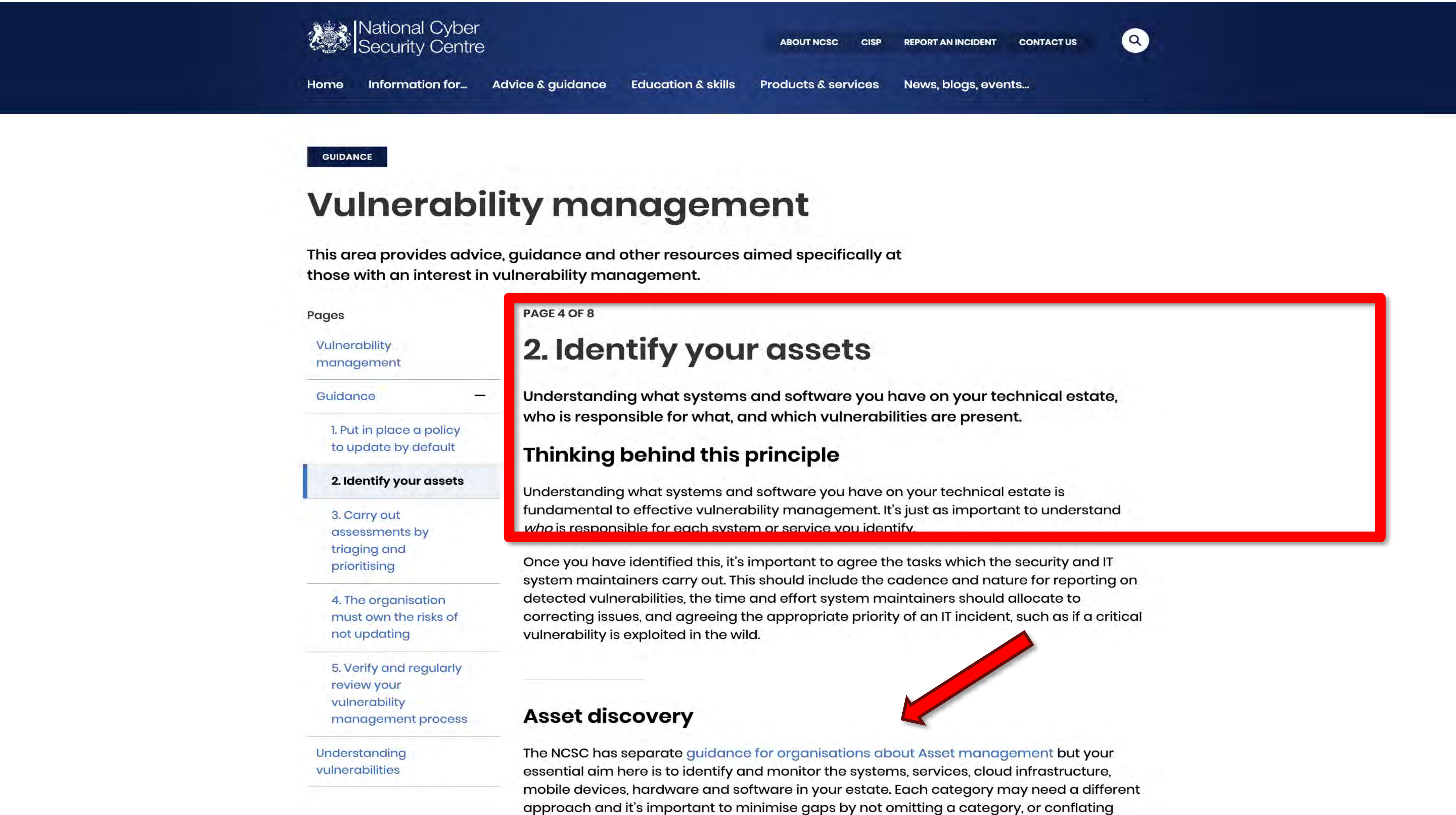
QSC24

Unified Attack Surface Management

with an Attacker's and Defender's View

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

April 24


National Cyber Security Centre
ABOUT NCSC
CISP
REPORT AN INCIDENT
CONTACT US
Home
Information for...
Advice & guidance
Education & skills
Products & services
News, blogs, events...
GUIDANCE

Vulnerability management

This area provides advice, guidance and other resources aimed specifically at those with an interest in vulnerability management.

Pages
Vulnerability management
Guidance
1. Put in place a policy to update by default
2. Identify your assets
3. Carry out assessments by triaging and prioritising
4. The organisation must own the risks of not updating
5. Verify and regularly review your vulnerability management process
Understanding vulnerabilities

PAGE 4 OF 8

2. Identify your assets

Understanding what systems and software you have on your technical estate, who is responsible for what, and which vulnerabilities are present.

Thinking behind this principle

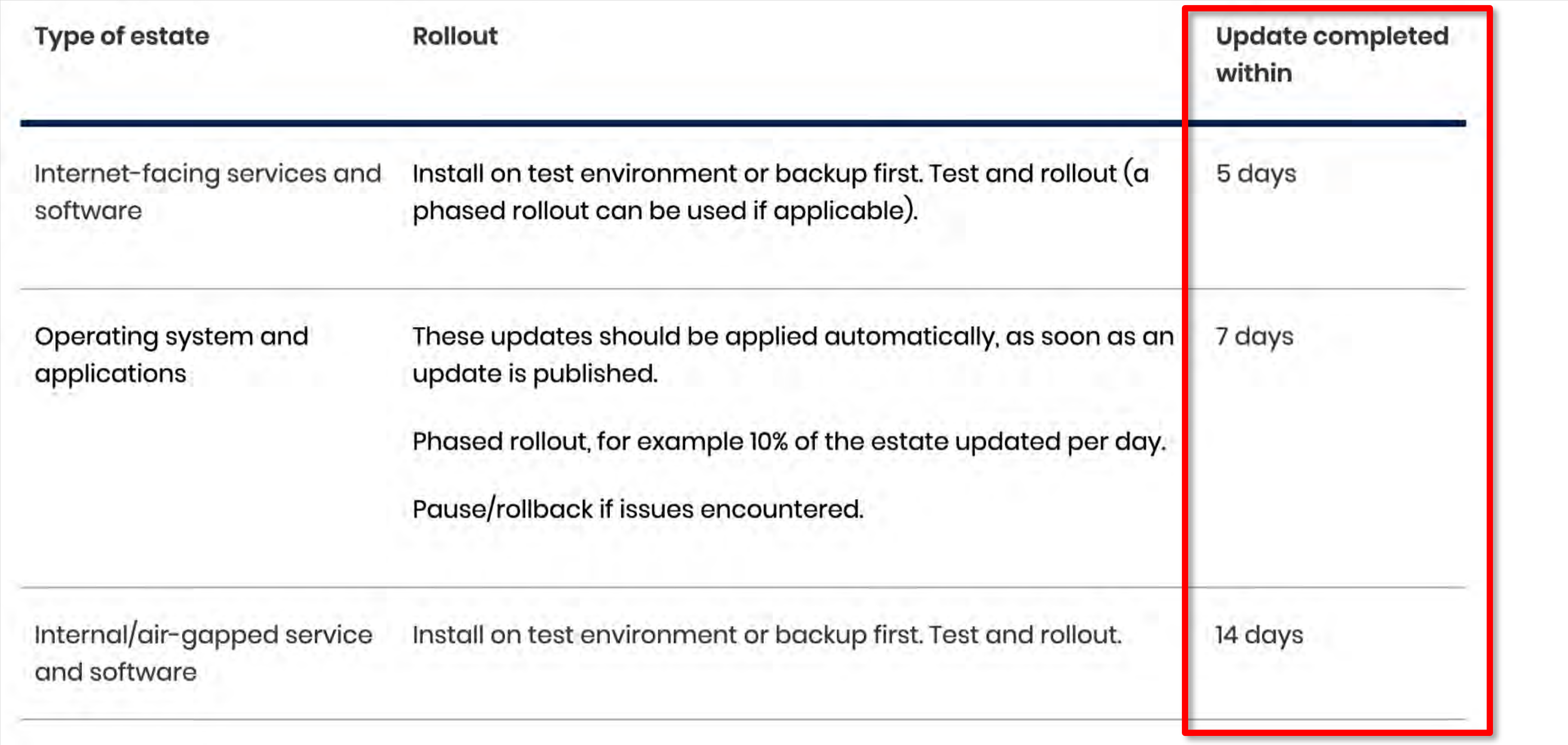
Understanding what systems and software you have on your technical estate is fundamental to effective vulnerability management. It's just as important to understand *who* is responsible for each system or service you identify.

Once you have identified this, it's important to agree the tasks which the security and IT system maintainers carry out. This should include the cadence and nature for reporting on detected vulnerabilities, the time and effort system maintainers should allocate to correcting issues, and agreeing the appropriate priority of an IT incident, such as if a critical vulnerability is exploited in the wild.

Asset discovery

The NCSC has separate guidance for organisations about Asset management but your essential aim here is to identify and monitor the systems, services, cloud infrastructure, mobile devices, hardware and software in your estate. Each category may need a different approach and it's important to minimise gaps by not omitting a category, or conflating

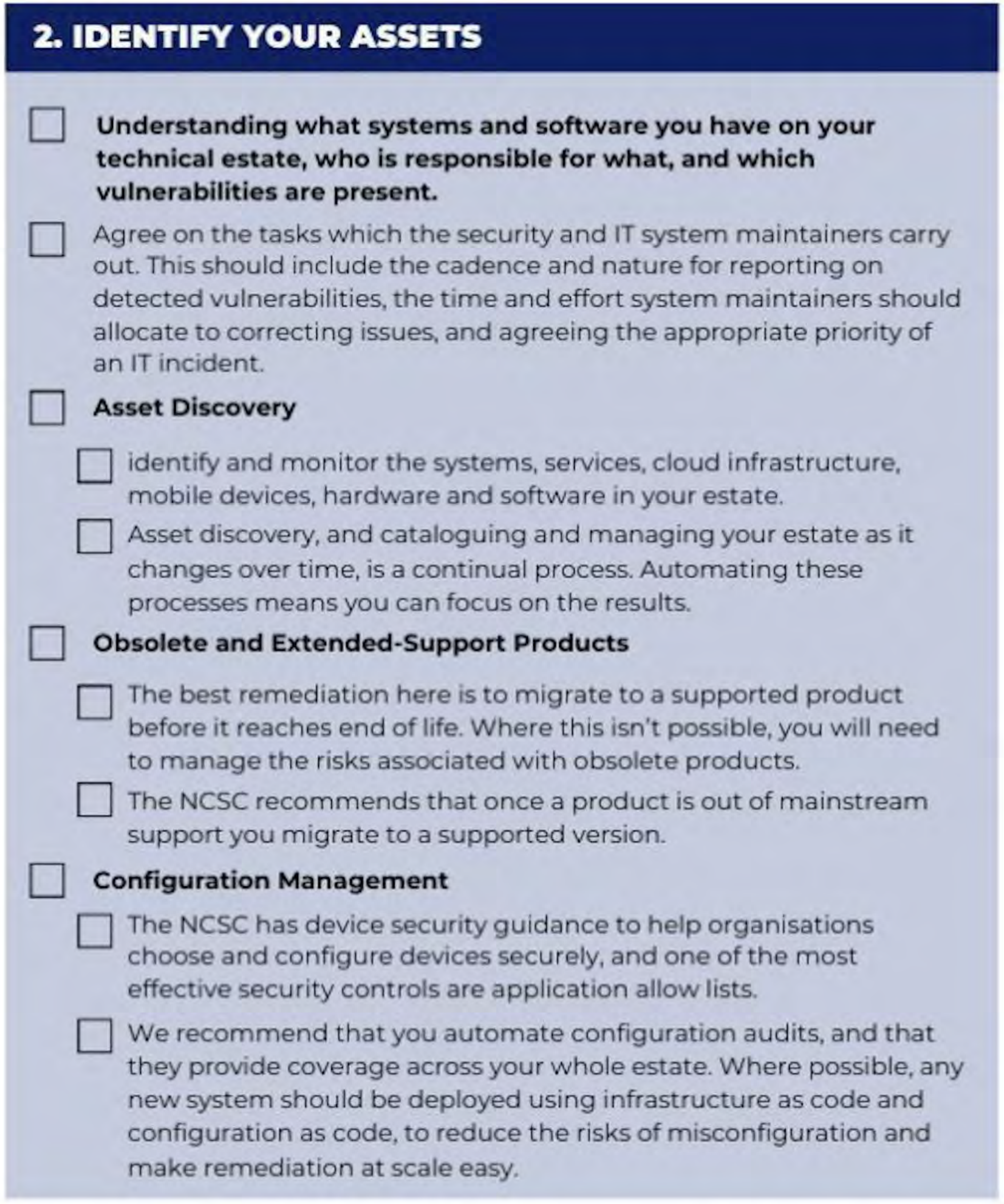
National Cyber Security Centre



Type of estate	Rollout	Update completed within
Internet-facing services and software	Install on test environment or backup first. Test and rollout (a phased rollout can be used if applicable).	5 days
Operating system and applications	These updates should be applied automatically, as soon as an update is published. Phased rollout, for example 10% of the estate updated per day. Pause/rollback if issues encountered.	7 days
Internal/air-gapped service and software	Install on test environment or backup first. Test and rollout.	14 days

NCSC Guideline for Asset Management Program

1. Asset Discovery should include on-prem, cloud infra, hardware, mobile devices, **Digital footprints, Internet-connected devices**
2. Map Assets, software, systems and vulnerabilities to the **owners and dept**
3. Identify & Reduce the risk from **Obsolete (EoL/EoS) & Extended-support Products**
4. **Accurate and availability** of information in **CMDB** supported by tools for collection
5. Identify & Reduce **the risk of Misconfig** and make **Remediations at scale easy**



2. IDENTIFY YOUR ASSETS

□ **Understanding what systems and software you have on your technical estate, who is responsible for what, and which vulnerabilities are present.**

□ Agree on the tasks which the security and IT system maintainers carry out. This should include the cadence and nature for reporting on detected vulnerabilities, the time and effort system maintainers should allocate to correcting issues, and agreeing the appropriate priority of an IT incident.

□ **Asset Discovery**

- □ identify and monitor the systems, services, cloud infrastructure, mobile devices, hardware and software in your estate.
- □ Asset discovery, and cataloguing and managing your estate as it changes over time, is a continual process. Automating these processes means you can focus on the results.

□ **Obsolete and Extended-Support Products**

- □ The best remediation here is to migrate to a supported product before it reaches end of life. Where this isn't possible, you will need to manage the risks associated with obsolete products.
- □ The NCSC recommends that once a product is out of mainstream support you migrate to a supported version.

□ **Configuration Management**

- □ The NCSC has device security guidance to help organisations choose and configure devices securely, and one of the most effective security controls are application allow lists.
- □ We recommend that you automate configuration audits, and that they provide coverage across your whole estate. Where possible, any new system should be deployed using infrastructure as code and configuration as code, to reduce the risks of misconfiguration and make remediation at scale easy.

Qualys CyberSecurity Asset Management (CSAM) Can Help…

Align with NCSC Asset Management guideline & Turbocharge Risk-Based VM Program

Step 0 of Measuring Risk

Managing Your Internal and External Attack Surface Risk

Find and close asset visibility gaps

✓ Entire Attack Surface Coverage

✓ Most comprehensive asset discovery in the market

Discover over 30% more assets

Turbocharge VM with business context

✓ Improve Asset Coverage for the VM Program

✓ Drive accurate risk prioritization based on asset category, asset configuration and business context.

5x effectiveness for ACS

Internal assets

Agent, Scanner, Sensors

External assets

Open-source Tech & Qualys Internet scanner

SHODAN

Scanner

Whois Identity for everyone

DNS

Cloud assets

Monitor your Cloud environment

aws

ORACLE

Assets from 3rd parties

API-Based Connectors

Active Directory

servicenow

bmc helix

vmware

IoT/OT and rogue assets

Passive Network Sensing & CAPS

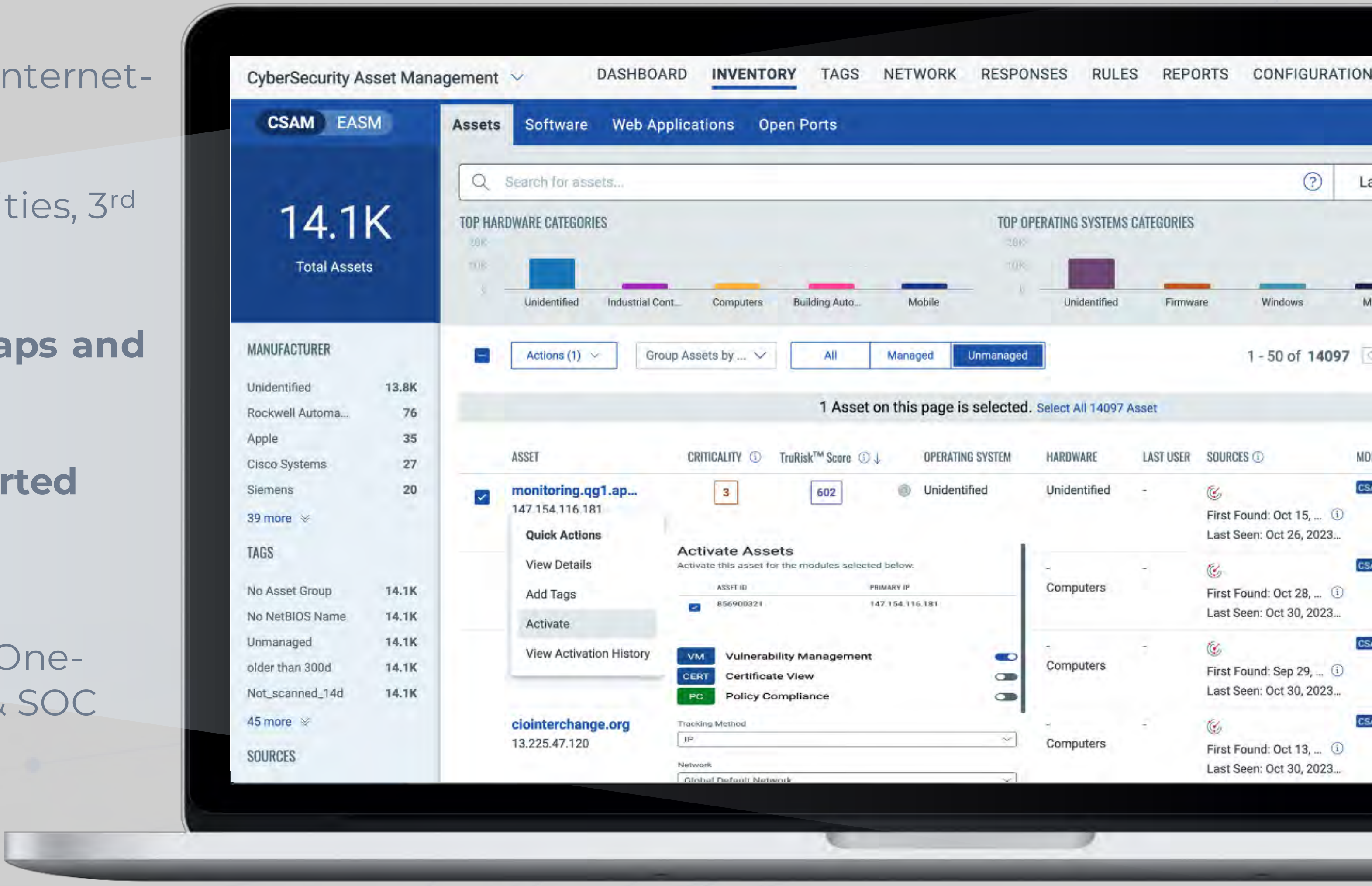
External Attack Surface Discovery & Monitoring

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



CyberSecurity Asset Management

DASHBOARD INVENTORY TAGS NETWORK RESPONSES RULES REPORTS CONFIGURATION

CSAM EASM

Assets Software Web Applications Open Ports

14.1K
Total Assets

Search for assets...

TOP HARDWARE CATEGORIES

TOP OPERATING SYSTEMS CATEGORIES

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

Actions (1) | Group Assets by ... | All | Managed | Unmanaged | 1 - 50 of 14097

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...

Quick Actions
- View Details
- Add Tags
- Activate
- View Activation History

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.

Patent Pending EASM Discovery Technology

United States Patent

Patent Pending: 18385892

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

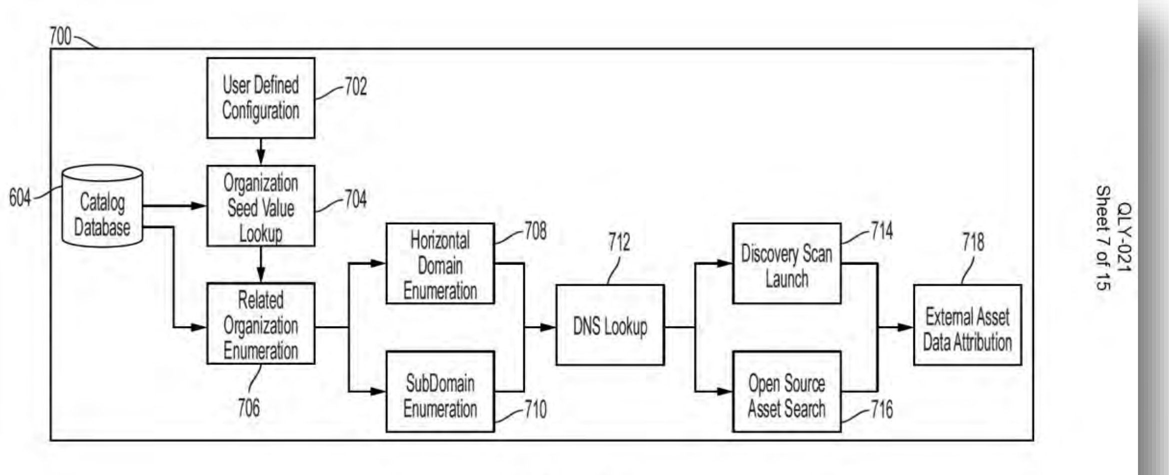

700
User Defined Configuration
702
604
Catalog Database
Organization Seed Value Lookup
704
Related Organization Enumeration
706
Horizontal Domain Enumeration
708
SubDomain Enumeration
710
712
DNS Lookup
Discovery Scan Launch
714
Open Source Asset Search
716
718
External Asset Data Attribution
QLY-021
Sheet 7 of 15

FIG. 7

Summary

- Helps discover 30-40% average unknown internet-facing assets with high fidelity and confidence scores.
- Identify Organizations internet-facing assets along with its Subsidiaries and M&A's with high accuracy.
- Reduce **Noise created by typical EASM solutions** that use sub-optimal vuln detection based on basic banner-grabbing techniques etc.

Open-source Technology & Qualys Internet scanner

SHODAN
Whois Identity for everyone
DNS
WIKIPEDIA The Free Encyclopedia
Qualys Scanner
BGP
crunchbase
Google
SEC.gov | EDGAR
owler A Meltwater Offering

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

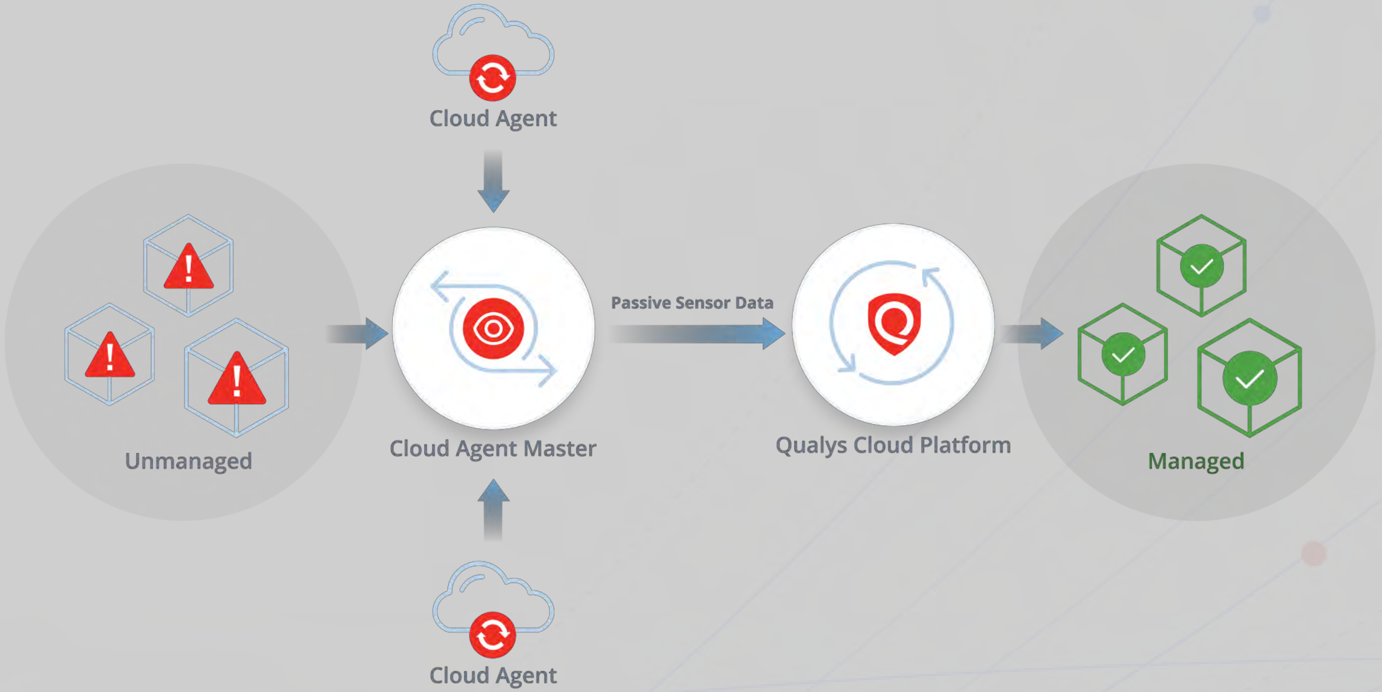
✓ **Get away from the limitation of network taps**

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.



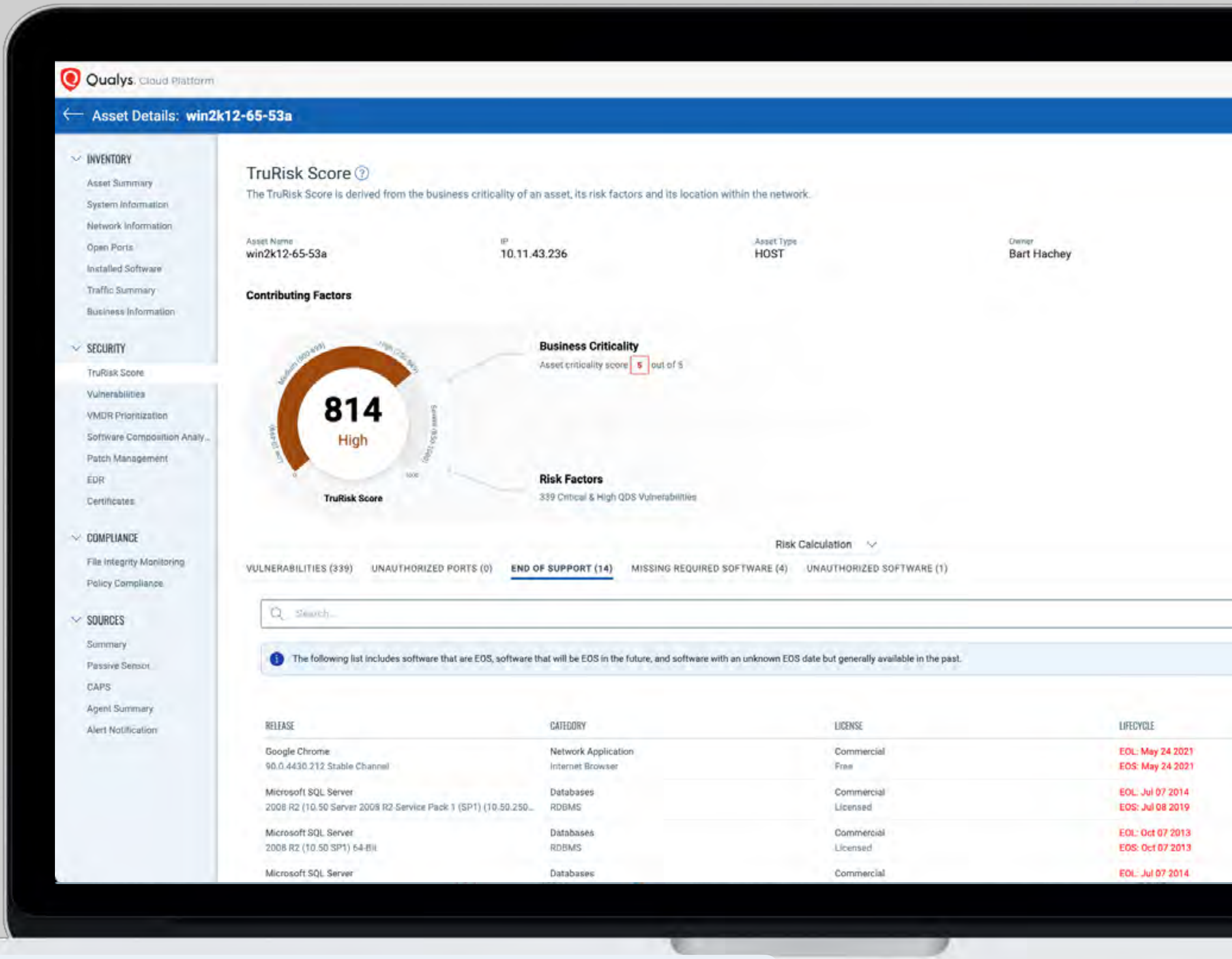
Identify Rogue Devices even in IOT environment without a massive investment in sensors and new systems

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: win2k12-65-53a

IP: 10.11.43.236

Asset Type: HOST

Owner: 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

Qualys.

Purpose-built Inventory for Cyber Security Team

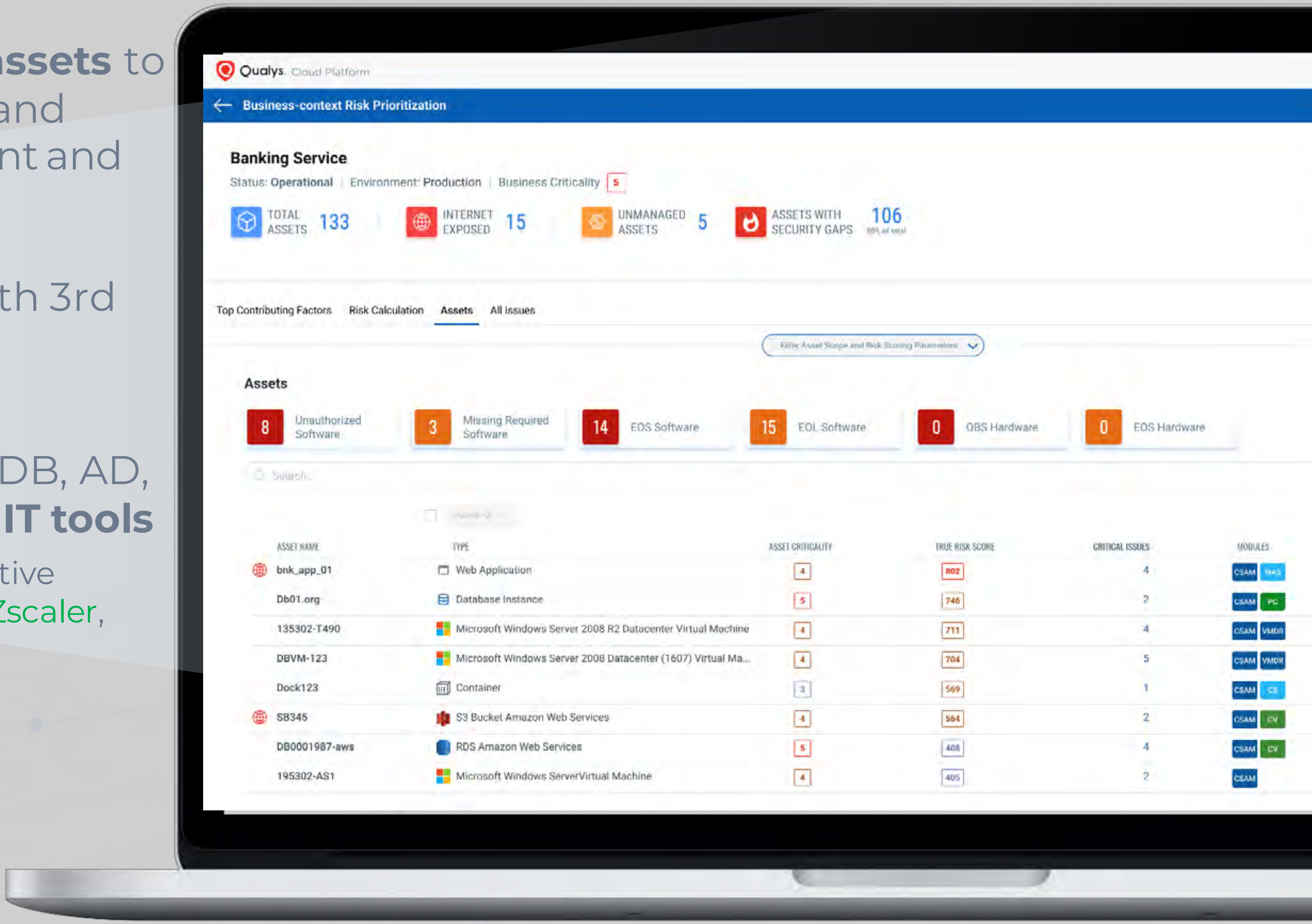
Risk-Based Prioritization

… 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

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

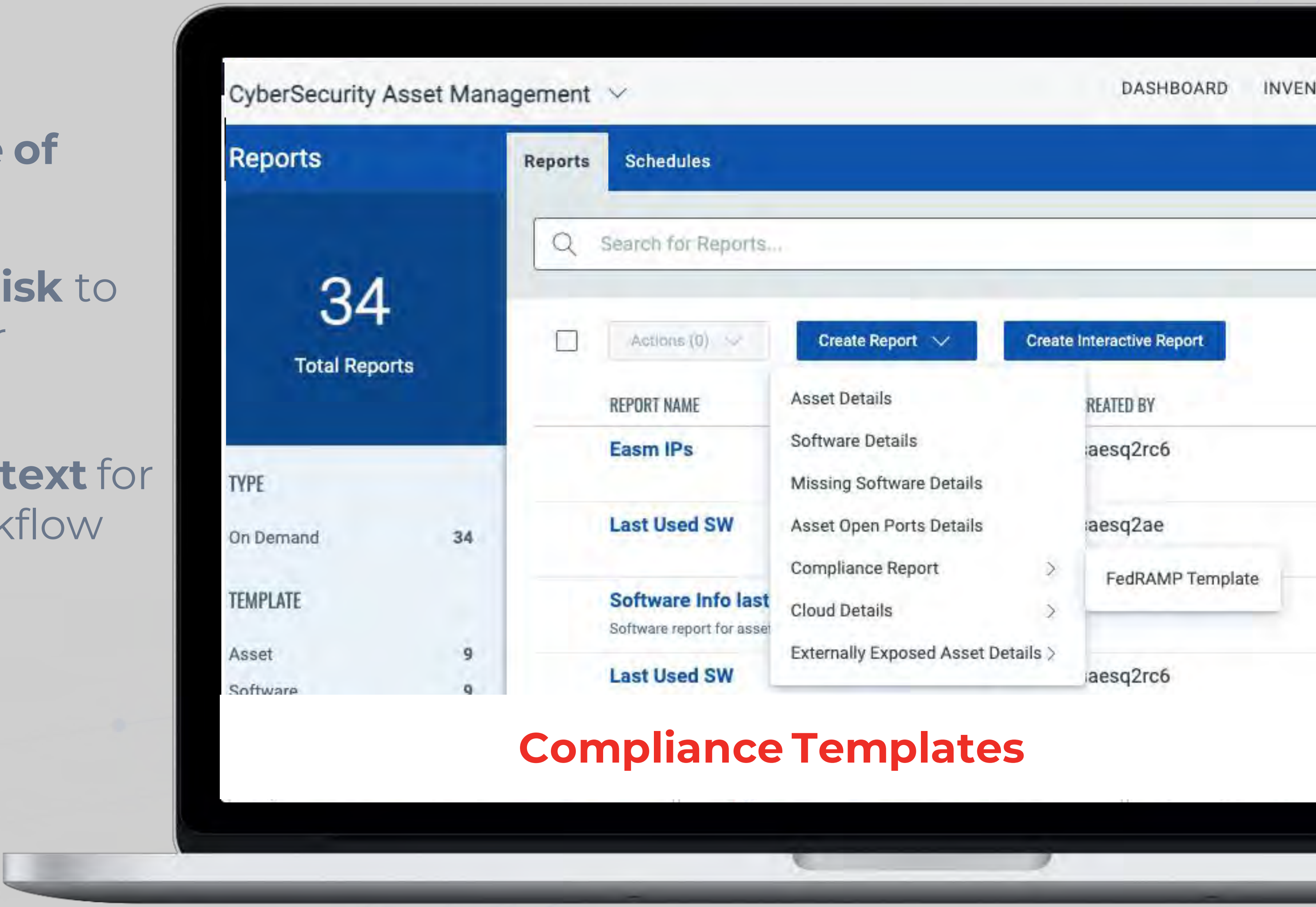
- Discover **Cloud, On-prem, Data center, IT, OT/IoT** and **Rogue Assets**
- Security, **compliance**, and **Risk-based** prioritization
- Orchestrate and Automate Workflow across IT and Security

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



CyberSecurity Asset Management

DASHBOARD INVEN

Reports

Reports Schedules

Search for Reports...

34

Total Reports

TYPE

On Demand	34

TEMPLATE

Asset	9
Software	9

□ Actions (0) Create Report Create Interactive Report

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

Create Report menu:

- Asset Details
- Software Details
- Missing Software Details
- Asset Open Ports Details
- Compliance Report >
  - FedRAMP Template
- Cloud Details >
- Externally Exposed Asset Details >

Compliance Templates

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

Turbocharge your Risk-Based VM Program

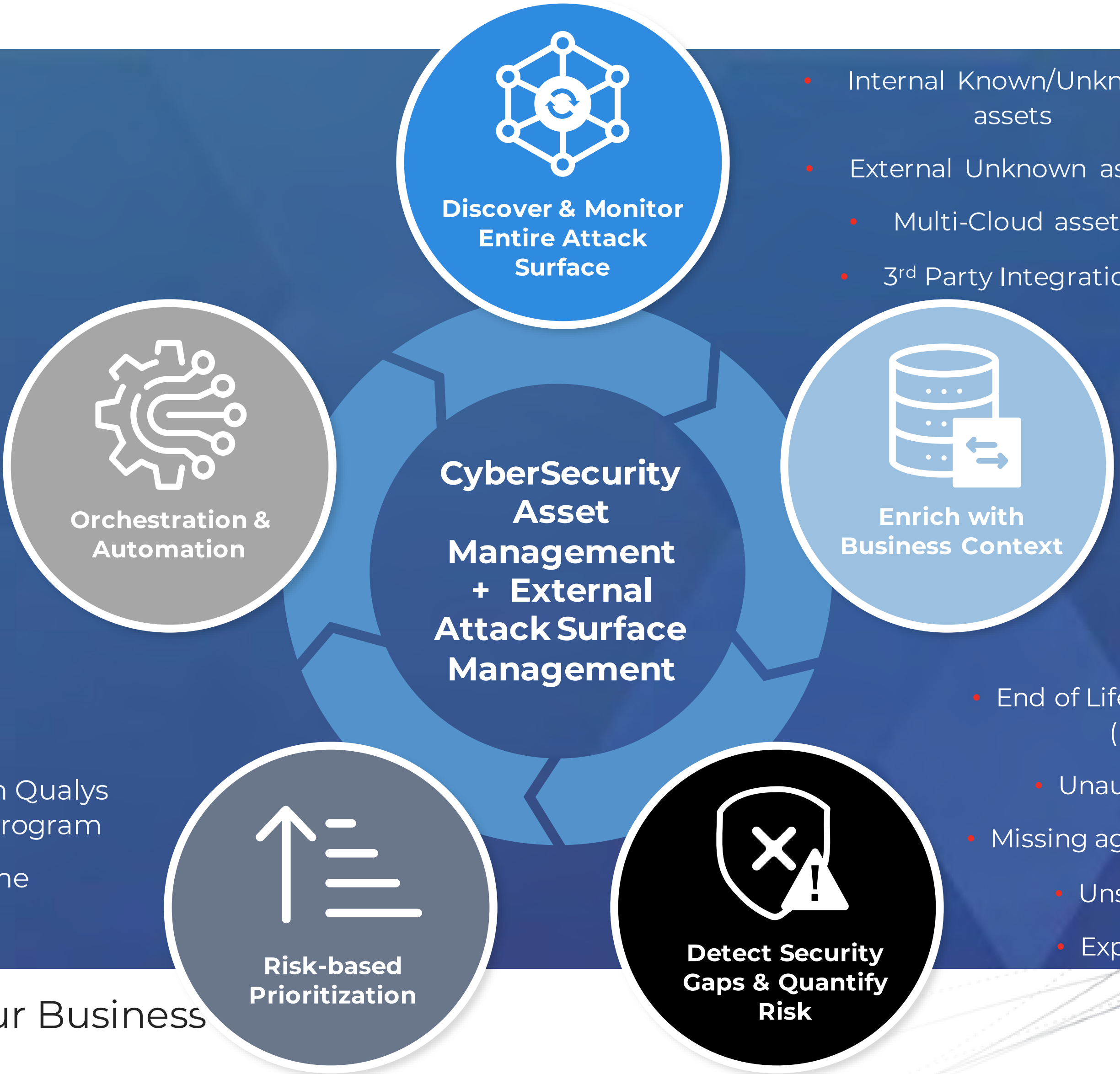
Monitor & Reduce Attack Surface

Accelerate Incident triage & remediation workflow

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

Enable Risk-Based Prioritization, reporting & remediation

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



Discover & Monitor Entire Attack Surface

Enrich with Business Context

Detect Security Gaps & Quantify Risk

Risk-based Prioritization

Orchestration & Automation

CyberSecurity Asset Management + External Attack Surface Management

Improve asset coverage Complement ServiceNow Discovery and SCCM tools

- Internal Known/Unknown assets
- External Unknown assets
- Multi-Cloud assets
- 3rd Party Integration

Bring missing assets to CMDB & QLYS

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

Bring missing cyber risk asset context to CMDB & SNOW VR

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

ROI: Delivering Business Outcomes

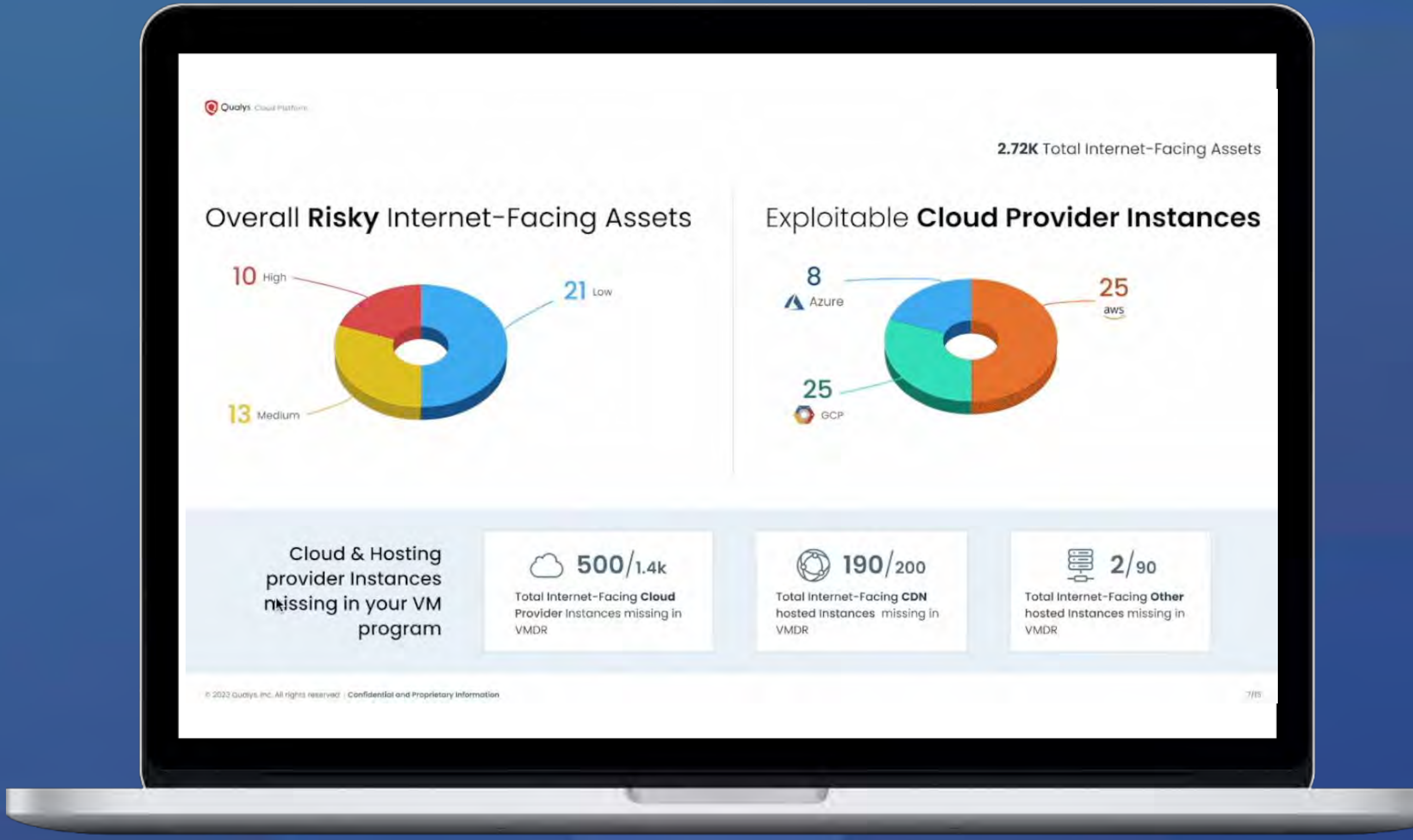
Reduce the Attack Surface with a Unified Approach

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**

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

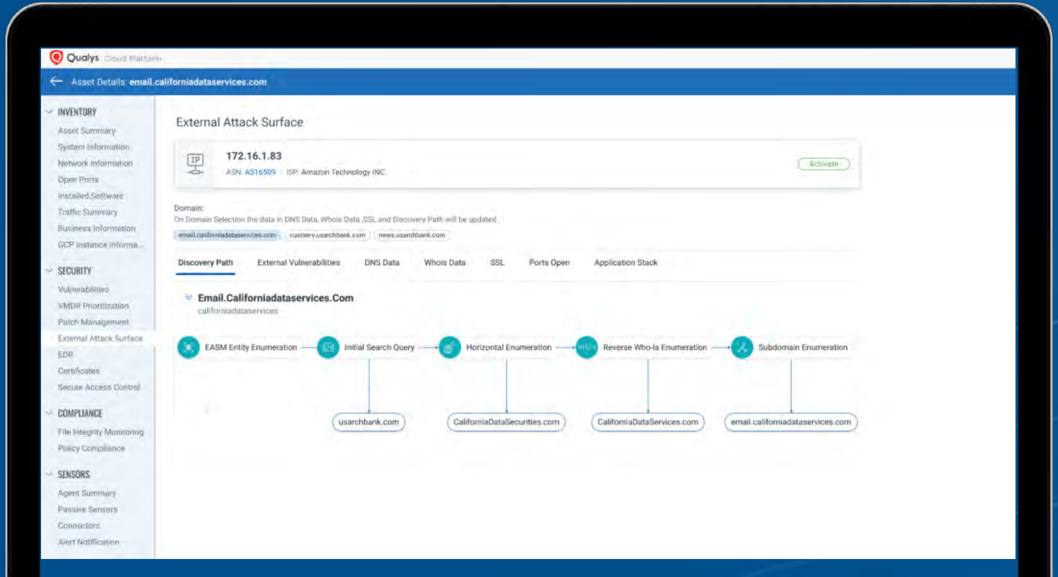
190/200
Total Internet-Facing **CDN** hosted Instances missing in VMDR

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:

CyberSecurity Asset Management (CSAM) 2.0 + EASM



Asset Details: email.californiadataservices.com

External Attack Surface

172.16.1.83
ASN: AS16509 | ISP: Amazon Technology INC.

Domain:
On Domain Selection the data in DNS Data, Whois Data ,SSL and Discovery Path will be updated

email.californiadataservices.com | custserv.usarchbank.com | news.usarchbank.com

Email.Californiadataservices.Com
californiadataservices

Turn on CSAM + EASM for your Environment:

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

Demo

Qualys®