Attack Surface Management: The Crucial First Step in Controlling Your Risk

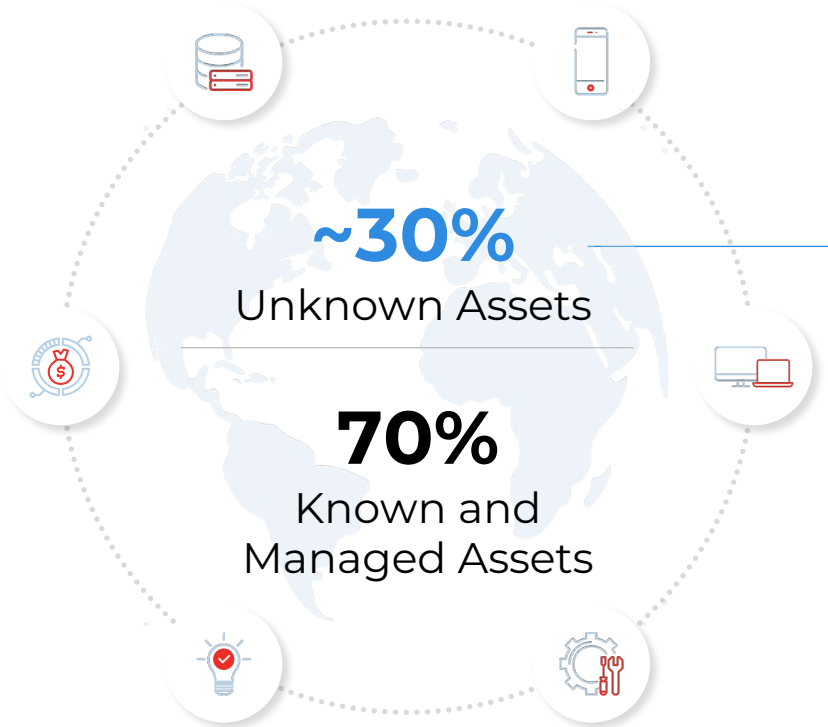
Kunal Modasiya
Vice President, Product Management
Attack Surface Management,
Cloud & Container Security, Web App & API Security

How many assets you have?

The Crucial First Step in building Attack Surface Management Program is knowing all your assets.

Impact of Unknown Assets

Not Known to Your VM, But Known to Attackers



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**.

Success Formula

For Your Attack Surface Management Program

01 Discover and inventory **ALL assets** with **business context**

02 Monitor **cyber risk with toxic combinations** beyond CVEs

03 Operationalize with IT systems to **remediate faster**

Outcomes

- Meet **compliance requirements** (FISMA, FEDRAMP, DORA, PCI, etc.)
- Set the foundation for actionable **cyber risk management** across your environment

Asset Management, CAASM, EASM...

Multiple consoles to do the job?

IT Asset Management & CMDB

- ✓ Known internal assets
- ✓ Great source for IT use cases (Warranty, licensing, etc.)
- ✓ Business Context: who owns/ manages assets

- ✗ Does not have Cyber Risk context
- ✗ Limited discovery & coverage

Cyber Asset Attack Surface Management (CAASM)

- ✓ Quickly ingest and correlate asset data from 3rd-party tools
- ✓ Confirm security coverage from multiple sources

- ✗ Not real-time
- ✗ Data becomes stale
- ✗ Data is limited & not always actionable, e.g. can't find log4j, EoL/EoS, etc

External Attack Surface Management (EASM)

- ✓ Discover External Internet-facing Unknown assets
- ✓ Attribute assets to your different Subsidiaries and M&A
- ✓ List of CVEs and misconfigs

- ✗ Noise and false-positives
- ✗ Additional cost to correlate and integrate with your VM Program

Challenge: Disjoined portals, no single view of risk ...and increased TCO

One Platform for Centralized Risk Management

Enrich & Contextualize for Cyber Risk Quantification

Security Finding Data Aggregation

Prioritization with TruRisk™ Score

Unified Attack Surface Management

Asset Exposure	EoL/EoS TechDebt	Missing Controls
Misconfigurations	Custom Attributes	Unsanctioned Services
Org, Subsidiary, M&A	Criticality & Business Impact	Environment & Status
Internet-Facing	Multi-Cloud	IoT/OT	End-points

Unified Risk Visibility and Assessment

Risk Remediation & Elimination

Qualys CyberSecurity Asset Management

Purpose-built for Cybersecurity teams for **Unified Attack Surface Program**

External Attack Surface

Attacker outside-in perspective

Continuously **monitor internet-facing digital footprint** to discover unknowns

Attribute assets with confidence to Subsidiaries & Lines of Business

Accurate risk prioritization with market-leading vuln detection, threat intel and toxic combinations

Internal Attack Surface

Defender inside-out perspective

Discover **Cloud, On-prem, Data center, IT, OT/IoT** and **Rogue Assets**

Maintain asset relation with Business Entities & Criticality to **drive accurate Risk Prioritization**

Accurate risk assessment with missing security controls & tech debt increasing asset's risk

Operationalize with IT tools to orchestrate remediation

Respond to Compliance Audits with out-of-box playbooks

Consolidate and reduce TCO!

External Attack Surface Management (EASM)

Outside-in Attacker's View

Qualys

External Attack Surface Management (EASM)

Attackers' View – Outside-in perspective

Real-time Attack Surface Monitoring

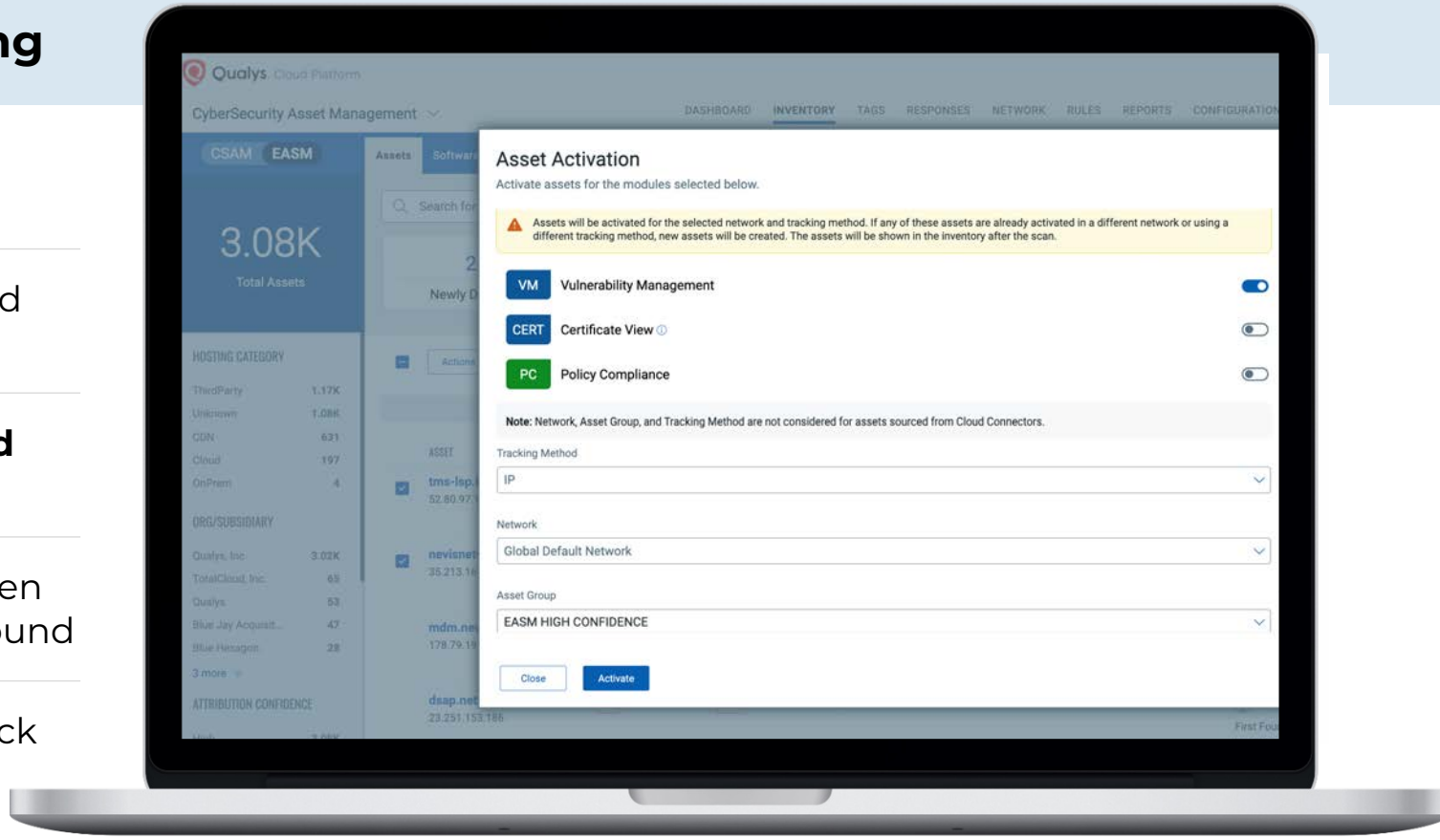
01 Discover '**Previously Unknown**' internet-facing assets

02 **Monitor Cyber Risk** for M&A Entities and Global Subsidiaries

03 **Identify** & **remediate security gaps and misconfiguration** issues

04 **Continuous monitoring:** Be alerted when unknown domains & subdomains are found

05 **Operationalize asset data** with One-click into VM, WAS, Patch, ITSM & SOC



Patent-pending EASM Discovery, Attribution & Risk Scoring

United States Patent

Patent Pending: 18385892

Title of Invention:
SYSTEM AND METHOD OF DISCOVERING EXTERNAL ATTACK SURFACE BASED ON IDENTIFICATION DATA

User Input:
Org / Top Domain Name

1 — Organization Name Lookup

EASM Catalog validates Org & Domain

2 — Subsidiary Enumeration

Fetch all **subsidiaries & acquired companies**

3 — BGP lookup

Query **BGP ASN Catalog** for related orgs and Netblocks.

4 — Horizontal Enumeration

Query **Whois** for **primary domains** of Parent Org and Subsidiaries.

5 — Subdomain Enumeration

Query **Whois ,** to find **sub-domains** of each **primary domains**

6 — DNS Lookup

Resolve all domains and subdomains to IP Addresses

7 — Scan

Scan by resolved **IPs**

crunchbase · owler (A Meltwater Offering) · Wikipedia (The Free Encyclopedia) · SEC.gov | EDGAR · BGP · Whois (Identity for everyone) · Google · DNS · SHODAN · Qualys Internet Scanners

Qualys Tech + Open Source & Commercial Feeds

Business Outcomes

With native, built-in Qualys EASM

36%

More assets discovered

Remove Blind-Spots

Find 30-40% unknown internet-facing assets with high fidelity and attribution confidence scores.

60%

Reduction in false positives

Accurate Risk Assessment

Leverage Qualys' market-leading Scanning to focus on critical, confirmed vulnerabilities while reducing noise.

3X

Faster Remediation

Operationalize Remediation

Fully integrated with CMDB & IT Workflows / ITSM to accelerate investigation, ticketing and significantly reduce MTTR.

Internal Attack Surface Visibility with Business & Cyber Context

Inside-out Defender's view

Qualys

Focus on Use Case and Progressive Discovery

Active Sensors

Agents Remote Scanners

Passive Sensors

NPS CAPS

Cloud Connectors

aws Azure ORACLE Google Cloud

Key IT Infra Connectors

Active Directory servicenow vmware bmc Webhook

Comprehensive visibility across your dynamic environment

Qualys.

Extending the Power of Qualys Agent
to Discover Unmanaged Assets

Connect for a LIVE DEMO
SSID: QSC Americas / QSC Americas 6E

Password: QSC_2024

CSAM with Cloud Agent Passive Scanner (CAPS)

Enables already-deployed Qualys Agents to discover unmanaged devices **in real time**

Complete Internal Attack Surface Coverage

Completes your inventory risk program with visibility to IoT devices, unauthorized cloud instances and any network devices

Lays the Foundation for Zero Trust Security Architecture

Proactively identifies in real-time devices connected to the network that are not authenticated, missing security agents, or otherwise, untrusted.

Fast-tracks CMDB Accuracy and Coverage

Correlates discovered assets to the configuration management database (CMDB), enabling IT with comprehensive visibility

Extend your Inventory with Connectors

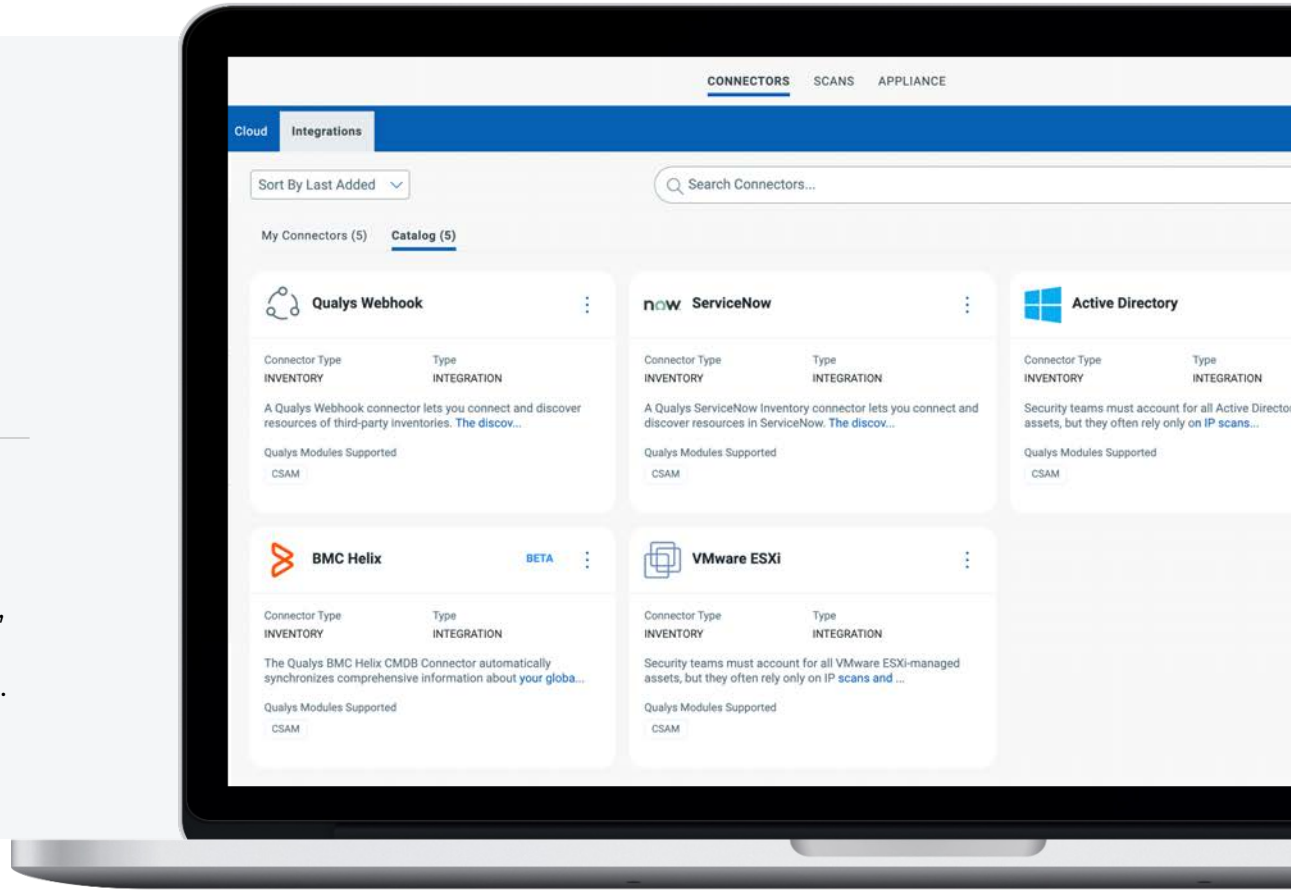
Integrating with Key IT Tools

Find Assets Missing in Qualys

Completes your inventory risk program with visibility to IoT devices, unauthorized cloud instances and any unmanaged devices, while integrating with VMDR & Compliance assessment program with one-click.

Automate VM/PM Workflows

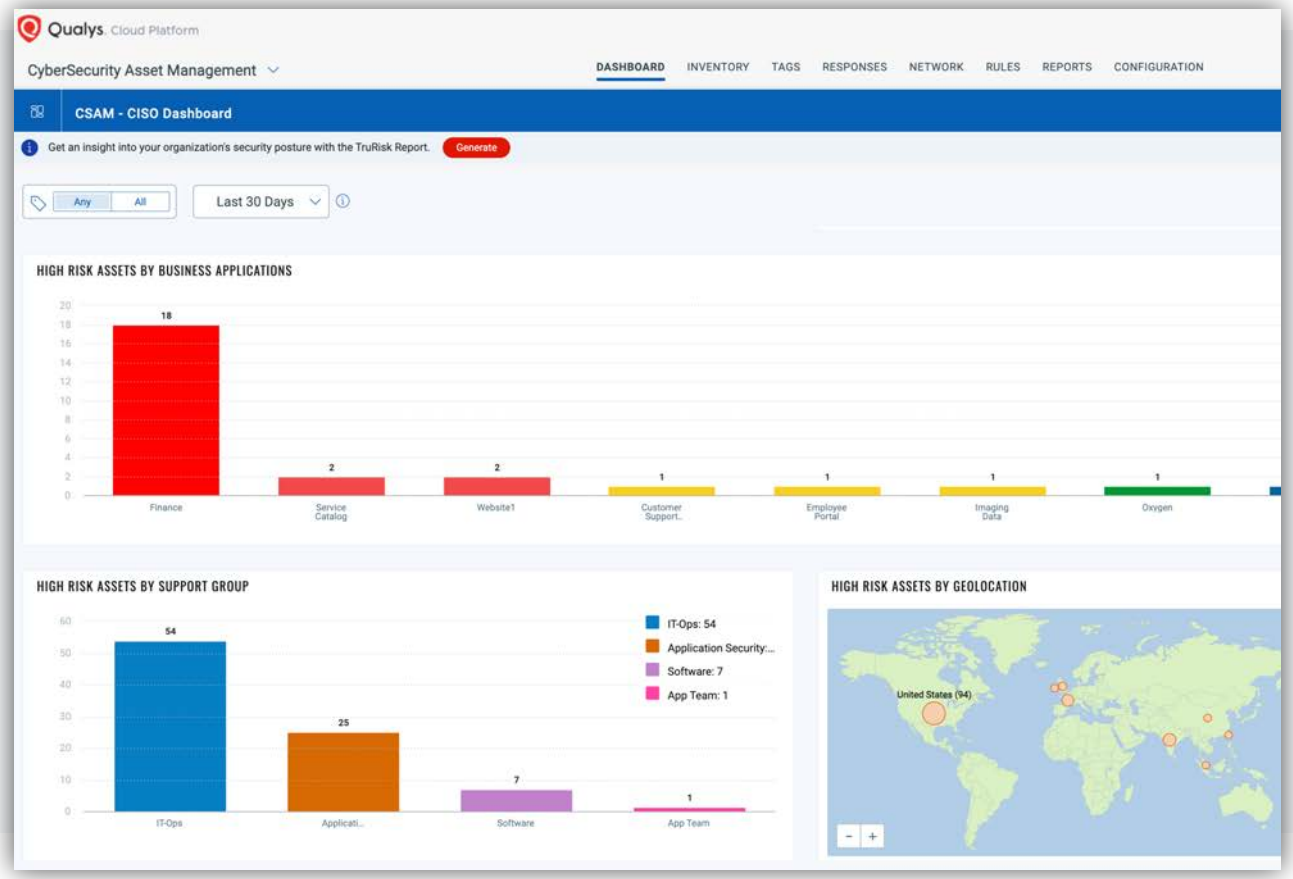
Import key attributes, such as Business Units, Groups, virtual machine labels & custom attributes, to automate vuln prioritization and patch management.



Enrich Asset with Business Context

To drive accurate Risk Scoring & Assessment

- Asset Ownership
- Business App/Service
- Support Group
- Environment & Status
- Criticality
- Custom Attributes & more



Inventory Risk Assessment

With Risk Factors Beyond Vulnerabilities

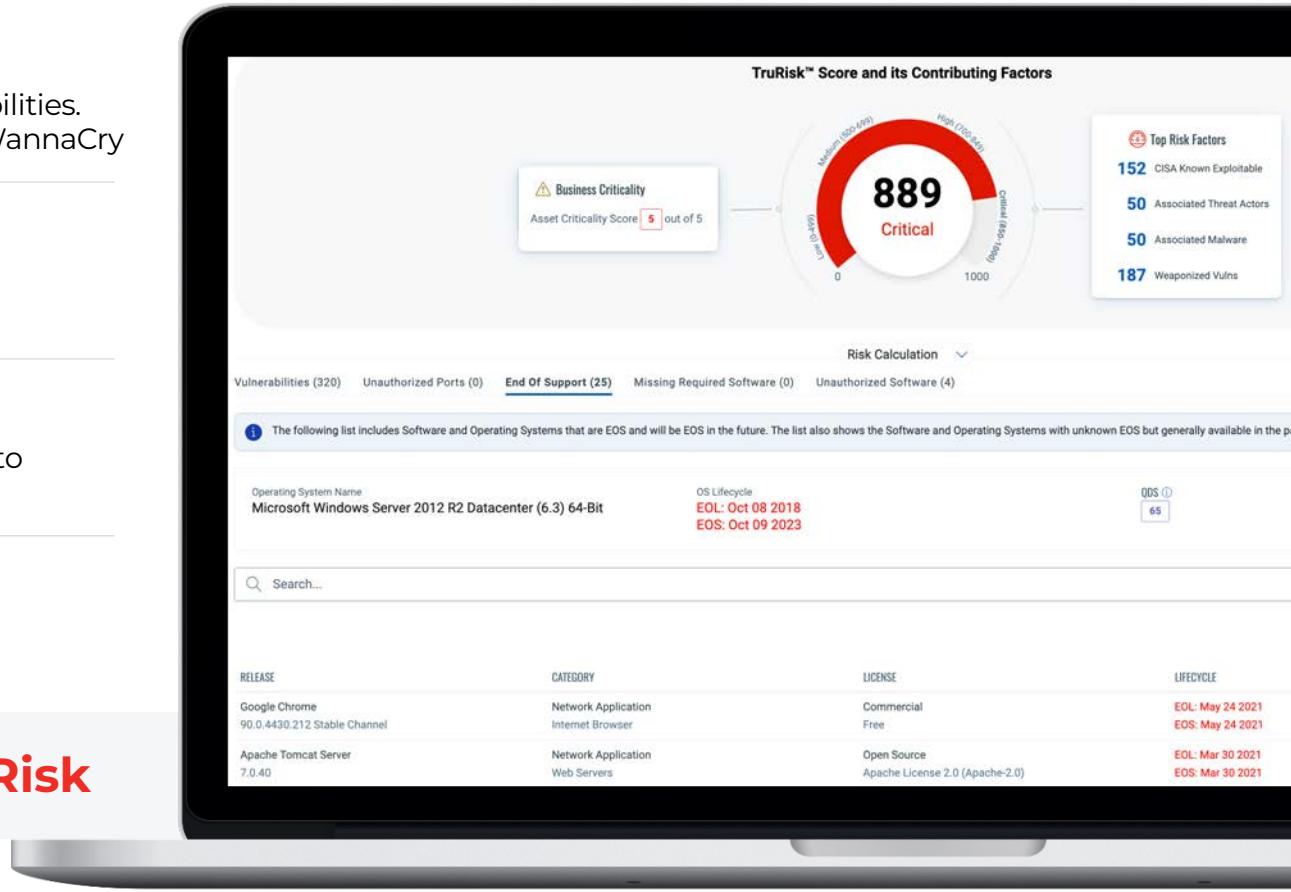
01 **Tech Debt (EoL/EoS)**
End-of-life and end-of-support tech contains unpatchable vulnerabilities. Damage multipliers from high-profile attacks such as log4shell & WannaCry

02 **Risky or Unauthorized Ports**
Misconfigured internet-facing ports can expose backdoors to the environment.

03 **Missing Security Controls**
Identify missing EDR agents or other required IT/Security software to mitigate risk proactively.

04 **Unauthorized Software**
This software shouldn't be in the environment. In addition, 40% of unauthorized software is EoL/EoS.

CSAM includes "toxic combinations" in TruRisk



Align Security and IT Ops for Faster Remediation

Qualys

Engage with Every Key Stakeholder

To Drive Business Outcomes

Measure cyber risk

with a single source of truth for asset data, criticality, and key risk indicators.

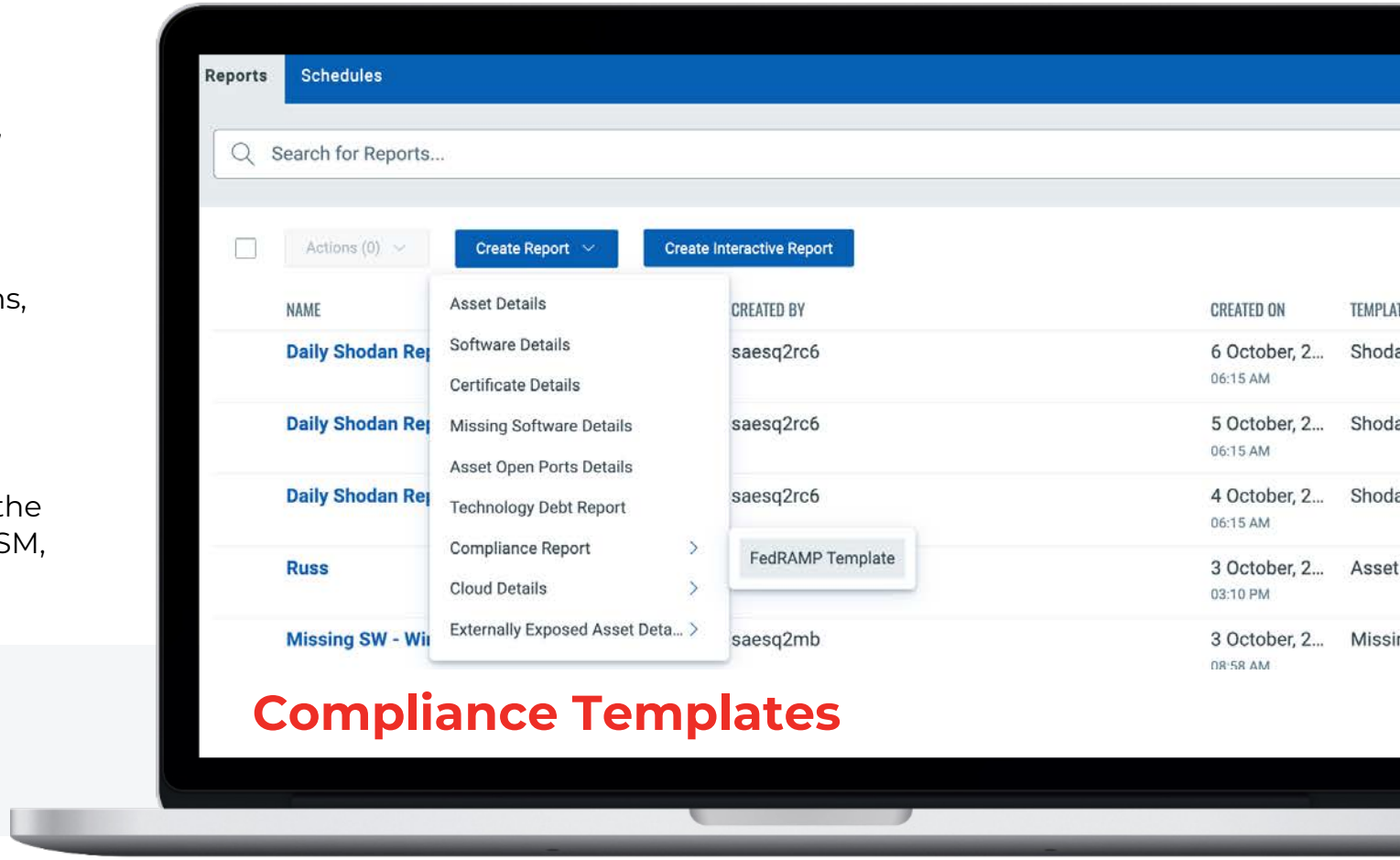
Communicate cyber risk

to all stakeholders, including SecOps teams, IT teams, executive stakeholders, and compliance auditors.

Eliminate cyber risk

with a fully-integrated approach through the Enterprise TruRisk Platform and CMDB, ITSM, SIEM tools, etc.

Provide value to all stakeholders with flexible reporting & tracking



Compliance Templates

Keep Your CMDB Up-to-Date

To Align Security and IT Ops Teams

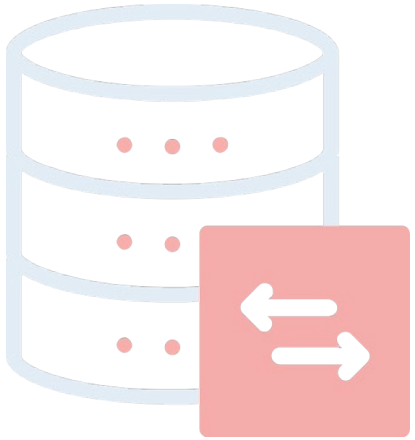
CMDB

bmc servicenow

Asset Criticality
Is the asset connected to crown jewels?
Criticality

Business Context
Asset owner, support group, etc.
Owner, Support Group

App Dependency
Dependencies, relationship mapping
Business Service



Qualys

EASM OT/IoT

Complete Inventory
IT, OT/IoT, External, Cloud, Software, etc.

EoL/EoS, Missing Agents

Cyber Risk Context
EoL/EoS, unauthorized services, missing security controls, weak SSL, etc.

Asset Config

Asset & Software
Software Catalog, Certificates, Config.

Eliminate cyber risk. Eliminate business disruption
...and Fix your Broken CMDB!

Driving Business Outcomes

Qualys

Prioritize and Reduce Attack Surface Risk Exposure

Drive business outcomes and ROI

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	**<5 Days**

Positive Business Outcomes

Drive business outcomes and ROI

	Quickly meets and remediates **PCI-DSS requirements for inventory**, end-of-life, unauthorized software, and more
	Reduced their MTTR (mean-time-to-remediate) by half, automating **risk-based prioritization and ticketing**
	Reduced tech debt with real-time **EOL/unauthorized software** tracking
	Saving 365 person-days each year on **asset/software discovery** and management
	Uses CSAM to continuously track **FedRAMP compliance** of their cloud infrastructure

Qualys Ranked as a “Strong Performer”

Among Top Vendors in Forrester Wave™ for ASM

01	**Innovation:**	“Qualys has a strong ASM roadmap, which includes enhancing attack surface coverage, and consolidating factors from 3rd parties into Qualys TruRisk”
02	**Qualys Strategy:**	“Qualys brings risks into proactive security…”
03	**Strong Remediation:**	”Qualys provides strong remediation workflows for security policy gaps and exposures..”
04	**Ease of use:**	“Reference customers appreciated how Qualys’ consolidated product provides ease of use”

“Qualys is a good choice for existing Qualys customers or users that are prioritizing remediation capabilities.”

Demo Time

Seeing is believing....

Qualys

Customer Success: VERTIV™

Mike Orosz

CISO

About Vertiv

Leading provider of equipment and services for data centers

Founded: 1965 as Liebert Corp; 2016 Launched as Vertiv

Headquarters: Columbus, Ohio (global presence)

Employees: 27,000

Revenue: $6.9B

VERTIV™

Architects of Continuity

Meeting the world's accelerating demand for data – with passion and innovation

Critical Requirements
for Attack Surface Management

- **Visibility** across complex, hybrid IT environments must be persistent
- **Dynamic** nature of cybersecurity threats demands rapid identification – Unprotected
- **EOL/EOS** technology tracking is a core element of proactive risk avoidance
- **Unauthorized software** detection must be near real time
- **Blind-spots** unintentionally occur but can be remediated

DE-RISK YOUR **BUSINESS**

How We Use CyberSecurity Asset Management?

- **Complete asset and software visibility** across our hybrid environment
- Accelerated, proactive detection of **EOL/unauthorized software to near-real-time**
- Risk remediation prioritization based on **asset criticality and business impact**
- CMDB integrations to operationalize ITSM ticketing, to **accelerate patching**

Outcomes

- **Significantly** Reduced MTTR (mean-time-to-remediate)
- **Quickly** meet SLA expectations and compliance requirements


Qualys®