Qualys.

GUIDE

Implementing Risk-Based Vulnerability Management

February 2023

Table of Contents

Foundational Vulnerability Management Framework

Establishing a Vulnerability Management program enables an organization to properly identify, prioritize, and remediate vulnerabilities on information technology assets used to conduct business operations. A mature vulnerability management program is a foundational element of any functioning cybersecurity program.

Organizations should choose to adopt a successful program strategy to apply high-level functions; to identify, protect, detect, and respond to vulnerability management. Each function defines key objectives that can be incorporated into a vulnerability management process. Meeting these key objectives will contribute to a more mature cybersecurity strategy.

Identify

Develop an understanding of information assets that are used to meet business needs and the risk to business operations

- ✓ Inventory assets, software, and applications
- ✓ Assign business context and criticality to an asset
- ✓ Ingest threat intelligence and map it to vulnerabilities
- ✓ Use threats, vulnerabilities, likelihood, and impact to prioritize remediation

Protect

Implement safeguards to limit the impact of a malicious event

- ✓ Document a vulnerability management plan to include policies, processes, procedures, and controls

Detect

Implement solutions to identify vulnerabilities

- ✓ Perform vulnerability scans and continually assess the effectiveness of the scans

Respond

Implement activities to act on new vulnerabilities

- ✓ Investigate and remediate findings
- ✓ Establish processes on how to respond to vulnerabilities
- ✓ Certain vulnerabilities identified are accepted within risk tolerance or subject to risk reduction through mitigation where remediation is not possible

In addition to these key objectives, successful VM programs have a defined scope, exception tracking, reporting, and metrics. These functions and objectives are supported by the NIST Cybersecurity framework.[1]

While these elements serve as an important foundation for vulnerability management the sheer number of vulnerabilities disclosed daily creates a challenge for Cybersecurity and IT teams seeking the most expedient way to reduce risk to the organization. Organizations should therefore pivot to a risk-based approach to address the most significant flaws to reduce risk to critical systems and make efficient use of limited resources.

1. Framework for Improving Critical Infrastructure Cybersecurity

Risk-Based Vulnerability Management (RBVM)

The scale of vulnerabilities identified in large organizations in today's threat landscape has made the practice of managing them a seemingly endless challenge. Traditional vulnerability management programs tend to adopt an "everything is a risk" approach which leads to frustration among IT remediation teams to remediate an exponentially increasing pool of vulnerabilities many of which do not pose a real risk to the organization.

Instead of using arbitrary methods to prioritize remediation organizations should refine their remediation methods to enrich vulnerability data with business context, threat intelligence, data science, and machine learning to prioritize vulnerabilities that are most likely to be exploited thereby causing the most harm to a given organization. This requires vulnerability management programs to use more accurate methods of assessing risk to keep pace with evolving threats.

Five Pillars to Building a Risk-Based Vulnerability Management Program

1 Identify

Build a comprehensive up-to-date inventory of all assets across modern fragmented IT environments. This includes on-premises, public cloud, mobile devices, OT environments, and items that are hosted outside of your network or that are internet-facing. Maintaining an asset inventory of hardware and software is core to any successful cybersecurity program.

2 Context

Use business context to assign criticality to assets e.g., production assets hosting critical information vs dev systems. Use threat intelligence to enrich understanding of vulnerabilities e.g., which ones are exploited in the wild, have an exploit available, and the ease with which they can be exploited. These are vulnerabilities that are more likely to be exploited.

3 Assess

Perform continuous vulnerability assessment to maintain an accurate picture of risk as often as possible. Perform secure configuration assessments to validate system hardening is consistent with adopted security controls based on industry standard guides such as Centre for Internet Security (CIS) or DISA STIGs.

4 Remediate

Use the combination of asset criticality assignment and threat intelligence to prioritize the remediation of vulnerabilities that pose the most significant risk to the business and mission-critical applications. Implement automation where possible to proactively patch and configure systems to reduce resource constraints on remediation teams. Automate ticket creation to assign vulnerability triage tasks to remediation teams for action.

5 Monitor

Implement actionable metrics to convey risk to operational and executive teams. These metrics will aid in decisions on allocating resources to tackle risk items and measure program effectiveness.

Unlock the Value of Qualys VMDR to Drive a Risk-Based VM Program

Using a risk-based approach to remediating vulnerabilities is revolutionizing the way organizations traditionally approach vulnerability management with an all-or-nothing strategy of remediation. Prioritizing the remediation of vulnerabilities that are most likely to be exploited on critical systems will greatly improve risk posture and reduce remediation fatigue.

Qualys VMDR with Qualys TruRisk™ helps organizations quantify cyber risk so that they can accurately measure it, take steps to reduce exposure, track risk reduction trends over time, and better measure the effectiveness of their cyber security program. The chart below illustrates at a high level how teams can use VMDR to operationalize their risk-based vulnerability management program against the five pillars of RBVM.

PILLAR	OBJECTIVE	QUALYS VMDR APPROACH
Identify	Inventory Assets and Services Exposed to the Public Internet	Automate attack surface discovery using the Qualys Internet Scanners and Qualys Cybersecurity Asset Management (CSAM) with External Attack Surface Management (EASM)[2] to discover blind spots for internet-connected assets
	Inventory Internal On-Premises Assets	Automate asset discovery with Qualys VMDR by deploying Qualys scanner appliances, agents, passive sensors, and more
	Inventory Public Cloud Workloads	Configure Qualys Cloud connectors to inventory virtual workloads on Public Cloud accounts
Context	Assign Criticality to Assets	Assign criticality to assets using Qualys TruRisk™ or directly import and assign business criticality to assets using Global AsssetView or CSAM from a CMDB such as ServiceNow[3]
Assess	Continuous Vulnerability Scanning	Perform regular vulnerability scanning of the environment using Qualys VMDR. Realtime vulnerability scanning every 4 hours or less with Qualys agents
	System Configuration Auditing and Security Hardening	Perform regular configuration audits using Qualys Secure Configuration Assessment (SCA)
Remediate	Prioritize Vulnerability Remediation	Pinpoint vulnerabilities that pose the most risk to the organization by using Qualys TruRisk™ Qualys Detection Scores on critical assets. Automate remediation using Qualys Patch Management and dispatch tickets to remediation teams with Qualys VMDR for IT Service Management (ITSM) integration[4]
Monitor	Use Metrics to Evaluate Program Efficacy	Monitor asset posture in real time using Qualys dashboards that aggregate risk data with near real-time visibility

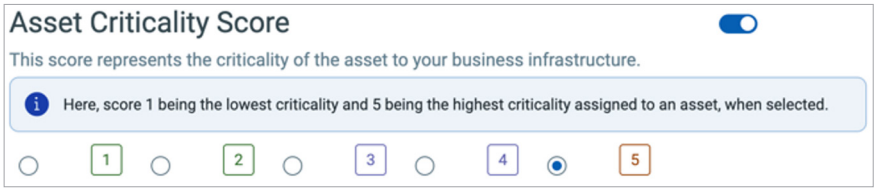
2. Introducing CyberSecurity Asset Management 2.0 with Natively Integrated External Attack Surface Management
3. Implement Risk-Based Vulnerability Management with Qualys TruRisk™: Part 1
4. Close the Gap Between IT & Security with Our New App: Qualys VMDR for ITSM

Automate Asset Discovery with Near Real-Time Visibility

To effectively manage vulnerabilities based on risk, it is crucial to have a complete understanding of the complex and dispersed IT landscape. In addition to utilizing scanner tools, incorporating Qualys Cloud Agents and Qualys Cloud Connectors can provide real-time inventory data. Integrating with solutions such as ServiceNow CMDB and CSAM with EASM can also help identify additional assets and potential areas of vulnerability that may have been overlooked.

Assign Business Context and Criticality to High-Value Assets

Assign an asset criticality score (ACS) of 1-5 to assets to identify high-value assets in risk score calculation. ACS can be assigned dynamically through CMDB sync, asset tagging, or manually to each asset in Global AssetView or CSAM. The maximum asset criticality score is assigned when multiple tags are applied to the same asset.[5]



Use Qualys TruRisk™ to Prioritize and Remediate the Most Critical Threats

Qualys TruRisk™ calculates a total risk score that represents the likelihood of exploitation by using business criticality, CVSS score, threat intelligence, and applied mitigation controls. Arbitrary-based scoring systems only represent the vulnerability metrics of the risk equation without consideration of real-time threat data that is commonly used to decide where the business needs to focus its efforts on trying to lower its risk exposure.

Qualys begins by assessing over 185K known CVEs including those that do not have a registered QID based on external threat and exploit intelligence and assigns it a Qualys Vulnerability Score (QVS).[6]

Each vulnerability registered as a QID in the Qualys knowledge base is assigned a Qualys Detection Score (QDS) ranging from 0-100. The QDS score combines the QVS score with applied mitigation controls for a given vulnerability. In the case where multiple CVEs are assigned to a QID, the highest QVS is selected.[6]

QDS SCORE	SEVERITY	DESCRIPTION
>=90	Critical	CVSS Critical, exploited in the wild, weaponized exploit available, trending on social media, and the dark web
70-89	High	CVSS Critical or High, weaponized exploit available but no evidence of exploitation
40-69	Medium	CVSS High, no exploits available
1-39	Low	CVSS Low, low risk of exploitation

5. Implement Risk-Based Vulnerability Management with Qualys TruRisk™: Part 1
6. In-Depth Look Into Data-Driven Science Behind Qualys TruRisk

The platform uses a weighted average of all identified vulnerabilities identified by QDS on an asset and ACS to compute a score of 0-1000.[6] Organizations can quickly identify assets that are in most critical need of remediation with TruRisk™.

TruRisk SCORE	SEVERITY	DESCRIPTION
850-1000	Critical	Mission-critical assets with multiple critical vulnerabilities
700-849	High	High-value asset with multiple critical or high vulnerabilities or is exposed to the internet
500-699	Medium	Moderate-value assets with critical or high vulnerabilities
0-499	Low	Low-value assets with multiple vulnerabilities

Cybersecurity programs calculate risk by applying the basic risk formula (Risk = Likelihood x Impact) to allow decision-makers to apply limited IT resources effectively.

Risk = Likelihood x Impact

Likelihood is calculated as (Threat x Vulnerabilities). By using Qualys TruRisk™ we can accurately gauge the threat portion of this equation instead of relying only on threat levels using CVSS or Qualys Severity levels alone.

Risk = (Threat x Vulnerabilities) x Impact

The TruRisk™ values that overlay this formula represent risk as an Asset Risk Score (ARS) that equals a weighted vulnerability Qualys Detection Score (QDS) multiplied by the impact that is determined by applying an Asset Criticality Score (ACS) on a given asset.[6] The weighted average of vulnerabilities scales based on the count and severity of vulnerabilities identified on scanned assets.[6]

ARS = QDS (weighted average of vulnerabilities) x ACS

6. In-Depth Look Into Data-Driven Science Behind Qualys TruRisk

Visualize Prioritization and Monitor Trends with Real-Time Dashboards

Qualys VMDR prioritization provides a risk-based view of assets. This customizable view can prioritize based on asset criticality, QDS, and TruRisk™ scores for focused remediation.[7] VMDR reporting now includes QDS, ACS, and ARS values.[8]

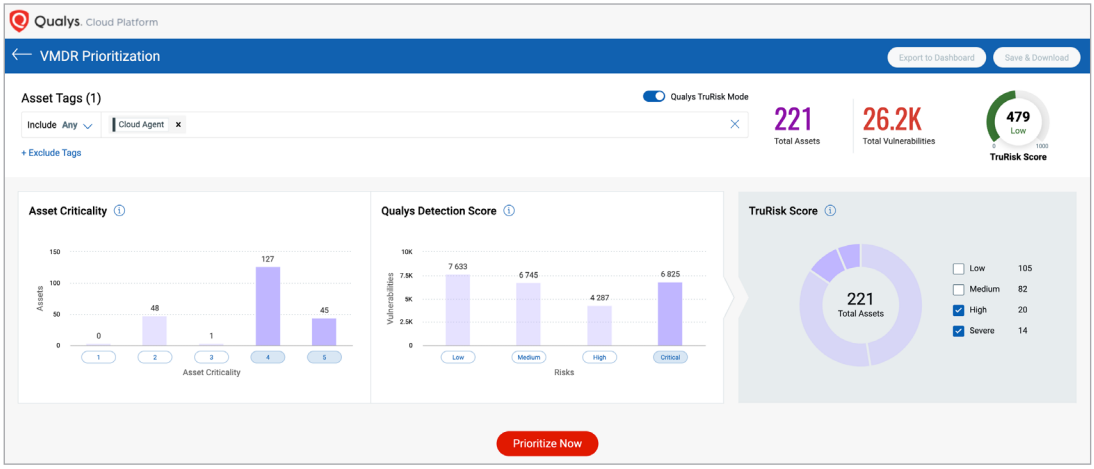


Figure 1 Qualys TruRisk™ Quickly Visualizes Prioritization of Assets for Remediation

Use Qualys Dashboards with prioritization data to review organizational risk posture with near real-time visibility. The dashboards use prioritization data by gathering information from across the Qualys platform captured by the suite of sensors to a single place for visualization. Customize TruRisk™ dashboard widgets with trending enabled to demonstrate risk reduction over time and measure the effectiveness of the vulnerability management program.[7]

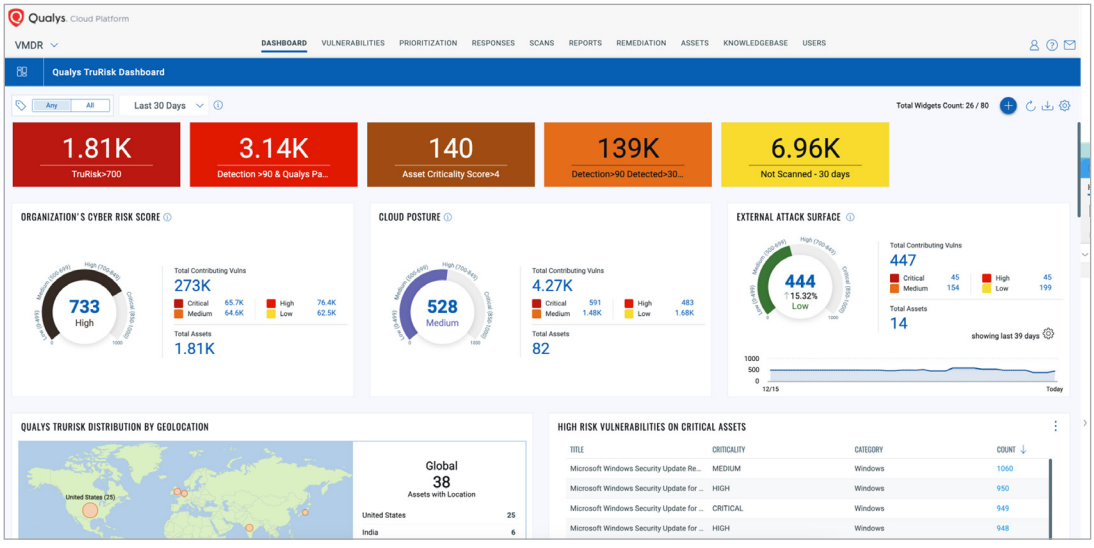


Figure 2 Customize trending Qualys dashboards to monitor and trend risk posture

7. Implement Risk-Based Vulnerability Management with Qualys TruRisk™: Part 3
8. A Deep Dive into VMDR 2.0 with Qualys TruRisk™

Reduce Risk with Automated Vulnerability Remediation

The ad-hoc prioritization report shows vulnerabilities with available patches which can be sent to Qualys Patch Management for individual remediation. Proactive patching can be set up using automated deployments to reduce MTTR for critical assets' newly discovered vulnerabilities.[9]

Examples of automated zero-touch patch policies:

- ✓ External or Internet Facing assets with a vulnerability score (QDS) >= 90
- ✓ High Value Assets with an ACS of 4 or 5 with a vulnerability score (QDS) >= 90
- ✓ Remediate client-side vulnerabilities in browsers (Google Chrome, Firefox) with a score of 90 or higher

Read the following blogs for more information on implementing a risk-based vulnerability management program with VMDR.

References

A Deep Dive into VMDR 2.0 with Qualys TruRisk™

Implement Risk-Based Vulnerability Management with Qualys TruRisk™ : Part 1

Implement Risk-Based Vulnerability Management with Qualys TruRisk™ : Part 2

Implement Risk-Based Vulnerability Management with Qualys TruRisk™: Part 3

In-Depth Look Into Data-Driven Science Behind Qualys TruRisk

Risk-based Remediation Powered by Patch Management in Qualys VMDR 2.0

Introducing CyberSecurity Asset Management 2.0 with Natively Integrated External Attack Surface Management

Close the Gap Between IT & Security with Our New App: Qualys VMDR for ITSM

Framework for Improving Critical Infrastructure Cybersecurity

9. Risk-based Remediation Powered by Patch Management in Qualys VMDR 2.0