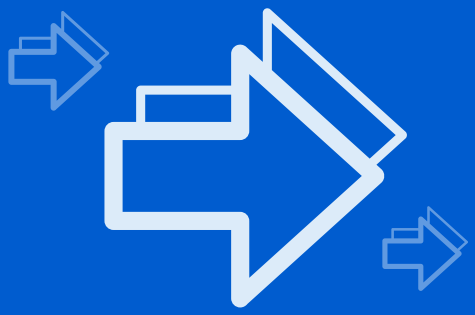
QUALYS®

STEP-BY-STEP GUIDE:

Migrating from McAfee Vulnerability Manager (MVM) to Qualys VM



On October 22, 2015, McAfee announced the End of Life (EOL) for McAfee Vulnerability Manager (MVM) 7.5, and the MVM3200 and MVM2200 appliances. On January 11, 2016, McAfee will no longer sell MVM software or appliances, and full service support for these solutions will end in January 2018 for MVM software, and January 2019 for MVM appliances.

Summary

Now that McAfee MVM has reached the end of its life, it's the perfect opportunity for you to consider evolving your vulnerability management program to the next level. Rather than simply replacing one legacy point solution with another, consider upgrading to best-in-class, cloud-based vulnerability management.

Key benefits include:

- ***Rapid deployment*** – start scanning in minutes, without complicated server and database installations or costly professional services
- ***Broad coverage*** – gain full visibility into all your assets, from every angle – on-premise, internal and external as well as those in private and public clouds
- ***Free online and in-person product training*** – attend product training workshops and earn your Qualys certification without any cost to you

To get you started, we've collected key recommendations from others who have successfully completed this migration.

STEP-BY-STEP GUIDE:

Recommendations

1 Re-Assess Scan Procedures

Use this time to evaluate your existing scan protocols and procedures to determine if they still apply. For example, review the list of ad-hoc scans, decommissioned groupings, "special" reports, and other details of your vulnerability management program to determine if they're still appropriate or necessary. Since you and your team are moving to a new solution, this is the perfect time for a fresh clean start.

2 Schedules and Reporting

Gather all reporting requirements (e.g. PCI, HIPAA, Internal IT Audit, etc.) and extract these from MVM and save. Typically, the key components that you'll need include: Scans, Scan Schedules, Reports. Identify which reports you'll need for historical purposes, and for how long. Run these, and prepare them for exporting out of MVM. Create a list of all reports you'll need to set up in Qualys, so that you'll be prepared once the transition is complete. Finally, review and verify your current scan schedules in preparation for the transition. the transition.

3 Operations and Administration

For operational purposes, make sure that you collect all procedural information that is unique to your environment. Key components to extract include: Users and Administrators, Scan Configurations (in Qualys we call these Option Profiles), and Exceptions (for system vulnerabilities that either can't be fixed or won't be fixed due to critical business requirements or exclusions for machines that shouldn't be scanned). It may also be a good time to verify the relevance and accuracy of these exceptions. You may discover that they are no longer necessary or applicable.

4 Run VMs in Parallel (if possible)

Consider running both solutions in parallel for a specified period of time (e.g. 3 months). Running MVM and Qualys VM in parallel for a short period of time will provide a number of benefits:

- It will give your organization time to familiarize yourself with the new solution as well as set expectations with key stakeholders on the new reports and dashboards that will be coming.
- When you're ready to cut over to Qualys VM exclusively, you'll already have 3 months of historical data for trending and analysis.

5 Integrate and Exercise New Features

Built on a flexible and open architecture, Qualys VM offers APIs so that you can export and correlate your vulnerability data into the other systems in your security infrastructure (SIEMs, IT-GRC, etc.). Additionally, as a multi-functional, extensible, cloud-based platform, Qualys offers security capabilities beyond vulnerability management to enhance your overall security and compliance program. Once you're ready to explore these, contact your Qualys Technical Account Manager for a free, hands-on trial.

Frequently Asked Questions

What servers or databases do I need to license, install and configure to prepare for a Qualys VM deployment?

None. Since Qualys VM is a cloud-based service, there are no additional licenses to purchase, no databases to maintain, and no servers to procure. As soon as you subscribe to Qualys VM, you'll be able to begin scanning immediately, with nothing to install and no significant changes to your infrastructure. As a SaaS provider, Qualys VM handles all database and server administration, tuning and configuration. Your team can focus entirely on what matters most - vulnerability and compliance management.

Additionally, because Qualys is so easy to setup, you'll be able to start scanning without the need to hire costly professional services for the installation. Your Qualys Technical Account Manager is available to assist – at no charge - whenever you're ready to get started. We also offer free and unlimited online and in person training classes to all of our customers, and 24/7 support is always included at no additional charge.

Why can't Qualys import my historical data into its platform?

MVM and Qualys VM use different taxonomies and architectural components. While Qualys offers APIs for integrating data with SIEMs and other security management systems, attempts to import and synthesize disparate vulnerability data is a complex process that offers questionable value or benefit.

If we can't migrate historical data, how will we continue to measure the effectiveness of our vulnerability management program over time?

Look at this change as an opportunity to evaluate your KPIs, determining if they remain an effective measure of your organization's security and compliance goals.

When it comes to security, the current state is always more important than the status of your organization and its assets 6 months ago (or longer). Old vulnerability data is, by its nature, bad and unreliable vulnerability data. Freeing your organization from the limitations associated with bad data provides the opportunity for a fresh start to your security and compliance program.

How can I explain the benefits of this migration to my executive team?

While change in general may often raise concerns, in this case, your executive team will appreciate the following benefits of Qualys VM:

- **Lower CapEx:** No need to procure hardware or purchase additional software licenses. As a SaaS provider, Qualys doesn't require SQL Server, IIS Server or any other foundational components to work.
- **Lower OpEx:** Without the need to maintain databases or servers, you'll be able to reduce overall operating costs. You'll also never need to worry about restoring or repairing corrupted databases, or installing server patches.
- **Increased Efficiency:** Because Qualys maintains the entire underlying infrastructure, your team will be free to focus on improving security and compliance versus laborious and time-consuming systems administration tasks.
- **Free Product Training:** Qualys is pleased to offer free instructor-led training, with hands-on labs, either in person at our global training facilities or online via WebEx. We also offer free attendance to our customers at our annual Qualys Security Conference, which includes informative keynotes, product roadmap overviews, and hands-on training sessions.

Where can I get more information about a Qualys VM deployment?

Please download our **Rollout Guide** to learn how to deploy Qualys VM in your organization.

QUALYS® CONTINUOUS SECURITY

Qualys, Inc. - Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world.
To find an office near you, visit **http://www.qualys.com**