



Qualys VMDR TruRisk, FixIT, and ProtectIT Playbook

More Security with Less Complexity

February 13, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.

919 E Hillsdale
Blvd4th Floor

Foster City, CA
944041 (650) 801
6100

Qualys VMDR TruRisk, FixIT, and ProtectIT Playbook	3
What is Qualys offering?	3
Capabilities.....	4
Let's Get Started.....	5
Qualys VMDR TruRisk: Comprehensive Risk-Based Vulnerability Management.....	5
Step 1 - Identify Assets.....	5
Step 2 - Discover Vulnerabilities	6
Step 3 - Prioritize Vulnerabilities with TruRisk.....	6
Step 4 - Deploy Missing Patches	7
Reference How-to Videos:	8
Qualys VMDR TruRisk FixIT- Automated Remediation.....	9
Step 1 - Deploy Patches	9
Step 2 - Roll Back Windows Patches	10
Reference How-to Videos:	10
Qualys VMDR TruRisk ProtectIT: Anti-Virus & Anti-malware Protection	11
Step 1- Enable EDR and Malware Protection in Configuration Profile.....	11
Step 2 - Configure Rule-Based Alerts for Events.....	11
Step 3 - View Events and Detection.....	12
Reference How-to Videos:	12
Which VMDR TruRisk package is best for you?	13

Qualys VMDR TruRisk, FixIT, and ProtectIT Playbook

As cybercriminals become more innovative, the attack surface is expanding. Due to their increased vulnerability to ransomware, denial-of-service attacks (DoS), distributed denial-of-service attacks (DDoS), and man-in-the-middle attacks, small and midsize businesses are prime targets.

Qualys VMDR TruRisk can help small and midsize companies *mitigate cyber risks* without draining their budgets or diverting their human resources. VMDR TruRisk *enables organizations* to *scale* small security teams to *implement* enterprise-grade VM programs, including patch management and endpoint detection and response.

What is Qualys offering?

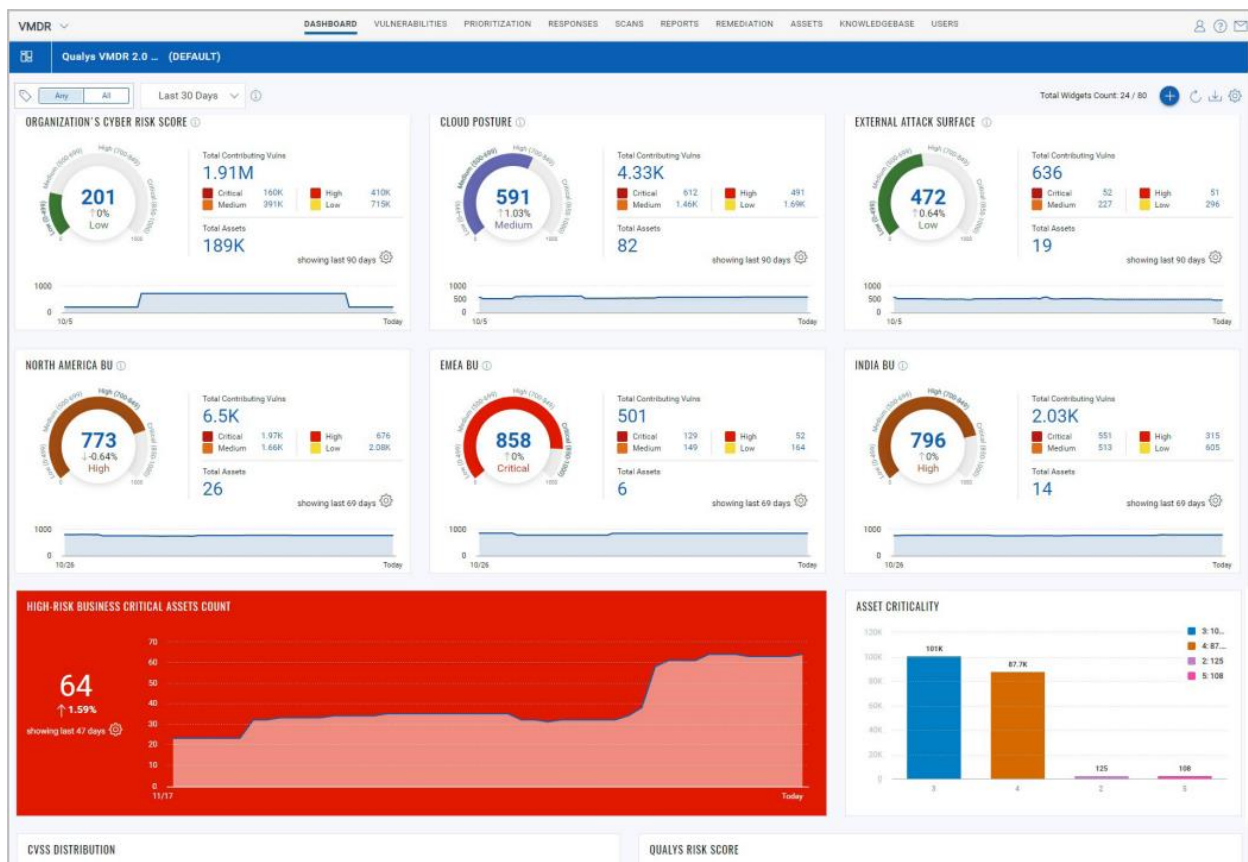
Qualys VMDR TruRisk is available in three packages, allowing organizations to optionally add remediation (Patch Management) capabilities with VMDR TruRisk FixIT and endpoint detection and response (Multi-Vector EDR) capabilities with VMDR TruRisk ProtectIT.



Capabilities

- **Simplified** product packaging
- **Low Total Cost of Ownership (TCO):** Gain orchestrated prediction, prevention, detection, and response with a single app, one cloud-based console, and one-click deployment.
- **Easy to Use:** No hardware to buy or manage. Easy to deploy. Software auto updates. Setting up takes less than 10 minutes.
- **Efficient:** Quantifying cyber risk allows organizations to measure it accurately, take steps to reduce exposure, track trends over time, and measure the effectiveness of their cyber security program.
- **Automated Vulnerability Assessment and Remediation:** Compared with other solutions, the Qualys bundle package automatically detects vulnerabilities and extends remediation configuration changes up to **40% faster**.
- **Compliance and Enforcement:** Achieve Compliance and stay compliant. For nearly all compliance and regulatory directives, including PCI, HIPAA, CIS, and more, VMDR TruRisk offers templated reports and compliance controls.

The Qualys VMDR TruRisk Playbook guides you through managing, remediating, and protecting your small and midsize business's environment against vulnerabilities.



The [Qualys blog](#) is a great place to learn more about Vulnerability Management, and the [Qualys documentation](#) can help you set up and configure Qualys apps as required.

Let's Get Started

The solution helps security and IT teams increase efficiency and save time by providing shared context and the ability to create drag-and-drop workflows to automate time-consuming vulnerability management operational processes, including vulnerability assessment of ephemeral cloud assets.

Qualys VMDR TruRisk: Comprehensive Risk-Based Vulnerability Management





VMDR automatically *detects, prioritizes, and provides threat intelligence* based on 25+ threat feeds and *enables you to assess* the risk that high-profile exploited vulnerabilities pose to your assets. Qualys *upgraded VMDR TruRisk approach* allows businesses to *prioritize vulnerabilities, assets, and groups of assets based on their actual risk*.

Benefits:

- Instantly **assess** and **prioritize** threats based on relevant context.
- **5x** faster threat detection leveraging risk-based prioritization.
- Enterprise can focus on **40%** fewer critical vulnerabilities for priority remediation.
- **Threat-based prioritization** based on *continuously updated real-time threat indicators*.
- **Real-time alerting** by email of critical vulnerabilities.
- Initiate **deployment** of missing patches from the prioritization report directly.
- Complete **asset visibility** and **classification** for on-prem or cloud assets.
- **Continuous security hygiene** for all workstations, servers, databases, and other technologies based on CIS benchmarks.
- SSL certificates for expiry monitoring.
- PCI assessment with approved ASV scan.

Here are the high-level steps you can take to get started with VMDR. Refer to the following documentation for detailed steps and explanations.

[VMDR Onboarding Videos](#) | [VMDR Getting Started Guide](#) | [VMDR Online Help](#)

 Identify Assets Continuously discover your IT assets that are on-prem, cloud, mobile, container, applications providing 100% real-time visibility	 Discover Vulnerabilities & Misconfigurations Detect vulnerabilities with six-sigma accuracy and use CIS Benchmarks to uncover misconfigurations	 Prioritize Threats with TruRisk™ Use, TruRisk, real-time threat indicators, and machine learning to prioritize vulnerabilities with the highest risk	 Integrate with ITSM to Deploy Missing Patches Remediate vulnerabilities prioritized using TruRisk, with automated ITSM workflows and effortlessly deploy the most relevant superseding patches.
---	---	--	---

Step 1 - Identify Assets

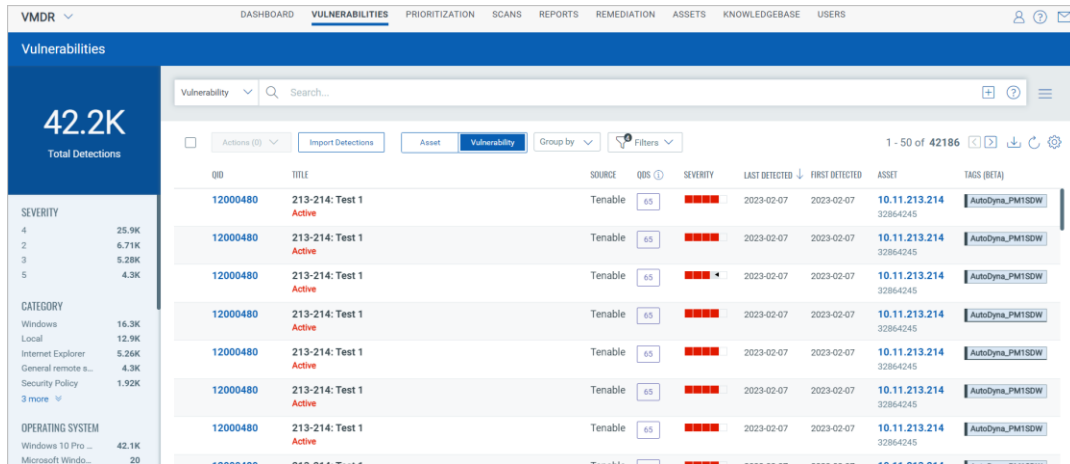
1. The first step is to *install or upgrade* the existing cloud agents for VMDR to identify assets. *Tags* are then *assigned to your assets* to better organize them.
2. Now you can *start building your inventory* by installing cloud agents.
 - [Install new agents](#)
 - [Upgrade existing agents](#)

To learn more, download the [Cloud Agent Getting Started Guide](#).

Step 2 - Discover Vulnerabilities

With your inventory built, you can now search for vulnerabilities by vulnerability and asset. The Vulnerabilities tab provides a comprehensive view of vulnerability posture by continuously identifying misconfigurations.

With the **Patch Management add-on**, you can patch Qualys patchable vulnerabilities with a single click.



The screenshot displays the Qualys VMDR interface for the 'Vulnerabilities' tab. On the left, a sidebar shows '42.2K Total Detections' and a breakdown by severity (4: 25.9K, 2: 6.71K, 3: 5.28K, 5: 4.3K) and category (Windows: 16.3K, Local: 12.9K, Internet Explorer: 5.26K, General remote s...: 4.3K, Security Policy: 1.92K, 3 more). Below this, the 'OPERATING SYSTEM' section lists 'Windows 10 Pro ...' with 42.1K and 'Microsoft Windo...' with 20. The main table lists vulnerabilities with columns: QID, TITLE, SOURCE, QDS, SEVERITY, LAST DETECTED, FIRST DETECTED, ASSET, and TAGS (BETA). The table shows multiple entries for '213-214: Test 1' with a severity of 'Active' and a QDS of 65. The assets listed are '10.11.213.214' and '32864245'. The table is paginated to show '1 - 50 of 42186' items.

QID	TITLE	SOURCE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	TAGS (BETA)
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW
12000480	213-214: Test 1 Active	Tenable	65	Active	2023-02-07	2023-02-07	10.11.213.214 32864245	AutoDyna_PMT1SDW

Step 3 - Prioritize Vulnerabilities with TruRisk

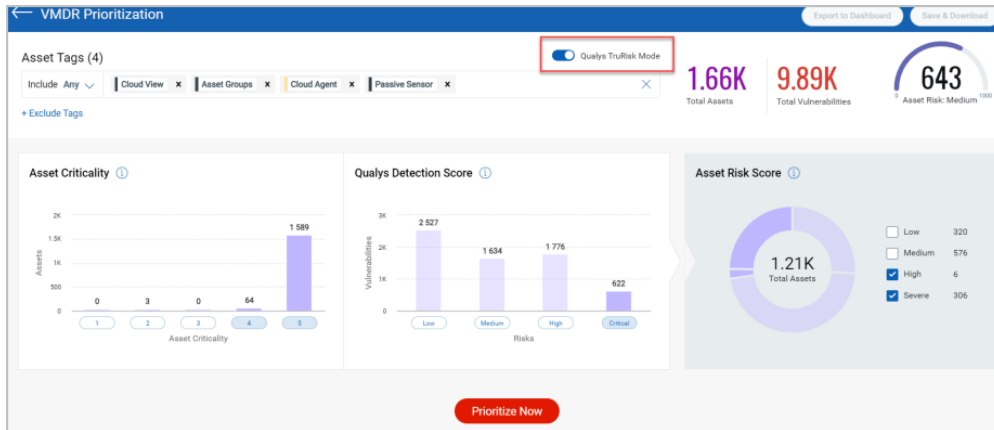
You can prioritize your most critical threats based on real-time threat indicators and identify what needs to be remedied first.

Based on the following two options, you can prioritize the remediation of vulnerabilities:

- Age, RTI, and Attack Surface
- Qualys TruRisk™ Mode

You can use **TruRisk** to assess your assets' risk scores and prevent attacks. Asset risks can be quantified using the Qualys Detection Score and TruRisk Score.

- **TruRisk Score** is intelligence-driven vulnerability severity scoring.
- **Qualys Detection Scores** identify the location of assets' vulnerabilities, their business and operational criticality, associations with business-critical applications, and context about an asset's exposure to attack.



In the **Prioritization** tab, click **Reports** > Click **Start Prioritizing** > Select at least one **Asset tag** to display the prioritized list of vulnerabilities associated with the assets.

VMDR					
DASHBOARD VULNERABILITIES PRIORITIZATION SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS					
Prioritization Reports Threat Feed					
Search reports... 9 Reports					
Actions (0) Start Prioritizing 1 - 9 of 9					
NAME	FORMAT	STATUS	CREATED ON	CREATED BY	
csv	CSV	Completed	a day ago 01:07 am	quays_wa29	
test report	CSV	Completed	6 days ago 11:34 pm	quays_wa29	
test	CSV	Completed	6 days ago 11:32 pm	quays_wa29	
TestDownload	PDF	Completed	2022-12-01 03:19 am	quays_wa29	
TestDownload	PDF	Completed	2022-11-07 08:24 am	quays_wa29	
reporting_test_1	PDF	Completed	2022-05-09 12:46 am	quays_wa29	
reporting	PDF	Completed	2022-05-08 09:28 pm	quays_wa29	

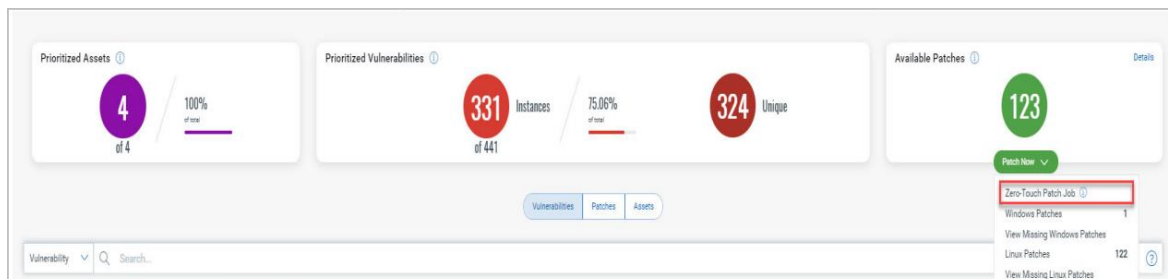
Related Topics

[Reading the VMDR Prioritization Report](#) | [Export The Dashboard](#) | [Save and Download VMDR Reports](#) | [TruRisk Score Widget](#)

Step 4 - Deploy Missing Patches

A **Zero-Touch Patch Job** automates proactively patching current and future vulnerabilities based on the criteria selected during the Prioritization report generation. With a *recurring schedule*, you can update Zero-Touch patches without worrying about future vulnerabilities for real-time threats.

Note: The Patch Management add-on is required to deploy patches.



To learn more, see [VMDR Getting Started Guide](#).

Reference How-to Videos:

[How to create an activation key for Cloud Agent deployment](#)

[Create a Configuration Profile to define performance, blackout windows, and assign assets](#)

[Obtain files and commands necessary to deploy Cloud Agents via command line or third-party tools](#)

[Install agents and verify the success of the installation](#)

[How to launch a scan and view the results](#)

[Create TruRisk dashboard and add Risk Score widget to it](#)

[Know more about the TruRisk score components](#)

Qualys VMDR TruRisk FixIT- Automated Remediation

Qualys VMDR TruRisk FixIT package includes Qualys Patch Management and VMDR capabilities.

The Qualys VMDR module enables you to discover, assess, prioritize, and identify patches for critical vulnerabilities. With Patch Management, you can *automate* patch management on Windows and Linux assets. You can *make informed decisions* with rapid *visibility into your asset's updates*. Patches can be *deployed instantly* as they become available.

Benefits:

All the benefits of VMDR TruRisk

+

- **40%** faster remediation than other solutions.
- **Consolidate IT and Security Tools** for vulnerability assessment and remediation.
- **Automated patching** for cloud and on-prem assets (operating systems & 100+ 3rd party applications)
- **"Set it and forget it"** patch rules for automatic ransomware and malware remediation.
- **Discovery and remediation** of CISA-known.

Here are the high-level steps you can take to get started with Patch Management. Refer to the following documentation for detailed steps and explanations.

[Deploying Patch Jobs on Assets](#) | [Patch Management Getting Started Guide](#)

Step 1 - Deploy Patches

1. *(Optional)* Start by **creating custom assessment profiles** to add Windows assets with specific tags. Set the interval you want the cloud agent to collect patch information. Go to **Configuration > Create Profile**.
2. Next, **review the patches** that are missing and already installed on the Patches and Assets tab.
3. **Install missing patches on assets** by creating a deployment job through the Jobs tab, Assets tab, or Patches tab. For detailed steps, refer to [Deploying Patch Jobs on Assets](#).
4. **Review the missing and installed** Windows patches is the last step here. The Patches tab shows by default the patches that are missing on your hosts that were detected by the Patch Management scan. For more information, refer to [Reviewing Missing and Installed Windows Patches](#).

Patch Management

New Updates

DASHBOARD

PRIORITIZED PRODUCTS

PATCHES

ASSETS

JOBS

CONFIGURATION

Person icon

Help icon

Menu icon

Patches

1
Total Patch

APP FAMILY

.Net

1

VENDOR

Microsoft

1

CATEGORY

Non-Security Pat...

1

TYPE

Application

1

VENDOR SEVERITY

None

1

WindowsLinuxMac

Patch

Search...

Actions (0)

Filters

1 - 1 of 1

PreviousNextRefreshSettings

PATCH TITLE	PUBLISHED DATE	ARCHIT	BULLETIN / KB	CATEGORY	QID	VENDOR SEVERITY	PATCH STATUS	
							MISSING	INSTALLED
.NET Framework 4.8.1	2022-08-08	X86_X64	MSFT-QN481 QN481	Non-Security ...	-	None	1	0

Step 2 - Roll Back Windows Patches

1. The first step is like the steps mentioned in the Deploy Patches section. You **create custom assessment profiles** and **review the missing and installed** Windows patches.
2. Next, **create a patch rollback job** if you want to roll back patches from Windows assets. Rolling back patches should be done with precision.
Go to Jobs > Windows > Create Job, and click Rollback Job.
For detailed instructions, refer to [Rolling Back Patches from Windows Assets](#).
3. In the final step, **review the job results** to determine whether all patches were successfully installed or rolled back.
Go to Jobs > from the Quick Actions menu of a job > click View Progress.
For detailed instructions, refer to [Reviewing Job Results](#).

You can also use the **zero-touch patching** capability to identify and deploy proper patches for remediating vulnerabilities intelligently. Refer to [Zero-Touch Patch Job](#).

Reference How-to Videos:

[Set up a patch job from the Qualys TruRisk Dashboard](#)

[Use Zero-Touch Prioritized Products to create a hands-off job to patch endpoint systems](#)

[Patch Management Videos](#)

Qualys VMDR TruRisk ProtectIT: Anti-Virus & Anti-malware Protection

Qualys VMDR TruRisk ProtectIT package includes *Qualys Endpoint Protection with Patch Management and VMDR* capabilities. Qualys Endpoint protection consists of *Machine Learning (ML) and Behavior-based Anti-virus* and *Qualys Endpoint Detection and Response (EDR)*. By combining signatures, machine learning models, and behavior technologies, Anti-Virus **blocks** zero-day attacks, ransomware, and phishing. Endpoints are continuously *monitored* and *remedied* for suspicious activity by EDR. EDR captures system activity to *identify* malware indicators of compromise and threats from threat actors. A *single agent* handles real-time incident responses and remediation. You can *detect, prevent, and respond* to attacks throughout their entire lifecycle with Qualys Endpoint Protection.

Refer to the following documentation for detailed steps and explanations.

[EDR Onboarding Videos](#) | [EDR Getting Started Guide](#) | [EDR Online Help](#)

Step 1- Enable EDR and Malware Protection in Configuration Profile

1. Make sure your cloud agents are configured for EDR and malware protection.
Go to the **Cloud Agent > Agents** tab and identify the agent that has EDR enabled.
2. EDR data collection requires this:
 - a. Turn on the EDR module for the profile.
 - b. Turn on the **Enable Malware Protection** for the profile to activate anti-malware.

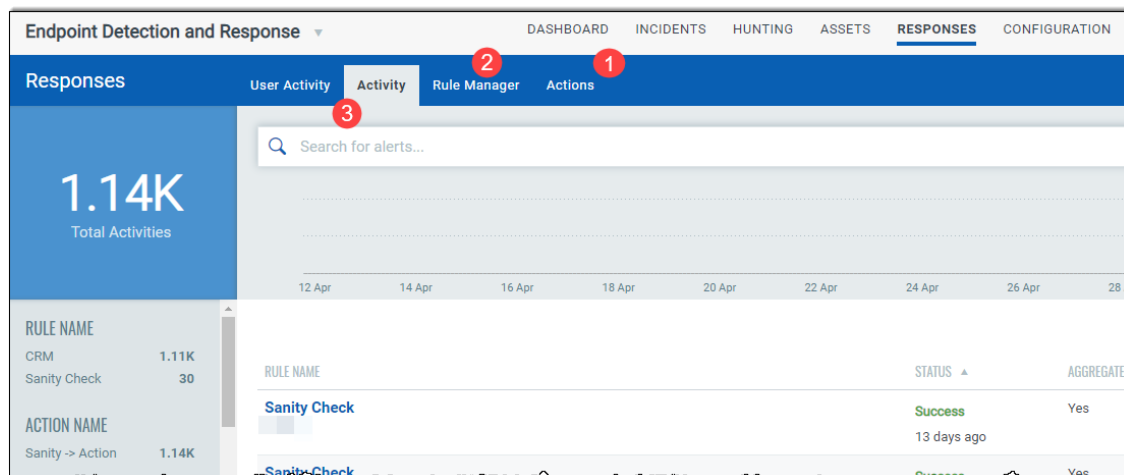
For detailed steps and explanations, refer to [Enable EDR module](#) | [Enable Malware Protection](#)

To activate your already deployed agents for EDR, refer to [Cloud Agent application](#) video.

Step 2 - Configure Rule-Based Alerts for Events

1. Configure EDR to **monitor events** for conditions specified in a rule and send alerts if events matching the condition are detected.
2. Configure a rule action for EDR to **send alerts** when events matching a condition occur. Alerts will be sent to you based on the rule action settings.
3. Specify the conditions for **triggering the rule** and select rule actions to **send the alert** when the rule is triggered.

For detailed steps and explanations, refer to [Configure rule-based alerts for events](#).



Step 3 - View Events and Detection

You can find all detections and events under the Hunting tab. The following remediation actions are available for File, Mutex, Network, and Process events: Quarantine File | Delete File | Kill Process

For detailed steps and explanations, refer to [View Event Details](#).

Reference How-to Videos:

[Activate deployed agents for EDR](#)

[Investigating incidents with Qualys EDR](#)

[Enabling Malware Protection with Qualys](#)

Which VMDR TruRisk package is best for you?

There are probably a lot of questions on your mind. We recommend the following packages based on our research and experience.

You can choose VMDR TruRisk when:

VMDR TruRisk (Vulnerability Management for a Small to Mid-Sized Business)				
CAPABILITY	DESCRIPTION	VMDR TruRisk	VMDR TruRisk FixIT	VMDR TruRisk ProtectIT
Vulnerability Assessment	Comprehensive vulnerability assessment with support for over 70k+ CVEs	✓	✓	✓
Reporting	Standard and custom vulnerability reporting	✓	✓	✓
API Support	Launch Scans, download reports, all through a single unified API	✓	✓	✓
Asset Inventory	Inventory all known & unknown assets across on-prem and cloud	✓	✓	✓
Asset Classification	Automatically classify assets based on OS, manufacturer, application and more. Dynamically tag and organize assets	✓	✓	✓
Threat Intelligence	Identify high-risk vulnerabilities based on best-in-class vulnerability intelligence, and pinpoint impacted assets	✓	✓	✓
TruRisk Prioritization	Prioritize vulnerabilities exploited in the wild by ransomware with TruRisk Prioritization	✓	✓	✓
Scan External Assets	Scan external/Internet-facing assets with a single consolidated solution	✓	✓	✓
PCI ASV Assessment	Scan assets PCI compliance	✓	✓	✓
Configuration Assessment (CIS)/System Hardening	Scan assets for misconfiguration and system hardening based on CIS guidance	✓	✓	✓
SSL Certificate Management	Monitor SSL certificates for expiry. Prevent business outage. Inventory certificates and renew expired certificates	✓	✓	✓
Patch Detection and CVE Correlation	Accurately identify patches to remediate vulnerabilities	✓	✓	✓
Unified Dashboard	Create customizable executive dashboards	✓	✓	✓

You can choose VMDR TruRisk FixIT when:

VMDR TruRisk FixIT (add Patch Automation)				
CAPABILITY	DESCRIPTION	VMDR TruRisk	VMDR TruRisk FixIT	VMDR TruRisk ProtectIT
Patch Operating Systems	Patch Windows, Linux and Mac Operating systems		✓	✓
Automated Remediation	Automate Patch Deployment. Deploy patches based on pre-defined criteria such as TruRisk Score or Real Time Threat Indicators		✓	✓
Custom Remediation	Defined pre and post-deployment scripts before/after deploying patches		✓	✓
Patch Third-Party Applications	Patch 100+ third-party applications		✓	✓
Cloud Based Patching	100% cloud patching from vendor's websites, CDNs: NO VPN required		✓	✓

You can choose VMDR TruRisk ProtectIT when:

VMDR TruRisk Protect IT (add Endpoint Protection)				
CAPABILITY	DESCRIPTION	VMDR TruRisk	VMDR TruRisk FixIT	VMDR TruRisk ProtectIT
Anti-Virus & Ransomware Protection	Block zero-days, ransomware, script-based, and phishing attacks using multi-layered behavior and ML-based malware detection techniques			✓
Incident Response	Incident visualization, root cause analysis and response and remediation workflows			✓
Native VMDR Integration	Identify critical unprotected assets, correlate detected threats to vulnerabilities, patches, and misconfiguration to prevent future attacks			✓
Threat Hunting	Hunt for zero-day threats and search for Indicators of Compromise (IOCs) to identify attack-related behavior			✓