QSC24

VMDR: Putting the M Back in *V*ulnerability *M*anagement:

A Holistic Approach to Cybersecurity Risk

Joe Petrocelli
VP, Product Management

Agenda

01 The State of VM Today

02 Proactive VM

03 What’s new with Qualys VMDR?

04 Demo & Call to Action

05 Customer Showcase

The State of Vulnerability Management Today

Qualys®

The State of Vulnerability Management Today

01

Traditional Approaches Falling Short

- ✓ Slow to detect new, exploitable CVEs
- ✓ Failure to cover the entire dynamic attack surface
- ✓ Lack threat intel and cyber risk context to prioritize

73%

of CISOs feel that Vulnerability Assessment Alone is Inadequate

74%

of CISOs feel that Human Error is to Blame

The State of Vulnerability Management Today

89%

Of CISOs feel that Modernization has Created Blind Spots

02

Evolving Threat Landscape

- ✓ Time to exploitation is faster than ever
- ✓ Cybersecurity community is reactive
- ✓ Exposures on assets unknown to SecOps teams

2169

Average number of new vulns every month

The State of Vulnerability Management Today

76

Average number of Security Tools in an Enterprise

80%

Of enterprises observe fewer breeches when they adopt a Risk Centered Approach

03

Need for Comprehensive Strategy

- ✓ 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

Challenge: A Holistic Approach to VM

Prioritizing Across a Dynamic Threat Landscape

Diverse Environments

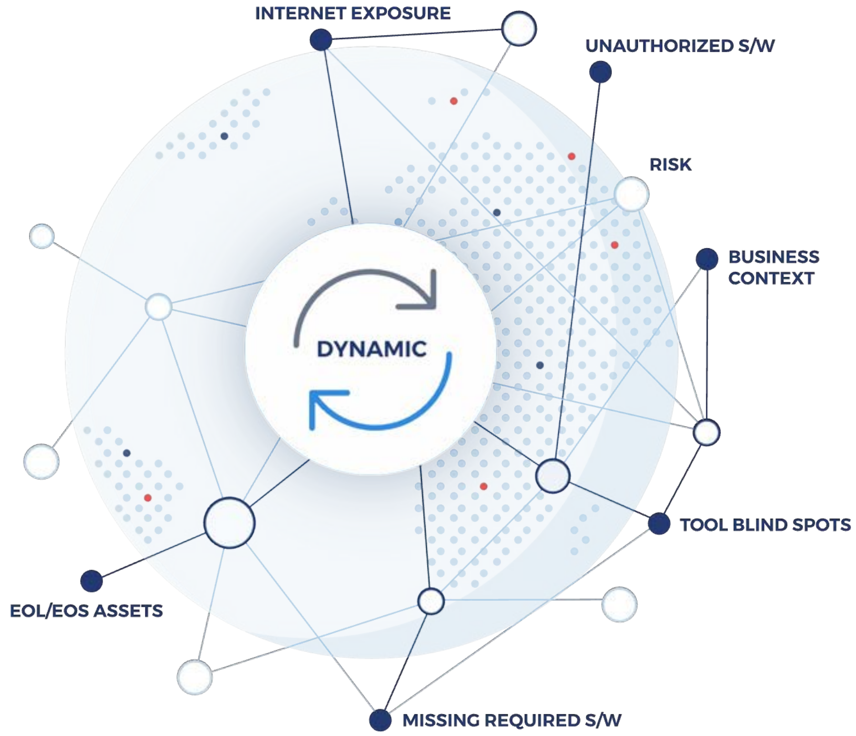
Modern IT landscapes span multiple clouds, endpoints, networks, and applications, increasing complexity.

Expanded Attack Surface

More entry points for attackers means greater risk exposure for organizations.

Holistic Management

A comprehensive approach like using the Qualys Risk Operations Center is crucial to identify and mitigate vulnerabilities across all assets.



Undesired Outcomes

Endless Cycle of Failed Results

Inventory gaps on external attack surface, IoT/OT devices, blind to software components, and stale CMDBs, leading to a breach

Security Teams **waste time remediating inconsequential vulnerabilities**, which **don’t reduce risk**

IT Teams miss SLAs for high-risk vulnerabilities, expanding the window for attackers

Security & IT Teams **waste countless hours communicating risk through spreadsheets, reports & manual processes**

Failures expose organization to unnecessary risk

Failure to Remediate Efficiently

What Is Financial Impact?

$4.9 M	Average Breach Cost
$2.2 M	Manual Remediation Cost (Labor)
287 Days	Breach Remediation Time (Reactive)

Shifting from Reactive to Proactive with Risk-Based Vulnerability Management

Qualys®

Risk-Based Vulnerability Management

01

Identify Assets

Create a comprehensive inventory of all IT assets and their criticality to the business.

02

Assess Vulnerabilities

Evaluate vulnerabilities based on severity, exploitability, and potential business impact.

03

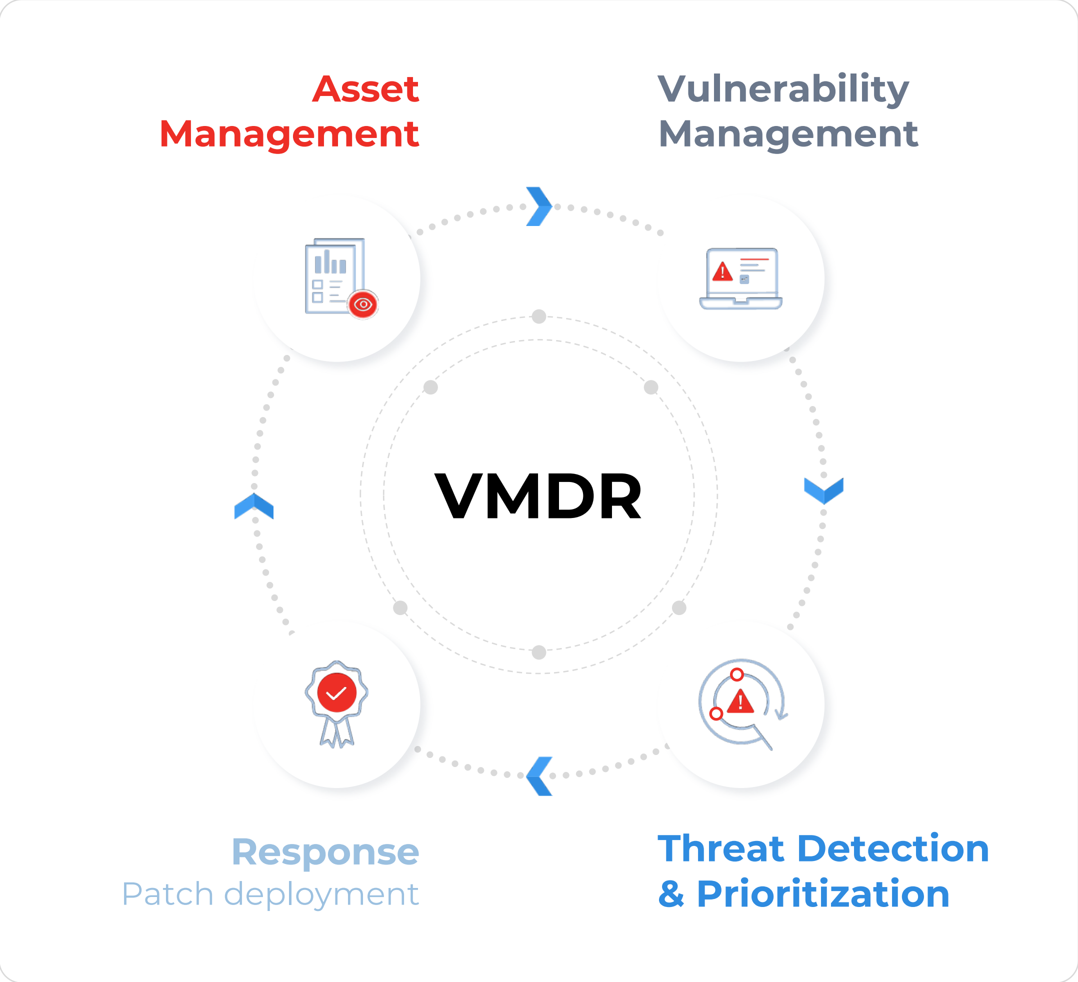
Prioritize Risks

Rank vulnerabilities to focus remediation efforts on the most critical issues first.

04

Allocate Resources

Assign personnel to address high-priority vulnerabilities efficiently.



Risk-Based VM (RBVM) Foundation

Key Components & Outcomes

04 Remediate

Workflow Automation
ITSM (ServiceNow, Jira, Qflow)

Patch Management
Remediate Vulnerabilities

Mitigation
Mitigate vulnerabilities or isolate assets

Reduce Cyber Risk Across the Enterprise
Attach cybersecurity actions to business outcome

03 Prioritize

Risk Prioritization
Qualys TruRisk Scoring

Attack Surface
Attack Surface Management (EASM)

Threat Intelligence
25+ threat & exploit intelligence

02 Assess

Asset Inventory
Native-integrated on prem/cloud asset inventory

Certificate Inventory
Track Expired/ Expiring Certificates

Vulnerability Assessment
Real time Vulnerability and Configuration Assessment

Regulatory Compliance
Compliance Assessment (PCI, CSF, HIPAA, 800-53 & more)

01 Discover

Vulnerability Coverage
100K+ CVEs, sub-24hr coverage for critical CVEs

CIS/DISA STIGS Hardening
Attack Surface Hardening (300+ Policies)

Speed and Accuracy
- <4-hour vuln detection
- 99.99966% accuracy

Comprehensive Sensors
Agents, virtual/physical scanners, passive sensors, external scanners

APIS
API-First solution, integrate with 3rd party reporting platforms

What Does It Mean to Be Proactive?

Prioritize and Remediate According to RTIs

Continuous Monitoring

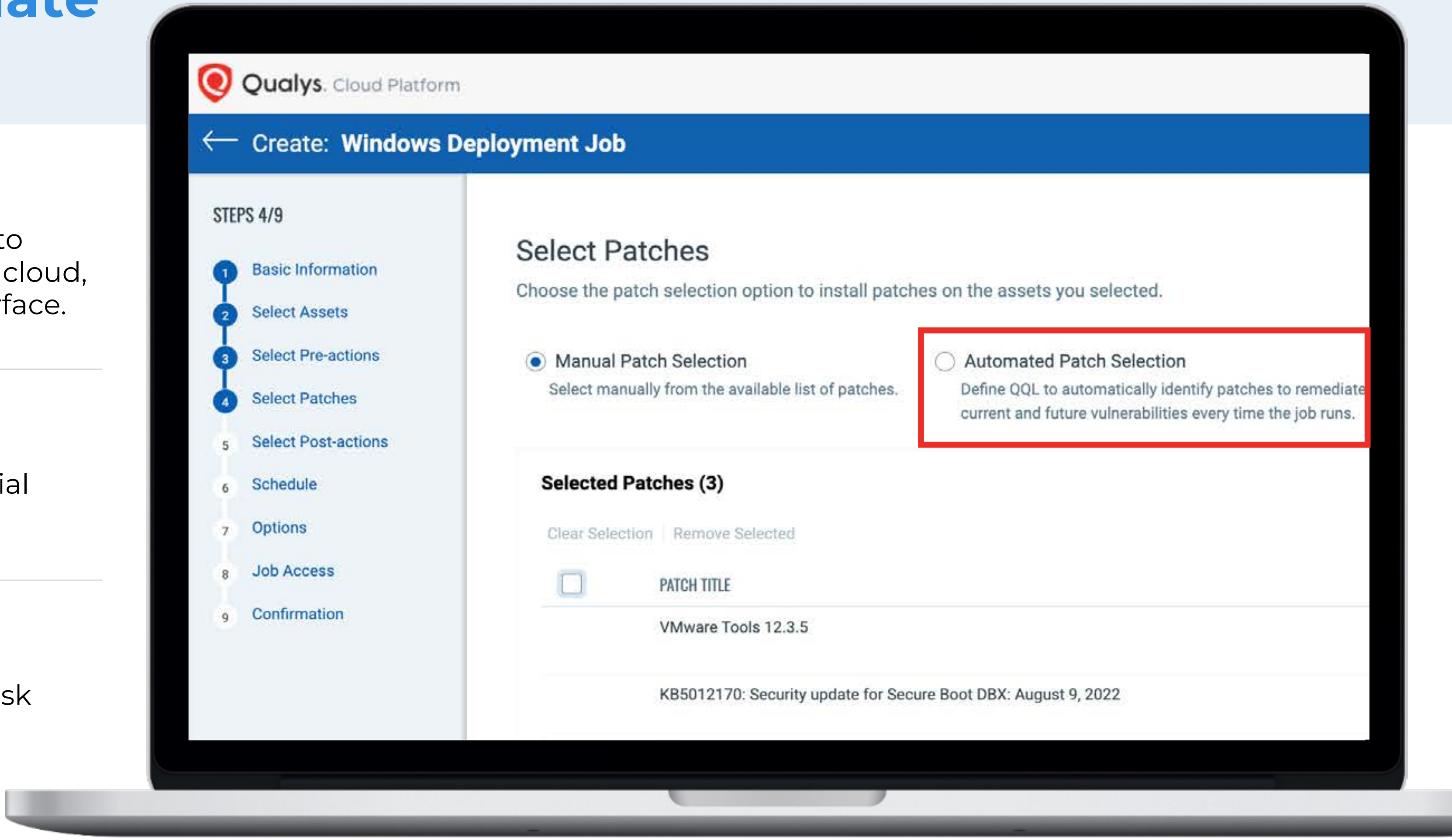
Implement real-time vulnerability detection to identify and prioritize threats, whether in the cloud, on prem, OT/IoT, or on the external attack surface.

Integrate Threat Intelligence

Incorporate threat feeds to anticipate potential exploits and prioritize accordingly.

Automate Remediation

Deploy self-healing systems to address low-risk vulnerabilities without manual intervention.



Qualys. Cloud Platform

Create: **Windows Deployment Job**

STEPS 4/9

1 Basic Information
2 Select Assets
3 Select Pre-actions
4 Select Patches
5 Select Post-actions
6 Schedule
7 Options
8 Job Access
9 Confirmation

Select Patches

Choose the patch selection option to install patches on the assets you selected.

● Manual Patch Selection
Select manually from the available list of patches.

○ Automated Patch Selection
Define QQL to automatically identify patches to remediate
current and future vulnerabilities every time the job runs.

Selected Patches (3)

Clear Selection | Remove Selected

□	PATCH TITLE
	VMware Tools 12.3.5
	KB5012170: Security update for Secure Boot DBX: August 9, 2022

You Can’t Do This Manually

Leveraging Automation in Your VM Program

Automated Discovery

Continuously scan networks to identify new assets and potential vulnerabilities.

Intelligent Reporting

Generate customized reports and dashboards to track vulnerability trends and remediation progress.

Orchestrate Remediation

Automate patch deployment and configuration changes to streamline the fix process.

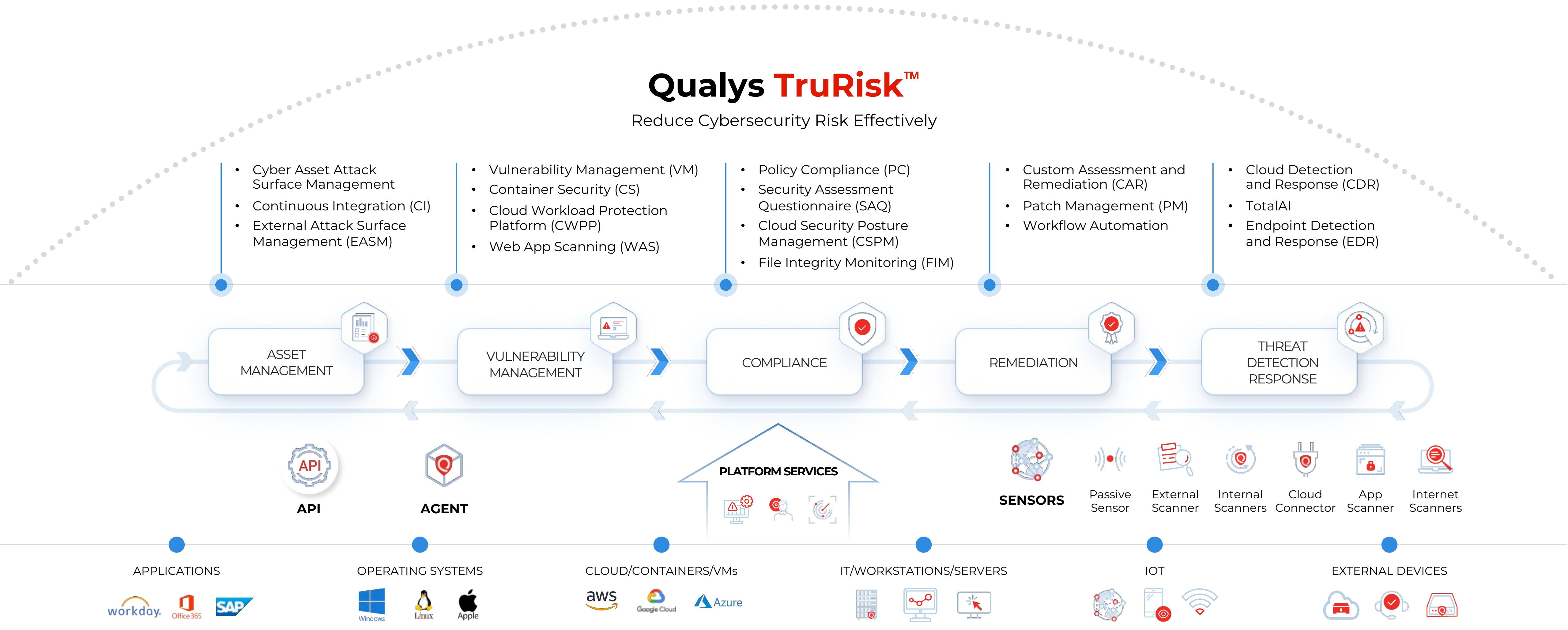
Compliance Monitoring

Automatically assess and report on compliance with security standards and regulations.

Qualys VMDR

Qualys®

Qualys Enterprise TruRisk™ Platform



Qualys TruRisk™

Reduce Cybersecurity Risk Effectively

- Cyber Asset Attack Surface Management
- Continuous Integration (CI)
- External Attack Surface Management (EASM)

- Vulnerability Management (VM)
- Container Security (CS)
- Cloud Workload Protection Platform (CWPP)
- Web App Scanning (WAS)

- Policy Compliance (PC)
- Security Assessment Questionnaire (SAQ)
- Cloud Security Posture Management (CSPM)
- File Integrity Monitoring (FIM)

- Custom Assessment and Remediation (CAR)
- Patch Management (PM)
- Workflow Automation

- Cloud Detection and Response (CDR)
- TotalAI
- Endpoint Detection and Response (EDR)

ASSET MANAGEMENT

VULNERABILITY MANAGEMENT

COMPLIANCE

REMEDIATION

THREAT DETECTION RESPONSE

API

AGENT

PLATFORM SERVICES

SENSORS

Passive Sensor

External Scanner

Internal Scanners

Cloud Connector

App Scanner

Internet Scanners

APPLICATIONS

workday. Office 365 SAP

OPERATING SYSTEMS

Windows Linux Apple

CLOUD/CONTAINERS/VMs

aws Google Cloud Azure

IT/WORKSTATIONS/SERVERS

IOT

EXTERNAL DEVICES

DE-RISK YOUR **BUSINESS**

Qualys.

Measure Risk with TruRisk™

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

Measure Cyber Risk

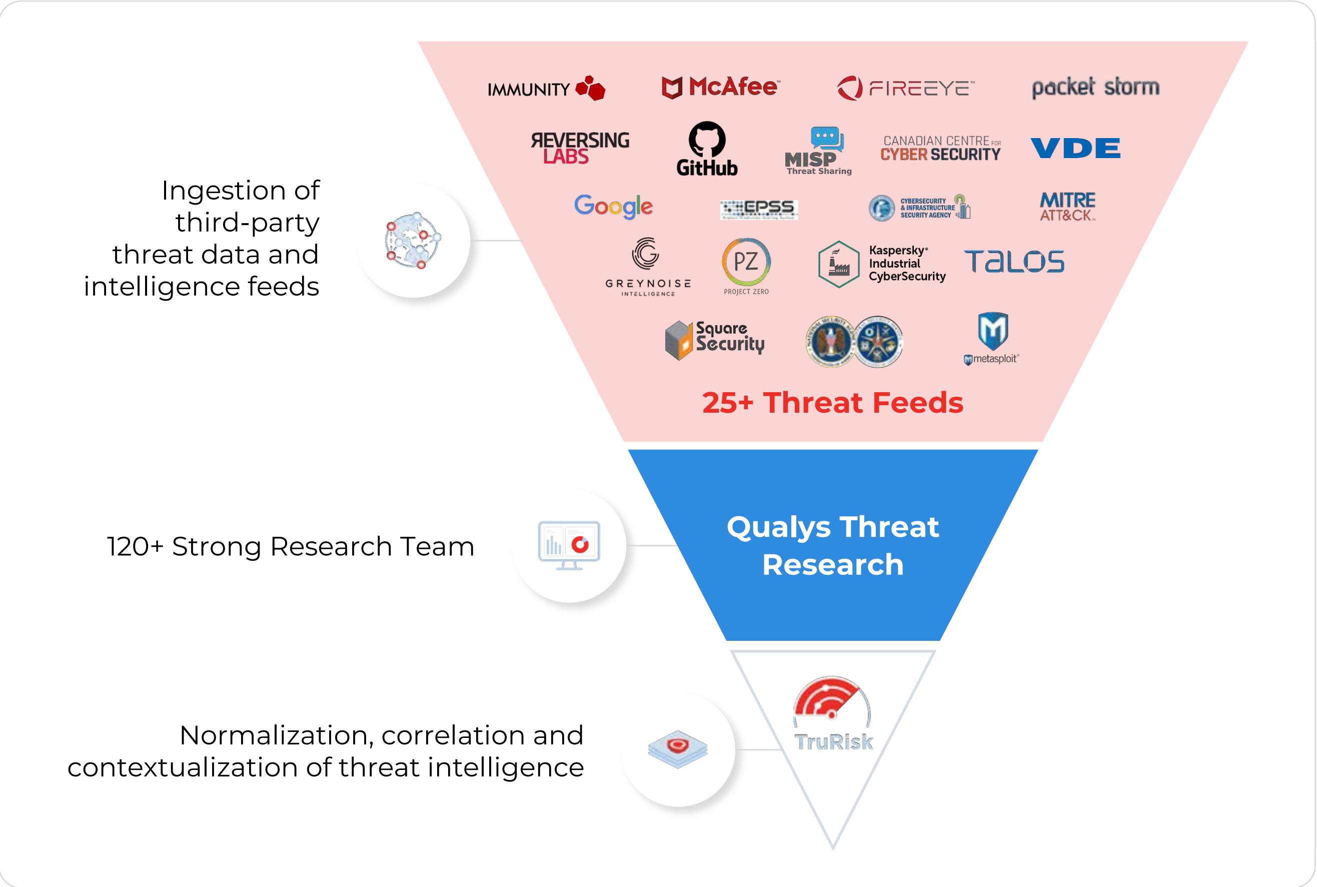
Quantify risk across vulnerabilities, assets, and groups of assets helping organizations proactively reduce risk exposure and track risk reduction over time with Qualys TruRisk

Prioritize Based On Real Risk

Prioritize based on context from the **4-E**s: **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



Ingestion of third-party threat data and intelligence feeds

25+ Threat Feeds

120+ Strong Research Team

Qualys Threat Research

Normalization, correlation and contextualization of threat intelligence

TruRisk

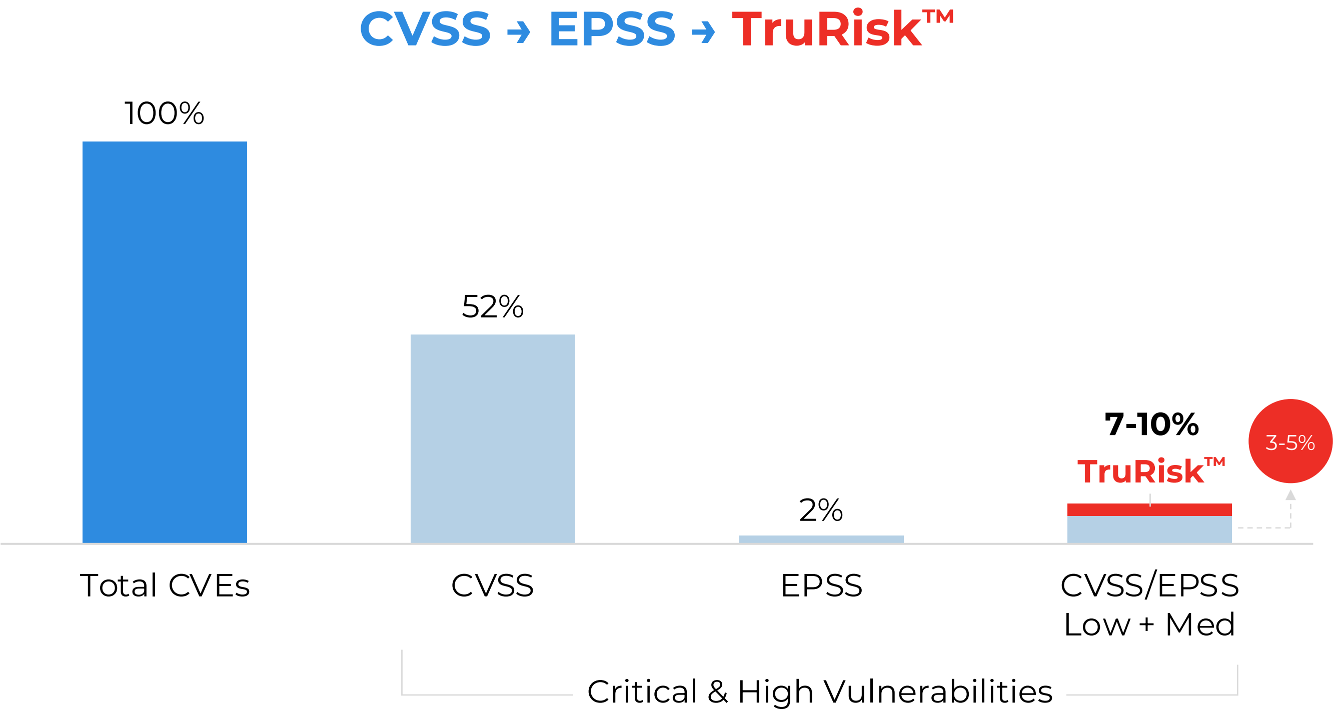
Industry Leading Prioritization with TruRisk™

Cut 52% to **<10% with TruRisk™**

CVSS
Too Many

EPSS
Too Few

TruRisk™
Just Right!



Qualys Risk Operations Center

Challenges with Status Quo

74%
CISOs who feel Vuln Assessment is inadequate

89%
CISOs feel that modernization has created choas

4 Days a Week
Time “wasted” fixing what doesn’t matter

Measure and Prioritize Risk

Enterprise TruRisk™ Platform

- Asset Context
- Endpoints
- Infrastructure
- CI/CD
- Cloud

Reassess Risk Score

Reduction of Risk

Drive Action

- Automated Patching
- Host Isolation
- Mitigation Techniques
- Remediation Workflows

Customer Outcomes

Enterprise Visibility → Risk Prioritization → Risk Quantification → Reduction of Risk

DE-RISK YOUR **BUSINESS**

Qualys.

What's New in VMDR?

Qualys

Roadmap

TruRisk

TruRisk™ Customization

- Toggle Modules
- Customize Score
- Customize TruRisk™ Formula & Weights
- Customize Severity Bands

IPv6 Support

- Expansion to 25k unique IPv6 ranges
- IPv6 Support for Cloud Instances - AWS, Azure & Cloud Perimeter Scans
- PCI Merchant Portal to support IPv6 Scans
- Certificate Assessment for IPv6 addresses

Exception Management

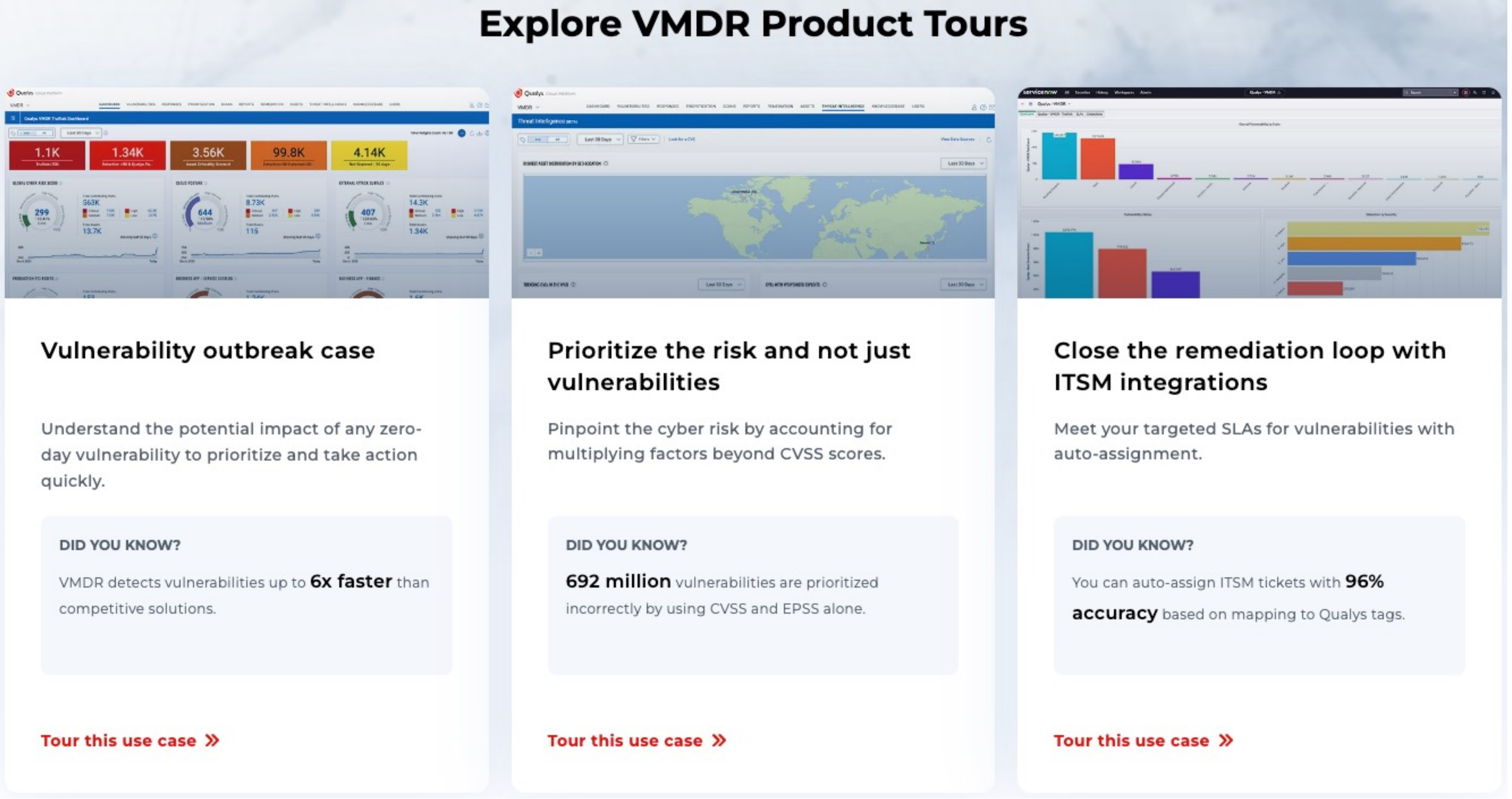
- Change QDS & Severity of Vulns
- Classify Vulns as Risk Accepted or False Positives
- Multi-layered Exception Approval Workflows

UX Overhaul

- Navigation Menu
- New User Onboarding
- Scan Management
- Reporting
- Knowledgebase
- Remediation
- Assets
- Vulnerabilities

*Subject to change

Call to Action!



Explore VMDR Product Tours

Vulnerability outbreak case

Understand the potential impact of any zero-day vulnerability to prioritize and take action quickly.

DID YOU KNOW?

VMDR detects vulnerabilities up to **6x faster** than competitive solutions.

Tour this use case »

Prioritize the risk and not just vulnerabilities

Pinpoint the cyber risk by accounting for multiplying factors beyond CVSS scores.

DID YOU KNOW?

692 million vulnerabilities are prioritized incorrectly by using CVSS and EPSS alone.

Tour this use case »

Close the remediation loop with ITSM integrations

Meet your targeted SLAs for vulnerabilities with auto-assignment.

DID YOU KNOW?

You can auto-assign ITSM tickets with **96% accuracy** based on mapping to Qualys tags.

Tour this use case »

https://www.qualys.com/apps/vulnerability-management-detection-response/#product-tour

Qualys®