QSC 23

Journey From Siloed Security Data to Enterprise TruRisk Management

Shailesh Athalye
Senior VP Product Management, Qualys

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

New & Constant Cyber Risk Challenges

Qualys.

Risk Has Many Definitions

Different Tools Measure Risk Differently

SaaS

OBSIDIAN AppOmni ADAPTIVE SHIELD

Code

BLACKDUCK VERACODE GitHub snyk

IOT

ARMIS CLAROTY

Vuln Management

Qualys RAPID7 tenable

Applications

Acunetix hackerone WhiteSource

Public Cloud

WIZ paloalto orca security aqua

Data

Laminar eureka

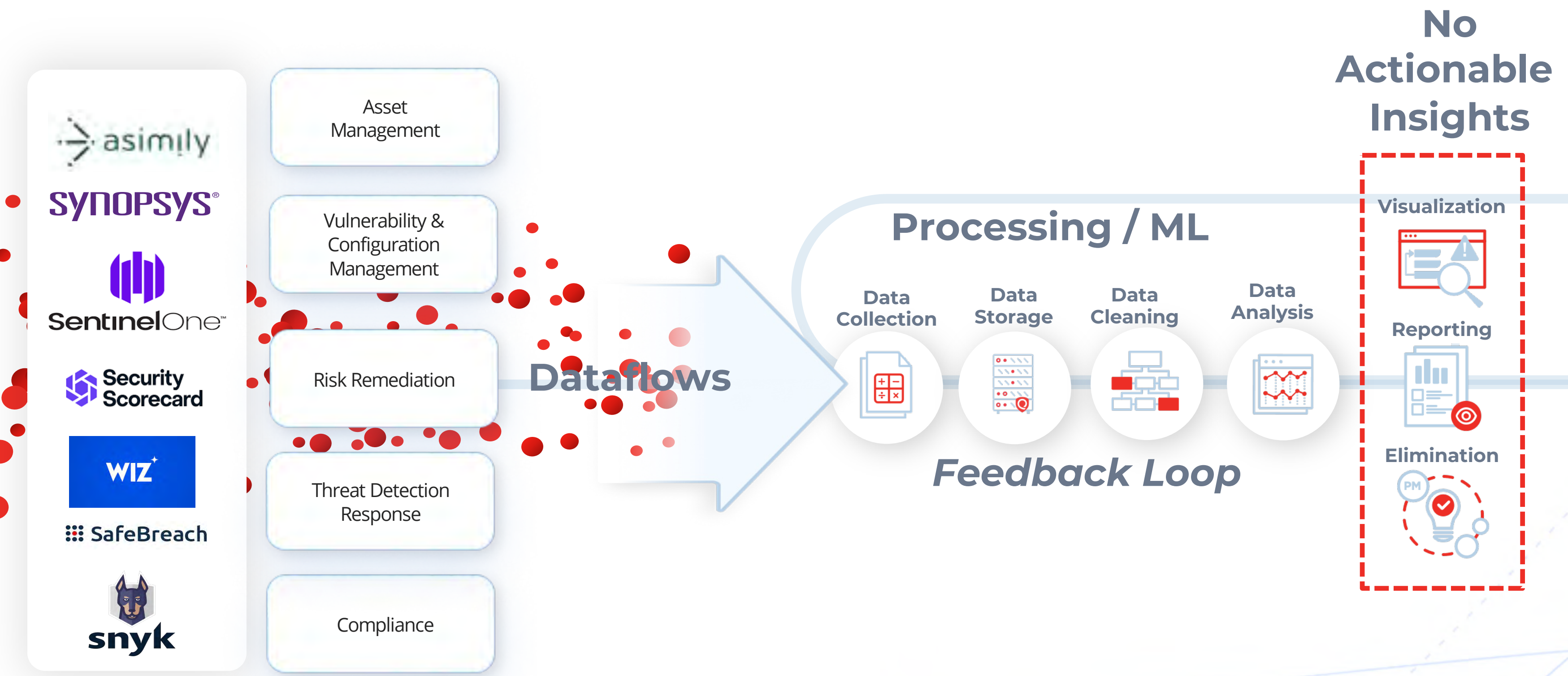
Qualitative Ranks	Quantitative Scores	CVSS
Category 1	50	2.2

What is my Cyber Risk

Qualys.

Too Much Data – Few Insights

Too Many Reporting Tools that Don't Scale



- Blindspots?
- Anomalous behavior?
- Threat context?
- Business context?
- Compensating controls?
- Compliance?
- Risk reduction plans?

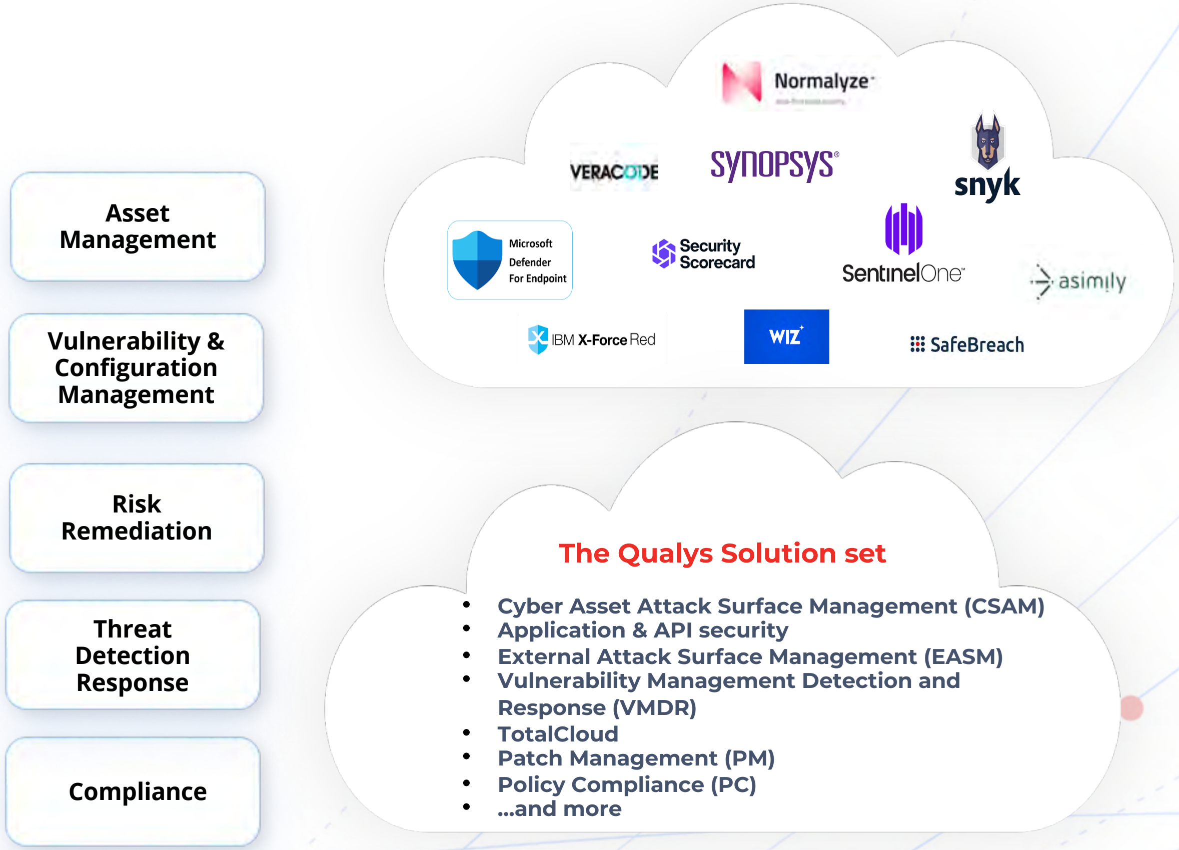
Qualys.

Need Context – Business, Threats & Insights

Lack of Threat & Business context

1. **Ransomware:**
   CVEs related to vulnerabilities
2. **Dark Web chatter:**
   CVEs related to your industry talked in dark web
3. **Known Malware:**
   CVEs exploited by by known threat actors

Unable to view unified 'Toxic Insights'



The Qualys Solution set

- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
- Policy Compliance (PC)
- ...and more

Qualys.

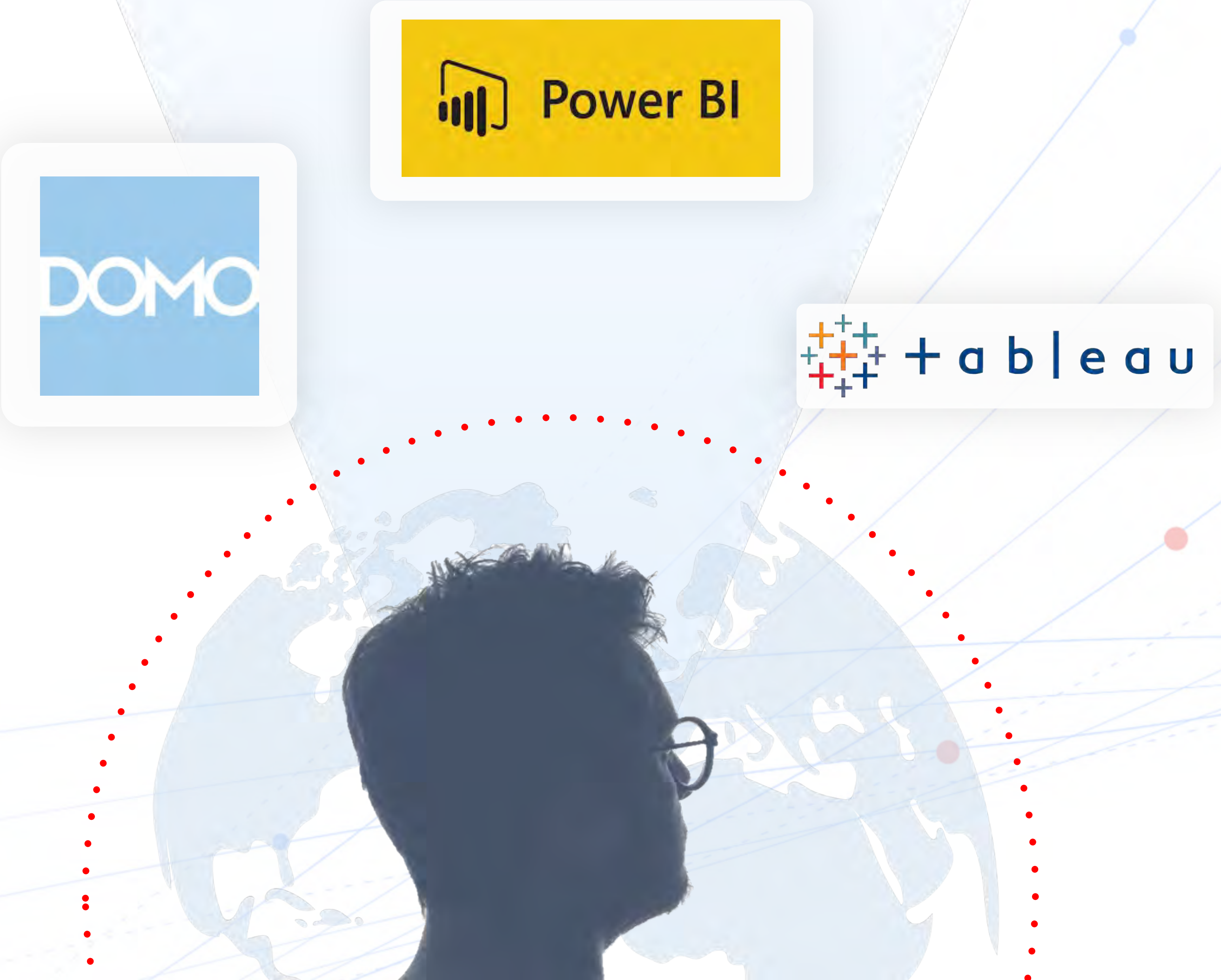
No Single Source of Truth for Communication

Too Many Consolidate to Communicate Tools that Don’t Scale

Expensive to build, manage, or buy

Don’t provide a unified risk view of risk

Waste resources and distract business focus



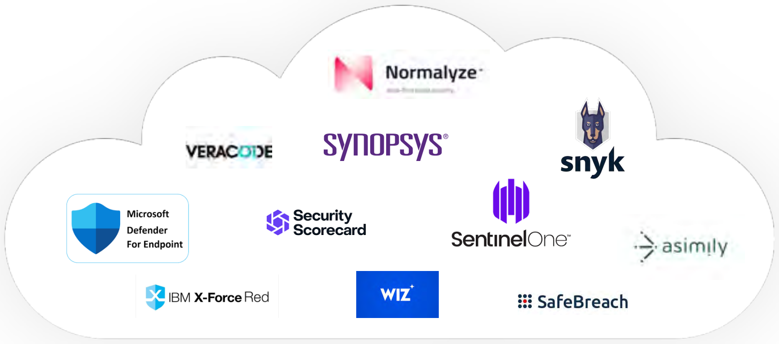
Which tools should I use communicate cyber risk?

Qualys.

Communicate Risk

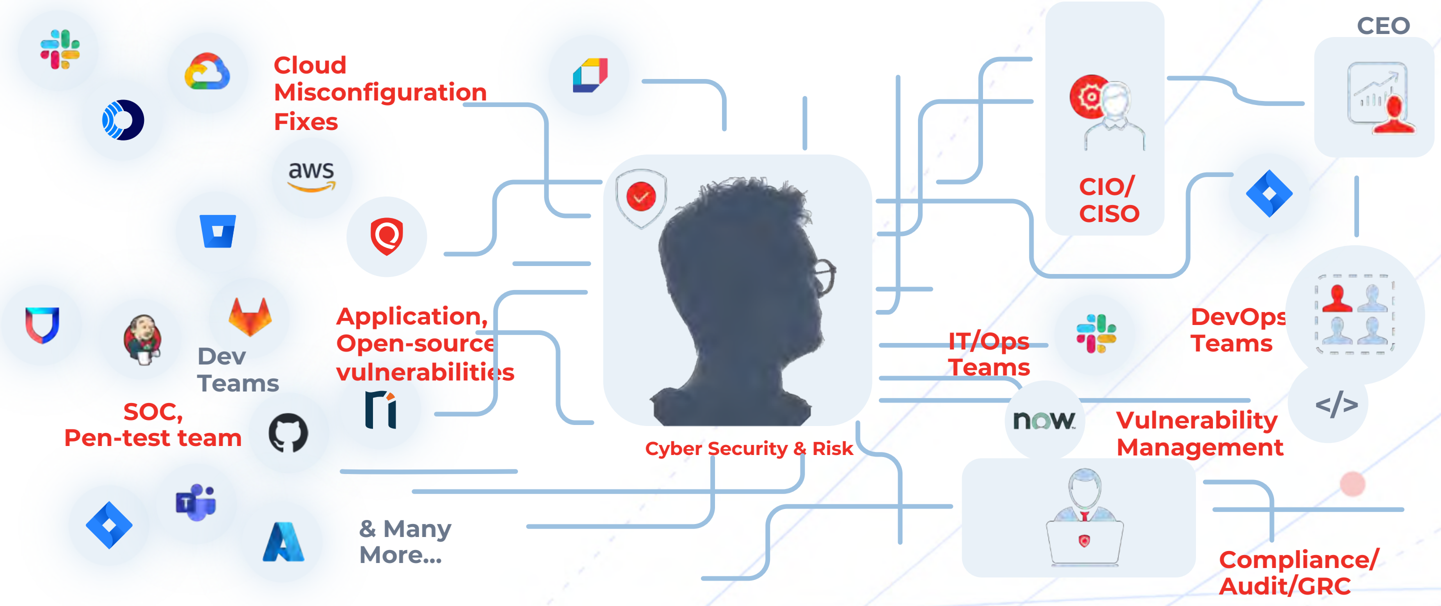
Challenge of Communicating Right Data to Right Team

Amplified by *10



The Qualys Solution set

- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
- Policy Compliance (PC)
- **...and more**



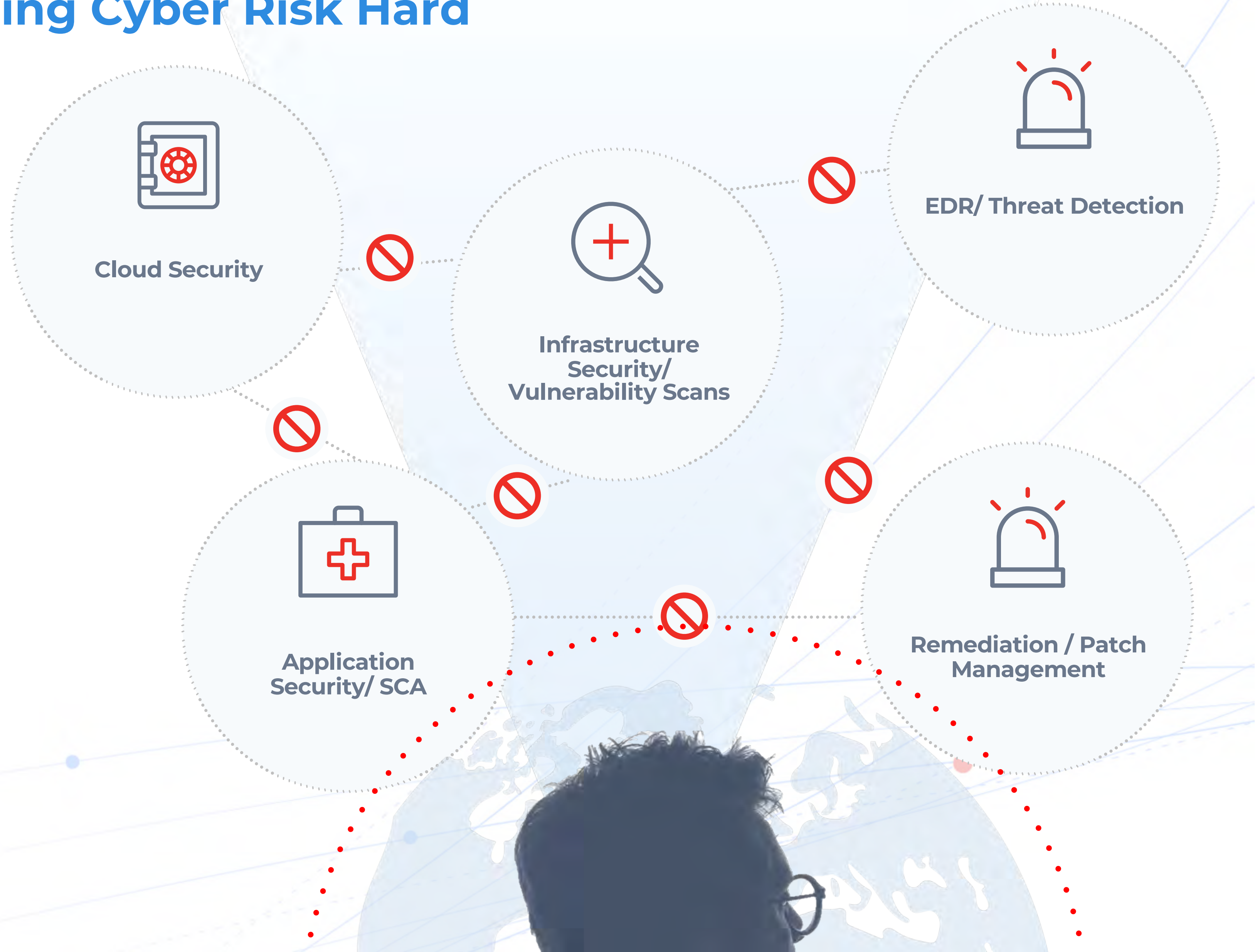
Too Many Tools, Few Solutions

Silo'd Tools Make Managing Cyber Risk Hard

Too many tools – what do I trigger right action?

How do I eliminate the risk?

What is the prioritized risk elimination plan and tool for elimination?


Cloud Security
Infrastructure Security/ Vulnerability Scans
EDR/ Threat Detection
Application Security/ SCA
Remediation / Patch Management

Top Exploited Vulnerabilities Are Not 0-days

Patching Hygiene Continues to be a Problem

Attackers continue to **exploit old vulnerabilities**

...and these vulnerabilities **remain unpatched**

Top 10 Vulns Exploited by Threat Actors

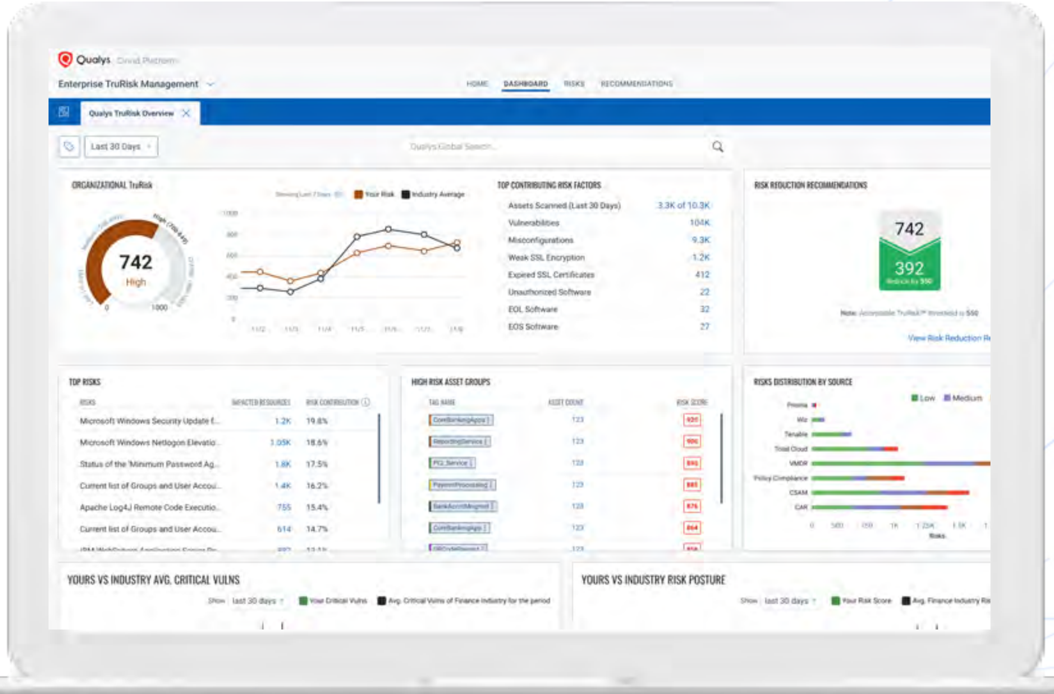
CVE-2017-0199
CVE-2017-11882
CVE-2012-0158
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-34473
CVE-2021-27065
CVE-2021-34523
CVE-2021-31207

30+ Days to remediate weaponized vulnerabilities

What Customers Are Asking For

Unified Risk View

- ✓ **Aggregate cyber risk** across **Qualys & Non-Qualys Products** (cloud, application, infrastructure, etc)
- ✓ Share a **common language to communicate cyber risk** to key stakeholders
- ✓ **Transition away** from difficult to manage in-house or expensive risk reporting tools
- ✓ Consolidate on **Qualys Cloud Platform for managing Cyber Risk**



TOP CONTRIBUTING RISK FACTORS

Assets Scanned (Last 30 Days)	3.3K of 10.3K
Vulnerabilities	104K
Misconfigurations	9.3K
Weak SSL Encryption	1.2K
Expired SSL Certificates	412
Unauthorized Software	22
EOL Software	32
EOS Software	27

TOP RISKS

RISKS	IMPACTED RESOURCES	RISK CONTRIBUTION
Microsoft Windows Security Update f...	1.2K	19.8%
Microsoft Windows Netlogon Elevatio...	1.05K	18.6%
Status of the 'Minimum Password Ag...	1.8K	17.5%
Current list of Groups and User Accou...	1.4K	16.2%
Apache Log4J Remote Code Executio...	755	15.4%
Current list of Groups and User Accou...	614	14.7%

HIGH RISK ASSET GROUPS

TAG NAME	ASSET COUNT	RISK SCORE
CoreBankingApps	123	920
ReportingService	123	906
PCI_Service	123	895
PaymentProcessing	123	885
[illegible]	123	876
CoreBankingApp	123	864

The Solution

Qualys.

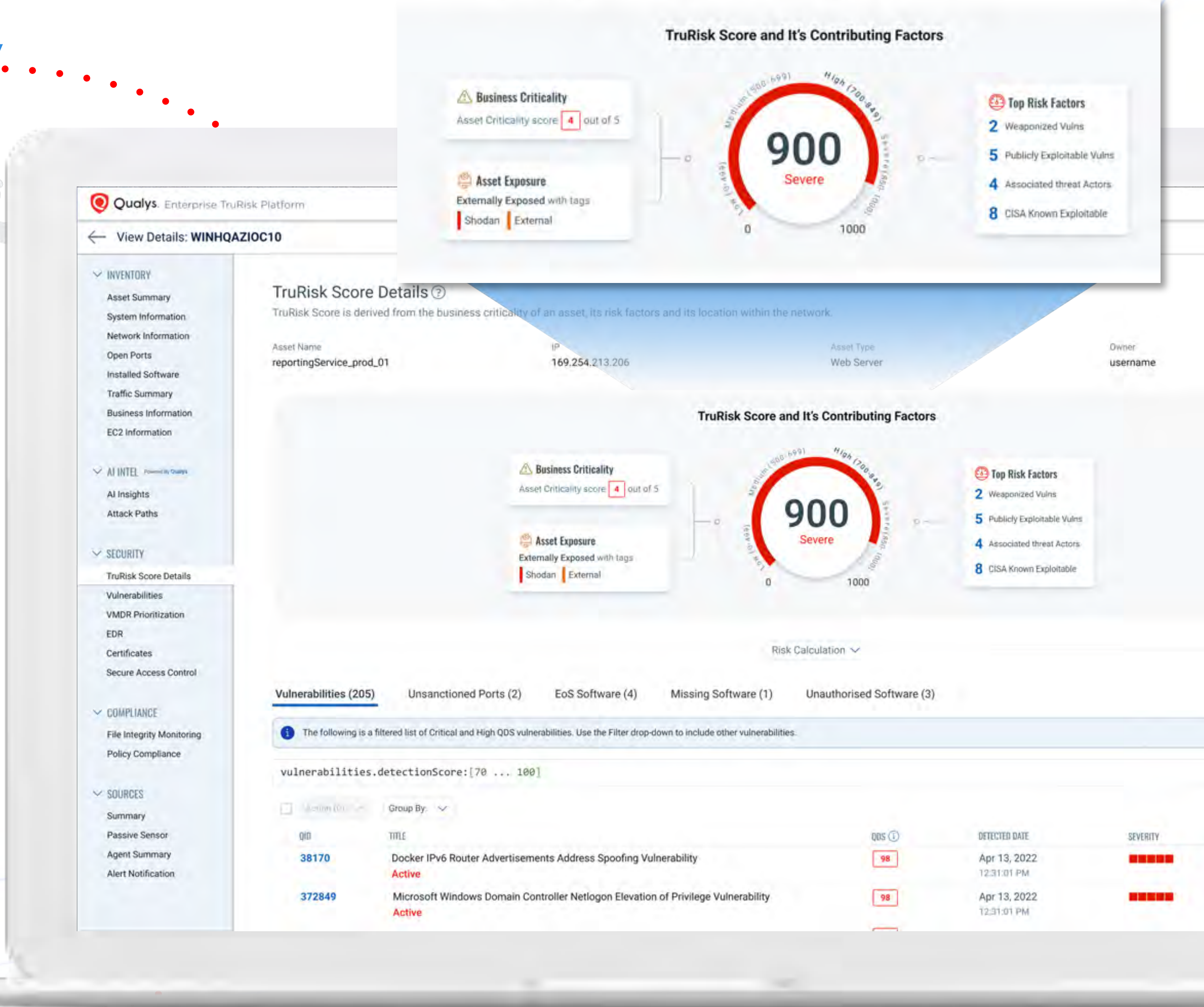
Manage Cyber Risk

Across the Enterprise Effectively

1. Measure Risk Across The EcoSystem

2. Communicate Cyber Risk in form of Intrinsic Business Value at Risk

3. Eliminate Risk



TruRisk Score and It's Contributing Factors

Business Criticality
Asset Criticality score 4 out of 5

Asset Exposure
Externally Exposed with tags
Shodan | External

Top Risk Factors
2 Weaponized Vulns
5 Publicly Exploitable Vulns
4 Associated threat Actors
8 CISA Known Exploitable

View Details: WINHQAZIOC10

TruRisk Score Details

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

Asset Name: reportingService_prod_01
IP: 169.254.213.206
Asset Type: Web Server
Owner: username

TruRisk Score and It's Contributing Factors

Business Criticality
Asset Criticality score 4 out of 5

Asset Exposure
Externally Exposed with tags
Shodan | External

900
Severe
0
1000

Top Risk Factors
2 Weaponized Vulns
5 Publicly Exploitable Vulns
4 Associated threat Actors
8 CISA Known Exploitable

The following is a filtered list of Critical and High QDS vulnerabilities. Use the Filter drop-down to include other vulnerabilities.

```
vulnerabilities.detectionScore:[70 ... 100]
```

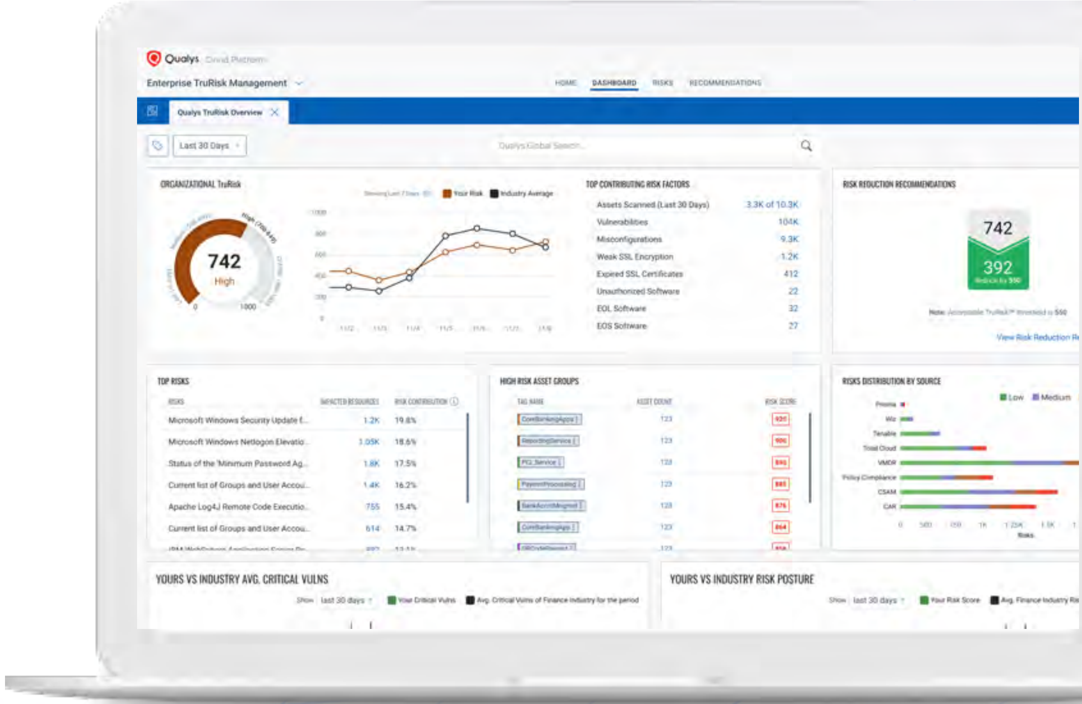
QID	TITLE	QDS	DETECTED DATE	SEVERITY
38170	Docker IPv6 Router Advertisements Address Spoofing Vulnerability Active	98	Apr 13, 2022 12:31:01 PM	■■■■■
372849	Microsoft Windows Domain Controller Netlogon Elevation of Privilege Vulnerability Active	98	Apr 13, 2022 12:31:01 PM	■■■■■

Qualys.

Aggregate All Risks

Unified Risk View

- ✓ **Single pane of glass view** for all risks across Qualys and Non-Qualys sources.
- ✓ **Search & Correlate Risk** by connecting the dots across multiple sources
- ✓ **Uniformly Score Risk** across risk findings from Qualys & Non-Qualys sources
- ✓ **Ingest Data** by using multiple sources. Connectors, APIs, Files and more



Enterprise TruRisk Management

Qualys TruRisk Overview

Last 30 Days

ORGANIZATIONAL TruRisk

742 High

TOP CONTRIBUTING RISK FACTORS

Assets Scanned (Last 30 Days)	3.3K of 10.3K
Vulnerabilities	104K
Misconfigurations	9.3K
Weak SSL Encryption	1.2K
Expired SSL Certificates	412
Unauthorized Software	22
EOL Software	32
EOS Software	27

RISK REDUCTION RECOMMENDATIONS

742

392

TOP RISKS

RISKS	IMPACTED RESOURCES	RISK CONTRIBUTION
Microsoft Windows Security Update f...	1.2K	19.8%
Microsoft Windows Netlogon Elevatio...	1.05K	18.6%
Status of the 'Minimum Password Ag...	1.8K	17.5%
Current list of Groups and User Accou...	1.4K	16.2%
Apache Log4J Remote Code Executio...	755	15.4%
Current list of Groups and User Accou...	614	14.7%

HIGH RISK ASSET GROUPS

TAG NAME	ASSET COUNT	RISK SCORE
CoreBankingApps	123	931
ReportingService	123	906
PCI_Service	123	891
PaymentProcessing	123	885
BankAcctMngmt	123	876
CoreBankingApps	123	864

RISKS DISTRIBUTION BY SOURCE

YOURS VS INDUSTRY AVG. CRITICAL VULNS

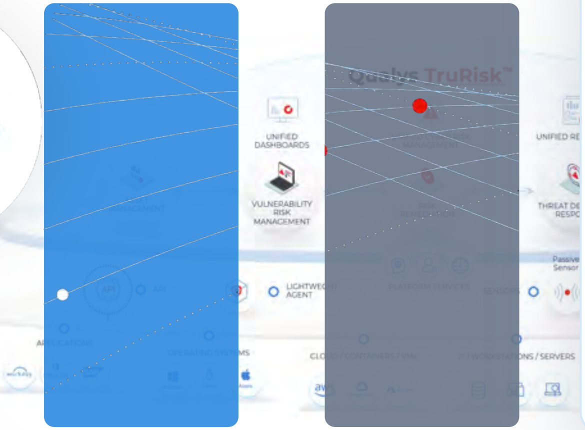
YOURS VS INDUSTRY RISK POSTURE

Measuring TruRisk Across Eco-System

Normalyze
VERACODE
SYNOPSYS
snyk
Microsoft Defender For Endpoint
Security Scorecard
SentinelOne
asimily
IBM X-Force Red
WIZ
SafeBreach

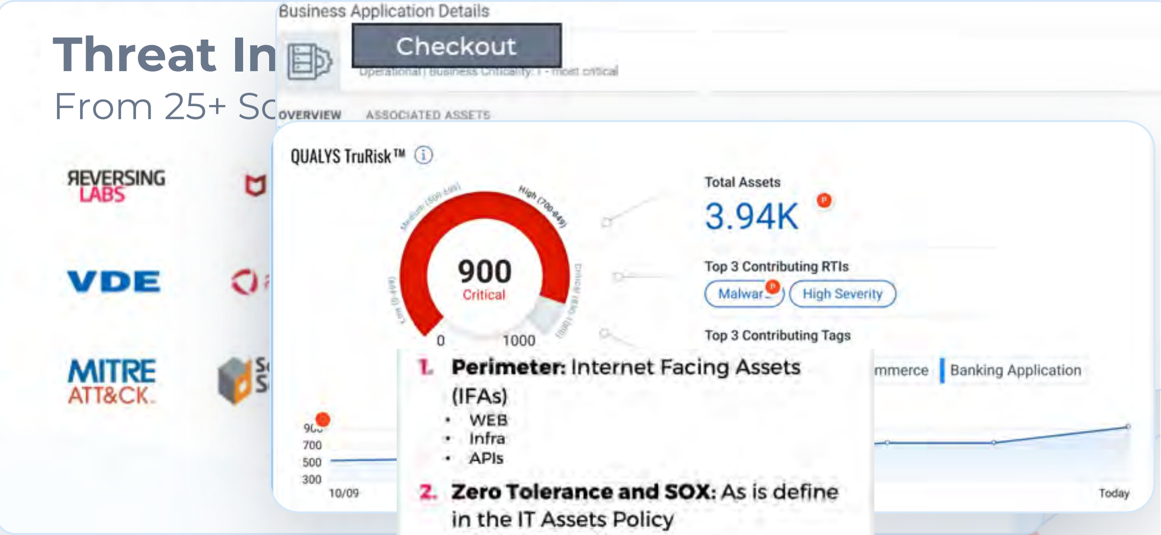
The Qualys Solution set

- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
- Policy Compliance (PC)
- ...and more



Normalization

Correlation



1. **Perimeter:** Internet Facing Assets (IFAs)
   - WEB
   - Infra
   - APIs
2. **Zero Tolerance and SOX:** As is define in the IT Assets Policy
   - DMZ (Front, Back)
   - Authentication (AD, ADFS, LDAP)
   - Payment and Cards Systems
   - AML
   - CSNET
   - SOX Systems
3. **Workstations**
4. **Internals:** Any other Server/infra in the internal network

Context

1. **Ransomware:**
   CVEs related to vulnera
2. **Dark Web chatter:**
   CVEs related to your in
3. **Known Malware:**
   CVEs exploited by by known threat actors

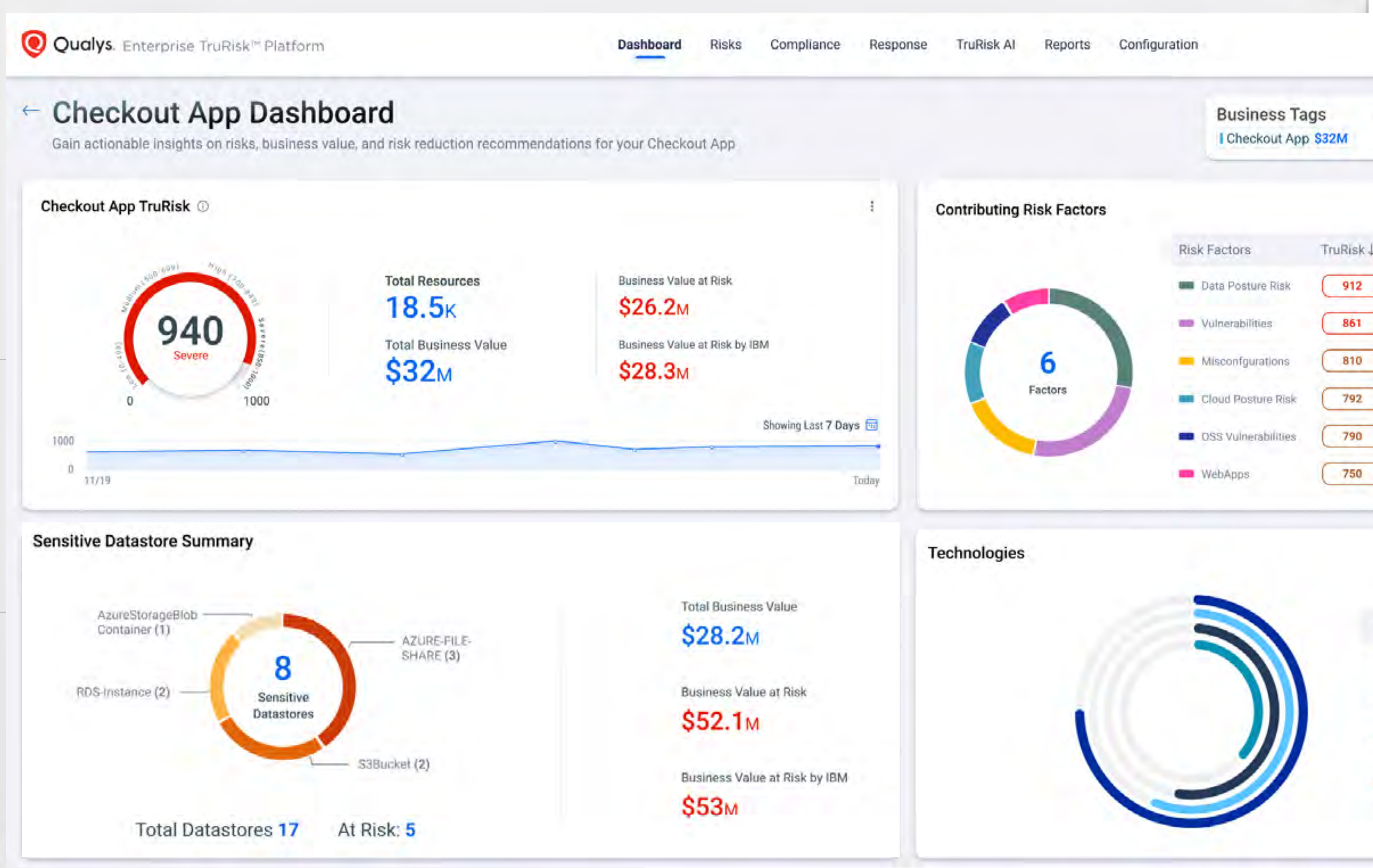
Communicate Cyber Risk

To All Stakeholders

1. Measure Risk Across The Ecosystem

2. **Communicate Cyber Risk in form of Intrinsic Business Value at Risk**

3. Eliminate Risk



Qualys. Enterprise TruRisk™ Platform

Checkout App Dashboard

Gain actionable insights on risks, business value, and risk reduction recommendations for your Checkout App

Business Tags

Checkout App $32M

Checkout App TruRisk

940 Severe

Total Resources 18.5K

Total Business Value $32M

Business Value at Risk $26.2M

Business Value at Risk by IBM $28.3M

Showing Last 7 Days

Contributing Risk Factors

6 Factors

Risk Factors	TruRisk ↓
Data Posture Risk	912
Vulnerabilities	861
Misconfgurations	810
Cloud Posture Risk	792
OSS Vulnerabilities	790
WebApps	750

Sensitive Datastore Summary

8 Sensitive Datastores

Total Datastores 17 At Risk: 5

Total Business Value $28.2M

Business Value at Risk $52.1M

Business Value at Risk by IBM $53M

Technologies

Qualys.

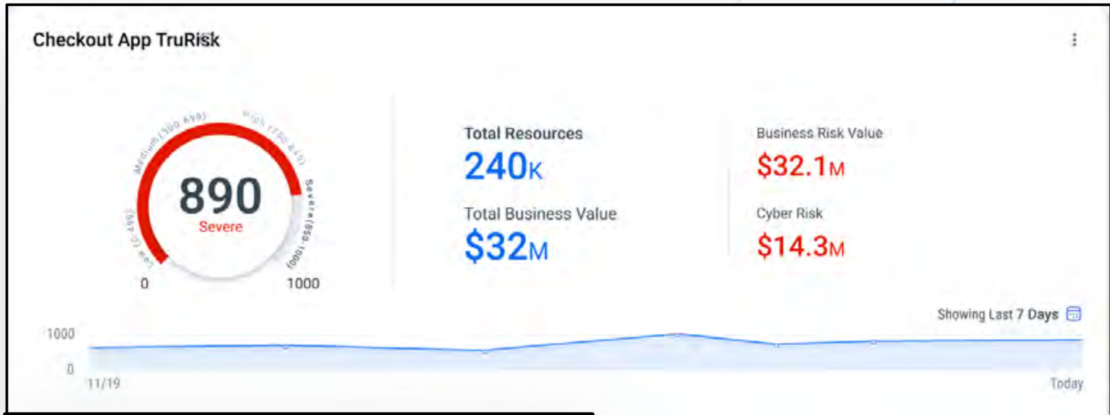
Communicate Risks

One TruRisk, Multiple Communication Paths

- ✓ **Define** Business value per Business app
  Quantify TruRisk with intrinsic value & loss due to risk & communicate risk to the board, execs

- ✓ **Compare Risk** across business units, peers , geos. Demonstrate the key Risk Factors and their financial impact due to risk

- ✓ **Customize Risk per your GRC definitions**
  Adjust the risk to your organizations needs before communicating it to the teams



Checkout App TruRisk

890 Severe

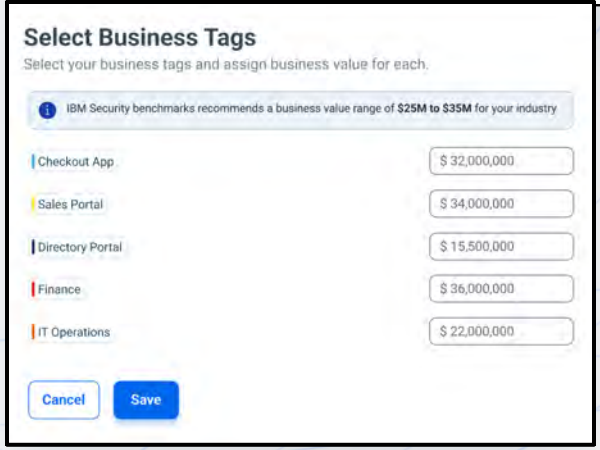
Total Resources 240K

Total Business Value $32M

Business Risk Value $32.1M

Cyber Risk $14.3M

Showing Last 7 Days



Select Business Tags

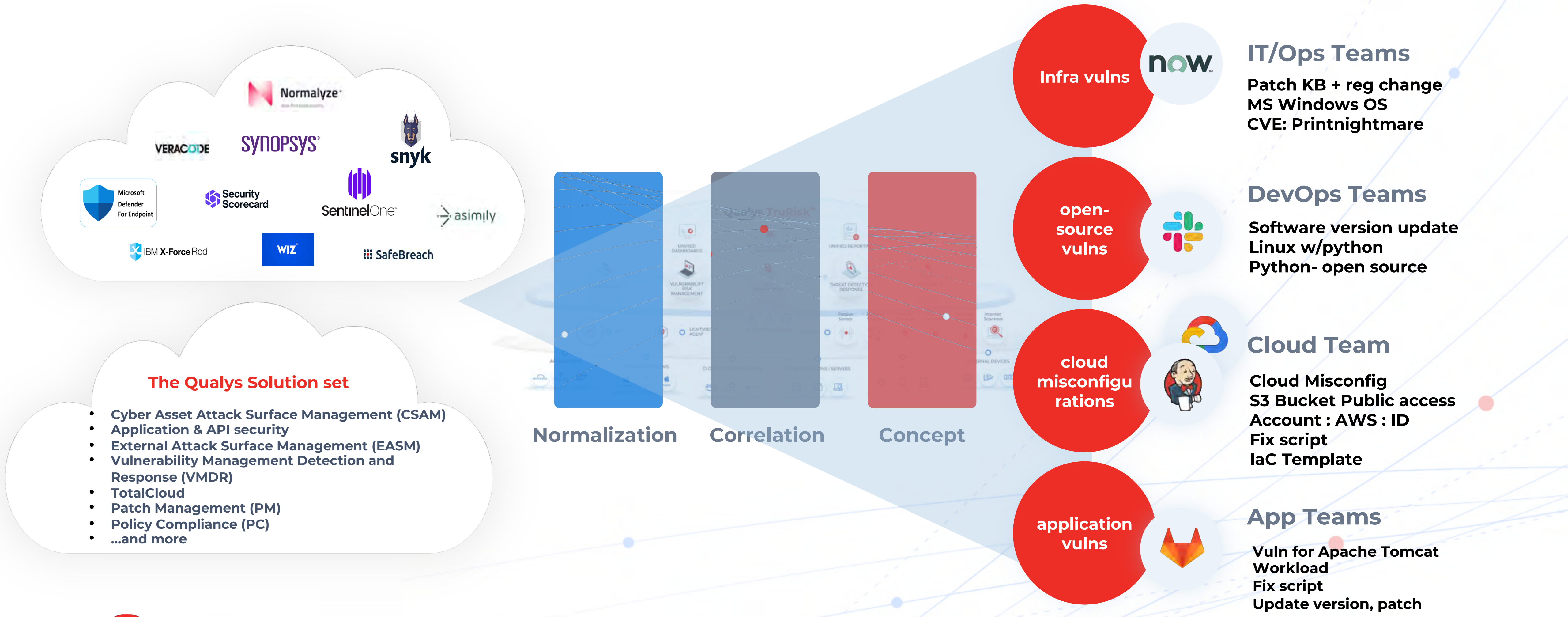
Select your business tags and assign business value for each.

IBM Security benchmarks recommends a business value range of **$25M to $35M** for your industry

Checkout App	$ 32,000,000
Sales Portal	$ 34,000,000
Directory Portal	$ 15,500,000
Finance	$ 36,000,000
IT Operations	$ 22,000,000

Communicating TruRisk

Right Data, with Right Context to Right team



The Qualys Solution set

- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
- Policy Compliance (PC)
- …and more

IT/Ops Teams

Patch KB + reg change
MS Windows OS
CVE: Printnightmare

DevOps Teams

Software version update
Linux w/python
Python- open source

Cloud Team

Cloud Misconfig
S3 Bucket Public access
Account : AWS : ID
Fix script
IaC Template

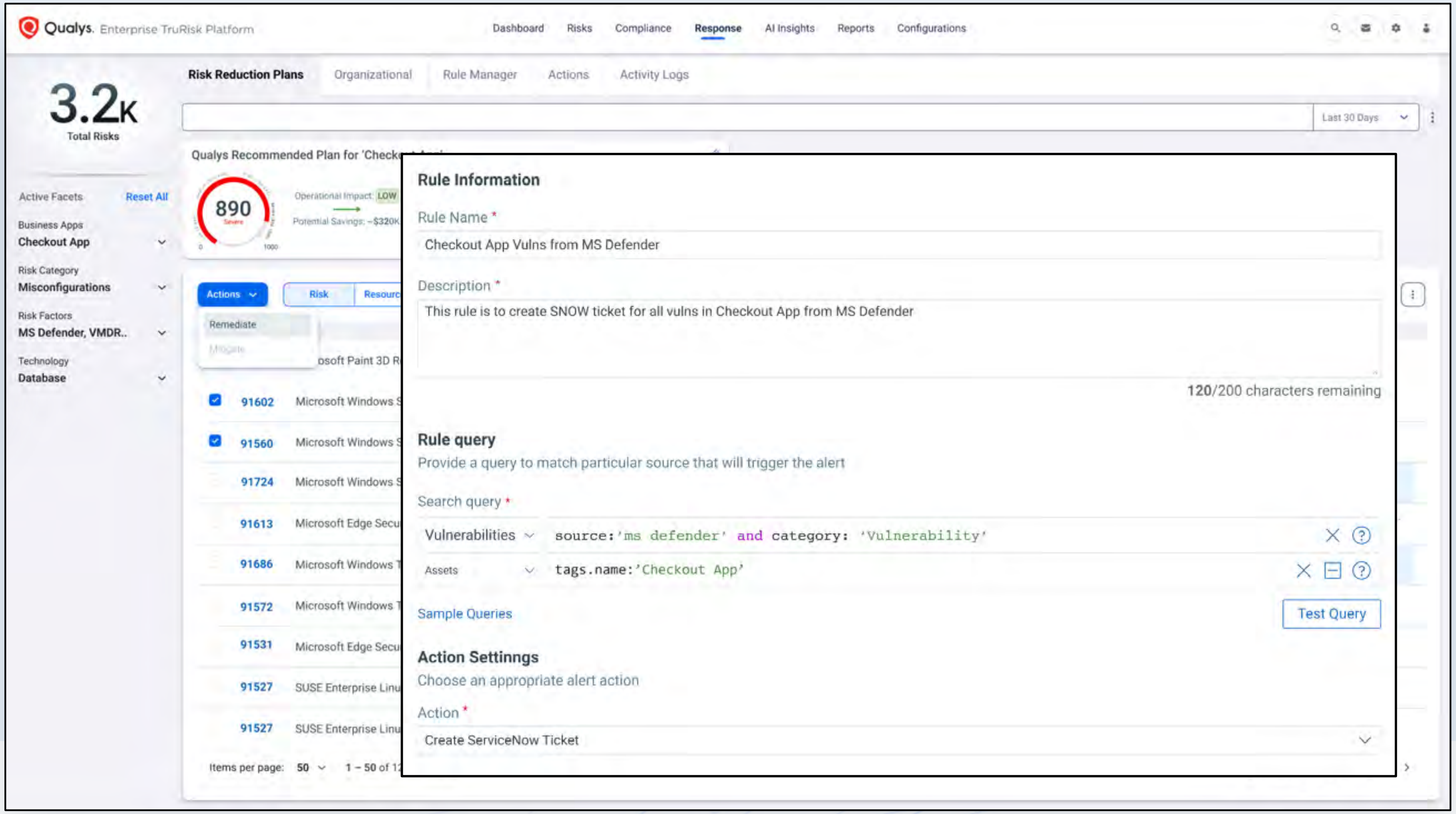
App Teams

Vuln for Apache Tomcat
Workload
Fix script
Update version, patch

Qualys.

Communicating TruRisk... in Language of IT Operations

Communicate non-Qualys risks factors with TruRisk as tickets to IT teams from certified, trusted Qualys platform, saving time & efforts



Business Apps: Checkout App

Risk Category: Misconfigurations

Risk Factors: MS Defender, VMDR..

Technology: Database

osoft Paint 3D R

☑	91602	Microsoft Windows S
☑	91560	Microsoft Windows S
	91724	Microsoft Windows S
	91613	Microsoft Edge Secu
	91686	Microsoft Windows T
	91572	Microsoft Windows T
	91531	Microsoft Edge Secu
	91527	SUSE Enterprise Linu
	91527	SUSE Enterprise Linu

Rule Information

Rule Name *

Checkout App Vulns from MS Defender

Description *

This rule is to create SNOW ticket for all vulns in Checkout App from MS Defender

120/200 characters remaining

Rule query

Provide a query to match particular source that will trigger the alert

Search query *

Vulnerabilities
```
source:'ms defender' and category: 'Vulnerability'
```

Assets
```
tags.name:'Checkout App'
```

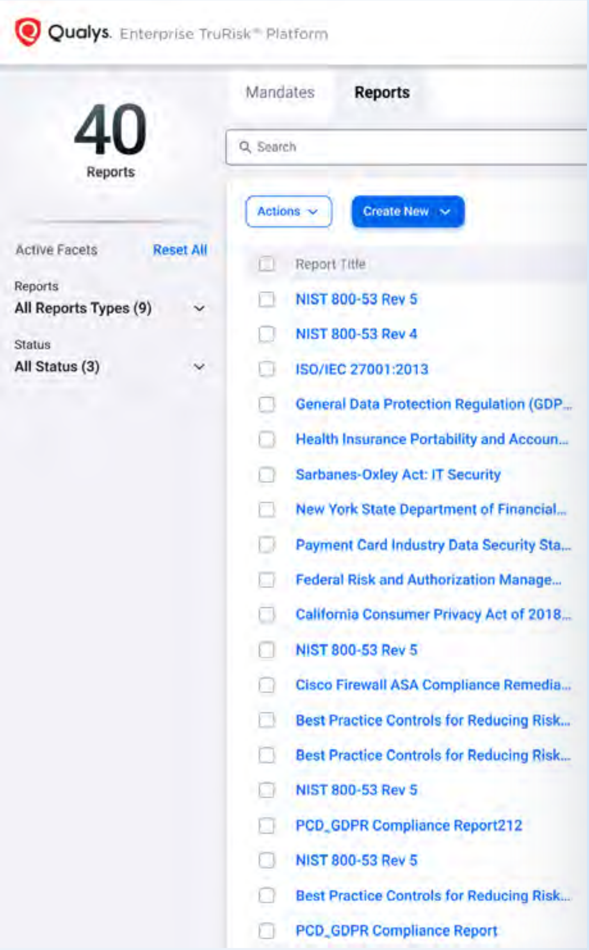
Action Settinngs

Choose an appropriate alert action

Action *

Create ServiceNow Ticket

Communicating TruRisk... in Language of Compliance



Qualys. Enterprise TruRisk™ Platform

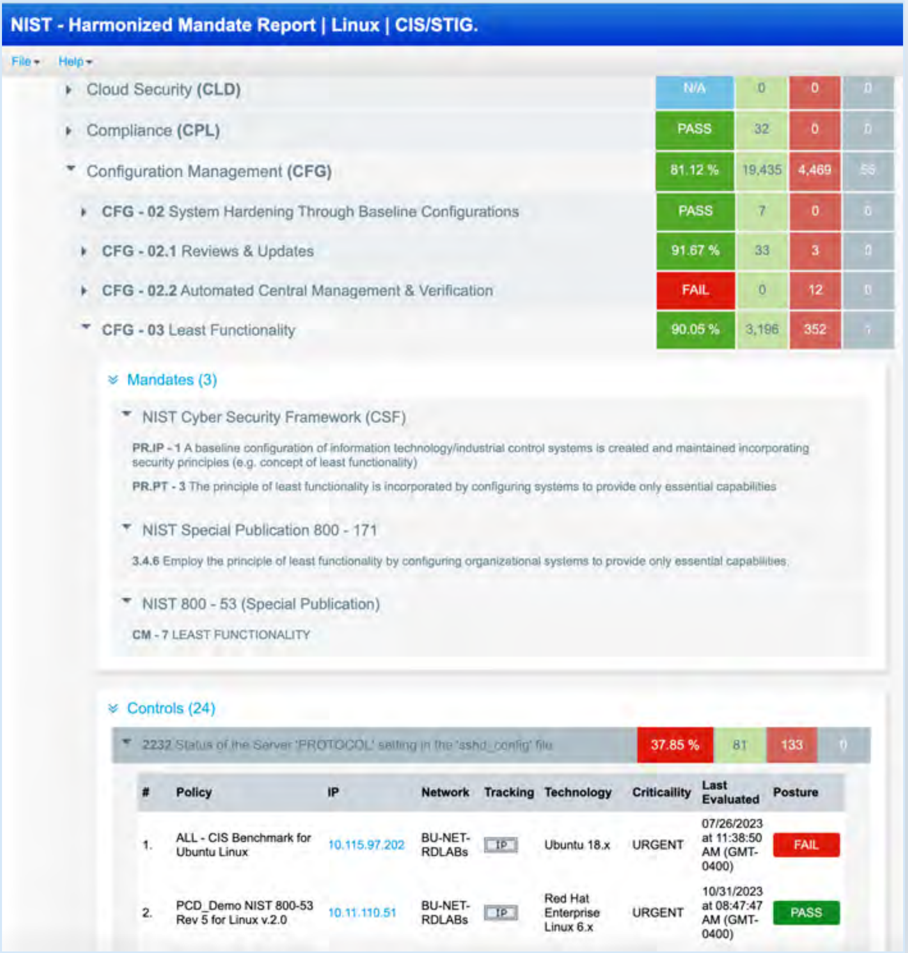
40

Reports

Reports: All Reports Types (9)

Status: All Status (3)

☐	Report Title
☐	NIST 800-53 Rev 5
☐	NIST 800-53 Rev 4
☐	ISO/IEC 27001:2013
☐	General Data Protection Regulation (GDP...
☐	Health Insurance Portability and Accoun...
☐	Sarbanes-Oxley Act: IT Security
☐	New York State Department of Financial...
☐	Payment Card Industry Data Security Sta...
☐	Federal Risk and Authorization Manage...
☐	California Consumer Privacy Act of 2018...
☐	NIST 800-53 Rev 5
☐	Cisco Firewall ASA Compliance Remedia...
☐	Best Practice Controls for Reducing Risk...
☐	Best Practice Controls for Reducing Risk...
☐	NIST 800-53 Rev 5
☐	PCD_GDPR Compliance Report212
☐	NIST 800-53 Rev 5
☐	Best Practice Controls for Reducing Risk...
☐	PCD_GDPR Compliance Report



NIST - Harmonized Mandate Report | Linux | CIS/STIG.

Cloud Security **(CLD)**	N/A	0	0	0
Compliance **(CPL)**	PASS	32	0	0
Configuration Management **(CFG)**	81.12 %	19,435	4,469	55
CFG - 02 System Hardening Through Baseline Configurations	PASS	7	0	0
CFG - 02.1 Reviews & Updates	91.67 %	33	3	0
CFG - 02.2 Automated Central Management & Verification	FAIL	0	12	0
CFG - 03 Least Functionality	90.05 %	3,196	352	1

Mandates (3)

NIST Cyber Security Framework (CSF)

PR.IP - 1 A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

PR.PT - 3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST Special Publication 800 - 171

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

NIST 800 - 53 (Special Publication)

CM - 7 LEAST FUNCTIONALITY

Controls (24)

2232 Status of the Server 'PROTOCOL' setting in the 'sshd_config' file	37.85 %	81	133	0

#	Policy	IP	Network	Tracking	Technology	Criticality	Last Evaluated	Posture
1.	ALL - CIS Benchmark for Ubuntu Linux	10.115.97.202	BU-NET-RDLABs	IP	Ubuntu 18.x	URGENT	07/26/2023 at 11:38:50 AM (GMT-0400)	FAIL
2.	PCD_Demo NIST 800-53 Rev 5 for Linux v.2.0	10.11.110.51	BU-NET-RDLABs	IP	Red Hat Enterprise Linux 6.x	URGENT	10/31/2023 at 08:47:47 AM (GMT-0400)	PASS

Communicate Aggregated Risk Factors (Qualys + non-Qualys) for **Comprehensive Compliance Reporting**

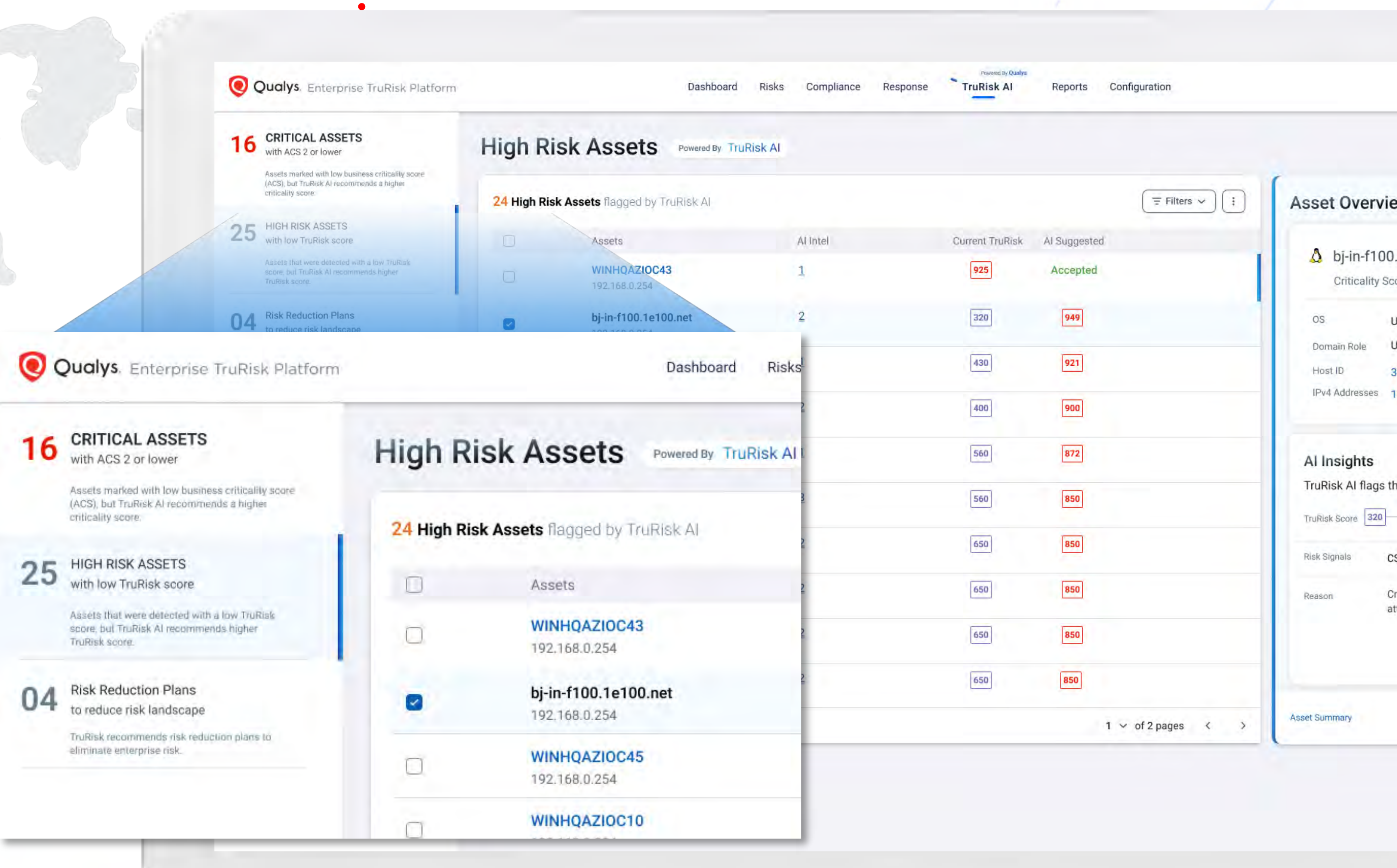
Manage & Reduce Cyber Risk

Go Beyond Patching Alone

1. Measure Risk Across The Ecosystem

2. Communicate Cyber Risk in form of Intrinsic Business Value at Risk

3. Eliminate Risk



Qualys. Enterprise TruRisk Platform

Dashboard | Risks | Compliance | Response | Powered By Qualys TruRisk AI | Reports | Configuration

16 CRITICAL ASSETS with ACS 2 or lower

Assets marked with low business criticality score (ACS), but TruRisk AI recommends a higher criticality score.

25 HIGH RISK ASSETS with low TruRisk score

Assets that were detected with a low TruRisk score, but TruRisk AI recommends higher TruRisk score.

04 Risk Reduction Plans to reduce risk landscape

TruRisk recommends risk reduction plans to eliminate enterprise risk.

High Risk Assets Powered By TruRisk AI

24 High Risk Assets flagged by TruRisk AI

Filters

☐	Assets	AI Intel	Current TruRisk	AI Suggested
☐	WINHQAZIOC43 192.168.0.254	1	925	Accepted
☑	bj-in-f100.1e100.net 192.168.0.254	2	320	949
☐	WINHQAZIOC45 192.168.0.254		430	921
☐	WINHQAZIOC10	2	400	900
			560	872
		3	560	850
		2	650	850
		2	650	850
		2	650	850
		2	650	850

1 of 2 pages

Asset Overvie

bj-in-f100.

Criticality Sco

OS U

Domain Role U

Host ID 3

IPv4 Addresses 1

AI Insights

TruRisk AI flags th

TruRisk Score 320

Risk Signals CS

Reason Cr at

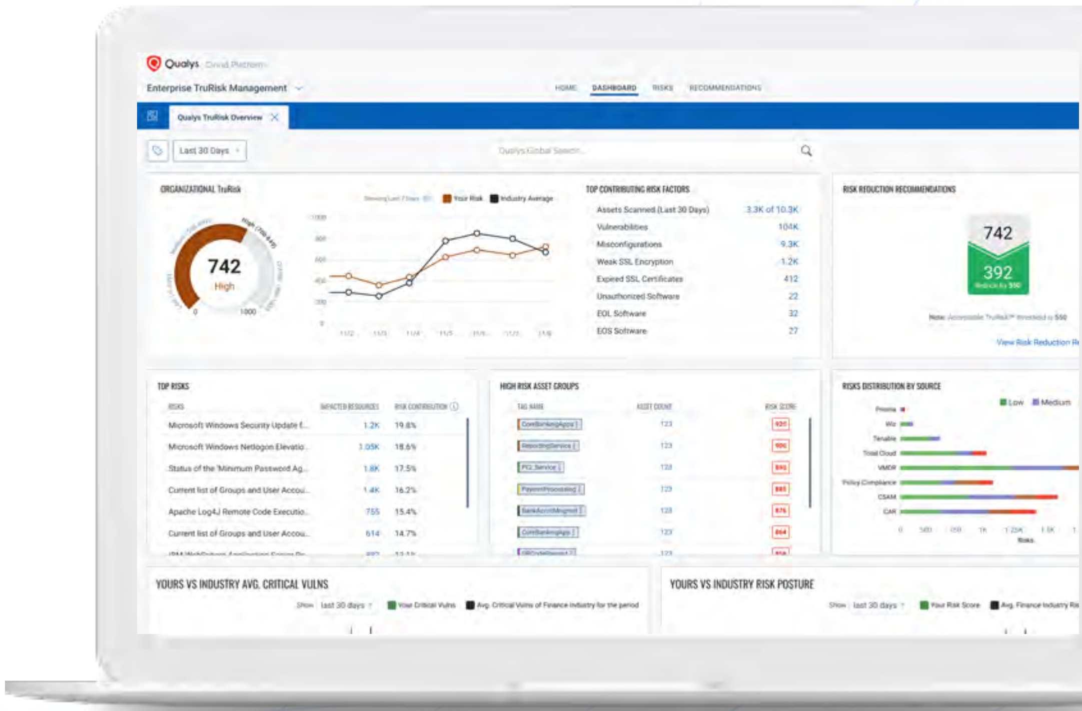
Asset Summary

Qualys.

Eliminate Risks

Balance Risk Reduction with Operational Impact

- ✓ **Reduce Time of Exposure** Identify Top Risks that will reduce the most risk across the organization, while balancing operational impact
- ✓ **Mitigate Risk.** Mitigate Risk that cannot be eliminated by leveraging compensating controls and mitigations from network, firewall & more.



TOP CONTRIBUTING RISK FACTORS

Assets Scanned (Last 30 Days)	3.3K of 10.3K
Vulnerabilities	104K
Misconfigurations	9.3K
Weak SSL Encryption	1.2K
Expired SSL Certificates	412
Unauthorized Software	22
EOL Software	32
EOS Software	27

TOP RISKS

RISKS	IMPACTED RESOURCES	RISK CONTRIBUTION
Microsoft Windows Security Update f...	1.2K	19.8%
Microsoft Windows Netlogon Elevatio...	1.05K	18.6%
Status of the 'Minimum Password Ag...	1.8K	17.5%
Current list of Groups and User Accou...	1.4K	16.2%
Apache Log4J Remote Code Executio...	755	15.4%
Current list of Groups and User Accou...	614	14.7%

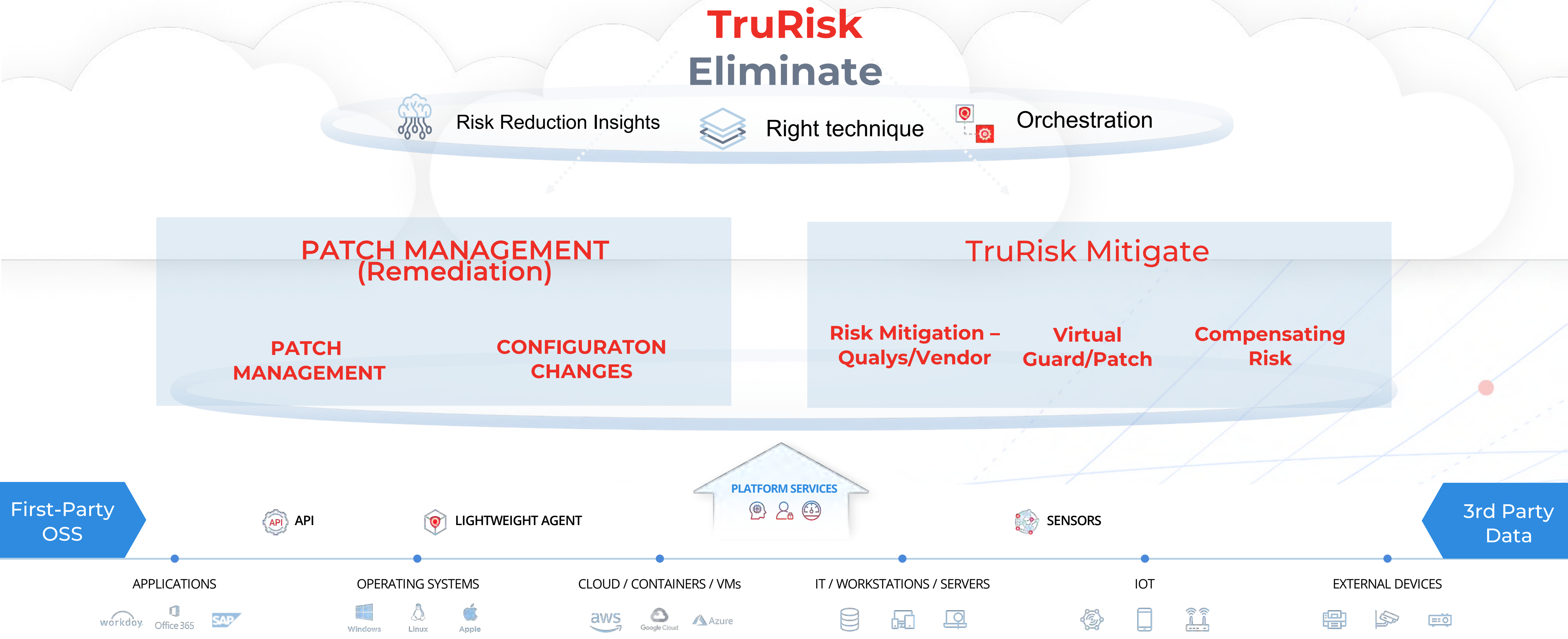
HIGH RISK ASSET GROUPS

TAG NAME	ASSET COUNT	RISK SCORE
CoreBankingApps	123	920
ReportingService	123	906
PCI_Service	123	890
PaymentProcessing	123	885
BankAcctMngmt	123	876
CoreBankingApps	123	864

Qualys.

TruRisk Eliminate

Remediate, Mitigate, Compensate, Virtually Guard



TruRisk Eliminate

Risk Reduction Insights

Right technique

Orchestration

PATCH MANAGEMENT (Remediation)

PATCH MANAGEMENT

CONFIGURATON CHANGES

TruRisk Mitigate

Risk Mitigation – Qualys/Vendor

Virtual Guard/Patch

Compensating Risk

First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

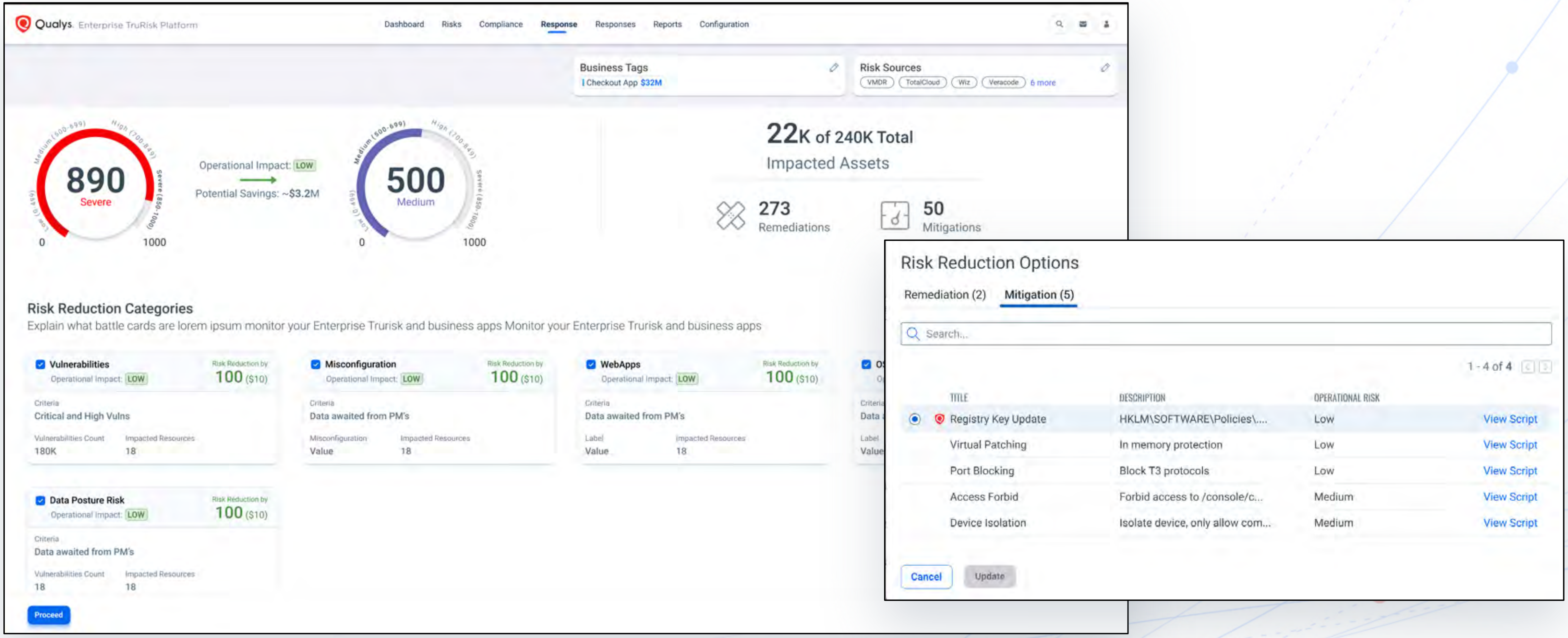
CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Eliminating Risk … with Techniques Beyond Patching, balancing Operational Impact



Business Tags

| Checkout App $32M

Risk Sources

VMDR TotalCloud Wiz Veracode 6 more

890 Severe

Operational Impact: LOW

Potential Savings: ~$3.2M

500 Medium

22K of 240K Total Impacted Assets

273 Remediations

50 Mitigations

Risk Reduction Categories

Explain what battle cards are lorem ipsum monitor your Enterprise Trurisk and business apps Monitor your Enterprise Trurisk and business apps

☑ Vulnerabilities — Operational Impact: LOW — Risk Reduction by 100 ($10)
Criteria: Critical and High Vulns
Vulnerabilities Count: 180K — Impacted Resources: 18

☑ Misconfiguration — Operational Impact: LOW — Risk Reduction by 100 ($10)
Criteria: Data awaited from PM's
Misconfiguration: Value — Impacted Resources: 18

☑ WebApps — Operational Impact: LOW — Risk Reduction by 100 ($10)
Criteria: Data awaited from PM's
Label: Value — Impacted Resources: 18

☑ O
Criteria: Data
Label: Value

☑ Data Posture Risk — Operational Impact: LOW — Risk Reduction by 100 ($10)
Criteria: Data awaited from PM's
Vulnerabilities Count: 18 — Impacted Resources: 18

Risk Reduction Options

Remediation (2) | Mitigation (5)

Search...

1 - 4 of 4

	TITLE	DESCRIPTION	OPERATIONAL RISK	
●	Registry Key Update	HKLM\SOFTWARE\Policies\....	Low	View Script
	Virtual Patching	In memory protection	Low	View Script
	Port Blocking	Block T3 protocols	Low	View Script
	Access Forbid	Forbid access to /console/c...	Medium	View Script
	Device Isolation	Isolate device, only allow com...	Medium	View Script

Risk Mitigation, to Reduce Risk, Beyond Patching

Use Case #1 (IT Ops) - Patch

Traditional Patching Capabilities

1. Patching
2. Conf changes (ex. change regkey)

Use Case #2 (SecOps) - Mitigate

Immediate but Temporary Shield - Security Team doesn't want to "wait" while IT Ops Can Fix the Identified Issues

3. Uninstall (ex. BitTorrent)
4. Isolate device from network
5. Close ports (ex. port 21 FTP)
6. Stop services/processes
7. Specific script per vuln (vendor provided or Qualys provided)
8. Update cloud setting or call cloud function (ex. remove app from firewall, call Lambda)
9. In Memory updates (Live Kernel Patching)

Use Case #3 (SecOps) – Virtual Patching

For Critical Assets turn on "Focused" Threat Detection & Monitoring for Select Exposure

10. Memory and network protection
11. In Memory updates (Live Kernel Patching)
12. Stop services/processes

Use Case #4 (SecOps/ITOps)- Compensating control

Allow custom "fixes" where customer can write their own scripts/choose building blocks (ex. Registry keys, uninstalling software etc.)

13. Build your own script for remediation
14. Specific script per vuln (vendor provided or Qualys provided)

Sample of 107 Weaponized Vulns in 2022

Targeting Servers and Workstations

17 Vulns (16%)

Integrated & automated Remediation

3rd party software
Chrome/Firefox/Safari/Adobe

Functionality broken <1%

14 Vulns (13%)

Mitigated with Official Vendor Suggested Mitigations

Example: CVE-2022-24112, In `conf/config.yaml`, ensure `batch-requests` is disabled.

.

76 Vulns Left (71%)

Not easily patchable or mitigated

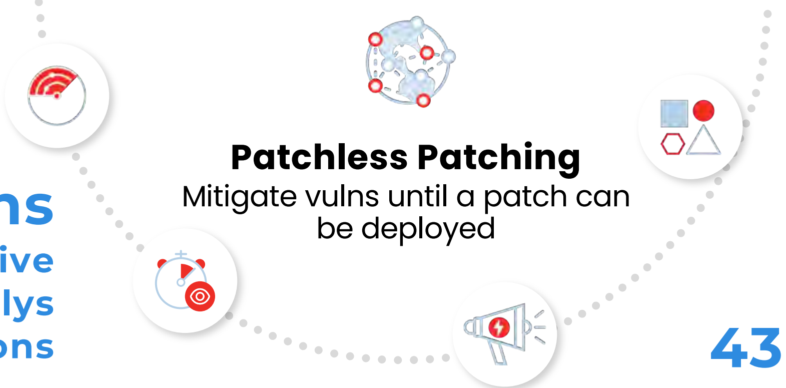
Requires Adaptive Mitigation, hybrid approach to mitigation

Adaptive Remediation

Adaptive Hybrid remediations to mitigate the risk of the remaining 76 vulnerabilities

Level (H): Higher operational risk (48%): Disable Lua scripting and Restart the Redis service.

Level (L): Lower operational risk (52%): Block or restrict access to TCP port 8732 , Disable the SCVMM integration



Patchless Patching

Mitigate vulns until a patch can be deployed

49 vulns

Adaptive Qualys mitigations

31 vulns

Memory protections

“Virtually patched” by memory guarding technology
Vuln example: Bluekeep

4 vulns

Kernel Virtual Patching

Use Linux kernel live patching technologies

43 vulns

Network protections

“Virtual protection” by (Blue Hexagon) AI/ML traffic-based analysis & blocking
Vuln example: Log4Shell

Risk of 100% of Vulnerabilities can be mitigated with Adaptive, Hybrid Remediation techniques

Qualys.

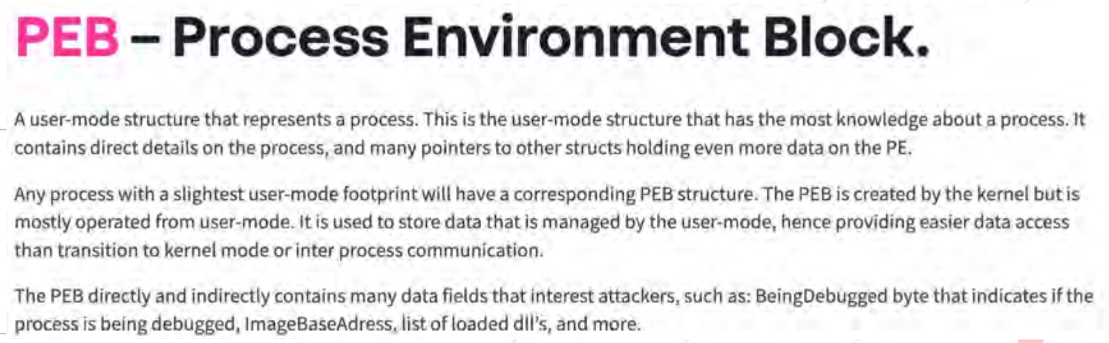
BlueKeep (CVE-2019-0708) – Memory Exploit Protection

- **Affects:** All Microsoft Windows Operating System

- **The Vulnerability:** BlueKeep is a remote code execution vulnerability that exists in Remote Desktop Services. BlueKeep is a pre-authentication USE-After-Free vulnerability and requires no user interaction to exploit.

- **Impact:** Complete control of the affected vulnerable system. No User Interaction Needed To Exploit

- **Solution:** With Qualys Cloud Agent Vulnerability Guard protection, out-of-the box prevent exploitation of such memory corruption vulnerabilities by encrypting data fields in Process Environment Block (PEB)



PEB – Process Environment Block.

A user-mode structure that represents a process. This is the user-mode structure that has the most knowledge about a process. It contains direct details on the process, and many pointers to other structs holding even more data on the PE.

Any process with a slightest user-mode footprint will have a corresponding PEB structure. The PEB is created by the kernel but is mostly operated from user-mode. It is used to store data that is managed by the user-mode, hence providing easier data access than transition to kernel mode or inter process communication.

The PEB directly and indirectly contains many data fields that interest attackers, such as: BeingDebugged byte that indicates if the process is being debugged, ImageBaseAdress, list of loaded dll's, and more.

Technology Partners

Measure, Communicate, and Eliminate Cyber Risk Effectively

Goal

Microsoft Defender For Endpoint

SYNOPSYS®

snyk

VERACODE

Security Scorecard

SentinelOne™

asimily

IBM X-Force Red

WIZ

SafeBreach

Demo

Qualys.

QSC23