OPSWAT.

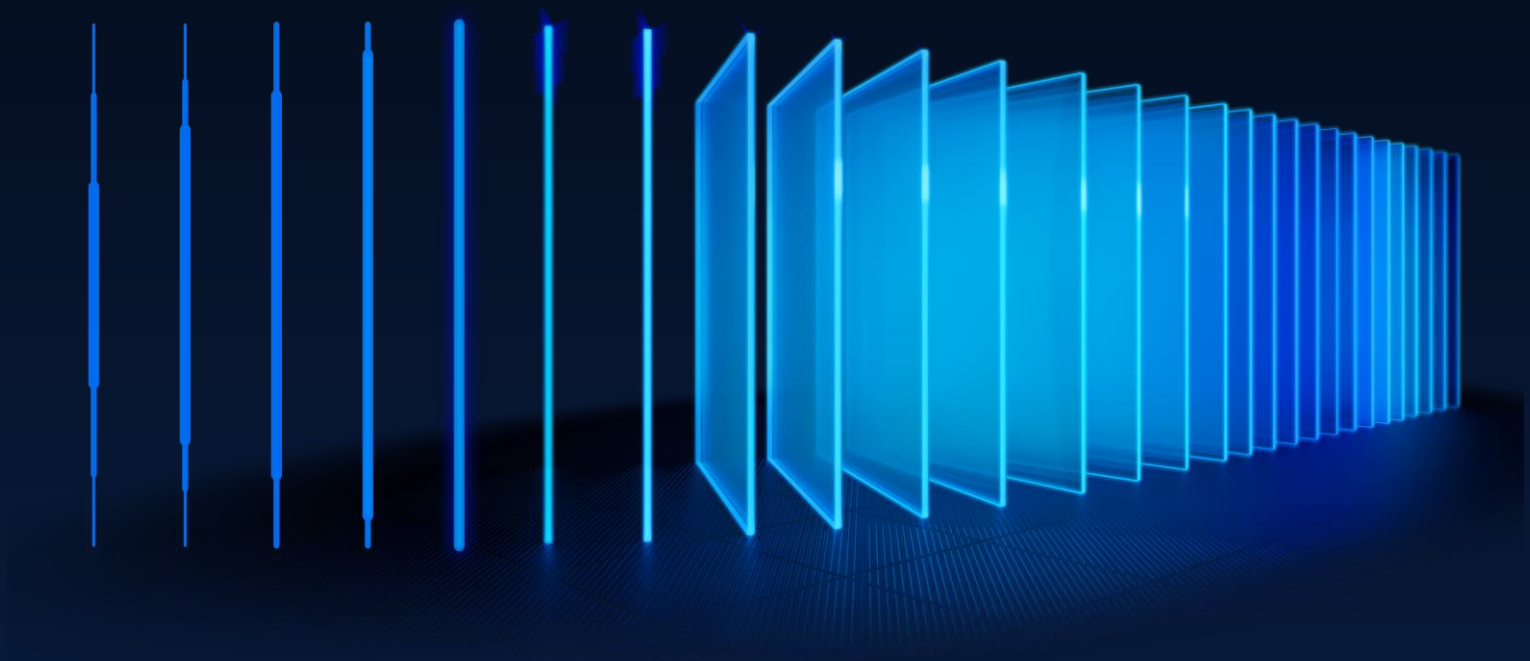
# SDK News

## MetaDefender Endpoint Security SDK Update

August 2025

Announcement Date

2025/08/12



OPSWAT.

# Contents


**SDK News** ..... 1

MetaDefender Endpoint Security SDK Release Announcement August 2025 ..... 3

1 – What's New? ..... 3

1.1 V3V4 Adapter now using libc++ instead of libstdc++ ..... 3

1.2 Introduce new fields in the Server data in the Analog package ..... 3

1.3 New value for requires_reboot field in patch_aggregation.json file ..... 4

1.4 Introduce new patch-related information in GetLatestInstaller ..... 4

1.5 Track WUA service Startup Type with new startup_type field ..... 5

1.6 New parameter force_install added to improve installer reliability ..... 5

1.7 Clearer file names for Windows AppRemover downloads ..... 5

1.8 Deprecation Notice: Eliminate - Method ID: 40002 ..... 6

2– Upcoming Changes ..... 7

2.1 FetchRemoteData Method for Linux package manager repository refresh ..... 7

2.2 Non-security Microsoft patch support ..... 7

2.3 Realtime monitoring on macOS ..... 7

2.4 Differential Update for Windows Update Offline data ..... 8

2.5 Update the value format of sdk_version inside the checksums.json file on macOS ..... 8

3 – Required Actions ..... 9

3.1 CVE-2025-0131 ..... 9

3.2 We moved the OesisPackageLinks.xml behind the VCR gateway ..... 9

3.3 End of Support for AppRemover package with the old engine on macOS ..... 9

3.4 End of Support for Windows 7 & Windows 8 ..... 10

3.5 Behavior change in the Installer Signature Check feature ..... 10

4 – Detailed SDK Information ..... 11

4.1 Windows Support Charts ..... 11

4.2 Mac Support Charts ..... 11

4.3 Linux Support Charts ..... 11

4.4 SDK API Documentation ..... 11

5 – Contact ..... 11

# MetaDefender Endpoint Security SDK Release Announcement
# August 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 projects. Prepare for an epic upgrade that'll take your security to the next level.

### 1.1 V3V4 Adapter now using libc++ instead of libstdc++

ENHANCEMENT, MAC, LIBRARY UPDATE

We're excited to announce that all Mac V3V4 Adapter libraries are now officially built using libc++ instead of libstdc++. This shift will bring better support for modern C++ standards, faster compilation, and better optimizations.

You will need to change your compile process for the macOS to add support for the libc++ library.

### 1.2 Introduce new fields in the Server data in the Analog package

NEW FEATURE, ANALOG, DATA UPDATE NEEDED

We introduce new patch-related information that contains hash string of patches in the server files of Analog package as follows:

In patch_system_aggregation.json:

```
"analog_id": {
    ...
    "download_link": {
        ...
        "sha1": <string>
    },
    "optional": <bool>
    ...
}
```

In patch_aggregation.json:

```
"analog_id": {
    ...
    "download_link": {
        ...
        "sha256": <string>
        },
    ...
}
```

## 1.3 New value for requires_reboot field in patch_aggregation.json file

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

Due to the specific behavior of certain products that require updating the Microsoft Visual C++ Redistributable, two different restart scenarios may occur:

- If the machine already has the up-to-date version of Microsoft Visual C++ Redistributable, the installation of the target product does not require a restart.
- If the machine has an outdated version of Microsoft Visual C++ Redistributable, the installation of the target product does require a restart.

This behavior impacts how the MDES SDK handles the requires_reboot field. Since this condition is environment-dependent and cannot be predicted, we are introducing a new value called "conditional" to represent such cases. The "conditional" value allows the SDK to recognize and respond appropriately to these dynamic restart requirements.

## 1.4 Introduce new patch-related information in GetLatestInstaller

NEW FEATURE, DATA UPDATE NEEDED

We introduced new patch-related information that contains vendor name, description, required restart information of patches in the json out of GetLatestInstaller method as below:

```
result: {
  ...
  "description": <string>,
  "vendor": <string>,
  "reboot_required": <bool>,
  "optional": <bool>
}
```

## 1.5 Track WUA service Startup Type with new startup_type field

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED

The GetAgentState output now includes a new field: startup_type — available for Windows Update Agent (WUA) only. This numeric field reflects the startup type of the wuauserv service (responsible for Windows Update), based on the standard defined by Microsoft's ServiceStartMode.

If the value is invalid or falls outside the expected range, it will return -1, indicating an unknown startup type. This enhancement offers better insight into WUA behavior and configuration across endpoints.

## 1.6 New parameter force_install added to improve installer reliability

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED

We've introduced a new optional parameter, force_install, in the InstallFromFile method input to address specific installer execution issues— hang or fail to execute due to Windows Integrity Level restrictions.

When set to true, force_install enables the SDK to take additional steps to allow trusted installers to run successfully in environments where strict security settings may otherwise block execution. By default, this flag is false to maintain secure behavior.

Use this option **only when you trust the installer source.**

## 1.7 Clearer file names for Windows AppRemover downloads

ENHANCEMENT

We've updated the file naming on MyOPSWAT download portal to clearly indicate the package type — [Native Package] or [V3V4 Adapter Package] — making it easier to find the right build at a glance.

## 1.8 Deprecation Notice: Eliminate - Method ID: 40002

DEPRECATION

We'd like to inform that the API method 40002 - Eliminate, is now deprecated and will be removed in a future update.

The method will remain temporarily available but will no longer receive updates or enhancements. While it still works for now, we recommend planning for its removal in a future release and migrating to supported alternatives.

OPSWAT.

# 2– Upcoming Changes

## 2.1 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 developing a new method: FetchRemoteData. This method allows users to explicitly refresh the package manager's repository data before invoking patch-related methods.

The initial release will support Zypper, and is expected next month. 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.

## 2.2 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.

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**

## 2.3 Realtime monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

This autumn, 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.

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

## 2.4 Differential Update for Windows Update Offline data

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

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

This feature will include two new Analog packages, named analogv2.zip and analogv2_baseline.zip, which contain the new files wuo_baseline.dat (in analogv2_baseline) and wuo_delta.dat (in analogv2). These files allow customers to implement differential updates by initially distributing both files 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**

## 2.5 Update the value format of sdk_version inside the checksums.json file on 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 will be 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”

OPSWAT.

# 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

Starting January 1, 2026, support for Windows 7 and Windows 8 (server versions included) will be removed from the SDK. 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