QSC25 EMEA

Putting the 'M' in Vulnerability Management

Kunal Modasiya

Senior Vice President, Product Management, GTM and Growth

The State of Vulnerability Management Today

01

Traditional Approaches Falling Short

- Slow to detect new, exploitable CVEs (**40% increase** in new CVEs in 2024)
- Complexity of **expanding attack surface** causing disjointed views of risk
- Lack threat intel and cyber risk context to prioritize

02

Evolving Threat Landscape

- Time to exploitation is faster than ever (**11.6 days** on average)
- Cybersecurity community is reactive
- Exposures on assets unknown to SecOps teams (**70% of orgs** experience an attack on unknown assets)

03

Response is slow and disjointed

- VM is happening in a silo
- No universal language of risk across cloud, endpoints, OT/IoT, external assets, etc.
- Patch and remediation is disconnected from business risk

Focus on What Matters

The Vulnerability Landscape

2024 CVE Stats:

- Over **40,000** new CVEs disclosed
- Only **245 (0.61%)** have weaponized exploit code

CISA KEV Catalog:

- **1,351** actively exploited CVEs (**0.48%** of **279,795** total CVEs)

Most vulnerabilities aren't actively exploited.

Real-World Threat - Black Basta Ransomware:

- Targets **62 CVEs**, e.g., Log4Shell (CVE-2021-44228), Follina (CVE-2022-30190)

- Exploits a small, high-impact set of vulnerabilities

Attackers prioritize exploitable weaknesses.

Qualys.

Fast Weaponization

Attackers have an 11-day advantage

30.6 Days
Mean Time to Remediate

57.7% Remediated Vulnerabilities

19.5 Days
Time to Weaponize

11.1 Days
Exploitation Opportunity

Not only are attackers an average of **11 days faster** to exploit vulnerabilities than defenders are to patch them, but over **40% of weaponized vulnerabilities go unpatched**.

National Cyber Security Centre

5 Days	14 Days
External	Internal

Following NCSC recommendations would even the odds against attackers.

3 Days Actual Patch Deployment

Where's all that remaining time going?

Qualys.

How do we solve it?

3 simple steps...

01 Unified inventory with cyber risk context

02 Prioritize with real-time threat intelligence

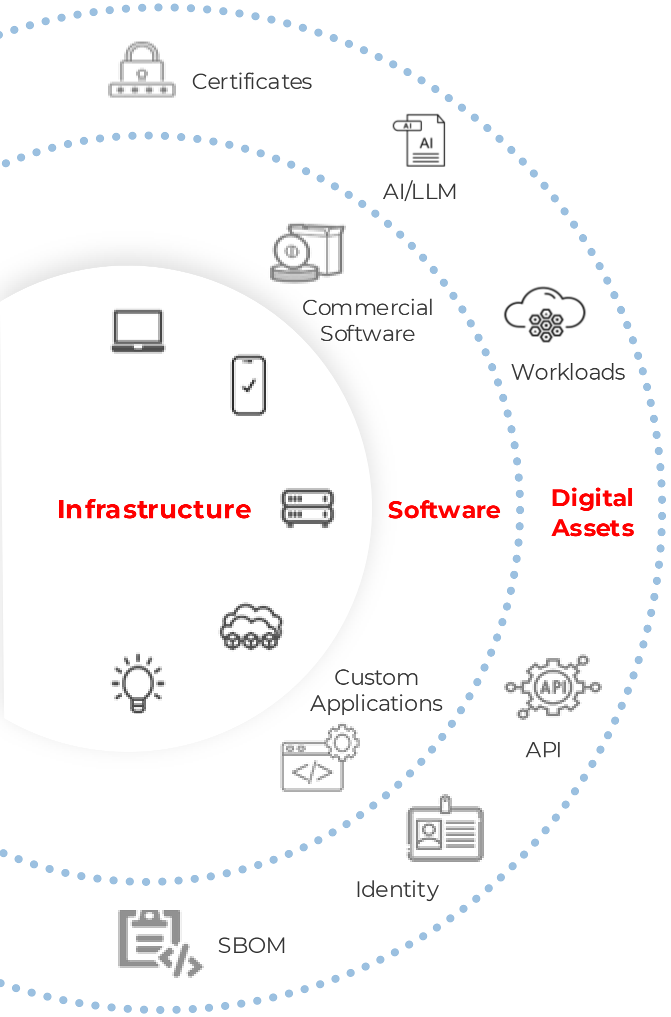
03 Orchestrate remediation based on risk

Unified Attack Surface Discovery

Build a complete inventory with cyber risk context
100% Coverage for RBVM program

Qualys.

Step 0 of Your Unified Risk-Based VM Program



Cloud Connectors

aws ORACLE

Key IT Infra Connectors

Active Directory servicenow vmware bmc Webhook

Active Sensors

Agents Remote Scanners

Passive Sensors

NPS CAPS

Cyber Inventory with business and risk context

Internal and External Attack Surface

Integrated w/Risk Management Program

Qualys. | De-risk Your Business

Patent-Pending EASM

With Real-time Discovery, Attribution & Risk Scoring

01

Discover ‘Previously Unknown’ internet-facing assets

- Domains & Subdomains, parked domains
- Websites, Certificates & APIs
- IP Addresses & Cloud Services

02

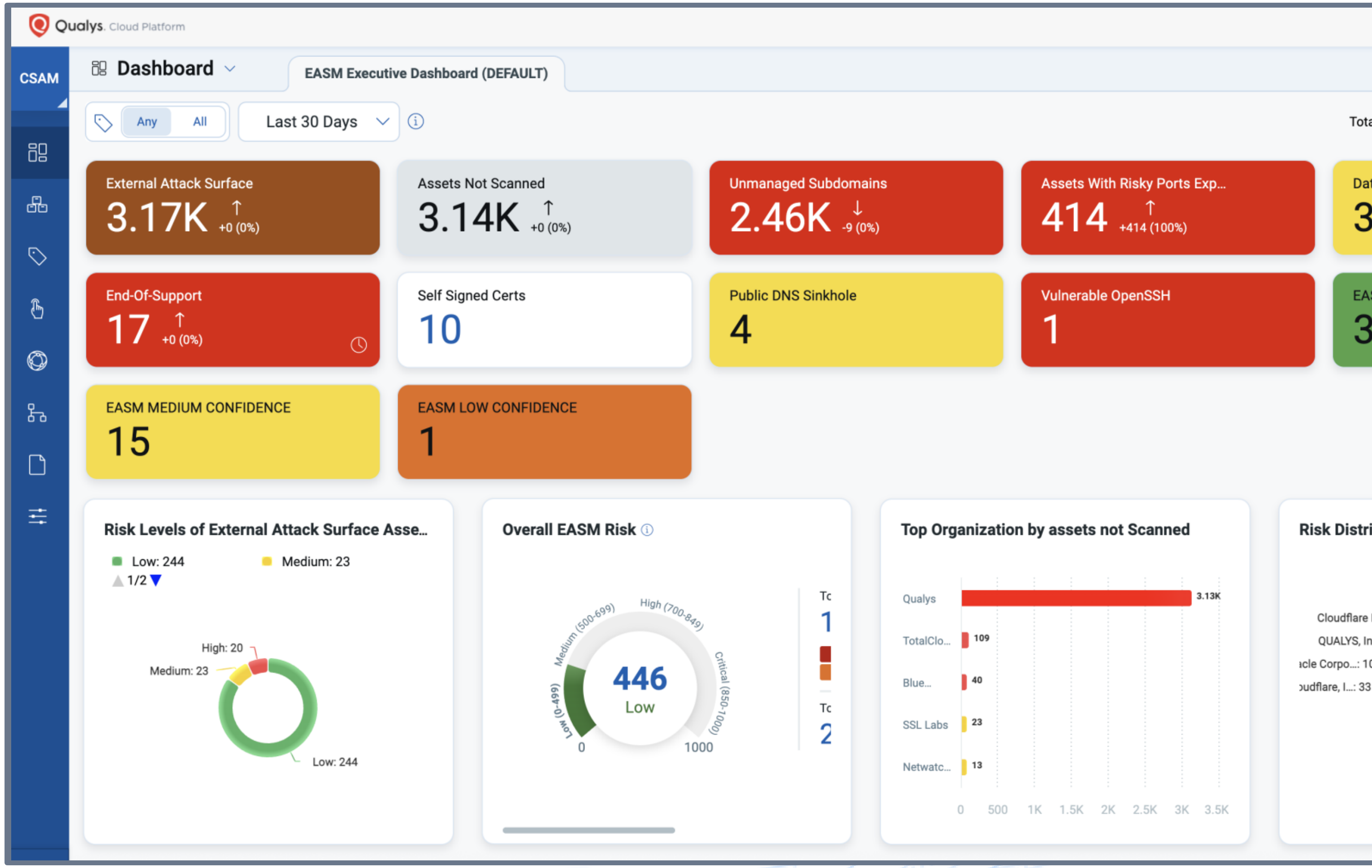
Monitor Global Subsidiaries and M&A

- Third-Party Risk Visibility
- Attack Surface Mapping w/ Attribution Score
- Business Entity, DNS, WHOIS, ISP, Certificates
- Look-alike & typo squatting

03

Detect & Prioritize Risk

- Exploitable Vulnerabilities
- Risky Unsanctioned Ports (SSH, RDP, ..)
- Exposed Databases and Admin Consoles
- Weak Certificates
- EoL/EoS software and more



External Attack Surface 3.17K ↑ +0 (0%)

Assets Not Scanned 3.14K ↑ +0 (0%)

Unmanaged Subdomains 2.46K ↓ -9 (0%)

Assets With Risky Ports Exp... 414 ↑ +414 (100%)

End-Of-Support 17 ↑ +0 (0%)

Self Signed Certs 10

Public DNS Sinkhole 4

Vulnerable OpenSSH 1

EASM MEDIUM CONFIDENCE 15

EASM LOW CONFIDENCE 1

Qualys. | De-risk Your Business

Comprehensive TruRisk Insights

With Risk Factors Beyond Vulnerabilities

01 **Tech Debt (EoL/EoS)**

End-of-life and end-of-support tech contains unpatchable vulnerabilities.

02 **Risky or Unauthorized Ports**

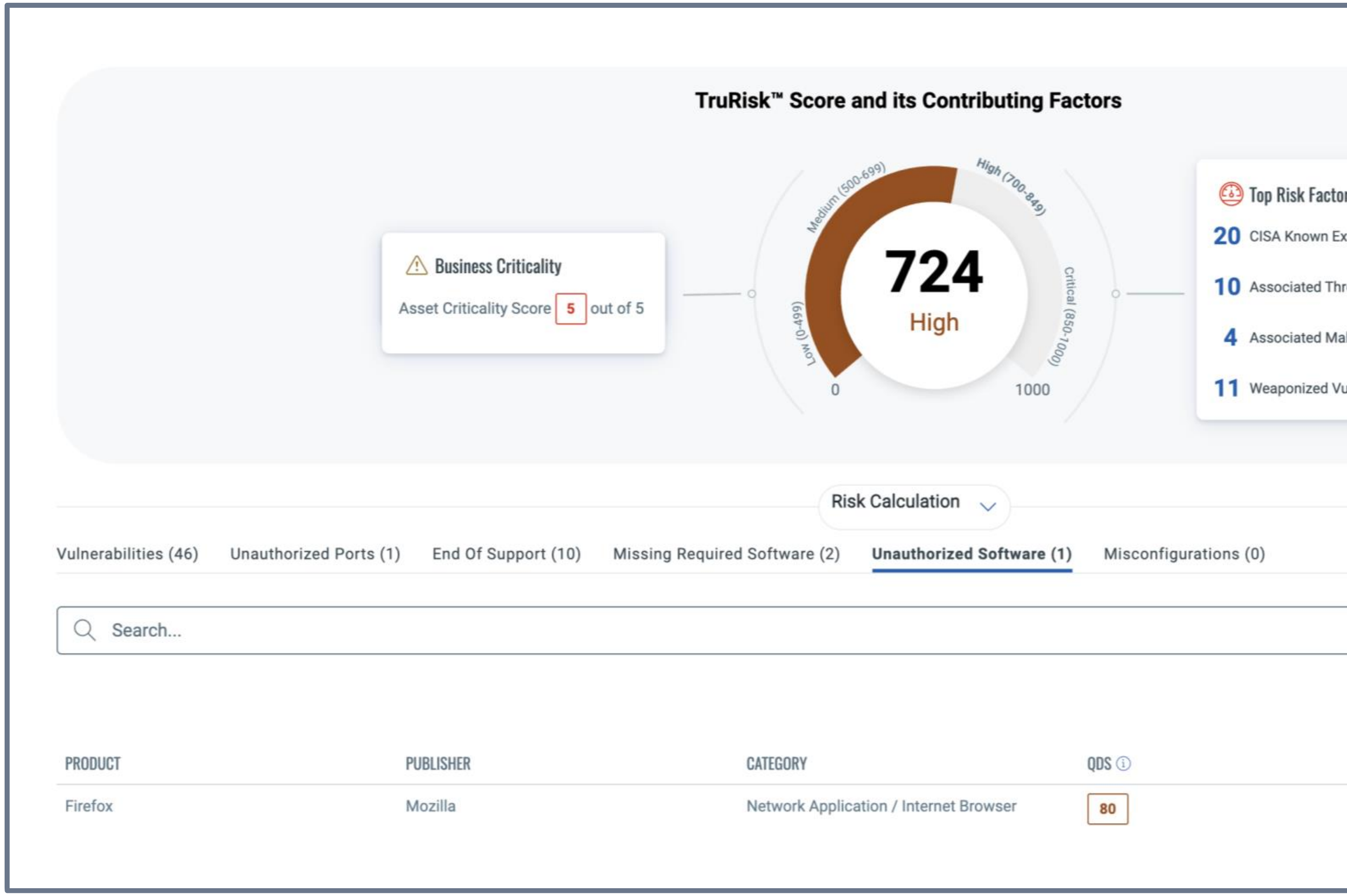
Misconfigured internet-facing ports can expose backdoors to the environment.

03 **Missing Security Controls**

Identify missing EDR agents or other required IT/Security software to mitigate risk proactively

04 **Unauthorized Software**

unauthorized software and associated vulnerabilities as a vector within TruRisk Scoring



TruRisk™ Score and its Contributing Factors

Business Criticality

Asset Criticality Score 5 out of 5

Top Risk Factor

20 CISA Known Ex

10 Associated Thr

4 Associated Ma

11 Weaponized Vu

Risk Calculation

Vulnerabilities (46) | Unauthorized Ports (1) | End Of Support (10) | Missing Required Software (2) | **Unauthorized Software (1)** | Misconfigurations (0)

Search...

PRODUCT	PUBLISHER	CATEGORY	QDS ⓘ
Firefox	Mozilla	Network Application / Internet Browser	80

Enrich Asset with Business Context

To drive accurate Risk Scoring & Assessment

Asset Ownership

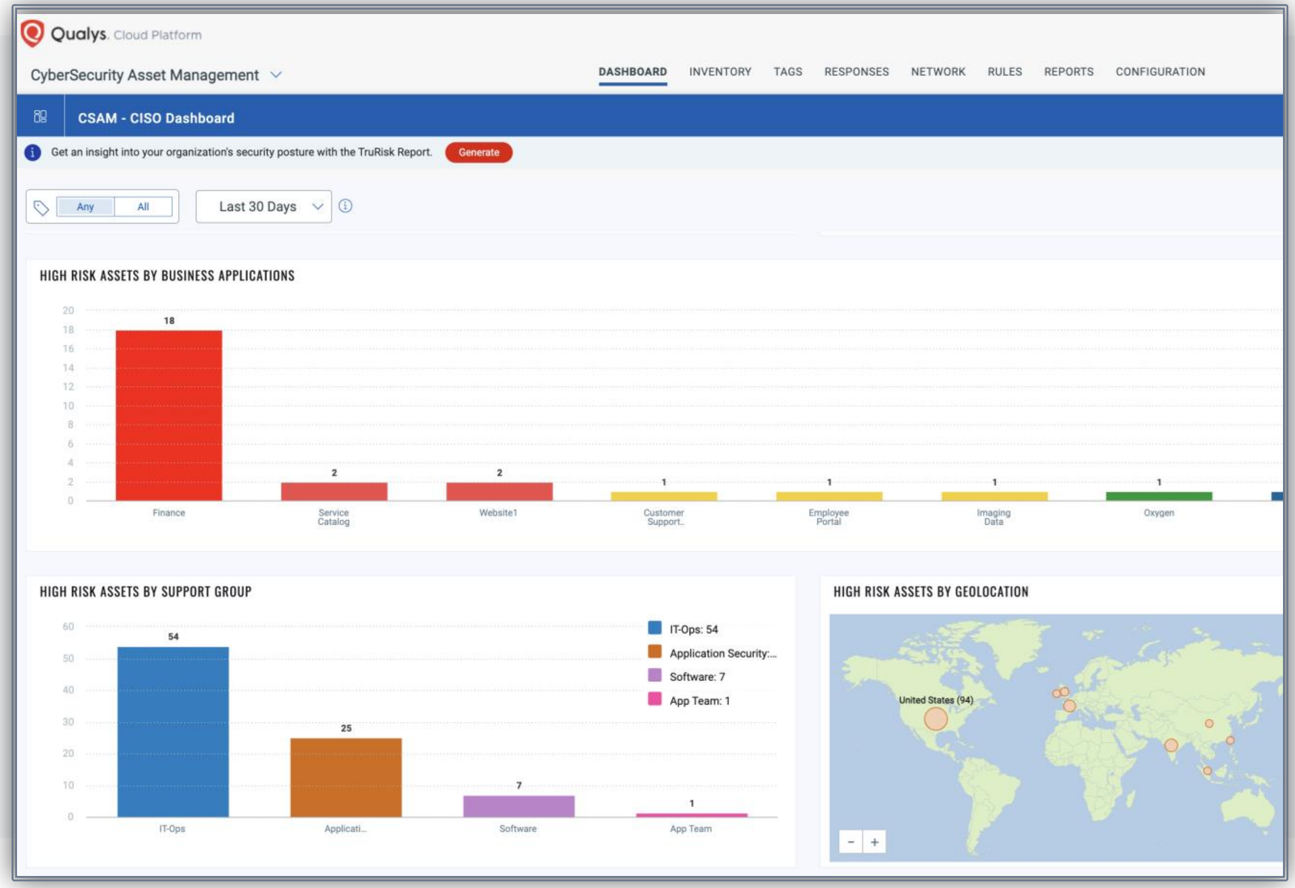
Business App/Service

Identity

Environment & Status

Business Criticality

Custom Attributes & more



Get an insight into your organization's security posture with the TruRisk Report.

Risk Prioritization

with business context
& real-time threat intelligence

Qualys®

Prioritize Risk with TruRisk™ 2.0

Vulnerabilities (CVSS / EPSS)

Malware

Exploit Type Real Threat Indicator

Certificates

Unauthorized Software

CISA KEV

Exploited by malware threat actors

Asset Critically

Unauthorized Ports

EoL & EoS SW, OS, HW

Trending – Chatter, Dark Web

Exploit Code maturity

Location of the Asset

Required SW Missing

Custom Rule-based Risk factor

IMMUNITY

REVERSING LABS

GREYNOISE INTELLIGENCE

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

McAfee

VDE

MITRE ATT&CK

GitHub

MISP Threat Sharing

PZ PROJECT ZERO

CANADIAN CENTRE FOR CYBER SECURITY

Square Security

metasploit

Kaspersky Industrial CyberSecurity

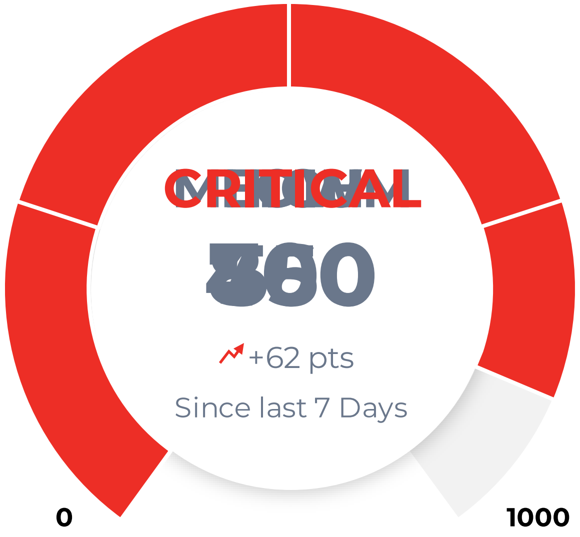
Google

EPSS

TALOS

packet storm

FIREEYE



TruRisk™ Score

Total Assets

110K

Total Findings

1.5M

Top Risk Factors

CISA/NCSC Vulnerabilities 143.2K	Internet Exposed Assets 20.4K
Misconfigurations 92.4K	Incidents 19

DE-RISK YOUR **BUSINESS**

Qualys.

MITRE ATT&CK Matrix Prioritization

Get an Attacker-centric View

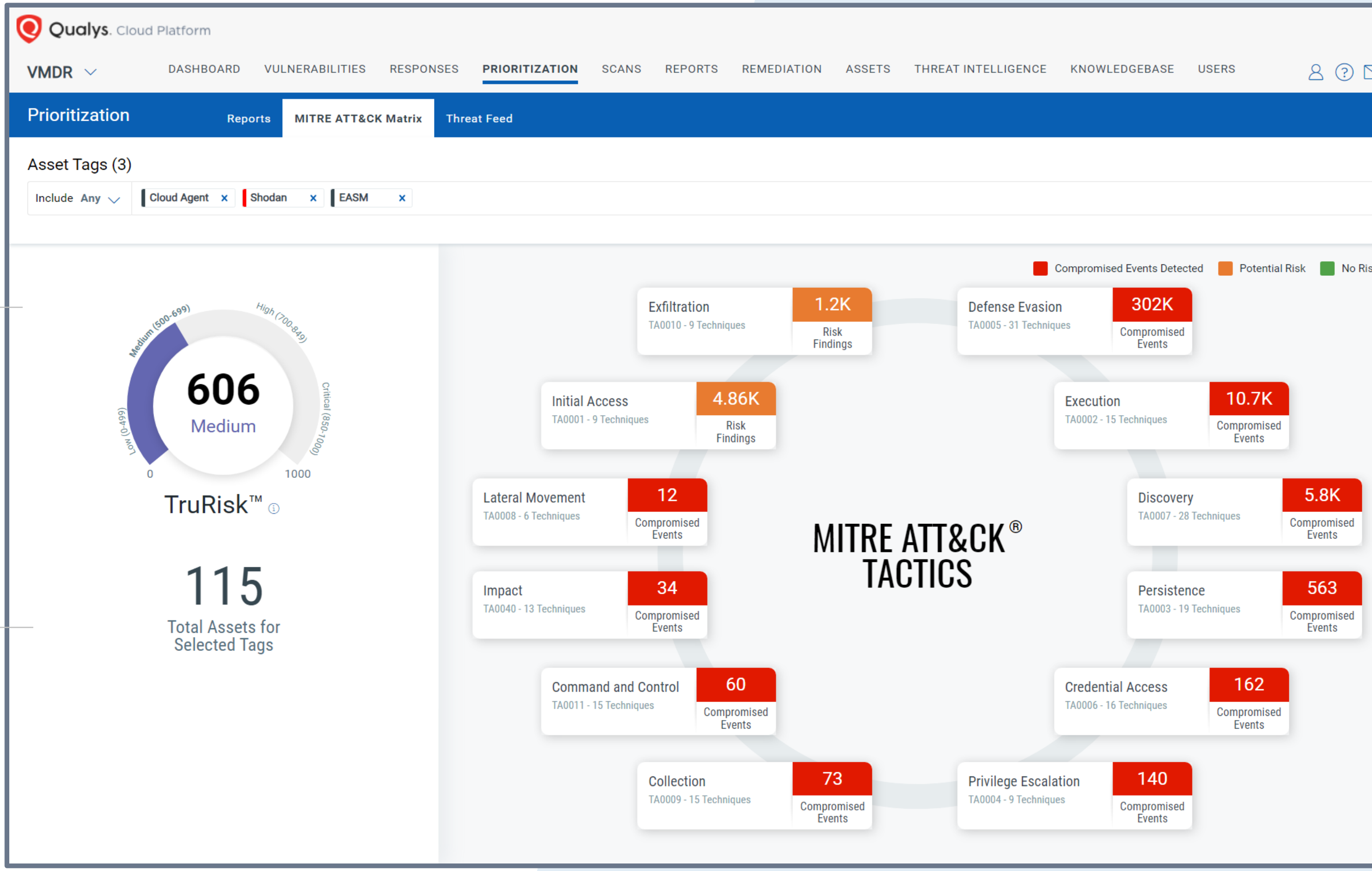
View your top ATT&CK Tactics and Techniques from an **attacker's perspective** and adopt **Threat-Informed Defense** to reduce risk

Holistic ATT&CK View

A consolidated ATT&CK view of **vulnerabilities** from VMDR, **mis-configurations** from PC, **incidents** from EDR, and **asset details** from CSAM (e.g., external-facing asset identification and RDP port details)

Eliminate Attack Paths

Leverage MITRE ATT&CK insights to identify, prioritize, **eliminate attack paths** and **break kill chains** proactively using integrated Patch Management



Asset Tags (3)

Include Any | Cloud Agent × | Shodan × | EASM ×

🟥 Compromised Events Detected 🟧 Potential Risk 🟩 No Ris

606 Medium

TruRisk™

115 Total Assets for Selected Tags

Tactic	Techniques	Count	Type
Exfiltration	TA0010 - 9 Techniques	1.2K	Risk Findings
Defense Evasion	TA0005 - 31 Techniques	302K	Compromised Events
Initial Access	TA0001 - 9 Techniques	4.86K	Risk Findings
Execution	TA0002 - 15 Techniques	10.7K	Compromised Events
Lateral Movement	TA0008 - 6 Techniques	12	Compromised Events
Discovery	TA0007 - 28 Techniques	5.8K	Compromised Events
Impact	TA0040 - 13 Techniques	34	Compromised Events
Persistence	TA0003 - 19 Techniques	563	Compromised Events
Command and Control	TA0011 - 15 Techniques	60	Compromised Events
Credential Access	TA0006 - 16 Techniques	162	Compromised Events
Collection	TA0009 - 15 Techniques	73	Compromised Events
Privilege Escalation	TA0004 - 9 Techniques	140	Compromised Events

AI/ML-Powered Vulnerability Prioritization

Leverage AI/ML to detect & prioritize critical risk with maximum efficiency

01 **TruRisk: AI-Powered Risk Scoring**

Reduces critical vulns by 85%

02 **AI-Powered Threat Detection**

Identify threats in real-time with deep learning AI-based detection

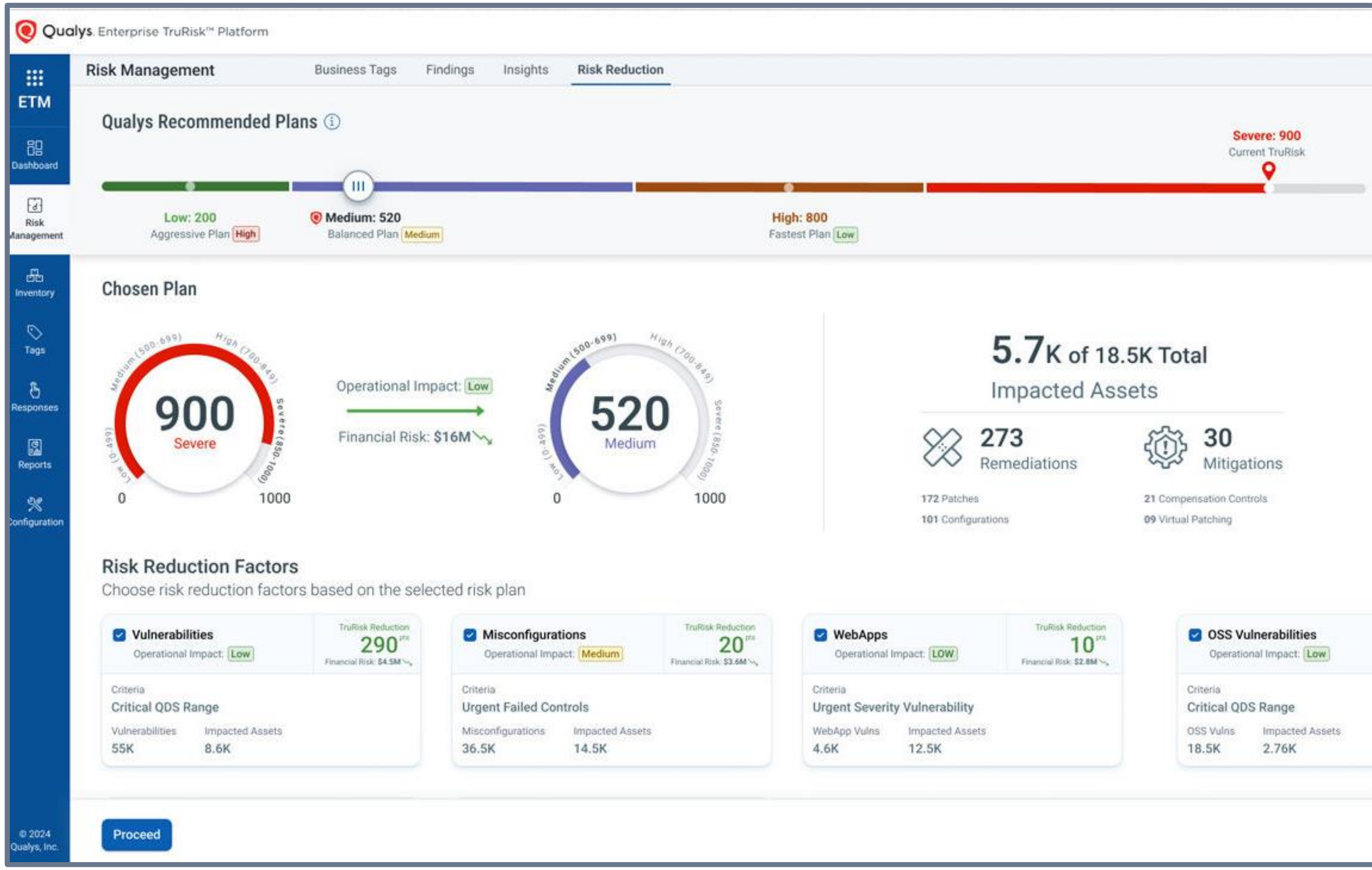
03 **Asset Criticality Detection**

Automatically prioritize business-critical assets

04 **AI-Powered Incident Investigation Workflow**

MISTRAL AI_

Actionable summary based on real-time aggregation of risk factors



Qualys Recommended Plans

Severe: 900
Current TruRisk

Low: 200
Aggressive Plan High

Medium: 520
Balanced Plan Medium

High: 800
Fastest Plan Low

Chosen Plan

900 Severe (Low (0-499), Medium (500-699), High (700-849), Severe (850-1000); 0–1000)

Operational Impact: Low

Financial Risk: $16M

520 Medium (Low (0-499), Medium (500-699), High (700-849), Severe (850-1000); 0–1000)

5.7K of 18.5K Total Impacted Assets

273 Remediations: 172 Patches, 101 Configurations

30 Mitigations: 21 Compensation Controls, 09 Virtual Patching

Risk Reduction Factors

Choose risk reduction factors based on the selected risk plan

Factor	Operational Impact	TruRisk Reduction	Financial Risk	Criteria	Count	Impacted Assets
☑ Vulnerabilities	Low	290 pts	$4.5M	Critical QDS Range	Vulnerabilities 55K	8.6K
☑ Misconfigurations	Medium	20 pts	$3.6M	Urgent Failed Controls	Misconfigurations 36.5K	14.5K
☑ WebApps	LOW	10 pts	$2.8M	Urgent Severity Vulnerability	WebApp Vulns 4.6K	12.5K
☑ OSS Vulnerabilities	Low			Critical QDS Range	OSS Vulns 18.5K	2.76K

Orchestrate Remediation

with native capabilities and robust connected workflows

Qualys.

Don’t Just Measure Risk—Eliminate It!

TruRisk™ Eliminate

Address All Types Of Vulnerabilities with or without a Patch

TruRisk Patch

- Test and deploy patches to fix vulns
- Fully automate patch deployment based on risk
- Windows, Mac, Linux OS and 3rd party app support
- **110M patches deployed natively by Qualys customers in 2024**

TruRisk Mitigate

- Remediate vulns that don’t have a patch
- Mitigate vulns that cannot be patched due to operational risk
- Address Zero Day vulns before the patch is available

TruRisk Isolate

- Isolate device to ensure vulns cannot be exploited
- Allow exceptions to ensure device can be patched and managed

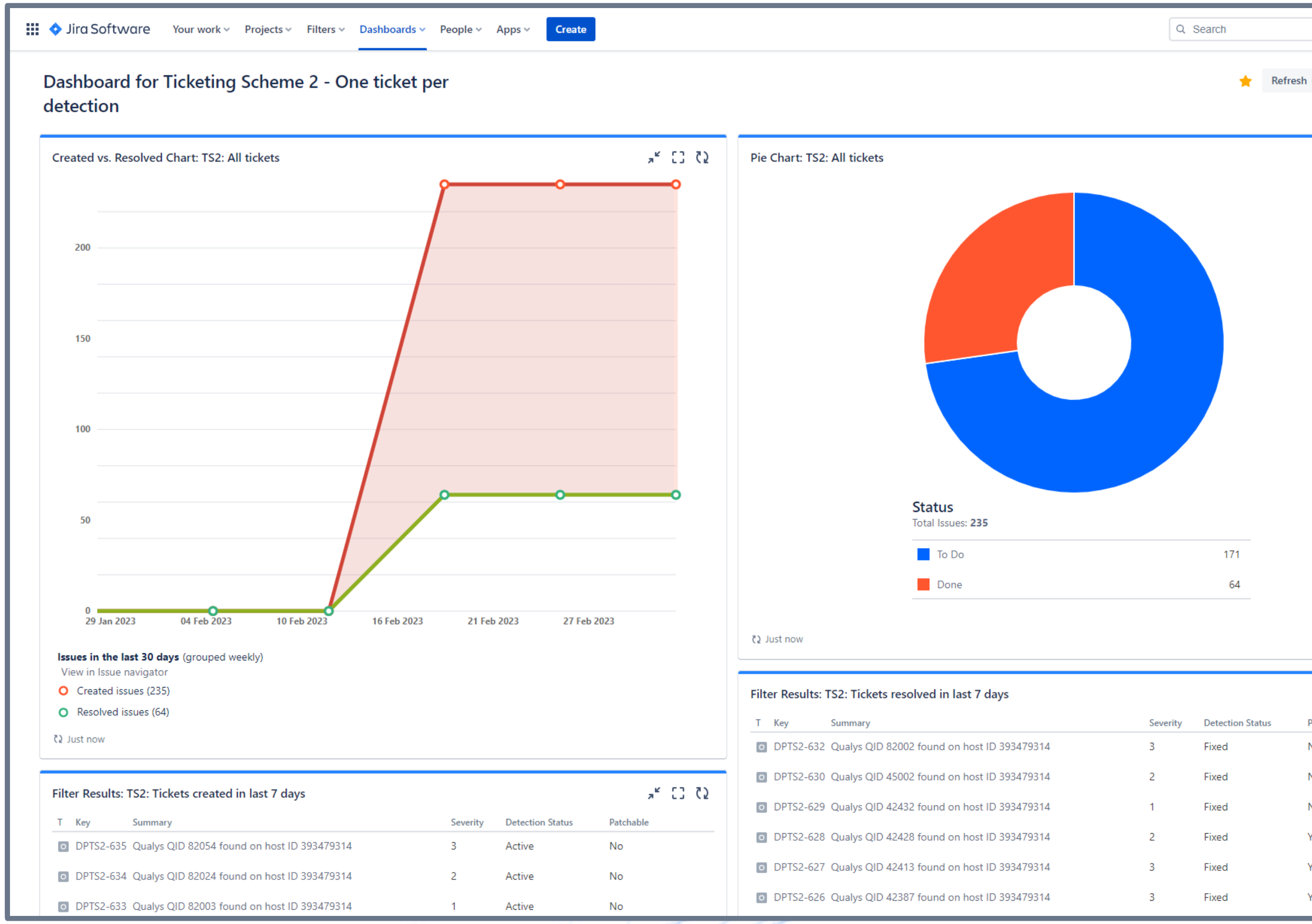
One Click Workflow

Scan, Prioritize, and Remediate Risk to Discovered Assets

01 Activate New Assets for VM/PC and more

02 Assess the Risk of Web Applications

03 Alert & orchestrate ticking with Systems like Jira, Splunk, and ServiceNow



Dashboard for Ticketing Scheme 2 - One ticket per detection

Created vs. Resolved Chart: TS2: All tickets

Issues in the last 30 days (grouped weekly)

View in Issue navigator

○ Created issues (235)

○ Resolved issues (64)

Just now

Pie Chart: TS2: All tickets

Status

Total Issues: **235**

🟦 To Do	171
🟥 Done	64

Just now

Filter Results: TS2: Tickets created in last 7 days

T	Key	Summary	Severity	Detection Status	Patchable
▣	DPTS2-635	Qualys QID 82054 found on host ID 393479314	3	Active	No
▣	DPTS2-634	Qualys QID 82024 found on host ID 393479314	2	Active	No
▣	DPTS2-633	Qualys QID 82003 found on host ID 393479314	1	Active	No

Filter Results: TS2: Tickets resolved in last 7 days

T	Key	Summary	Severity	Detection Status	P
▣	DPTS2-632	Qualys QID 82002 found on host ID 393479314	3	Fixed	N
▣	DPTS2-630	Qualys QID 45002 found on host ID 393479314	2	Fixed	N
▣	DPTS2-629	Qualys QID 42432 found on host ID 393479314	1	Fixed	N
▣	DPTS2-628	Qualys QID 42428 found on host ID 393479314	2	Fixed	Y
▣	DPTS2-627	Qualys QID 42413 found on host ID 393479314	3	Fixed	Y
▣	DPTS2-626	Qualys QID 42387 found on host ID 393479314	3	Fixed	Y

Qualys. | De-risk Your Business

Qualys Workflow Automation & Orchestration (QFlow)

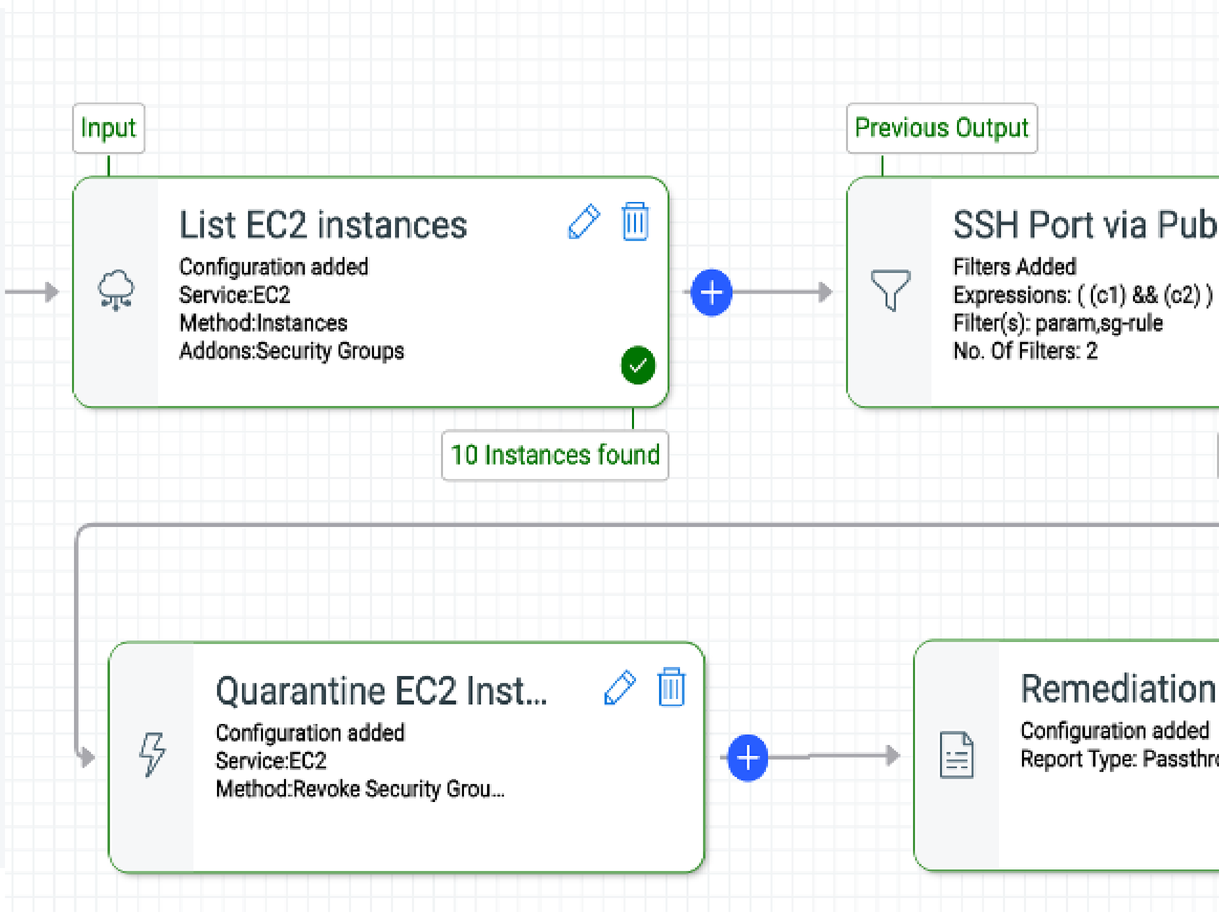
No Code / Low Code – 300+ out-of-box Playbook

Simplify workflow creation with drag and drop visual nodes and no code

Customize security control workflows and scale inventory discovery

Enrich the security teams by automating efforts to manage security programs efficiently

Orchestrate remediation workflows and integrate with DevOps and ITSM tools



Input

List EC2 instances
Configuration added
Service:EC2
Method:Instances
Addons:Security Groups

10 Instances found

Previous Output

SSH Port via Pub
Filters Added
Expressions: ((c1) && (c2))
Filter(s): param,sg-rule
No. Of Filters: 2

Quarantine EC2 Inst...
Configuration added
Service:EC2
Method:Revoke Security Grou...

Remediation
Configuration added
Report Type: Passthr

Driving Business Outcomes

Qualys.

Prioritize and Reduce Attack Surface Exposure

Drive business outcomes and ROI

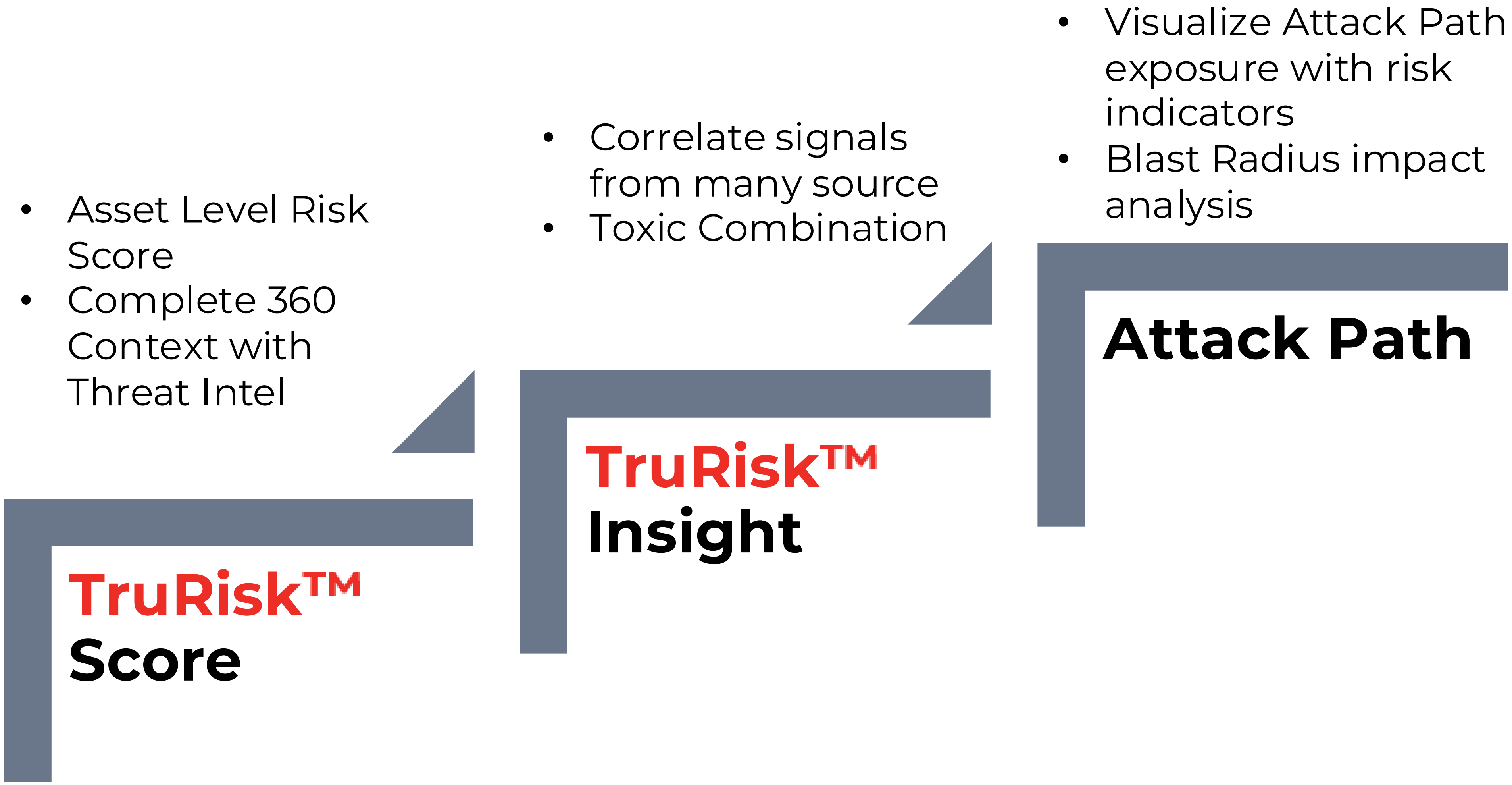
Mean-Time-to-Discovery	30 Days	→	**2 Days**
Asset Coverage	~50-70%	→	**~100%**
Tech Debt Mitigation	Reactive	→	**Planned up to 12 months**
Mean-Time-to-Remediation	30+ Days	→	**<5 Days (To meet NCSC's Requirements)**

Demo Time
Seeing is believing

Qualys®

Qualys®

Risk Prioritization with Qualys Enterprise TruRisk™ Platform



TruRisk™ Score

- Asset Level Risk Score
- Complete 360 Context with Threat Intel

TruRisk™ Insight

- Correlate signals from many source
- Toxic Combination

Attack Path

- Visualize Attack Path exposure with risk indicators
- Blast Radius impact analysis