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

The #1 Vulnerability Management solution expands to establish a new, game-changing category

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

- 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.

- Innoculate 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 new approach is required. Introducing

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 assesses 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.

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 assesses 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.

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 vulnerability management**
  VMDR has the same vulnerability management capabilities you know and trust.

- **Drastically reduce time and money**
  A single cloud platform saves organizations save significant resources and the time otherwise required to install multiple agents and consoles, and work on integrations.

**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.
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.

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.

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.

Real-time vulnerability and misconfiguration detection

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.

Patching and remediation at your fingertips

Confirm and repeat

VMDR closes the loop and completes the vulnerability management lifecycle from a single plane 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.

“With VMDR, Qualys integrates highly valued and much-needed asset visibility with vulnerability management so that IT teams can have full visibility of their global IT assets (known and unknown). This provides the ability to identify the exposures of those assets in real time, and to prioritize remediation by combining real-time threat indicators with asset context to remediate with one click and then audit the process.”

Scott Crawford
Research Vice President at 451 Research
VMDR includes a new threat prioritization engine. It correlates multiple real-time threat indicators (RTIs) with new machine learning models that analyze historic trends and current threats, and combine with asset criticality, to accurately pinpoint only the small number of highly potent threats that, once remediated, significantly reduce an organization's risk. Instant workflow that kicks off patching with Qualys Cloud Agents further reduces risk by eliminating the huge gap that traditional, siloed tools insert between detection and patch deployment.

### Screenshot: VMDR Prioritization Report

**ASSETS**

<table>
<thead>
<tr>
<th>Tags</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance, Marketing, Human Resources, Engineering, Operations</td>
<td>379</td>
</tr>
</tbody>
</table>

**VULNERABILITIES**

- Total Vulnerabilities: 1343
- Service Level Agreement
  - Pre-SLA (260)
  - 0-15+ Days (122)
  - 16-30 Days (108)
  - 31-60 Days (412)
  - 61-90 Days (211)
  - 90+ Days (230)

**Prioritized Vulnerabilities**

- 37 of 1.3K
- 2.75% of Total Vulnerabilities

**Deploy Patches**

- 5 on 38 hosts
- On 10% of total Hosts

**QID** | **CVE** | **TITLE** | **PRIORITIZATION SCORE** | **HOSTS** | **Patch**
---|---|---|---|---|---
91534 | CVE-2019-0708 | Microsoft Windows Remote Desktop Services Remote Code Execution... | 10 | 23 | ![Patch](button)
371361 | CVE-2018-15982 | Adobe Security Update for Flash Player (APSB18-42) | 9.8 | 19 | ![Patch](button)
90694 | CVE-2019-0708 | Microsoft Windows Cumulative Security Update of ActiveX Kill Bits (M... | 9.8 | 28 | ![Patch](button)
Screenshot: VMDR Filters

Use highly responsive dynamic filters, powered by the Qualys highly scalable elastic backend, to create powerful visualizations that accurately pinpoint various threats across millions of assets in your global hybrid network. Quickly view your network from different lenses and build powerful, highly customized dashboards.
Qualys VMDR® — See for yourself

Priced on a per-asset basis, VMDR saves on deployment, administration, and software subscription costs with lightweight, easily deployed, and self-updating Cloud Agents and Virtual Scanners.

Request a full trial (unlimited scope) at qualys.com/trial

<table>
<thead>
<tr>
<th>Apps and services</th>
<th>What it does</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASSET MANAGEMENT</strong></td>
<td></td>
</tr>
<tr>
<td>Asset Discovery</td>
<td>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.</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td>Get up-to-date real-time inventory for all IT assets. VMDR includes:</td>
</tr>
<tr>
<td></td>
<td>• On-premises Device Inventory – Detect all devices and applications connected to the network including servers, databases, workstations, routers, printers, IoT devices, and more.</td>
</tr>
<tr>
<td></td>
<td>• Certificate Inventory – Detect and catalog all TLS/SSL digital certificates (internal and external facing) from any Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>• Cloud Inventory – Monitor users, instances, networks, storage, databases and their relationships for a continuous inventory of resources and assets across all public cloud platforms.</td>
</tr>
<tr>
<td></td>
<td>• Container Inventory – Discover and track containers hosts and their information – from build to runtime.</td>
</tr>
<tr>
<td></td>
<td>• Mobile Device Inventory – Detect and catalog every mobile device, with extensive information about the device, its user, its configuration, and its apps.</td>
</tr>
<tr>
<td>Asset Categorization and Normalization</td>
<td>Gather detailed information, such as an assets’ details, running services, installed software, and more. Eliminate the variations in product and vendor names and categorize them by product families on all assets.</td>
</tr>
<tr>
<td>Enriched Asset Information</td>
<td>Get advanced in-depth details including, hardware/software lifecycles (EOL/EOS), software license auditing, commercial and open sources licenses, and more.</td>
</tr>
<tr>
<td>CMDB Synchronization</td>
<td>Bi-directionally synchronize asset information between Qualys and the ServiceNow CMDB.</td>
</tr>
<tr>
<td><strong>VULNERABILITY MANAGEMENT</strong></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Continuously detect software vulnerabilities with the most comprehensive signature database, across the widest range of asset categories. Qualys is the market leader in VM. Includes unlimited Qualys Virtual Scanners and Cloud Agents</td>
</tr>
<tr>
<td>Configuration Assessment</td>
<td>Assess, report and monitor security-related misconfiguration issues based on the Center for Internet Security (CIS) benchmarks.</td>
</tr>
<tr>
<td>Additional Assessment Add Ons</td>
<td>• Certificate Assessment – Detect and catalog every TLS/SSL digital certificates (internal and external facing) from any Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>• Cloud Security Assessment – Continuously monitor and assess your PaaS/IaaS resources for misconfigurations and non-standard deployments.</td>
</tr>
<tr>
<td></td>
<td>• Container Security Assessment – Scan images in your environment for high-severity vulnerabilities, unapproved packages and older or test release tags, and assess their impact. Includes plug-ins for CI/CD tools such as Jenkins, and others.</td>
</tr>
<tr>
<td><strong>THREAT DETECTION &amp; PRIORITIZATION</strong></td>
<td></td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td>Alerts you in real time about network irregularities. Identifies threats and monitors unexpected network changes before they turn into breaches.</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>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.</td>
</tr>
<tr>
<td><strong>RESPONSE</strong></td>
<td></td>
</tr>
<tr>
<td>Patch Detection</td>
<td>Automatically correlate vulnerabilities and patches for specific hosts, decreasing your remediation response time. Search for CVEs and identify the latest superseding patches.</td>
</tr>
<tr>
<td>Patch Management via Third-Party Vendors</td>
<td>Integrates with your existing patch deployment solutions, like SCCM and other third-party solutions, to significantly reduce patch time.</td>
</tr>
<tr>
<td>Patch Management via Qualys Cloud Agents</td>
<td>Speed up patch deployment by eliminating dependence on third-party patch deployment solutions by using Qualys Cloud Agents.</td>
</tr>
<tr>
<td>Container Runtime Protection</td>
<td>Protect and secure running containers for policy enforcement. (Available Q1 2020 Beta)</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Remotely monitor, manage and secure mobile devices. (Available Q2 2020 Beta)</td>
</tr>
</tbody>
</table>

**QUALYS SENSORS WITH UNPRECEDENTED SCALABILITY**

VMDR 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.

**OTHER INTEGRATED QUALYS CLOUD APP ADD ONS**


For more information about these apps, visit qualys.com/apps