OPSWAT.

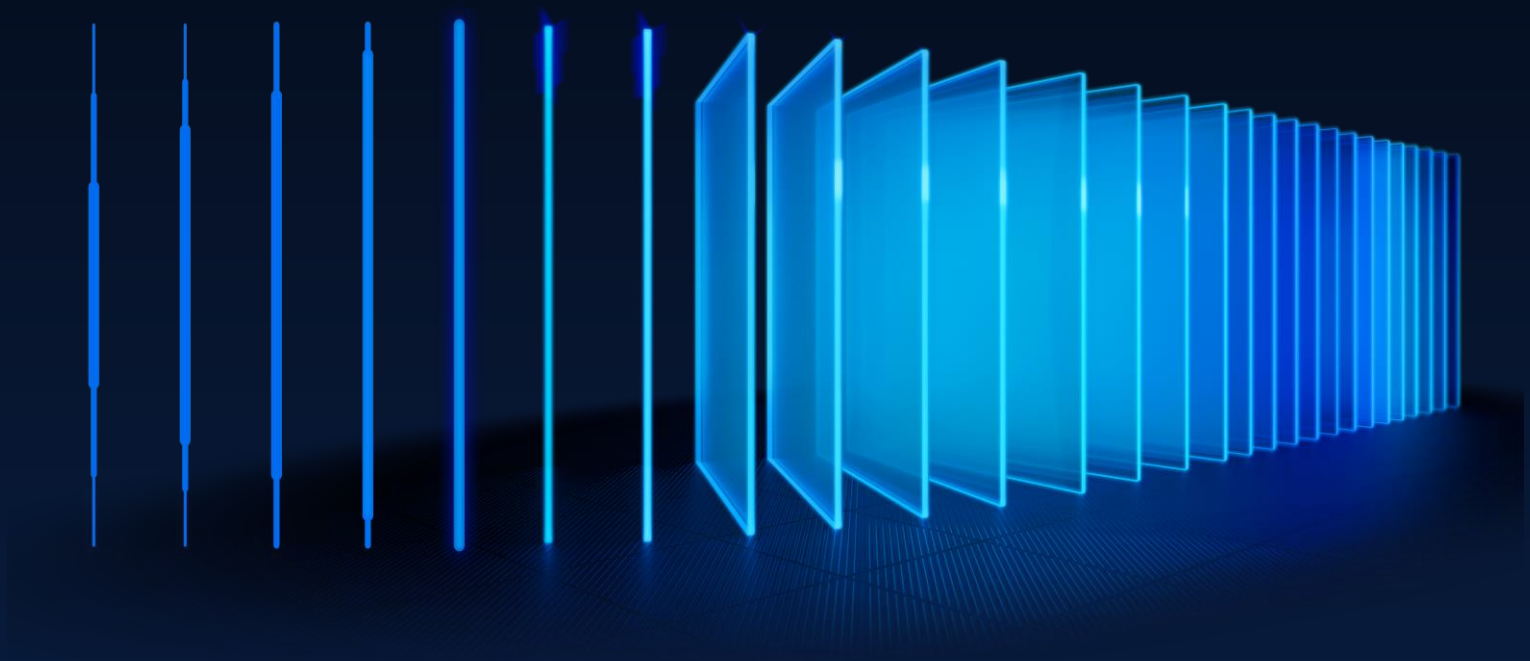
SDK News

MetaDefender Endpoint Security SDK Update

October 2025

Announcement Date

2025/10/13



OPSWAT.

Contents

MetaDefender Endpoint Security SDK Release Announcement
October 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 Patching for Microsoft SQL Express 2022 moves to WUO

FIX, ANALOG PACKAGE, DATA UPDATE NEEDED

We've streamlined how patching is delivered for Microsoft SQL Express 2022.

Previously, patching for Microsoft SQL Express 2022 was handled as a third-party application, which might cause asynchronization with your device's Windows update. This approach has been removed since this release.

Going forward, Microsoft SQL Express 2022 will be updated exclusively through the Windows Update Offline feature (wuo.dat), ensuring better alignment with Microsoft's native update mechanisms and improved reliability.

1.2 Known Issues about SQL Server 2016 SP3

KNOWN ISSUE, WINDOWS

When you call GetLatestInstaller for SQL Server 2016 Service Pack 3 (SP3) version 13.0.6300.2, two available KBs might be returned: KB5058717 and KB5058718.

However, we observed a behavior where one KB is installed first, then attempts to install the other, the second installation will fail, and our SDK will return WA_VMOD_ERROR_INSTALLATION_FAILED.

This is expected since Microsoft's applicability rules list both KBs as valid for the same product version. However, these two KBs belong to different lines (Cumulative Update (CU) builds and Azure Connect Pack builds). After one KB is installed, it effectively moves to that line, making the second update inapplicable.

1.3 Non-security Microsoft patch support

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED, CODE CHANGE

The SDK is now 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

1.4 SDK now supports macOS 26.0 beta and Oracle Linux 10.0

ENHANCEMENT, WINDOWS, MAC, ENGINE UPDATE NEEDED

We've enhanced our SDK to ensure full compatibility with macOS 26.0 beta and Oracle Linux 10.0.

Our team has verified and made some updates, so our SDK now works seamlessly on these platforms, reflecting the latest OS changes and requirements.

This validation ensures customers can begin planning and testing on these upcoming platforms with confidence.

1.5 Pass-through NVD CPE Data now available in the GetProductVulnerability

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We're excited to introduce pass-through support for National Vulnerability Database (NVD) Common Platform Enumeration (CPE) information for patching third-party applications.

This update enables customers to access detailed CPE data for each patch directly in the SDK, using the standard CPE 2.3 format. The new CPE field is now included in the output of the GetProductVulnerability method for supported platforms (Windows, macOS, Linux), and documentation has been updated accordingly.

CPE Object Schema *(found in result.cves[].details.cpe[])*

```
{
  "cpe_2_3": string, // required
  "version_start_include": string, // optional
  "version_start_exclude": string, // optional,
  "version_end_include": string, // optional,
  "version_end_exclude": string, // optional
}
```

Complete Response Structure

```
{
  "result": {
    "cves": [
      {
        "cve": "CVE-2023-XXXX",
        "details": {
          "cpe": [
            {
              "cpe_2_3": "cpe:2.3:a:vendor:product:*:*:*:*:*:*:*:*",
              "version_start_include": "1.0.0",
              "version_end_exclude": "1.2.5"
            }
          ]
        }
      }
    ]
  }
}
```

2– Upcoming Changes

2.1 Real-time monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

In Q1-2026, 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.

Please note that this feature has been moved from Q4-2025 to Q1-2025.

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

2.2 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.

2.3 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.

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

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