OPSWAT.

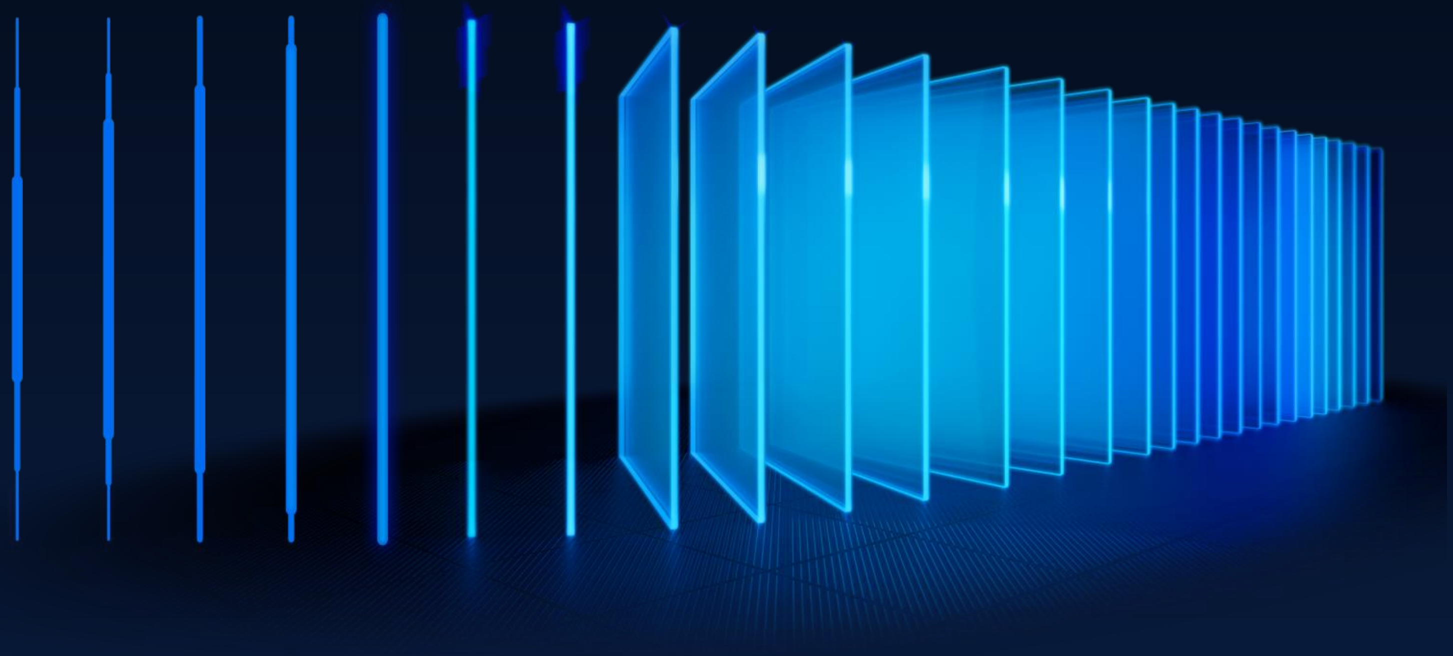
SDK News

MetaDefender Endpoint Security SDK Update

September 2025

Announcement Date

2025/09/09



Contents

MetaDefender Endpoint Security SDK Release Announcement
September 2025

Please review the Required Actions in section 3 that you need to take soon.

1 – What's New?

We are thrilled to unveil the latest updates to the MetaDefender Endpoint Security SDK this month. Get ready to supercharge your endpoint protection solutions with expanded support for more products and some new, exciting features. Build stronger defenses with advanced capabilities that integrate seamlessly into your products. Prepare for an epic upgrade that'll take your security to the next level.

1.1 FetchRemoteData Method for Linux package manager repository refresh

NEW FEATURE, LINUX, ENGINE UPDATE NEEDED, CODE CHANGE

In certain Linux distributions, patch management tools depend on up-to-date package repository metadata to accurately detect and apply updates. While our existing methods (such as GetMissingPatches, InstallMissingPatches, etc.) already support patching workflows, a repository refresh may be required beforehand in certain environments to ensure accurate results.

To better support this, we're adding a new method: FetchRemoteData. This method allows your Agent to explicitly refresh the package manager's repository data before invoking patch-related methods.

The initial release will support Zypper, and is expected in the October feature release. Broader distribution support will follow in future updates.

This enhancement improves visibility and control in Linux patch management—especially in environments where repository freshness impacts accuracy.

1.2 Differential Update for Windows Update Offline data

NEW FEATURE, ANALOG PACKAGE, ENGINE UPDATE NEEDED, CODE CHANGE

In the August release, the SDK introduced a new feature that enables customers to distribute smaller Windows Update Offline datasets to endpoints using a differential update mechanism.

This feature includes two new Analog packages, analogv2.zip and analogv2_baseline.zip, which contain the files wuo_baseline.dat (in analogv2_baseline) and wuo_delta.dat (in analogv2). These files allow customers to implement differential updates by initially distributing the baseline file to the endpoints. After that, for up to one year, customers will only need to distribute the smaller wuo_delta.dat file to keep the Windows Update Offline data up to date.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

1.3 Change to the value format of sdk_version inside the checksums.json file for macOS

NEW UPDATE, MAC, DATA UPDATE NEEDED, CODE CHANGE

In the August release, the value format of the sdk_version field in the checksums.json file of the macOS package was updated to align with the format used in the Windows and Linux packages. With this update, the sdk_version value in the macOS checksums.json file will no longer use an underscore (_) as a delimiter. Instead, a dot (.) will be used to separate version components.

For example: “sdk_version”: “4.3.4239.0”

1.4 New option for GetLatestInstaller method

NEW FEATURE, ALL PLATFORM, ENGINE UPDATE NEEDED

We’ve expanded the flexibility of the GetLatestInstaller method by introducing a new option for the download parameter: download=2.

Using this option, GetLatestInstaller method will return the patch_id only. No installer download and no download URL are included.

This update allows you to select the most appropriate workflow for your patching and compliance needs.

1.5 Version-Specific Patching for 3rd-Party Applications

ENHANCEMENT, ALL PLATFORM, ENGINE UPDATE NEEDED

We’re excited to announce the availability of version-specific patching for third-party applications across Windows, macOS, and Linux.

With the new optional requested_version field in the InstallFromFiles method, you can ensure only the intended version is installed, avoiding unexpected upgrades.

Our SDK performs strong verification using hash validation, file version extraction, etc. If a mismatch or unsupported lock occurs, clear error codes provide immediate feedback.

This update gives customers more control, reliability, and transparency in patch management.

2– Upcoming Changes

2.1 Non-security Microsoft patch support

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED, CODE CHANGE

In the September release, the SDK will be able to detect and install Microsoft non-security patches when using the Windows Update Offline functionality.

Currently, the Microsoft categories supported by the SDK are Security Updates, Service Packs, and Update Rollups.

With this update, the Microsoft categories we will be adding are Regular Updates and Critical Updates.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

2.2 Real-time monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

In Q4-2025, the SDK will provide **Real-time monitoring** on Mac operating systems. Unlike the current compliance checks, which are on-demand audits, real-time monitoring is dynamic, adapting to live events and rule changes as they occur.

More details will be provided in the coming months regarding which compliance statuses will be supported in this first phase.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

2.3 Support for the Windows 10 Extended Security Updates (ESU) program

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

After October 14, 2025, Microsoft will no longer provide security patches, feature updates, or technical support for Windows 10. Windows 10 systems will still function, but become progressively vulnerable to security threats and software compatibility issues.

Therefore, Microsoft is introducing the Windows 10 Extended Security Updates (ESU) program, which gives customers the option to receive security updates for PCs enrolled in the program.

To extend support for Windows 10 and ensure the MDES SDK remains compatible with future updates of Windows 10, we have decided to continue supporting Windows 10 via the Windows 10 Extended Security

Updates (ESU) program. This support will be applied to devices running Windows 10, version 22H2 with KB5046613, or a later update installed, and having an active ESU subscription.

2.4 Track EDR/XDR agent's last connection time with GetAgentState method

ENHANCEMENT, ALL PLATFORM, DATA UPDATE NEEDED

We're excited to share that GetAgentState method will soon include a new field: last_connection_time_to_server.

This enhancement provides visibility into the last time an EDR/XDR agent successfully connected to its server.

The new information is included in the response automatically; no changes are required to your existing API calls.

2.5 Enhanced Installer Verification with InstallFromFiles

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We're enhancing the InstallFromFiles method to support passing an expected SHA-256 hash for installer verification. If the installer's hash does not match, the SDK will now return a WAAPI_ERROR_HASH_MISMATCH error, ensuring greater integrity and security during patch installations.

This enhancement will be available on Windows first, with Linux and macOS support coming in later releases.

3 – Required Actions

3.1 CVE-2025-0131

VULNERABILITY, WINDOWS

An incorrect privilege management vulnerability in the OPSWAT MetaDefender Endpoint Security SDK used by the Palo Alto Networks GlobalProtect™ app on Windows devices allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY\SYSTEM. However, execution requires that the local user also successfully exploits a race condition, which makes this vulnerability difficult to exploit.

To address CVE-2025-0131, please upgrade your MDES SDK to version 4.3.4451 or later.

3.2 We moved the OesisPackageLinks.xml behind the VCR gateway

SECURITY UPDATE, VCR GATEWAY

Starting December 31st, 2024, the OesisPackageLinks.xml file are relocated behind the VCR Gateway for enhanced security, replacing its currently public location.

Since September 1st, 2024, the file can be accessed via the VCR Gateway. You can download the file by following these steps: copy and paste this URL: https://vcr.opswat.com/gw/file/download/OesisPackageLinks.xml?type=1&token=<authorization_token> into your browser and replace **<authorization_token>** with your unique token. If you don't have a unique token, please contact support.

This update ensures continued and secure access, and users should have updated their systems to accommodate this change.

3.3 End of Support for AppRemover package with the old engine on macOS

END OF SUPPORT, MAC

As we have refactored the AppRemover module on macOS to provide a more optimized and streamlined experience, two packages of the AppRemover module on macOS are being maintained on the My OPSWAT Portal: AppRemover OSX and AppRemover OSX V2.

Starting January 1, 2026, the OSX package will be removed. We recommend upgrading to AppRemover OSX V2 to ensure your system receives all new updates and comprehensive technical support for the AppRemover module.

3.4 End of Support for Windows 7 & Windows 8

END OF SUPPORT, WINDOWS

After careful consideration, support for Windows 7 and Windows 8 (server versions included) will be removed from the SDK beginning January 1st 2027 (one year later than previous planned).

To ensure security, compatibility, and optimal performance with MDES SDK, we recommend upgrading endpoints to a supported Microsoft operating system.

3.5 Behavior change in the Installer Signature Check feature

BEHAVIOR CHANGE, ALL PLATFORM, CODE CHANGE

Starting November 1, 2025, a behavior change will be applied to the Installer Signature Check feature to enhance security maturity. When the digital signature of an installer is checked during the patching process:

- (no change) If the installer's digital signature is valid and passes the check, the installer will be verified by the SDK, and the patching process will continue as normal.
- (no change) If the installer's digital signature is invalid and fails the check, an appropriate error message will be returned, and the installation process will be aborted.
- (NEW) If the installer's digital signature is missing, an appropriate error message will be returned, and the installation process will also be aborted.

Tips: If you receive an error due to a missing or invalid digital signature, you can use the skip_signature_check flag of the InstallFromFiles method to bypass the Installer Signature Check feature.

4 – Detailed SDK Information

This is just the tip of the iceberg! You can view all the supported applications on our support charts:

4.1 Windows Support Charts

4.2 Mac Support Charts

4.3 Linux Support Charts

4.4 SDK API Documentation

5 – Contact

Are you a customer and have questions about this list? Please contact our trusted support team at opswat-support@opswat.com.

OPSWAT.

OPSWAT is a global leader in IT, OT, and ICS critical infrastructure cybersecurity, and for the last 20 years has continuously evolved an end-to-end solutions platform that empowers public and private sector organizations with the critical advantage needed to protect their complex networks and ensure compliance. OPSWAT solves customers’ cybersecurity challenges around the world with zero-trust solutions and patented technologies across every level of their infrastructure, securing their networks, data, and devices, and preventing known and unknown threats, zero-day attacks, and malware.

For more information visit
www.opswat.com