Qualys

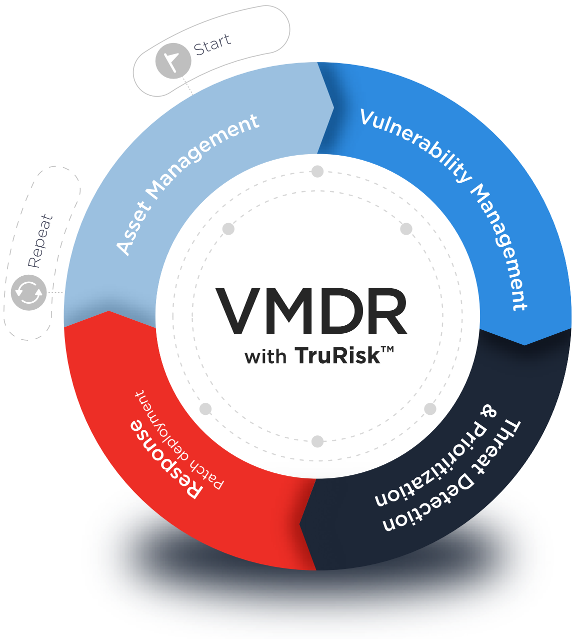
besecure
Managed E-Business Security™

# VMDR® 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 Cloud, IT, OT, and IoT landscape—all from a single platform.



VMDR with Built-in Orchestration

### Prioritize Critical Threats

TruRisk

Qualys TruRisk™ comprehensively quantifies risk across your attack surface, including vulnerabilities, misconfigurations, and digital certificates, reducing critical vulnerabilities by up to 85%.

### Remediate Threats 6x Faster

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.

### Streamline Workflows with No-code Workflows

Flow

Leverage drag-and-drop visual no-code workflows to automate various time-consuming and complex vulnerability management and IT 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.

### Runtime Software Composition Analysis (Runtime SCA)

Enable SCA in Agent Profile with a single click in configuration profile for deep file system scanning, continuous evaluation, and data enrichment in VMDR.

## One solution for risk-based discovery, assessment, detection, and response for custom and third-party applications.

With Custom Assessment and Remediation (CAR), VMDR customers can use and action scripting languages like Python, PowerShell, and many others to enrich the Qualys out-of-the-box signature library with customer-defined logic for nearly any zero-day threat, risk scenario, and home-grown application. When coupled with risk-based prioritization provided by TruRisk, VMDR offers holistic security coverage using a single agent for any application or any network environment.

## Seamless integration with ITSM and CMDB accelerates risk reduction across the enterprise.

Qualys VMDR seamlessly integrates with IT Service Management (ITSM), 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 or Jira helps to automate and operationalize vulnerability management across the enterprise and between IT and Security teams.

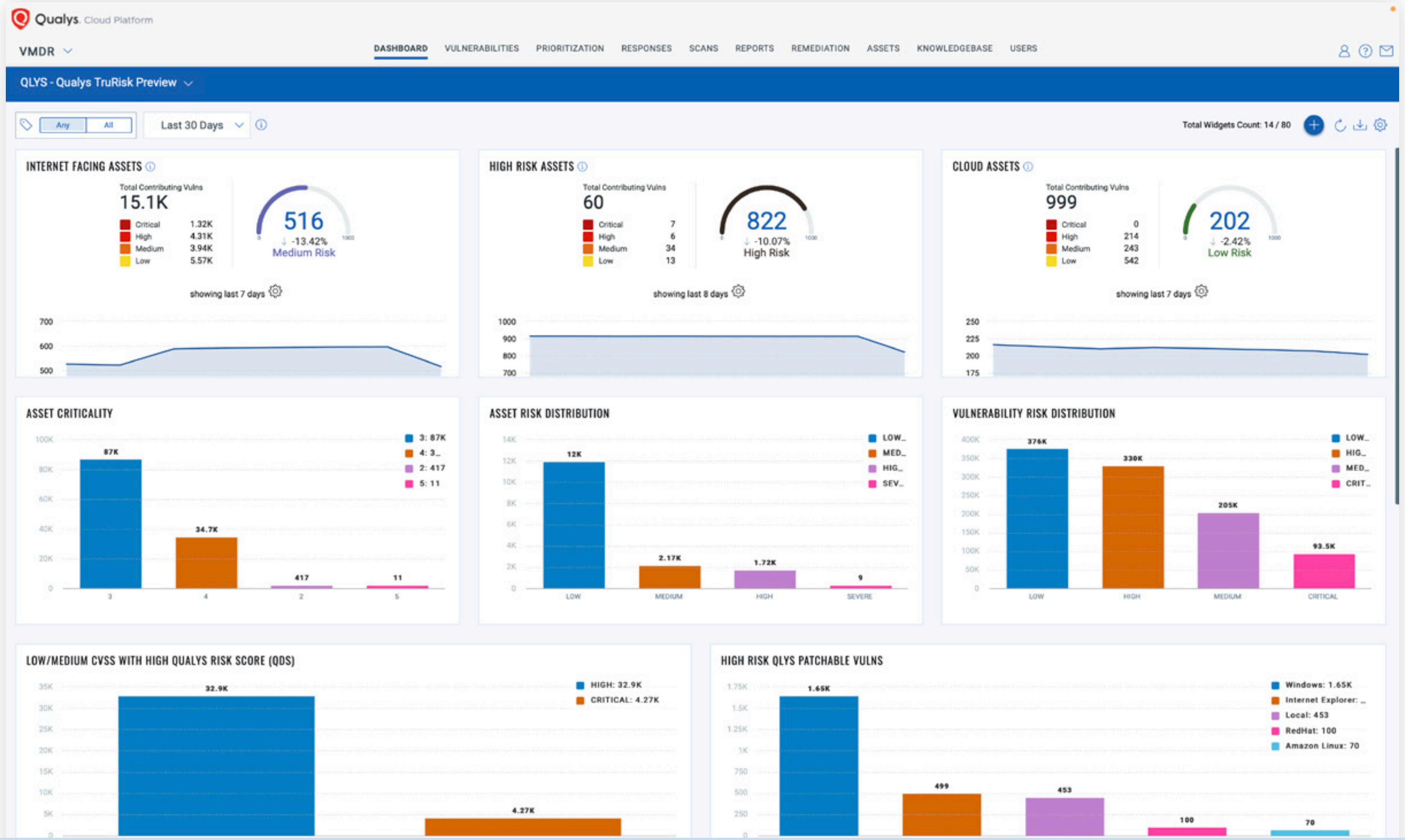
With VMDR, you get a risk-based vulnerability management solution that prioritizes vulnerabilities, misconfigurations, assets, and groups of assets based on risk, reduces risk by remediating vulnerabilities at scale, and helps organizations measure security program effectiveness by tracking risk reduction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

**Automates workflows to reduce risks at scale**

Qualys VMDR is powered by the Qualys TruRisk 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 Qualys Flow. From asset discovery to risk-based assessment to detection and response, VMDR automates the entire process and significantly accelerates an organization's ability to respond to threats, thus preventing possible exploitation.

**Pricing**

Qualys VMDR, as well as security packages VMDR FixIT and ProtectIT, is priced on a per-asset basis and does not require a software update to start.



KEY BENEFITS

### Flexible and Easy to Deploy

No hardware to buy or manage—it's all in the cloud. Get set up in 10 minutes or less with unlimited virtual scanners. You can provision a scanner and be ready to go in no time. For small and mid-sized businesses, VMDR TruRisk FixIT and ProtectIT packages offer enterprise-grade VM, Patch Management and Endpoint Security right-sized for your business.

### More Security with Less Complexity

VMDR offers enterprise-grade vulnerability management with the ability to expand security stack functionality with one single agent. Leverage VMDR FixIT packages to extend remediation and patch vulnerabilities up to 40% faster than other solutions. Automatically block malware and ransomware infections with VMDR ProtectIT.

### Detect Threats with Your Own Logic

By adding Custom Assessment and Remediation (CAR), leverage VMDR to detect, manage, and remediate vulnerabilities in custom-developed, first-party software with your own logic and threat signatures.

1

ASSET MANAGEMENT

### Automated Asset Identification and Categorization

Knowing what's active in a global hybrid IT environment is fundamental to security. VMDR 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 enables customers to automatically detect vulnerabilities and critical misconfigurations per CIS benchmarks in real time. With support for 86K+ vulnerabilities and comprehensive coverage for CIS benchmarks, organizations can respond to threats faster. Qualys VMDR with 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

ADVANCED REMEDIATION

### Custom Remediation Management

After prioritizing vulnerabilities by risk, VMDR's integrated patch management and Custom Assessment and Remediation (CAR) add-ons allows you to secure new attack surfaces with first-party vulnerability detections for custom software by creating your own custom checks to detect open-source risks associated with embedded components and software. With these advancements, you can now use scripting languages like Python, PowerShell, and many others to enrich the Qualys out-of-the-box signature library with customer-defined logic for nearly any zero-day threat, risk scenario, and home-grown application.

### Confirm and Repeat

VMDR 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 also drastically reduces your total cost of ownership.

# VMDR® with Qualys TruRisk™— An All-in-One Risk-based VM 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**<br>Get up-to-date real-time inventory for all IT assets | • On-premises Device Inventory: Detect all devices and applications connected to the network, including servers, databases, workstations, routers, printers, IoT devices, and more.<br>• Certificate Inventory: Detect and catalog all TLS/SSL digital certificates—both internal and external facing—from any Certificate Authority.<br>• Cloud Inventory: Monitor users, instances, networks, storage, databases, and their relationships for a continuous inventory of resources and assets across all public cloud platforms.<br>• Container Inventory: Discover and track container hosts and their information—from build to runtime.<br>• 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**<br>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. | ○ | |
| **Qualys Flow**<br>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. | ○ | |
| **First-party Risk Management with CAR** | Use scripting languages like Python, PowerShell, and many others to enrich the Qualys out-of-the box signature library with customer-defined logic for nearly any zero-day threat, risk scenario, and home-grown application. | | ○ |
| **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 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.