Qualys.

Better Together: Consolidate PCI and Vulnerability Management Needs with Qualys VMDR

Continuously monitor and secure your entire digital landscape—from internet-facing to internal assets and web applications—to ensure PCI compliance and reduce cyber risk.

The Challenge

For any business that relies on digital payments and payment card storage, compliance with the Payment Card Industry Data Security Standard (PCI DSS) has evolved over the years to adapt to the ever-changing threat landscape. PCI 4.0, the latest iteration of these standards, is yet another crucial milestone that significantly enhances the security and compliance measures for companies that store payment card data. However, while PCI 4.0 does represent an advancement in payment security, it is also can be a challenge for organizations to maintain and modernize their compliance posture in a way the compliments and works in unison with their vulnerability management program.

The Solution

With Vulnerability Management Detection and Response (VMDR), Qualys is helping customers gain the edge in their compliance journey by unifying a Risk-Based Vulnerability Management (RBVM) approach with PCI 4.0 compliance management and reporting, in a single platform. With Qualys VMDR, businesses of any size now can manage and perform timely vulnerability remediation wherever they may reside on the network, directly in-step with PCI 4.0 requirements.

When it comes to Vulnerability Management, accepting less than complete PCI support is no longer required. With Qualys VMDR, you get both.

VMDR and PCI Capabilities and Benefits:

PCI Compliance

PCI ASV scanning is included as a standard feature at no extra cost linked to the VMDR platform. Expand the PCI program to include internal PCI network scanning with pass/fail reporting.

Low TCO and Easy to Use

No hardware to buy or manage. Easy to deploy. Software auto updates. Get setup in 10 minutes or less. **Starts at $2,195**

VMDR and PCI Capabilities and Benefits:

Consolidate Cyber Security Tooling

Consolidate external scanning, web application scanning, patch management, file integrity monitoring, cloud security posture management and more with one unified Qualys TruRisk platform.

Asset Discovery

Automatically discover every asset in the organization including public cloud workloads, assets exposed to the internet, mobile devices, containers, OT, IOT, and unmanaged devices that are connected to the network. Inventory all hardware and software then classify and tag all business-critical assets.

Risk-Based Prioritization

TruRisk

Quantify risk by leveraging over 25 sources of real-time threat intelligence and machine learning to measure the likelihood of vulnerability exploitation. Prioritize remediation on vulnerabilities that will reduce exposure to the organization.

CIS System Hardening

Analyze, measure, and monitor for misconfiguration issues based on the Center of Information Security (CIS) benchmarks.

Certificate Management

Detect and catalog all TLS/SSL certificates for internet facing and internal network assets. Assess certificates and TLS server configurations for certificate issues and vulnerabilities. Renew expiring certificates directly through Qualys.

Automated Workflows

Flow

Auto-remediate specific issues and even quarantine assets using Qualys Flow (QFlow) with flexible, no-code rules.

Continuous Monitoring

Monitor and respond to unexpected network changes with real time alerting.

Asset Inventory

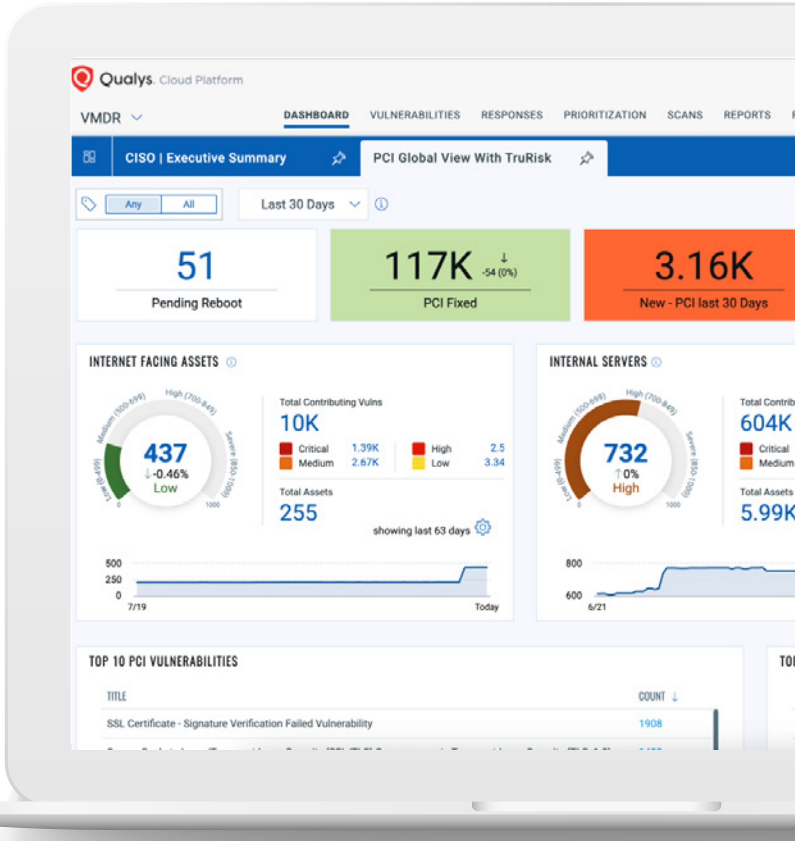
Build and automatically maintain an up-to-date inventory in real time for all IT assets on the local network, public cloud, and mobile devices.

Vulnerability Detection

Discover and identify critical vulnerabilities and reduce cybersecurity risk in real time and across your internal, external, cloud, hybrid IT, OT, and IoT landscape.

Patch Detection

Automatically correlate vulnerabilities and patches to decrease remediation time.



TITLE	COUNT ↓
SSL Certificate - Signature Verification Failed Vulnerability	1908

Key Use Cases for Qualys VMDR

USE CASE CHALLENGE	SOLUTION	OUTCOMES
Continuous Cardholder Data Environment Monitoring PCI-DSS requires organizations to scan in scope networks once every 90 days. Scans that result in high-risk vulnerabilities will need to be mitigated and fixed which could risk a compliant merchant status. A non-compliant merchant status would be considered legally vulnerable if a customer card data is accessed during a breach.	Qualys VMDR continuously scans your infrastructure for vulnerabilities, prioritizes them based on risk of exploitation, and offers guidance to mitigate risk effectively	Continuous vulnerability scanning will significantly increase the likelihood of a passing ASV scan and decrease the cyber risk associated with business-critical applications.
Vulnerability Management Assets and applications are exposed to a rising number of vulnerabilities and targeted malware that can infect various areas of the network. 80% of vulnerabilities can be exploited without needing special privileges.	Qualys VMDR performs continuous and robust vulnerability assessments on all assets. Hardware, software, and firmware-based vulnerabilities impacting all applications are covered using numerous sensors and the Qualys optional cloud agent.	Provides continuous protection for all internal, cloud, and mobile assets across the organization. Manage vulnerabilities on endpoints to reduce risk posed cyber threats.
Certificate Management Using weak or expiring digital certificates on customer facing web sites poses a risk to securing a private transaction and eroding trust with customers.	Qualys Certificate Assessment analyzes a TLS server and the certificates and generates a grade to reflect the strength of the strength of the secure server configuration. Certificates are analyzed and correlated with the Qualys vulnerability detection engine to quickly identify issues with expiration or weak algorithms to prioritize for remediation.	Proactive resolution of TLS services and certificate issues is ensured prior to any potential risk to customer data, delivering a secure solution. Additionally, certificates are consistently renewed and updated, preventing browser warnings caused by expired or weak certificates.

Learn more about VMDR and PCI Compliance. **Contact your Qualys representative to get started with a risk-free trial.**