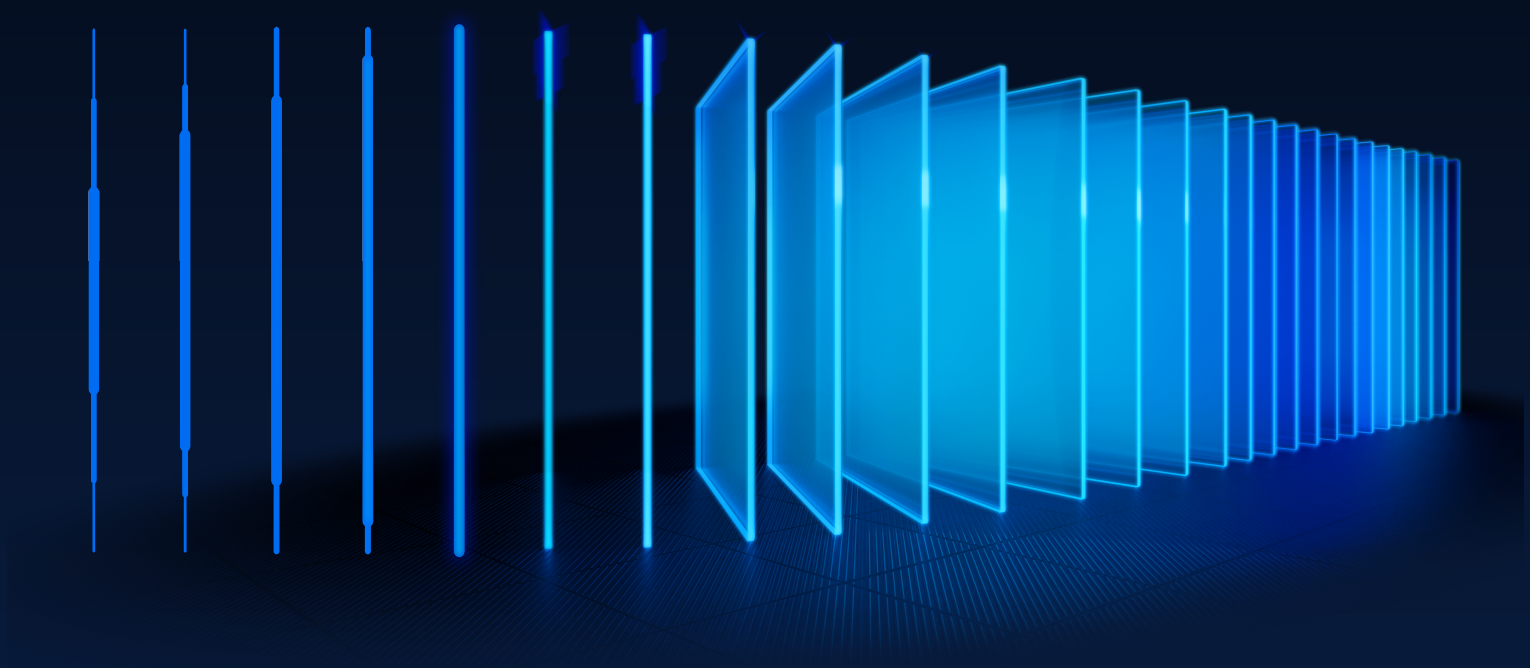
OPSWAT.

# SDK News

## MetaDefender Endpoint Security SDK Update

June 2025

| | |
|---|---|
| Announcement Date | 2025/06/10 |
| Document Version | 1.0 |



OPSWAT.

# Contents

OPSWAT.

# MetaDefender Endpoint Security SDK Release Announcement
# June 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 Improved Microsoft knowledge base (KB) information in the Server data

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We've introduced a new file in the Analog package, named kb_info.json, located in the server folder. This file provides enhanced support for Microsoft KB metadata. With kb_info.json, you can:

- Query KB metadata such as name, ID, and publish date
- Query relationships between KBs, including superseded KBs
- Query the relationship between KBs and the CVEs they address

### 1.2 Enhanced "Restrict Bundle" functionality for macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED

We now support a new option that allows customers to efficiently filter all values in a predefined set, without having to specify each value individually.

The new option is: all_predefined_values. When used with the Restrict Bundle Search function, the SDK will restrict the search to all locations that match the predefined bundle values, and it will automatically include any new locations that are added to new versions of the macOS.

Additionally, the SDK supports exclusion of specific values by using entries prefixed with :except: alongside all_predefined_values. Example: all_predefined_values:except:photos,user_home

### 1.3 Improved CPE data for Linux CVEs in vuln_system_association.json

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We've added **new CPE data for Linux CVEs**, with a particular focus on Red Hat systems. This CPE data can be found under the "cpe" key within the affected_packages object in vuln_system_association.json.

Example entry: "cpe:/o:redhat:enterprise_linux:9:*:*:*"

## 2– Upcoming Changes

### 2.1 Non-security Microsoft patch support

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED, CODE CHANGE

In the June 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**

### 2.2 Realtime monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

This summer, 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**

### 2.3 V3V4 Adapter to use libc++ instead of libstdc++

ENHANCEMENT, MAC, LIBRARY UPDATE

Soon, all Mac V3V4 Adapter libraries will be built via 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.

OPSWAT.

### 2.4 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.

## 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 with the following URL:
https://vcr.opswat.com/gw/file/download/OesisPackageLinks.xml?type=1&token=<authorization_token>

If you're having trouble accessing the build, this could be the cause. Please contact support for assistance.

OPSWAT.

### 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.

## 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 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

OPSWAT.

Protecting the World's Critical Infrastructure