

PRODUCT UPDATE 4.9.1.0 - OCTOBER 19, 2022

MSV 4.10.2.2 contains defect resolutions and a critical security fix. We recommend you apply that update as soon as reasonably possible. If you're unable to upgrade at this time, use the instructions in **Manage User Admin Account** (<https://docs.mandiant.com/home/manage-user-admin-account>) to either set a password for the account or disable the account if it's not being used.

This note is for customers who meet the following criteria:

- Protected Theater is hosting images that use UEFI as the boot method
- Protected Theater is on a version earlier than 4.9.0.0/5.9.0.0 that needs to be updated

Before starting the upgrade, we strongly recommend that you take a snapshot of the PT VM first. Also, take note that that versions prior to 4.10.0.0 are EoS as per **Security Validation Software Version Support** (<https://docs.mandiant.com/home/msv-software-version-policy>), so we also recommend that you upgrade to the latest available Security Validation release.

When UEFI is used as the boot method, Protected Theater versions before 4.9.0.0/5.9.0.0 were continually accumulating snapshots. As of 4.9.0.0/5.9.0.0, only a single snapshot layer is being maintained, with all prior snapshots being folded into that single disk layer. Before upgrading, check the available disk space on the volume storing the PT's images to determine if there's enough free space to successfully perform the upgrade.

To complete a PT upgrade to 4.9.0.0/5.9.0.0, or higher, from a version prior to 4.9.0.0/5.9.0.0:



1. Take a snapshot of the PT VM.
2. Check the number of snapshots & disk space required. To do this,
 - a. Look in the **/opt/apps/verodin/node/images** directory & identify files that have a ten-digit number at the end of their filename. These are the snapshot layers that will get folded together into a single snapshot layer file on upgrade.
 - b. Calculate the disk space required for the upgrade by adding up the file sizes of all the snapshot layers. Round up slightly to ensure a buffer of available disk space.
3. Add disk space, if necessary.
 - a. If the sum total of all snapshot layers (from 1a) is greater than or close to the amount of free disk space remaining on the PT volume holding the images, increase the volume's disk space.
 - b. If the sum total of all snapshot layers (from 1a) is less than the amount of free disk space, continue to the upgrade step.
4. Perform the PT upgrade.
5. Once the upgrade has completed, any disk space added to accomplish the upgrade can be reclaimed.

If you need any assistance with this process, please contact your TSC or CSM.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.9.1.0 of the MSV platform.

General Enhancements

- Exposed SMTP ID of emails sent by jobs in Email Theater
- Actors now collect CrowdStrike Endpoint Security Technology logs from host
- Added Red Hat Enterprise Linux (RHEL) 9 support for Actors

Bug Fixes

- Resolved Report Builder charts time zone configuration issues

- Fixed Report layout issues when Heat Map cells contain long actor names
- Fixed issue with new day selection in Report Builder filter forcing 3-day date window
- Addressed issue with Active Directory groups syncing with Google authentication
- Push Actor NGINX config body size now large enough to support actor update size increase
- Fixed issue with CTTA job queues
- Corrected host CLI action errors for local defender log search
- Paused state integrations now longer support query
- Addressed Windows 10 Endpoint Actors file dependency issue
- Corrected issue with newly scheduled repeating jobs in UI
- Fixed HTTPS/HTTP connection issues failing under certain conditions
- Improved performance of drag/drop actions
- Addressed threat intelligence data load failures in TAAM
- Content pack screen now correctly attributes user performing upload

To download documentation and software (appliance images, installers, and update packages), visit the [Validation Section of the Docs Portal \(https://docs.mandiant.com/home/security-validation-on-prem-and-saas\)](https://docs.mandiant.com/home/security-validation-on-prem-and-saas).