



VMDR[®] 2.0 with Qualys TruRisk[™]

Risk-based Vulnerability Management, Detection, and Response

Redefining Cyber Risk Management for the Enterprise

Discover, assess, prioritize, and patch critical vulnerabilities and reduce cybersecurity risk in real time across your global hybrid IT, OT, and IoT landscape — all from a single cloud platform.



VMDR with Built-in Orchestration



Identify the Highest Risk Assets

Qualys TruRisk[™] comprehensively quantifies risk across your attack surface including vulnerabilities, misconfigurations, and digital certificates. Risk is assessed based on business criticality and exploit intelligence from hundreds of sources to proactively measure, track, and communicate risk.



Quickly Remediate Threats at Scale

Rule-based integrations with ITSM tools (ServiceNow, JIRA) automatically assign remediation tickets to vulnerabilities prioritized by risk with dynamic tagging. Remedial actions and orchestration directly from ITSM close vulnerabilities faster and reduce MTTR.



Automate Tasks with No-code Workflows

As part of Qualys Cloud Platform, QFlow technology delivers drag and drop visual no-code workflows to automate a variety of time-consuming and complex vulnerability management tasks.



Receive Preemptive Attack Alerts

Prevent the spread of malware by correlating actively exploited CVEs using malware and external threat indicators. Includes threat intelligence from 180,000+ vulnerabilities and 25+ threat and exploit intelligence sources to identify your organization's unique risks and prevent attacks.

A single solution for risk-based cybersecurity discovery, assessment, detection, and response.

VMDR® 2.0 with Qualys TruRisk™ offers a risk-based vulnerability management solution to prioritize vulnerabilities and assets based on risk and business criticality.

Seamless integration accelerates risk reduction across the enterprise

Qualys VMDR 2.0 seamlessly integrates with configuration management databases (CMDB) and patch management solutions to quickly discover, prioritize, and automatically remediate vulnerabilities at scale to reduce risk. Tight integration with ITSM solutions such as ServiceNow ITSM helps to automate and operationalize vulnerability management across the enterprise.

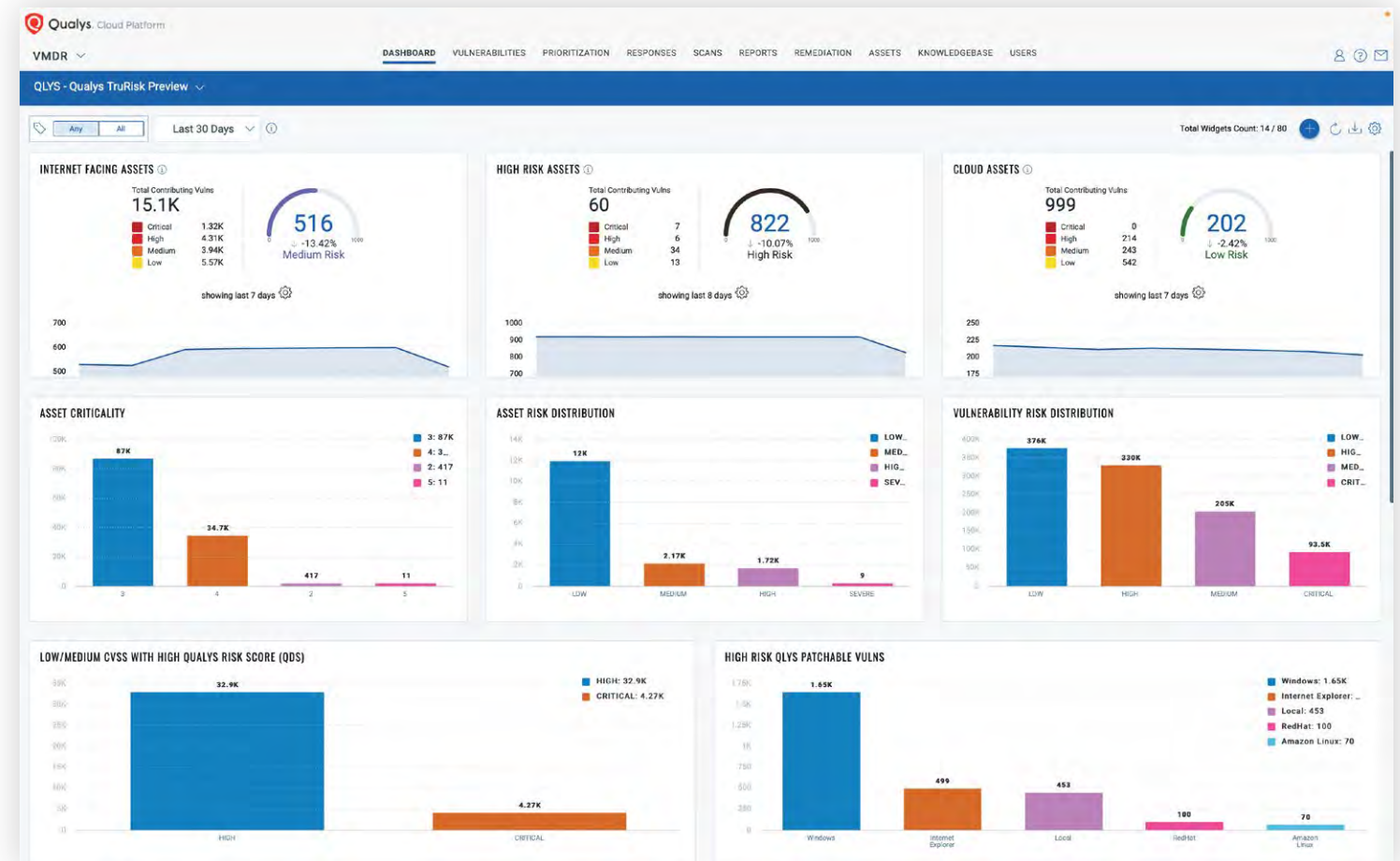
With VMDR 2.0, you get a risk-based vulnerability management solution that prioritizes vulnerabilities, misconfigurations, assets, and groups of assets based on risk, reduces risk by remediating vulnerabilities at scale, and helps organizations measure security program effectiveness by tracking risk reduction over time.

Automates workflows to reduce risks at scale

Qualys VMDR 2.0 is powered by the Qualys Cloud Platform, combining the lightweight Qualys Cloud Agent, virtual scanners, and network analysis (passive scanning) capabilities. It brings together all the key elements of an effective vulnerability management program into a single service unified by powerful no-code orchestration workflows out of the box using QFlow. From asset discovery to risk-based assessment to detection and response, VMDR 2.0 automates the entire process and significantly accelerates an organization's ability to respond to threats, thus preventing possible exploitation.

Pricing

Qualys VMDR 2.0 is priced on a per-asset basis and does not require a software update to start. Sign up for a free trial or request a quote.



Key Benefits

- It's all in the cloud**
No need for bulky appliances. Everything is in the cloud and ready to run.
- Easy to deploy**
Deployment is incredibly simple. With unlimited virtual scanners, you can provision a scanner and be ready to go in no time.
- Includes VM**
VMDR 2.0 with Qualys TruRisk has the same vulnerability management solution capabilities that you have come to know and trust, as well as many other great services.
- Drastically reduces time and money**
Using a single cloud platform and a single agent, organizations save significant resources and time typically required to install multiple agents, multiple consoles, and integrations.

1 ASSET MANAGEMENT
Automated asset identification and categorization
Knowing what's active in a global hybrid IT environment is fundamental to security. VMDR 2.0 enables customers to automatically discover and categorize known and unknown assets, continuously identify unmanaged assets, and create automated workflows to manage them effectively.
After the data is collected, customers can instantly query assets and their attributes to get deep visibility into hardware, system configuration, applications, services, network information, and more.

2 VULNERABILITY MANAGEMENT
Real-time vulnerability and misconfiguration detection
VMDR 2.0 enables customers to automatically detect vulnerabilities and critical misconfigurations per CIS benchmarks in real time. With support for 62,000+ vulnerabilities and comprehensive coverage for CIS benchmarks, organizations can respond to threats faster. VMDR 2.0 with Qualys TruRisk continuously identifies material risks to your IT, including business-critical vulnerabilities and misconfigurations on the industry's widest range of devices, operating systems, and applications.

3 THREAT PRIORITIZATION
Automated risk-based prioritization
VMDR with Qualys TruRisk leverages comprehensive threat and exploit intelligence to automatically assess your true risk based on multiple factors. These include exploit code maturity, active exploitation in the wild, the criticality of the asset, and its location. VMDR provides a risk score so that organizations can quantify risks, track risk reduction over time, and assess the effectiveness of their cybersecurity programs.

4 PATCH MANAGEMENT
Patching and remediation at your fingertips
After prioritizing vulnerabilities by risk, VMDR 2.0's integrated patch management add-on holistically remediates vulnerability risk by applying patches, applying workarounds, and fixing configurations across the environment. No-code visual workflow automation is enabled with QFlow technology. QFlow ensures policy-based, recurring automated jobs keep systems up to date, providing proactive patch management for security and non-security patches. This significantly reduces the vulnerabilities the IT operations team must chase down as part of a remediation cycle.

Confirm and repeat
VMDR 2.0 closes the loop and completes the vulnerability management lifecycle from a single pane of glass that offers real-time customizable dashboards and widgets with built-in trending. Priced on a per-asset basis and delivered in the cloud with no software to update, VMDR 2.0 also drastically reduces your total cost of ownership.

VMDR® 2.0 with Qualys TruRisk™ — An All-in-One Solution

Included
Add on

ASSET MANAGEMENT			
Asset Discovery	Detect and inventory all known and unknown assets that connect to your global hybrid IT environment — including on-premises devices and applications, mobile, endpoints, clouds, containers, OT, and IoT. Includes Qualys Passive Scanning Sensors.	○	
Asset Inventory Get up-to-date real-time inventory for all IT assets	<ul style="list-style-type: none"> • On-premises Device Inventory: Detect all devices and applications connected to the network including servers, databases, workstations, routers, printers, IoT devices, and more. • Certificate Inventory: Detect and catalog all TLS/SSL digital certificates — both internal and external facing — from any Certificate Authority. • Cloud Inventory: Monitor users, instances, networks, storage, databases, and their relationships for a continuous inventory of resources and assets across all public cloud platforms. • Container Inventory: Discover and track container hosts and their information — from build to runtime. • Mobile Device Inventory: Detect and catalog Android, iOS/iPad OS devices across the enterprise, with extensive information about the device, its configurations, and installed apps. 	○	
Asset Categorization and Normalization	Gather detailed information such as asset details, running services, installed software, and more. Eliminate the variations in product and vendor names and categorize them by product families on all assets.	○	
VULNERABILITY MANAGEMENT			
Vulnerability Management	Continuously detect software vulnerabilities using the industry's most comprehensive signature database, across the widest range of asset categories. Qualys is the market leader in VM.	○	
Qualys TruRisk Quantify risk posture	Accurately quantify cybersecurity risk posture across vulnerabilities, assets, and groups of assets — measuring and providing actionable steps that reduce exposure and increase cybersecurity program effectiveness.	○	
QFlow Automate workflow	Automate and orchestrate operational tasks with a no-code visual workflow building environment to rapidly streamline security programs and responses.	○	
Configuration Assessment	Assess, report, and monitor security-related misconfiguration issues based on the Center for Internet Security (CIS) benchmarks.	○	
Certificate Assessment	Assess your digital certificates — both internal and external — and TLS configurations for certificate issues and vulnerabilities.	○	
THREAT DETECTION & PRIORITIZATION			
Continuous Monitoring	Alerts in real time about network irregularities. Identify threats and monitor unexpected network changes before they turn into breaches.	○	
Threat Protection	Pinpoint your most critical threats and prioritize patching. Using real-time threat intelligence and machine learning, take control of evolving threats and identify what to remediate first.	○	
Custom Assessment & Remediation	Proactively detect and rapidly respond to zero-day vulnerabilities, incidents and threats with custom scripting and security controls.		○
RESPONSE			
ITSM Tool Integrations	Rule-based integrations with ITSM tools (ServiceNow, JIRA) automatically assign tickets and enable orchestration of remediation, further reducing MTTR.	○	
Patch Detection	Automatically correlates vulnerabilities and patches for specific hosts, decreasing your remediation response time. Search for CVEs and identify the latest superseding patches.	○	
Patch Management via Qualys Cloud Agent	Rapidly remediate vulnerability risk holistically by applying the right OS, third-party patches, fixing configurations or applying the right mitigations.		○
Patch Management for Mobile Devices	Uninstall or update vulnerable apps, alert users, reset or lock devices, change passcodes, and more.		○
Container Runtime Security	Secure, protect, and monitor running containers in traditional host-based container and Container-as-a-Service environments with granular behavioral policy enforcement.		○
Certificate Renewal	Renew expiring certificates directly through Qualys.		○

VMDR 2.0 also includes UNLIMITED: Qualys Virtual Passive Scanning Sensors (for discovery), Qualys Virtual Scanners, Qualys Cloud Agent, Qualys Container Sensors, and Qualys Virtual Cloud Agent Gateway Sensors for bandwidth optimization.