What's New in Morphisec Unified Threat Prevention 3.5

Introduction

Morphisec Unified Threat Prevention provides earliest-stage, proactive threat prevention that promotes organizational efficiency and reduces risk. Morphisec's patented Moving Target Defense technology prevents attacks other cyber platforms fail to detect, using a deterministic prevention model that does not impact system performance.

Version 3.5 of Morphisec Unified Threat Prevention delivers unprecedented visibility, including vastly enhanced attack analytics, along with increased protection.

HIGHLIGHTS OF THIS VERSION INCLUDE:

- An integration with Microsoft Windows Defender AV
- New attack trajectory visualization and drilldown
- Expanded attack classification capabilities
- Extended prevention mechanisms
- Security and performance enhancements
- Revamped dashboards
- Expanded Attack Logs

MS Windows Defender AV integration

A cornerstone of the latest version is the integration with Microsoft Windows Defender Antivirus (AV), which allows enterprises to better leverage the embedded security features in the Windows 10 operating system. Morphisec Security Center now provides a consolidated view of all attacks on the endpoint, including real-time attacks and severity levels prevented by both Morphisec and Windows Defender AV in a single, centralized location.

Attack Trajectory Visualization and Drilldown

The Attack Details Dashboard now displays a graph of the full attack trajectory along with detailed data including user, attack type, attack techniques, attacked processes and severity level. The trajectory shows all attack stages, beginning with infiltration and pre-execution. Selecting a stage displays relevant information such as signature, file path, integrity level and any command line instructions.

Expanded Attack Classification Capabilities

Morphisec categorizes prevented attacks by type and, when available, by name, for use in attack dashboards and reports. This information is generated by the classification engine, a feature of the Management Server. This release includes significant improvements to the classification engine.

- Newly identified attacks: The updated engine contains additional detailed information about the attacks.

- Online attack classification updates: The classification engine connects to the Morphisec Cloud to download new classification information on a regular schedule in order to ensure that dashboards and reports present the most current attacks and severity scores are based on the most up-to-date set of data.

- Automatic and manual attack reclassification: When new classification information becomes available, the Management Server automatically reclassifies existing attacks that were previously unclassified. The user may also re-classify manually to receive updated information immediately.

- Filtering: Users are now able to filter the attack dashboard by attack name and category.

Extended Prevention Mechanisms

- Process spoofing: Morphisec Unified Threat Prevention can now protect child processes even when parent processes are spoofed.

- Restricted zones: Morphisec Unified Threat Prevention now extends its morphing capabilities to morph applications originating in restricted/internet zones on Windows 7 regardless of whether they appear in the Protection Plan.

Security and Performance Enhancements

- Encrypted communications: The communication between the Management Server and the Apache Solr repository is now encrypted, allowing attack logs to be safely distributed in an unprotected environment.

- Performance: Management Server enhanced performance for better scalability.

Revamped Dashboards

The Morphisec Security Center dashboards have been fully revamped to deliver better visibility, improved usability, and more control.

- UI enhancements: The main dashboard has been redesigned for increased at-a-glance visibility with a clearer, more visually distinct layout.

- Status clarification: Protection status names in the main dashboard and the Protector dashboard have been changed to be clearer and more precise.

- VDI upgrades: We have improved VDI lifecycle management by allowing the user to define an organizational offline timeout, after which pooled VDIs will be removed from the Protector dashboard.

Expanded Attack Logs

New fields have been added to the attack log to provide additional critical information for quicker analysis and remediation in critical attack situations (see the user guide for exact descriptions). These include:

- PowerShell command line was added for ransomware attacks.

- The original file name is included when the process name was changed.

Fixed Issues

Installation

When the assigned Active Directory user had special characters in the password, the Management Server installation would fail.

Dashboards

Protectors: After upgrading the Management Server to a newer version, on a different machine, some of the Protectors were not shown in the Protector dashboard.

Attacks: An attack report that was generated for a duration of a single day would be empty.

Attacks: Some attacks would be incorrectly classified as remote threat injection attacks.

Plans: Adding a Protector to a Troubleshooting plan, uninstalling the Protector and reinstalling it would result in the Protector machine name not showing in the Troubleshooting plan Protector list.

Settings: Switching between tabs in the Settings page would always display an Unsaved Changes message, even if there were no changes.

Settings: In the User settings, usernames could not contain spaces.

Protection

Fixed a compatibility issue with Proxy Pro

Morphisec Protector could not run alongside BitDefender anti-ransomware

Known Issues

Installation

Protector: BeyondTrust Privileged Remote Access running on Windows10 prevents all installers requiring msiexec from running, including the Morphisec Protector installer.

Protector: Installing flash player with BeyondTrust shows the installer as a threat.

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.

Server: The Solr data folder cannot contain any spaces.

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.

Protection

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 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.

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. To work around this issue, 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.

Running ThinkCell 8 build 25160 32-bit on Windows 10 causes PowerPoint to hang, if protected by Morphisec ETP. Workaround: Update to ThinkCell 9.0.26.806.

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 (EAT Access filtering, EAF) turned on.

Some applications that use the VMProtect packer may be viewed as malicious by Morphisec ETP. 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.

Bluekeep attacks are always stopped, and attack 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 tperformed 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

Attacks: For attacks on Google Chrome and Mozilla Firefox browsers, the attack URL is not shown in the Attack table or the Single Attack dashboard.

Protector: MS Windows Server 2019 is identified as 2016 in the OS column.

Protector: If a machine underwent an upgrade, a Protector appears twice, once with each operating system.

Protection Plans: Uninstalling a Protector does not remove it from a troubleshooting plan if it was associated with one.

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

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

Protection Plans: There is no warning in the Management Dashboard when changing a Protection Plan name to a name of a plan that already exists.

Login: When running the SAML integration, the dashboard session times out every 30 minutes regardless of user activity

Reports

Report mail schedule does not take daylight saving time into account

Deployment

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.

Active Directory: The Management Server cannot be configured to connect to Active Directory using TLS with a certificate, only without one.

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

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.