



# Measure, Communicate & Eliminate Your Cyber Risk with Qualys Platform

**Shailesh Athalye**  
**Senior VP Product Management, Qualys**

# Challenge of Measuring Risk

## 1. Need to Know Assets from Business Context

### CMDB != Inventory for Cyber Risk

- ⊗ Lacks Comprehensiveness
- ⊗ Lacks context from Business Criticality



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



# Challenges of Measuring Risk

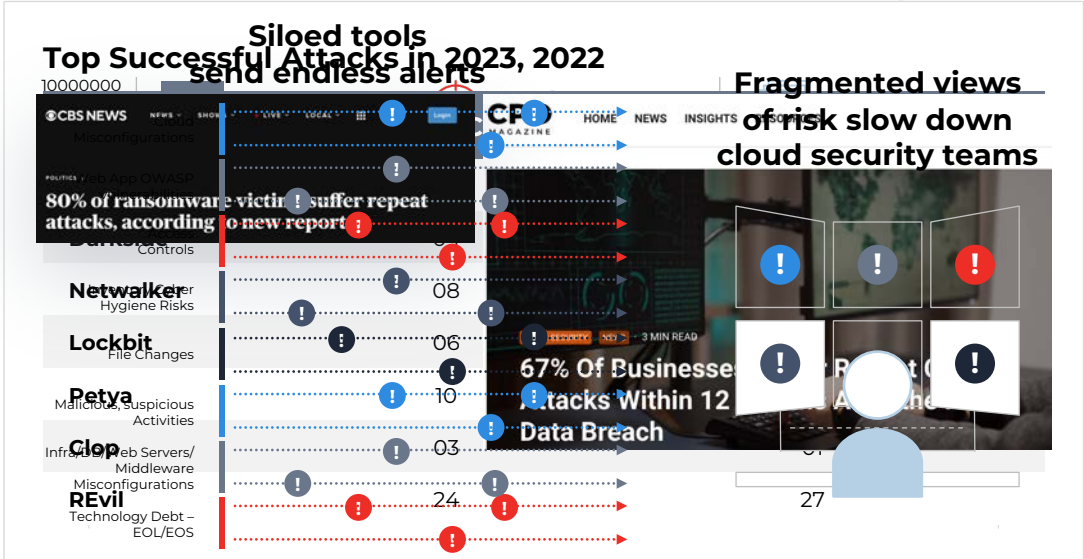
## 2. Context of Threats, Risk

⊗ Inability to collect data – Comprehensively & Accurately

⊗ Lack of Threat context

- 01 **Ransomware:**  
Vulnerabilities exploited in top attacks
- 02 **Dark Web chatter:**  
Vulnerabilities applicable to your industry talked in dark web
- 03 **Known Malware:**  
CVEs exploited by known threat actors

⊗ Unable to view unified ‘Toxic Insights’ from siloed findings



# Communicating Risk - Challenges

## Communication per Persona & their Roles...



### CISOs/Executives

What is business critical, overall picture



### Management/Leads

Cloud or web apps or infra vs app risks



### IT Operations - Fix

What to fix, so what? - priorities, how, beer (?)

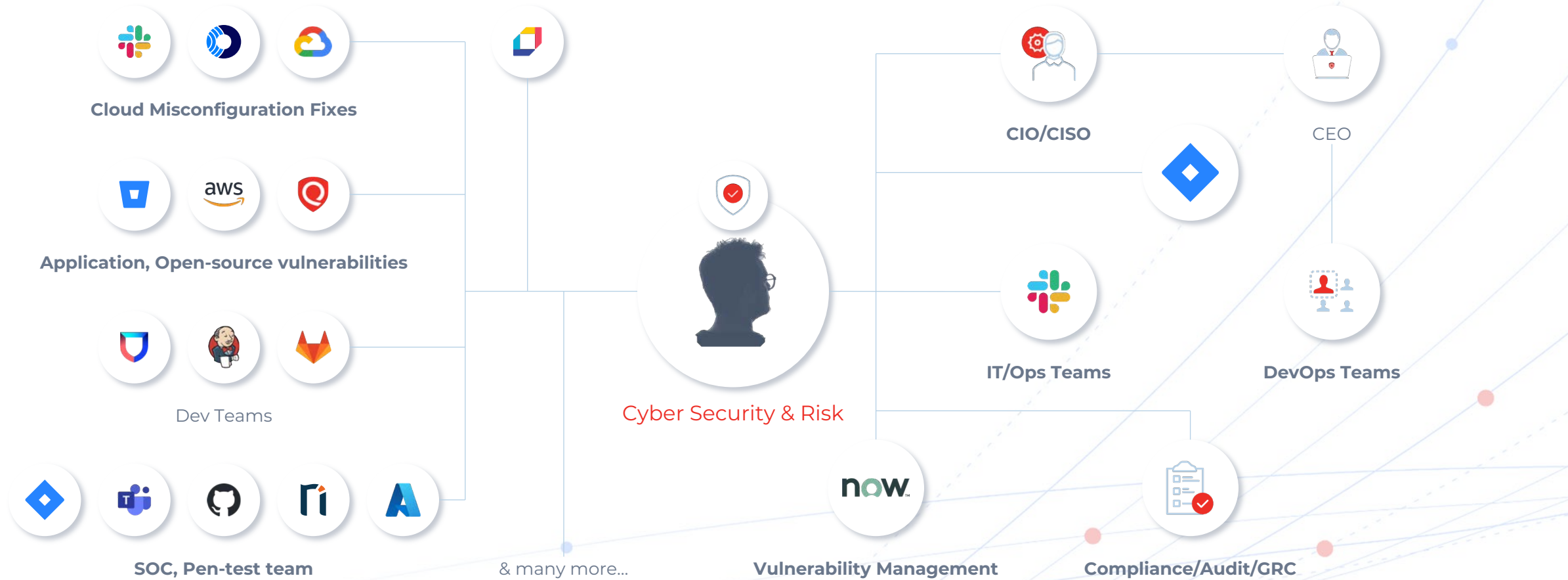


### Compliance - show Evidence

Regulatory/standards view, audit-ready

CVSS	Risk	Host	Protocol	Port	Name
	None	10.1.1.22	tcp	0	MS KB3152550: Update to Improve Wireless Mouse Input Filtering
	None	10.1.1.22	tcp	0	Microsoft Windows Hosts File
	None	10.1.1.22	tcp	0	Microsoft Windows PowerShell Execution Policy
	None	10.1.1.22	tcp	0	Microsoft Windows DNS Cache
	None	10.1.1.22	tcp	0	Internet Explorer Typed URLs
	None	10.1.1.22	tcp	0	MUICache Program Execution History
	None	10.1.1.22	tcp	0	Recent File History
	None	10.1.1.22	tcp	0	User Shell Folders Settings
	None	10.1.1.22	tcp	0	User Download Folder Files
	None	10.1.1.22	tcp	445	Microsoft Security Rollup Enumeration
	None	10.1.1.22	tcp	445	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
	None	10.1.1.22	tcp	445	Server Message Block (SMB) Protocol Version 1 Enabled
	None	10.1.1.22	tcp	445	Microsoft .NET Security Rollup Enumeration
	None	10.1.1.22	tcp	445	Microsoft Windows SMB Versions Supported (remote check)
	High	10.1.1.22	tcp	445	Windows Defender Antimalware/Antivirus Signature Definition Check
	None	10.1.1.22	tcp	445	Microsoft Windows Network Adapters
	None	10.1.1.22	tcp	3389	TLS Version 1.0 Protocol Detection
	None	10.1.1.7	tcp	3000	HTTP Server Type and Version
	None	10.1.1.7	icmp	0	ICMP Timestamp Request Remote Date Disclosure
	None	10.1.1.7	tcp	22	SSH Server Type and Version Information
	None	10.1.1.7	udp	0	Traceroute Information
	None	10.1.1.7	tcp	3000	Web Server No 404 Error Code Check
	None	10.1.1.7	tcp	22	SSH Protocol Versions Supported
	None	10.1.1.7	udp	123	Network Time Protocol (NTP) Server Detection
	None	10.1.1.7	udp	53	DNS Server Detection
	None	10.1.1.7	tcp	53	DNS Server Detection

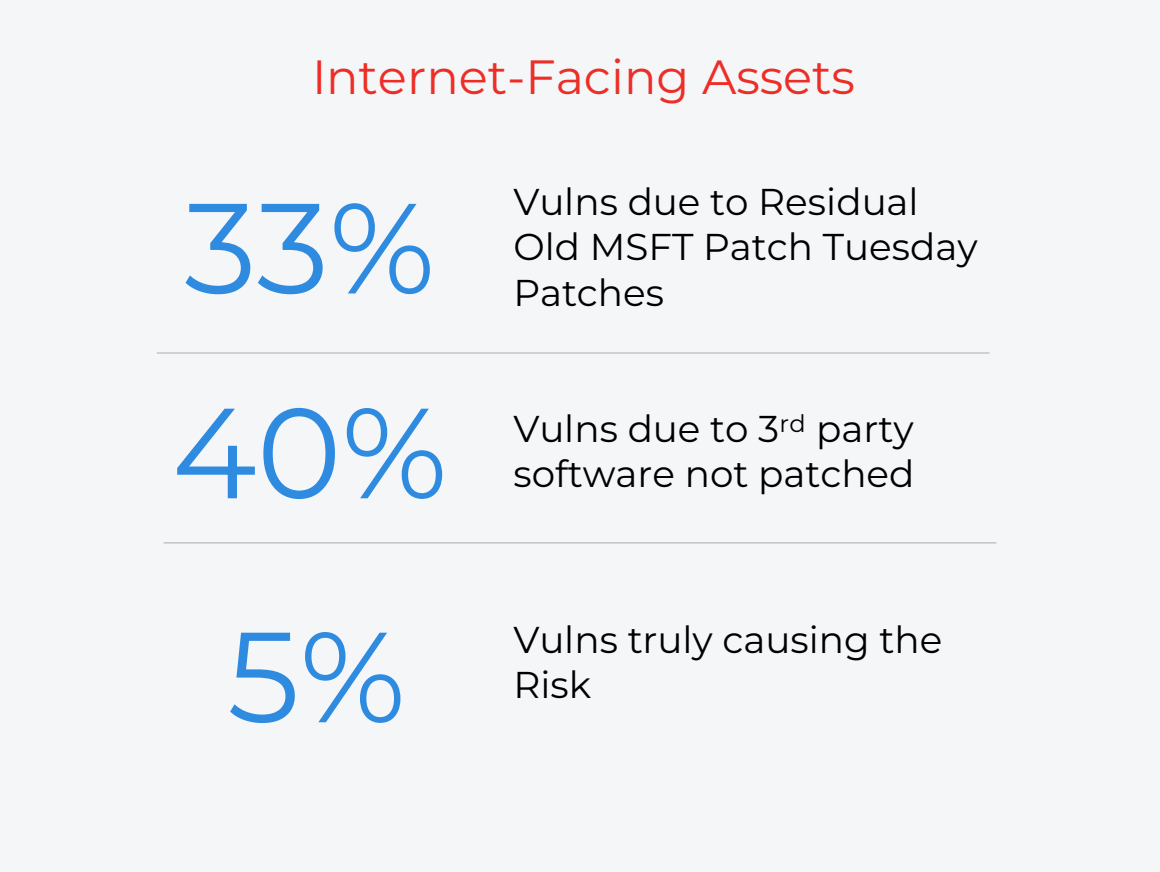
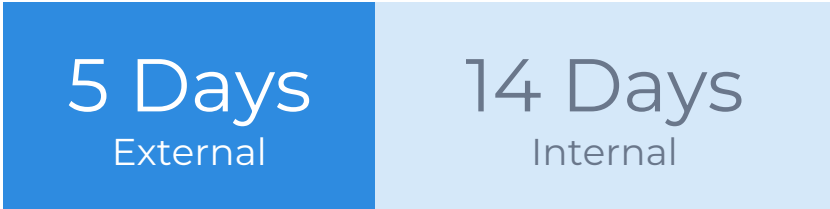
# Challenge of Communicating Right Data to Right Teams



# Challenges of Eliminating Risk Per SLA

## 3. Elimination of Risk per Aggressive Timelines in Limited Patching Cycles...

### NCSC Guidelines



# Qualys Enterprise TruRisk Platform



# Qualys Enterprise TruRisk Platform

Qualys  
TruRisk™



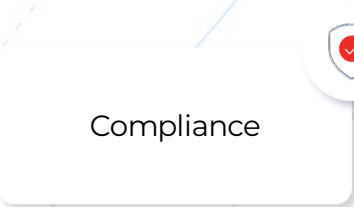
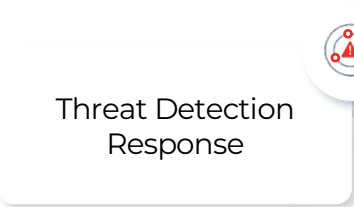
**Internal & External Inventory Risk Management with Business Context**

**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

Applications

Operating Systems

Cloud / Containers / VMs

IT / Workstations / Servers

IOT

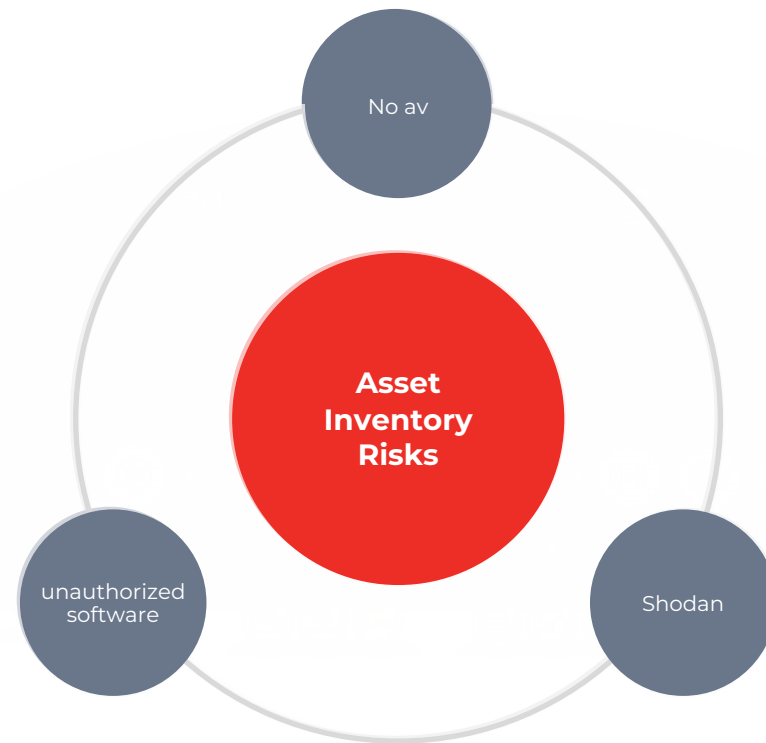
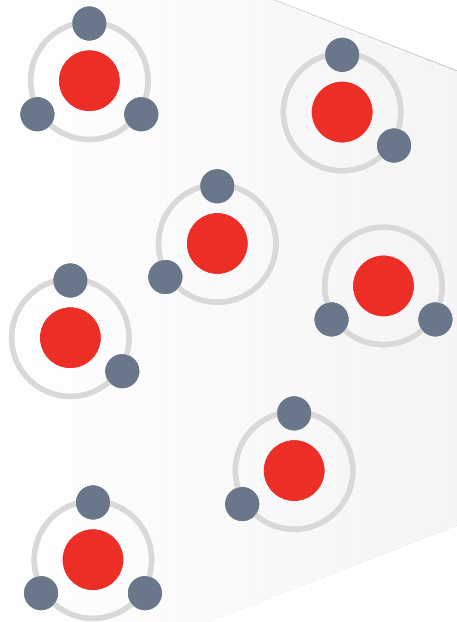
External Devices





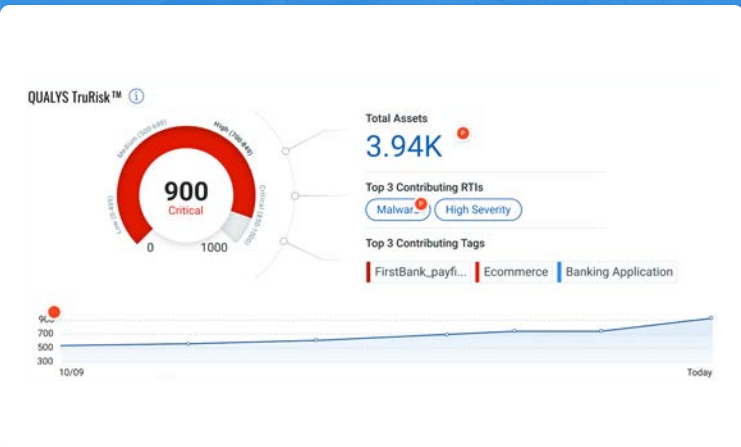
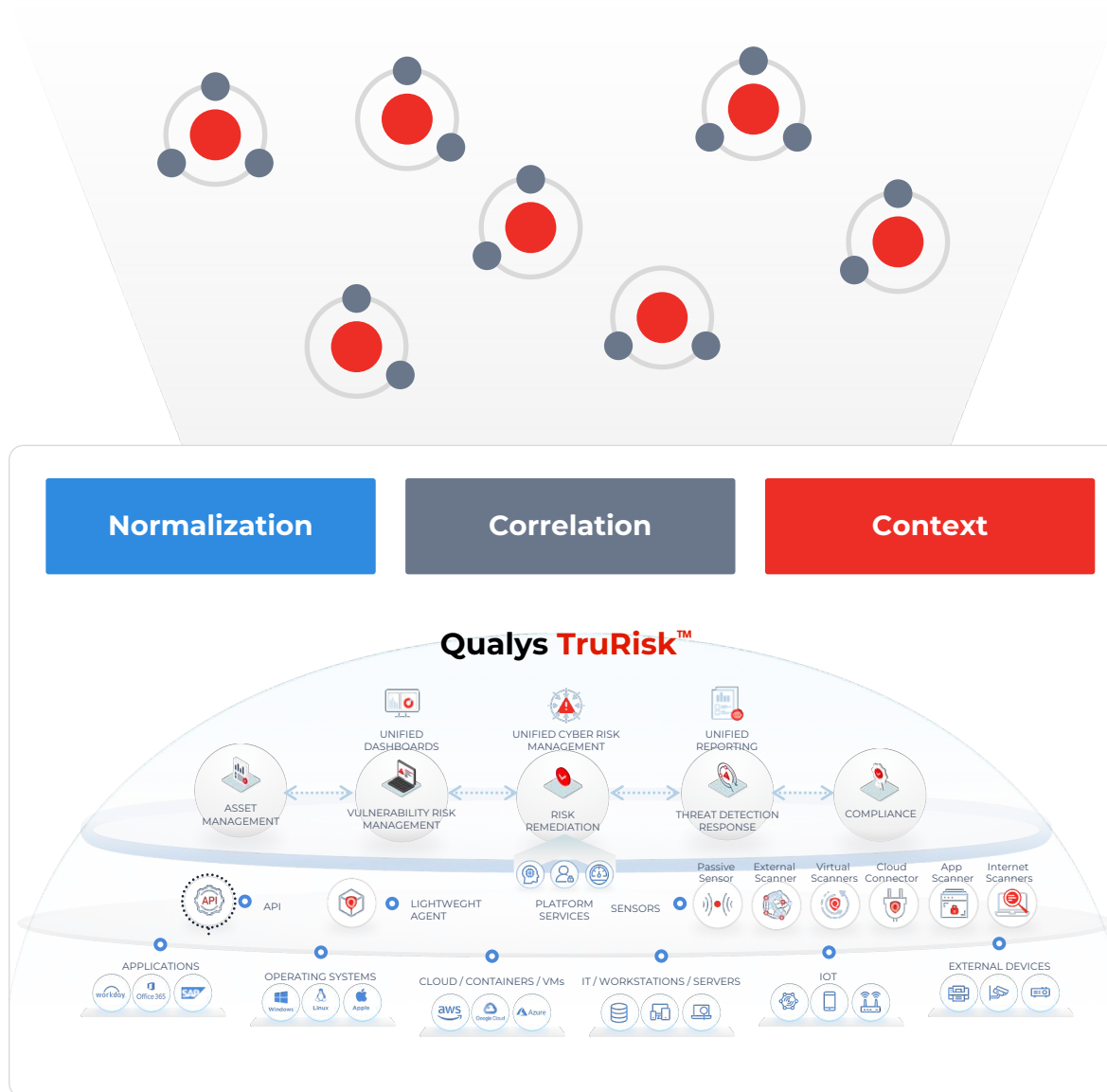
# Measuring TruRisk

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



# Measuring TruRisk

Collecting and Unifying Risk Factors, with Threat and Business Context

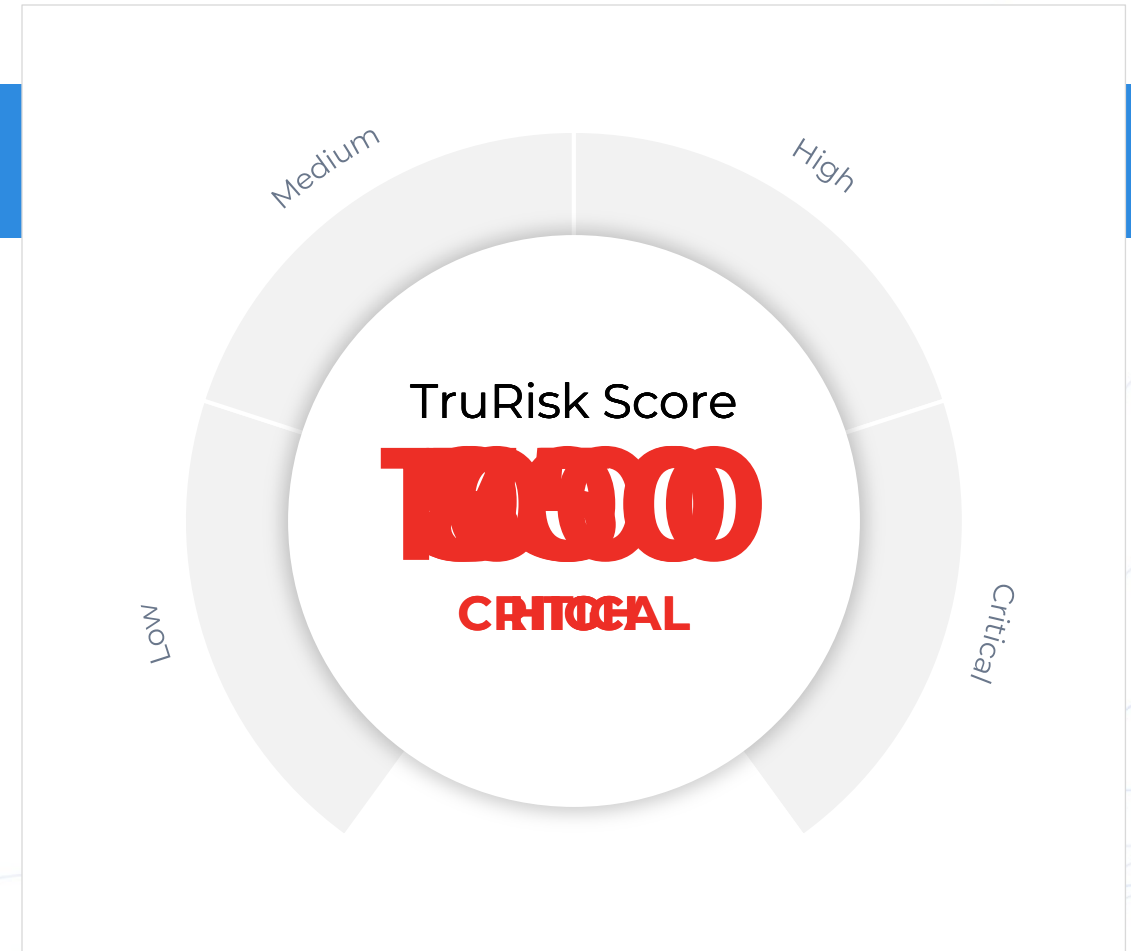


- 1 **Internet Facing Assets (IFAs)**
  - WEB
  - Infra
  - APIs
- 2 **Zero Tolerance and SOX**  
As is define in the IT Assets Policy
  - DMZ (Front, Back)
  - Authentication (AD, ADFS, LDAP)
  - Payment and Cards System
  - AML
  - GSNET
  - SOX Systemps
- 3 **Workstations**
- 4 **Internals**  
Any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

# TruRisk... By Correlating Security Data

## Contributing Factors

- External facing
- Ransomware vulnerabilities
- RDP misconfiguration
- Business-critical asset
- Not running Anti-virus software



# Step 0 of Measuring Risk

## Continuous Internal and External Attack Surface Management

01

### Manage Inventory Risk with Cyber Risk & Business Context

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

02

### 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



# Qualys Cloud Agent Passive Sensor

## Continuous Internal Attack Surface Discovery

### ✓ Discover unknown rogue devices passively using same 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

### ✓ DNS Based Sensing

No more spouses' phones coming in your Qualys Environment










# Communicating Risk

## Contextual Communication Per Persona/Responsibilities

### External Attack Surface Summary Report

GENERATED FOR Acme Corporation

#### External Attack Surface Summary

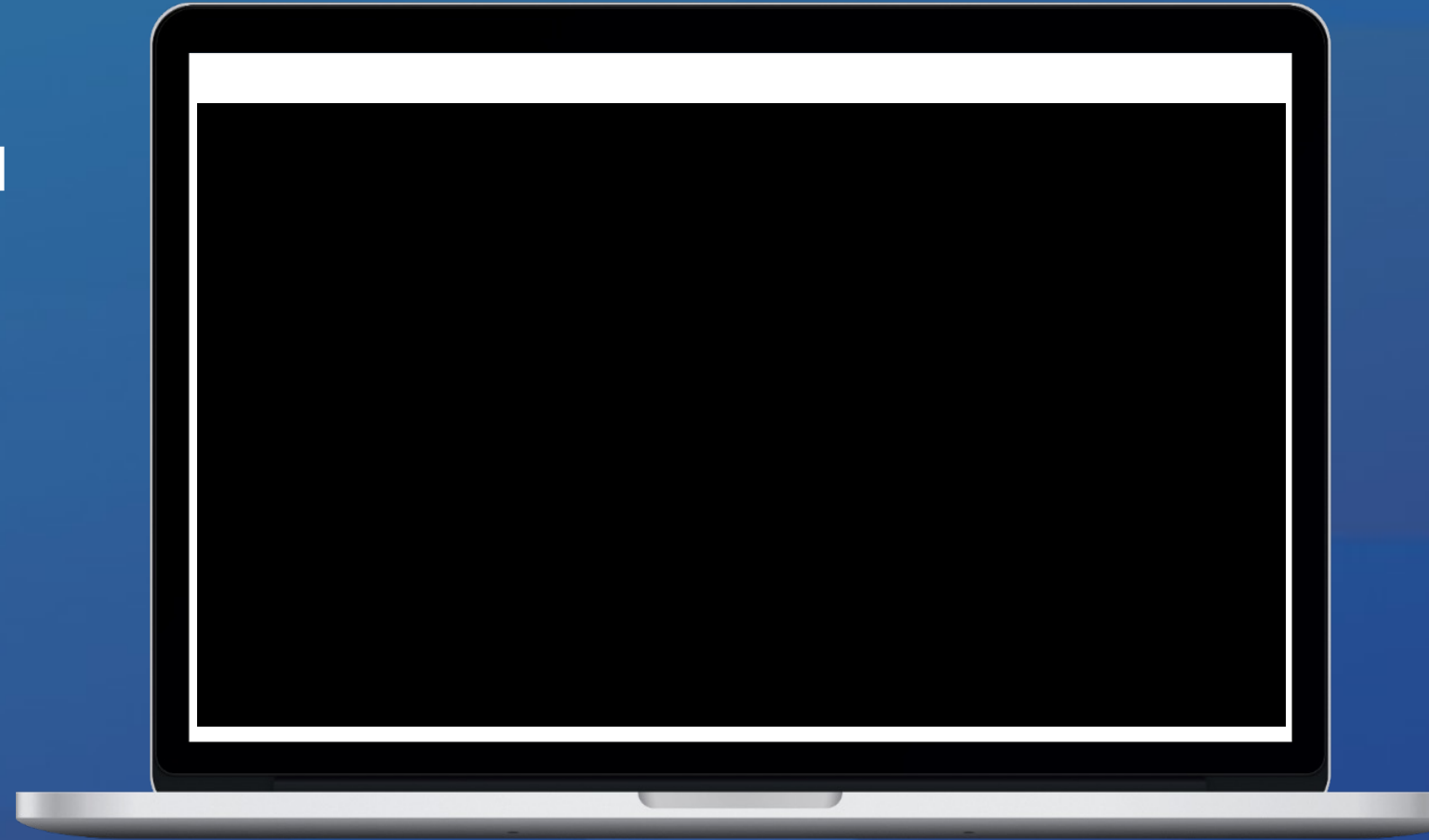
 <b>2.78K</b> Total Internet-facing Assets	 <b>2.78K</b> Assets missing in VMDR	
 <b>8</b> Organization/Subsidiaries	 <b>66</b> Domains	 <b>1.55K</b> Subdomains
 <b>2</b> Databases	 <b>1.09K</b> Web Servers	

### 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**

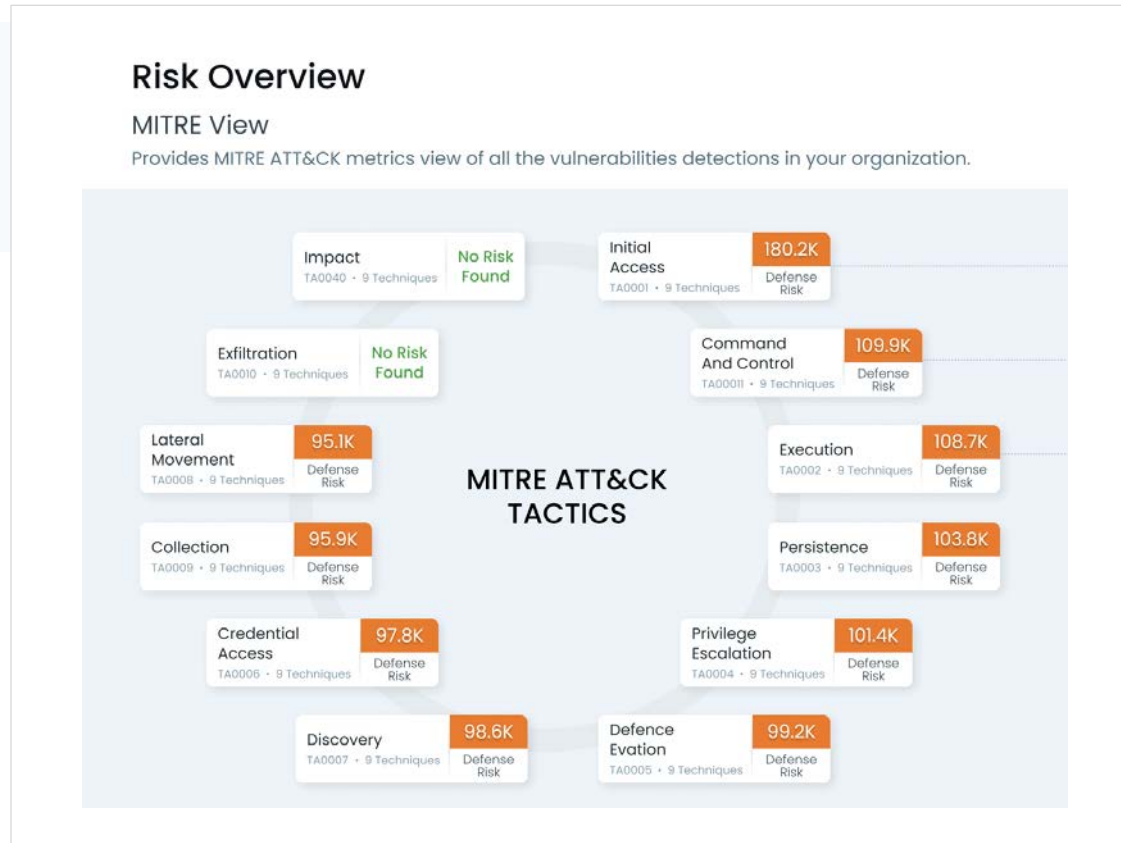
# Tech-Debt (EoL/EoS) Risk Report

- 1. View Your Tech-Debt (EoL/EoS) across hybrid environment**
- 2. Proactively plan of upgrade of upcoming EoL/EoS**
- 3. TruRisk Based Prioritization**



# Communicating Risk (SOC)

## 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



# Communicating Compliance

## Be-Audit Ready, without Putting in Manual Efforts of Mapping Compliance

Category	Status	Pass	Fail	Warn
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

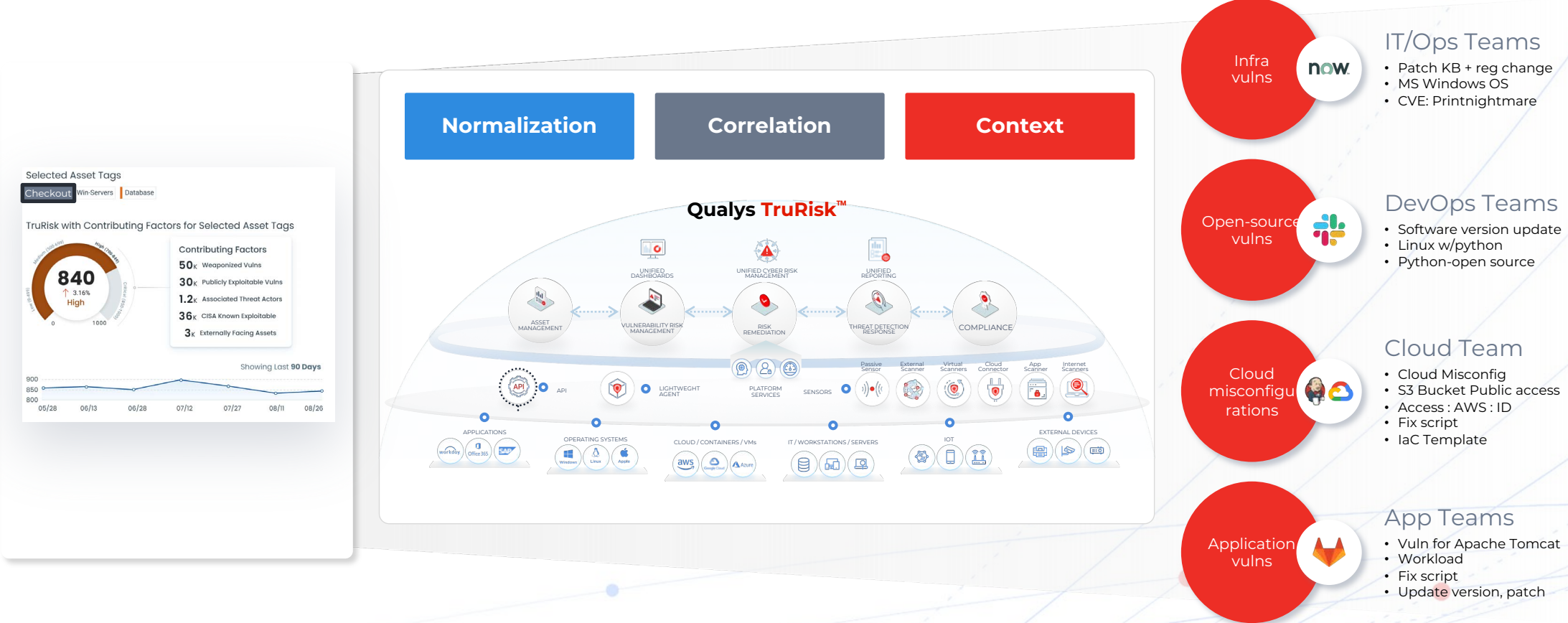
#	Policy	IP	Network	Tracking	Technology	Criticality	Last Evaluated	Posture
1.	ALL - CIS Benchmark for Ubuntu Linux	10.115.97.202	BU-NET-RDLABs	IP	Ubuntu 18.x	URGENT	07/26/2023 at 11:38:50 AM (GMT-0400)	FAIL
2.	PCD_Demo NIST 800-53 Rev 5 for Linux v2.0	10.11.110.51	BU-NET-RDLABs	IP	Red Hat Enterprise 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 **TruRisk** to Right People

Reducing **Time to Communicate** to Remediate faster, close security issues faster!



# Put Communication of Risk To Right People with Right Context on **Auto Pilot**

**Rule Details**  
Provide the following information to create the rule

**Rule Information**

Rule Name \*  
Create Tickets in ServiceNow

Description \*  
For Critical Vuls create tickets in ServiceNow

**Rule Query**

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

Search query \*

Vulnerabilities ▼ vulnerabilities.vulnerability.category:"SCA" and vulnerabilities.vulnerability.qid:985157 × ?

Assets ▼ tag.name: 'EASM' × ?

Sample Queries

Test Query

**Trigger Criteria**  
Provide the match criteria

Trigger Criteria \*  
Single Match ▼

**Action Settings**  
Choose an appropriate alert action

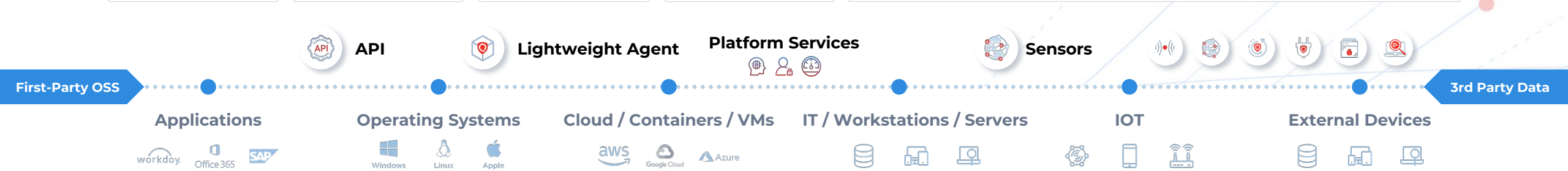
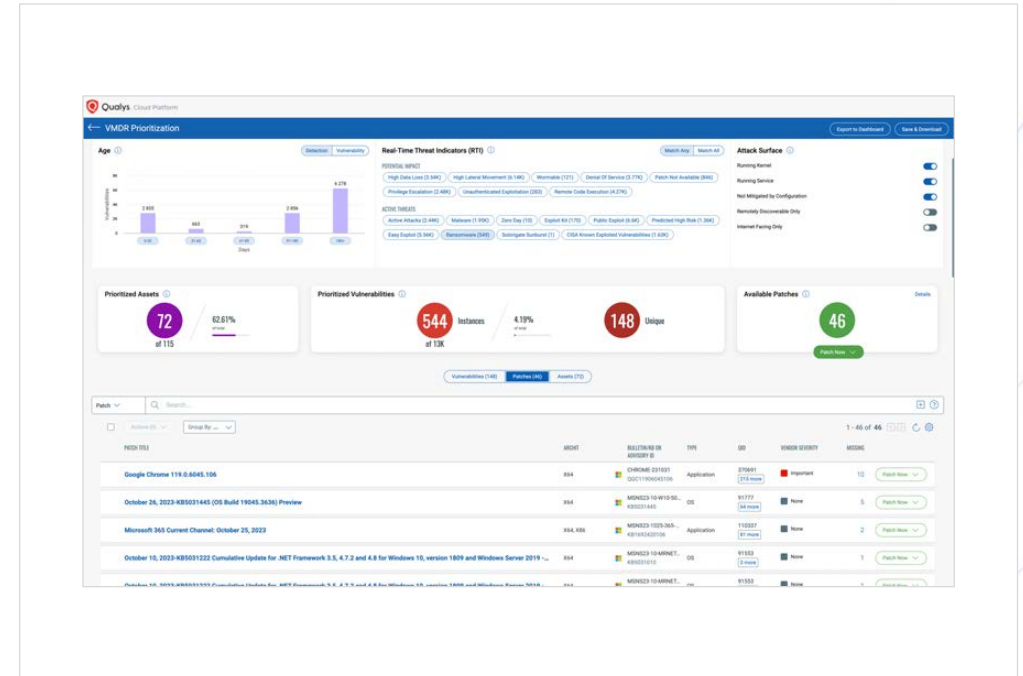
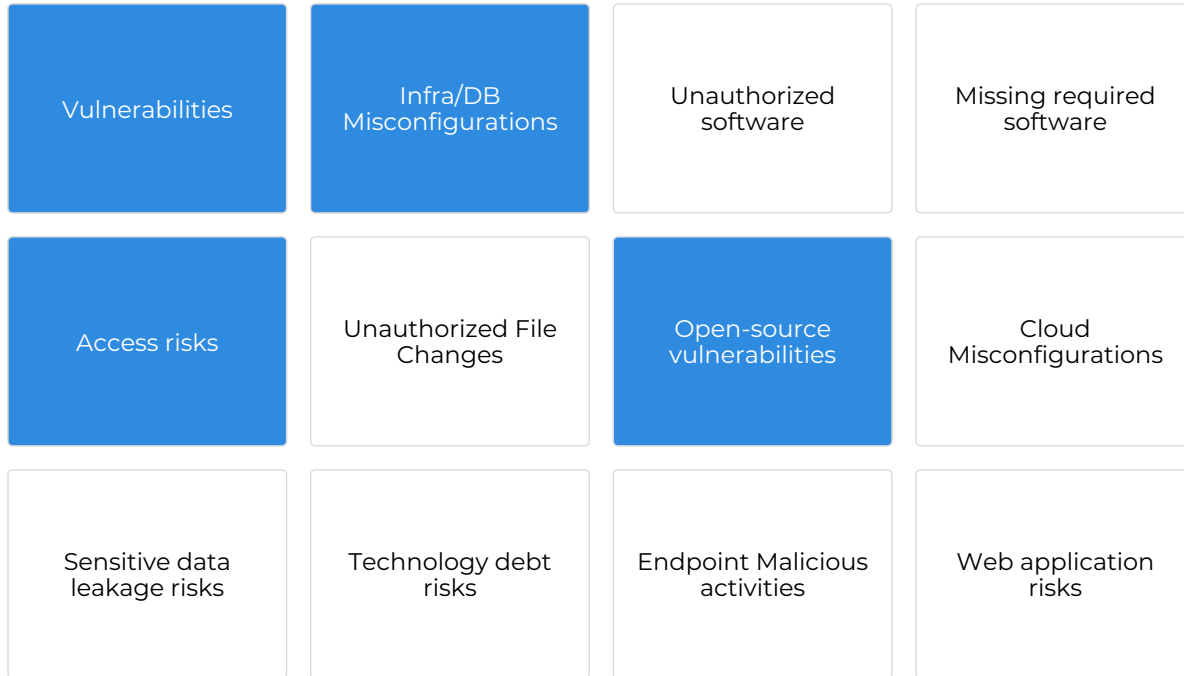
Actions \*  
ServiceNow: Push Mechanism × ▼

## Reduces Time & Efforts to Respond

- ✓ Auto ticketing to reduce efforts
- ✓ Rule-based ticketing, ownership assignment, and auto closure
- ✓ Manage change approvals and deploy remediations directly from ITSM

# Eliminating Risk Comprehensively

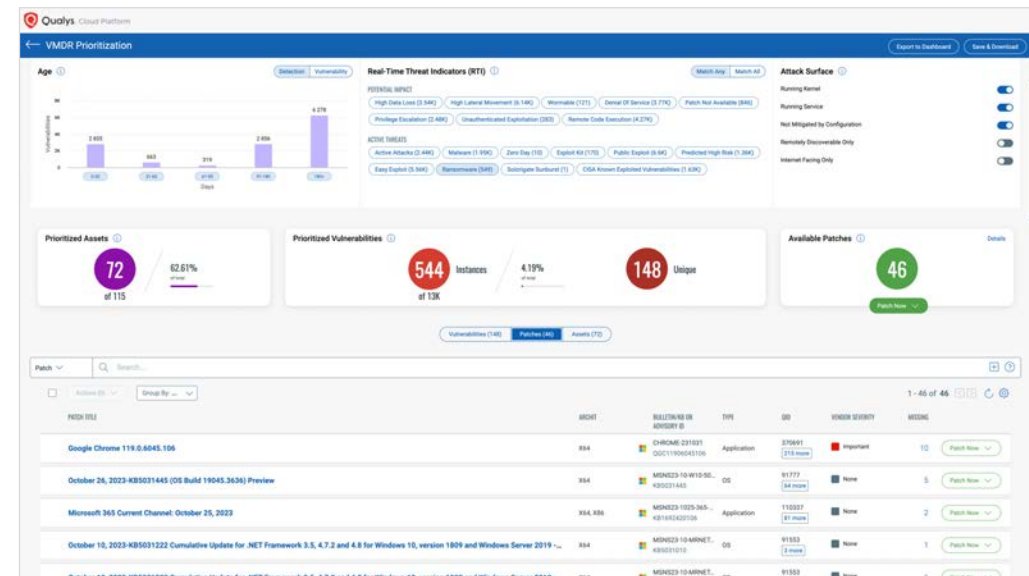
## Across Risk Factors



# Eliminating Risk of **Vulnerabilities** Which Matter the Most!

Risk-Based Remediation for Mac, Linux, Windows and 100+ 3<sup>rd</sup> party software

- ✓ Auto Maps Right Remediations to Right Vulnerabilities
- ✓ Drives Remediation Plans to Reduce Risk, Count of Risky vulnerabilities
- ✓ Rule-based, RBAC, ITSM-Integrated Controlled Automation



# Impact of Qualys Patch Management

54M

Patches Deployed  
Last Year

35%

Avg reduction in  
MTTR

60%

Reduction in vulns  
on internet-facing  
assets within

5

days

5% customers in 0-5 days MTTR

9% customers in 6-10 days

32% customers in 11 to 17 days

Prevented 8  
out of Top 10  
Ransomware  
Attacks, including:

- ✓ Conti
- ✓ Lockbit
- ✓ ClOp
- ✓ Petya
- ✓ REvil

# 30-Days Free Service to Eliminate Risk, Aligning with NCSC Guidelines

01

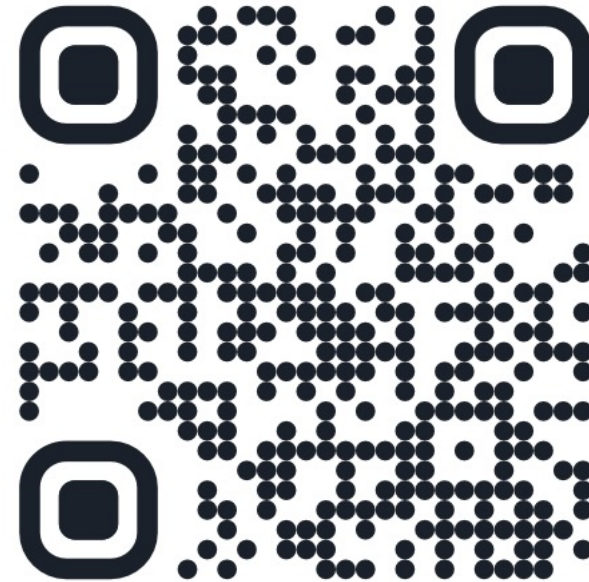
Know External-Facing Assets

02

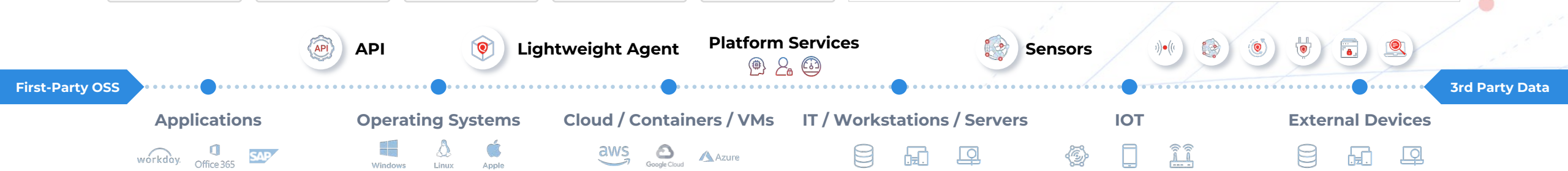
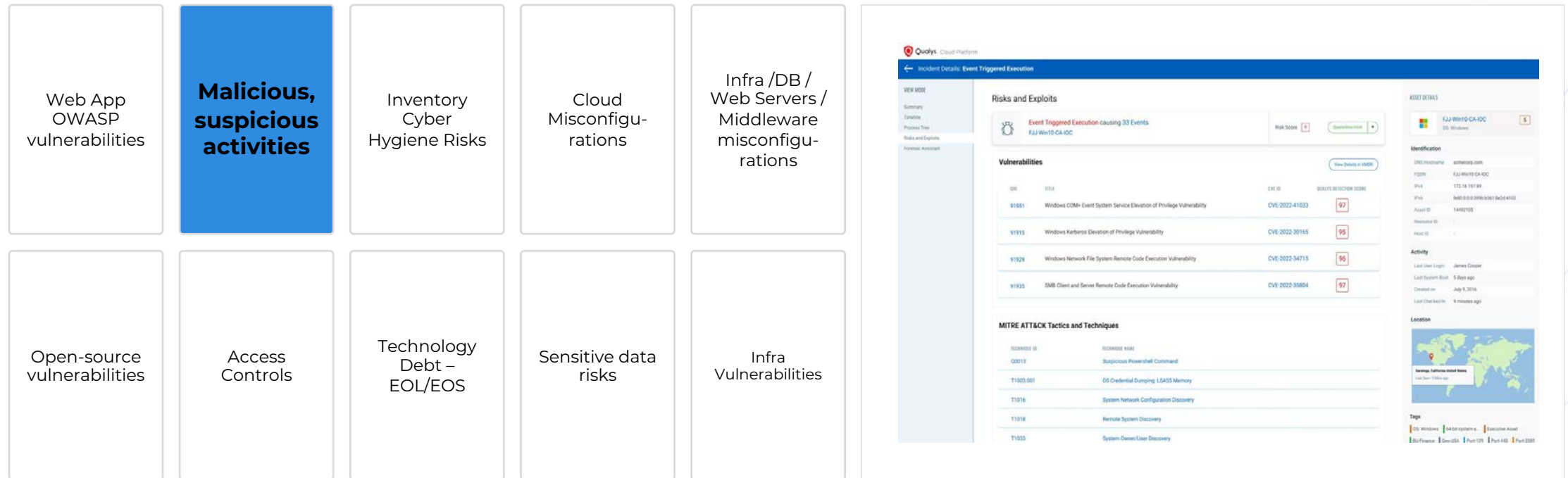
Prioritize Risky Vulnerabilities - Ransomware, CISA/NCSC/Malware-exploited

03

Automated, Smart Patch deployment to eliminate within 5 days, suited for your environment

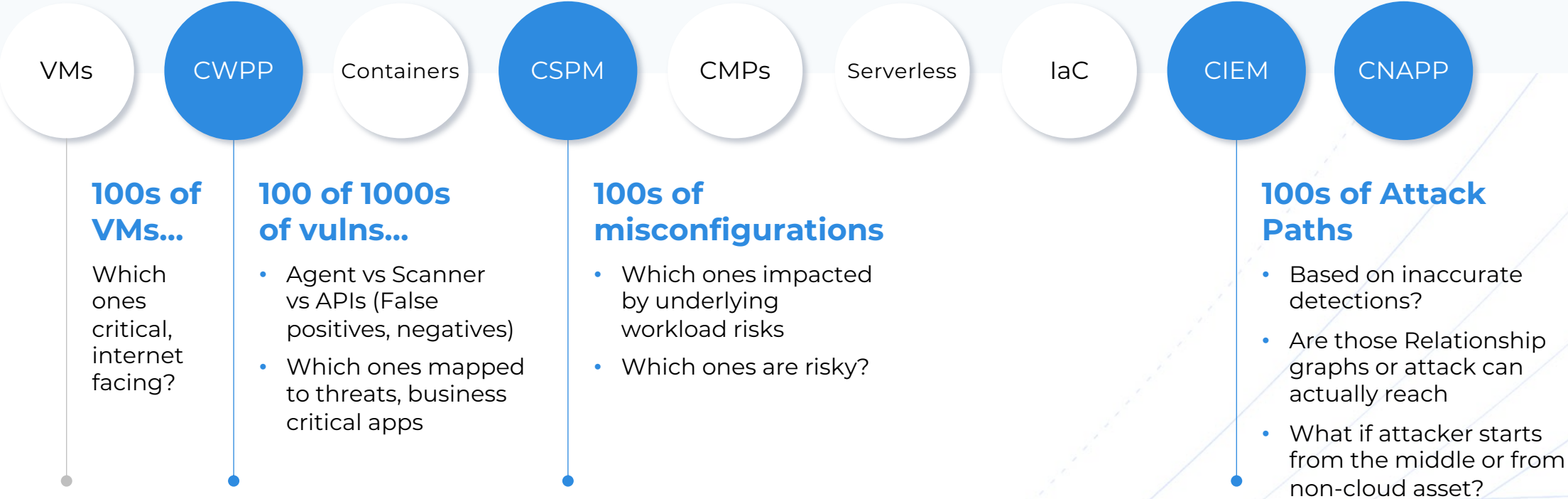


# Endpoint Detection & Response w/Prevention





# Questions Raised Due to Siloed Cloud Security



**I need a tool which shows accurate vuln data, and risk as when I am compromised, I can't tell management – I had tool with good looking UI – Banking Customer**

# Extending the Power of TruRisk for Cloud

## TruRisk™ Score



**Cloud Security Posture Management (CPSM)**



**External Facing Assets**  
CISA-known Exploitable Vulnerability



**Suspicious Connection**  
Cloud Detection and Response (CDR)

68  
External Facing Assets

14%

# What's Next...



# Further Challenges of Measuring Risk

Every tool is measuring risk differently, what are top 10 Risks?

## SaaS



## IOT



## Applications



## Data



## Code



## Vuln Management



## Public Cloud



### Qualitative

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

### Quantitative

- ⊗ 10, 50, 100
- ⊗ 1-5

### CVSS

- ⊗ 1-10



# Communicate Risk

For Intrinsic Business Value & Loss

**01** Need to Prioritize Cyber Risk  
per Business Value & Loss  
What's the impact on business

**02** Inability to Know  
Contributions by each Risk  
Finding to communicate with  
Correct Priority



# Communicate Risk

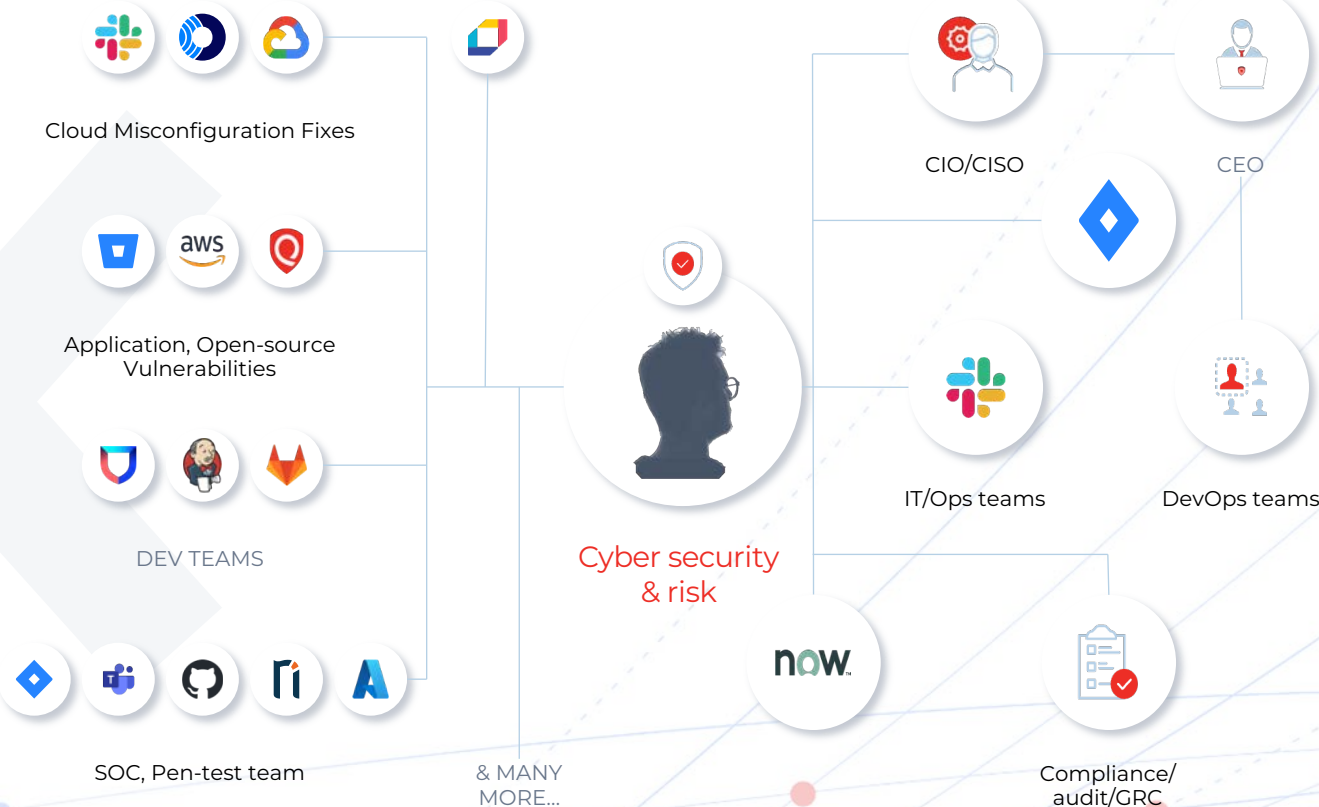
## Challenge of Communicating Right Data to Right Team



### 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

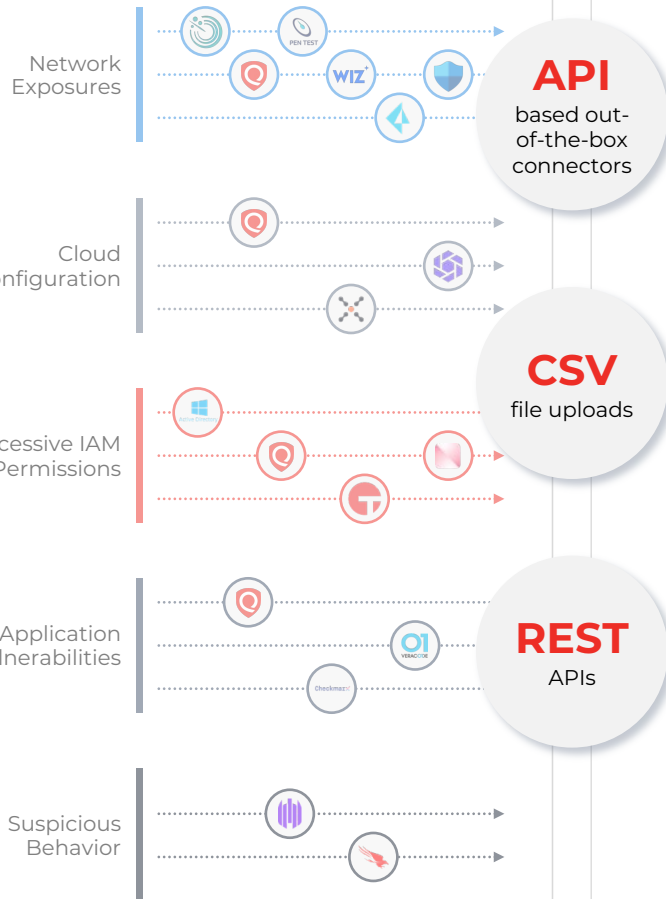
Amplified by \*10



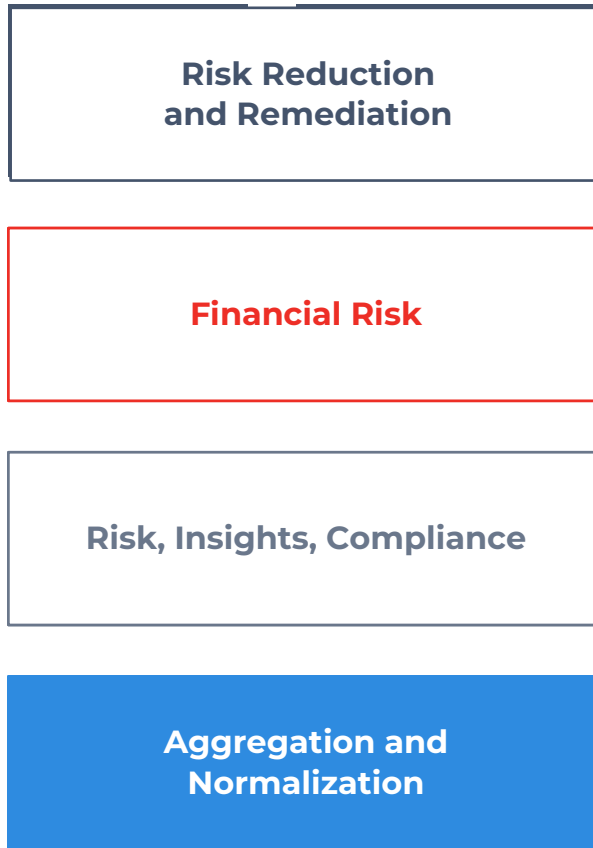
# Extending the Power of the Qualys TruRisk Platform for **Your Security Eco System**



## Siloed tools send endless alerts



## Qualys Enterprise True Risk Platform

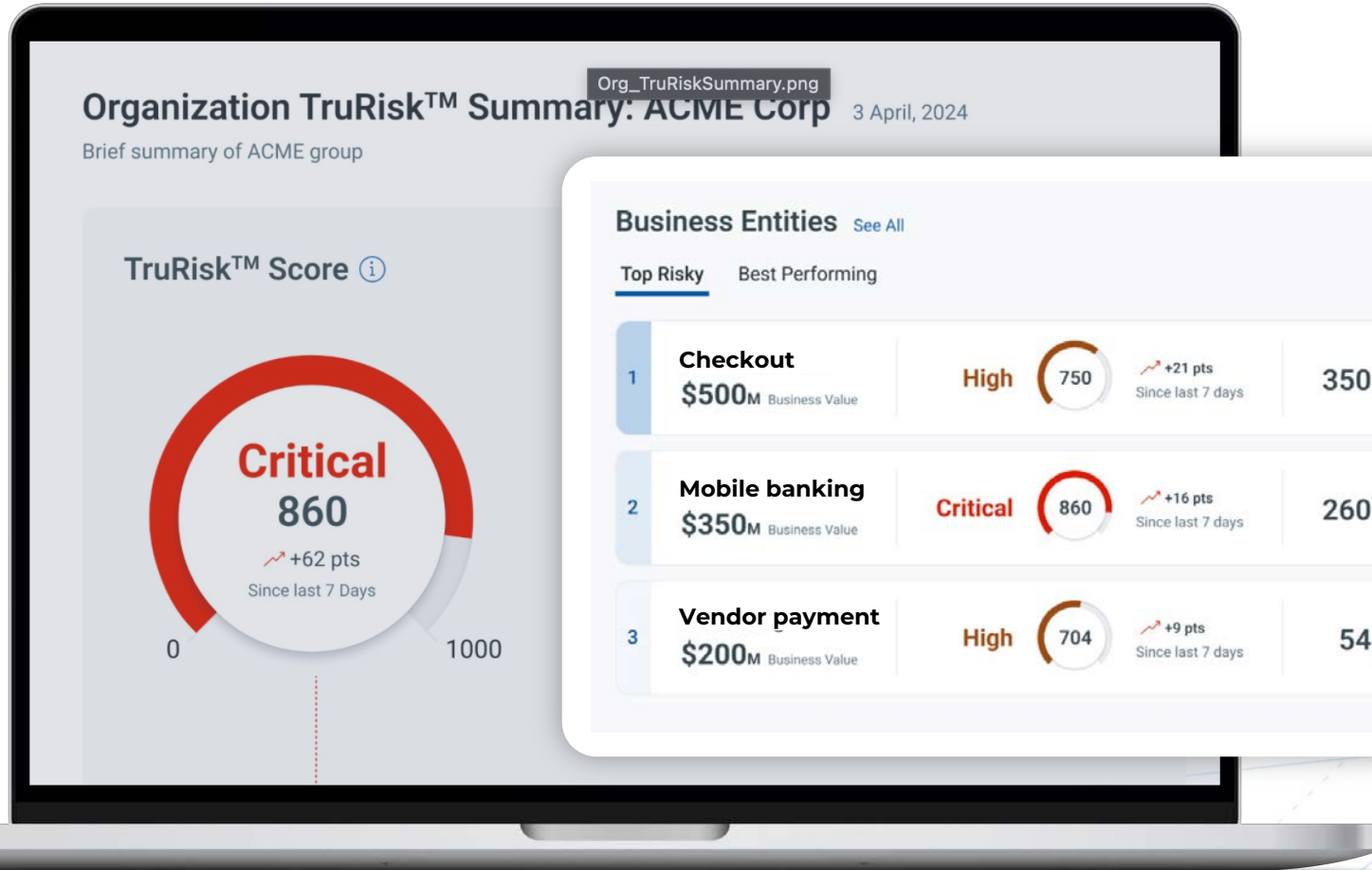


## Risk Reduction and Remediation

- ✓ **Passive Response – Ticketing, Exceptions, Notifications**
- ✓ **Active Risk Elimination – Patching, Mitigation**

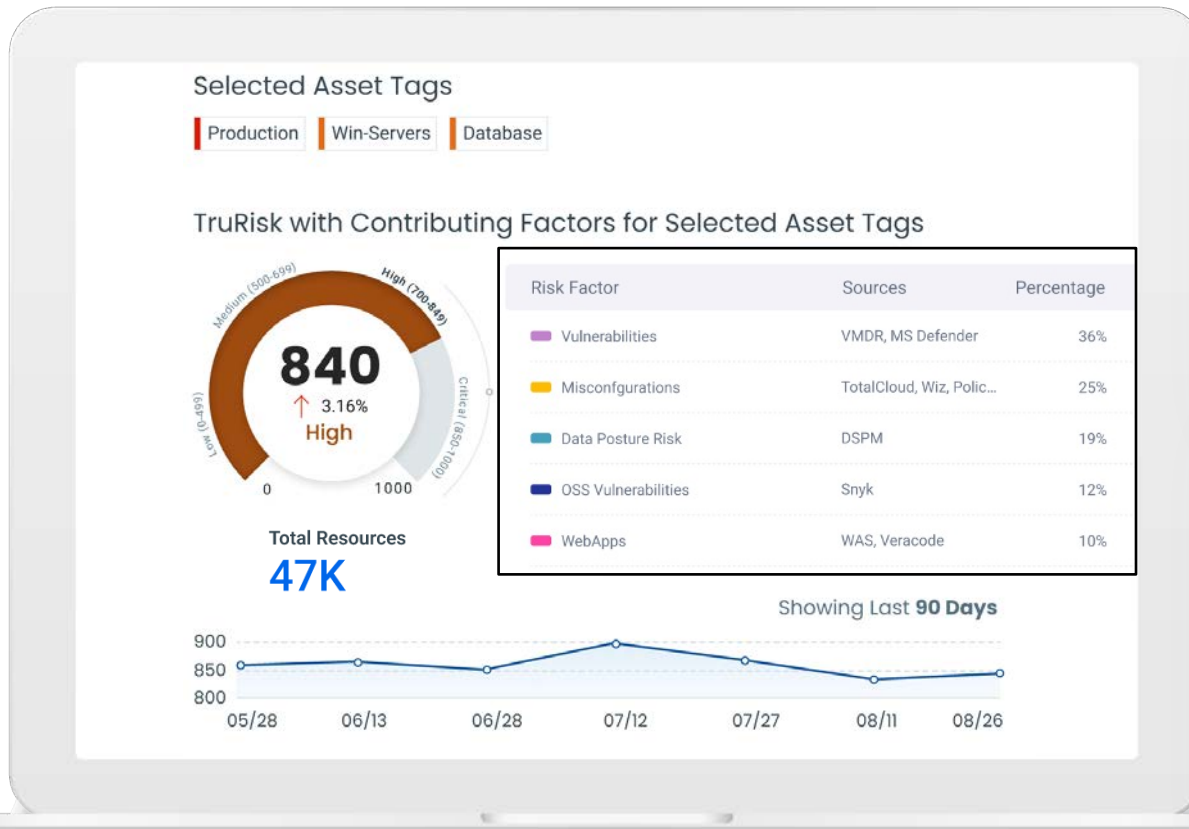


# Measuring **TruRisk** For Business Impact



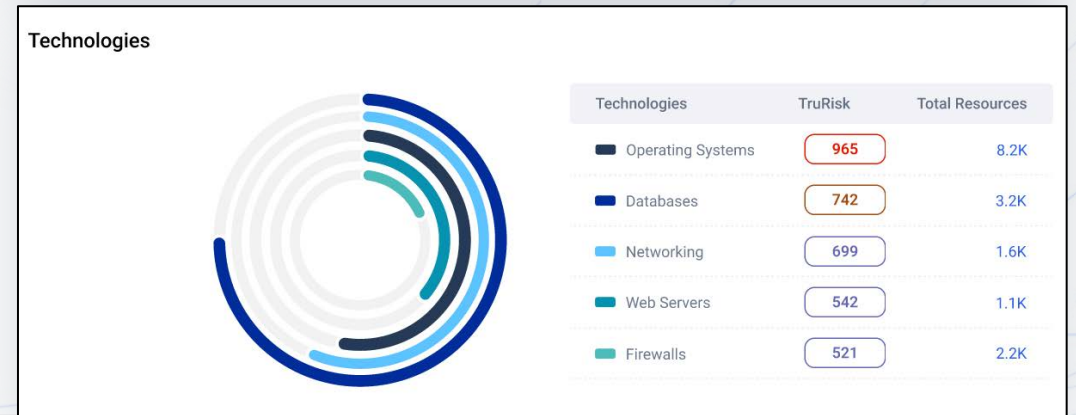
**Know The  
TruRisk of  
Business  
Entities**

# Measuring **TruRisk** Across the Security Findings



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



# Communicate Not Just the Risk Score... but **Risk Insights...**

## Insights



### Key Highlights

The organization's TruRisk score of **860** exceeds that of 75% of industry peers.



### Get More Insights

**40% of business entities (4 out of 10) exceed the defined risk appetite**, with the **Checkout App**, valued at \$500M, being the most critical among them. [View details](#) to analyze the Checkout App's risk profile.

**63% of your assets (69.3K out of 110K) are non-compliant**, contributing to multiple compliance failures including NIST 800-53 Rev 5. Initiate [compliance review](#) to address gaps.

**35% of the assets (38.5K out of 110K) are above the TruRisk threshold** out of which 60% belong to your critical business units. Set up [alerts](#) to stay informed when TruRisk of the assets crosses the threshold.

**47% of your identified risks (705K out of 1.5M) are critical**, out of which 7% (49.4K) have failed to meet SLAs. 83K of your risks were remediated on time. Explore [risk reduction plans](#) for critical findings.

# Get Risk Reduction Plans to Reduce Risk Across the Findings... Not Just Vulnerabilities

The screenshot displays the Qualys Enterprise TruRisk Platform interface. The main heading is "Recommended Plan B for 'Checkout App'". The interface includes a sidebar with navigation options like "Risk Redu...", "ETM", "Home", "Dashboard", "Risk Management", "TruLens", "Inventory", "Compliance", "Reports", and "Configuration".

Key metrics and statistics are shown in a summary bar:

- High: 750
- Business Value: \$500M
- Total Assets: 18.5K
- Total Findings: 230K
- Prioritized: 5.7K of 18.5K (15%)
- Prioritized Findings: 11.2K instances of 172K (6.5%)
- Remediations: 273
- Mitigations: 60
- 750 High / 450 Low

Below the summary bar, there are several charts and filters:

- Ransomware Vulns: 6.2K (+1.22 (10%) Last 30 Days)
- CISA/ NCSA: 7.4K (+10 (1%) Last 30 Days)
- Qualys Patchable: 5.7K
- Mitigations: 4.1K
- Compliance Remediations: 2.2K

A table of findings is displayed below, with columns for TYPE, TITLE, QDS, SOURCES, IMPACTED ASSET, REMEDIATION, and MITIGATION. The table is filtered to show "Critical" findings.

TYPE	TITLE	QDS	SOURCES	IMPACTED ASSET	REMEDATION	MITIGATION
Vulnerability	CVE-2024-1550 - Mozilla Firefox Multiple Vulnerabilities (MFS2024-05)	100	Qualys VMDR	1.3K	Firefox 123.0 Patch	Uninstall App Mitigation
Vulnerability	CVE-2023-21527 - Microsoft Windows Support Diagnostic Tool (MSDT) Remote...	98	VMDR	4.2K	October 10, 2023-KB50313...	Access Forbid Mitigation
Vulnerability	CVE-2021-4104 - Oracle WebLogic Server Multiple Vulnerabilities (Log4Shell)	97	VMDR	2.3K	Patch not available	RegKey Update Mitigation
Misconfiguration	EOL-Internet Explorer (IE) 11 on June 15, 2022	96	CSAM	1K	Patch not available	Uninstall App Mitigation
Misconfiguration	Unauthorized port TCP 8080 is open	95	MS Defender	600	Patch not available	Port Block Mitigation
Vulnerability	CVE-2024-29064 - Microsoft Windows Security Update for April 2024	95	MS Defender	4.8K	Security Cumulative Update... Patch & Config	Mitigation not available
Vulnerability	CVE-2021-36942 - Microsoft Windows Local Security Authority (LSA) Spoofing Vuln...	93	VMDR	400	Security Cumulative Update... Patch & Config	Mitigation not available

# Threat-Centric Risk Management

## BREAKING NEWS

Threat in the wild – WildCat64

## INFORMATION

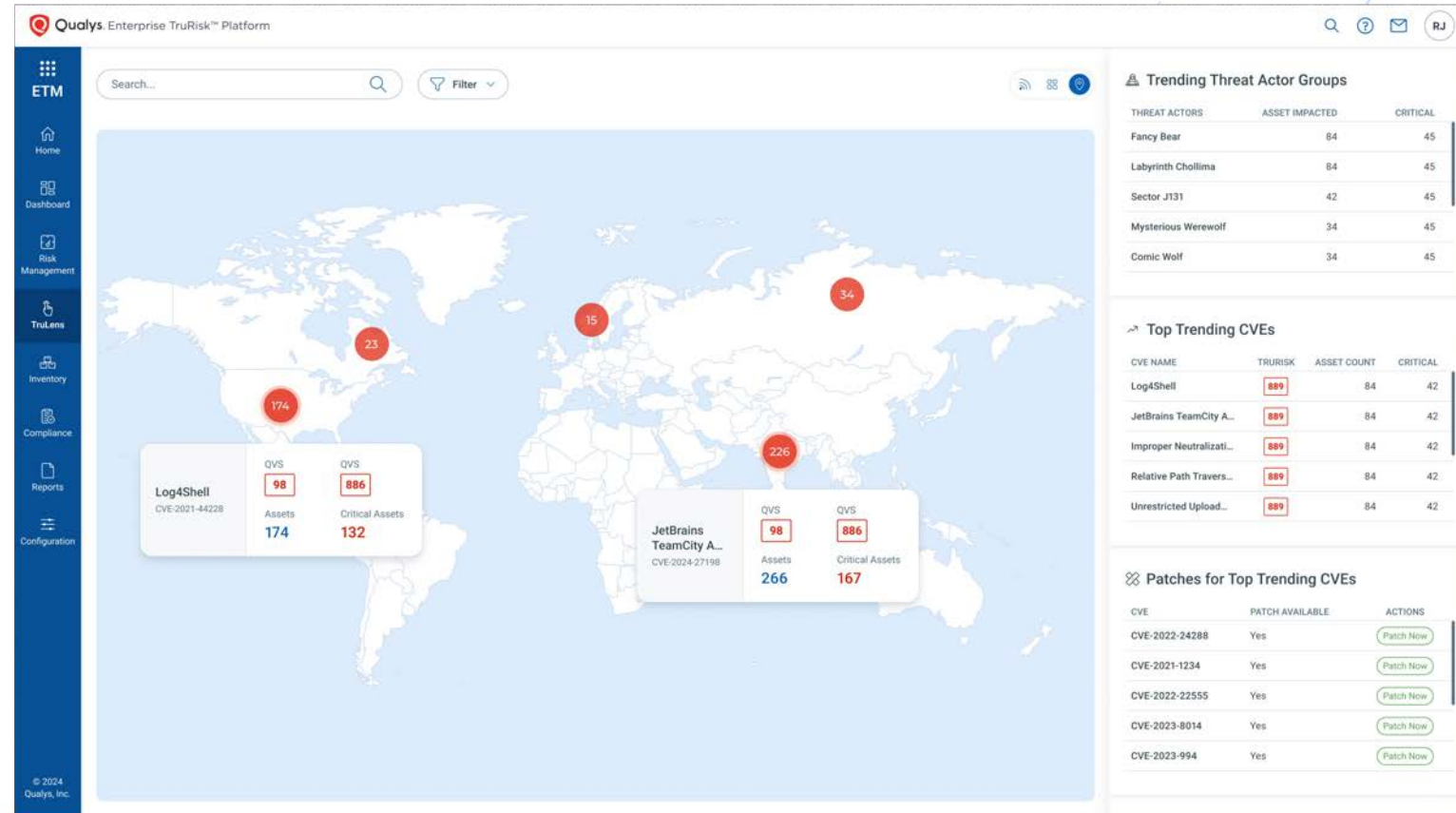
What is it? How bad is it?  
Where is it affecting the most?

## INSIGHTS

Am I affected by this? Which  
Business App? Is it Critical?

## ACTION

How do I fix it? What is the  
Recommendation, Action Plan



# TruRisk AI to Help Detect Blind Spots of Risk



## Business Asset Criticality

Find business critical assets that need to be prioritized for protection but are accidentally marked as low value



## Security Blind Spots

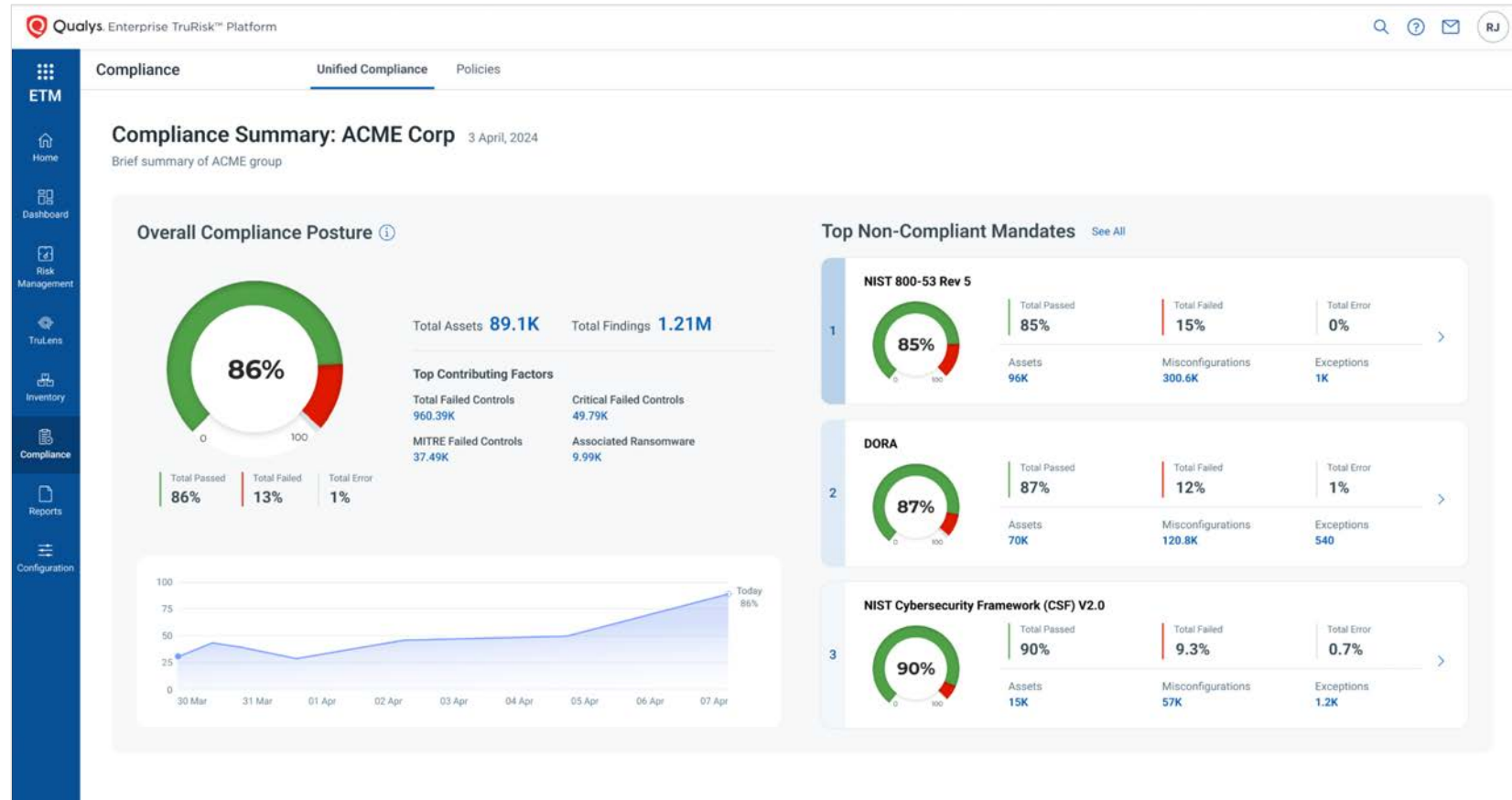
Identify hidden risks that are hiding in plain sight



## Hello Qualys... Speak English to Me

Move away from domain/vendor/product specific language to natural language

# Measure, Communicate Compliance



Communicate Aggregated data sources (Qualys + non-Qualys) for **Comprehensive Compliance**

Get Executive, Management and Operational Compliance views to know Failures causing most violations

# Need to Reduce Risk! With or Without Patching

If Patching Taking Time,  
how can I still Reduce  
Risk?

What are Options beyond  
Patching

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



**30+ Days to  
remediate  
weaponized  
vulnerabilities**



# TruRisk Eliminate

Patching Complimented with Risk Mitigation for Comprehensive Risk Reduction

## TruRisk Eliminate



Risk Reduction Insights



Right technique



Orchestration

### PATCH MANAGEMENT (Remediation)

PATCH MANAGEMENT

CONFIGURATON CHANGES

### TruRisk Mitigate

Risk Mitigation – Qualys/Vendor

Virtual Guard/Patch

Risk Compensation

PLATFORM SERVICES



API



LIGHTWEIGHT AGENT



SENSORS

First-Party OSS

3rd Party Data

APPLICATIONS



OPERATING SYSTEMS



CLOUD / CONTAINERS / VMs



IT / WORKSTATIONS / SERVERS



IOT



EXTERNAL DEVICES



# Comprehensive Risk Reduction

## Use Case #1 (IT Ops) - Patch

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

## Use Case #2 (SecOps) - Mitigate

3. Mitigation script per vuln (vendor or Qualys)
4. Isolate/Quarantine device from network
5. Close ports (ex. port 21 FTP)
6. Stop or Disable services/processes
7. Update cloud setting or call cloud function (ex. remove app from firewall, call Lambda)
8. Custom script (to reduce exposure of software, assets)

## Use Case #3 (SecOps) – Virtual Patching

9. Memory and network protection
10. In Memory updates (Encrypted memory blocks)

## Use Case #4 (SecOps/ITOps)- Compensate Risk

11. Uninstall software (ex. BitTorrent)

# 107 Weaponized Vulns in 2022/23

## Targeting Servers and Workstations



**17 Vulns (16%)**

**Integrated & automated Remediation**

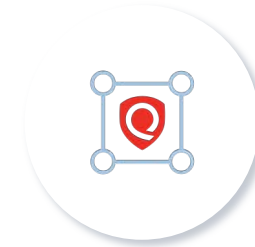
3rd party software  
Chrome/Firefox/Safari/Adobe  
Functionality broken <1%



**14 Vulns (13%)**

**Mitigated with Official Vendor Suggested Mitigations**

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



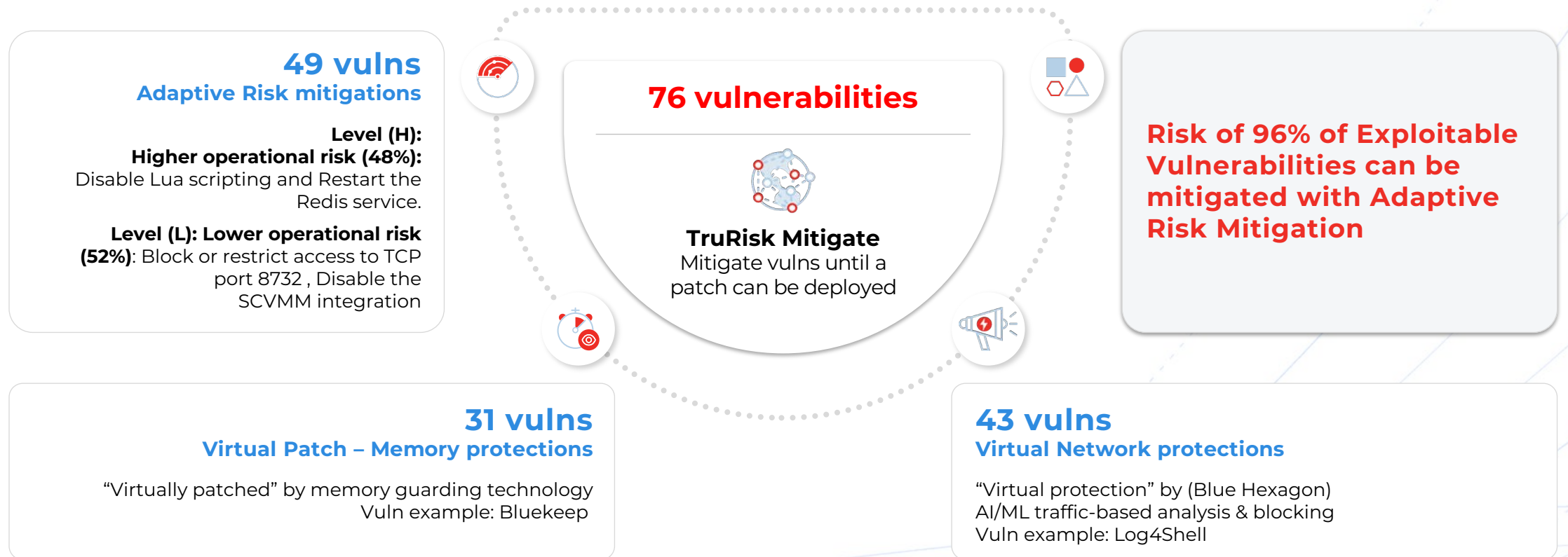
**76 Vulns Left (71%)**

**Not easily patchable or mitigated**

Requires Adaptive Mitigation,  
hybrid approach to mitigation

# Adaptive Risk Reduction w/ **TruRisk Eliminate**

## Adaptive Risk Mitigation to Reduce Risk





Qualys®

---

# Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

**De-risk your business.**