OPSWAT.

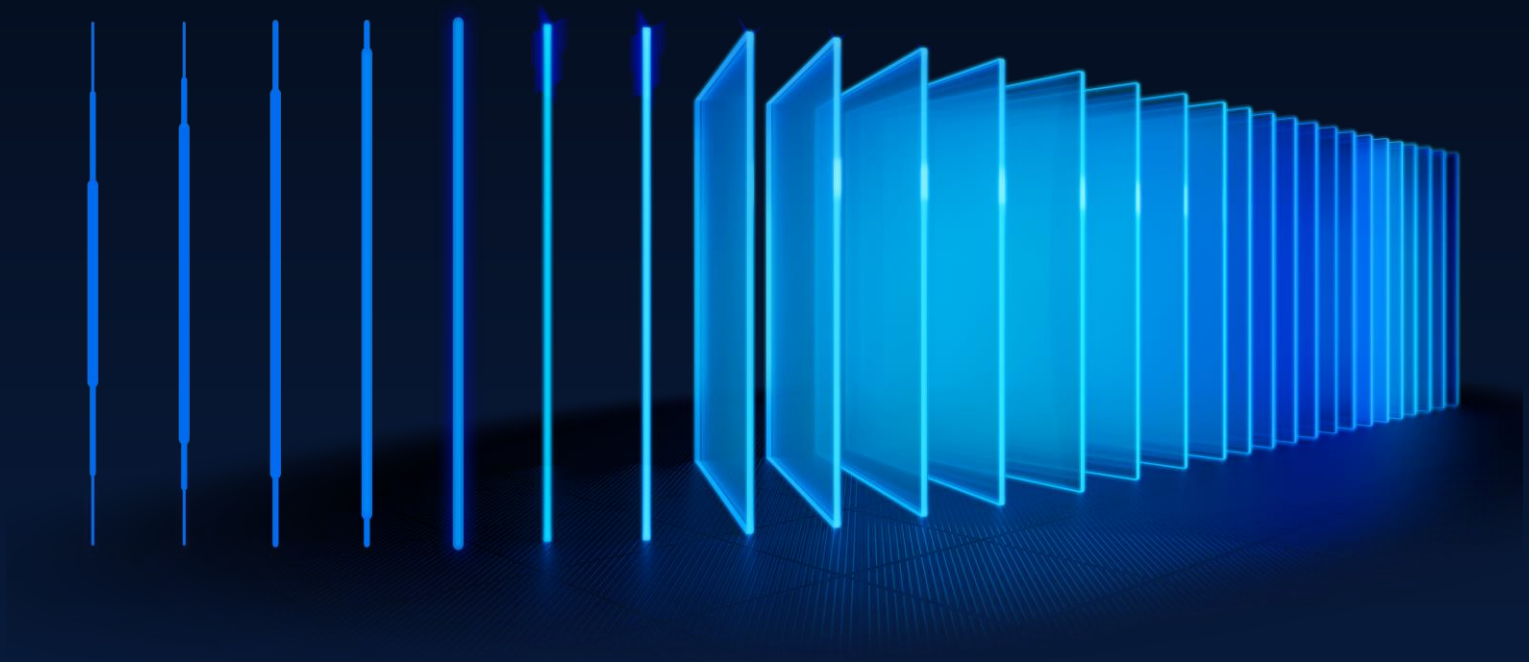
SDK News

OESIS Framework Update

January 2026

Announcement Date

2026/01/13



OPSWAT.

Contents

OPSWAT.

OESIS Framework Release Announcement
January 2026

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 OESIS Framework 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 Distro-specific files for Linux vulnerability data

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We have updated the Linux vulnerability data delivery in OESIS by splitting the original *liv.dat* file into smaller, distro-specific files.

Customers can now use dedicated files for each supported distribution: *liv_ubuntu.dat*, *liv_mint.dat*, *liv_debian.dat*, *liv_redhat.dat*, *liv_alma.dat*, *liv_rocky.dat*, *liv_amazon.dat*, *liv_oracle.dat*, and *liv_suse.dat*.

This change helps reduce the size of the vulnerability database you need to download to each endpoint, improving efficiency and performance.

All the *liv_<distro>.dat* files are now available under *analog.zip* in the */client* folder. In addition, each dat file can be downloaded individually via the VCR gateway using the standard format **https://vcr.opswat.com/gw/file/download/liv_**<distro>**.dat?type=1&token=**<authorized_token>.

The existing *liv.dat* file will continue to be delivered and supported to ensure backward compatibility for current integrations.

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

1.2 Improved control for patching Microsoft Office with force_close

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED

We have enhanced the behavior of Microsoft Office MSI patching when Office applications are open during installation. This enhancement applies to Office 2007, 2010, 2013, and 2016 MSI products patched via the WUO InstallFromFile flow.

When any Office application (such as Word, Excel, PowerPoint, or Access) is running and you install a patch:

- With force_close = 0, the SDK now returns WA_VMOD_ERROR_CANNOT_TERMINATE_PRODUCT, users might need to close Office and retry the installation.

- With force_close = 1, the SDK force-closes all running Office applications before continuing the patch and reports the closed processes in the blocking_processes field.

This gives integrators clearer control over the user experience when patching Office: either preserve user sessions and ask them to close Office, or apply updates immediately by closing running Office apps automatically.

1.3 Changes to Delta Updates packaging for Windows Update Offline (WUO)

BEHAVIOR CHANGE, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We have updated the Delta Updates packaging for Windows Update Offline (WUO) data in analog.zip to simplify distribution and prepare for future enhancements. Going forward, we will no longer publish the following legacy files:

- analogv2.zip
- analogv2_baseline.zip
- wuo_baseline.dat
- wuo_delta.dat

Instead, the new WUOv2 data (wuov2_baseline.dat and wuov2_delta.dat) are now included in analog.zip package under the client folder, and they are fully documented in header.json and the updated How_to_use_Analog_files.pdf guide. This change increases the analog.zip size by approximately 44 MB.

To use Delta Updates with WUO, customers must migrate to WUOv2 by ensuring that endpoints first receive the matching wuov2_baseline.dat file **before** deploying the corresponding wuov2_delta.dat file.

Please note that there is no longer a 30-day grace period to switch to a new baseline, so wuov2_baseline.dat and wuov2_delta.dat must always match on the endpoint for Delta Updates to work properly.

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

1.4 New "usable_download_link" field in products.json

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We have added a new "usable_download_link" boolean field to each product entry in analog/server/products.json. This field indicates whether the installer download link from GetLatestInstaller(download=0) is valid or not.

- If "usable_download_link" is true, agents will be able to use the download link.
- If "usable_download_link" is false, agents should not attempt to use it.

This update will help improve reliability by providing clear guidance to agents. To reduce failed download attempts, please plan to update your integration logic to check this field before fetching installer links.

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

1.5 Detect Per-User Applications for All Users

NEW FEATURE, ALL PLATFORMS, ENGINE UPDATE NEEDED, CODE CHANGE

We have enhanced our SDK to enable detection of per-user applications across Windows, MacOS, and Linux platforms. A new flag, detect_all_users_products, has been added to the DetectProducts method.

By default, this field is false and detection is limited to only applications installed for the active user and those available to all users (system-wide). When detect_all_users_products is set to true, this field enables detection of all applications installed on the device, including those specific to other user accounts.

On Windows, when detect_all_users_products is enabled, the output will include a new installed_for_users field for each detected product. This field lists all users (by SID and username) who have the product installed in per-user mode.

This enhancement provides a comprehensive view of software inventory across all user profiles on a device.

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

1.6 New success code 1005 is introduced

NEW FEATURE, ALL PLATFORMS, ENGINE UPDATE NEEDED, CODE CHANGE

We introduced a new success code, WA_VMOD_INSTALLATION_NEED_APPLICATION_RESTART (1005), which may be returned when patching an application that requires an application restart to complete the process. This new success code helps users clearly distinguish between the following two restart behaviors:

- **OS restart required:** This behavior may occur after an application patch is applied, and an operating system restart is required to fully complete the patching process. This scenario is indicated by the success code WA_VMOD_INSTALLATION_NEED_RESTART (1003).
- **Application restart required:** This behavior may occur after an application patch is applied, and only the application itself needs to be restarted to fully complete the patching process. This scenario is indicated by the success code WA_VMOD_INSTALLATION_NEED_APPLICATION_RESTART (1005).

2– Upcoming Changes

2.1 New Software Categories for Compliance

NEW FEATURE, ALL PLATFORMS, ENGINE UPDATE NEEDED, CODE CHANGE

We are pleased to announce that our Q1-2026 release will introduce three new software categories: Vulnerability Management, Artificial Intelligence, and Gaming.

All new categories will include comprehensive support methods such as version detection, running state, installation directories, and more.

Stay tuned for further details as we approach the release date.

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

As of October 14, 2025, Microsoft no longer provides 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 Framework 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 Support for Patching Multiple App Instances on macOS

ENHANCEMENT, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

We are pleased to inform you that our team is actively investigating ways to improve patching support on macOS.

In the future release, our SDK will support patching multiple instances of applications, even when they are renamed or installed outside the standard Applications folder.

This enhancement ensures that after patching, only the latest version remains, eliminating unpatched or vulnerable duplicates across all locations.

2.4 The Mozilla Firefox patching behavior is changed on Windows

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

Effective January 13, 2026, the value of the “requires_reboot” parameter on server-side data, which could be used during the patching process, will change from 0 (restart not required) to 2 (conditional restart).

In addition, when patching Mozilla Firefox using the InstallFromFiles method, the return codes will be as follows:

- *(Current)* If Mozilla Firefox does not require the application to restart after patching, the return code will be WAAPI_OK (0).
- *(New)* If Mozilla Firefox does require the application to restart after patching, the return code will be WA_VMOD_INSTALLATION_NEED_APPLICATION_RESTART (1005).

This change reflects an update on Mozilla Firefox’s patching behavior. An application restart is now required after patching to fully upgrade the application version. Without a restart, the patching process will not be completed, and the application version will remain unchanged.

OPSWAT.

3 – Required Actions

3.1 CVE-2025-0131

VULNERABILITY, WINDOWS

An incorrect privilege management vulnerability in the OPSWAT OESIS Framework 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 Framework to version **4.3.4451** or later.

3.2 We moved the OesisPackageLinks.xml behind the VCR gateway

SECURITY UPDATE, VCR GATEWAY

Since **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> in to 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 the OESIS Framework, 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