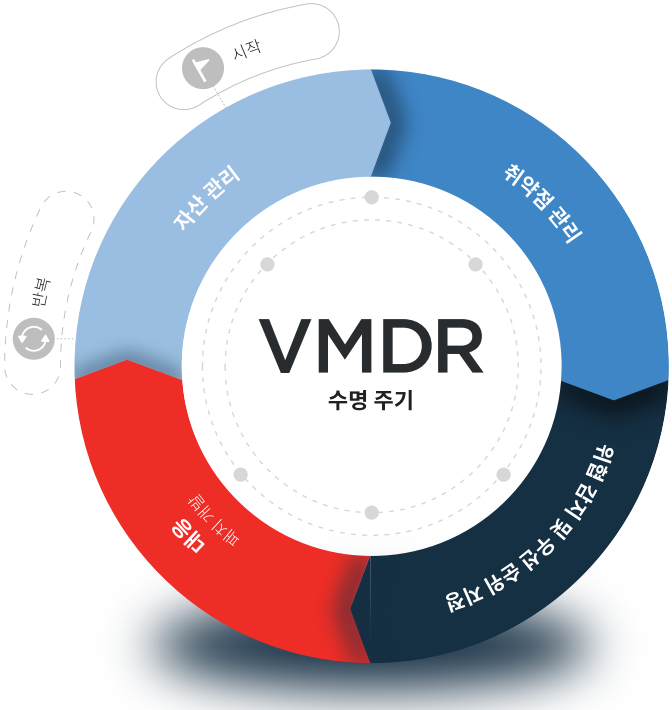
단일 플랫폼.
단일 에이전트.
단일 보기.

Qualys는 조직이 IT, 보안 및 규정 준수를 간소화하고 통합하도록 지원합니다.
Qualys Cloud Platform과 그 단일 Cloud Agent는 조직이 글로벌 하이브리드 IT 환경 전반에서
예방부터 감지, 대응까지 실시간으로 보안을 유지할 수 있도록 단일 보기를 제공합니다.

Qualys VMDR® — 일체형 취약점 관리, 감지 및 대응

최고의 취약점 관리 솔루션을 한 단계 업그레이드

단일 솔루션을 통해 글로벌 하이브리드 IT 환경 전반에서 중대한 취약점에 대해 실시간으로 검색, 평가하고, 우선 순위를 지정하고 패치를 적용하세요.



오케스트레이션 기능이 내장된 VMDR

글로벌 하이브리드 IT에서 알려지지 않은 자산 포함 모든 자산 식별

글로벌 하이브리드 IT 환경에서 포괄적으로 사용되는 사항들을 파악하는 것은 보안 유지의 출발점입니다. 벤더 수명 주기 정보 등의 세부 정보가 포함된, 체계적으로 분류된 완전한 인벤토리를 위해 알려지지 않은 자산 포함 모든 IT 자산을 자동으로 감지합니다.

6시그마 정확도로 취약점 및 구성 오류 분석

CIS 벤치마크에 따라 자산별로 취약점 및 중요한 구성 오류를 자동으로 감지합니다.

가장 긴급한 사항에 집중하기

향상된 상관 관계 파악 기능 및 기계 학습을 사용하여 가장 중요한 자산에 대한 가장 위험한 취약점에 자동으로 우선 순위를 지정하여 취약점을 수천 가지에서 정말 중대한 몇백 가지로 줄입니다.

가장 심각한 위협으로부터 자산 보호

버튼 하나로 가장 적절한 대체 패치를 배치함으로써 모든 규모의 환경 전반에서 취약점 및 위협에 대해 빠르게 조치합니다.

오늘날의 프로세스에는 다중 지점 솔루션을 사용하는 다양한 팀이 관련되므로 중요한 패치 프로세스가 복잡해지고 시간도 많이 걸립니다.

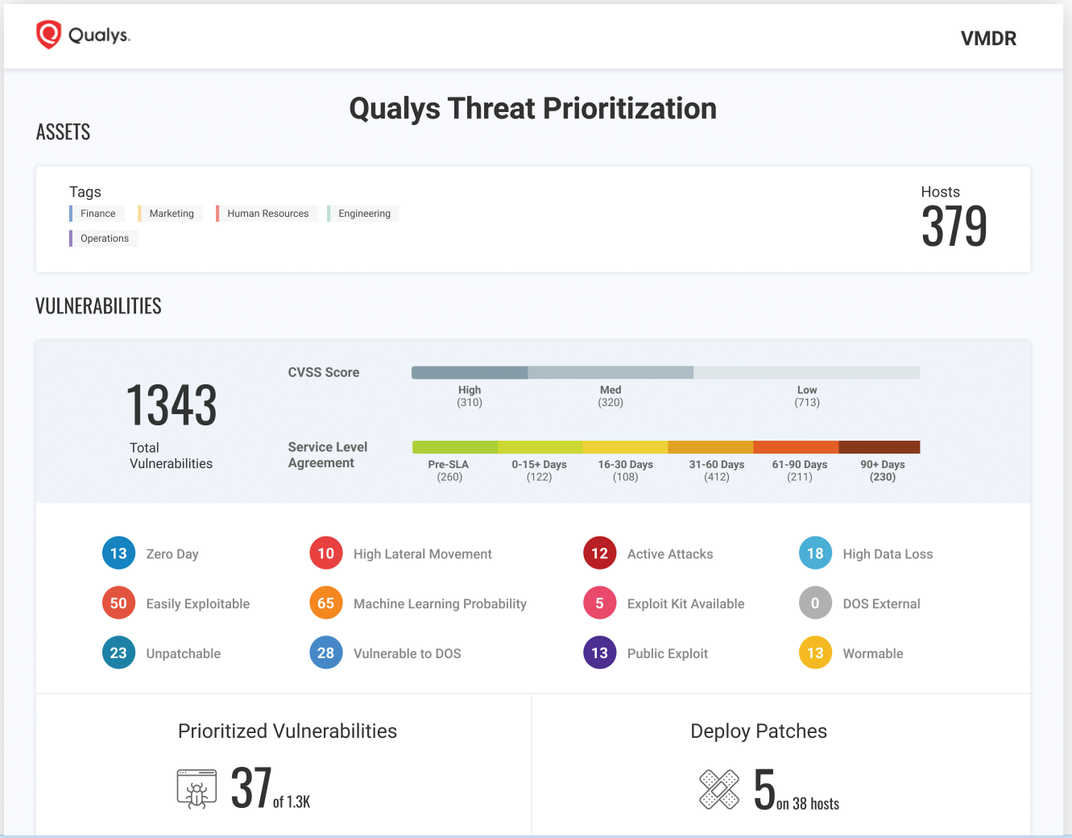
기존의 엔드포인트 솔루션은 서로 잘 연결되지 않으므로 통합 문제, 거짓 양성 및 지연 문제가 발생합니다. 결과적으로 디바이스가 식별되지 못하고, 중요한 자산이 잘못 분류되고, 취약점의 우선 순위가 잘못 지정되고, 패치가 부분적으로만 적용되는 문제가 생깁니다.

검색, 평가, 인식 및 대응을 위한 단일 앱.

강력한 경량 Cloud Agents, Virtual Scanners 및 Network Analysis(패시브 스캐닝)와 결합된 Qualys Cloud Platform은 강력하고 즉시 사용 가능한 오케스트레이션 워크플로로 통합된 단일 앱으로 효과적인 취약점 관리 프로그램의 4가지 핵심 요소를 제공합니다. Qualys VMDR®을 사용하여 조직에서는 네트워크에 나타나는 관리되지 않는 자산을 포함하여 사용자 환경의 모든 자산을 자동으로 검색하고, 모든 하드웨어 및 소프트웨어를 인벤토리화하고, 중요한 자산을 분류하고 태그를 지정할 수 있습니다. VMDR은 이러한 자산에 최신 취약점이 나타나는지 지속적으로 평가하고, 악용 가능한 취약점에 우선 순위를 적용하기 위해 최신 위협 인텔리전스 분석을 적용합니다. 마지막으로 VMDR은 취약한 자산을 위한 최신 대체 패치를 자동으로 감지하고, 손쉽게 배포해 조치합니다.

내장형 오케스트레이션

VMDR은 이러한 모든 기능을 단일 앱 워크플로로 전달하여 전체 프로세스를 자동화하고, 조직이 위협에 대응하여 잠재적 악용을 방지하는 능력을 크게 개선합니다.



주요 이점

모든 과정이 클라우드에서 진행

대규모 장치가 필요하지 않습니다. 모든 작업이 클라우드에서 진행되므로 바로 실행할 수 있습니다.

쉬운 배포

배포가 굉장히 간단합니다. 무제한 가상 스캐너를 사용하면 스캐너를 가동하고 즉시 실행할 수 있습니다.

VM 포함

VMDR에는 여러분이 잘 알고 신뢰하는 취약점 관리 솔루션에 더하여 다른 여러 유용한 앱도 있습니다.

시간과 비용을 획기적으로 절감

단일 클라우드 플랫폼을 사용함으로써 조직은 여러 에이전트, 여러 콘솔 및 통합을 설치하는 데 필요한 리소스와 시간을 획기적으로 절약할 수 있습니다.

1

자산 관리

자동 자산 식별 및 분류

글로벌 하이브리드 IT 환경에서 포괄적으로 사용되는 사항들을 파악하는 것은 보안 유지의 출발점입니다. VMDR을 사용하여 고객은 알려진 자산 및 알려지지 않은 자산을 자동으로 검색 및 분류하고, 관리되지 않는 자산을 지속적으로 식별하고, 효과적으로 자산을 관리하기 위한 자동 워크플로를 생성할 수 있습니다.

데이터가 수집되면 고객은 자산 및 모든 특성을 즉시 쿼리하여 하드웨어, 시스템 구성, 애플리케이션, 서비스, 네트워크 정보 등을 자세히 파악할 수 있습니다.

2

취약점 관리

실시간 취약점 및 구성 오류 감지

VMDR을 사용하여 고객은 CIS 벤치마크에 따라 자산별로 취약점 및 중요한 구성 오류를 자동으로 감지할 수 있습니다. 구성 오류는 보안 및 규정 준수 실패로 이어져 CVE(일반적인 취약점 및 노출) 없이도 자산을 취약하게 만듭니다. VMDR은 산업 분야에서 사용되는 가장 광범위한 디바이스, 운영 체제 및 애플리케이션의 심각한 취약점과 구성 오류를 지속적으로 식별합니다.

3

위협 우선 순위 지정

조치 작업에 자동으로 우선 순위 지정

VMDR은 실시간 위협 인텔리전스 및 기계 학습 모델을 사용하여 가장 중요한 자산의 가장 위험한 취약점에 자동으로 가장 높은 우선 순위가 적용됩니다. 기계 학습 모델은 심각한 위협이 될 가능성이 가장 높은 취약점을 강조 표시하고 여러 단계의 우선 순위를 제공하며, 악용 가능, 능동 공격 및 고도의 횡적 이동과 같은 지표는 위험 상태에 있는 현재 취약점을 나타냅니다.

4

패치 관리

간편한 패치 적용 및 조치

VMDR은 위험에 따라 취약점에 우선 순위를 지정한 후에 가장 적절한 대체 패치를 배치하여 모든 규모의 환경에서 타겟팅된 취약점에 대해 빠르게 조치합니다. 그뿐 아니라 정책 기반의 자동 반복 작업으로 시스템을 최신 상태로 유지하여 보안 및 비보안 패치를 사전에 관리합니다. 이를 통해 운영 팀이 조치 주기의 일부로 파악해야 하는 취약점을 획기적으로 줄일 수 있습니다.

확인 및 반복

VMDR은 반복 루프를 닫고, 추세 파악 기능이 내장된, 실시간 사용자 지정이 가능한 대시보드와 위젯을 제공하는 단일 창구에서 취약점 관리 주기를 완료합니다. VMDR은 자산을 기준으로 가격이 부과되며 업데이트할 소프트웨어가 없으므로 총 비용을 획기적으로 절감합니다.

Qualys VMDR® — 일체형 솔루션

		포함	추가 기능
자산 관리			
자산 검색	온-프레미스 디바이스 및 애플리케이션, 모바일, 엔드포인트, 클라우드, 컨테이너, OT 및 IoT를 비롯하여 글로벌 하이브리드 IT 환경에 연결된 알려지지 않은 자산 포함 모든 자산을 감지하고 인벤토리화합니다. Qualys Passive Scanning Sensors를 포함합니다.	○	
자산 인벤토리 모든 IT 자산에 대한 최신 실시간 인벤토리를 얻을 수 있습니다.	• **온-프레미스 디바이스 인벤토리** – 서버, 데이터베이스, 워크스테이션, 라우터, 프린터, IoT 디바이스 등을 비롯하여 네트워크에 연결된 모든 디바이스와 애플리케이션을 감지합니다. • **인증서 인벤토리** – 모든 인증 기관의 모든 TLS/SSL 디지털 인증서(내부 및 외부)를 감지하고 분류합니다. • **클라우드 인벤토리** – 모든 공용 클라우드 플랫폼에서 사용되는 리소스 및 자산에 대한 지속적인 인벤토리를 위해 사용자, 인스턴스, 네트워크, 스토리지, 데이터베이스 및 해당 관계를 모니터링합니다. • **컨테이너 인벤토리** – 빌드부터 런타임에 이르기까지 컨테이너 호스트 및 해당 정보를 검색하고 추적합니다. • **모바일 디바이스 인벤토리** – 디바이스, 해당 구성 및 설치된 애플리케이션에 대한 광범위한 정보를 포함하여 기업 전반의 Android, iOS/iPadOS 디바이스를 감지하고 분류합니다.	○	
자산 분류 및 표준화	자산의 세부 정보, 실행 중인 서비스, 설치된 소프트웨어 등 자세한 정보를 수집합니다. 제품 및 벤더 이름의 변형을 제거하고, 모든 자산에서 제품군별로 분류합니다.	○	
풍부한 자산 정보	하드웨어/소프트웨어 수명 주기(EOL/EOS), 소프트웨어 라이센스 감사, 상용 및 오픈 소스 라이센스 등을 비롯한 심도 깊은 고급 세부 정보를 얻습니다.		○
CMDB 동기화	Qualys와 ServiceNow CMDB 사이에서 자산 정보를 양방향으로 동기화합니다.		○
취약점 관리			
취약점 관리	광범위한 자산 범주에서 가장 포괄적인 서명 데이터베이스를 사용하여 소프트웨어 취약점을 지속적으로 감지합니다. Qualys는 VM 분야의 선두주자입니다.	○	
구성 평가	CIS(Center for Internet Security) 벤치마크를 기준으로 보안 관련 구성 오류를 평가하고, 보고하고, 모니터링합니다.	○	
인증서 평가	디지털 인증서(내부 및 외부)와 TLS 구성에서 인증서 문제 및 취약점을 평가합니다.	○	
추가적인 자산 관련 추가 기능	• **모바일 디바이스 취약점 및 구성 오류 평가** – 디바이스, OS, 앱 및 네트워크 취약점을 지속적으로 감지하고 중요한 모바일 디바이스 구성을 모니터링합니다. • **클라우드 보안 평가** – PaaS/IaaS 리소스를 지속적으로 모니터링하고 구성 오류 및 비표준 배포 문제를 평가합니다. • **컨테이너 보안 평가** – 사용자 환경의 컨테이너 이미지와 실행 중인 컨테이너에 심각한 취약점, 승인되지 않은 패키지가 있는지 검사하고 조치를 주도합니다. CI/CD 도구 및 레지스트리용 플러그인으로 빌드 단계에서 검사 기능을 포함합니다.		○
위협 감지 및 우선 순위 지정			
지속적인 모니터링	실시간으로 네트워크 불규칙 상황을 경고합니다. 손상으로 이어지기 전에 위협을 식별하고 예기치 않은 네트워크 변경을 모니터링합니다.	○	
위협으로부터 보호	가장 심각한 위협을 알아내고 패치 적용에 우선 순위를 지정합니다. 실시간 위협 인텔리전스 및 기계 학습을 사용하여 진화하는 위협을 통제하고, 먼저 조치할 사항을 파악합니다.	○	
대응			
패치 감지	특정 호스트에 대한 취약점과 패치 간 관계를 자동으로 파악하여 조치 대응 시간을 줄입니다. CVE를 검색하고 최신 대체 패치를 식별합니다.	○	
Qualys Cloud Agents를 통한 패치 관리	Qualys Cloud Agents를 사용하여 타사 패치 배포에 대한 의존을 줄임으로써 패치 배포를 가속화합니다.		○
모바일 디바이스에 대한 패치 관리	취약한 앱을 제거 또는 업데이트하고, 사용자에게 경고하고, 디바이스를 리셋하거나 잠그고, 암호를 변경하는 등의 관리를 합니다.		○
컨테이너 런타임 보안	세분화된 행동 정책 시행을 통해 기존의 호스트 기반 컨테이너 및 서비스형 컨테이너(Container-As-A-Service) 환경에서 실행 중인 컨테이너를 보호하고 모니터링합니다.		○
인증서 갱신	Qualys를 통해 직접 만료 예정인 인증서를 갱신할 수 있습니다.		○

VMDR에는 다음을 비롯한 여러 기능이 포함되어 있습니다. Qualys Virtual Passive Scanning Sensors(검색용), Qualys Virtual Scanners, Qualys Cloud Agents, Qualys Container Sensors 및 Qualys Virtual Cloud Agent Gateway Sensors(대역폭 최적화용)

퀄리스 코리아
경기도 안양시 동안구 학의로 282, 금강펜테리움IT타워 A동 1102호
Contact Point
강원호 지 사 장 / wonho.kang@qualys.com
김주형 기술이사 / aaron.kim@qualys.com 010-4879-5179