Measure, Communicate & Eliminate Your Cyber Risk with Qualys Platform

Shailesh Athalye
Senior VP Product Management, Qualys

Indiana Jones

“It’s important… Trust me.”

Qualys.

Approach of ‘Indiana Jones’ of Cyber Risk

~~A systematic approach to de-risking their digital ecosystems~~

Security Teams

- Measure Cyber Risk
- Communicate Cyber Risk
- Eliminate Cyber Risk

Qualys.

Challenges

Challenge of Measuring Risk

Knowing Your Internal and External Attack Surface

CMDB != Inventory for Cyber Risk

- Lacks Comprehensiveness
- Lacks Cyber Risk context

35%

Unknown Assets but known your attackers!

20%

Assets Not Running AV/EDR

Lack of Business context, resulting in More work post VM, Risk assessment

45%

Of Critical Assets are Missing Business Criticality

80

Hours spent to make unknown asset, as managed, prioritizing risk for asset with low criticality

Qualys.

Challenges of Measuring Risk

Context for the 'Top 10' Risk Factors

- **Inability to collect data – Comprehensively & Accurately**
- **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'**

First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

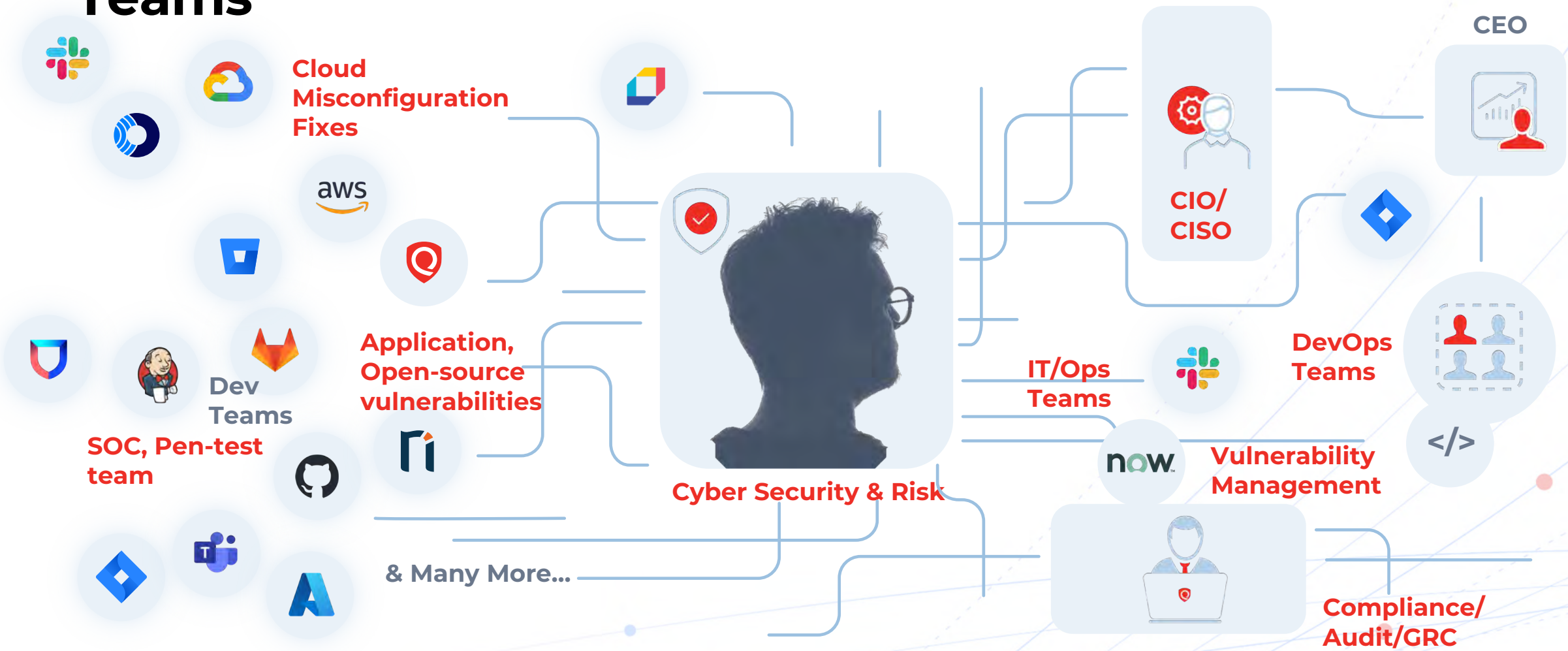
CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Challenge of Communicating Right Data to Right Teams



Qualys.

Challenges of Eliminating Risk

IT not Risk, based Elimination

Vulnerability Closure != Patch

IT/Ops needs ‘Exact Remediations’

Not knowing ‘Low hanging Fruits’, which won’t terrify IT teams, w/o uttering the word ‘automate’

48K
Patches from Microsoft, 10K from third parties

440K
All Vulnerabilities

128K
3rd Party Software on workstations

Chrome:	Firefox:	Adobe:	iTunes:
2647	2131	1530	613
(2008-2023)	(2003-2023)	(2004-2023)	(2005-2023)

Qualys.

Eliminating Risk – Problem of Whack-o-Mole Instead of Risk Prevention

Top Attacks of 2021, 2022 & 2023 have happened using Exploitable, Ransomware-Exploited or CISA catalogue provided vulnerabilities, not patched

Malware	Known CVEs	Known Misconfigurations
Conti	24	61
Darkside	04	54
Netwalker	08	03
Petya	10	06
REvil	24	27

Qualys.

The Solution

Qualys.

Qualys Enterprise TruRisk Platform

Qualys TruRisk™

Context of Threats | **Business Intelligence** | **Orchestration**

Internal & External Inventory Risk Management with Business Context

Detect, Prioritize vulnerabilities, Misconfigurations

Remediate vulns, misconfigs with Automation and intelligent workflows

Monitor, detect & respond & Prevent threats with Risk, business context

Drive compliance Monitoring, Reporting for Industry mandates, standards

First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Step 0 of Measuring Risk

Knowing Your Internal and External Attack Surface

1 Manage Inventory Risk with Cyber Risk & Business Context

External attack surface, EOL/EOS, Open-source, Unauthorized software, Absence of Security tooling

2 Simplifies & Fast-tracks Vulnerability & Inventory Programs

Continuous discovery, inventory risk meta-data for baselining CMDB, with complete VMDR with business context

Internal assets

Agent, Scanner, Sensors

IOT/OT assets

Passive Network Sensor

Assets from 3rd parties

API-Based Connectors

Active Directory

servicenow

bmc helix

vmware

External assets

Open-source Tech & Qualys Internet canner

SHODAN

Scanner

DNS

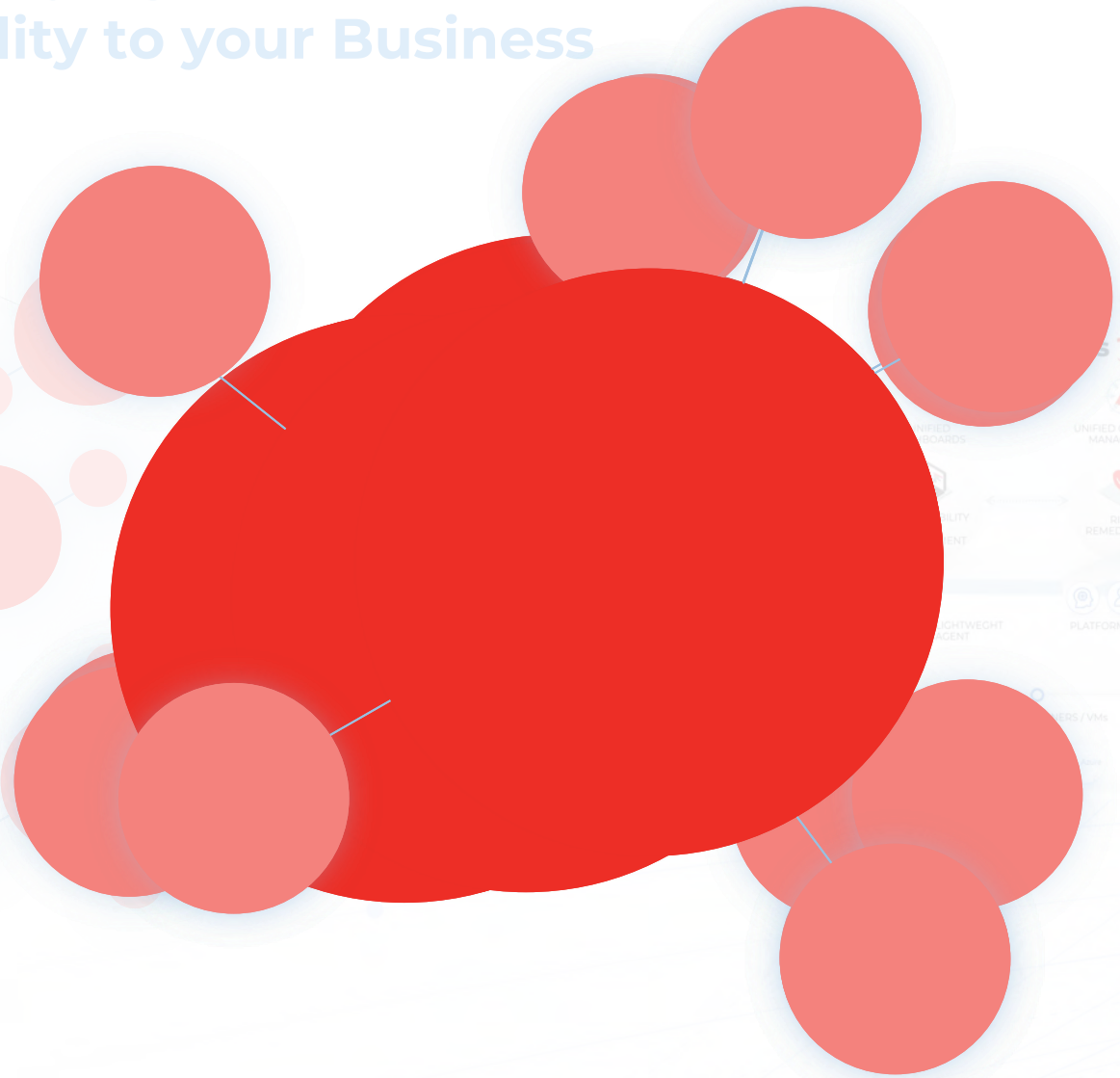
Whois

Identity for everyone

Qualys.

Measuring TruRisk

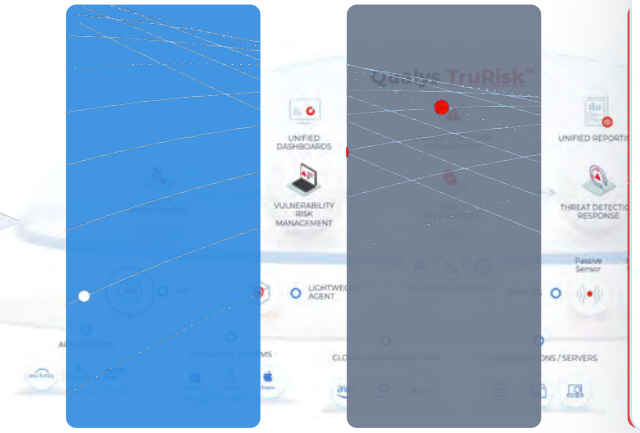
Collecting & Unifying Risk Factors, Correlated & Contextualized for Threats, Criticality to your Business



Qualys.

Measuring TruRisk

Collecting & Unifying Risk Factors, with Threat & Business Context



Normalization Correlation

Context

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

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
   - GSNET
   - SOX Systems
3. **Workstations**
4. **Internals:** Any other Server/infra in the internal network

Qualys.

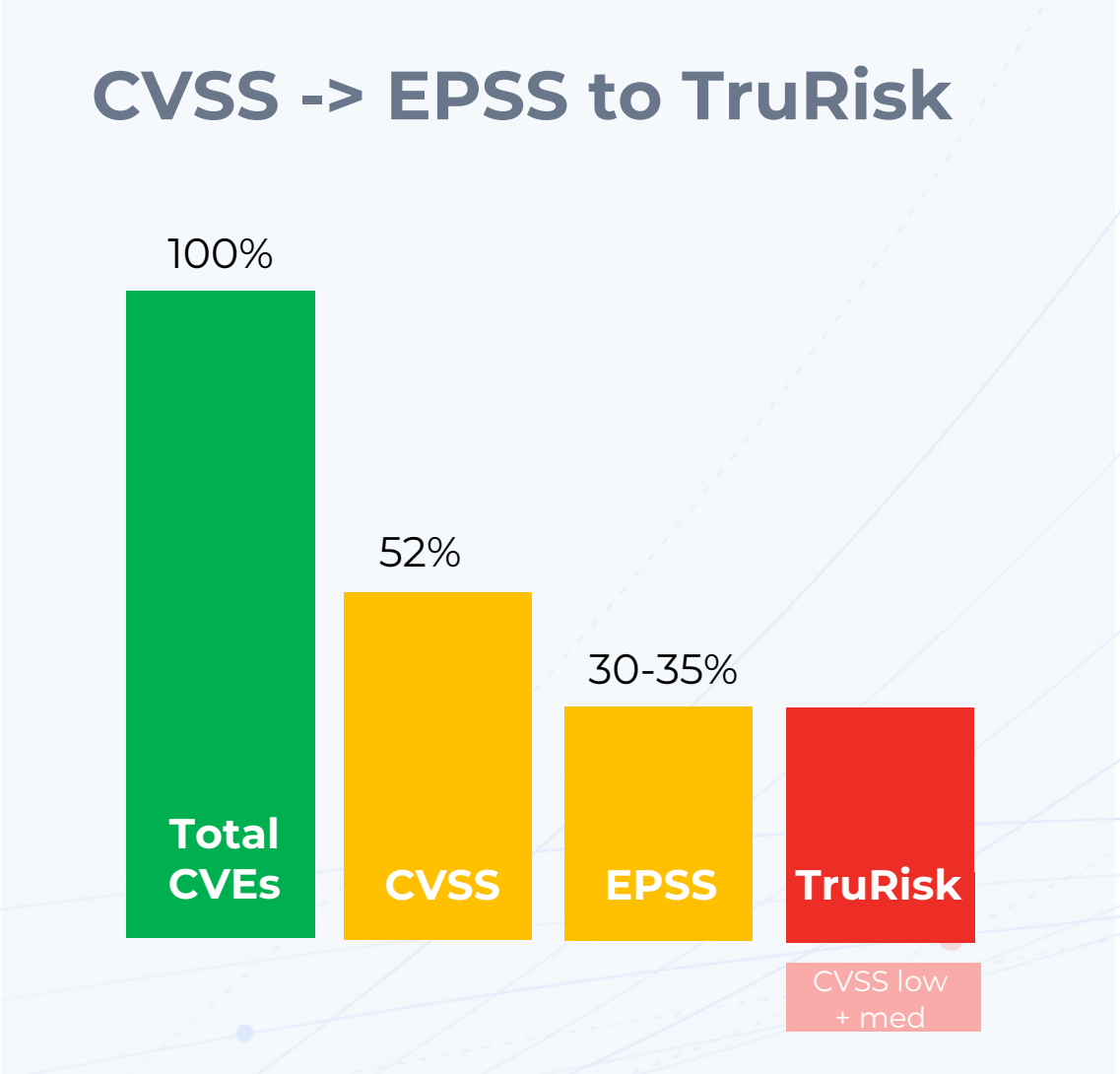
Outcome of Measuring TruRisk

Up to 85%

fewer vulnerabilities

~80%

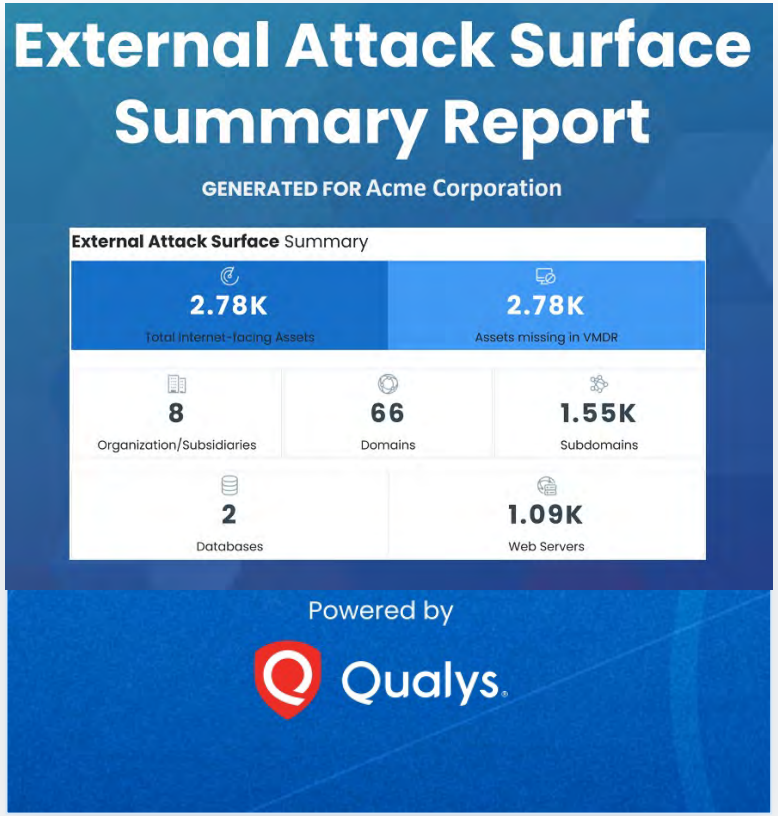
less ‘Ransomware’ vulnerabilities



Qualys.

Communicating Risk

Contextual Communication Per Persona/Responsibilities



Communicating to Executives

Unified, Quantified, Prioritized Cybersecurity Risk score

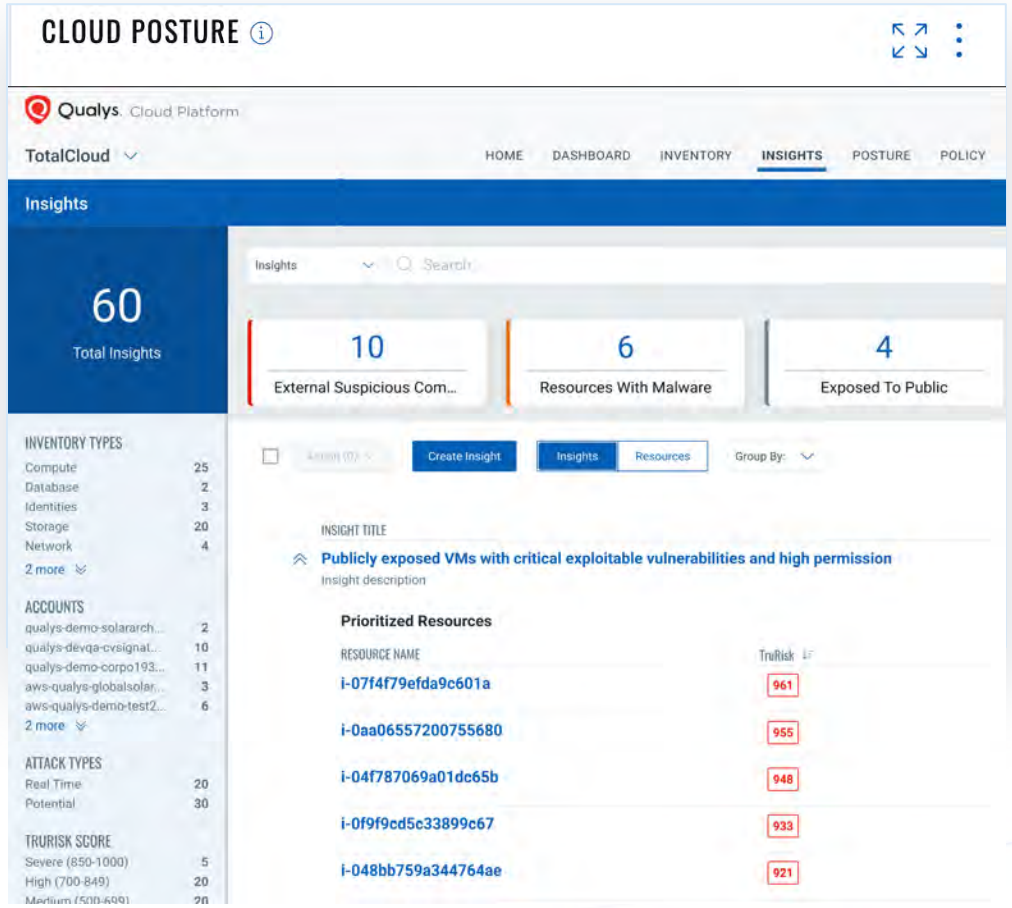
Talks Business language & Factors Contributing to Risk to Business
(which business critical app has highest risk)

Provides actionable recommendations to eliminate, reduce risk

Qualys.

Communicating Risk

Contextual Communication Per Persona/Responsibilities



Communicating to Risk Category Management

Actionable Views of Prioritized Risk Factors impacting Business Risk

Know in Detail – the dependencies impacting risk you are responsible with context of threats, priorities and trends

Qualys.

Communicating Risk

Contextual Communication Per Persona/Responsibilities

Communicating Risk to Threat & SOC Team

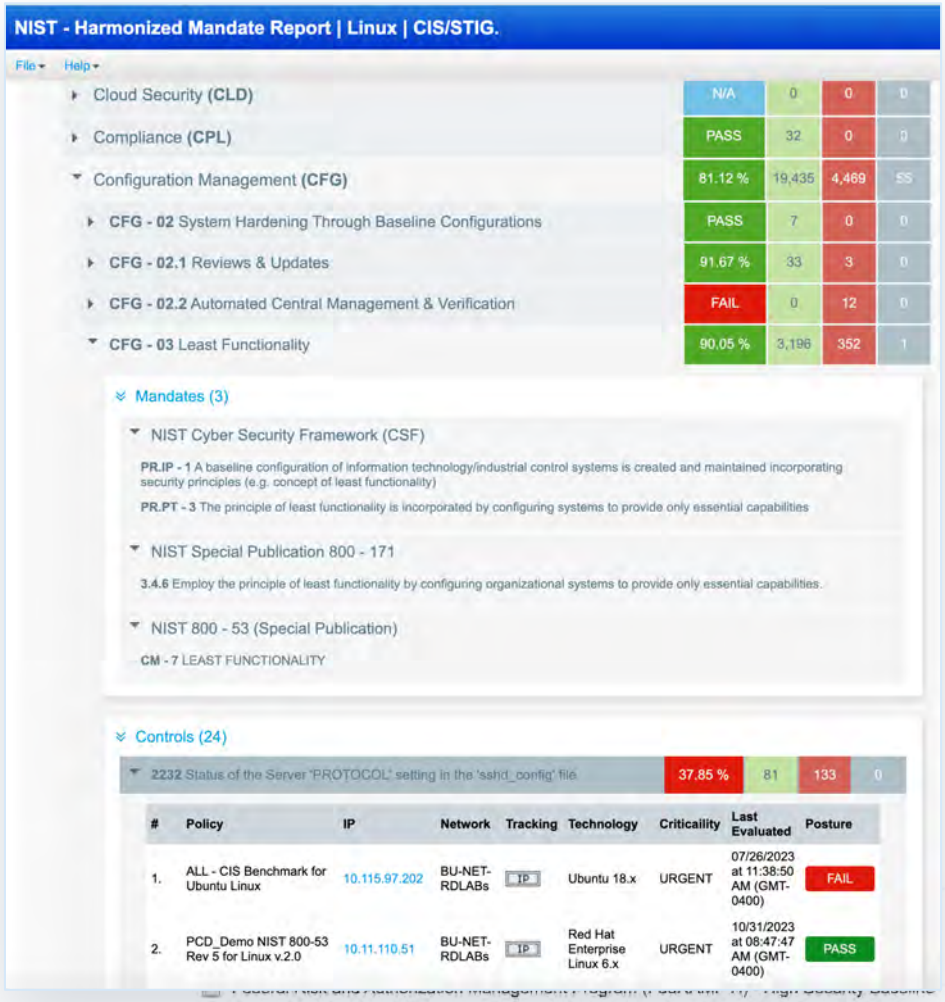
Proactively communicate TruRisk with risk indicators & business context to known Attack techniques reduce the risk of attacks

Prioritize security monitoring based on TruRisk

Qualys.

Communicate Compliance

Be-Audit Ready



Communicating to Audit/Compliance

Mapping of 50+ mandates, requirements to Qualys provided risk factors

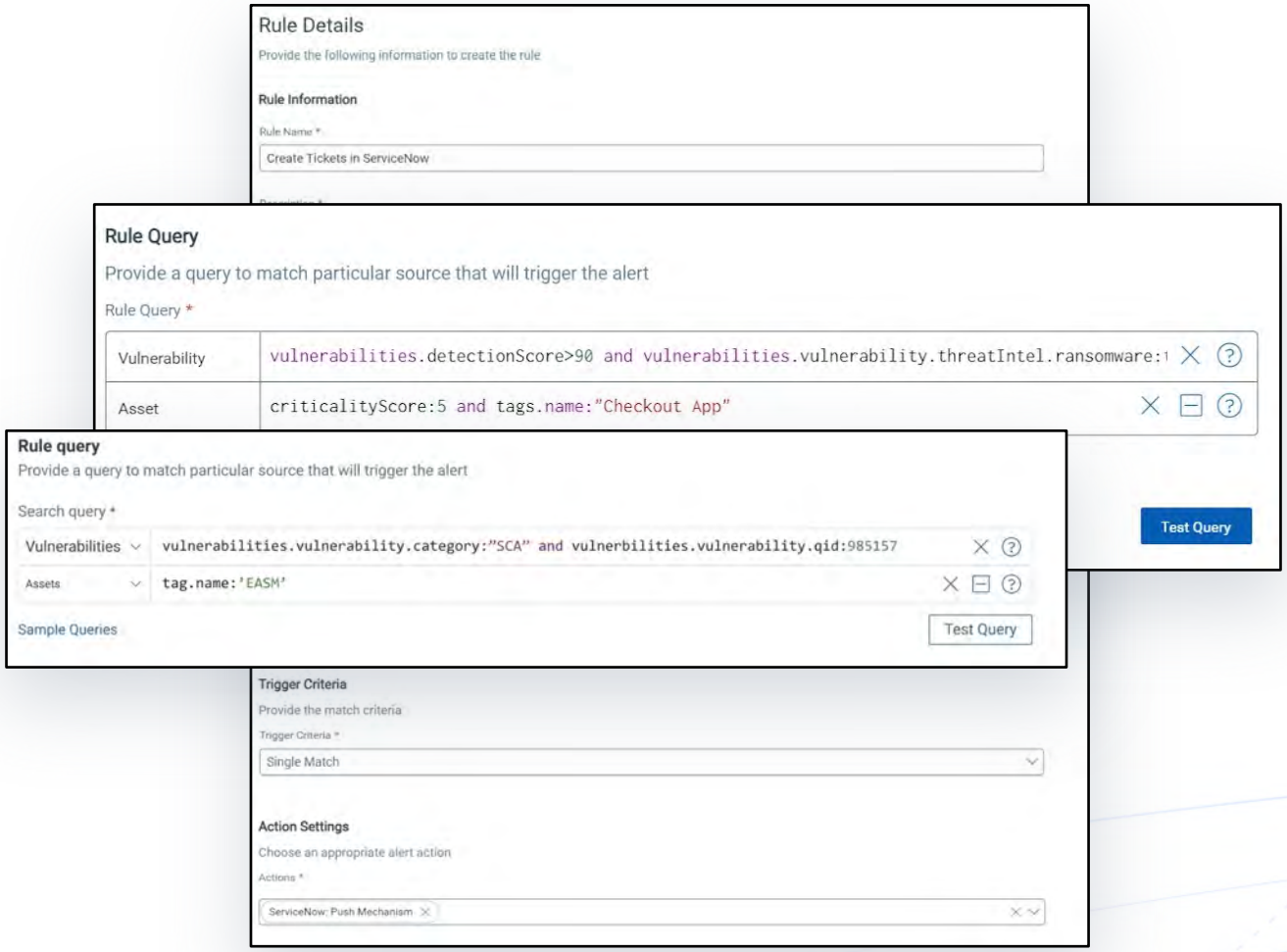
Talks the language of 'which compliance requirement' failing, why, which assets

Provide RBAC supported access or send tickets with context to compliance teams

Qualys.

Communicating Risk

Contextual Communication Per Persona/Responsibilities



Communicating to Teams to remediate

Auto ticketing to move beyond spreadsheets

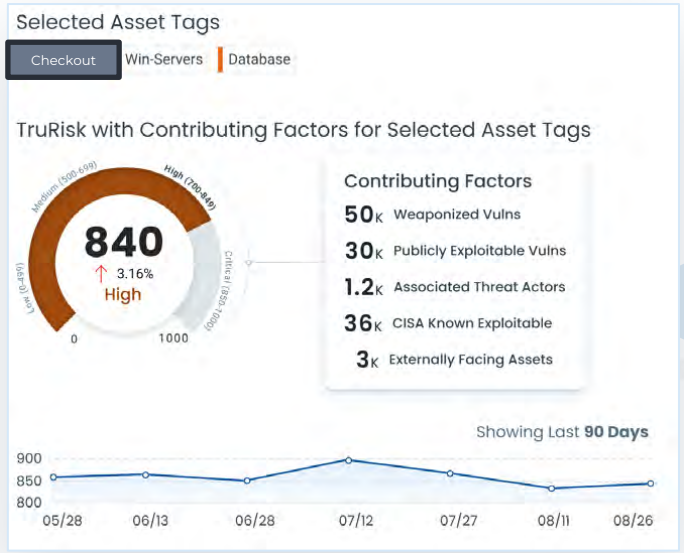
Rule-based ticketing, ownership assignment, and auto closure

Manage change approvals and deploy remediations directly from ITSM

Qualys.

Communicating TruRisk

Right Data, with Right Context to Right team



Infra vulns

IT/Ops Teams

Patch KB + reg change
MS Windows OS
CVE: Printnightmare

open-source vulns

DevOps Teams

Software version update
Linux w/python
Python- open source

cloud misconfigurations

Cloud Team

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

application vulns

App Teams

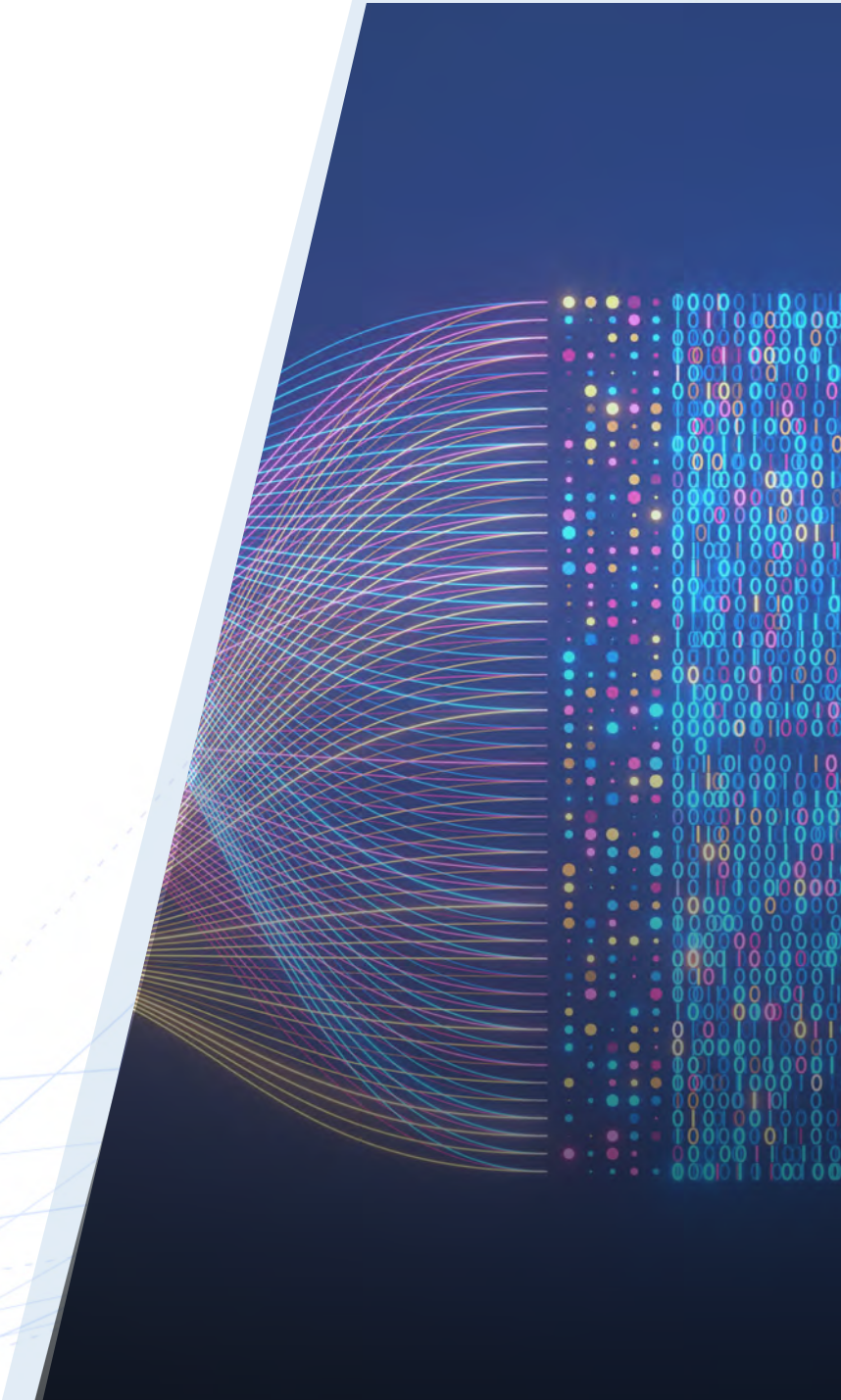
Vuln for Apache Tomcat
Workload
Fix script
Update version, patch

Qualys.

Eliminating Risk

Across Risk Factors

- Vulnerabilities
- Misconfigurations
- Unauthorized software
- Missing required software
- Open-source Vulnerabilities
- Infra Misconfigurations
- Sensitive data risks
- Technology debt risks
- Web application risks
- Emerging threats
- Endpoint Malicious activities
- Access control risks



Qualys.

Eliminating Risk

Risk-based Elimination, across Attack Surfaces, Risk Categories

Web App OWASP vulnerabilities

Malicious, suspicious Activities

Inventory Cyber Hygiene Risks

Cloud Misconfigurations

Infra/DB/Web Servers/ Middleware Misconfigurations

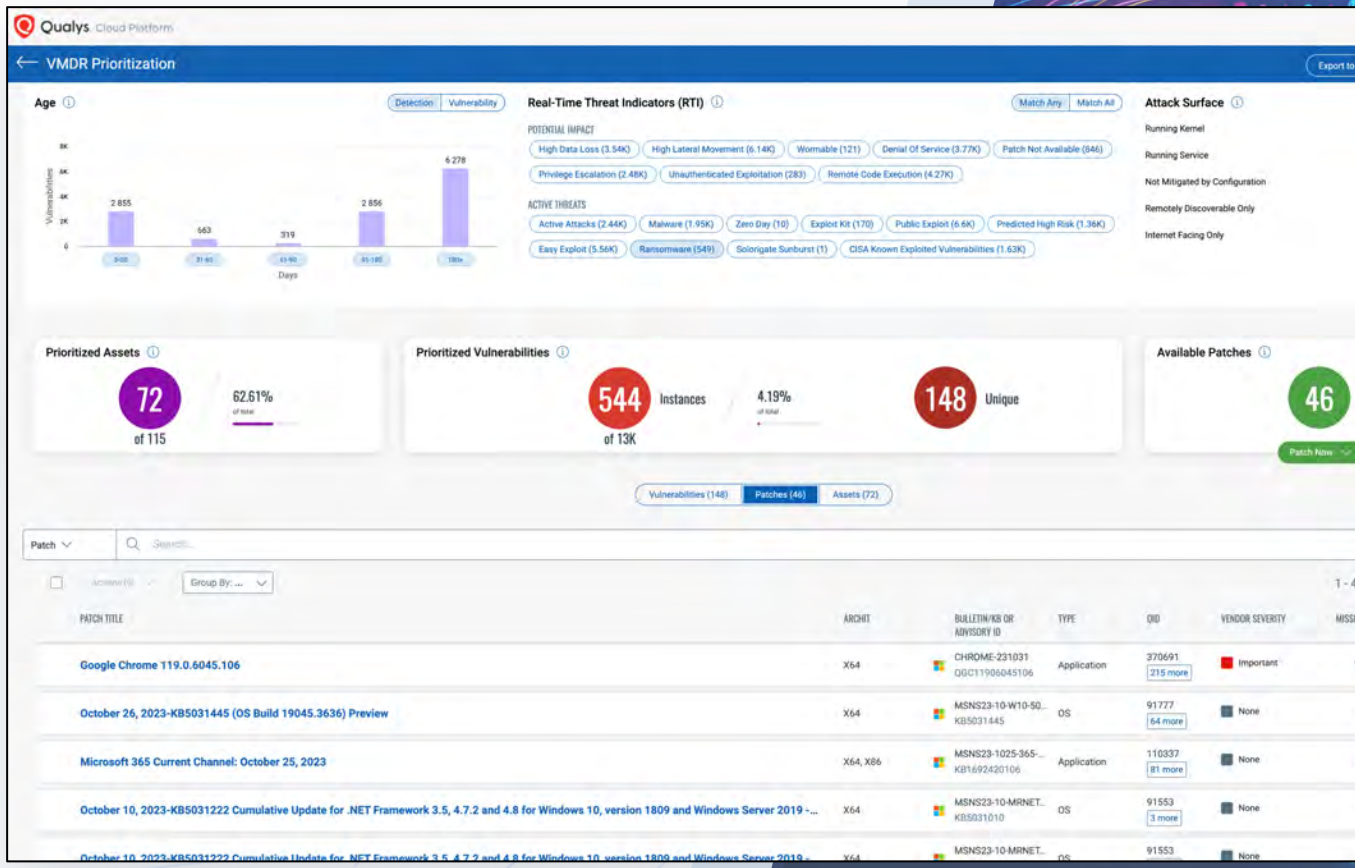
Open-source vulnerabilities

Access Controls

Technology Debt – EOL/EOS

Sensitive data risks

Infra Vulnerabilities



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

Risk-based Elimination, for prioritized vulnerabilities

Web App OWASP vulnerabilities

Malicious, suspicious Activities

Inventory Cyber Hygiene Risks

Cloud Misconfigurations

Infra/DB/Web Servers/ Middleware Misconfigurations

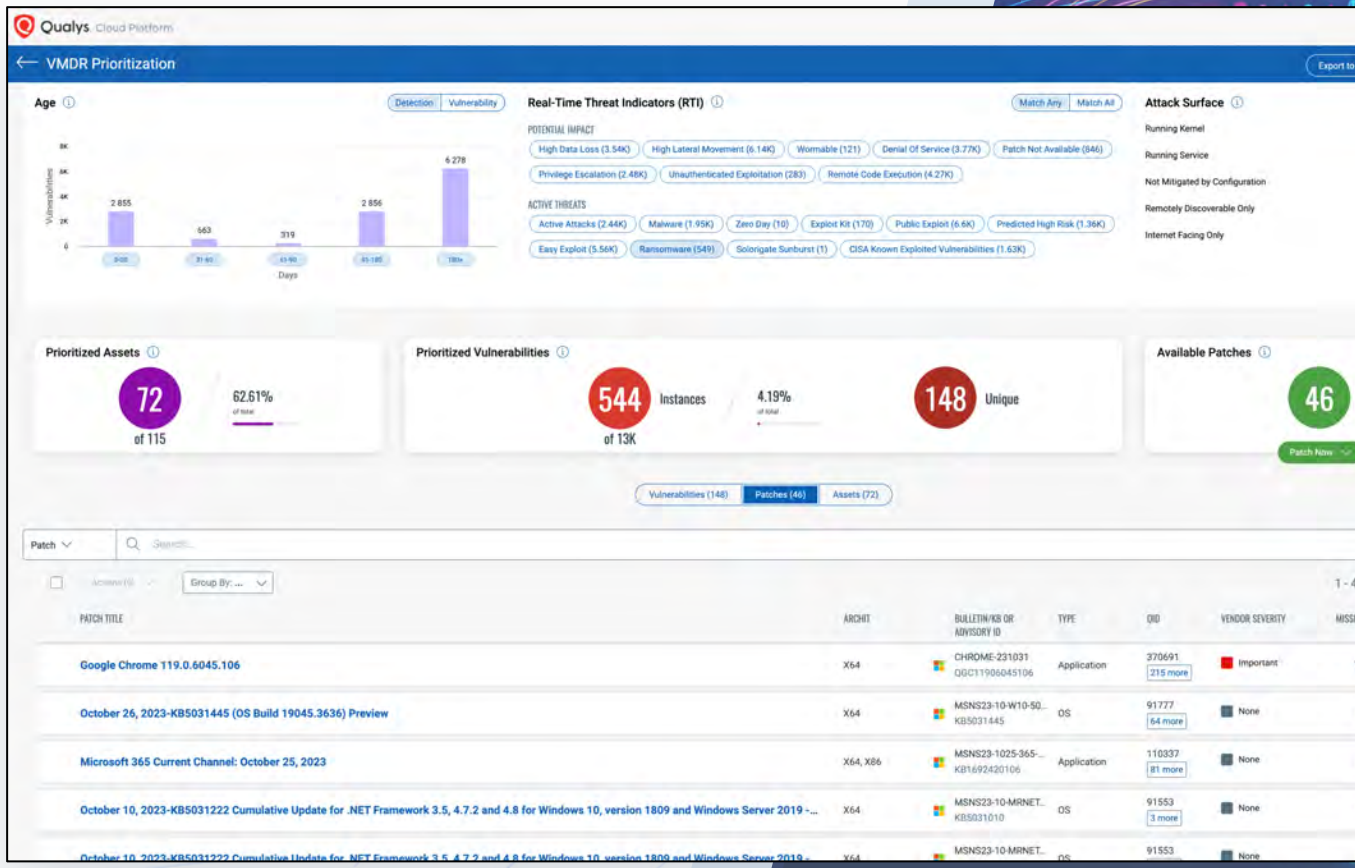
Open-source vulnerabilities

Access Controls

Technology Debt – EOL/EOS

Sensitive data risks

Infra Vulnerabilities



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

Risk-based Elimination, for Cloud

Web App OWASP vulnerabilities

Malicious, suspicious Activities

Inventory Cyber Hygiene Risks

Cloud Misconfigurations

Infra/DB/Web Servers/ Middleware Misconfigurations

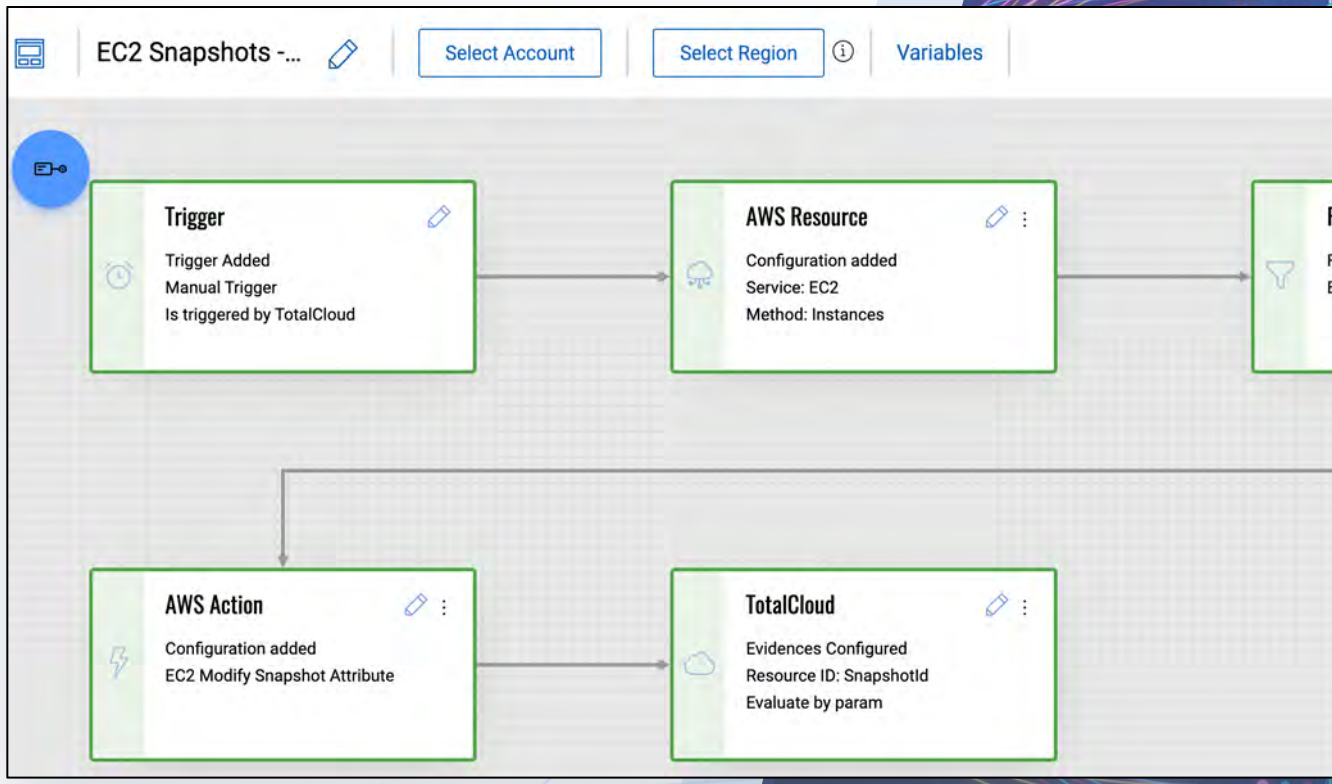
Open-source vulnerabilities

Access Controls

Technology Debt – EOL/EOS

Sensitive data risks

Infra Vulnerabilities



First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

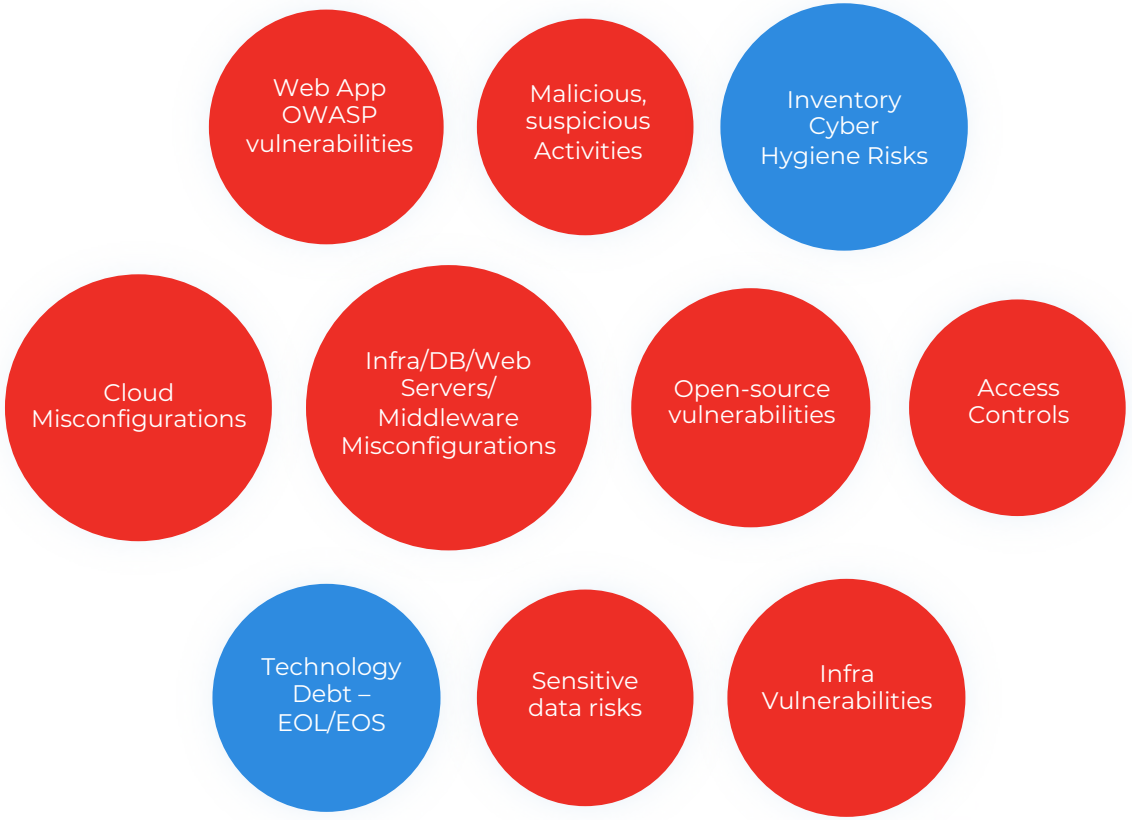
IT / WORKSTATIONS / SERVERS

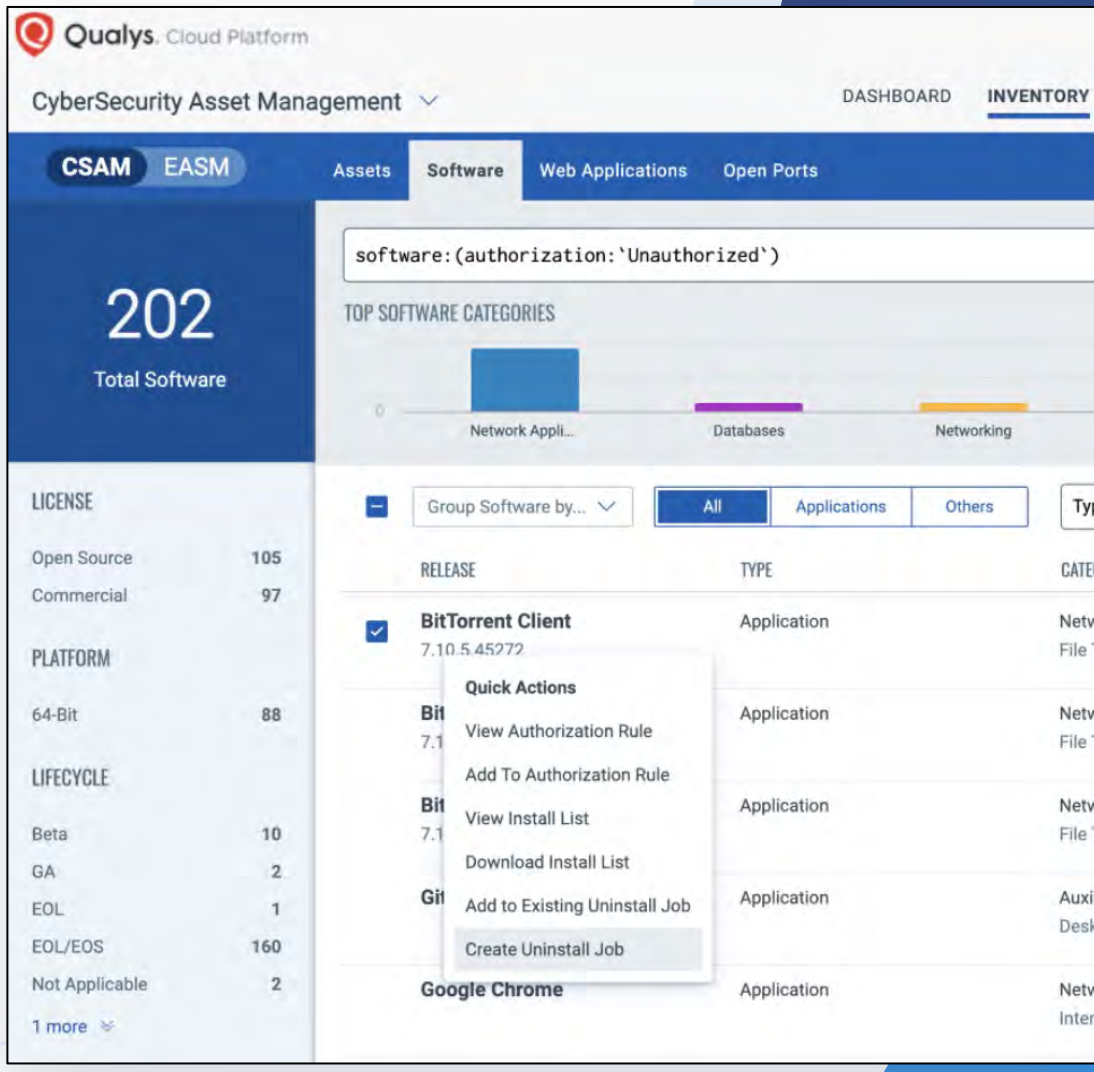
IOT

EXTERNAL DEVICES

Eliminating Risk

Risk-based Elimination, for Inventory





First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Not Just Eliminating, but Preventing Risk

Web App OWASP vulnerabilities

Malicious, suspicious Activities

Inventory Cyber Hygiene Risks

Cloud Misconfigurations

Infra/DB/Web Servers/ Middleware Misconfigurations

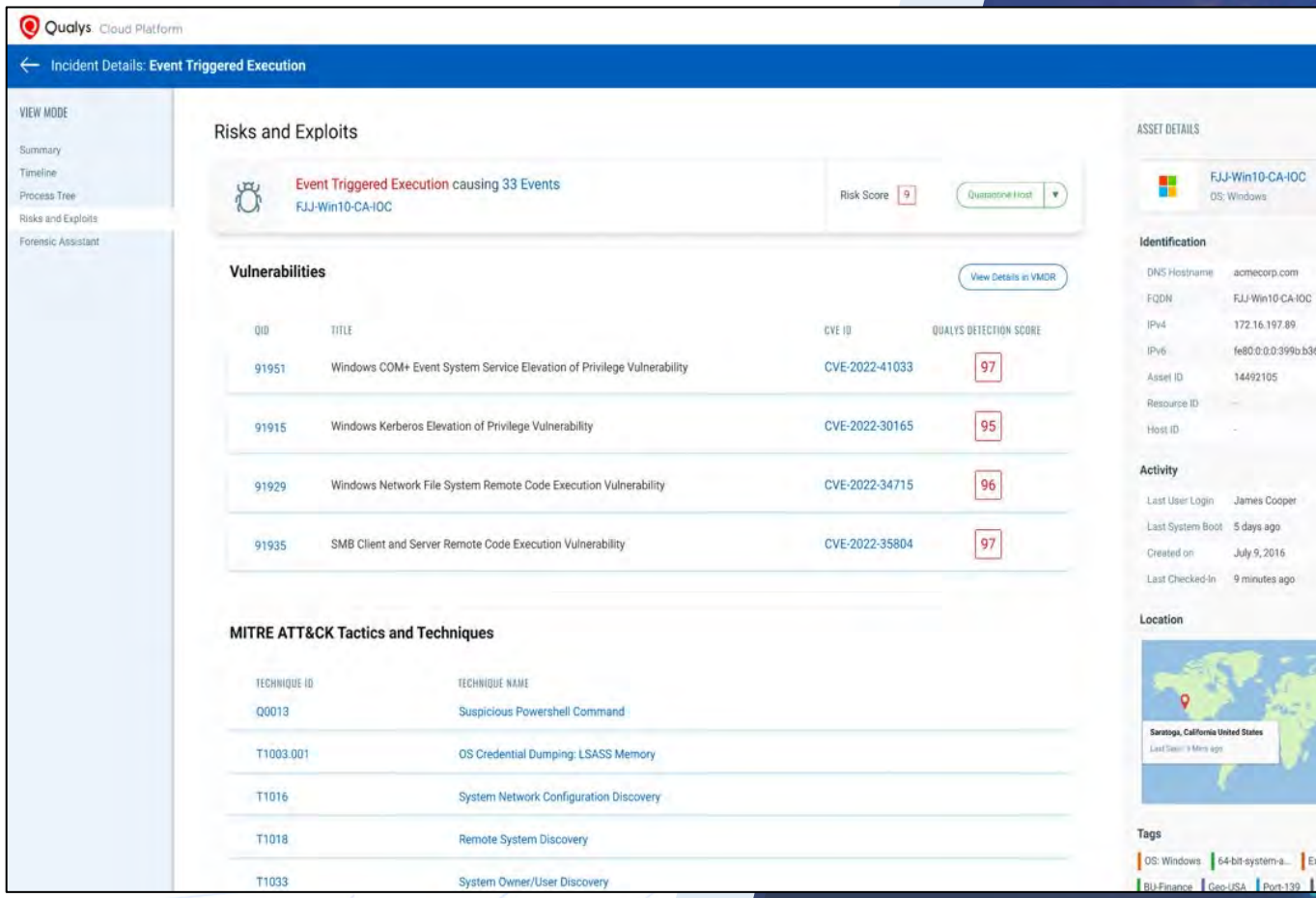
Open-source vulnerabilities

Access Controls

Technology Debt – EOL/EOS

Sensitive data risks

Infra Vulnerabilities



First-Party OSS

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS

3rd Party Data

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

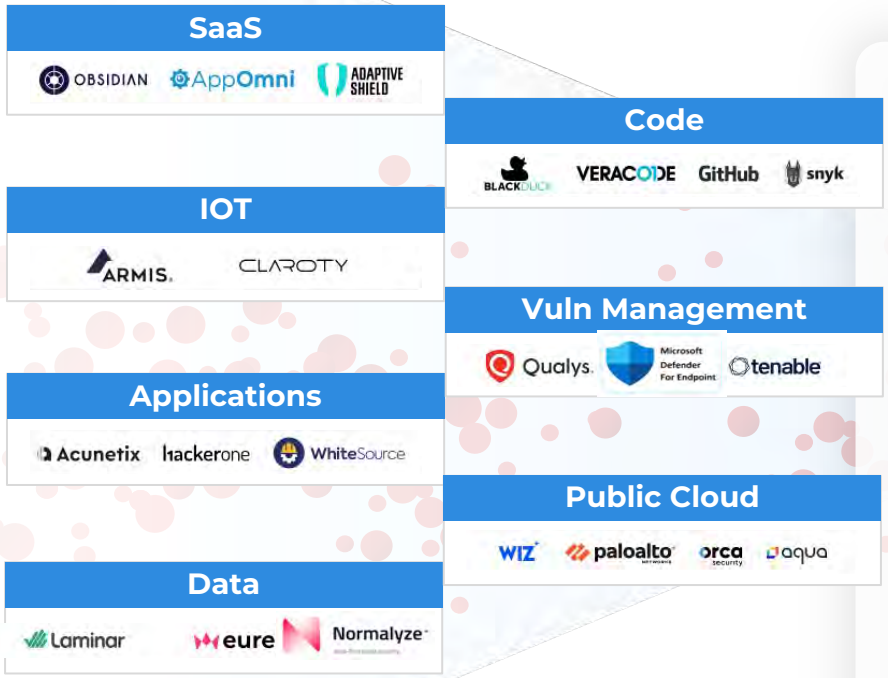
De-risk your business.

What’s Next...

Qualys.

Further Challenges of Measuring Risk

Every tool measures risk differently, with/without Threat, Business context



Qualitative

- Severe / Critical
- Urgent / Low
- Medium / High
- Pass / Fail
- Category 1,2,3 etc..

Quantitative

- 10, 50, 100
- 1-5

CVSS

- 1-10

Qualys.

Communicate Risk

For Intrinsic Business Value & Loss

1. No Tie up for Cyber Risk to the Business Value & Loss.
   What's the impact on business

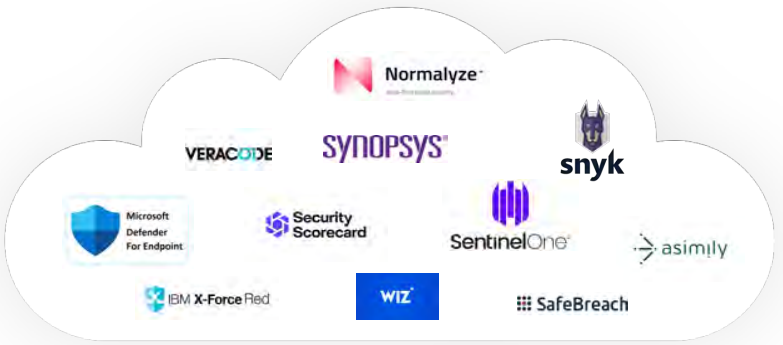
2. Inability to communicate risk to right teams on their impact on organization's TruRisk

Qualys.

Communicate Risk

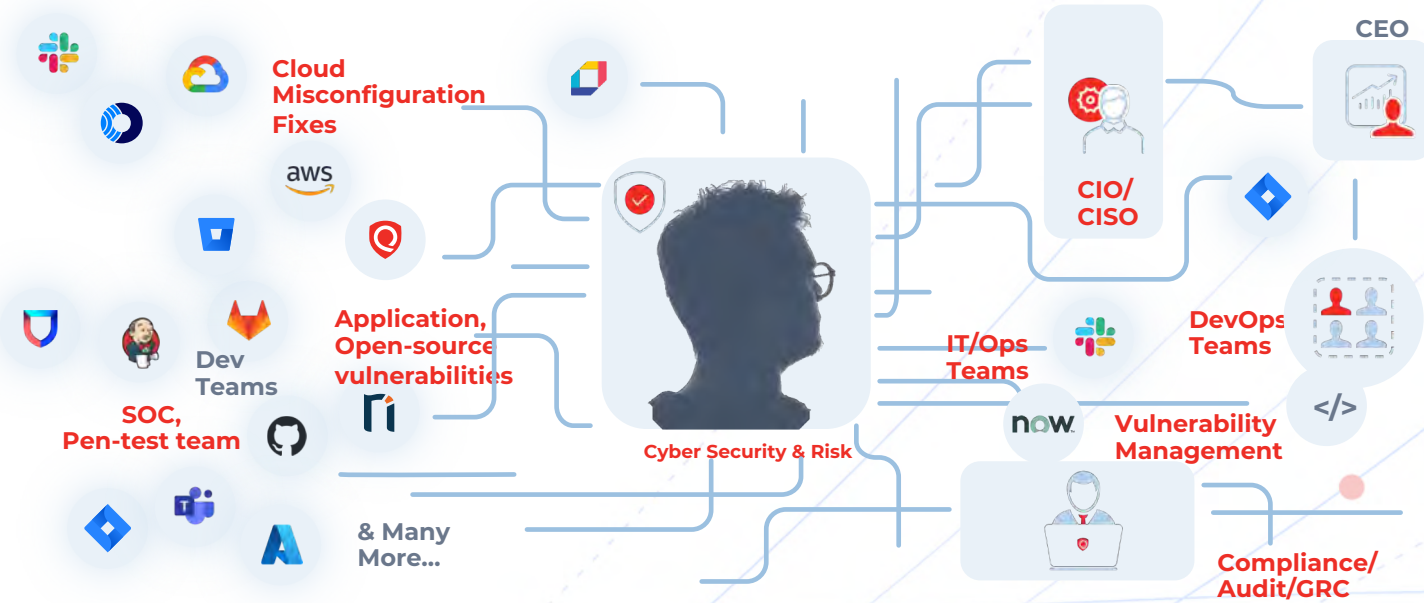
Challenge of Communicating Right Data to Right Team

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**



Qualys.

Need to Reduce Risk, w/o Patch Dependency

Patching Hygiene Doesn't Improve, Then what?

Attackers continue to **exploit old vulnerabilities & remain unpatched**

What are Options beyond Patching

Top 10 Riskiest Vulns, not 0 days, Exploited by Threat Actors

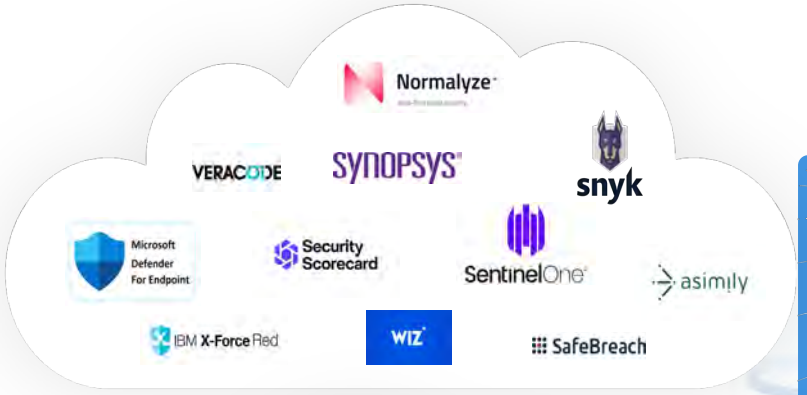
30+ Days to remediate weaponized vulnerabilities

Qualys.

Extending the Power of the Qualys **TruRisk** Platform for **Eco-System** Risk Management

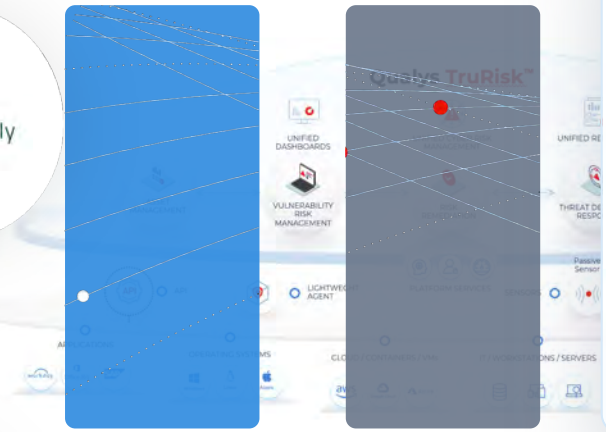
Qualys.

Measuring TruRisk Across Eco-System

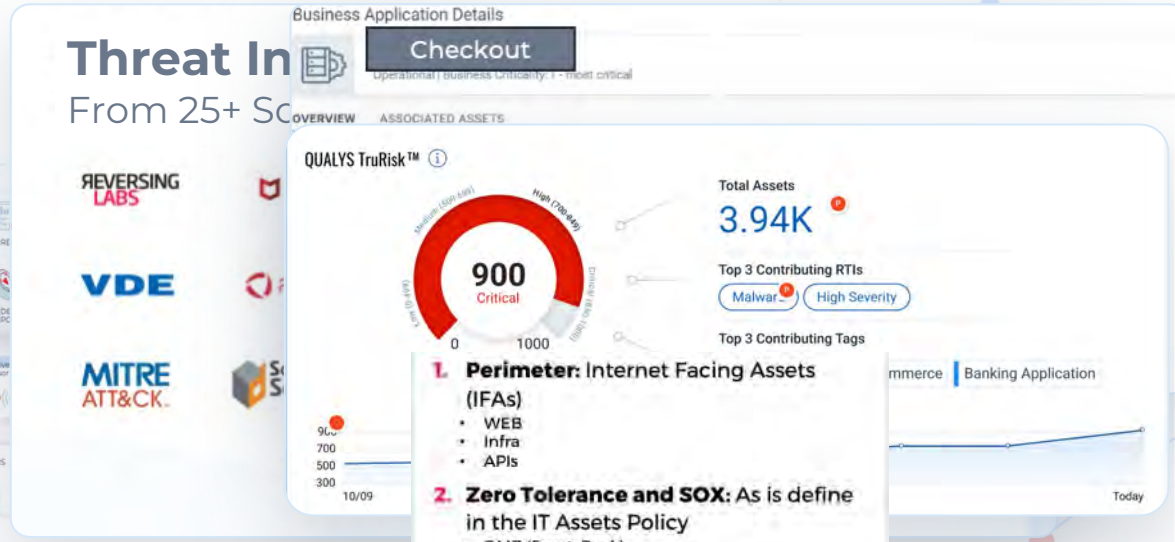


The Qualys Solution set

- 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**

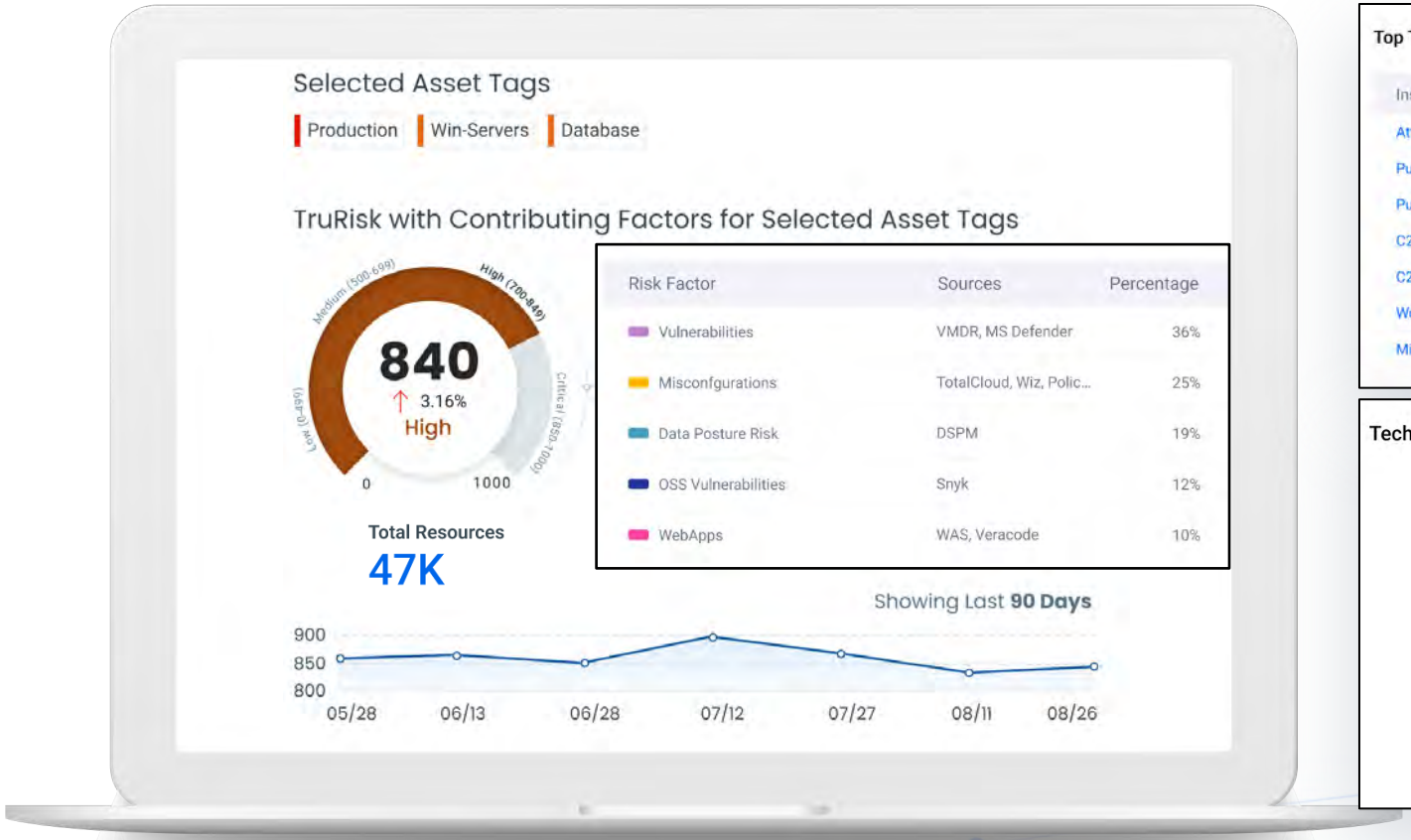


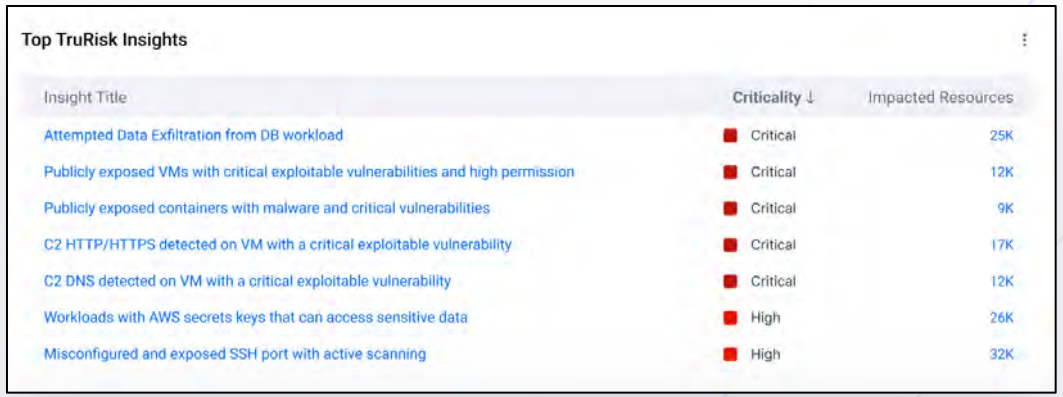
Context

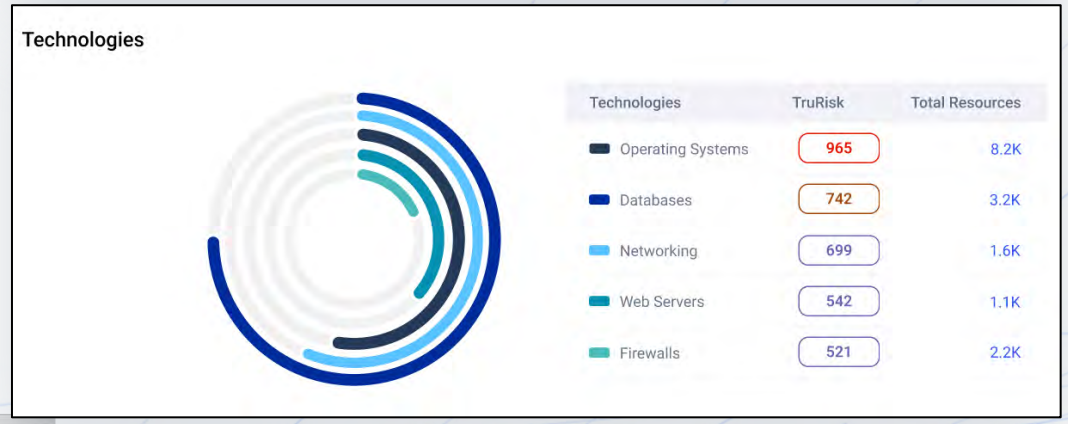
1. **Ransomware:**
   CVEs related to vulnera
2. **Dark Web chatter:**
   CVEs related to your in
3. **Known Malware:**
   CVEs exploited by by known threat actors

Qualys.

Measuring TruRisk Across the Eco-System

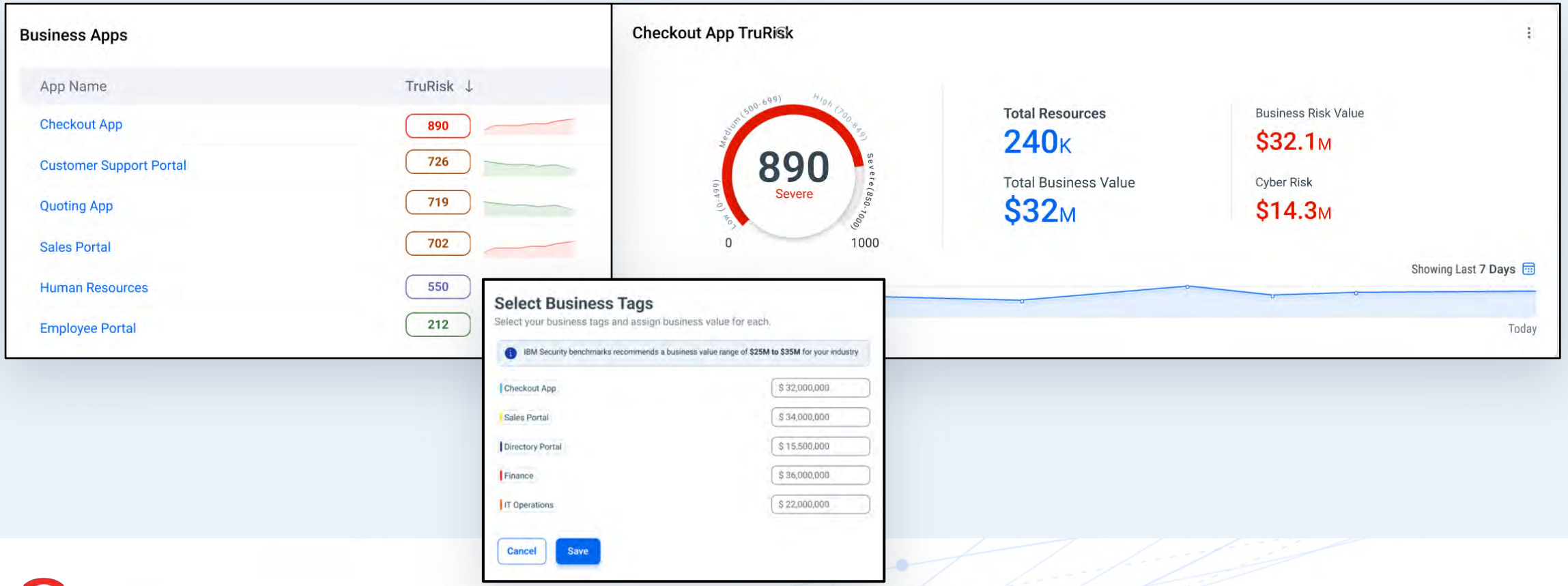






Qualys.

Communicating TruRisk to Executives in Language of Business Value & Loss



Qualys.

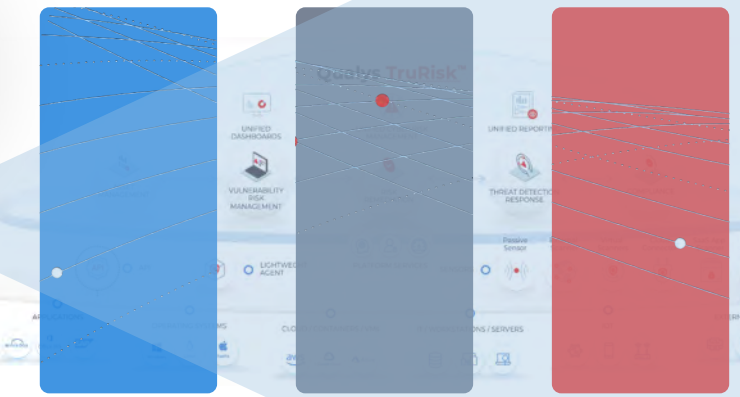
Communicating TruRisk

Right Data, with Right Context to Right team

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 Concept

Infra vulns

open-source vulns

cloud misconfigurations

application vulns

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

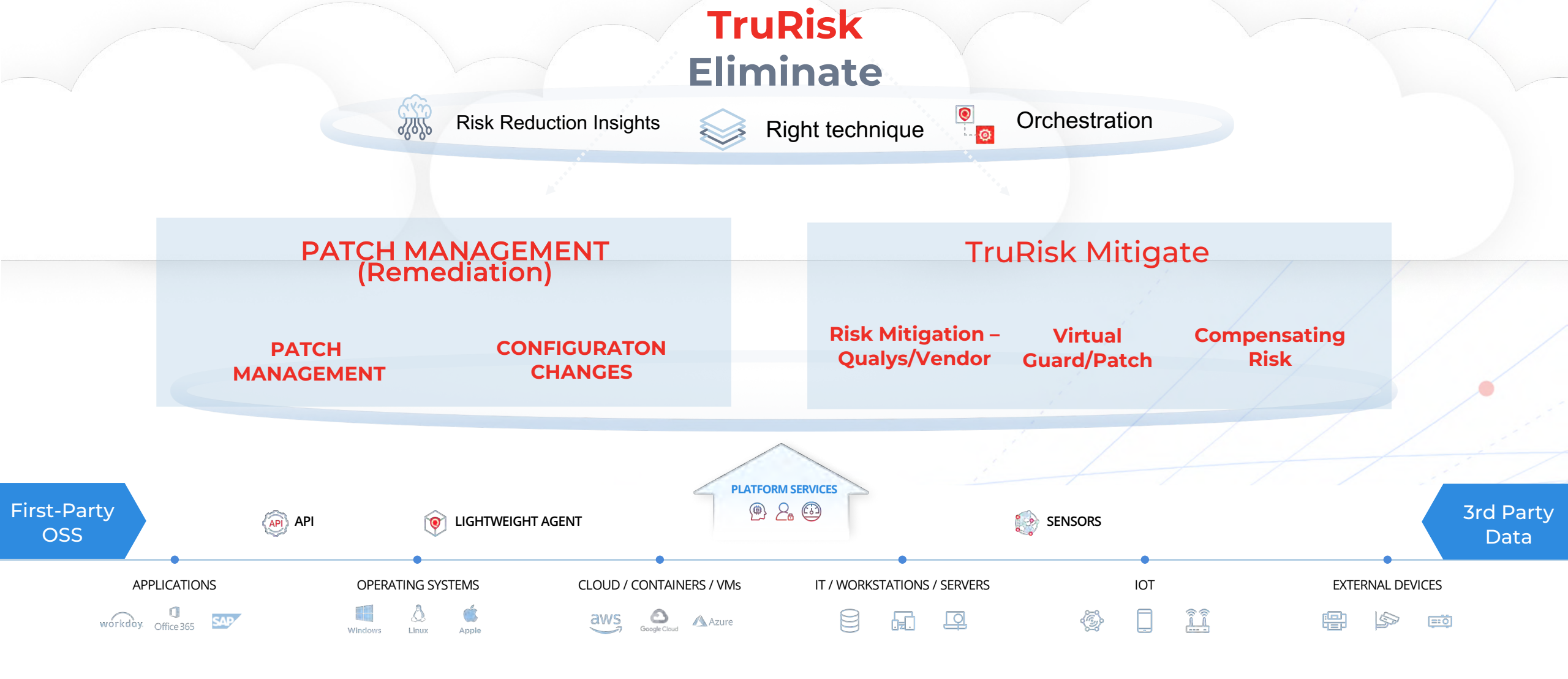
App Teams

Vuln for Apache Tomcat
Workload
Fix script
Update version, patch

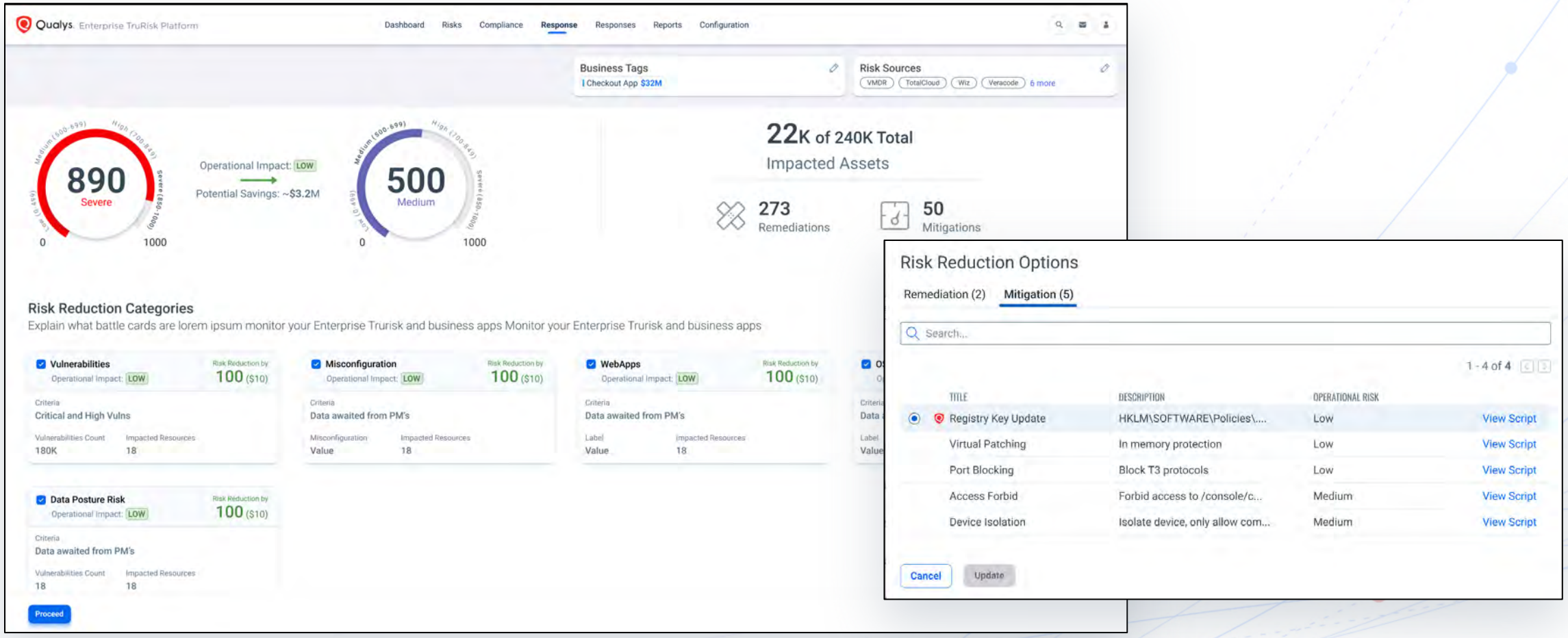
Qualys.

TruRisk Eliminate

Remediate, Mitigate, Compensate, Virtually Guard



Eliminating Risk … with Techniques Beyond Patching, balancing Operational Impact



Qualys.

Risk Mitigation

Going Beyond Patching

Risk Mitigation: Vendor provided

Registry Keys, config Settings, User Permissions,

Virtual Patching

Temporary Shield To Protect Memory & Kernel Space

Risk Mitigation: Qualys

Uninstall Of Software, Port Blocking

Compensate Risk: Orchestration

Microsoft Defender, Palo Alto firewall changes with Qualys Qflow trigger

Accept Risk

Sap,zlinux, Mainframes , Databases with approvals

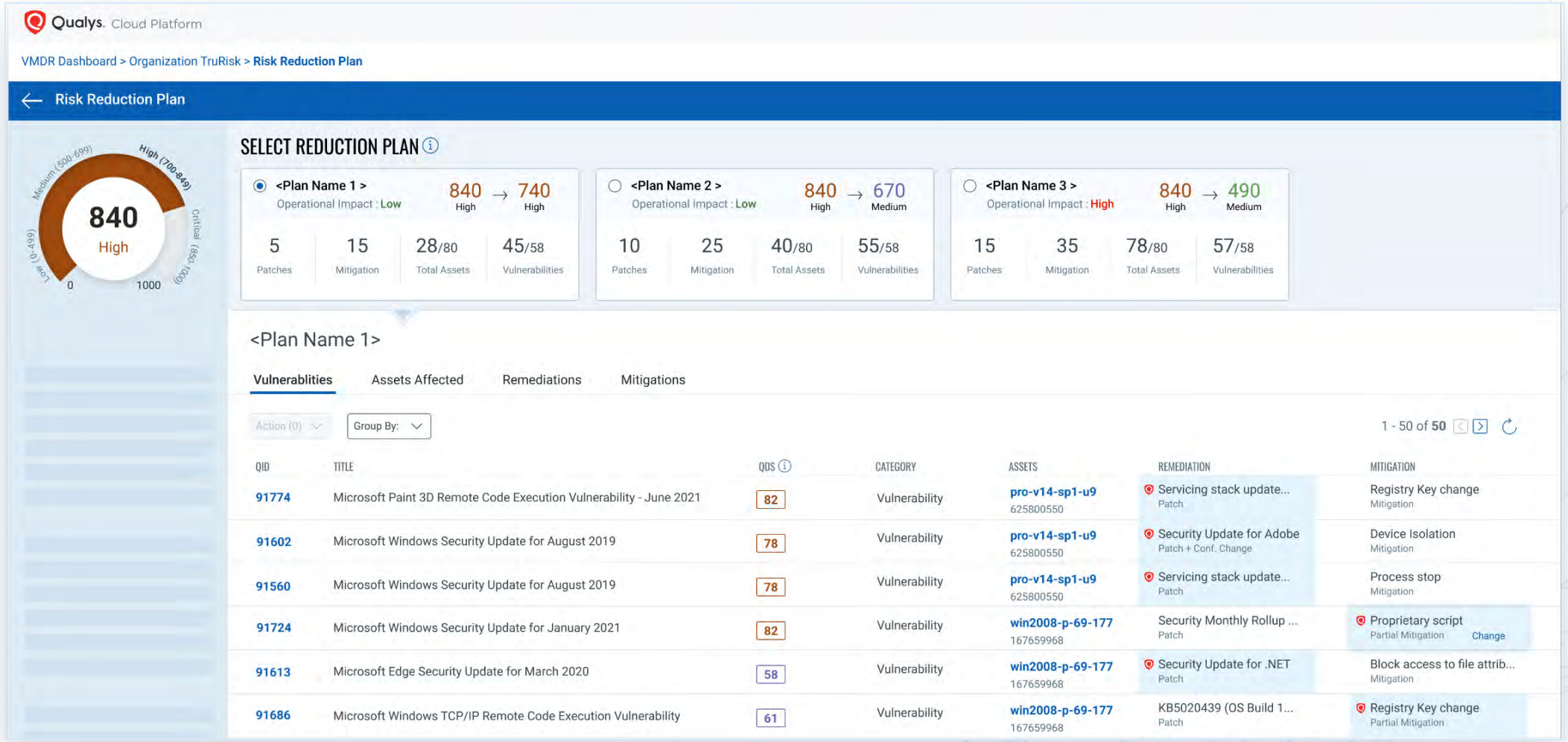
Modifying Access

Machine & User Identities

Qualys.

Eliminating Risk Effectively

Personalized Risk Reduction Recommendations



Qualys.

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

Qualys®


SC
23