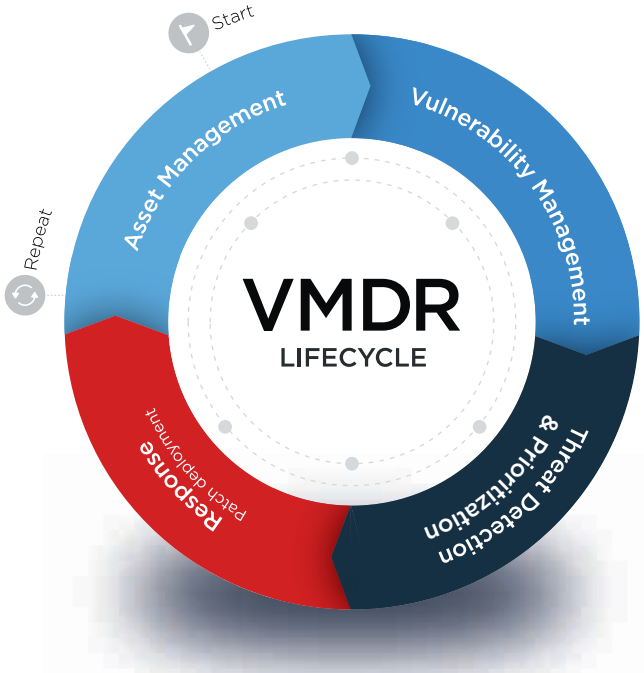
Qualys VMDR® — Soluzione completa di gestione, rilevamento e neutralizzazione delle vulnerabilità

La soluzione numero 1 di gestione delle vulnerabilità si è migliorata di nuovo

Individuazione, valutazione, classificazione per gravità e neutralizzazione delle vulnerabilità critiche in tempo reale nell'intero ambiente IT ibrido globale con una sola soluzione.



VMDR with Built-in Orchestration

Identifica tutte le risorse conosciute e sconosciute nel tuo ambiente IT ibrido globale

Sapere cosa sia attivo in un ambiente IT ibrido globale è essenziale per la sicurezza. Rileva automaticamente tutte le risorse IT conosciute e sconosciute del tuo ambiente per creare un inventario completo suddiviso per categorie e arricchito di dettagli come ciclo di vita del fornitore e molto altro.

Analizza le vulnerabilità e gli errori di configurazione con precisione six sigma

Rileva automaticamente le vulnerabilità e gli errori di configurazione critici di ogni risorsa in base ai benchmark CIS.

Concentra gli sforzi sulle questioni più urgenti

Usando correlazioni avanzate e il machine learning, è possibile individuare automaticamente le vulnerabilità più rischiose presenti sulle risorse più critiche scovando tra le migliaia rilevate le poche centinaia che davvero contano.

Metti al riparo le tue risorse dalle minacce più pericolose

Con un semplice pulsante puoi distribuire la patch più indicata per eliminare velocemente le vulnerabilità e le minacce da qualsiasi ambiente, a prescindere dalle sue dimensioni.

I processi odierni vedono il coinvolgimento di vari team che usano diverse soluzioni puntuali, situazione che comporta un aumento della complessità e del tempo richiesto dai processi di applicazione delle patch critiche.

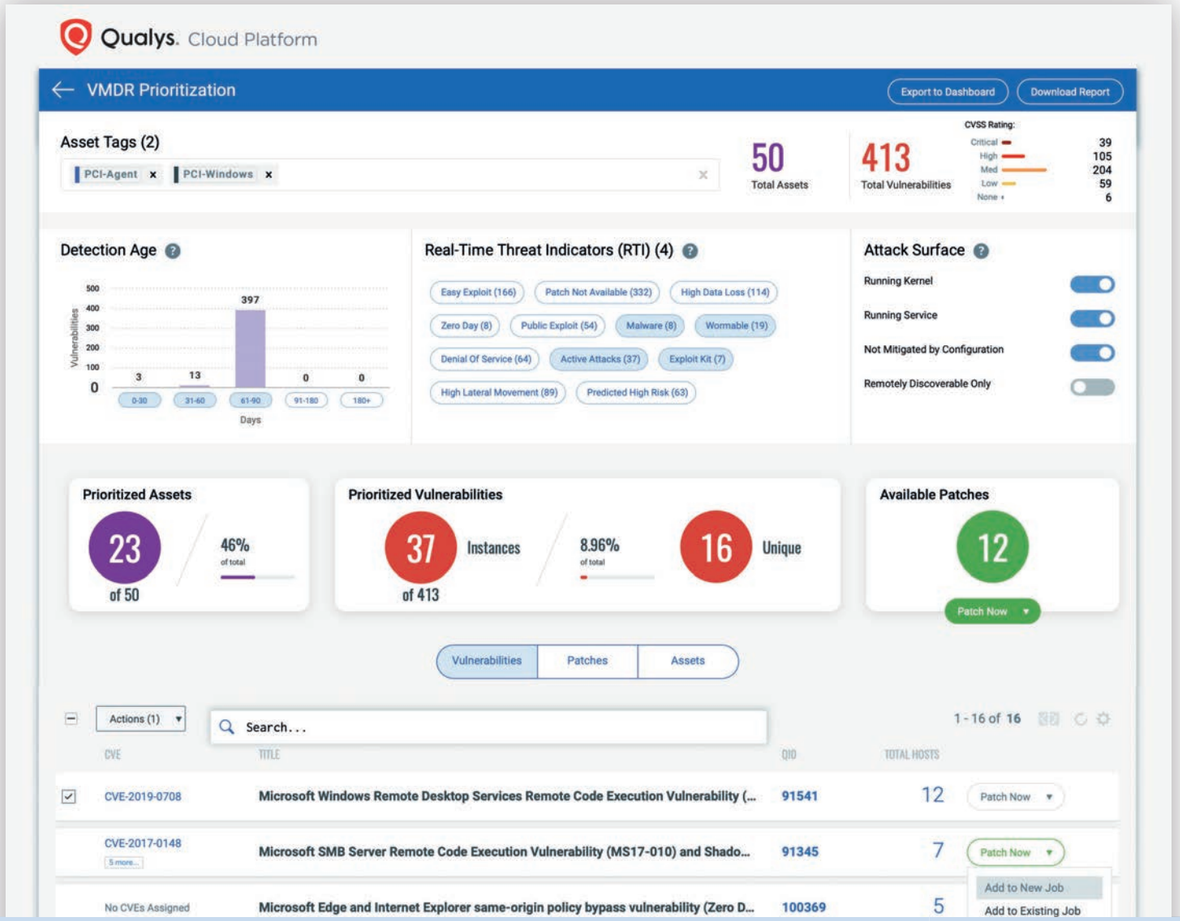
Le tradizionali soluzioni per gli endpoint non interagiscono efficacemente tra loro e causano problemi di integrazione, falsi positivi e ritardi. Il risultato? Nell'ambiente permangono dispositivi sconosciuti, risorse critiche vengono classificate erroneamente, la gravità delle vulnerabilità non viene valutata correttamente e le patch non vengono applicate organicamente.

Un'unica app per il rilevamento, la valutazione, l'individuazione e la neutralizzazione delle vulnerabilità.

Qualys Cloud Platform, associata a potenti agenti cloud leggeri, scanner virtuali e funzionalità di analisi di rete per la scansione passiva, riunisce i quattro elementi chiave che rendono efficace un programma di gestione delle vulnerabilità in un'unica app potenziata da avanzati flussi di orchestrazione pronti all'uso. Qualys VMDR® consente alle aziende di individuare automaticamente ogni risorsa presente nel proprio ambiente, compresi i dispositivi non gestiti che appaiono in rete, di compilare un inventario di tutti i componenti hardware e software e di classificare e contrassegnare le risorse critiche. VMDR tiene ininterrottamente sotto controllo queste risorse alla ricerca di anomalie e applica i servizi di raccolta e analisi delle minacce più all'avanguardia per assegnare una priorità maggiore alle vulnerabilità che possono essere sfruttate attivamente. Per finire, VMDR rileva automaticamente la patch più recente richiesta dalla risorsa vulnerabile e la implementa per effettuare il risanamento.

Orchestrazione incorporata

Poiché riunisce queste funzionalità in un'unica app, VMDR automatizza l'intero processo e accelera in modo significativo la capacità dell'azienda di neutralizzare le minacce, impedendo agli aggressori di sfruttarle.



Vantaggi principali

Soluzione cloud al 100%

Non servono dispositivi ingombranti. Tutto ciò che serve è nel cloud pronto per essere utilizzato.

Facile da implementare

L'implementazione è incredibilmente semplice. Il numero illimitato di scanner virtuali permette di attivarne uno immediatamente in qualsiasi momento.

Include la gestione delle vulnerabilità

VMDR contiene la stessa soluzione di gestione delle vulnerabilità che gli utenti già conoscono e di cui si fidano, oltre a moltissime altre straordinarie app.

Notevole risparmio di tempo e denaro

Adottando una singola piattaforma cloud, le aziende possono risparmiare tutto il tempo e le risorse che prima dedicavano all'installazione di molteplici agent, console e integrazioni.

1

GESTIONE DELLE RISORSE

Identificazione e classificazione automatiche delle risorse

Sapere cosa sia attivo in un ambiente IT ibrido globale è essenziale per la sicurezza. Con VMDR i clienti possono rilevare e classificare automaticamente le risorse note e sconosciute, identificare ininterrottamente le risorse non gestite e creare flussi di lavoro automatici per gestirle in modo efficace.

Una volta raccolti i dati, i clienti possono istantaneamente interrogare le risorse e i relativi attributi per acquisire una visione chiara su hardware, configurazione di sistema, applicazioni, servizi, reti e molto altro.

2

GESTIONE DELLE VULNERABILITÀ

Rilevamento di vulnerabilità ed errori di configurazione in tempo reale

VMDR consente ai clienti di rilevare automaticamente le vulnerabilità e gli errori critici di configurazione di ogni risorsa in base ai benchmark CIS. Gli errori di configurazione sono fonte di violazioni e di mancata conformità e contribuiscono a dare origine a vulnerabilità non riconducibili a codici CVE (vulnerabilità ed esposizioni comuni). VMDR rileva ininterrottamente vulnerabilità ed errori di configurazione critici sulla più ampia gamma del settore di dispositivi, sistemi operativi e applicazioni.

3

CLASSIFICAZIONE DELLE MINACCE PER GRAVITÀ

Assegnazione automatica delle priorità

Appoggiandosi a modelli di raccolta e analisi delle minacce in tempo reale e machine learning, VMDR individua automaticamente le vulnerabilità più rischiose presenti sulle risorse più critiche. Speciali indicatori quali vulnerabilità sfruttabile, attacco attivo o elevato spostamento laterale consentono di segnalare le vulnerabilità più rischiose presenti, mentre i diversi livelli di priorità applicati tramite i modelli di machine learning permettono di mettere in evidenza le vulnerabilità con più probabilità di diventare minacce gravi.

4

GESTIONE DELLE PATCH

Applicazione di patch e ripristino a portata di mano

Dopo avere assegnato la priorità alle vulnerabilità in base al rischio, VMDR procede alla bonifica in ambienti di qualsiasi dimensione distribuendo la patch più indicata. Inoltre, i processi ricorrenti e automatici basati su policy mantengono i sistemi aggiornati e consentono di gestire le patch, di sicurezza e non, in modalità proattiva, riducendo decisamente il numero di vulnerabilità che i team operativi devono verificare nell'ambito del ciclo di ripristino.

Conferma e ripetizione

Con VMDR, gli utenti possono chiudere il cerchio e completare il processo di gestione delle vulnerabilità utilizzando un unico pannello di controllo che comprende dashboard personalizzabili aggiornati in tempo reale e widget con trending incorporato. Grazie al prezzo per singola risorsa e all'assenza di software da aggiornare, con VMDR si ottiene una sensibile riduzione del costo totale di proprietà.

Qualys VMDR® — Valuta tu stesso

App e servizi	A che cosa serve	incluso	Componente
GESTIONE DELLE RISORSE			
Asset Discovery	Rileva e classifica tutte le risorse conosciute e sconosciute che si collegano al tuo ambiente IT ibrido globale, come i dispositivi e le applicazioni locali, gli endpoint, le risorse mobili, i cloud, i container e i dispositivi OT e IoT. Include i sensori di scansione passivi Qualys.	○	
Asset Inventory Crea un inventario aggiornato in tempo reale di tutte le risorse IT dell'ambiente.	• **On-premises Device Inventory** – Rileva tutti i dispositivi e le applicazioni collegate alla rete, come i server, i database, le workstation, i router, le stampanti, i dispositivi IoT e altro ancora. • **Certificate Inventory** – Rileva e cataloga tutti i certificati digitali TLS/SSL interni ed esposti a Internet emessi da una qualsiasi autorità di certificazione. • **Cloud Inventory** – Monitora utenti, istanze, reti, sistemi di archiviazione, database e le relative relazioni per compilare su base continua l'inventario delle risorse presenti in tutte le piattaforme di cloud pubblici. • **Container Inventory** – Identifica e traccia l'infrastruttura dei container in tutti gli ambienti. • **Mobile Device Inventory** – Rileva e cataloga tutti i dispositivi mobili dell'azienda, con informazioni approfondite su ogni dispositivo e memorizzandone la configurazione e le applicazioni installate.	○	
Asset Categorization and Normalization	Per ogni risorsa raccoglie informazioni dettagliate, i servizi in esecuzione, i software installati e molto altro. Elimina le varianti rappresentate dal nome del prodotto e del fornitore e le cataloga per famiglie di prodotti.	○	
Enriched Asset Information	Raccoglie informazioni estese e approfondite che includono dati come cicli di vita hardware/software (EOL/EOS), audit delle licenze software, licenze commerciali e open source e molto altro.		○
CMDB Synchronization	Sincronizza in modalità bidirezionale i dati sulle risorse tra Qualys e ServiceNow CMDB.		○
VULNERABILITY MANAGEMENT			
Vulnerability Management	Rileva ininterrottamente le vulnerabilità software con l'ausilio del più completo database delle firme disponibile che copre la più ampia gamma di categorie di risorse possibile. Qualys è il leader del mercato in materia di gestione delle vulnerabilità.	○	
Configuration Assessment	Valuta, segnala e monitora gli errori di configurazione in materia di sicurezza basandosi sui benchmark CIS (Center for Internet Security).	○	
Certificate Assessment	Valuta i certificati digitali (interni ed esposti a Internet) e le configurazioni TLS alla ricerca di problematiche e vulnerabilità.		
Componenti di valutazione aggiuntivi	• **Cloud Security Assessment** nell'ambiente alla ricerca di vulnerabilità gravi e pacchetti non approvati al fine di eseguire le attività di ripristino. È in grado di effettuare la scansione durante la fase di compilazione ricorrendo a plug-in per strumenti CI/CD e registri. • **Container Security Assessment** – Analizza le immagini dei container e i container in esecuzione nell'ambiente alla ricerca di vulnerabilità gravi e pacchetti non approvati al fine di eseguire le attività di ripristino. È in grado di effettuare la scansione durante la fase di compilazione ricorrendo a plug-in per strumenti CI/CD e registri.		○
RILEVAMENTO E CLASSIFICAZIONE DELLE MINACCE PER GRAVITÀ			
Continuous Monitoring	Avvisa in tempo reale sulle irregolarità della rete. Identifica le minacce e monitora le modifiche di rete inaspettate prima che si trasformino in violazioni.	○	
Threat Protection	Individua le minacce più critiche e definisce la priorità delle patch da applicare. Grazie all'uso di servizi di raccolta e analisi delle minacce in tempo reale e del machine learning, permette di mantenere il controllo sulle minacce in evoluzione e di individuare quelle da neutralizzare per prime.	○	
RISPOSTA			
Patch Detection	Crea automaticamente correlazioni tra le vulnerabilità e le patch, diminuendo il tempo di risposta per gli interventi di remediation. Cerca le vulnerabilità e le esposizioni comuni e individua le patch più recenti.	○	
Patch Management tramite fornitori terzi	Soluzione che si integra ai sistemi di distribuzione delle patch esistenti, come SCCM e altri sistemi esterni, riducendo in modo significativo i tempi di implementazione delle patch.		○
Patch Management tramite Qualys Cloud Agents	L'uso di Qualys Cloud Agents velocizza la distribuzione delle patch rendendo superfluo l'impiego di soluzioni di implementazione terze.		○
Container Runtime Protection	Protegge, mantiene sicuri e monitora i container in esecuzione in ambienti di container tradizionali basati su host e ambienti Container-As-A-Service tramite l'imposizione di policy granulari per l'analisi dei comportamenti. (Disponibile nel T2/T3 del 2020)		○
Mobile Device Management	Monitora, gestisce e protegge i dispositivi mobili da remoto. (Versione beta disponibile nel T2 del 2020)		○
Certificate Renewal	Consente di rinnovare i certificati in scadenza direttamente tramite Qualys (disponibile nel T2 del 2020)		
VMDR include, SENZA LIMITI: Qualys Virtual Passive Scanning Sensors (per il rilevamento), Qualys Virtual Scanners, Qualys Cloud Agents, Qualys Container Sensors e Qualys Virtual Cloud Agent Gateway Sensors per l'ottimizzazione della larghezza di banda.		○	

© 2020 Qualys, Inc. Tutti i diritti riservati. 4/20