



VMDR – The Journey to Risk Management and Beyond



Sandeep Potdar

Senior Director of Product Management, VMDR

Qualys



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

An abstract graphic in the bottom right corner consists of several thin white lines and dots. Some lines are solid, while others are dashed. The dots are colored in blue and red, scattered across the lower right portion of the blue background.

You can't **secure** what you can't **manage**.
You can't **manage** what you can't **measure**.
You can't **measure** what you can't **see**.

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

External

14 Days

Internal

Following NCSC recommendations would even the odds against attackers.

3 Days

Actual Patch Deployment

Where's all that remaining time going?

Measure Risk with **TruRisk™**

Continuously Measure Cyber Risk

01

Measure Accurately

Accurately measure, quantify, and track risk reduction over time, across vulnerabilities, assets, and business units

02

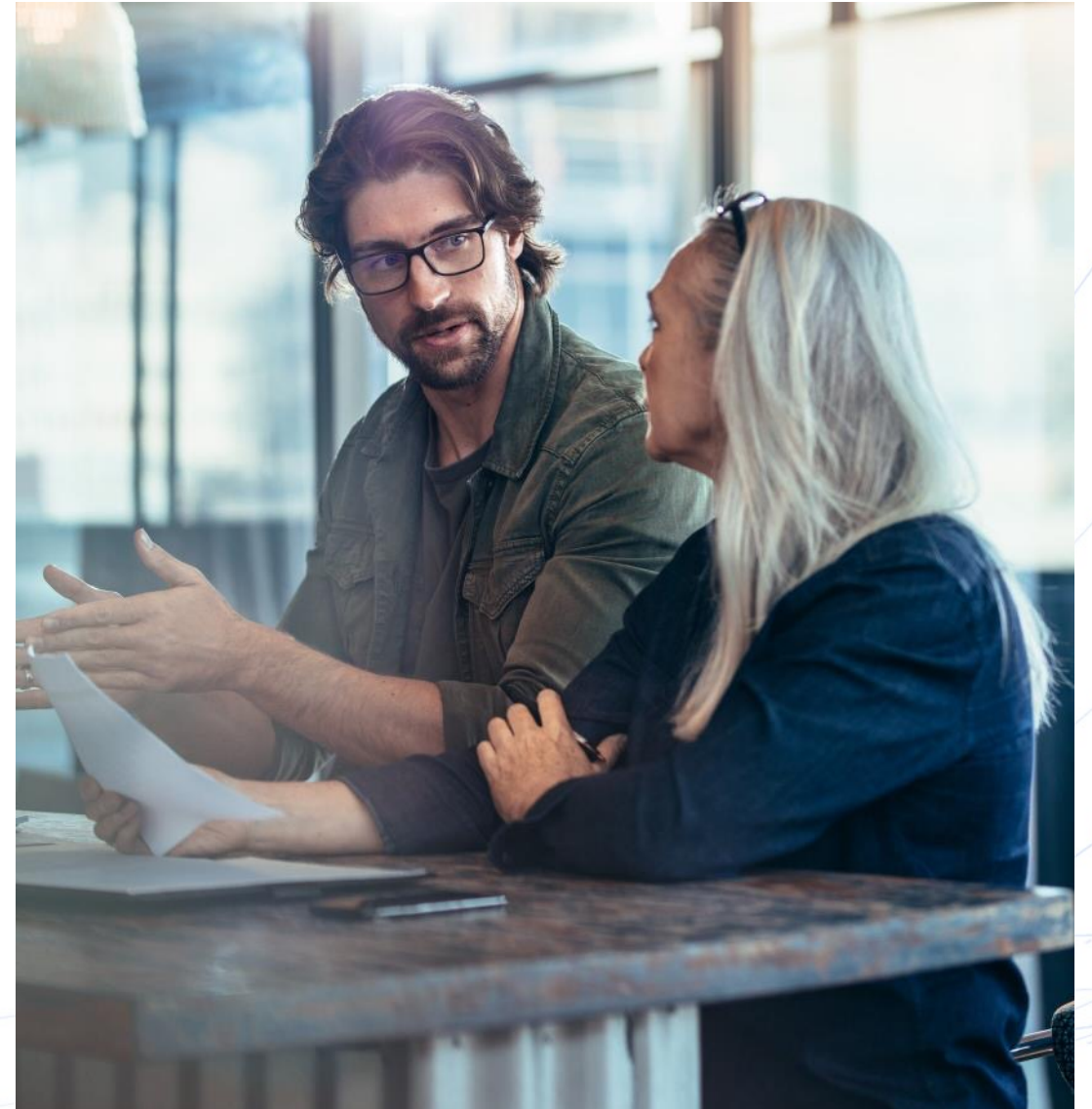
Communicate Precisely

Communicate risk across different teams, business units and geographic locations by leveraging dashboards, reports and ITSM tools

03

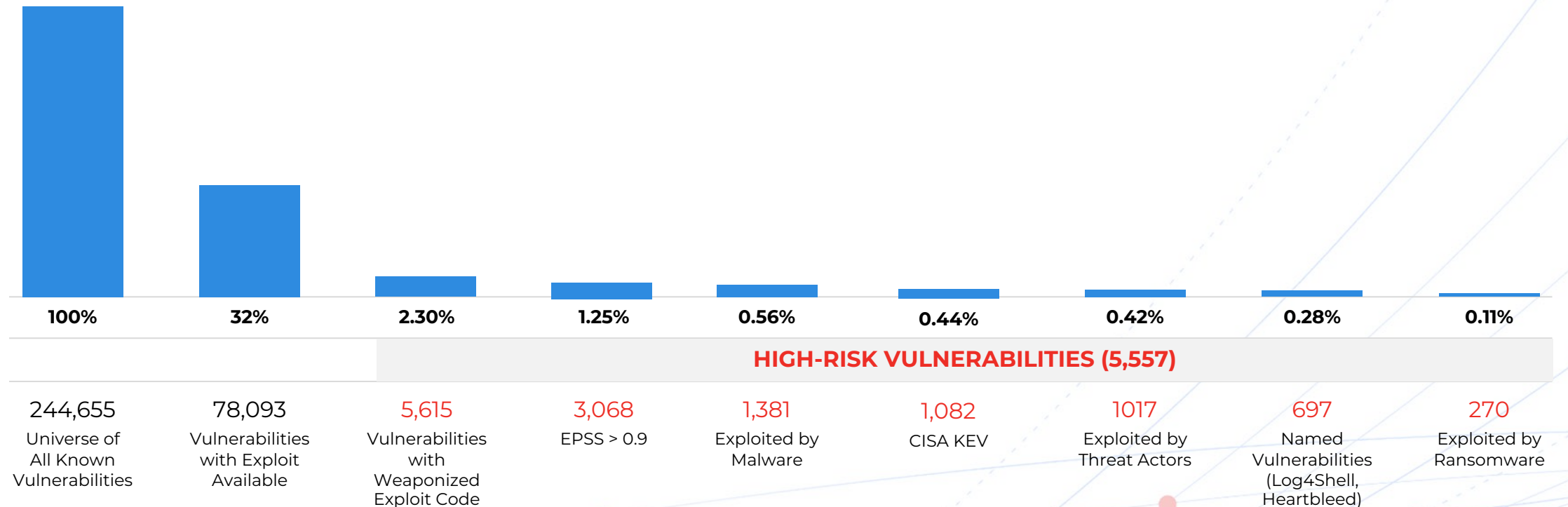
Eliminate Effectively

Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk



Many Ways To Measure Risk

How Do You Accurately Measure Risk?



Updated: Apr 9, 2024

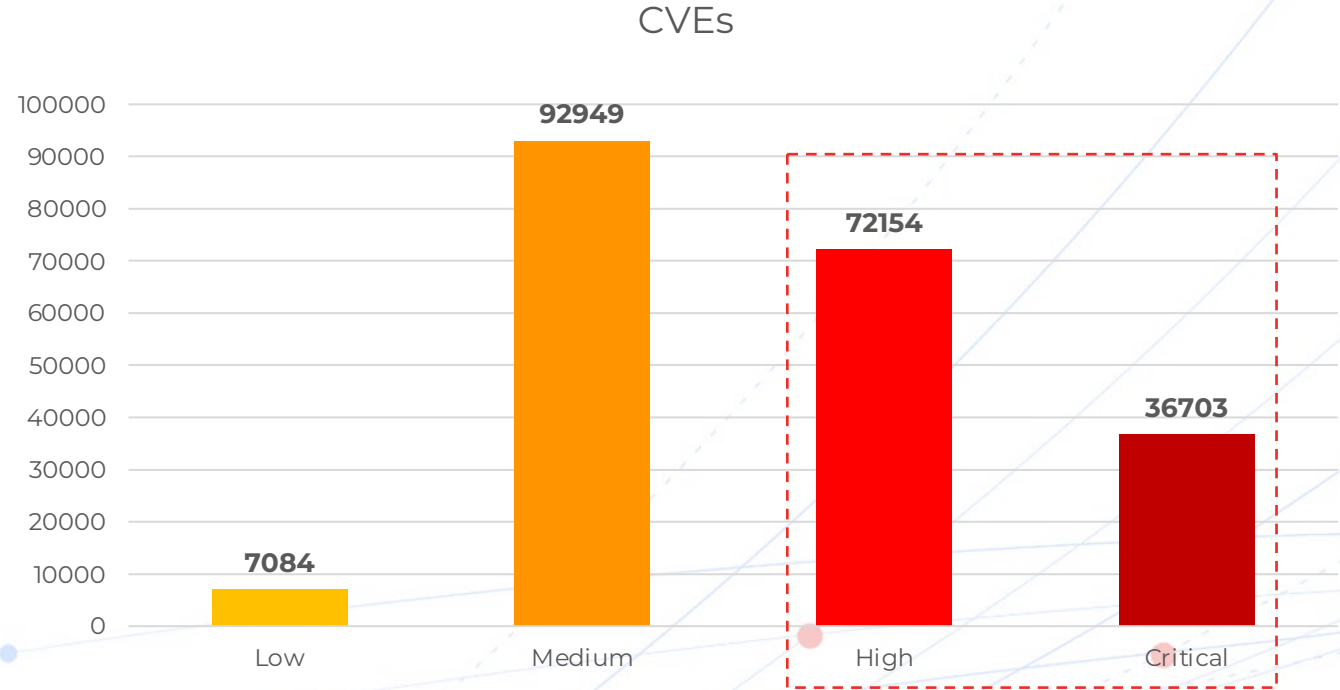
Measuring by CVSS

Focus on What Matters Most

52%

Too **many** vulnerabilities (105k+) are rated **high or critical** by CVSS

Common Vulnerability Scoring System (CVSS)



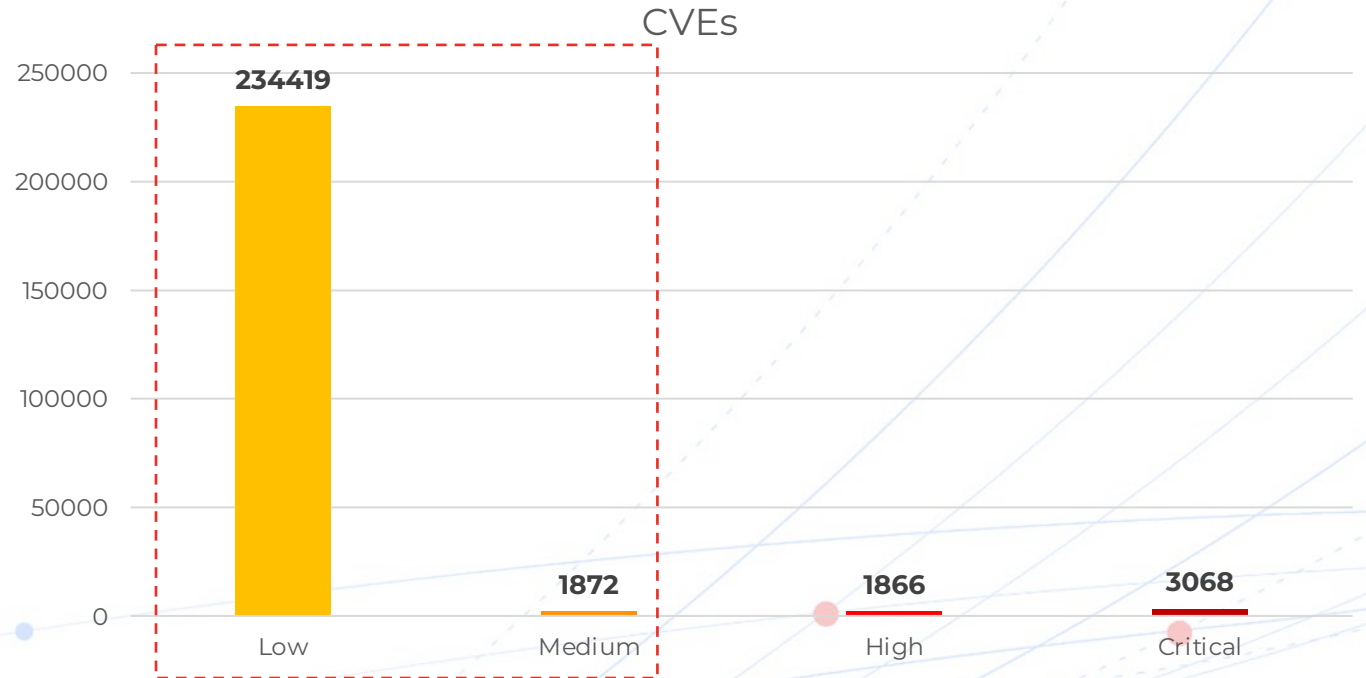
Measuring by EPSS

Focus on Reducing Risk, **Not Volume**

98%

Too **many** vulnerabilities (234K) are rated **low or medium** by EPSS

Exploit Prediction Scoring System (EPSS)





Sign in

Exploit Prediction Scoring System (EPSS)

- The EPSS Model
- Data and Statistics
- User Guide
- EPSS Research and Presentations
- **Frequently Asked Questions**
- Who is using EPSS?
- Open-source EPSS Tools
- API
- Related Exploit Research
- Blog
- Data Partners

Usage

What is EPSS, and what is it not?

EPSS is a measure of exploitability. Specifically, EPSS is estimating the probability of observing any exploitation attempts against a vulnerability in the next 30 days. This is accomplished by observing and recording exploitation attempts against vulnerabilities and then collecting as much information as we can about each of those vulnerabilities. Since EPSS is estimating the probability of exploitation activity, **EPSS is best used when there is no other evidence of active exploitation.** When evidence or other intelligence is available about exploitation activity, that should supersede the EPSS estimate (see “Everyone knows this vulnerability has been exploited...” question).

EPSS is only estimating the probability that a vulnerability will be exploited. EPSS does not account for any specific environmental, nor compensating controls, nor does it make any attempt to estimate the **impact** of a vulnerability being exploited. **EPSS is not, and should not be treated as a complete picture of risk**, but it can be used as one of the inputs into risk analyses. For a visual representation of this we turn to the Open Group Standard: [Risk Analysis \(O-RA\)](#), specifically Figure 2 titled,

Measure Risk with TruRisk™

The most accurate way to **measure & prioritize cyber risk**



Measure Cyber Risk

Quantify risk across vulnerabilities, assets, and groups of assets helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk



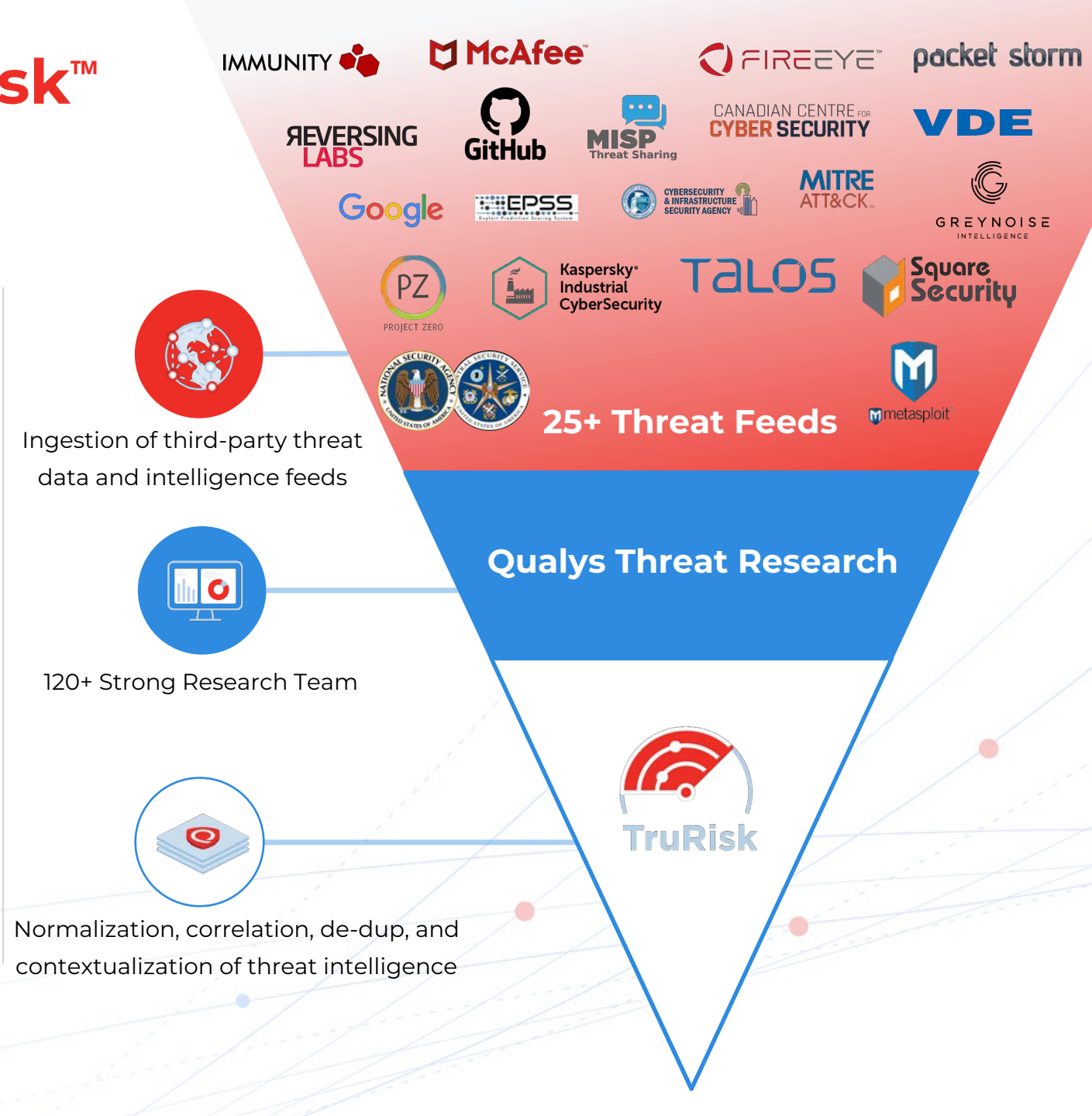
Prioritize Based On Real Risk

Prioritize based on context from the **4-Es: Exposure, Exploitation, Evidence, & Enterprise context**



Best-In-Class Threat Intelligence Included

Leverage insights from over 200k vulnerabilities sourced from over **25+ threat sources** to get best-in-class threat intelligence with the Qualys Cloud Threat DB



Industry Leading Prioritization with **TruRisk™**

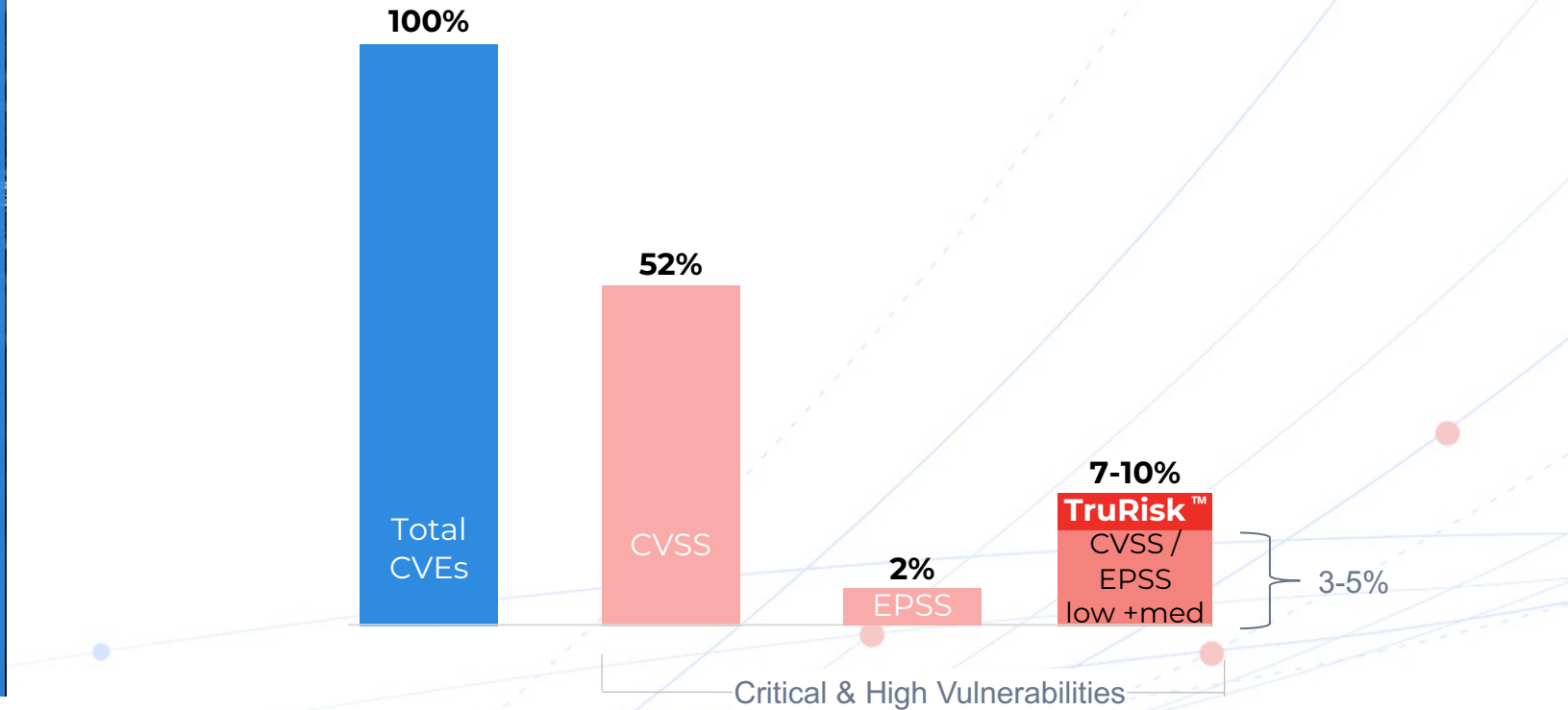
Cut 52% to <10% with **TruRisk™**

CVSS
Too Many

EPSS
Too Few

TruRisk™
Just Right!

CVSS → EPSS → **TruRisk™**



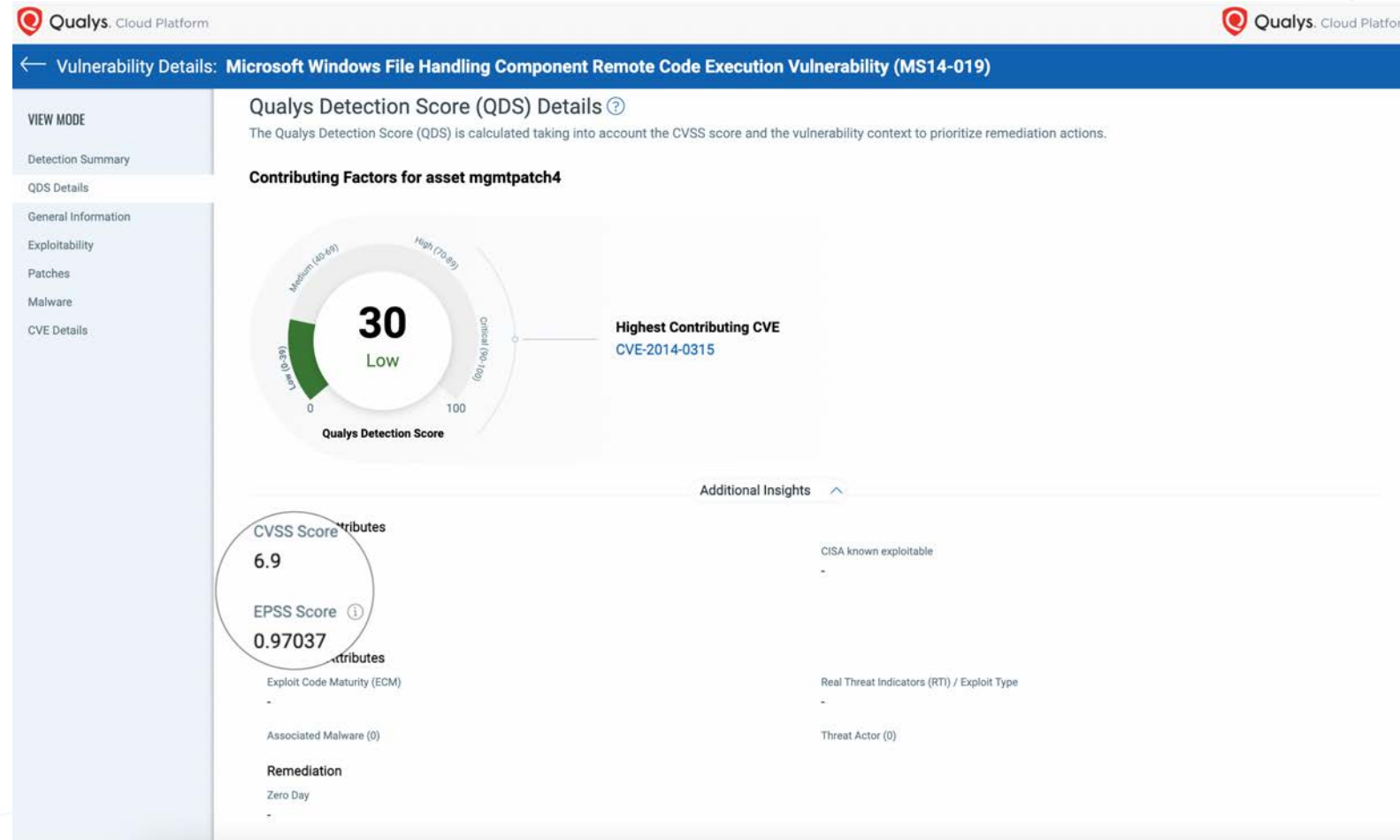
Medium-High CVSS, Critical EPSS, Low **TruRisk™** Microsoft Windows File Handling Component RCE (MS14-019)

CVSS 6.9

EPSS 0.97037

No Evidence
of Exploitation

No Exploits available



Low CVSS, Low EPSS, Critical **TruRisk™** VMware Tools Authentication Bypass Vulnerability (VMSA-2023-0013)

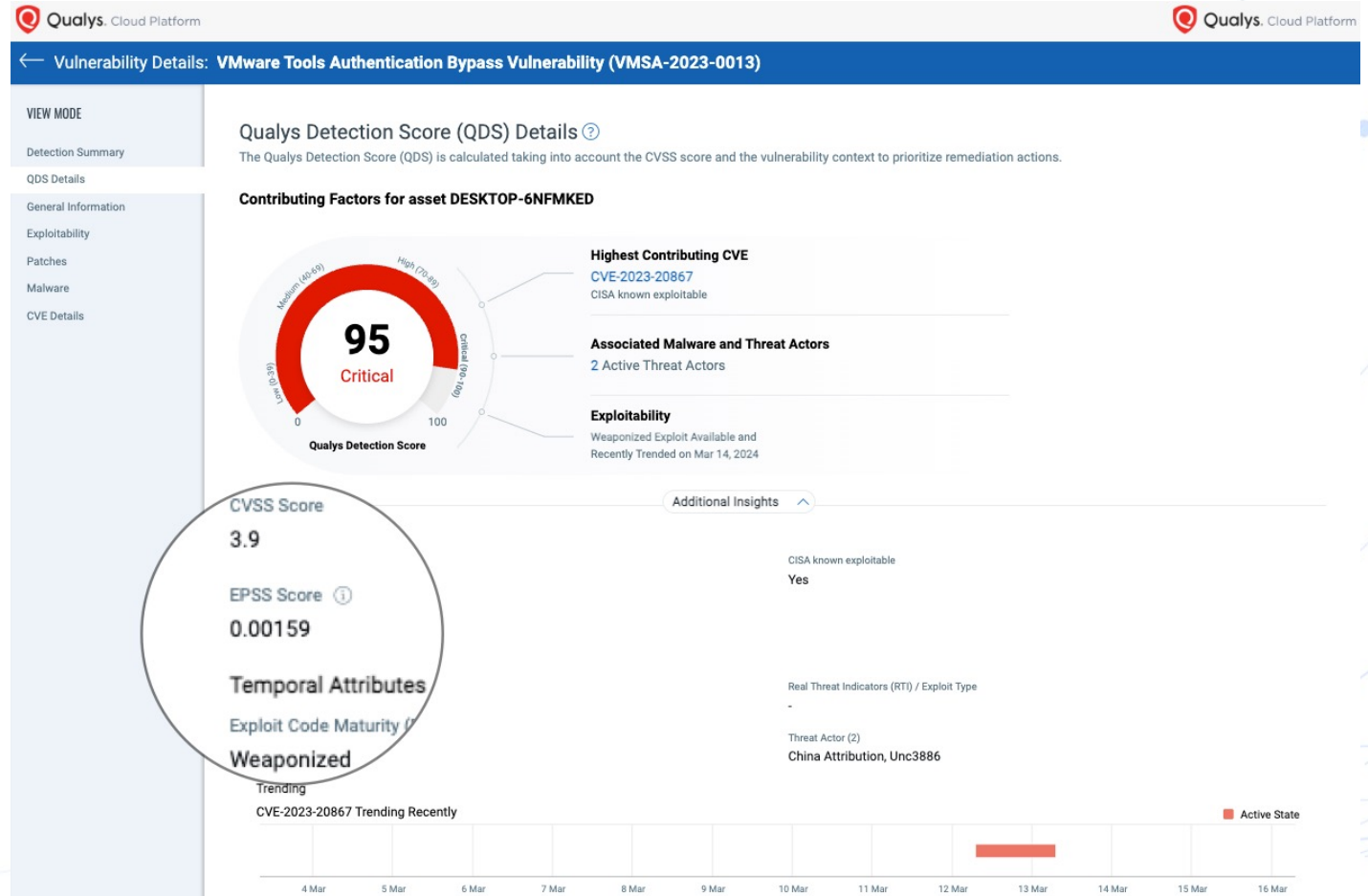
CVSS 3.9

EPSS 0.00159

CISA KEV

Weaponized PoC

Exploited by 2 Threat Actors & Trending



87M Vulnerabilities not prioritized by CVSS & EPSS

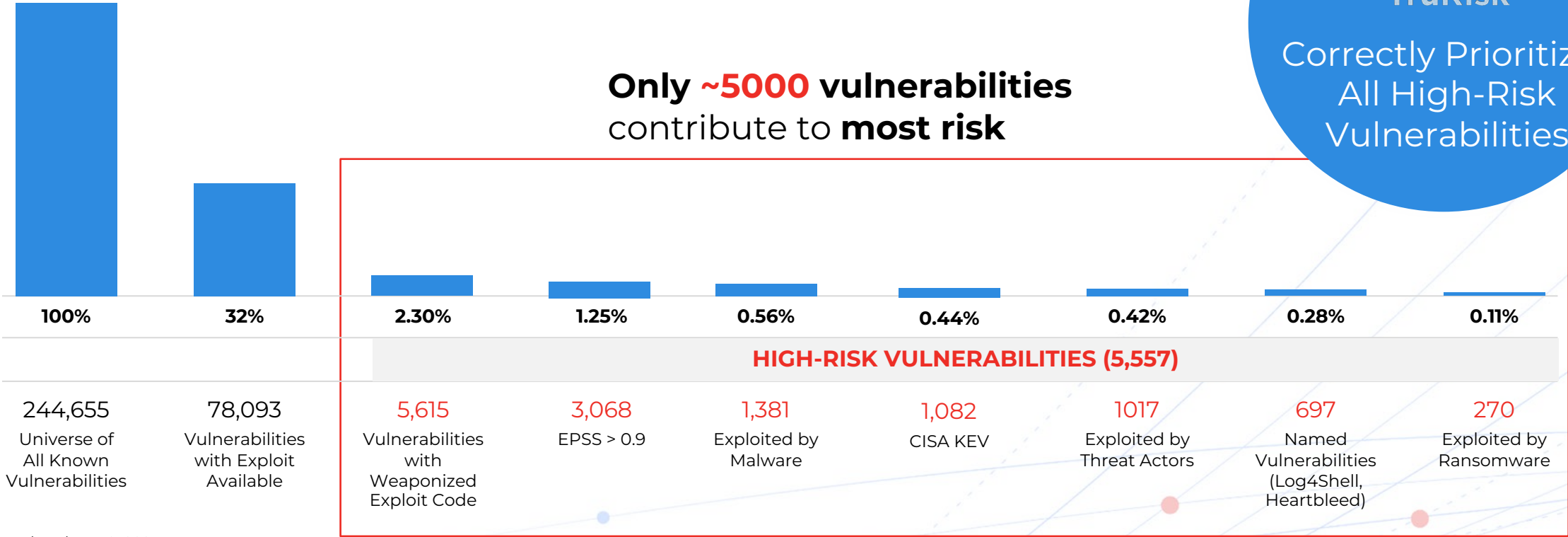
Never Miss a Beat

Focus on What Matters



Correctly Prioritizes
All High-Risk
Vulnerabilities

Only **~5000** vulnerabilities
contribute to **most risk**

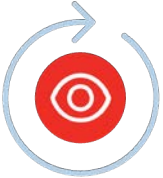


Updated: Apr 9, 2024



Qualys VMDR with TruRisk™

The **fastest**, the most **accurate**, and the most **comprehensive**



Coverage

Detect vulnerabilities with the industry-leading signature database across your entire attack surface (IT/OT/IoT, Cloud, External). With EASM, know your unknown risk too.



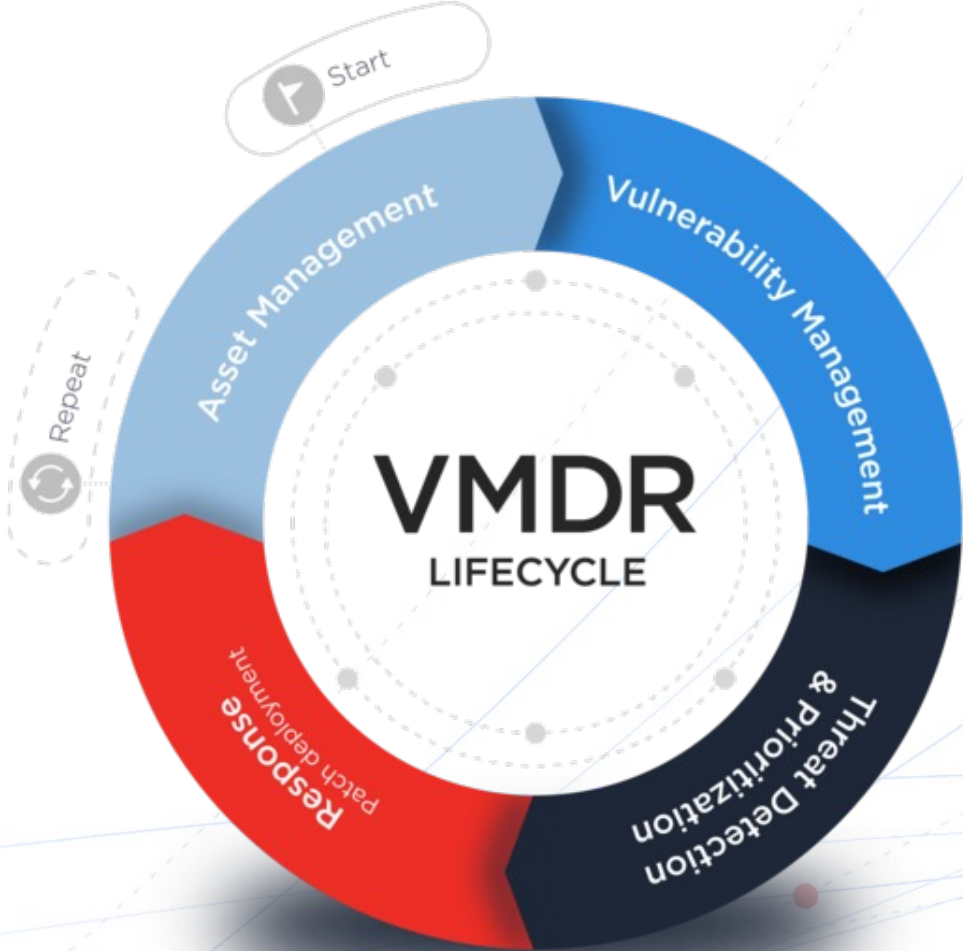
Accuracy

Six-sigma (99.99966%) accuracy combined with 25+ sources of threat intel drives pinpoint TruRisk™ Scoring and confident prioritization.



Speed

No scheduled agent scans required. Detect vulnerabilities in less than 4 hours—up to 6x faster than competitive solutions.



Announcing: Software Composition Analysis (Open Source)

Now available to
all VMDR
customers at no
charge!

56

No. of vulnerable
open-source packages
per asset

41%

OSS Vulnerabilities with
Exploits available on each
asset

91%

Packages had OSS with no
development activity in
the last two years

Qualys Cloud Platform

Asset Details: WIN-645CPM4DA60

Software Composition Analysis (SCA)

Vulnerabilities (52) **Software Components (559)**

Search...

The page displays up to maximum of 2000 components.

SOFTWARE NAME	SOFTWARE VERSION	TECHNOLOGY NAME	TARGET PATH
tomcat-embed-websocket:tomcat-embed-websocket	9.0.56	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
log4j:log4j	1.2.17	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
jackson-databind:jackson-databind	2.13.1	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...
ch.qos.logback:logback-core	1.2.10	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...
com.icegreen:greenmail	1.3	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
:spring-aop	5.3.15	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
logback-classic:logback-classic	1.2.10	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...
:spring-form	0.0.1-SNAPSHOT	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
org.subethamail:subethasmp	2.1.0	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...
:Spring Boot AutoConfigure	2.6.3	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
:spring-core	5.3.15	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
com.fasterxml:jackson.core:jackson-annotations	2.13.1	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...
org.attoparser:attoparser	2.0.5.RELEASE	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main.zip!Spring4Sh...
com.fasterxml:jackson.datatype:jackson-datatype-jsr...	2.13.1	Java	c:\Users\jerry\Downloads\Spring4Shell-POC-main\Spring4Shell...

Expand VMDR with Qualys Custom Assessment & Remediation (CAR)



Bring Your Own QID

Write your own vuln custom detection scripts to measure your risk



Run Your Own Remediation Scripts

Qualys agents run your custom scripts



Fully Integrated Into VMDR

Measure and communicate custom risk as part of VMDR



PowerShell



python™



Perl



Lua



vbscript

Communicate Risk with TruRisk™

Know Your Risk Posture from Every Angle

01

Measure Accurately

Accurately measure, quantify, and track risk reduction over time, across vulnerabilities, assets, and groups of assets

02

Communicate Precisely

Communicate risk across different teams, business units and geographic locations by leveraging dashboards, reports and ITSM tools

03

Eliminate Effectively

Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk

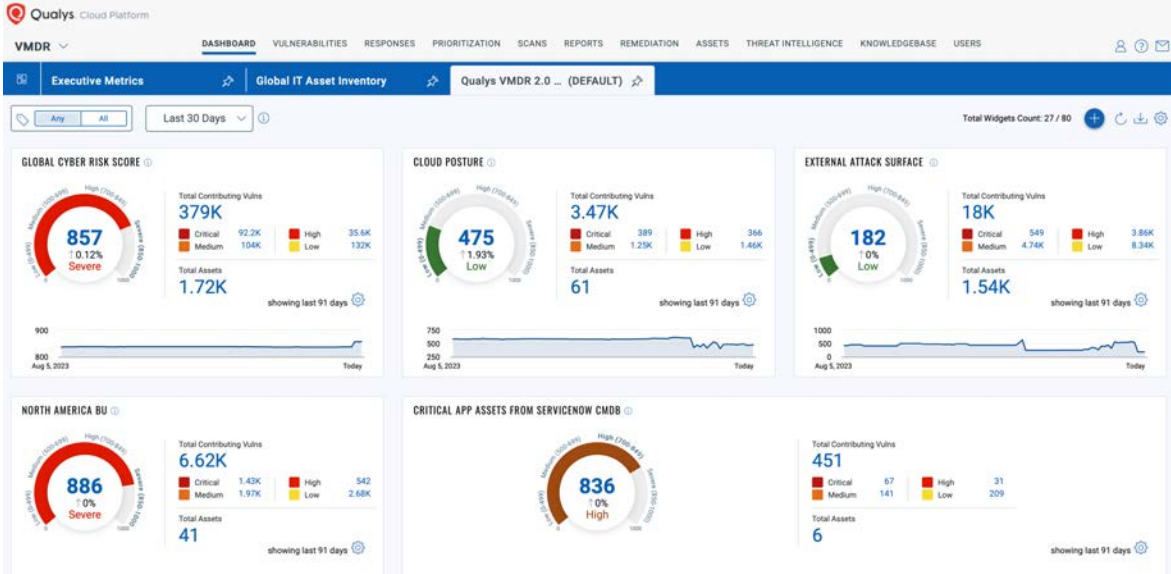


Communicate Risk with VMDR



Use Unified Dashboards To Communicate Risk

Create intuitive, customized **persona-based dashboards**, and share them across the organization from C-Level execs to practitioners



Communicate Risk with VMDR

✔ Use Unified Dashboards To Communicate Risk

Create intuitive, customized **persona-based dashboards**, and share them across the organization from C-Level execs to practitioners

✔ Integrate with ITSM & Ticketing Solutions

Use Vulnerability Tagging to achieve precise **Vulnerability Routing**. Automatically create **rule-based notifications** and **workflow tickets**, assign tasks to **rightful owners** (based on CMDB metadata), and **automatically close** them out upon remediation.

The screenshot shows the ServiceNow 'Assignment Rule' configuration interface. The rule is named 'App - Database Teams' and is associated with the application 'Qualys VMDR'. The execution order is set to 100. The rule is currently inactive. The configuration includes a table selection of 'Qualys - VMDR Task [x_qual5_vmdr_vuln_task_item]' and two conditions: 'Qualys Detection.QID.Catego...' is 'Database' and 'Qualys Detection.QID.Title' contains 'Database'. The interface also shows options to 'Update' and 'Delete' the rule, and a 'Related Links' section with 'Add to Update Set' and 'Find References'.

Communicate Risk with VMDR

✓ Use Unified Dashboards To Communicate Risk

Create intuitive, customized **persona-based dashboards**, and share them across the organization from C-Level execs to practitioners

✓ Integrate with ITSM & Ticketing Solutions

Use Vulnerability Tagging to achieve precise **Vulnerability Routing**. Automatically create **rule-based notifications** and **workflow tickets**, assign tasks to **rightful owners** (based on CMDB metadata), and **automatically close** them out upon remediation.

✓ Leverage TruRisk™ Report

Share the **State of the Union with executives** to understand the latest trends and landscape of risk for your organization, and implement prescriptive actions to mitigate risk



Eliminate Risk with **TruRisk™**

Ingesting the Best Intelligence Anywhere

01

Measure Accurately

Accurately measure, quantify, and track risk reduction over time, across vulnerabilities, assets, and business units

02

Communicate Precisely

Communicate risk across different teams, business units and geographic locations by leveraging dashboards, reports and ITSM tools





03

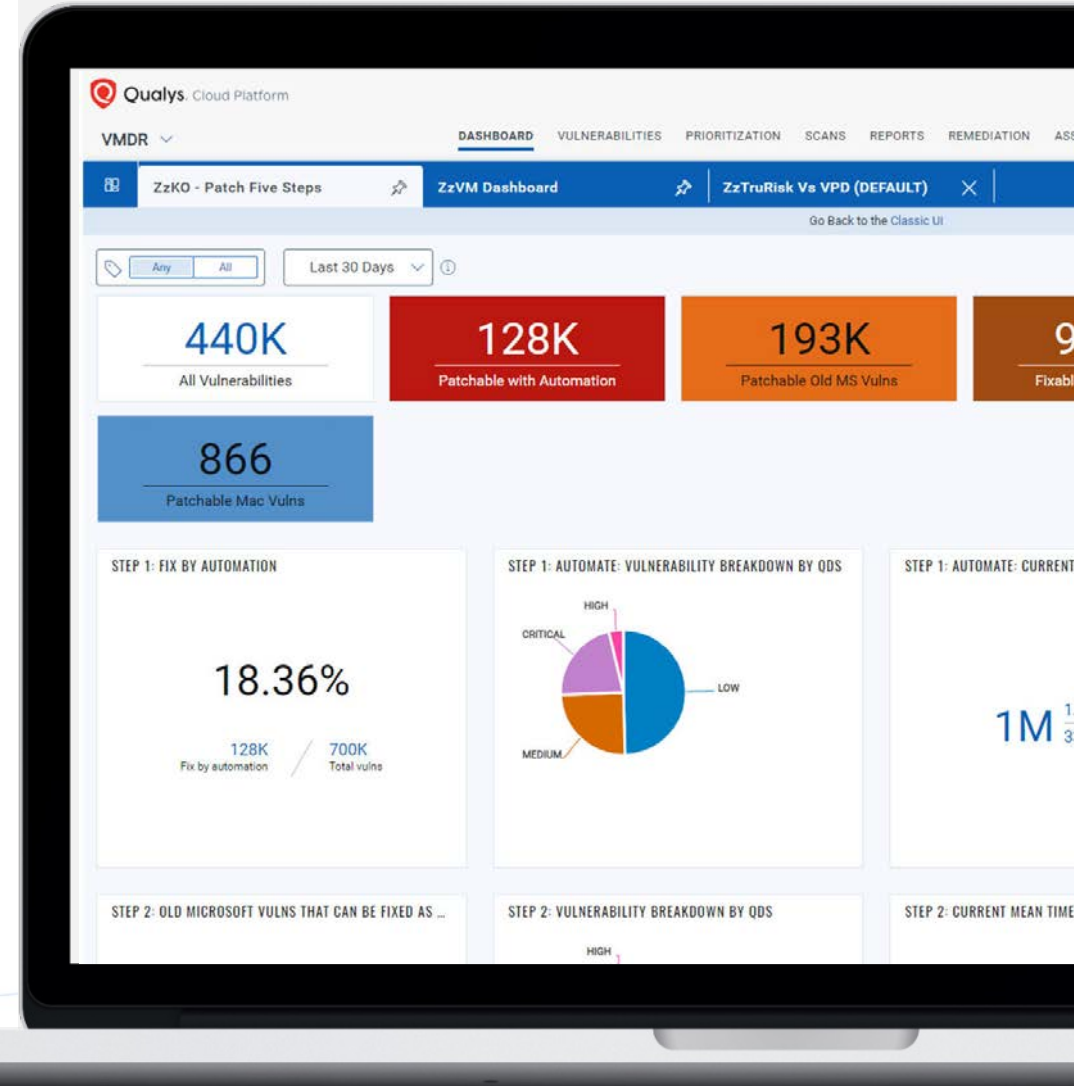
Eliminate Effectively

Patch any device anywhere, leverage multiple avenues from remediation to mitigation and block attack paths to eliminate risk



Eliminate Risk with Qualys Patch Management

-  **Patch Any Device, Anywhere**
Patch all major Windows, Linux & macOS, 3rd Party Apps. Run scripts to fix misconfigs or run custom remediation.
-  **Automated Risk Based Remediation**
Precisely identify patches to remediate vulnerabilities, and automatically remediate low impact, high risk vulnerabilities with zero touch automated patching.
-  **Track Remediation End To End**
Integrate with ITSM solutions to automatically create tickets, deploy patches upon approval drastically improving MTTR.
-  **Eliminate Attack Paths with MITRE ATT&CK Context**
Leverage MITRE ATT&CK Insights to identify and eliminate attack paths and break kill chains to reduce risk (e.g., lateral movement).



Introducing: 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



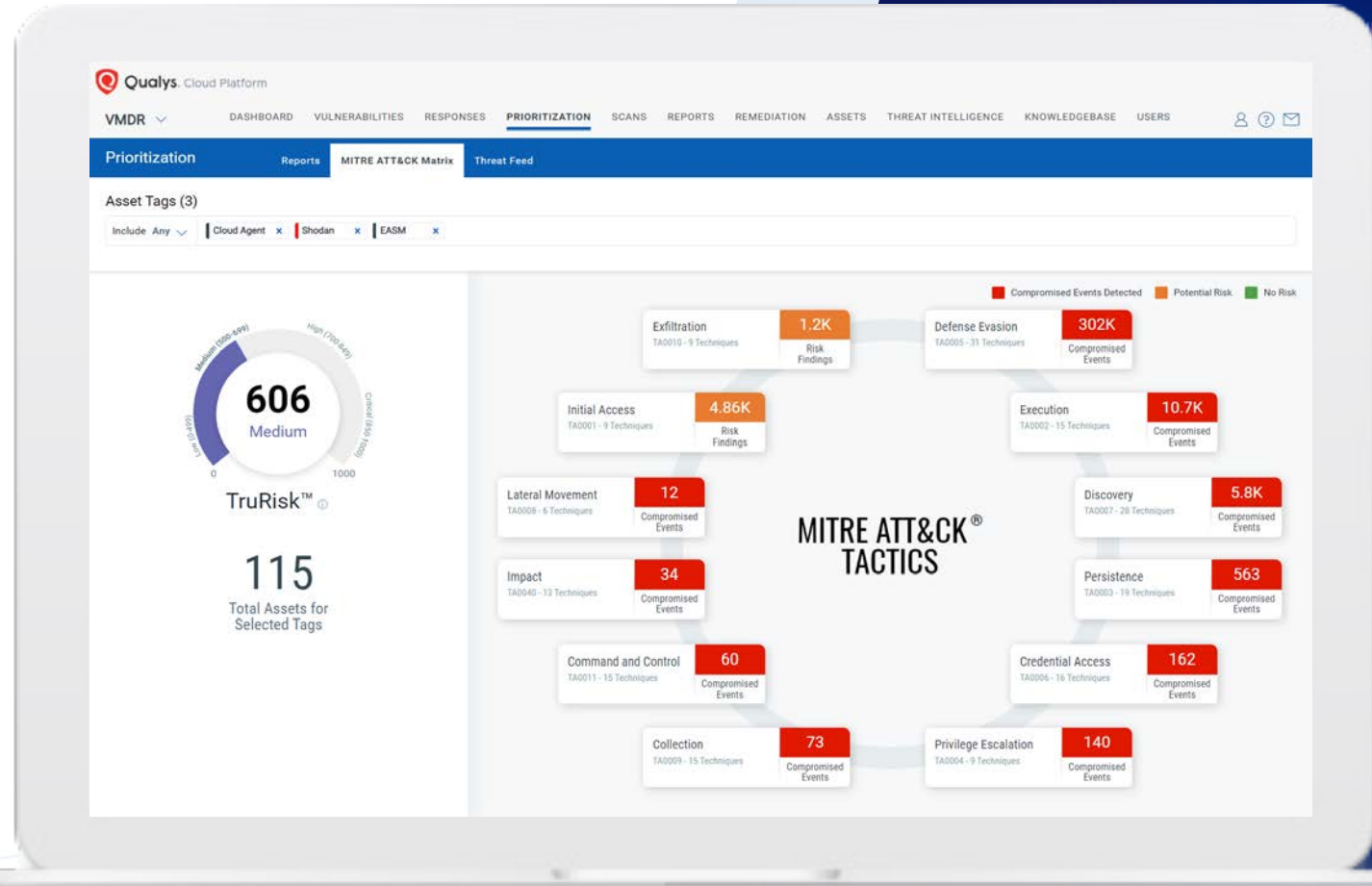
Holistic ATT&CK View

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



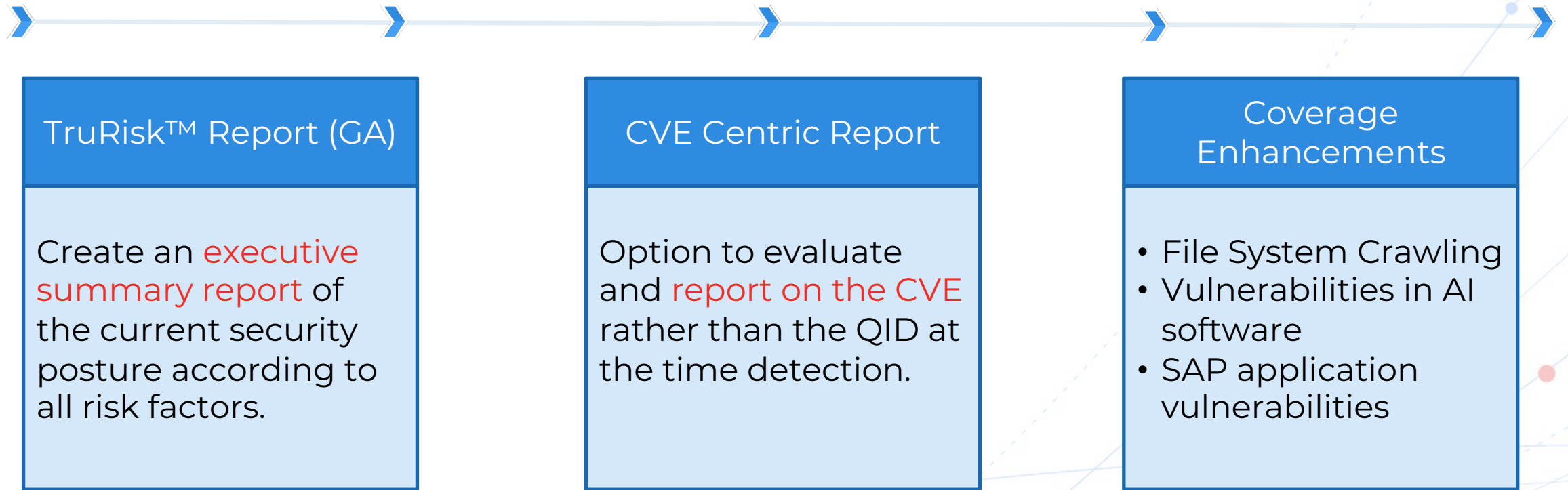
Demo



What's Next?

What's Next?

Top 3 Upcoming Features for VMDR



But wait... There's more!

2:20 PM
Ballroom 2

Remediating the Nightmares:
Preparing to Defend Against Multi-channel Vulnerabilities



Eran Livne

3:20 PM
Ballroom 2

CSAM / ITSM:
What Have we Learned, and How Can You Benefit?



Pablo Quiroga

4:10 PM
Main Stage

Measuring and Detecting Cloud Risks
with Artificial Intelligence



Kunal Modasiya



Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

An abstract graphic in the bottom right corner consists of several thin white lines and dots. Some lines are solid, while others are dashed. The dots are colored in blue and red, scattered across the lower right portion of the blue background.

One more thing...



