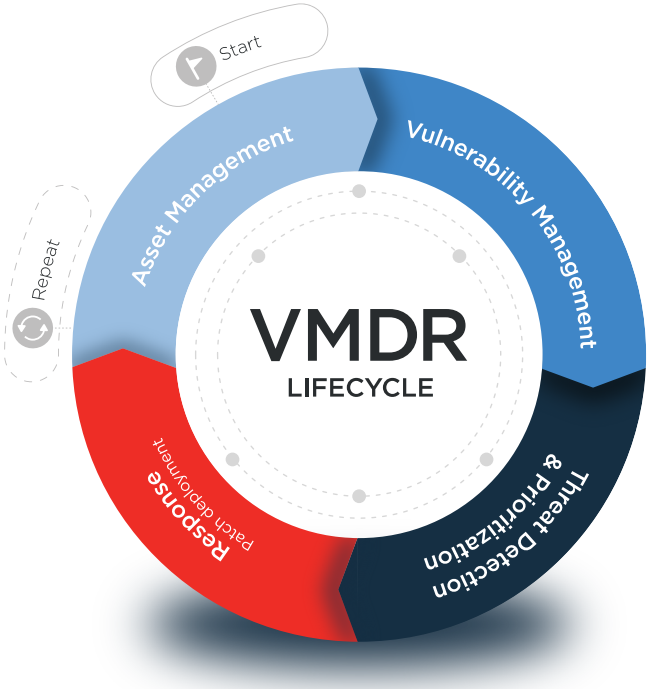
Qualys

Qualys VMDR® — All-in-One Vulnerability Management, Detection, and Response

Bringing the #1 Vulnerability Management solution to the next level

Discover, assess, prioritize, and patch critical vulnerabilities in real time and across your global hybrid-IT landscape — all from a single solution.



VMDR with Built-in Orchestration

Identify all known and unknown assets on your global hybrid-IT

Knowing what's active in a global hybrid-IT environment is fundamental to security. Automatically detect all known and unknown IT assets everywhere for a complete, categorized inventory enriched with details such as vendor lifecycle information and much more.

Analyze vulnerabilities and misconfigurations with six sigma accuracy

Automatically detect vulnerabilities and critical misconfigurations per CIS benchmarks, by asset.

Quickly focus on what's most urgent

Using advanced correlation and machine learning, automatically prioritize the riskiest vulnerabilities on the most critical assets, reducing thousands of vulnerabilities to the few hundred that matter.

Inoculate your assets from the most critical threats

With the push of a button, deploy the most relevant, superseding patch to quickly remediate vulnerabilities and threats across any size environment.

Today's processes involve different teams, using multiple point solutions — significantly adding complexity and time to the critical patching process.

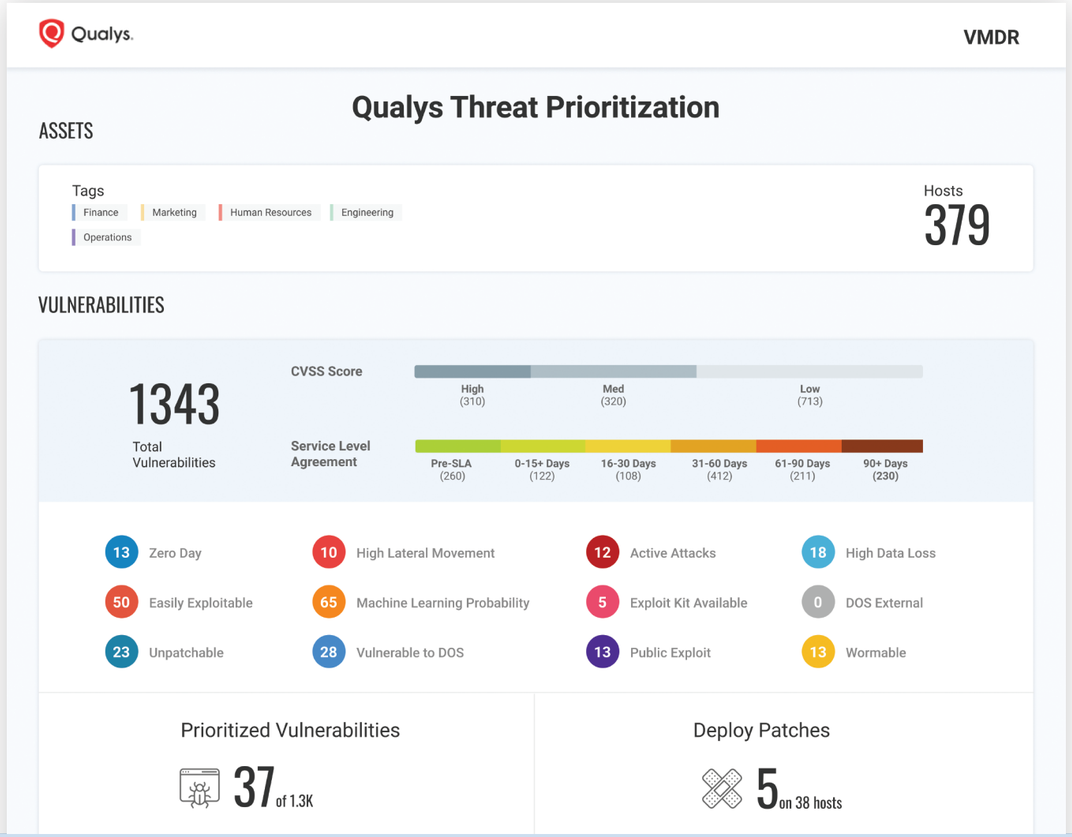
Traditional endpoint solutions don't interface well with each other, creating integration headaches, false positives, and delays. Ultimately, devices are left unidentified, critical assets are misclassified, vulnerabilities are poorly prioritized, and patches don't get fully applied.

A single app for discovery, assessment, detection and response.

The Qualys Cloud Platform, combined with its powerful lightweight Cloud Agents, Virtual Scanners, and Network Analysis (passive scanning) capabilities bring together all four key elements of an effective vulnerability management program into a single app unified by powerful out-of-the-box orchestration workflows. Qualys VMDR® enables organizations to automatically discover every asset in their environment, including unmanaged assets appearing on the network, inventory all hardware and software, and classify and tag critical assets. VMDR continuously asseses these assets for the latest vulnerabilities and applies the latest threat intel analysis to prioritize actively exploitable vulnerabilities. Finally, VMDR automatically detects the latest superseding patch for the vulnerable asset and easily deploys it for remediation.

Built-in Orchestration

By delivering all this in a single app workflow, VMDR automates the entire process and significantly accelerates an organization's ability to respond to threats, thus preventing possible exploitation.



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 spin a scanner up and be ready to go in no time.

Includes VM

VMDR has the same vulnerability management solution that you have come to know and trust, as well as many other great apps.

Drastically reduce time and money

Using a single cloud platform organizations save significant resources and the time required to otherwise 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 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 any 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, broken out by asset. Misconfigurations lead to breaches and compliance failures, creating vulnerabilities on assets without common vulnerabilities and exposures (CVEs). VMDR continuously identifies critical vulnerabilities and misconfigurations on the industry's widest range of devices, operating systems and applications.

3

THREAT PRIORITIZATON

Automated remediation prioritization

VMDR uses real-time threat intelligence and machine learning models to automatically prioritize the riskiest vulnerabilities on the most critical assets. Indicators such as Exploitable, Actively Attacked, and High Lateral Movement bubble up current vulnerabilities that are at risk while machine learning models highlight vulnerabilities most likely to become severe threats, providing multiple levels of prioritization.

4

PATCH MANAGEMENT

Patching and remediation at your fingertips

After prioritizing vulnerabilities by risk, VMDR rapidly remediates targeted vulnerabilities, across any size environment, by deploying the most relevant superseding patch. Additionally, policy-based, automated recurring jobs keep systems up to date, providing proactive patch management for security and non-security patches. This significantly reduces the vulnerabilities the operations team has to chase down as part of a remediation cycle.

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 with no software to update, VMDR drastically reduces your total cost of ownership.

Qualys VMDR® — 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.	• **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 (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/iPadOS devices across the enterprise, with extensive information about the device, its configurations, and installed apps.	○	
Asset Categorization and Normalization	Gather detailed information, such as an asset's details, running services, installed software, and more. Eliminate the variations in product and vendor names and categorize them by product families on all assets.	○	
Enriched Asset Information	Get advanced, in-depth details including, hardware/software lifecycles (EOL/EOS), software license auditing, commercial and open source licenses, and more.		○
CMDB Synchronization	Bi-directionally synchronize asset information between Qualys and the ServiceNow CMDB.		○
VULNERABILITY MANAGEMENT			
Vulnerability Management	Continuously detect software vulnerabilities with the most comprehensive signature database, across the widest range of asset categories. Qualys is the market leader in VM.	○	
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 (internal and external) and TLS configurations for certificate issues and vulnerabilities.	○	
Additional Assessment Add Ons	• **Mobile Device Vulnerability & Misconfiguration Assessment** – Continuously detect device, OS, apps, and network vulnerabilities and monitor critical mobile device configurations. • **Cloud Security Assessment** – Continuously monitor and assess your PaaS/IaaS resources for misconfigurations and non-standard deployments. • **Container Security Assessment** – Scan container images and running containers in your environment for high-severity vulnerabilities, unapproved packages and drive remediation efforts. Includes the ability to scan in the build phase with plug-ins for CI/CD tools and registries.		○
THREAT DETECTION & PRIORITIZATION			
Continuous Monitoring	Alerts you in real time about network irregularities. Identifies threats and monitors 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.	○	
RESPONSE			
Patch Detection	Automatically correlate 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 Agents	Speed up patch deployment by eliminating dependence on third-party patch deployment solutions using Qualys Cloud Agents.		○
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 Agents, Qualys Container Sensors, and Qualys Virtual Cloud Agent Gateway Sensors for bandwidth optimization.