MORPHISEC
Moving Target Defense

What's New in Morphisec Unified Threat Prevention 4.5.3

Introduction

Morphisec Unified Threat Prevention protects organizations against advanced threats, fileless malware, and zero days with the power of Morphisec's patented Moving Target Defense technology. The platform blocks attacks other cyber platforms fail to detect through a deterministic prevention model that does not impact system performance.

Version 4.5 of Morphisec Unified Threat Prevention improves Server and Workload protection, introduces a new set of protection mechanisms and enhances support for Morphisec Guard – Windows 10 native security components integration, in addition to many smaller features.

Highlights of This Version

Server and workload protection

Unified Threat Prevention Platform 4.5 introduces an additional protection capability for critical machines, running Windows Server operating systems. In many cases, critical machines cannot be stopped, even in case of attacks. For these situations, Morphisec Protection Plans now support the ability to define a set of machines, or a set of mechanisms on these machines, as running in a alert-only mode. This mode will use the same protection mechanisms but will not block the attack, instead only report it. The alert will appear in Morphisec attack reports, attack trajectory and dashboards, and the alert-only mode of the Protection Plan will be reflected in the Protector dashboards.

Protection mechanisms

The new version introduces a set of mechanisms that are aimed at protecting from additional, non-in-memory attacks:

- Attack Surface Reduction - Script Execution Notification: The new release notifies when there is a set of malicious call chains initiated by various Microsoft Office products.
- Privilege escalation: Attack chains need to elevate privileges to perform malicious actions. UAC bypass, which is a primary method for performing privilege escalation, is now blocked and reported on.
- Browser Access: The new release blocks the ability to steal credentials from within Microsoft Internet Explorer & Edge browsers using deception mechanisms.

Morphisec Guard

The 4.0 version of Morphisec Unified Threat Prevention introduced a set of capabilities around Windows 10 native security components. This release (4.5) bolsters these capabilities by adding support for security posture. The new release shows the state of the following as widgets in the main dashboard:

- Runtime Protection – shows machines with active Microsoft Defender AV
- Runtime Protection Updates – shows machines with updated Microsoft Defender AV definitions
- Drive Encryption – shows machines with Microsoft BitLocker enabled

Dashboards

The Security Center dashboards received a series of enhancements as well as optimization for smaller resolution screens such as tablets.

Dashboards were updated to consolidate all threat information in a single view:

- Alert-only and prevented threats
- Windows and Linux protection
- Morphisec protection and Microsoft native security information (in Morphisec Guard only)

Main dashboard:

- Updated the Protector status view and added new widgets to better reflect the overall protection posture

Protection plans:

- It is now possible to delete applications from the Protection plan
- The Protection plan has a new set of new protection mechanisms in the advanced section. If you are upgrading from a previous version, these mechanisms will be turned off in the client default Protection plan, since an upgrade does not modify plans that are being used. However, we recommend turning these on.
- The following collaboration applications were added to the default Protection plan in 4.5: GoToMeeting, Webex, Zoom, Slack, Microsoft Teams, and Skype. ***When upgrading to 4.5, we recommend adding these applications to your default plan.***

Protector dashboard:

- Additional filters were added to facilitate improved search capabilities

Email Notifications

You can now receive email notifications on threats by setting your preference in the Settings pane.

Actionable insights are now included in the body of the email threat notification for threats prevented by Morphisec Guard: Attack Name, Category, Severity, Attack Module, Application, Username, Machine Name, and Operating System.

In addition, you can select

- which type of threats to be notified about
- multiple email addresses to receive notifications
- the frequency of your notifications (real-time or aggregated)

Reports and auditing

This version introduces many enhancements in the Threats and Executive reports, as well as additional auditing features.

Threats report

- Improvements to the look and feel of the threats report
- Threats reports now include classification information

Executive reports

Implemented improvements based on customer feedback

Auditing

The following actions are now audited:

- Assigning and removing Protectors from Troubleshooting plans
- Enabling alert-only properties per feature or per machine in Protection plans
- Enabling and disabling features in Protection plans

Anti-Tampering

The Protection service was hardened and cannot be disabled by domain admins.

SIEM Parsers

Morphisec offers SIEM parsers which enable you to view Morphisec events in your SIEM either by using one of the following options or adding one of these to your existing SIEM:

- IBM QRadar
- McAfee ESM
- Splunk SIEM
- HP ArcSight
- LogRhythm

Fixed Issues

Installation and Startup

Upgrade: SIEM and LDAP certificate information were not retained upon upgrade or reinstallation.

Upgrade: Selecting *Use Existing Data* in the *Root User* screen would not the installation proceed.

Startup: High memory usage on system startup when the system contains a large number of attacks.

Sometimes the Solr service would not start automatically after server machine restart.

Fixed an issue regarding the occasional loss of Protector information during upgrade, archiving, or database restoration.

Dashboards

Settings: Popup messages in the Settings pane would hide some of the settings.

Settings: There was no input validation for incorrect proxy ports.

Protectors: Fixed problematic message when exporting Protectors.

Threats: Number of detected threats displayed was incorrect, although the full threat list was presented.

Threats: Morphisec threat log would not open in a specific sequence.

Protection Plans: Adding a new application to the application list did not display it without refreshing the list.

Protection Plans: Timeouts in the Advanced section were requested in seconds when they were actually defined in minutes.

MSSP: Success popup messages were missing.

Protection

Fixed a compatibility issue with CyberArk EPM

Fixed a compatibility issue with AutoCad

Fixed a compatibility issue with Symantec AV

Reports

Executive Reports: When the customer was not connected to the Morphisec Cloud, the Global Trends section of the Executive Reports was correctly empty, but without an error message.

Executive Reports: Some legend values were missing or unclear in some of the charts.

Executive Reports: Subject of mail containing the executive report did not include report dates.

Executive Reports: Styles were fixed.

Threats Report: Exact threat time was missing in Threats reports.

Threats Report: Could not download reports that contained over 150 threats.

Threats Report: Could not download the report after upgrade from Morphisec Management Server 3.0.0 to 4.5.0.

Server

Improvements to Management Server performance and scalability

Microsoft Defender for Endpoint (Formerly Microsoft Defender ATP)

Morphisec threat events would not appear in the Microsoft Defender for Endpoint Security Center due to an API change.

Microsoft Defender Visualization

Sometimes Microsoft Defender runtime protection events would appear with a wrong timestamp.

SIEM

Syslog events sent over TCP or SSL were not received by the SIEM server.

Notifications

Fixed the end user notification popup being placed in the wrong location on the screen.

An incorrect description appeared in the body of the email threat notification.

Some fields in the email threat notification were duplicated.

Known Issues

Deployment

Protector: BeyondTrust Privileged Remote Access running on Windows10 prevents all installers requiring msiexec from running, including the Morphisec Protector installer. **Workaround**: whitelist the installation file in the BeyondTrust GPO.

Protector: AVG version blocks the Protector installation, erroneously identifying it as an idp.alexa.51 virus.

Protector: If the tmp directory does not have execution privileges, the installer will not run. **Workaround:** make sure you run the installation from a folder that has execution privileges.

Protector: If the required .net version does not exist on the endpoint machine, and there is no internet connectivity for downloading the version, installation ends prematurely.

Protector: The Protector ignores an auto-configure Proxy and connects directly to the Management Server if that connectivity is available.

Protector: When installing or upgrading the protector via a current logged in user session, if there are other users who are currently logged in to the same computer, they will not see the protector tray icon once the install/upgrade is complete. Only the current user will see the new tray icon. For the other users to see the new tray icon, they will need to login again. *It is important to note that all users are protected nonetheless, regardless of the tray icon showing in the system tray or not.*

Apache Solr: The Solr data folder cannot contain any spaces.

PostgreSQL: Morphisec Management Server cannot connect to a PostgreSQL server running outside the LAN if the firewall rules are not set up correctly or PostgreSQL is not configured to allow outside-LAN connections. See the Morphisec Endpoint Server Installation and Administration Guide for further instructions.

PostgreSQL: If the Morphisec Management Server cannot connect to the designated PostgreSQL instance, it fails to start. If that happens, see the relevant service log for additional information. All logs can be found under the installation folder, under the specific service sub-folder.

Server: When trying to roll back a Management Server installation, sometimes the rollback fails. **Workaround:** Stop the Management Server service manually and rerun the operation.

Server: Morphisec Security Center cannot be installed in the following special Windows folders: Desktop, Documents, Downloads, Videos, Music, and Pictures.

Protection

Kingsoft Webshield and Morphisec Protector cannot run on the same computer at the same time. To enable Morphisec Protector to run effectively, Kingsoft Webshield must be disabled.

The Facebook and Facebook Messenger application downloaded from Microsoft Store cannot be protected by Morphisec Protector.

It is recommended that the installer application not be protected by Morphisec Protector when running the installation process of several security tools. **Workaround:** Do not include the installation process in your protection plan.

Emsisoft erroneously identifies the Protector installation as malicious. **Workaround:** From the Emsisoft console, enable the Protector installation to run, or whitelist it from the Emsisoft console.

When running FSecure DeepGuard alongside Morphisec Protector, you must disable its exploit detection functionality.

Morphisec Protector cannot run alongside Cisco AMP when AMP ExPrev (Exploit Prevention) is enabled. **Workaround:** Disable Exprev in Cisco AMP before running the Morphisec Protector.

Morphisec Protector sometimes cannot run alongside the 2002 release of QBS Software WRQ Reflection. **Workaround**: Run a newer release of the software.

When running TrendMicro OfficeScan12 alongside Morphisec Protector, **you must disable its Anti-Exploit Protection.**

In some rare cases, Morphisec cannot run alongside Sophos Hitman Pro. **Workaround**: Disable *Mitigate exploits in vulnerable applications: Protect office applications* in Hitman Pro.

McAfee Endpoint Protection sometimes flags the Morphisec Protector as malicious. **Workaround**: Whitelist Morphisec processes in the McAfee console.

AVG AV sometimes blocks the Protector installation. **Workaround**: Whitelist Morphisec Protector installation process in the AVG console.

If the Protector is installed in a folder other than a Program Files subfolder, it cannot protect Microsoft Applications unless you enable editing for the installation folder. **Workaround:** Install Morphisec Protector in Program Files folder.

Updating applications on Windows 8 while they are being protected by the Protector may cause them to crash once the update process is done. **Workaround:** Restart the applications after they are updated.

Some music applications running on Windows 8 may close the first time they run, when protected by Morphisec. **Workaround:** rerun the applications.

The MorphisecInstaller executable is identified as suspicious by Symantec Norton Sonar. **Workaround:** Mark the MorphisecInstaller as safe.

Kaspersky AV prevents any runtime protection from protecting lsass.exe.

Morphisec Protector recognizes Turbo Virtual Machine as malicious.

Morphisec Protector recognizes old and outdated versions of Nova PDF as vulnerable and malicious.

Morphisec Protector cannot be installed when Comodo AV is running.

Morphisec Protector recognizes VSDC free video editor as malicious.

On Windows 7, 32-bit applications that are protected by Morphisec cannot have the EMET Export Address Table Access rule turned on.

Some applications that use the VMProtect packer may be viewed as malicious by Morphisec. **Workaround:** Exclude these applications.

Emsisoft Anti-malware solution detects the Protector installation as malware.

Sophos Intercept X version 2.2.1 prevents the Mozilla Firefox browser from running if it is protected by Morphisec Protector.

When the CrowdStrike agent runs alongside the Morphisec Protector, it sometimes interferes with Morphisec protection. **Workaround**: Add exclusions for the Morphisec services in the CrowdStrike console.

Bluekeep attacks are always stopped, and threats information is sent to the Management Server, but sometimes the user notification is missing.

VBScript Blocking functionally blocks actions that are performed by untrusted VB scripts. If an action performed by a VBScript cannot run but should, you must add the website running the script to the Internet Explorer Trusted Sites zones on the relevant machines.

Dashboards

Threats: For threats on Google Chrome and Mozilla Firefox browsers, the URL is not shown in the Threats table or the Single Threats dashboard.

Logs: Attack log field values are truncated over a certain length. However, the rest of the log can be viewed.

Logs: There may be missing data in attack logs for Excel attacks when files over 10MB are loaded into Excel.

Logs: When exporting attack dumps, sometimes executable signatures do not get exported properly. This does not impact the rest of the log.

Logs: Parent process exectuable_signatures_ss will show up as empty if TrendMicro was running on the protected machine.

Main dashboard: The Threats graph can be viewed for the last 14 days at most. To view a longer time period, select the Threats dashboard.

Protectors: Sorting Protectors by license type does not show all Protectors, if there are Protectors from versions 3.0.1 or older.

Threats pane: The username in threats was fixed from *Domain/user* to *Domain\user* to be consistent with the path convention used in Microsoft threats. However, if you have a mix of old and new Protectors, you would have entries in both path conventions.

Reports

Executive reports (**for MSSP customers only**) - unable to generate a report containing data of more than three customers.

Executive reports: Month and Year are missing from the email subject sent for monthly reports - making all the emails look the same with no distinguishing details.

Executive reports: Legend in Protector by Operating System graph sometimes shows partial OS names.

Threats reports: Downloaded daily reports and scheduled daily reports are for different 24-hour periods.

Threats reports: this report can display up to 1,000 threats in a single report.

Microsoft Defender Visualization

In run-time Defender events, username is sometimes missing from the threat event description.