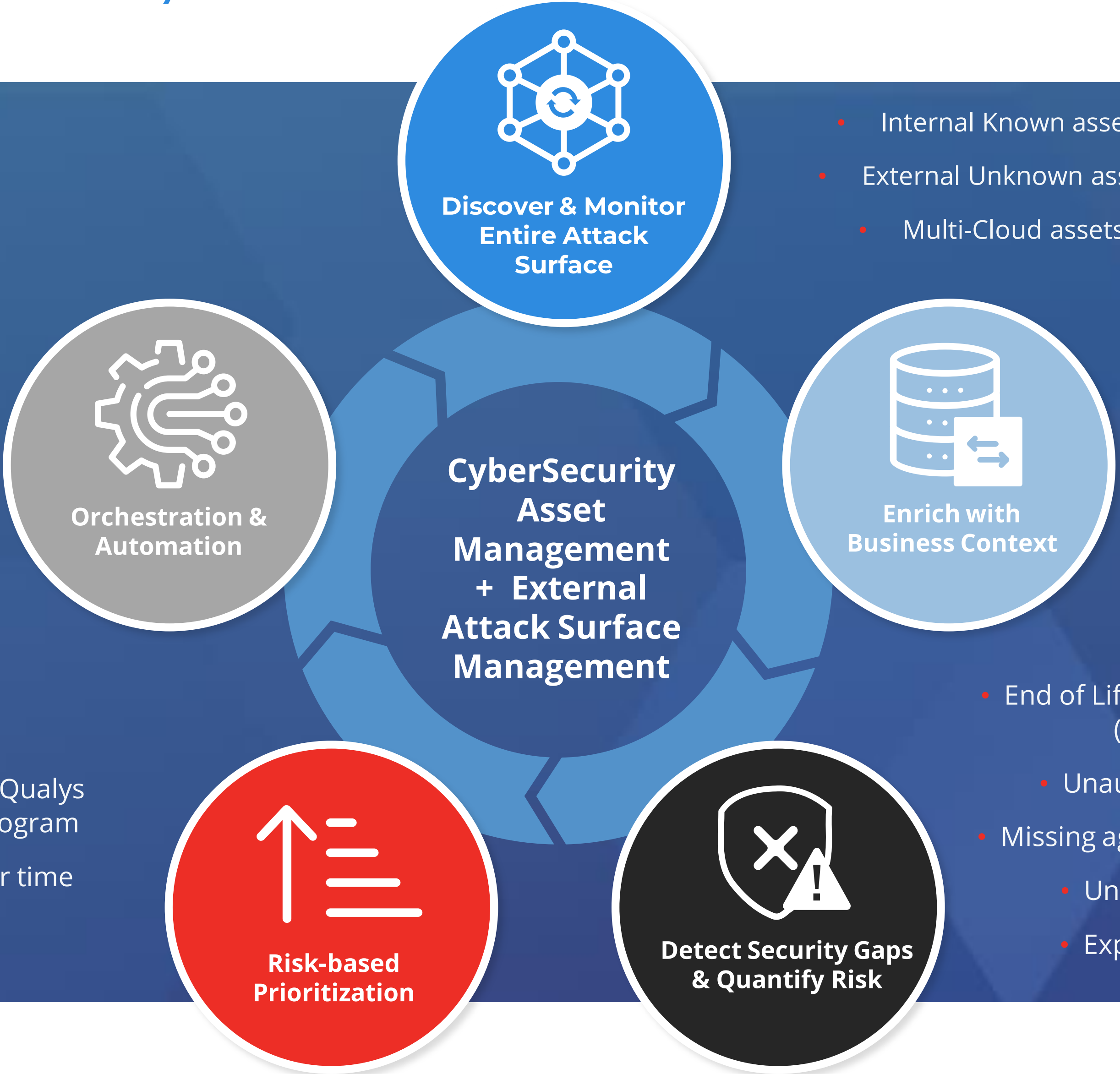
- Discover and continuously **monitor outside-in digital footprint internet-facing assets**
- **Natively integrate with VMDR** (or other) for vuln analysis and prioritization
- Continuously improve and implement **attack surface management (ASM)** strategies

Attack surface from a **defender inside-out** perspective.

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

Continuously Monitor and Reduce Attack Surface

Discover, Enrich, Detect, Prioritize and Orchestrate



CyberSecurity Asset Management + External Attack Surface Management

Discover & Monitor Entire Attack Surface

- Internal Known assets
- External Unknown assets
- Multi-Cloud assets

Enrich with Business Context

- Save time by automating CMDB updates
- Boost your CMDB with high-fidelity data
- Import Business Information and Criticality from 3rd-party sources

Detect Security Gaps & Quantify Risk

- End of Life (EOL) / End of Service (EOS) Software
- Unauthorized software
- Missing agents and security tools
- Unsanctioned ports
- Expired SSL certs, …

Risk-based Prioritization

- Extend risk-based detection with Qualys TruRisk to Asset Management program
- Quantify business cyber risk over time

Orchestration & Automation

- Automate VMDR, WAS scans & Patch remediation workflow
- Bi-Dir Workflow with CMDB, SIEM, Datalake
- Uninstall Software

Business Advantage

Simplified & Optimized Cyber Security 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.
Bi-directional CMDB sync providing business context

Reduced TCO

Reduced TCO with centralized platform that helps consolidates multiple siloed point products into Unified One-platform-one-agent.

Positive Business Outcomes

Delivering Powerful Results with CSAM

K™

Quickly meets and remediates **PCI-DSS requirements for inventory**, end-of-life, unauthorized software, and more

Shaw)

Reduced their MTTR (mean-time-to-remediate) by half, automating **risk-based prioritization and ticketing**

VERTIV™

Reduced tech debt with real-time **EOL/unauthorized software** tracking

Linked in®

Saving 365 person-days each year on **asset/software discovery** and management

Informatica

Uses CSAM to continuously track **FedRAMP compliance** of their cloud infrastructure

Qualys.

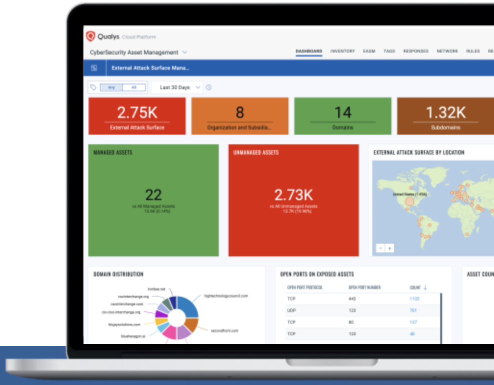
Get Your External Attack Surface Report

What’s Your Risk Posture?

Qualys Security Conference

Why is EASM Foundational?

You Can’t Secure What You Can’t See



OPEN PORT PROTOCOL	OPEN PORT NUMBER	COUNT
TCP	443	1103
UDP	123	701
TCP	80	137
TCP	123	40

715+ Customer Sign Up

~30% Unknown External Assets

415+ Active Customers

~44% Domains & Subdomains Not Inventoried

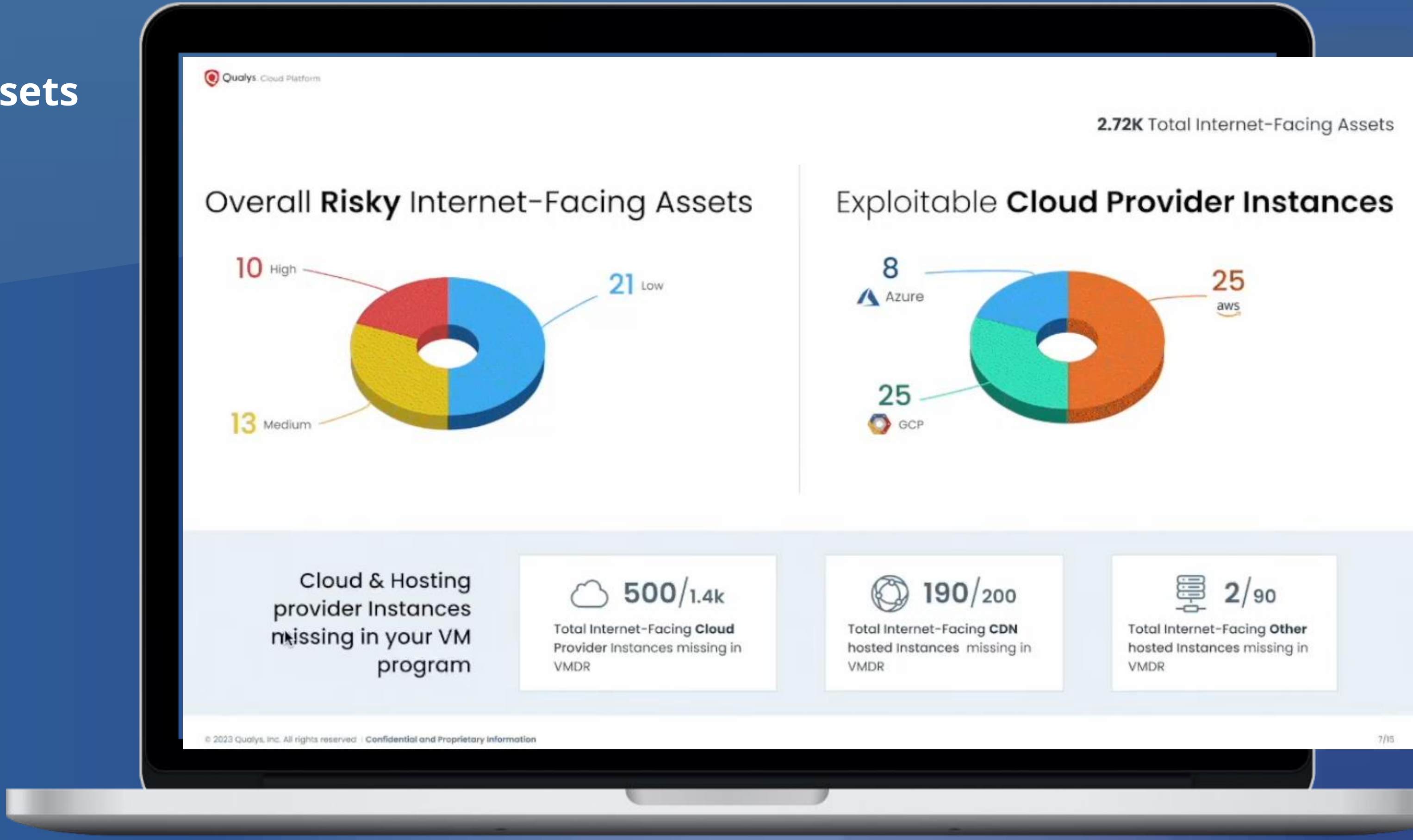
2M+ # of EASM Assets discovered

1 of 3 Average Undefined Subsidiaries

External Attack Surface Report

Get Yours Now

1. **Know your Risk on Internet-facing Assets**
2. **View Your Attack Surface**
3. **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

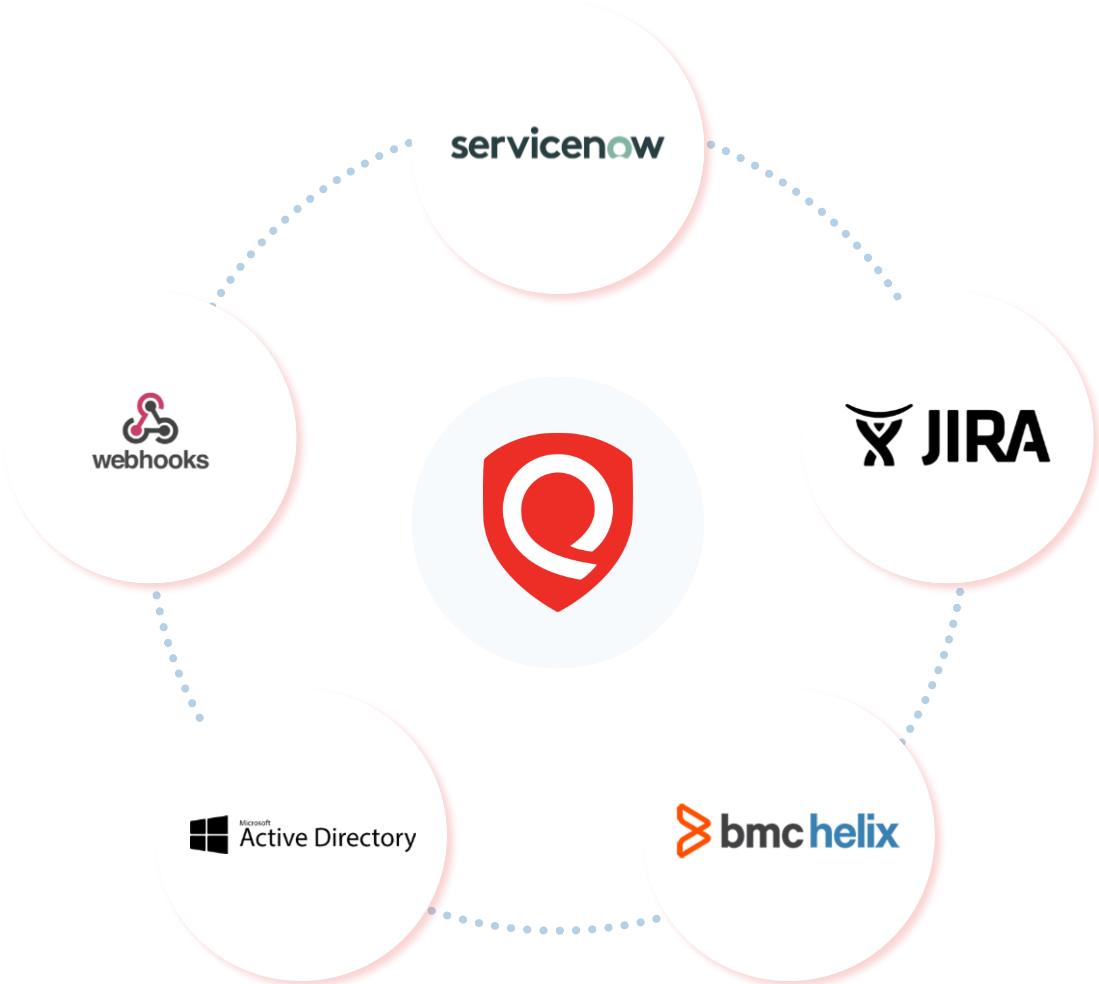
2/90 Total Internet-Facing **Other** hosted Instances missing in VMDR

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

7/15

Powered by:

Qualys Integrations with Third-party IT and Security Tools



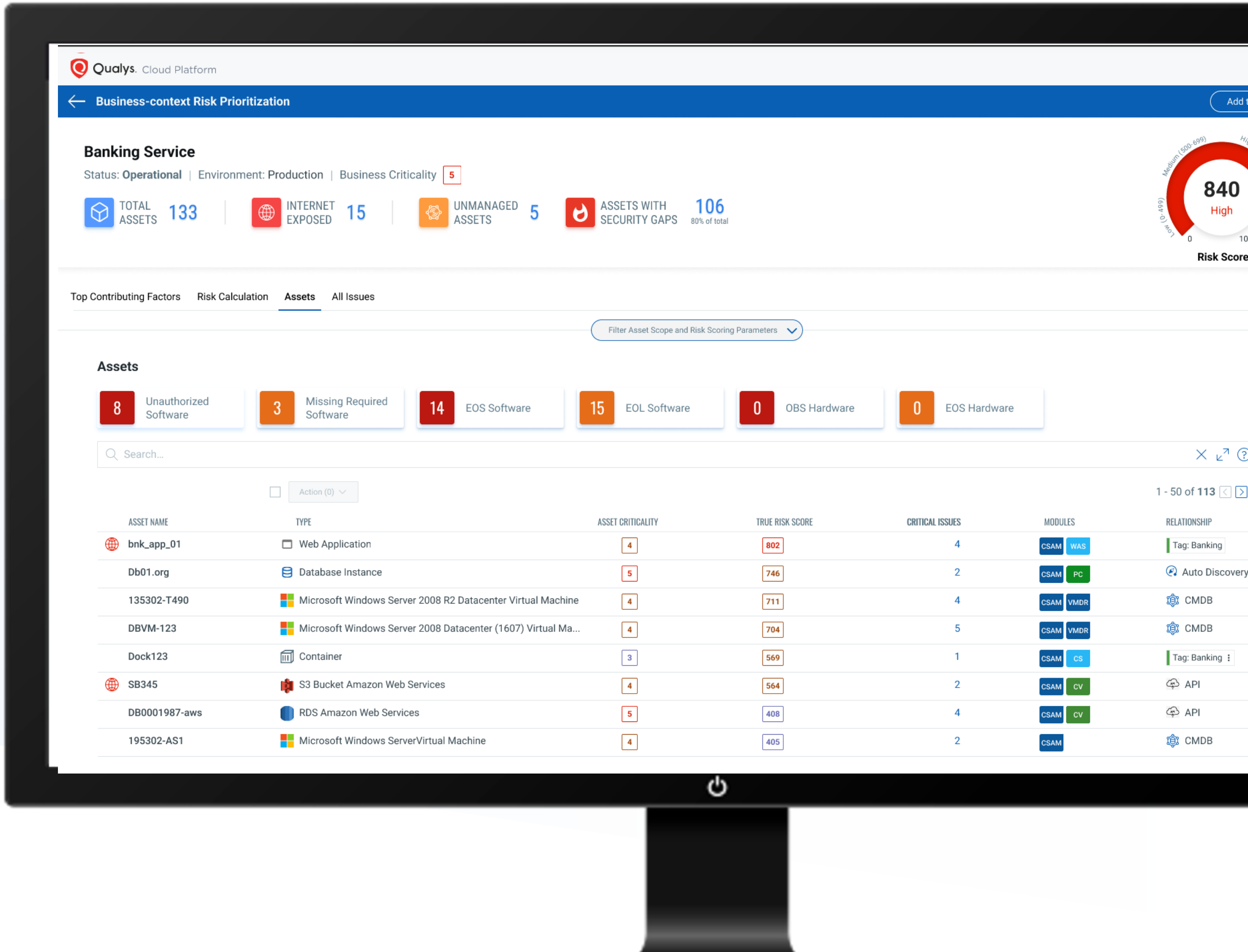
Risk-Based Prioritization

… with 3rd Party Integrations

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

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

3. **3rd Party Connectors** for CMDB, AD, Webhook, and **Security and IT tools**



Qualys. Cloud Platform

Business-context Risk Prioritization

Add t

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

840 High

Risk Score

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...

□ Action (0)

1 - 50 of 113

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

Challenges with CMDB Projects

Bridging the Gap Between IT and Security

IT Ops

- Laborious, time-consuming task to create & maintain 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

Gap

Security

- Manual effort in mapping vulnerabilities to CIs, 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

Severely impacted MTTR

Align Security and IT Ops teams

Close Tickets Faster w/ 2-way CMDB Sync

IT Ops

Continuously update asset intelligence to CIs in ServiceNow

- Create and Update CMDB CIs
- Risk Score - Open Ports - Asset Tags
- HW: Make, Model, BIOS, CPU, Memory, IP + NICs
- OS: Name, version
- SW: Name and Version, Unauthorized/Missing
- S/W, H/W and OS Lifecycle data (EOL/EOS)
- EASM details
- Certificates with ownership info
- Improve VMDR-ITSM Workflows with accurately mapping to CI items and with owner

Security

Provide Business Context to Qualys Users for Risk-Based Prioritization

- Asset enrichment in Qualys
- Operational Status
- Department
- Environment
- Owner - Managed by - Supported By -Support Group - Assigned Location
- Business Criticality
- auto-assign Asset risk score
- Assign Tags to Assets

Reduce MTTR & Increase Effectiveness

Close Tickets Faster w/ 2-way CMDB Sync

IT Ops

Improve CMDB hygiene with automated correlation and reconciliation of complete asset inventory

Close Tickets 50% Faster

Reduce Ticketing SLA Violations

Security

Reduce Mean-time-to-Remediate/Respond

Reduce Cyber Risk Exposure

Track Success and Improve IT-Security Workflows

+

Operationalize your CMDB

In Days. Not Months.

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

- ✓ Leverage current Qualys deployment of agents and scans to quickly populate asset inventory within CMDB

2 **Mature your CMDB**

- ✓ With Qualys fill the holes in your CMDB that other tools, such as ServiceNow Discovery or Microsoft SCCM, may not cover for more accurate ticketing assignment and task prioritization

3 **Continuous Asset Enrichment with Qualys**

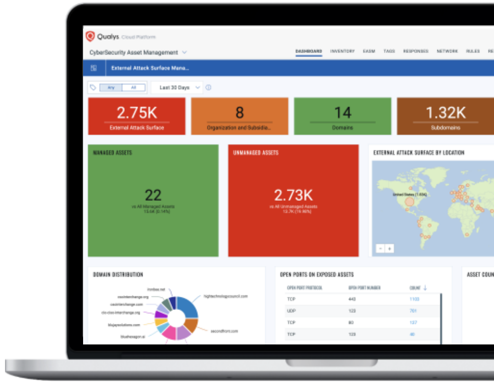
- ✓ Enrich CMDB with additional asset information from Qualys CSAM, providing actionable insights for external, ephemeral internet-facing assets, EOL software, domains, and more

Roadmap

FY 23

CSAM & EASM Roadmap

What's Been Delivered. What's Around the Corner


Qualys Cloud Platform
CyberSecurity Asset Management
External Attack Surface Mana...
2.75K
External Attack Surface
8
Organization and Subsidia...
14
Domains
1.32K
Subdomains
MANAGED ASSETS
22
UNMANAGED ASSETS
2.73K
EXTERNAL ATTACK SURFACE BY LOCATION
DOMAIN DISTRIBUTION
OPEN PORTS ON EXPOSED ASSETS

Q4 22

EASM

- **Enriched Visibility** - Subsidiaries, Domains, Subdomains, M&A org to uncover unknowns
- **Discover Security Gaps** - unsanctioned ports, expiring certificates, vulnerabilities
- **Unified Risk Score** - TruRisk
- One-click VMDR, CMDB Integration
- **Web App Scanning (WAS)** Integration

ServiceNow CMDB Sync App

- Sync SSL Certificate details to CMDB
- Extend **CMDB with EASM** attributes

H1 23

Risk-Based Prioritization

- Phase -1 TruRisk Prioritization

EASM

- Free EASM Assessment Report
- Discovery & attribution improvement
- Usability (group by, filter) enhancement

3rd party Integrations

- BMC Helix - CMDB
- Active Directory
- Webhook API Connector

ServiceNow CMDB Sync App

- Sync Qualys Tags to ServiceNow Tags
- Sync Custom Attributes as

H2 23

Core features

- Software usage monitoring
- Custom catalog ingestion

EASM

- M&A and 3rd party Risk Assessment
- Lightweight scanner
- Data leakage (password, cloud keys)
- Monitoring open Amazon S3 buckets
- Exposed code repos (i.e. GitHub, Docker)
- External to Internal IP mapping

3rd party Integration

- VMWare, Crowdstrike
- Azure AD

Qualys.

Demo

Qualys®

Qualys Security Conference

Qualys Security Conference

Agenda

01 Event Event Event

02 Event Event Event

03 Event Event Event

04 Event Event Event

05 Event Event Event

06 Event Event Event

Statistics

5000	Info info info info
405	Info info info info
6000	Info info info info
500	Info info info info
1924	Info info info info

Coming Soon

New ways of Risk-Based Prioritization

3rd Party Integration

“Quote quote quote quote quote quote quote quote quote quote quote quote quote”

Qualys®