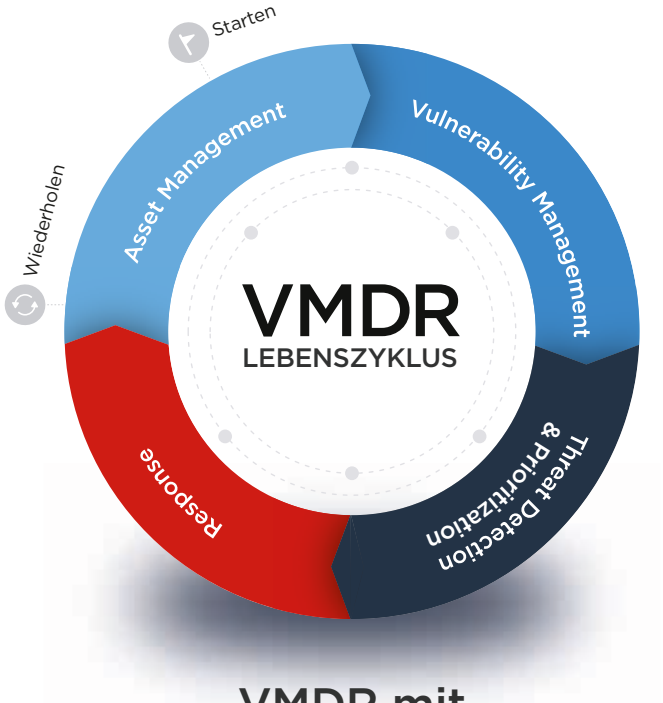
Qualys VMDR®: Die All-in-One-Lösung für Schwachstellenmanagement, Erkennung und Reaktion

Hebt die Schwachstellenmanagement-Lösung Nr. 1 auf die nächste Stufe

Entdecken, bewerten, priorisieren und patchen Sie in Echtzeit kritische Sicherheitslücken in Ihrer gesamten hybriden IT-Landschaft – alles mit einer einzigen Lösung.



VMDR mit integrierter Orchestrierung

Ermittlung aller bekannten und unbekannten Assets in Ihrer hybriden IT

Zu wissen, welche Assets in einer globalen, hybriden IT-Umgebung aktiv sind, ist eine grundlegende Voraussetzung für Sicherheit. VMDR erkennt automatisch alle bekannten und unbekannten IT-Assets in allen Umgebungen und liefert ein komplettes, nach Kategorien strukturiertes Inventar mit wichtigen Details, z. B. Lifecyle-Informationen der Anbieter und vieles mehr.

Analyse der Schwachstellen und Fehlkonfigurationen mit Six-Sigma-Genauigkeit

VMDR erkennt automatisch Schwachstellen und kritische Fehlkonfigurationen gemäß den CIS-Benchmarks, aufgeschlüsselt nach Assets.

Schneller Fokus auf die dringlichsten Probleme

Durch erweiterte Korrelationen und maschinelles Lernen werden automatisch die riskantesten Schwachstellen bei den kritischsten Assets priorisiert. So werden Tausende von Schwachstellen auf die wenigen hundert reduziert, die wirklich gefährlich sind.

Entschärfen der kritischsten Bedrohungen

Unabhängig von der Größe Ihrer IT-Umgebung ist: Sie können per Mausklick die wichtigsten Patches verteilen, um Schwachstellen und Bedrohungen schnell zu beheben.

An den heutigen Prozessen sind verschiedene Teams beteiligt, die zahlreiche Speziallösungen nutzen. Das erhöht die Komplexität und den Zeitaufwand beim Patchen erheblich.

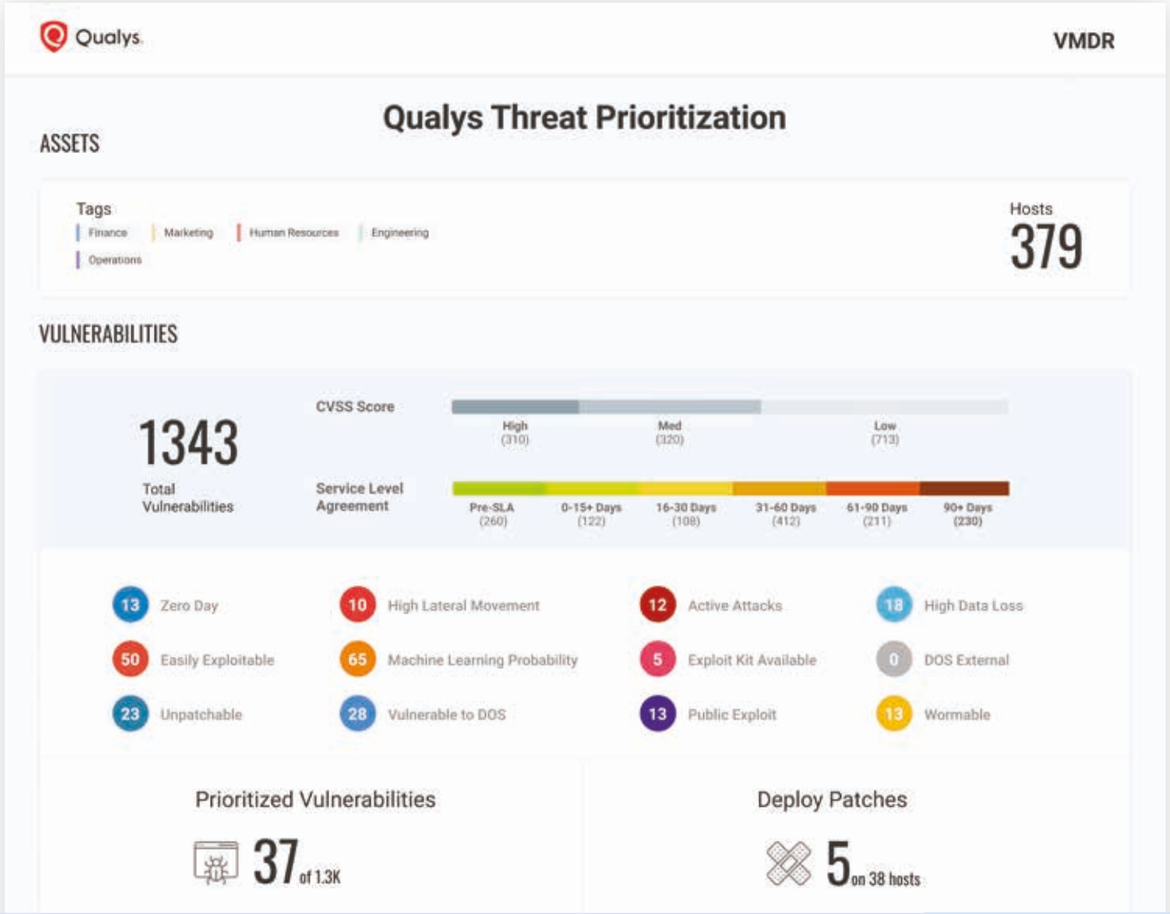
Herkömmliche Endpointlösungen kommunizieren nicht gut miteinander. Das führt zu Integrationsproblemen, Fehlalarmen und Verzögerungen. Geräte bleiben unerkannt, kritische Assets werden falsch klassifiziert, Schwachstellen schlecht priorisiert und Patches nicht vollständig angewandt.

Eine einzige Anwendung für die Erkennung, Analyse, Ermittlung und Reaktion.

Die Qualys Cloud-Plattform – kombiniert mit ihren leistungsstarken, schlanken Cloud-Agenten, virtuellen Scannern und Netzwerkanalysen (passives Scannen) – vereint alle vier Schlüsselelemente eines effektiven Schwachstellenmanagements in einer einzigen Anwendung. Dafür sorgen leistungsfähige, sofort verfügbare Orchestrierungs-Workflows. Qualys VMDR® erkennt automatisch alle Assets in Ihrer Umgebung – einschließlich nicht verwalteter Assets, die sich mit dem Netzwerk verbinden –, inventarisiert die gesamte Hardware und Software und klassifiziert und markiert kritische Assets. VMDR analysiert diese Assets kontinuierlich auf die neuesten Schwachstellen und wendet aktuelle Threat Intelligence-Analysen an, um aktiv ausnutzbare Schwachstellen zu priorisieren. Und schließlich ermittelt VMDR automatisch den jeweils aktuellsten Patch und stellt ihn problemlos bereit, um die Schwachstellen zu schließen.

Integrierte Orchestrierung

VMDR vereint all diese Aktionen in einem einzigen Anwendungs-Workflow und automatisiert den gesamten Prozess. So können Sie schneller auf Bedrohungen reagieren und verhindern, dass Schwachstellen ausgenutzt werden.



Die wichtigsten Vorteile

Alles in der Cloud

Keine sperrigen Appliances. Alles läuft in der Cloud und ist sofort einsatzbereit.

Einfache Bereitstellung

Die Bereitstellung ist außerordentlich einfach. Die virtuellen Scanner stehen in unbegrenzter Zahl zur Verfügung und können jederzeit sofort gestartet werden.

Mit Qualys VM

VMDR umfasst die bewährte Schwachstellenmanagement-Lösung Qualys VM, die Sie bereits kennen, sowie viele andere wertvolle Anwendungen.

Erheblich geringerer Zeit- und Kostenaufwand

Mit einer einzigen, integrierten Cloud-Plattform sparen Unternehmen erhebliche Mittel und die Zeit zur Implementierung zahlreicher Agenten, Konsolen und Integrationen.

1

ASSET MANAGEMENT

Automatische Identifizierung und Kategorisierung von Assets

Zu wissen, welche Assets in einer globalen, hybriden IT-Umgebung aktiv sind, ist eine grundlegende Voraussetzung für Sicherheit. Mit VMDR können die Kunden bekannte und unbekannte Assets automatisch erkennen und kategorisieren, unverwaltete Assets laufend identifizieren und automatisierte Workflows erstellen, um sie effektiv zu verwalten.

Sobald die Daten erfasst sind, können die Kunden die Assets und beliebige andere Attribute sofort abfragen, um tiefe Einsicht in die Hardware, Systemkonfigurationen, Anwendungen, Dienste, Netzwerkinformationen und mehr zu erhalten.

2

VULNERABILITY MANAGEMENT

Echtzeit-Erkennung von Schwachstellen und Fehlkonfigurationen

Mit VMDR können die Kunden automatisch Schwachstellen und kritische Fehlkonfigurationen gemäß den CIS-Benchmarks erkennen, aufgeschlüsselt nach Assets. Fehlkonfigurationen führen zu Sicherheitsverletzungen und Compliance-Verstößen und schaffen dadurch Sicherheitslücken ohne CVEs (Common Vulnerabilites and Exposures). VMDR ermittelt kontinuierlich kritische Schwachstellen und Fehlkonfigurationen beim branchenweit größten Spektrum von Geräten, Betriebssystemen und Anwendungen.

3

THREAT PRIORITIZATON

Automatisierte Priorisierung der Abhilfemaßnahmen

VMDR nutzt Echtzeit-Bedrohungsinformationen und Machine-Learning-Modelle, um automatisch die riskantesten Schwachstellen auf den wichtigsten Assets zu priorisieren. Aktuell gefährdete Schwachstellen werden anhand von Indikatoren wie „ausnutzbar“, „aktiv angegriffen“ und „starke laterale Bewegung“ bewertet, während Machine-Learning-Modelle diejenigen Schwachstellen hervorheben, die am ehesten zu einer gravierenden Bedrohung werden können. Dies schafft mehrere Priorisierungsebenen.

4

PATCH-MANAGEMENT

Schnelles Patchen, proaktives Patch-Management

Korreliert automatisch Schwachstellen und Patches für bestimmte Hosts und verkürzt damit Zeit zur Problembehebung. Sie können nach CVEs suchen und die aktuellsten Patches für sie finden.

Darüber hinaus bietet VMDR proaktives Patch-Management für sicherheits- und nicht sicherheitsrelevante Patches: Richtlinienbasierte, automatisierte, wiederkehrende Jobs halten die Systeme auf dem neuesten Stand. Dies reduziert deutlich die Schwachstellen, die das Betriebsteam im Rahmen eines Reparaturzyklus aufspüren muss.

Bestätigen und wiederholen

VMDR schließt den Lebenszyklus des Schwachstellenmanagements über eine einzige Konsole, die in Echtzeit anpassbare Dashboards und Widgets mit integrierter Trendfunktion bietet. Da sich der Preis nach der Anzahl der Assets richtet und der Kunde keine Software aktualisieren muss, senkt VMDR die Gesamtbetriebskosten drastisch.

Qualys VMDR® auf einen Blick

Anwendungen und Dienste	Leistungsmerkmale	Inklusive	Add-on
ASSET-MANAGEMENT			
Asset Discovery	Erkennt und inventarisiert alle bekannten und unbekannten Assets, die sich mit Ihrer globalen, hybriden IT-Umgebung verbinden – einschließlich lokaler Geräte und Anwendungen, mobiler Geräte, Endpoints, Cloud-Umgebungen, Containern, OT und IoT. Nutzt Qualys Passive-Scan-Sensoren.	○	
Asset Inventory Inventarisiert kontinuierlich sämtliche IT-Assets in Echtzeit.	• **Inventarisierung aller lokalen Geräte** – Erkennung aller mit dem Netzwerk verbundenen Geräte und Anwendungen, einschließlich Servern, Datenbanken, Workstations, Routern, Druckern, IoT-Geräten und mehr. • **Zertifikatsbestände** – Erkennung und Katalogisierung aller digitalen TLS/SSL-Zertifikate (interne und externe) von jeder Zertifizierungsstelle. • **Cloud-Inventarisierung** – Überwachung der Benutzer, Instanzen, Netzwerke, Speicher, Datenbanken und ihrer Verbindungen. So erhalten Sie ein laufend aktualisiertes Inventar aller Ressourcen und Assets auf sämtlichen Public-Cloud-Plattformen. • **Container-Inventarisierung** – Erkennung und Nachverfolgung von Container-Hosts und der zugehörigen Informationen – vom Build bis zur Runtime. • **Inventarisierung aller mobilen Geräte** – Erkennung und Katalogisierung aller mobilen Geräte mit ausführlichen Informationen zu jedem Gerät, seinem Benutzer, der Konfiguration und den Apps.	○	
Asset Categorization and Normalization	Erfasst detaillierte Informationen – z. B. Details zu einem Asset, laufende Dienste, installierte Software und mehr. Vereinheitlicht Produkt- und Anbieternamen und kategorisiert sie nach Produktfamilien auf allen Assets.	○	
Enriched Asset Information	Detaillierte Systeminformationen, einschließlich Hardware-/Software-Lebenszyklen (EOL/EOS), Prüfung der Softwarelizenzen, kommerzielle und Open-Source-Lizenzen und mehr.		○
CMDB Synchronization	Bi-direktionale Synchronisierung der Asset-Informationen zwischen Qualys und der ServiceNow CMDB.		○
SCHWACHSTELLENMANAGEMENT			
Vulnerability Management	Kontinuierliche Software-Schwachstellen-Erkennung: mit der branchenweit umfassendsten Signaturdatenbank und beim breitesten Spektrum von Asset-Kategorien. Qualys ist der Marktführer für Schwachstellenmanagement.	○	
Configuration Assessment	Bewertet, meldet und überwacht sicherheitsrelevante Fehlkonfigurationen, basierend auf den Benchmarks des Centers for Internet Security (CIS).	○	
Additional Assessment Add Ons	• **Certificate Assessment** – Prüft Ihre digitalen Zertifikate (interne und externe) und TLS-Konfigurationen auf Zertifikatsprobleme und Schwachstellen. • **Cloud security Assessment** – Überwacht und bewertet Ihre PaaS/IaaS-Ressourcen kontinuierlich auf Fehlkonfigurationen und nicht standardgemäße Implementierungen. • **Container Security Assessment** – Scannt die Images in Ihrer Umgebung auf gravierende Schwachstellen, nicht genehmigte Pakete sowie Tags von älteren oder Test-Releases und bewertet die Auswirkungen. Umfasst Plug-Ins für CI/CD-Tools wie Jenkins und andere.		○
ERKENNUNG UND PRIORISIERUNG VON BEDROHUNGEN			
Continuous Monitoring	Alarmiert Sie in Echtzeit bei Unregelmäßigkeiten im Netzwerk. Ermittelt Bedrohungen und überwacht das Netzwerk auf unerwartete Änderungen, bevor sie Schaden anrichten können.	○	
Threat Protection	Ermittelt Ihre gravierendsten Bedrohungen und priorisiert die Patches. Echtzeitinformationen über Bedrohungen und maschinelles Lernen helfen Ihnen, aufkommende Bedrohungen in Schach zu halten und festzustellen, welche vorrangig beseitigt werden müssen.	○	
REAKTION			
Patch Detection	Korreliert automatisch Schwachstellen und Patches für bestimmte Hosts und verkürzt damit Zeit zur Problembehebung. Sie können nach CVEs suchen und die aktuellsten Patches für sie finden.	○	
Patch Management via Third-Party Vendors	Integriert sich in Ihre vorhandenen Lösungen zur Bereitstellung von Patches, wie etwa SCCM und andere Drittanbieter-Lösungen. Dies reduziert den Zeitaufwand beim Patchen erheblich.		○
Patch Management via Qualys Cloud Agents	Die Qualys Cloud-Agenten machen Sie unabhängig von Drittanbieter-Lösungen zur Patch-Verteilung und beschleunigen dadurch das Verfahren.		○
Container Runtime Protection	Schutz und Absicherung laufender Container, um Richtlinien durchzusetzen. (Verfügbar im Q1 2020, Beta)		○
Mobile Device Management	Überwachung, Verwaltung und Schutz mobiler Geräte aus der Ferne. (Verfügbar im Q2 2020, Beta)		○
QUALYS-SENSOREN – UNERREICHT SKALIERBAR			
VMDR umfasst folgende Qualys-Sensoren IN UNBEGRENZTER ZAHL: virtuelle passive Scan-Sensoren (zur Erkennung), virtuelle Scanner, Cloud-Agenten, Container-Sensoren sowie virtuelle Cloud-Agent Gateway-Sensoren zur Bandbreitenoptimierung.		○	