Qualys

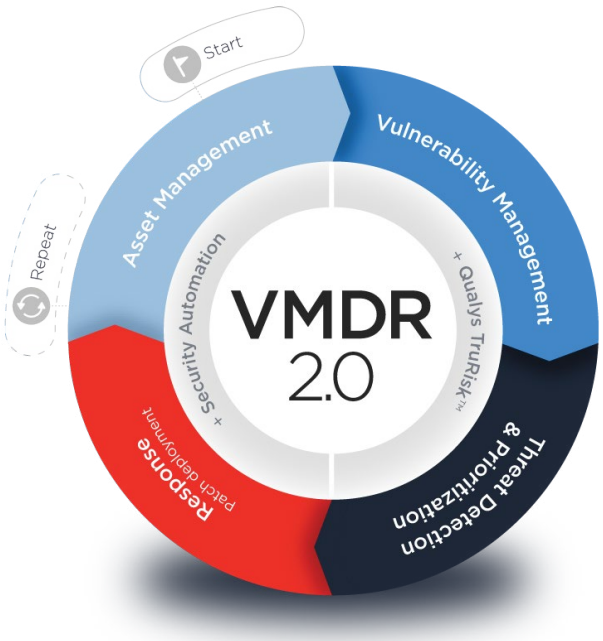
# VMDR® 2.0 với Qualys TruRisk™

## Quản lý lỗ hổng, phát hiện và phản ứng dựa trên mức độ rủi ro

### Tái định nghĩa quản trị rủi ro thông tin cho doanh nghiệp

---

Phát hiện, đánh giá, ưu tiên và vá các lỗ hổng nghiêm trọng và giảm rủi ro an ninh mạng theo thời gian thực xuyên suốt hạ tầng IT lai ghép, OT, và toàn cảnh IOT - Tất cả trên một nền tảng đám mây duy nhất.




VMDR với phân cấp có sẵn

TruRisk

### Xác định tài sản rủi ro nhất

Qualys TruRisk™ xác định một cách toàn diện rủi ro xuyên suốt bề mặt tấn công bao gồm lỗ hổng, cấu hình lỗi, và chứng thư số. Rủi ro được đánh giá dựa trên mức độ nghiêm trọng và kiến thức khai thác từ hàng trăm nguồn để chủ động đo lường, theo dõi, và thông báo mức rủi ro.

### Nhanh chóng khắc phục hiểm hoạ mọi cấp độ

Tích hợp theo quy luật với các công cụ ITSM (ServiceNow, JIRA) tự động gắn các phiếu khắc phục cho các lỗ hổng được ưu tiên bởi mức rủi ro với khả năng gắn thẻ động. Các hoạt động khắc phục và phân phối trực tiếp từ ITSM đóng lỗ hổng nhanh hơn và giảm thời gian khắc phục trung bình (MTTR).

### Tự động hoá nhiệm vụ với quy trình không mã

Là một phần của Qualys Cloud Platform, công nghệ QFlow cung cấp quy trình không mã trực quan kéo và thả để tự động nhiều nhiệm vụ tiêu tốn thời gian khác nhau và quản trị lỗ hổng phức tạp.

### Nhận các cảnh báo tấn công ưu tiên

Ngăn chặn mã độc lây lan bằng cách chủ động khai thác các CVE sử dụng các chỉ dấu hiểm hoạ bên ngoài và mã độc. Bao gồm thông tin hiểm hoạ từ180,000+ lỗ hổng và 25+ hiểm hoạ và nguồn thông tin khai thác để xác định các rủi ro độc nhất với doanh nghiệp của bạn và ngăn chặn các cuộc tấn công.

# Một giải pháp duy nhất cho khám phá, đánh giá, phát hiện, và phản ứng với rủi ro an ninh thông tin.

VMDR® 2.0 với Qualys TruRisk™ cung cấp giải pháp quản trị lỗ hổng dựa trên rủi ro để ưu tiên lỗ hổng và tài sản dựa trên rủi ro và mức độ nghiêm trọng với doanh nghiệp.

## Tích hợp đơn giản giúp tăng tốc giảm thiểu rủi ro xuyên suốt doanh nghiệp

Qualys VMDR 2.0 tích hợp đơn giản với cơ sở dữ liệu quản trị cấu hình (CMDB) và giải pháp quản trị bản vá để nhanh chóng phát hiện, ưu tiên, và tự động khắc phục lỗ hổng mọi cấp độ để giảm rủi ro. Tích hợp chặt chẽ với giải pháp ITSM như ServiceNow giúp tự động và vận hành quản trị lỗ hổng xuyên suốt doanh nghiệp.

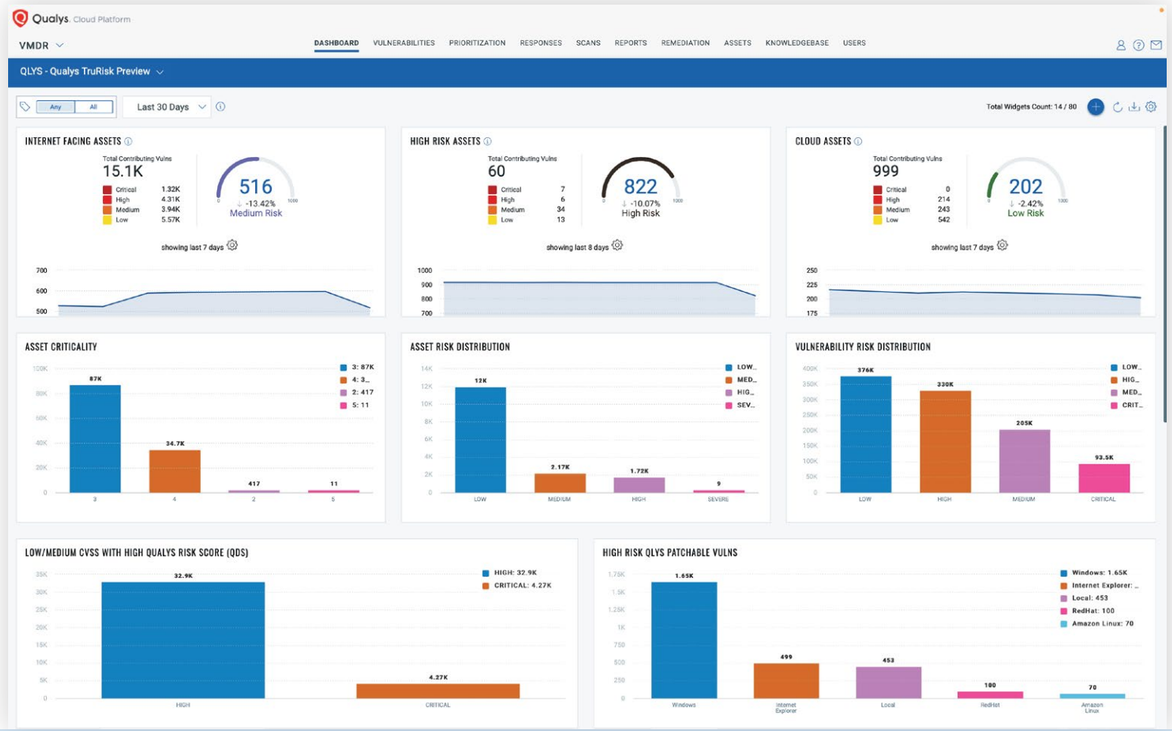
Với VMDR 2.0, giải pháp quản trị lỗ hổng dựa trên rủi ro giúp ưu tiên lỗ hổng, cấu hình lỗi, tài sản và nhóm tài sản dựa trên rủi ro, giảm rủi ro bằng cách khắc phục lỗ hổng mọi cấp độ, và giúp doanh nghiệp đo lường hiệu quả của chương trình bảo mật bằng cách theo dõi mức độ giảm thiểu rủi ro theo thời gian.

Tự động hoá quy trình để giảm thiểu rủi ro mọi cấp độ

Qualys VMDR 2.0 được phát triển bởi Qualys Cloud Platform, kết hợp với Qualys Cloud Agent, máy quét ảo, và khả năng phân tích mạng (rà soát bị động). Chúng cùng nhau mang lại những yếu tố quan trọng của một chương trình quản trị lỗ hổng hiệu quả vào một dịch vụ thống nhất duy nhất bằng công việc điều phối không mã mạnh mẽ sử dụng QFlow. Từ việc khám phá tài sản cho đến đánh giá rủi ro để phát hiện và phản ứng. VMDR 2.0 tự động toàn bộ quy trình và tăng tốc đáng kể khả năng của doanh nghiệp để phản ứng với hiểm hoạ, nhờ vậy ngăn chặn các cuộc khai thác có thể xảy ra.

Chi phí

Qualys VMDR 2.0 được tính phí dựa trên tài sản và không yêu cầu cập nhật phần mềm để bắt đầu. Đăng ký miễn phí để dùng thử hoặc yêu cầu báo giá




## Lợi ích chính

### Toàn bộ trên đám mây

Không cần thiết bị cồng kềnh. Toàn bộ đã có trên đám mây và sẵn sàng sử dụng.

### Dễ triển khai

Triển khai vô cùng dễ dàng. Với không giới hạn số lượng máy quét ảo, bạn có thể triển khai một máy quét và sẵn sàng sử dụng.

### Bao gồm VM

VMDR 2.0 với Qualys TruRisk có chung giải pháp quản trị lỗ hổng mà bạn biết và tin cậy, cũng như nhiều dịch vụ tuyệt vời khác.

### Giảm mạnh chi phí và thời gian

Sử dụng một nền tảng đám mây và một tác nhân, doanh nghiệp tiết kiệm đáng kể tài nguyên và thời gian yêu cầu để cài đặt nhiều tác nhân, nhiều giao diện quản trị và tích hợp.

1

**QUẢN TRỊ TÀI SẢN**

### Tự động xác định tài sản và phân loại

Biết được cái gì đang hoạt động trong môi trường IT lai ghép là cơ sở cho bảo mật. VMDR 2.0 cho phép khách hàng tự động khám phá và phân loại tài sản biết và chưa biết, liên tục xác định các tài sản chưa được quản trị, và tạo các quy trình tự động để quản lý chúng hiệu quả.

Sau khi dữ liệu được thu thập, khách hàng có thể ngay lập tức truy vấn tài sản và các thuộc tính của chúng để có cái nhìn sâu hơn vào phần cứng, cấu hình hệ thống, ứng dụng, dịch vụ, thông tin mạng và nhiều hơn thế.

2

**QUẢN TRỊ LỖ HỔNG**

### Phát hiện lỗ hổng và cấu hình lỗi thời gian thực

VMDR 2.0 cho phép khách hàng tự động phát hiện lỗ hổng và cấu hình lỗi nghiêm trọng theo CIS benchmark theo thời gian thực. Với sự hỗ trợ của 62,000+ lỗ hổng và hỗ trợ toàn diện cho CIS benchmarks, doanh nghiệp có thể phản ứng với hiểm hoạ nhanh hơn. VMDR 2.0 với Qualys TruRisk liên tục xác định các yếu tố rủi ro tới hệ thống IT, bao gồm các lỗ hổng nghiêm trọng và cấu hình lỗi trên dải rộng các thiết bị, hệ điều hành và ứng dụng trong ngành.

3

**ƯU TIÊN HIỂM HOẠ**

### Tự động ưu tiên dựa trên rủi ro

VMDR với Qualys TruRisk tận dụng thông tin khai thác và hiểm hoạ toàn diện để tự động đánh giá rủi ro thực sự dựa trên nhiều yếu tố. Việc này bao gồm khai thác mã kỹ càng, hiệu quả khai thác diện rộng, mức độ quan trọng của tài sản, và vị trí của nó. VMDR cung cấp điểm rủi ro để doanh nghiệp có thể xác định mức độ rủi ro, theo dõi giảm thiểu rủi ro theo thời gian, và đánh giá hiệu quả của chương trình an ninh mạng của họ.

4

**QUẢN TRỊ BẢN VÁ**

### Vá và khắc phục ngay trong tầm tay

Sau khi ưu tiên lỗ hổng theo rủi ro, VMDR 2.0 tích hợp với phần mở rộng quản trị bản vá một cách chặt chẽ, khắc phục rủi ro lỗ hổng bằng cách áp dụng bản vá, áp dụng các cách giải quyết, và sửa cấu hình xuyên suốt môi trường. Tự động hoá quy trình trực quan không mã được kích hoạt với công nghệ QFlow. QFlow đảm bảo dựa trên chính sách, định kỳ tự động hoá công việc giúp hệ thống luôn cập nhật, cung cấp quản trị bản vá chủ động cho các bản vá không bảo mật và bảo mật. Điều này giảm đáng kể lỗ hổng mà đội vận hành IT phải xử lý trong chu trình khắc phục.

### Xác nhận và lặp lại

VMDR 2.0 đóng vòng lặp và hoàn thành vòng đời quản trị lỗ hổng với một giao diện duy nhất cung cấp dashboards tuỳ biến và các widgets với xu hướng tích hợp sẵn. Mức giá dựa theo tài sản và được cung cấp trên đám mây mà không cần cập nhật phần mềm, VMDR 2.0 cũng giảm đáng kể tổng chi phí sở hữu.

# VMDR® 2.0 với Qualys TruRisk™ — Một giải pháp All-in-One

| | | Included | Add on |
|---|---|---|---|
| **QUẢN TRỊ TÀI SẢN** | | | |
| Asset Discovery | Phát hiện và thống kê toàn bộ tài sản đã biết và chưa biết có kết nối đến môi trường IT lai ghép toàn cầu của bạn — bao gồm các thiết bị tại chỗ và ứng dụng, di động, thiết bị điểm cuối, đám mây, vùng chứa, OT, và IoT. Bao gồm Qualys Passive Scanning Sensors. | ○ | |
| Asset Inventory<br>Cập nhật thời gian thực cho mọi tài sản IT | • Thống kê tiết bị tại chỗ: Phát hiện toàn bộ thiết bị và ứng dụng kết nối đến mạng bao gồm máy cơ sở dữ liệu, máy trạm, bộ định tuyến, máy in, thiết bị IoT, …<br>• Thống kê chứng thư: Phát hiện và phân loại toàn bộ chứng thư số TLS/SSL — gồm cả nội bộ và bên ngoài — từ bất kỳ hãng chứng thư nào.<br>• Thống kê đám mây: Giám sát người dùng, đối tượng, mạng, lưu trữ, cơ sở dữ liệu, và mối quan hệ của chúng cho việc thống kê liên tục tài nguyên, tài sản xuyên suốt các nền tảng đám mây công cộng.<br>• Thống kê vùng chứa: Phát hiện và theo dõi các máy chủ vùng chứa và thông tin của chúng — từ xây dựng đến khởi chạy.<br>• Thống kê thiết bị di động: Phát hiện và phân loại thiết bị Android, iOS/iPad OS trong doanh nghiệp, với các thông tin mở rộng về thiết bị, cấu hình của chúng và các app đã cài đặt. | ○ | |
| Phân loại tài sản và tiêu chuẩn hoá | Thu thập thông tin chi tiết như chi tiết tài sản, dịch vụ đang chạy, phần mềm cài đặt,… Loại bỏ các thay đổi trong tên sản phẩm và nhà cung cấp và phân loại chúng theo dòng sản phẩm trên toàn bộ các tài sản. | ○ | |
| **QUẢN TRỊ LỖ HỔNG** | | | |
| Vulnerability Management | Liên tục phát hiện lỗ hổng phần mềm sử dụng cơ sở dữ liệu dấu hiệu nhận biết toàn diện nhất trong ngành, bao phủ dải rộng các loại tài sản. Qualys là người dẫn đầu ngành trong VM. | ○ | |
| Qualys TruRisk<br>Xác định bức tranh rủi ro | Xác định chính xác bức tranh rủi ro an ninh xuyên suốt lỗ hổng, tài sản, và nhóm tài sản — đo lường và cung cấp các bước thực hiện để giảm lộ lọt và tăng cường hiệu quả cho chương trình bảo mật an ninh mạng. | ○ | |
| QFlow<br>Tự động quy trình | Tự động và phân phối nhiệm vụ vận hành với môi trường xây dựng quy trình trực quan không mã để nhanh chóng đơn giản hoá chương trình bảo mật và phản ứng. | ○ | |
| Configuration Assessment | Tài sản, báo cáo, và giám sát các vấn đề cấu hình bảo mật liên quan dựa trên Center for Internet Security (CIS) benchmarks. | ○ | |
| Certificate Assessment | Đánh giá chứng thư số của bạn — gồm cả chứng thư nội bộ và công cộng — và cấu hình TLS để xác định lỗ hổng và vấn đề chứng thư. | ○ | |
| **PHÁT HIỆN VÀ ƯU TIÊN HIỂM HOẠ** | | | |
| Continuous Monitoring | Cảnh báo thời gian thực về những bất thường trong mạng. Xác định hiểm hoạ và giám sát những thay đổi bất ngờ trước khi chúng chuyển thành xâm phạm. | ○ | |
| Threat Protection | Ghim những hiểm hoạ nghiêm trọng nhất và bản vá ưu tiên nhất. Sử dụng thông tin hiểm hoạ thời gian thực và máy học, chủ động kiểm soát các hiểm hoạ đang phát triển và xác định ưu tiên khắc phục. | ○ | |
| Custom Assessment & Remediation | Chủ động phát hiện và nhanh chóng phản ứng với lỗ hổng zero-day, sự cố và các hiểm hoạ với kịch bản tuỳ biến và kiểm soát bảo mật. | | ○ |
| **PHẢN ỨNG** | | | |
| ITSM Tool Integrations | Tích hợp dựa trên quy tắc với các công cụ ITSM (ServiceNow, JIRA) tự động gắn các phiếu hỗ trợ và cho phép phân loại khắc phục, hơn nữa giảm thiểu MTTR. | ○ | |
| Patch Detection | Tự động liên hệ lỗ hổng với các bản vá cho các máy chủ cụ thể, giảm thời gian phản ứng khắc phục. Tìm kiếm các CVE và xác định các bản vá thay thế mới nhất. | ○ | |
| Patch Management via Qualys Cloud Agent | Nhanh chóng khắc phục rủi ro lỗ hổng tổng thể bằng cách áp dụng đúng hệ điều hành, bản vá bên thứ ba, sửa cấu hình hoặc áp dụng đúng cách giảm thiểu mức độ nghiêm trọng. | | ○ |
| Patch Management for Mobile Devices | Gỡ bỏ hoặc cập nhật các ứng dụng có lỗ hổng, cảnh báo người dùng, đặt lại hoặc khoá thiết bị thay đổi mật mã, … | | ○ |
| Container Runtime Security | Củng cố, bảo vệ, và giám sát các vùng chứa đang chạy trong các máy chủ vùng chứa truyền thống và các môi trường vùng chứa như một dịch vụ với các cưỡng chế chính sách bảo mật. | | ○ |
| | | | |

VMDR 2.0 cũng bao gồm KHÔNG GIỚI HẠN: Qualys Virtual Passive Scanning Sensors (cho khám phá), Qualys Virtual Scanners, Qualys Cloud Agent, Qualys Container Sensors, và Qualys Virtual Cloud Agent Gateway Sensors cho việc tối ưu băng thông.

©2022 Qualys, Inc. All rights reserved. v220610