



Measure, Communicate & Eliminate Your Cyber Risk with Qualys Platform

Shailesh Athalye
Senior VP Product Management, Qualys

Indiana Jones

**“It’s important...
Trust me.”**



Approach of 'Indiana Jones' of Cyber Risk

A systematic approach to de-risking their digital ecosystems



Security Teams



Measure Cyber Risk

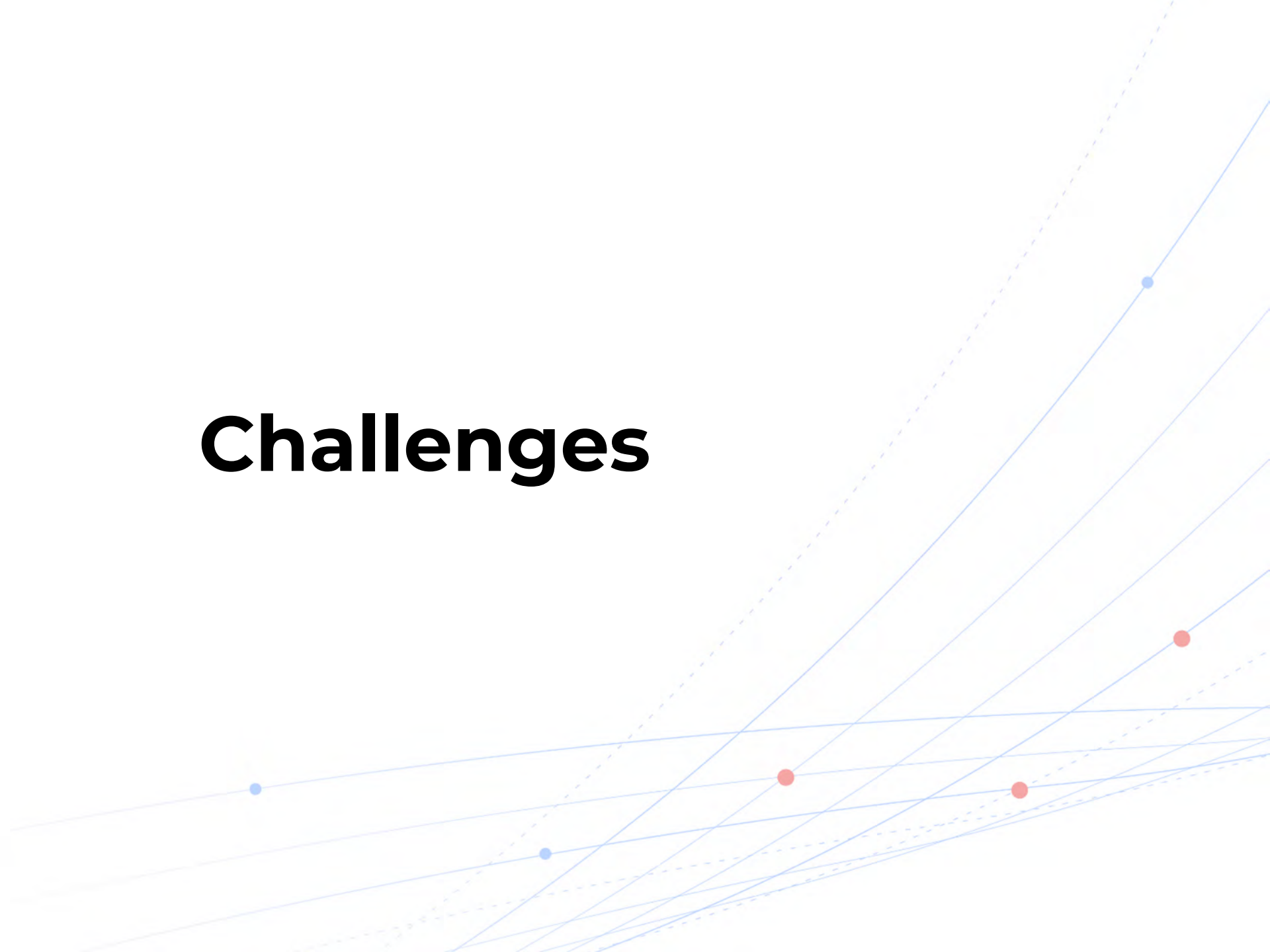


Communicate Cyber Risk



Eliminate Cyber Risk

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

Challenges of Measuring Risk

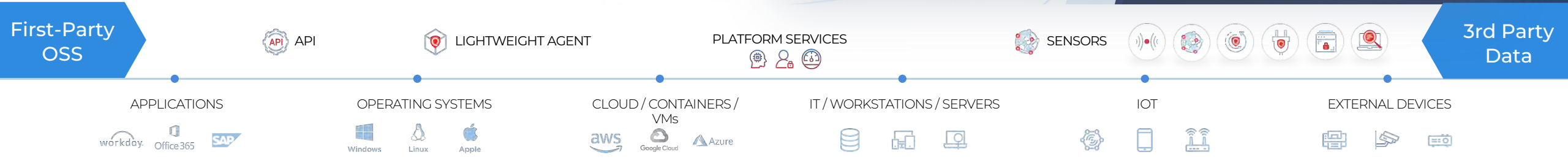
Context for the 'Top 10' Risk Factors

✗ Inability to collect data – Comprehensively & Accurately

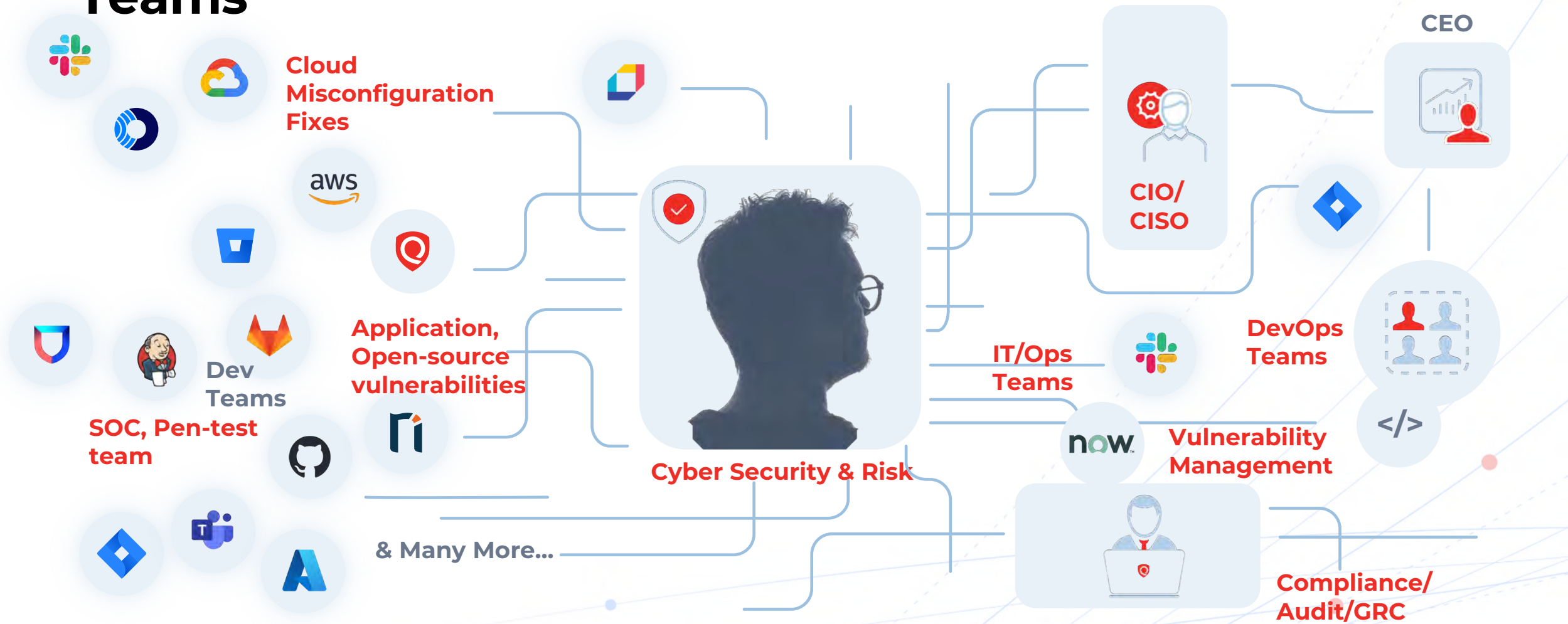
✗ Lack of Threat & Business context

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

✗ Unable to view unified 'Toxic Insights'



Challenge of Communicating Right Data to Right Teams



Challenges of Eliminating Risk

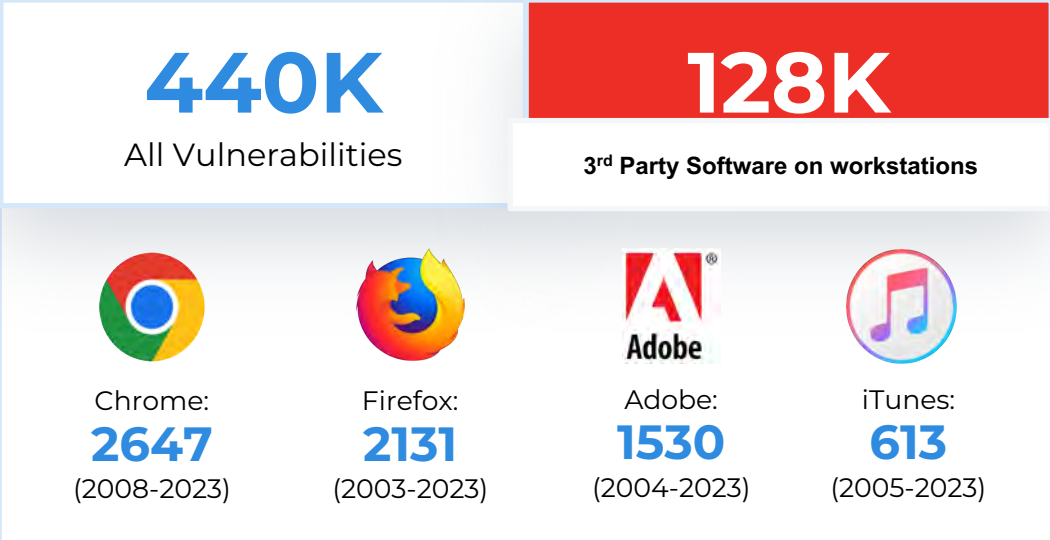
IT not Risk, based Elimination

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



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

The image shows two screenshots of news articles. The top screenshot is from CBS News, dated 2021, with the headline "80% of ransomware victims suffer repeat attacks, according to new report". The bottom screenshot is from CPO Magazine, dated 2023, with the headline "67% Of Businesses Suffer Repeat Cyber Attacks Within 12 Months After the First Data Breach".

The Solution

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

3rd Party
Data

API

LIGHTWEIGHT AGENT

PLATFORM SERVICES

SENSORS



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 VMDB with business context

Internal assets

Agent, Scanner, Sensors



IOT/OT assets

Passive Network Sensor



Assets from 3rd parties

API-Based Connectors



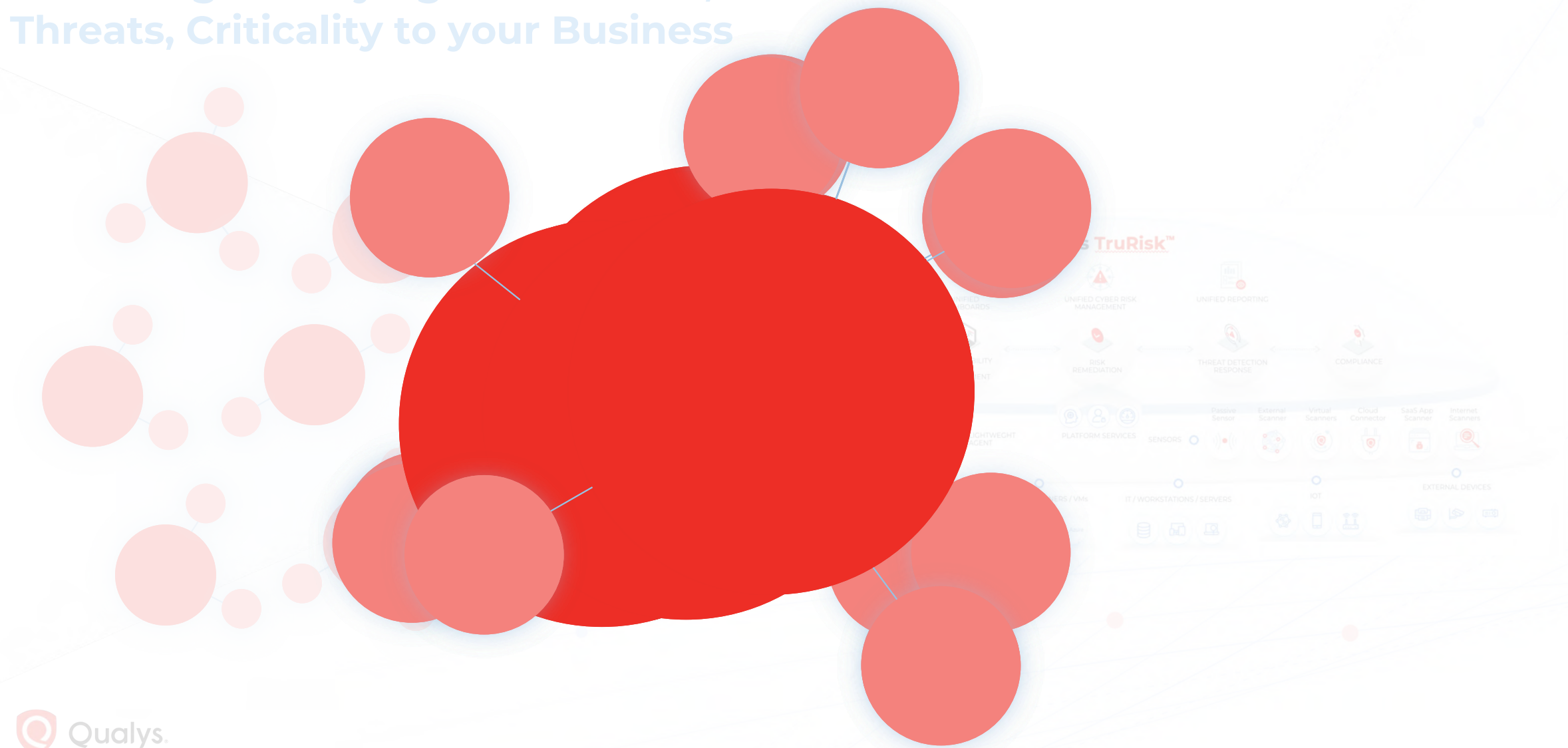
External assets

Open-source Tech & Qualys Internet scanner



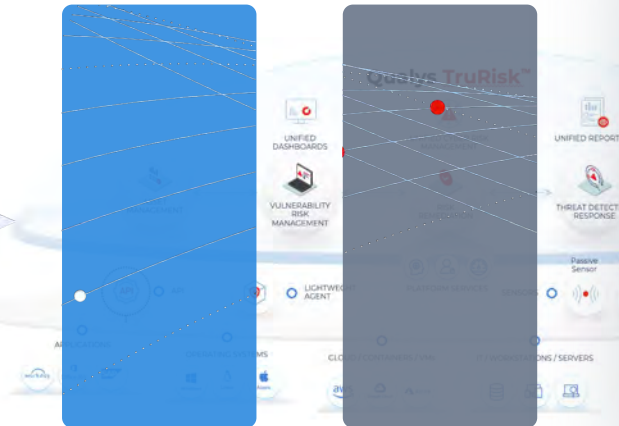
Measuring **TruRisk**

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

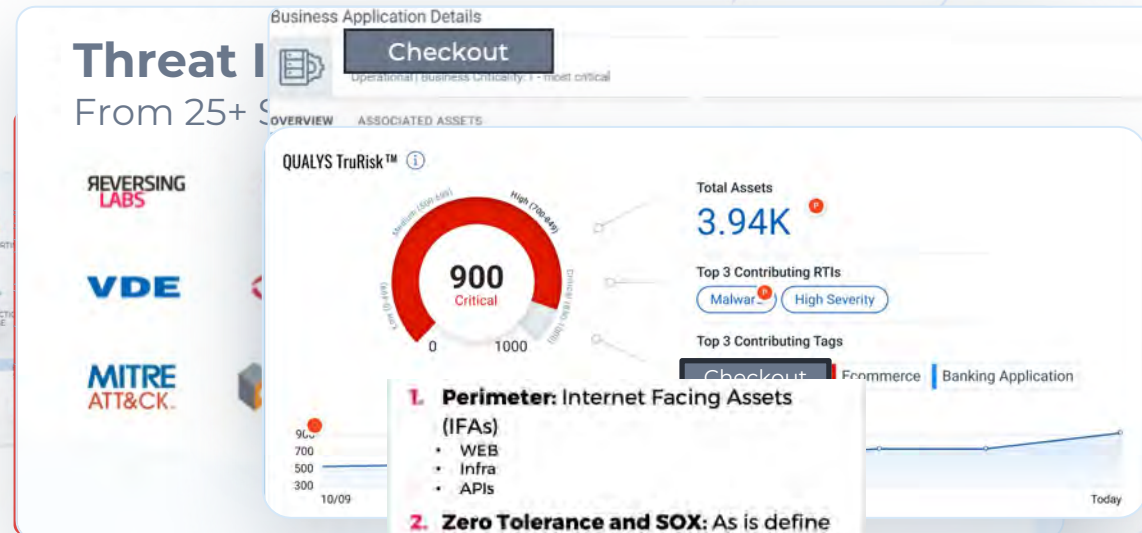


Measuring **TruRisk**

Collecting & Unifying Risk Factors, with Threat & Business Context



Normalization Correlation



Context

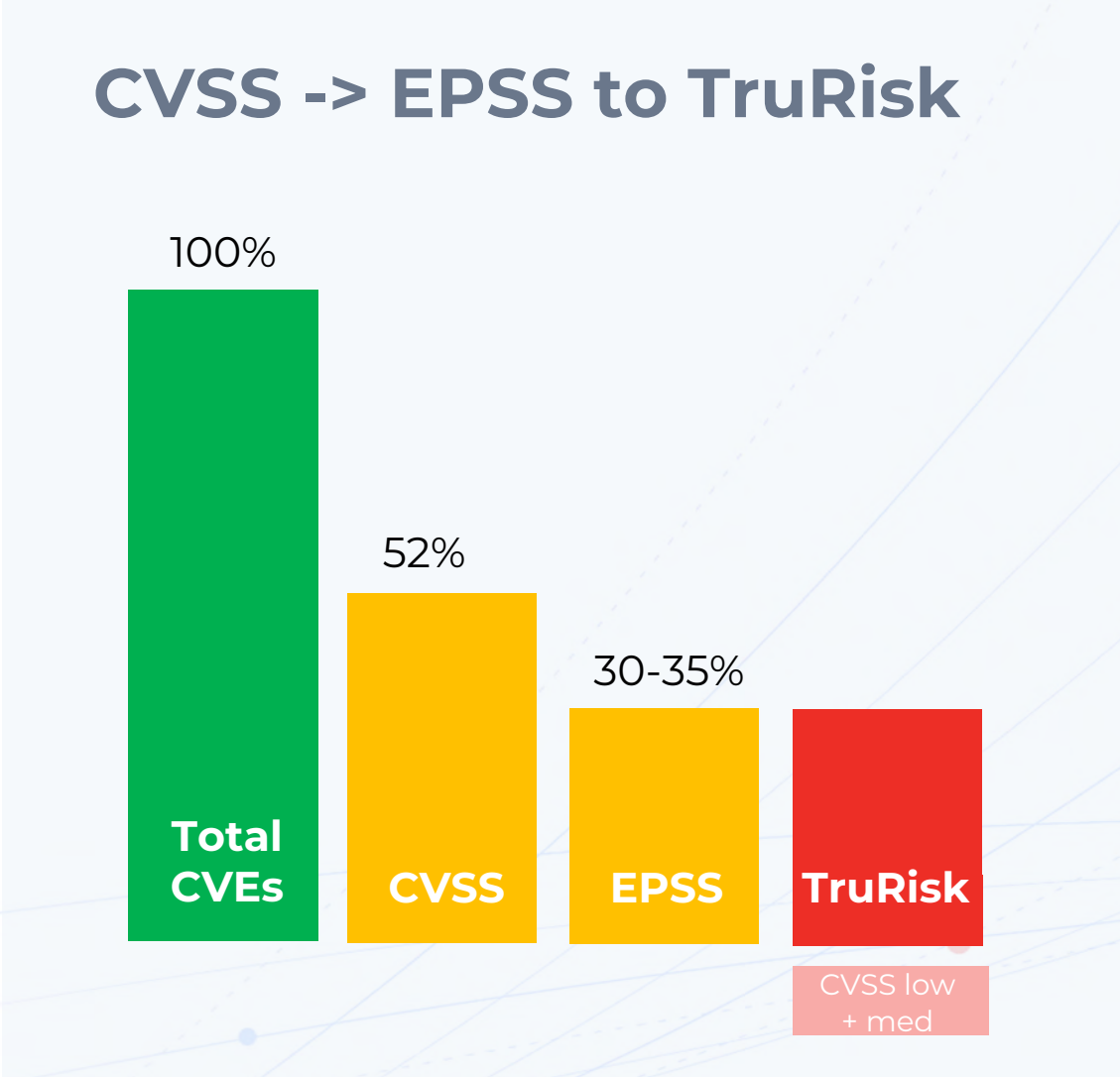
1. **Ransomware:** CVEs related to vulnerabilities exploited by ransomware
2. **Dark Web chatter:** CVEs related to your organization's assets
3. **Known Malware:** CVEs exploited by known threat actors

1. **Perimeter: Internet Facing Assets (IFAs)**
 - WEB
 - Infra
 - APIs
2. **Zero Tolerance and SOX:** As is defined 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

Outcome of Measuring TruRisk

Up to **85%**
fewer vulnerabilities

~80%
less 'Ransomware'
vulnerabilities



Communicating Risk

Contextual Communication Per Persona/Responsibilities



Communicating to Executives

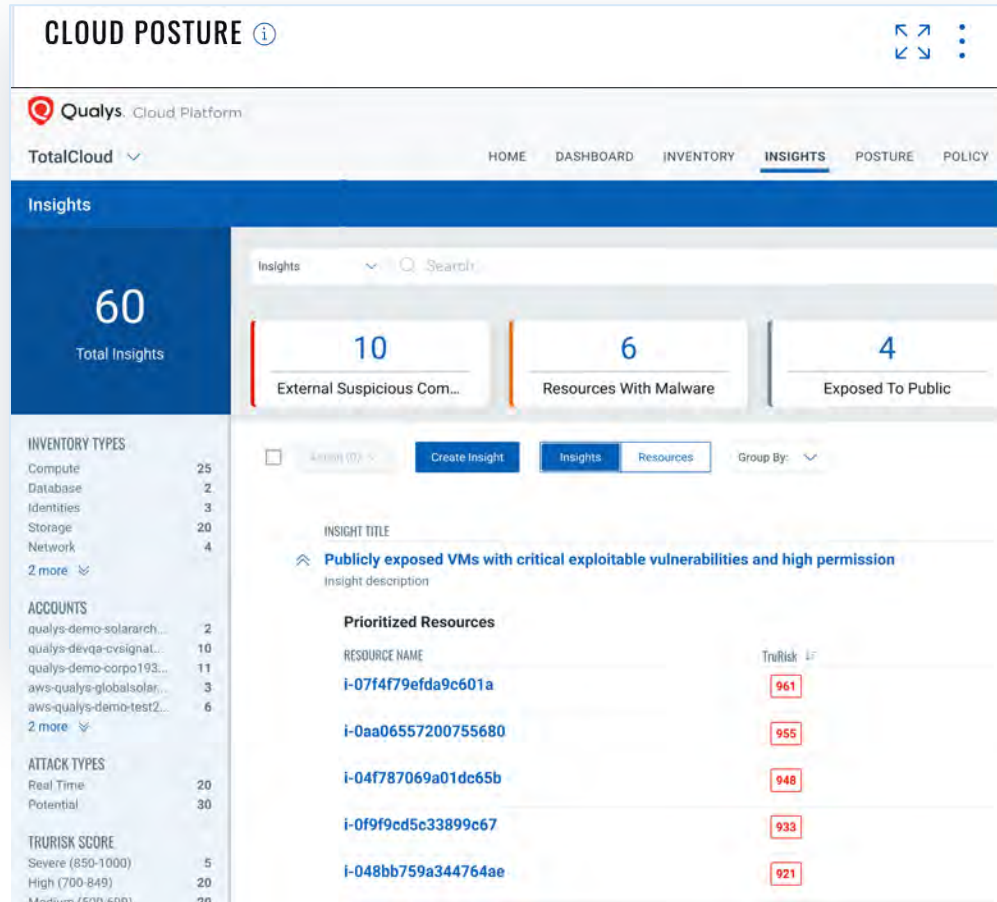
Unified, Quantified, Prioritized Cybersecurity Risk score

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

Provides actionable recommendations to eliminate, reduce risk

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

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

Communicate Compliance

Be-Audit Ready

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

File Help

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 v2.0	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

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

Communicating Risk

Contextual Communication Per Persona/Responsibilities

Rule Details

Provide the following information to create the rule

Rule Information

Rule Name *

Rule Query

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

Rule Query *

Vulnerability	<code>vulnerabilities.detectionScore>90 and vulnerabilities.vulnerability.threatIntel.ransomware:1</code>
Asset	<code>criticalityScore:5 and tags.name:"Checkout App"</code>

Rule query

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

Search query *

Vulnerabilities	<code>vulnerabilities.vulnerability.category:"SCA" and vulnerabilities.vulnerability.qid:985157</code>
Assets	<code>tag.name:'EASM'</code>

Sample Queries

Trigger Criteria

Provide the match criteria

Trigger Criteria *

Single Match

Action Settings

Choose an appropriate alert action

Actions *

ServiceNow: Push Mechanism

Communicating to Teams to remediate

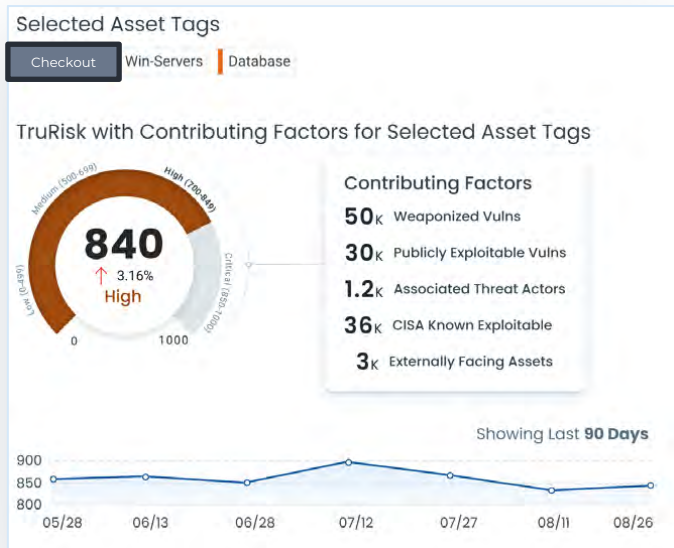
Auto ticketing to move beyond spreadsheets

Rule-based ticketing, ownership assignment, and auto closure

Manage change approvals and deploy remediations directly from ITSM

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

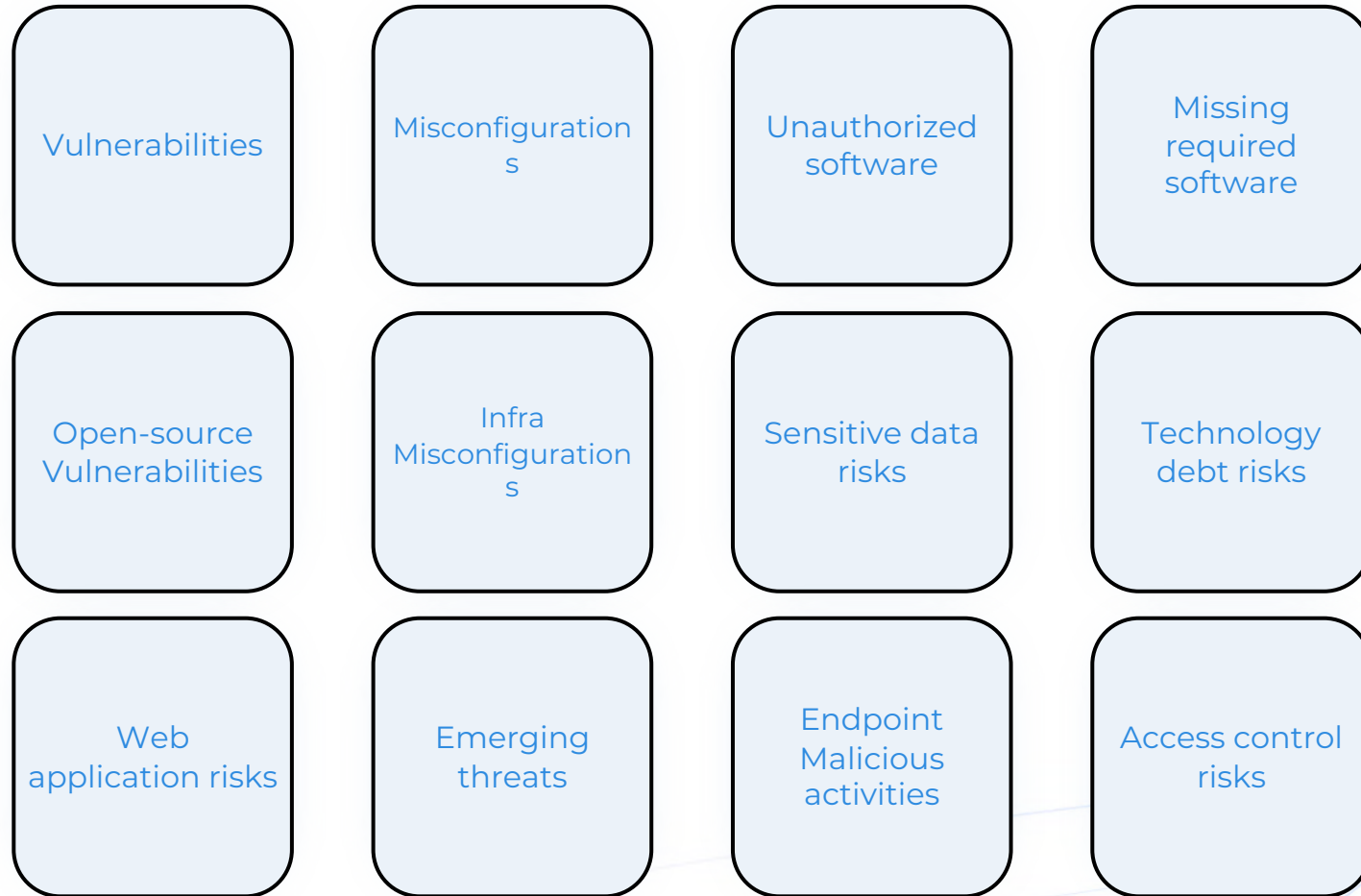
Cloud Team
 Cloud Misconfig
 S3 Bucket Public access
 Account : AWS : ID
 Fix script
 IaC Template

application vulns

App Teams
 Vuln for Apache Tomcat
 Workload
 Fix script
 Update version, patch

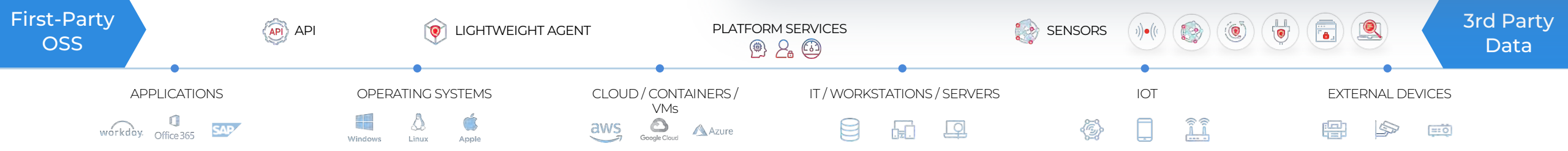
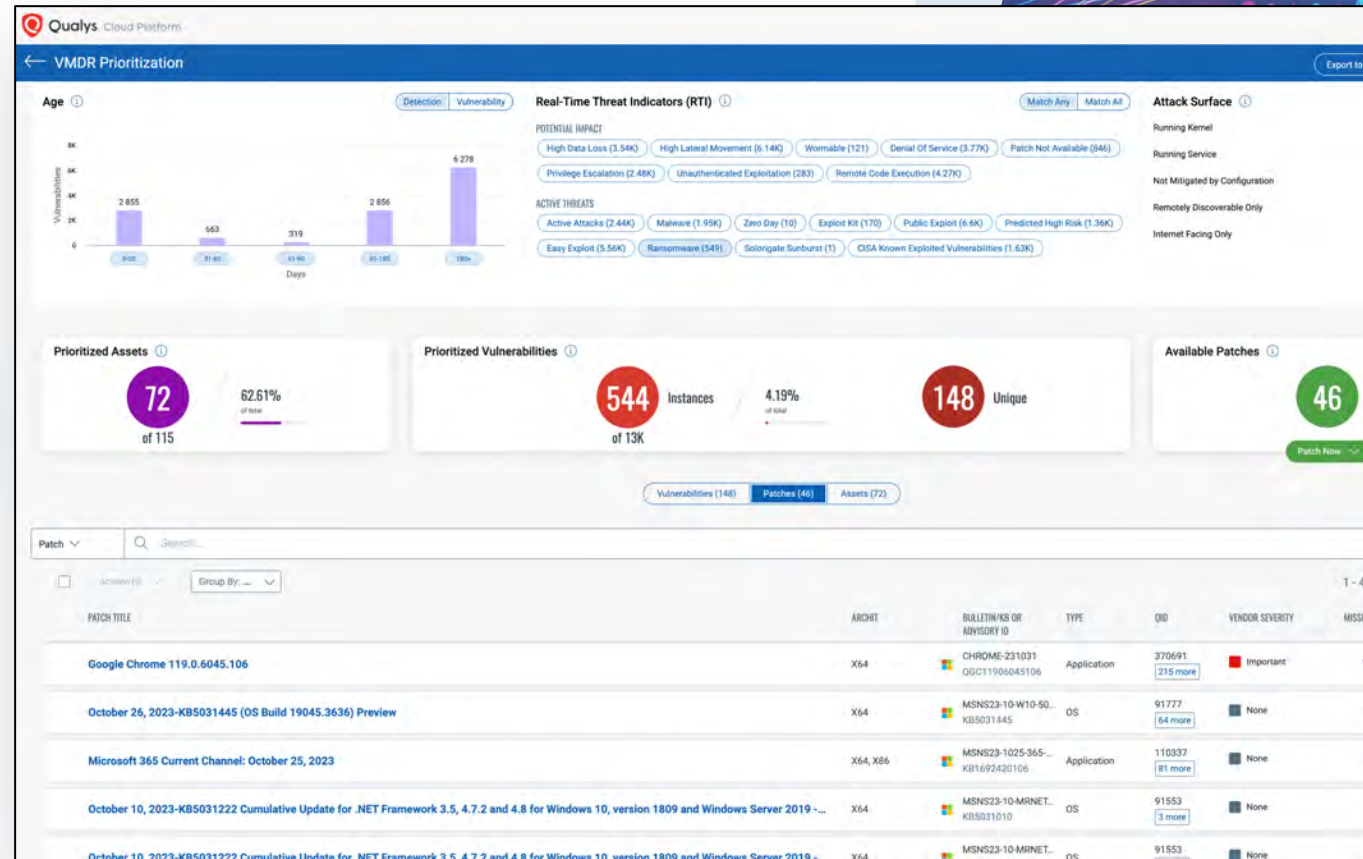
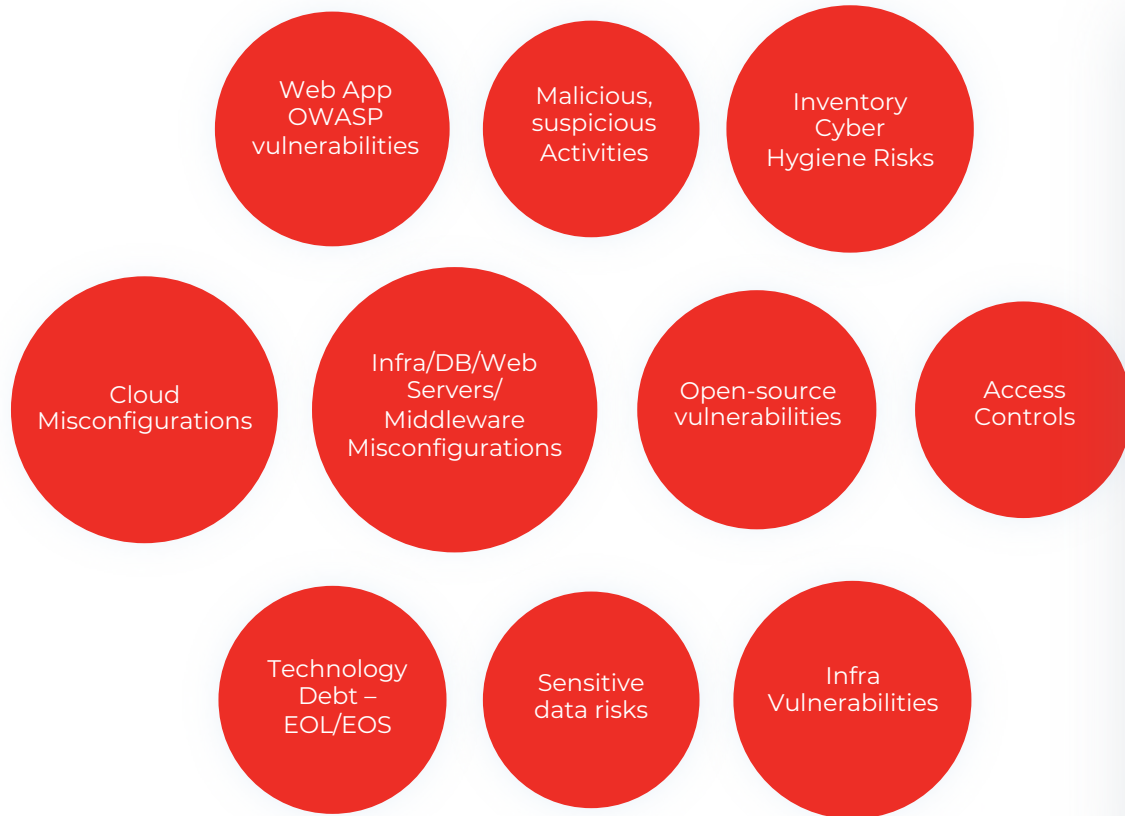
Eliminating Risk

Across Risk Factors



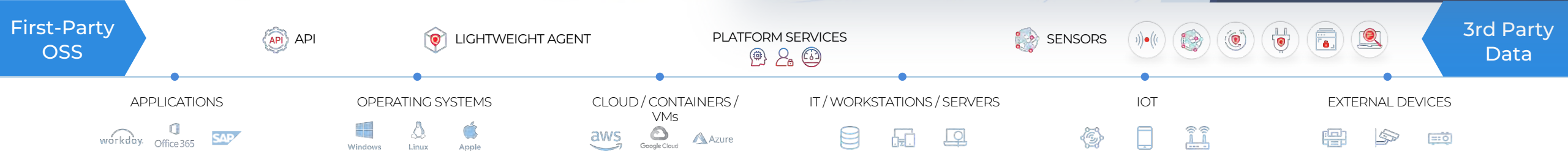
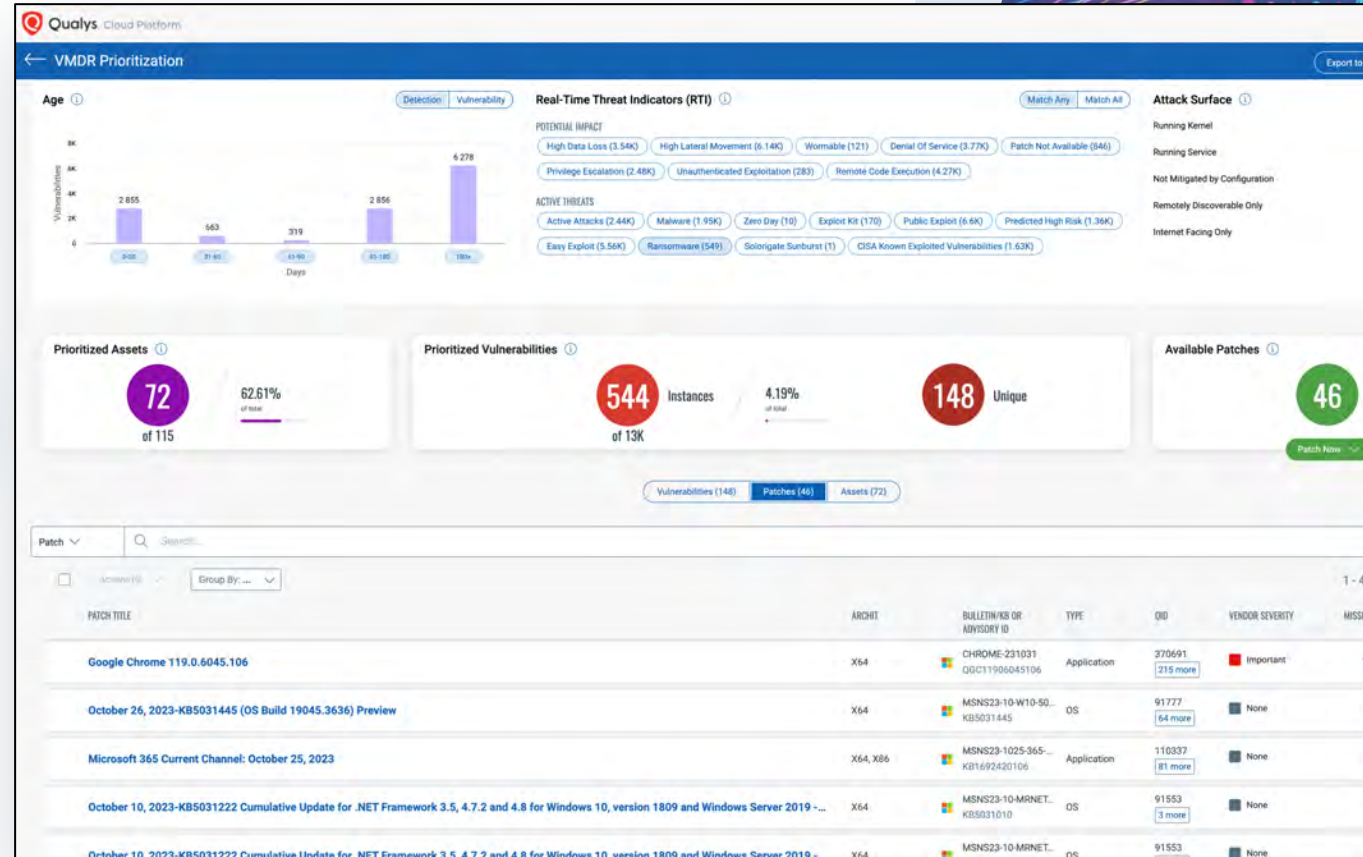
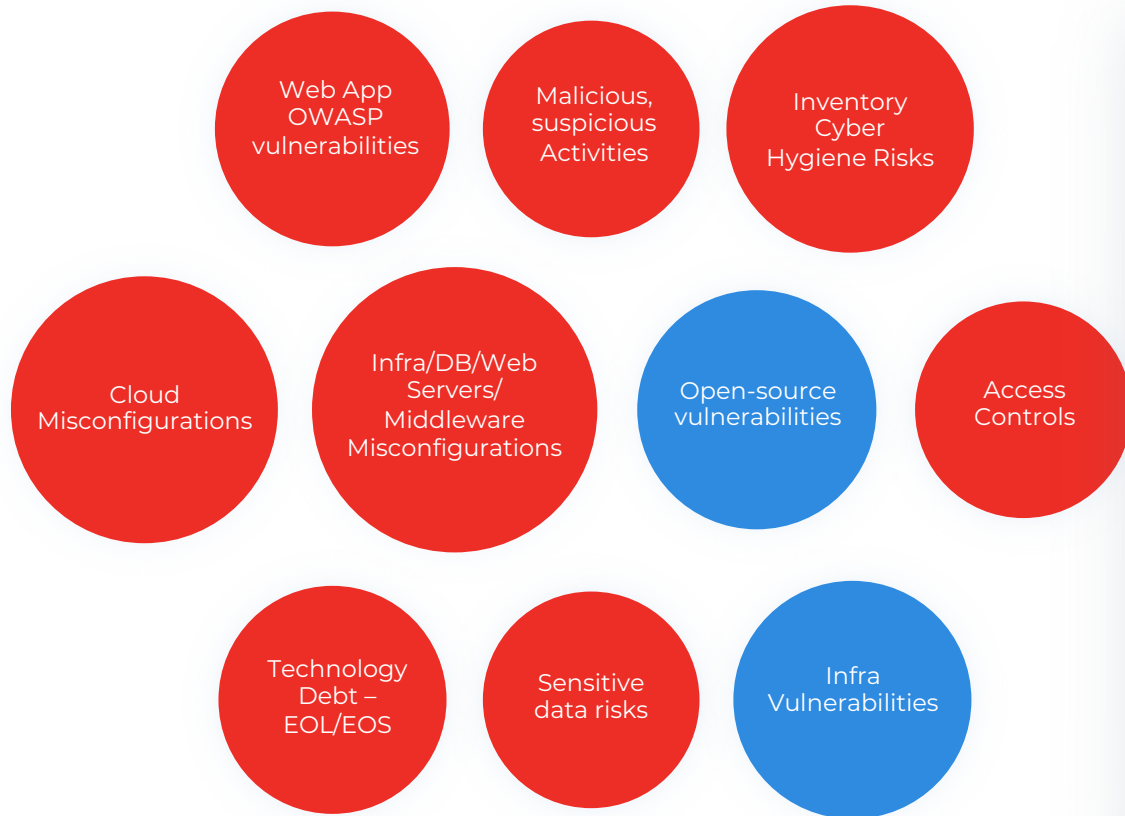
Eliminating Risk

Risk-based Elimination, across Attack Surfaces, Risk Categories



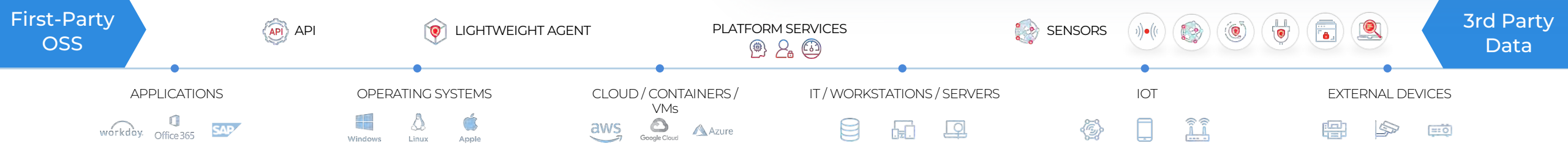
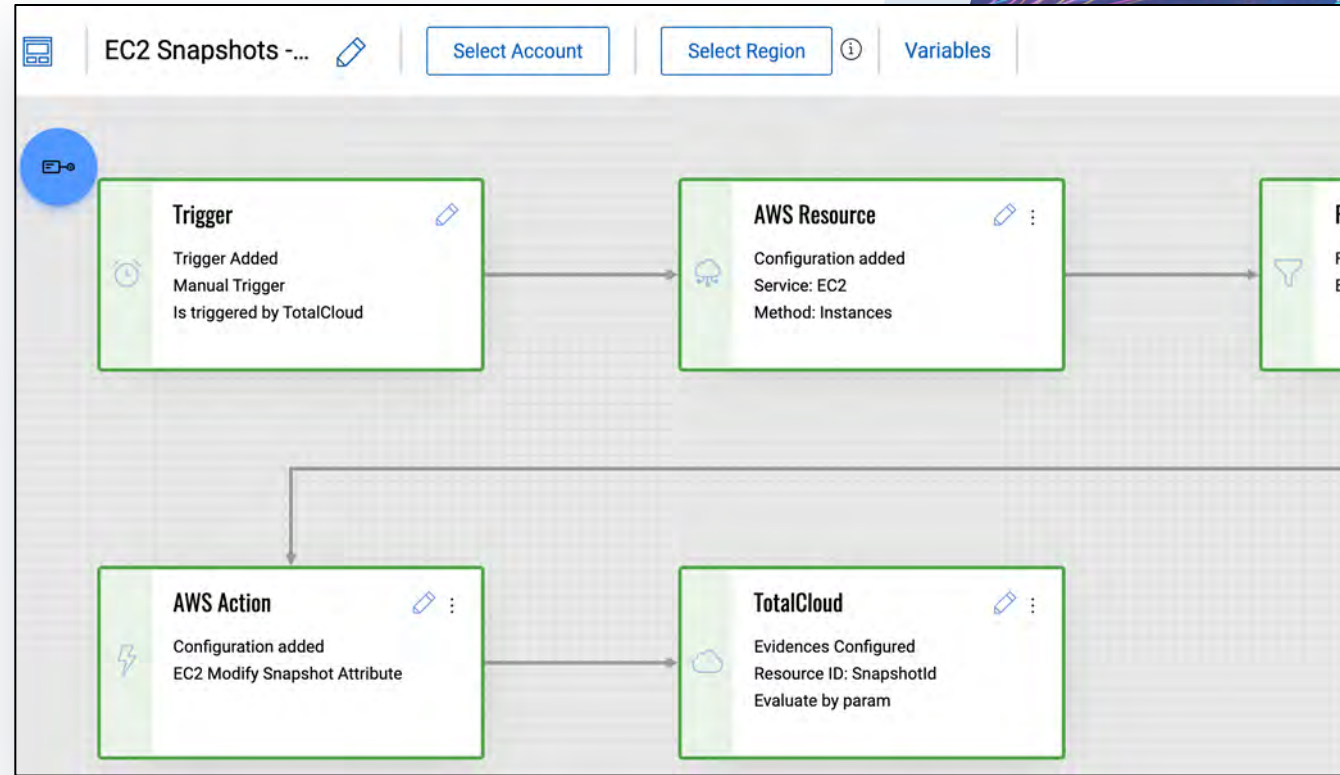
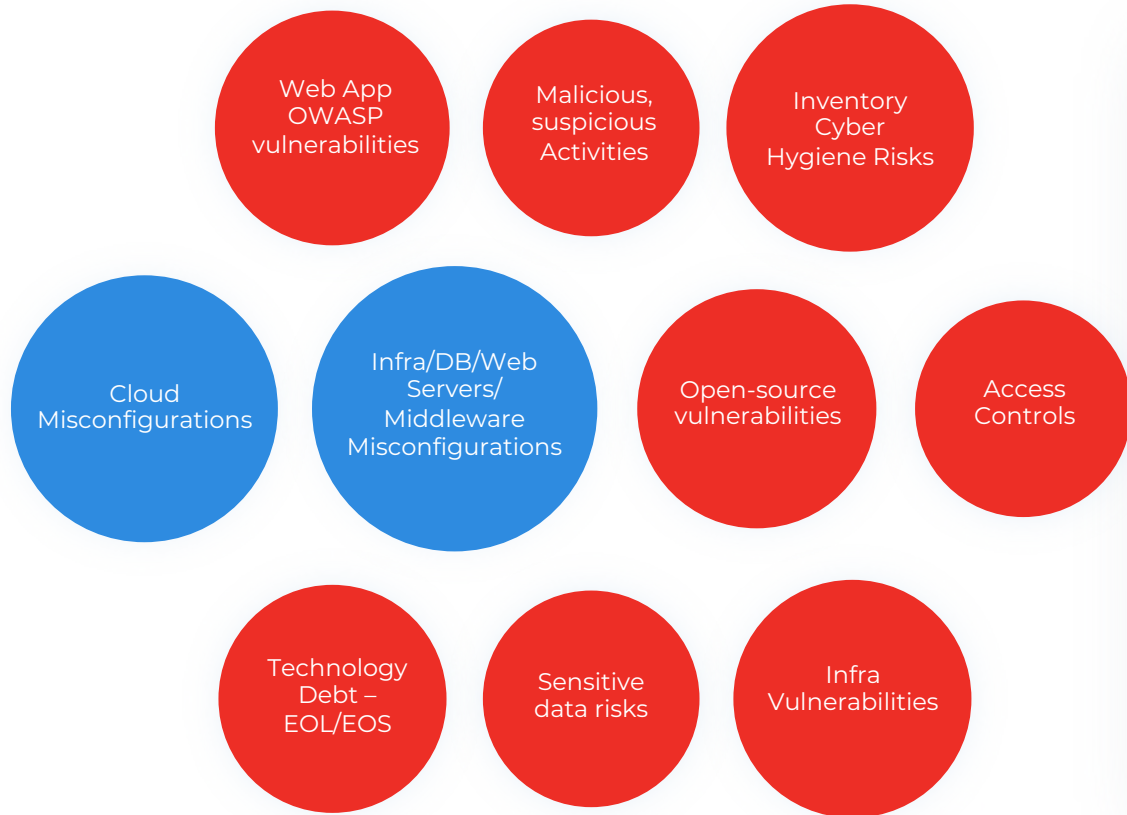
Eliminating Risk

Risk-based Elimination, for prioritized vulnerabilities



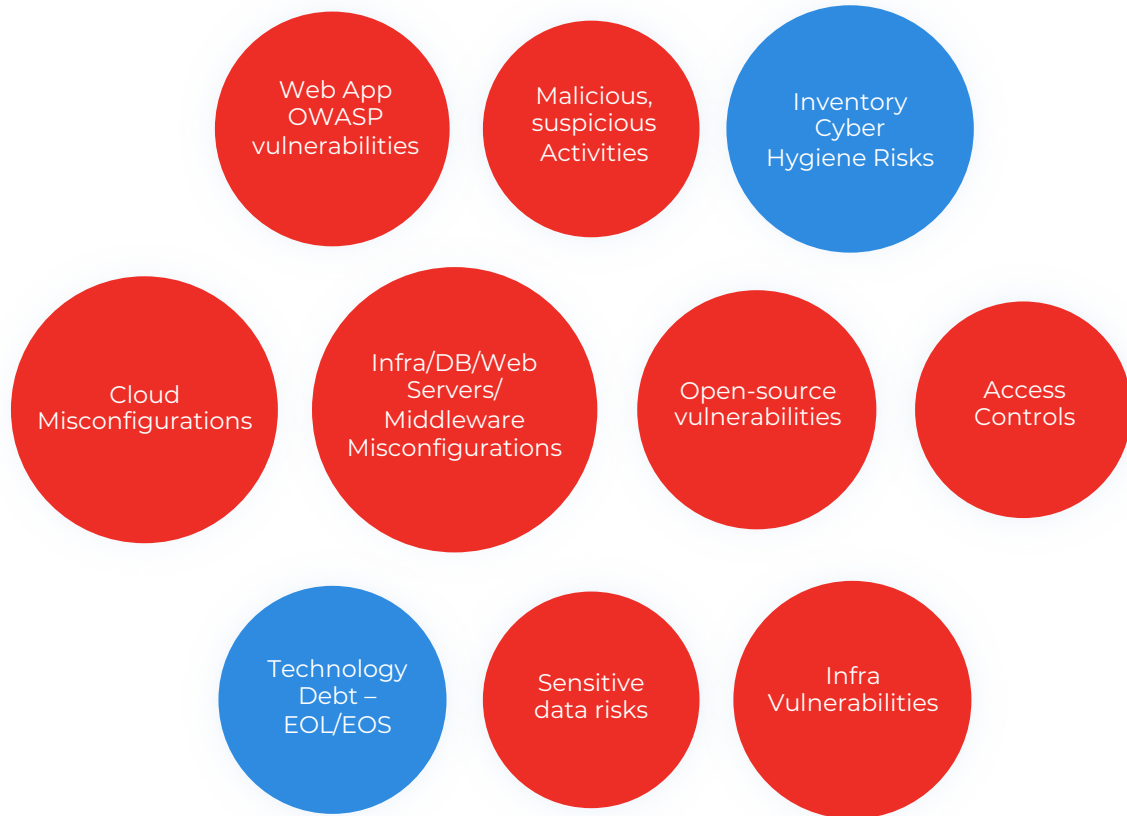
Eliminating Risk

Risk-based Elimination, for Cloud



Eliminating Risk

Risk-based Elimination, for Inventory



Qualys Cloud Platform
CyberSecurity Asset Management

DASHBOARD INVENTORY

CSAM EASM Assets Software Web Applications Open Ports

software: (authorization: 'Unauthorized')

202 Total Software

TOP SOFTWARE CATEGORIES

Network Appl... Databases Networking

LICENSE

Open Source	105
Commercial	97

PLATFORM

64-Bit	88
--------	----

LIFECYCLE

Beta	10
GA	2
EOL	1
EOL/EOS	160
Not Applicable	2

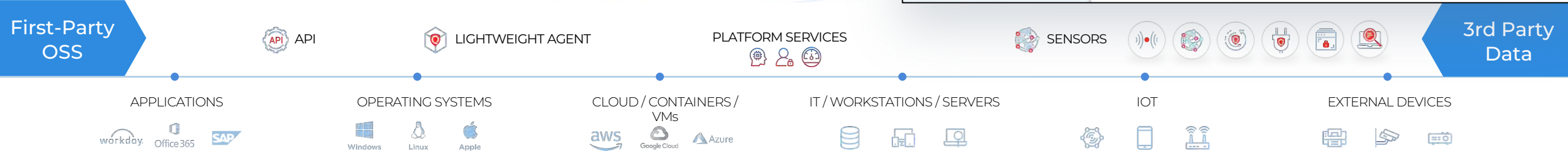
1 more

Group Software by... All Applications Others

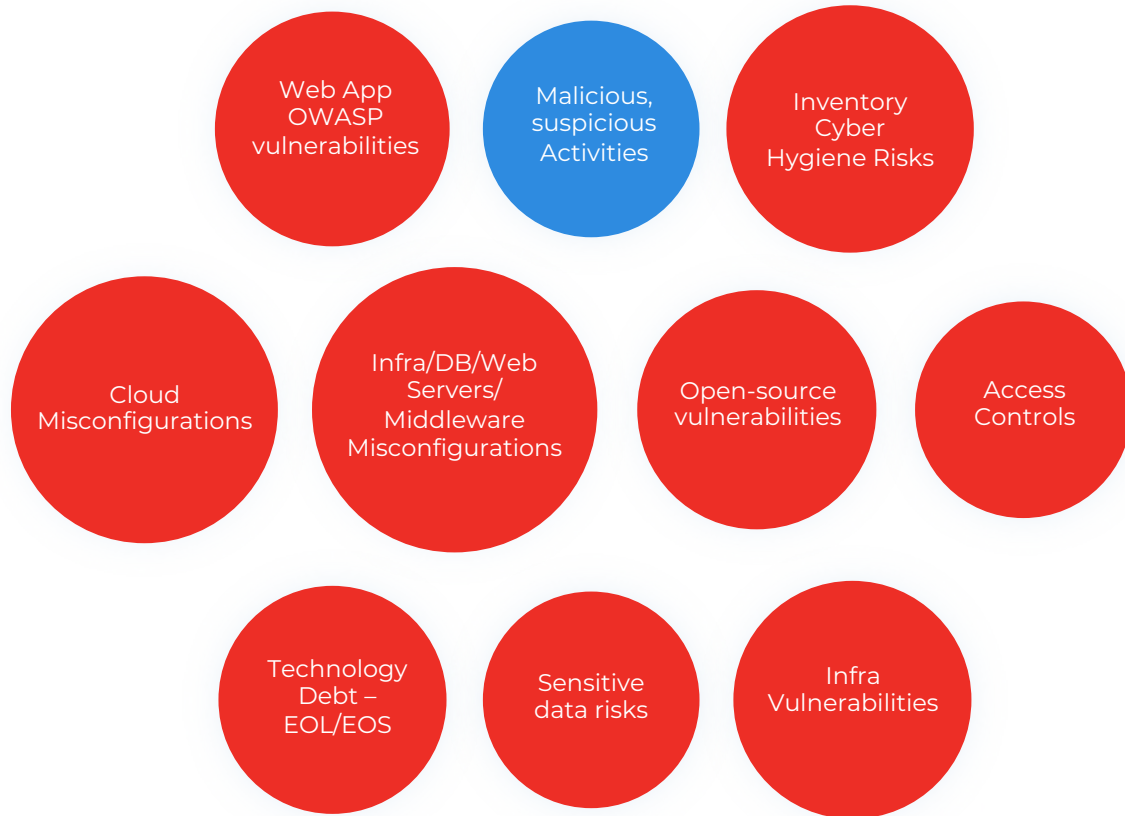
RELEASE	TYPE	CATE
<input checked="" type="checkbox"/> BitTorrent Client 7.10.5.45272	Application	Netw
<input type="checkbox"/> BitTorrent Client 7.10.5.45272	Application	Netw
<input type="checkbox"/> BitTorrent Client 7.10.5.45272	Application	Netw
<input type="checkbox"/> BitTorrent Client 7.10.5.45272	Application	Netw
<input type="checkbox"/> Google Chrome	Application	Netw

Quick Actions

- View Authorization Rule
- Add To Authorization Rule
- View Install List
- Download Install List
- Add to Existing Uninstall Job
- Create Uninstall Job



Not Just Eliminating, but Preventing Risk



Quyls Cloud Platform

Incident Details: Event Triggered Execution

VIEW MODE

Summary

Timeline

Process Tree

Risks and Exploits

Forensic Assistant

Risks and Exploits

Event Triggered Execution causing 33 Events
FJJ-Win10-CA-IOC

Risk Score 9

View Details in VMDR

Vulnerabilities

View Details in VMDR

QID	TITLE	CVE ID	QUALYS DETECTION SCORE
91951	Windows COM+ Event System Service Elevation of Privilege Vulnerability	CVE-2022-41033	97
91915	Windows Kerberos Elevation of Privilege Vulnerability	CVE-2022-30165	95
91929	Windows Network File System Remote Code Execution Vulnerability	CVE-2022-34715	96
91935	SMB Client and Server Remote Code Execution Vulnerability	CVE-2022-35804	97

MITRE ATT&CK Tactics and Techniques

TECHNIQUE ID	TECHNIQUE NAME
Q0013	Suspicious Powershell Command
T1003.001	OS Credential Dumping: LSASS Memory
T1016	System Network Configuration Discovery
T1018	Remote System Discovery
T1033	System Owner/User Discovery

ASSET DETAILS

FJJ-Win10-CA-IOC
OS: Windows

Identification

DNS Hostname: acmecorp.com
FQDN: FJJ-Win10-CA-IOC
IPv4: 172.16.197.89
IPv6: fe80:0:0:399b:b3c
Asset ID: 14492105
Resource ID:
Host ID:

Activity

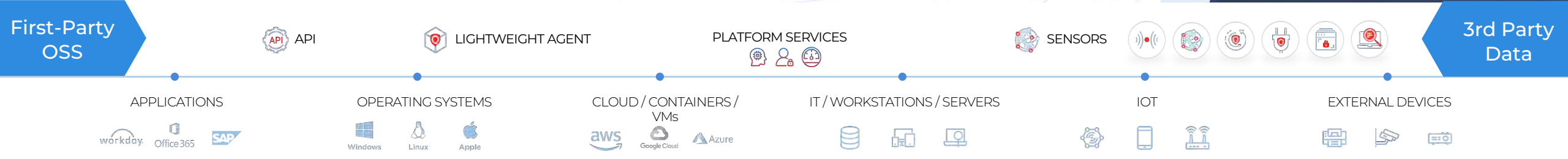
Last User Login: James Cooper
Last System Boot: 5 days ago
Created on: July 9, 2016
Last Checked In: 9 minutes ago

Location

Saratoga, California United States
Last Seen: 3 mins ago

Tags

OS: Windows | 64-bit-system-a... | ES
RJJ-Finance | Geo:USA | Port:139





Enterprise TruRisk™ Platform

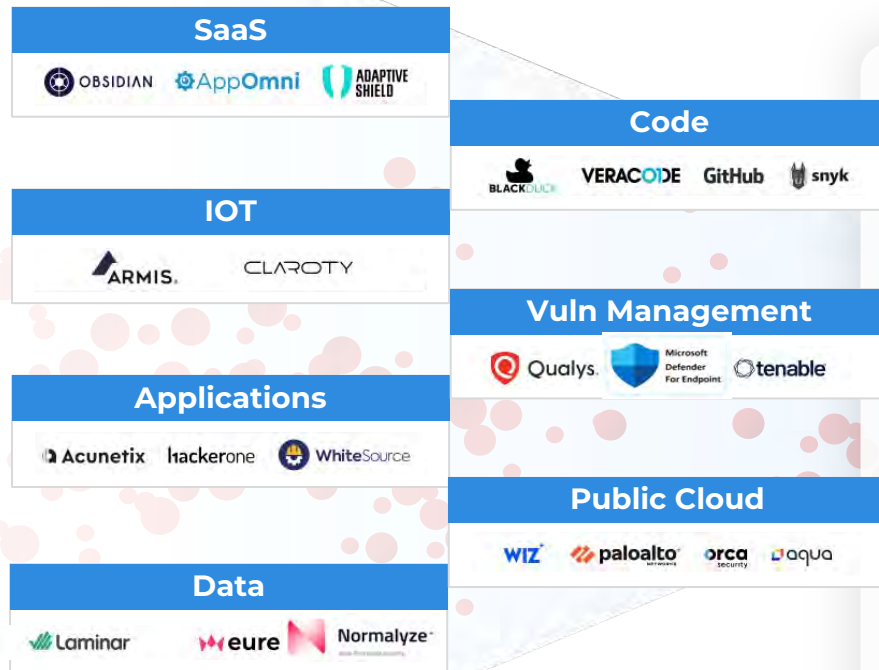
Measure, communicate, and eliminate cyber risk.

De-risk your business.

What's Next...

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

Communicate Risk

For Intrinsic Business Value & Loss

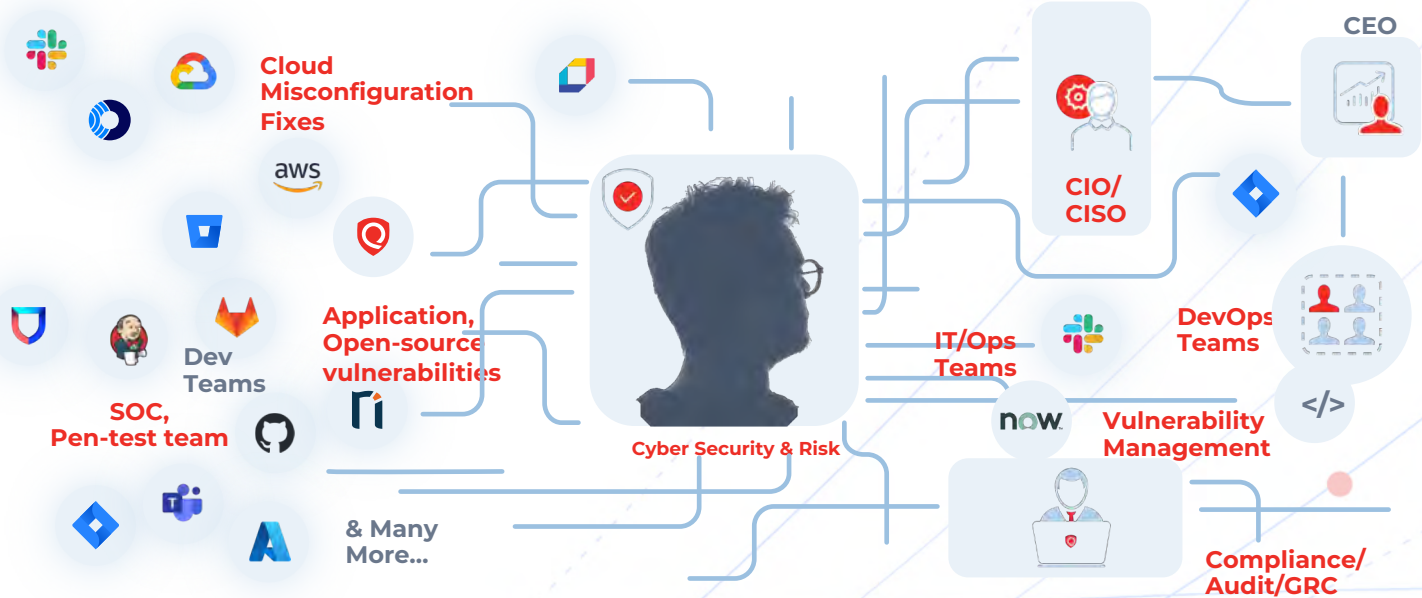
- 1** No Tie up for Cyber Risk to the Business Value & Loss.
What's the impact on business
- 2** Inability to communicate risk to right teams on their impact on organization's TruRisk



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

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

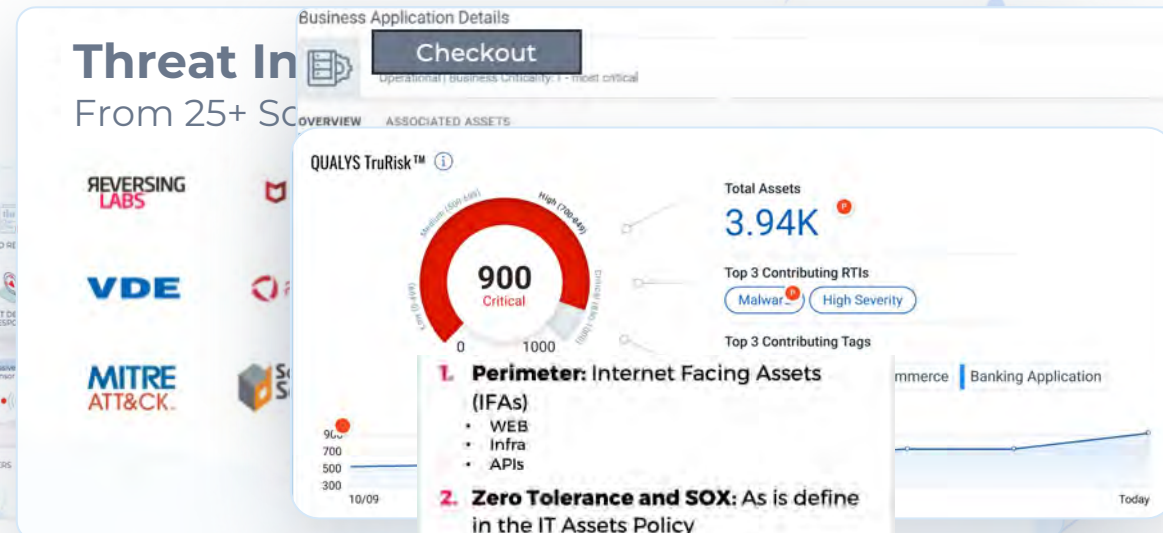
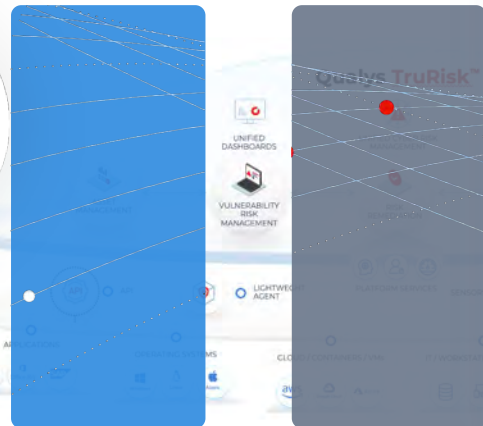
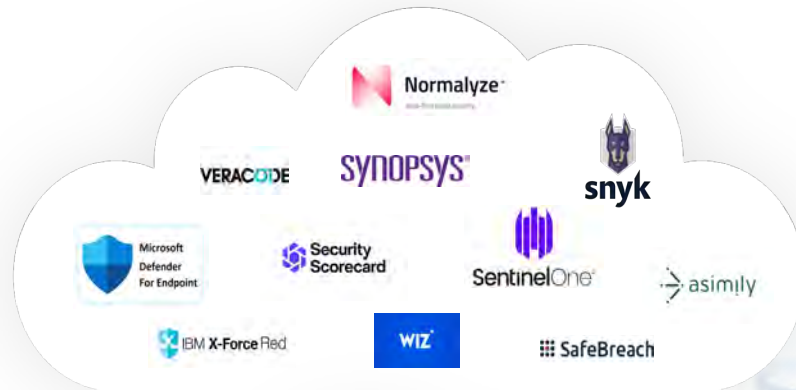
Top 10 Riskiest Vulns, not 0 days, Exploited by Threat Actors



30+ Days to remediate weaponized vulnerabilities

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

Measuring **TruRisk** Across Eco-System



The Qualys Solution set

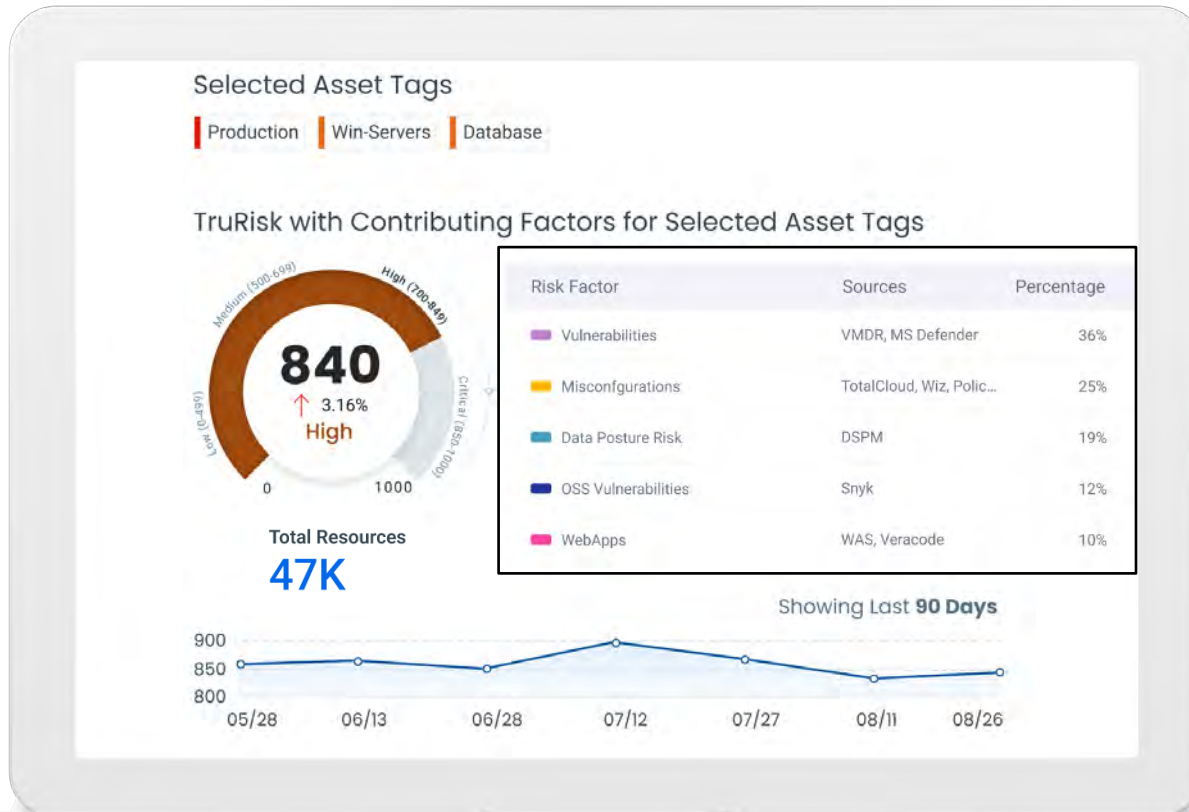
- Cyber Asset Attack Surface Management (CSAM)
- Application & API security
- External Attack Surface Management (EASM)
- Vulnerability Management Detection and Response (VMDR)
- TotalCloud
- Patch Management (PM)
- Policy Compliance (PC)
- ...and more

Normalization Correlation

1. Context

- Ransomware:** CVEs related to vulnerability
- Dark Web chatter:** CVEs related to your in
- Known Malware:** CVEs exploited by by known threat actors

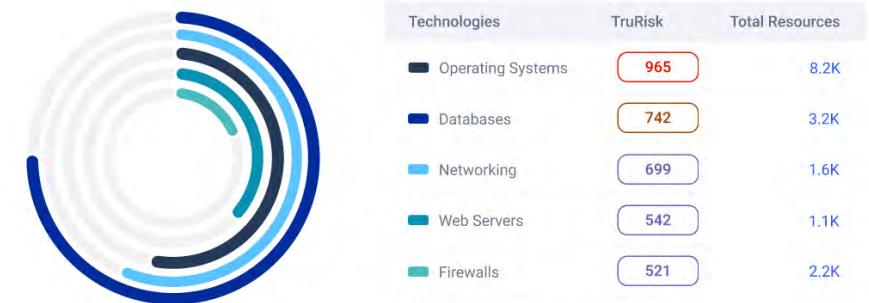
Measuring **TruRisk** Across the Eco-System



Top TruRisk Insights

Insight Title	Criticality ↓	Impacted Resources
Attempted Data Exfiltration from DB workload	Critical	25K
Publicly exposed VMs with critical exploitable vulnerabilities and high permission	Critical	12K
Publicly exposed containers with malware and critical vulnerabilities	Critical	9K
C2 HTTP/HTTPS detected on VM with a critical exploitable vulnerability	Critical	17K
C2 DNS detected on VM with a critical exploitable vulnerability	Critical	12K
Workloads with AWS secrets keys that can access sensitive data	High	26K
Misconfigured and exposed SSH port with active scanning	High	32K

Technologies



Communicating **TruRisk** to Executives in Language of **Business Value & Loss**

Business Apps

App Name	TruRisk ↓
Checkout App	890
Customer Support Portal	726
Quoting App	719
Sales Portal	702
Human Resources	550
Employee Portal	212

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.

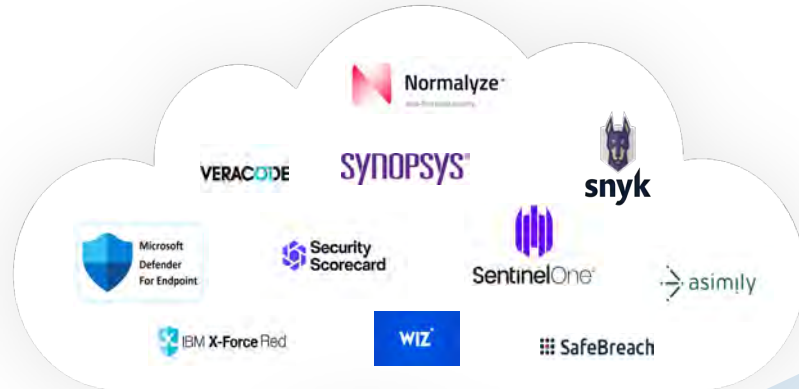
IBM Security benchmarks recommends a business value range of \$25M to \$35M for your industry

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

Cancel Save

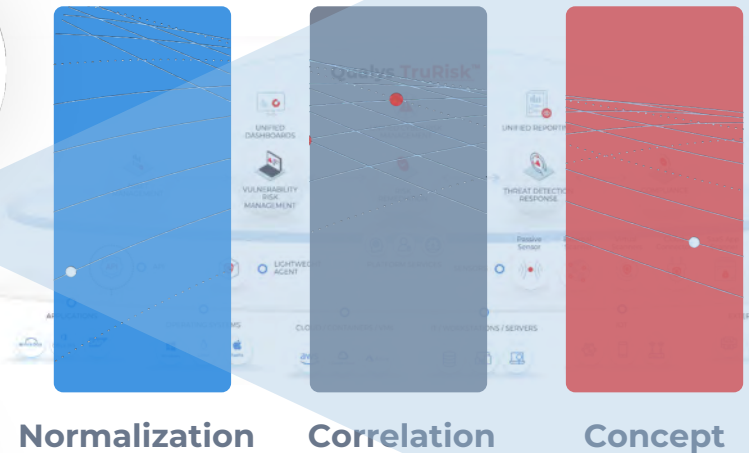
Communicating TruRisk

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

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

PLATFORM SERVICES



First-Party OSS



API



LIGHTWEIGHT AGENT



SENSORS

3rd Party Data

APPLICATIONS



OPERATING SYSTEMS



CLOUD / CONTAINERS / VMs



IT / WORKSTATIONS / SERVERS



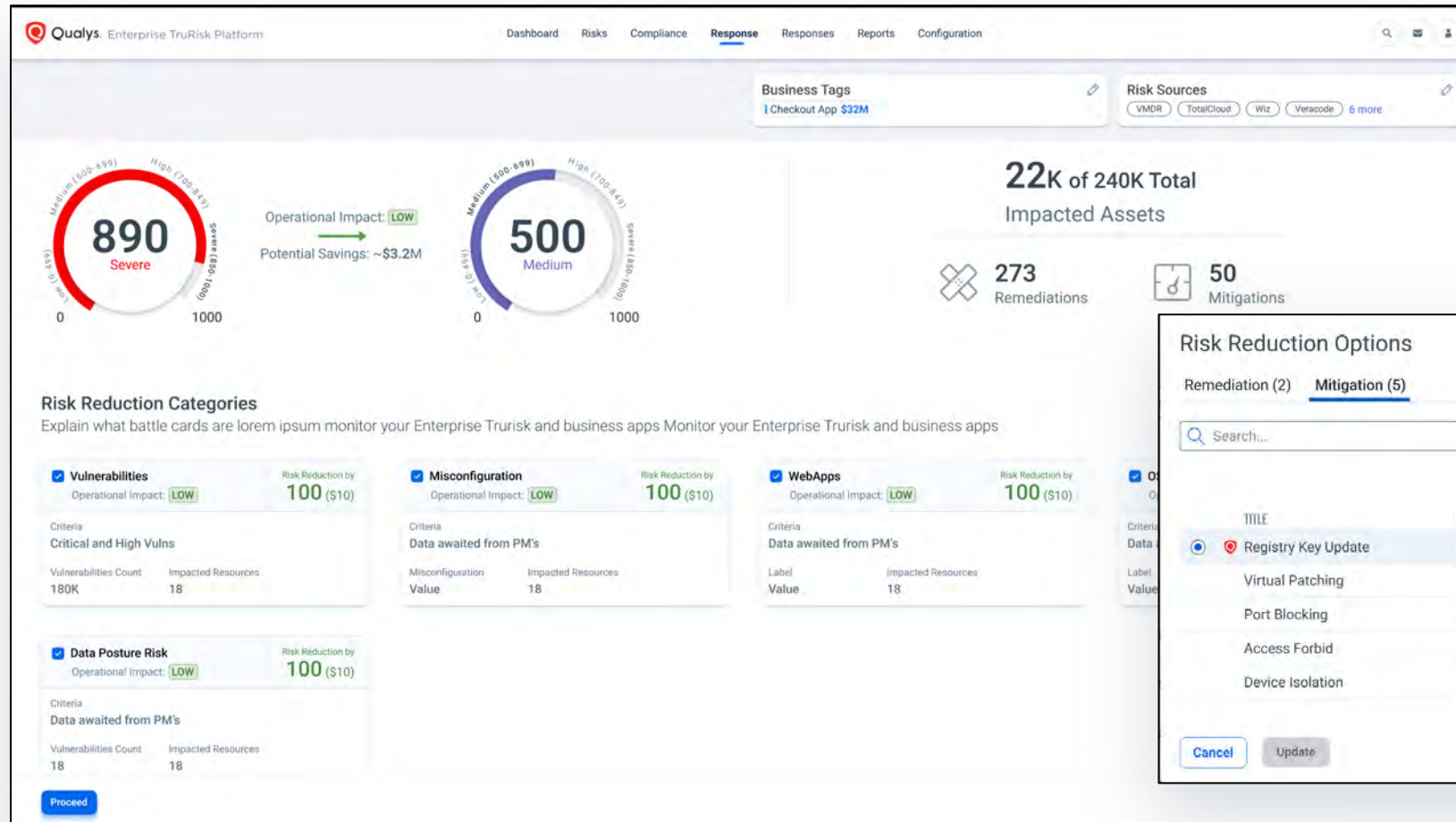
IOT



EXTERNAL DEVICES



Eliminating Risk ... with Techniques Beyond Patching, balancing Operational Impact



Risk Reduction Options

Remediation (2) **Mitigation (5)**

Search...

1 - 4 of 4

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

[Cancel](#) [Update](#)

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

Eliminating Risk Effectively

Personalized Risk Reduction Recommendations

Qualys Cloud Platform

VMDR Dashboard > Organization TruRisk > Risk Reduction Plan

← Risk Reduction Plan

SELECT REDUCTION PLAN ⓘ

<Plan Name 1 > 840 → 740
Operational Impact : Low

5	15	28/80	45/58
Patches	Mitigation	Total Assets	Vulnerabilities

<Plan Name 2 > 840 → 670
Operational Impact : Low

10	25	40/80	55/58
Patches	Mitigation	Total Assets	Vulnerabilities

<Plan Name 3 > 840 → 490
Operational Impact : High

15	35	78/80	57/58
Patches	Mitigation	Total Assets	Vulnerabilities

<Plan Name 1 >

Vulnerabilities Assets Affected Remediations Mitigations

Action (0) Group By: 1 - 50 of 50

QID	TITLE	QDS ⓘ	CATEGORY	ASSETS	REMEDIATION	MITIGATION
91774	Microsoft Paint 3D Remote Code Execution Vulnerability - June 2021	82	Vulnerability	pro-v14-sp1-u9 625800550	Serviceing stack update... Patch	Registry Key change Mitigation
91602	Microsoft Windows Security Update for August 2019	78	Vulnerability	pro-v14-sp1-u9 625800550	Security Update for Adobe Patch + Conf. Change	Device Isolation Mitigation
91560	Microsoft Windows Security Update for August 2019	78	Vulnerability	pro-v14-sp1-u9 625800550	Serviceing stack update... Patch	Process stop Mitigation
91724	Microsoft Windows Security Update for January 2021	82	Vulnerability	win2008-p-69-177 167659968	Security Monthly Rollup ... Patch	Proprietary script Partial Mitigation Change
91613	Microsoft Edge Security Update for March 2020	58	Vulnerability	win2008-p-69-177 167659968	Security Update for .NET Patch	Block access to file attrib... Mitigation
91686	Microsoft Windows TCP/IP Remote Code Execution Vulnerability	61	Vulnerability	win2008-p-69-177 167659968	KB5020439 (OS Build 1... Patch	Registry Key change Partial Mitigation



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.



