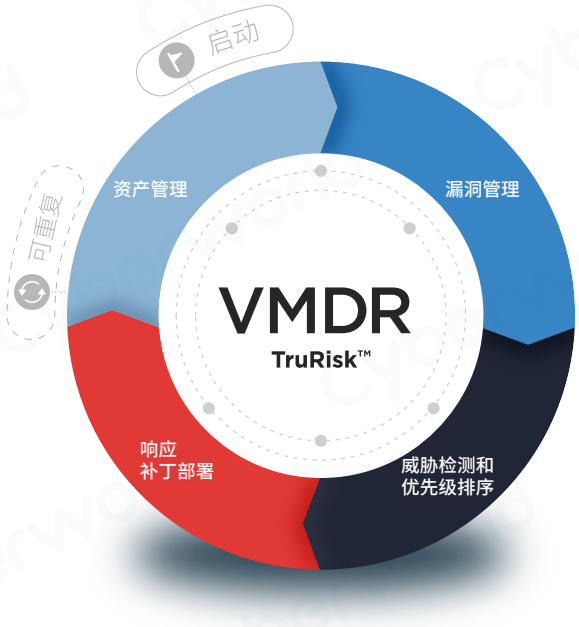
Qualys

Cyberworld

# Qualys TruRisk™ 平台的 VMDR®
# 基于风险的漏洞管理、检测和响应

## 重新定义企业网络风险管理

在混合云、IT、OT 和 IoT 环境中，通过单一管理平台来实时发现、评估、确定优先级和修复重大漏洞，从而降低网络安全风险。




VMDR内置编排功能

TruRisk

### 优先处理严重威胁

Qualys TruRisk™ 全面量化整个攻击面的风险，包括漏洞、错误配置和数字证书，将重大漏洞减少85%。

### 修复威胁速度提升 6 倍

与ITSM工具（ServiceNow、JIRA）基于规则的集成可通过动态标记自动将修复通知单分配给按风险优先级排序的漏洞。来自ITSM的修复措施和编排能更快地消除漏洞并缩短平均修复时间（MTTR）。

Flow

### 使用无代码工作流程

可视化拖放无代码工作流程能自动地执行各种耗时且复杂的漏洞管理和 IT 管理任务。

### 接收预防性攻击警报

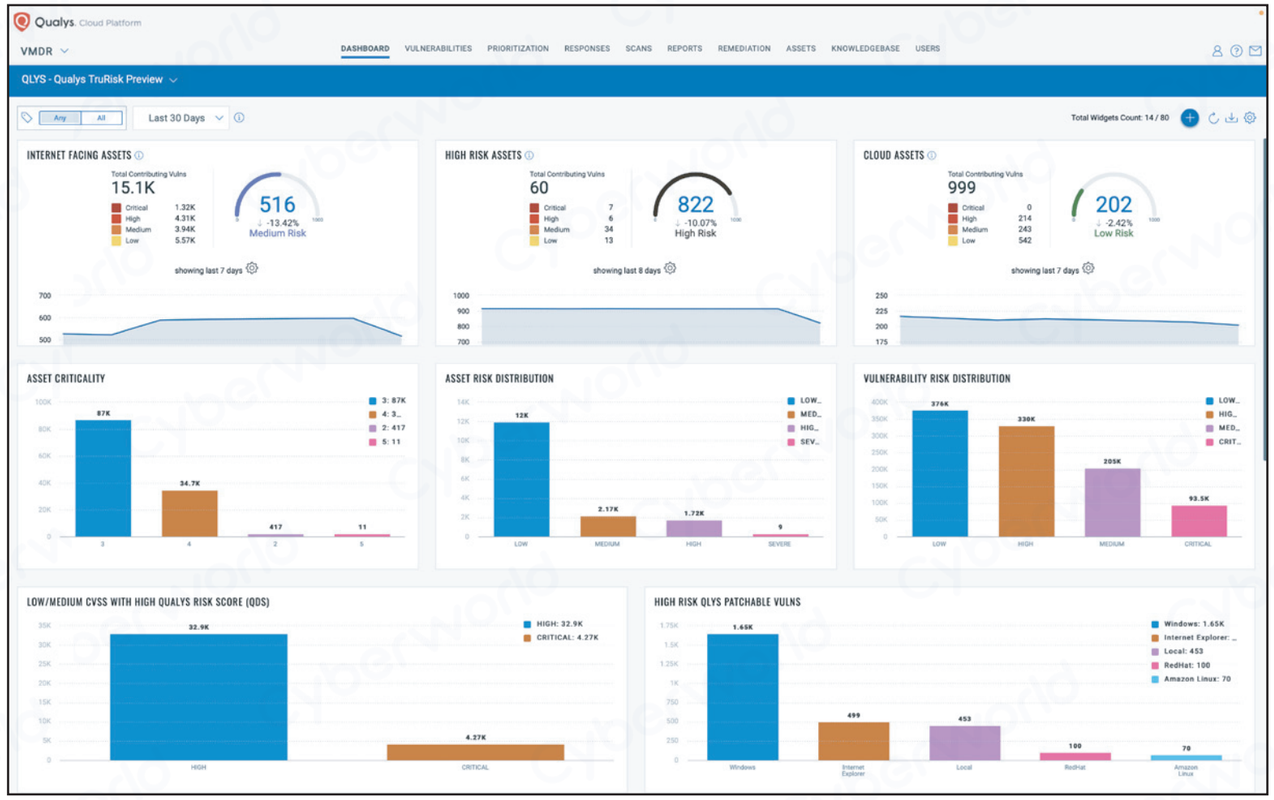
通过使用恶意软件和外部威胁指标关联主动利用的CVE，防止恶意软件传播。威胁情报来自超过18万个漏洞、超过25个威胁和漏洞利用情报源，可识别企业的独特风险并防止攻击。

### 运行时 SCA

只需在配置文件中单击一下，即可在 Agent Profile 中启用软件组成分析（SCA），以便在 VMDR 中进行深度文件系统扫描、持续评估和数据扩充。

# 一种针对自定义和第三方应用程序进行基于风险的发现、评估、检测和响应的解决方案

借助自定义评估和修复 (CAR)，VMDR 客户可以使用 Python、PowerShell 等脚本语言并执行操作，通过客户定义的逻辑来丰富Qualys开箱即用特征库，以应对几乎所有零日威胁、风险状况和内部开发的应用程序。结合TruRisk提供的基于风险的优先级排序，VMDR 使用单个代理为任何应用程序或网络环境提供全面的安全覆盖。




## VMDR 与 ITSM 、CMDB 无缝集成，可加速降低整个企业的风险

Qualys VMDR 与 IT 服务管理 (ITSM)、配置管理数据库 (CMDB) 和补丁管理解决方案无缝集成，可快速发现、确定优先级并自动地大规模修复漏洞，降低风险。VMDR 也与 ServiceNow 或 JIRA 等 ITSM 解决方案紧密集成，这有助于在整个企业和IT安全团队之间实现漏洞管理的自动化和可操作化。

使用VMDR，您可以获得基于风险的漏洞管理解决方案。该解决方案可根据风险确定漏洞、错误配置、资产和资产组的优先级。通过大规模修复漏洞来降低风险，并通过跟踪一段时间内的风险降低情况来帮助企业衡量安全计划的有效性。

**通过自动化工作流程来大规模降低风险**

Qualys VMDR 由 Qualys TruRisk 平台提供支持，结合了轻量级 Qualys Cloud Agent、虚拟扫描器和网络分析（被动扫描）功能。它将一个有效的漏洞管理计划的所有关键元素汇集到一个单一的服务中，并通过使用 Qualys Flow强大的开箱即用的无代码编排工作流程进行统一。从资产发现到基于风险的评估，再到检测和响应，VMDR自动化了整个流程，并显著加快了企业对威胁的响应能力，从而防止被利用。

**价格**

Qualys VMDR 和安全软件包 VMDR FixIT 、ProtectIT 是按资产数量定价。无需软件更新即可启动。

## 优点

### 灵活且易于部署

无需购买或管理硬件，一切都在云端进行。使用无限制的虚拟扫描器，能在10分钟或更短时间内完成设置。您可以配置一台扫描器，并随时准备好立即启动。针对中小型企业，VMDR TruRisk FixIT 和 ProtectIT 软件包提供适合您企业规模的企业级漏洞管理、补丁管理和端点防护。

### 更高的安全性和更低的复杂性

VMDR 提供企业级漏洞管理，能够使用单个代理扩展安全堆栈功能。VMDR FixIT 软件包与其他解决方案相比，打补丁修复漏洞的速度快 40% 。VMDR ProtectIT 能自动地阻止恶意软件和勒索软件感染。

### 用您自己的逻辑检测威胁

通过添加自定义评估和修复 (CAR)，利用VMDR通过您自己的逻辑和威胁特征来检测、管理和修复自定义开发的第一方软件中的漏洞。

1

### 资产管理

自动地识别和分类资产

在混合 IT 环境中了解什么是活跃的，这对安全具有根本重要性。VMDR 使客户能够自动发现已知和未知资产，并对其进行分类。持续识别未托管资产，并创建自动化工作流程，从而有效地管理这些资产。收集数据后，客户可以即时查询资产及其属性，深入了解硬件、系统配置应用程序、服务、网络信息等。

2

### 漏洞管理

实时检测漏洞和配置错误

VMDR 使客户能够根据 CIS 基准实时自动检测漏洞和严重错误配置。通过支持 86,000 多个漏洞和全面覆盖 CIS 基准，企业可以更快地响应威胁。VMDR 可持续识别 IT 面临的重大风险，包括行业最广泛的设备、操作系统和应用程序上的重大业务漏洞和错误配置。

3

### 威胁优先级

基于风险的自动优先级排序

VMDR利用全面的威胁和漏洞情报，根据多种因素自动评估您的真实风险。这些因素包括漏洞利用代码的成熟度、野外的主动利用、资产的重要性及其位置。VMDR提供风险评分，以便企业量化风险，通过跟踪一段时间内的风险降低情况来评估网络安全计划的有效性。

4

### 进阶修复

自定义修复管理

在按风险对漏洞进行优先级排序后，VMDR 的集成补丁管理和自定义评估和修复（CAR）加载项允许您通过创建自定义检查来检测与嵌入式组件和软件相关的开源风险。有了这些进步，您可以使用 Python、PowerShell等脚本语言并执行操作，通过客户定义的逻辑来丰富 Qualys 开箱即用特征库，以应对几乎所有零日威胁、风险状况和内部开发的应用程序。

### 确认并重复

VMDR 通过单一管理平台实现闭合环路并完成漏洞管理生命周期，该管理平台提供带有内置趋势的实时可自定义的仪表板和小部件。
VMDR 按资产数量定价，并在云端交付，无需更新软件，还可大幅降低您的总拥有成本。

# Qualys TruRisk™ 平台的 VMDR®
# 基于风险的一体化漏洞管理解决方案

| | | 包含 | 附加 |
|---|---|---|---|
| **资产管理** | | | |
| **资产发现** | 检测并厘清连接到全局混合 IT 环境的所有已知和未知资产，包括本地设备和应用程序、移动设备、端点、云、容器、OT 和 IoT，还包括 Qualys 被动扫描传感器。 | ○ | |
| **资产库存**<br>获取所有 IT 资产的最新实时库存 | • 本地设备库存：检测连接到网络的所有设备和应用程序，包括服务器、数据库、工作站、路由器、打印机、IoT设备等。<br>• 证书库存：检测并列出来自任何证书颁发机构的所有 TLS 和 SSL 数字证书（面向内部和外部）。<br>• 云库存：监察用户、实例、网络、存储、数据库及其关系，从而持续地盘点所有公共云平台上的资源和资产。<br>• 容器库存：从构建到运行时，发现并跟踪容器主机及其信息。<br>• 移动设备库存：检测并列出整个企业内的 Android、iOS 和 iPad OS 设备，提供有关设备、其配置和已安装应用程序的大量信息。 | ○ | |
| **资产分类和标准化** | 收集详细信息，例如资产的详细信息、正在运行的服务、已安装的软件等。消除产品和供应商名称的差异，并按所有资产的产品系列对它们进行分类。 | ○ | |
| **漏洞管理** | | | |
| **漏洞管理** | 使用业界最全面的特征数据库持续检测最广泛的资产类别的软件漏洞。<br>Qualys 是漏洞管理市场的领导者。 | ○ | |
| **Qualys TruRisk**<br>量化风险态势 | 准确量化漏洞、资产和资产组的网络安全风险态势，衡量并提供可操作的步骤，从而减少风险和提高网络安全计划的有效性。 | ○ | |
| **Qualys Flow**<br>自动化工作流程 | 使用无代码可视化工作流程构建环境自动化和编排操作任务，以快速简化安全程序和响应。 | ○ | |
| **配置评估** | 根据互联网安全中心 (CIS) 基准评估、报告、监察与安全相关的错误配置问题。 | ○ | |
| **证书评估** | 评估您的数字证书（内部和外部）以及 TLS 配置是否存在证书问题和漏洞。 | ○ | |
| **威胁检测和优先级排序** | | | |
| **持续监察** | 实时发出有关网络异常的警报。识别威胁并监察意外的网络变化，防止其违规。 | ○ | |
| **威胁防护** | 查明最严重的威胁并确定修复的优先级。使用实时威胁情报和机器学习，控制不断变化的威胁，并确定首先要修复的内容。 | ○ | |
| **使用自定义评估和修复（CAR）进行第一方风险管理** | 使用 Python、PowerShell 等脚本语言并执行操作，通过客户定义的逻辑来丰富Qualys开箱即用特征库，以应对几乎所有零日威胁、风险状况和内部开发的应用程序。 | | ○ |
| **响应** | | | |
| **ITSM工具集成** | 与 ITSM 工具（ServiceNow、JIRA）基于规则的集成可自动分配通知单并启用修复编排，从而进一步缩短平均修复时间（MTTR）。 | ○ | |
| **补丁检测** | 自动关联特定主机的漏洞和补丁，减少修复响应时间。搜索 CVE 并识别最新的替代补丁。 | ○ | |
| **通过 Qualys Cloud Agent 进行补丁管理** | 通过应用正确的操作系统、第三方补丁、修复配置或应用正确的缓解措施，快速全面修复漏洞风险。 | | ○ |
| **移动设备的补丁管理** | 卸载或更新易受攻击的应用程序、提醒用户、重置或锁定设备、更改密码等。 | | ○ |
| **容器运行时安全性** | 通过细粒度的行为策略实施，保护和监察传统基于主机的容器、容器即服务（CaaS）环境中正在运行的容器。 | | ○ |
| **证书更新** | 直接通过 Qualys 续订过期证书。 | ○ | |

VMDR 还包括无限制的：Qualys 虚拟被动扫描传感器（用于发现）、Qualys 虚拟扫描器、Qualys Cloud Agent、Qualys 容器传感器和用于带宽优化的Qualys 虚拟云代理网关传感器。