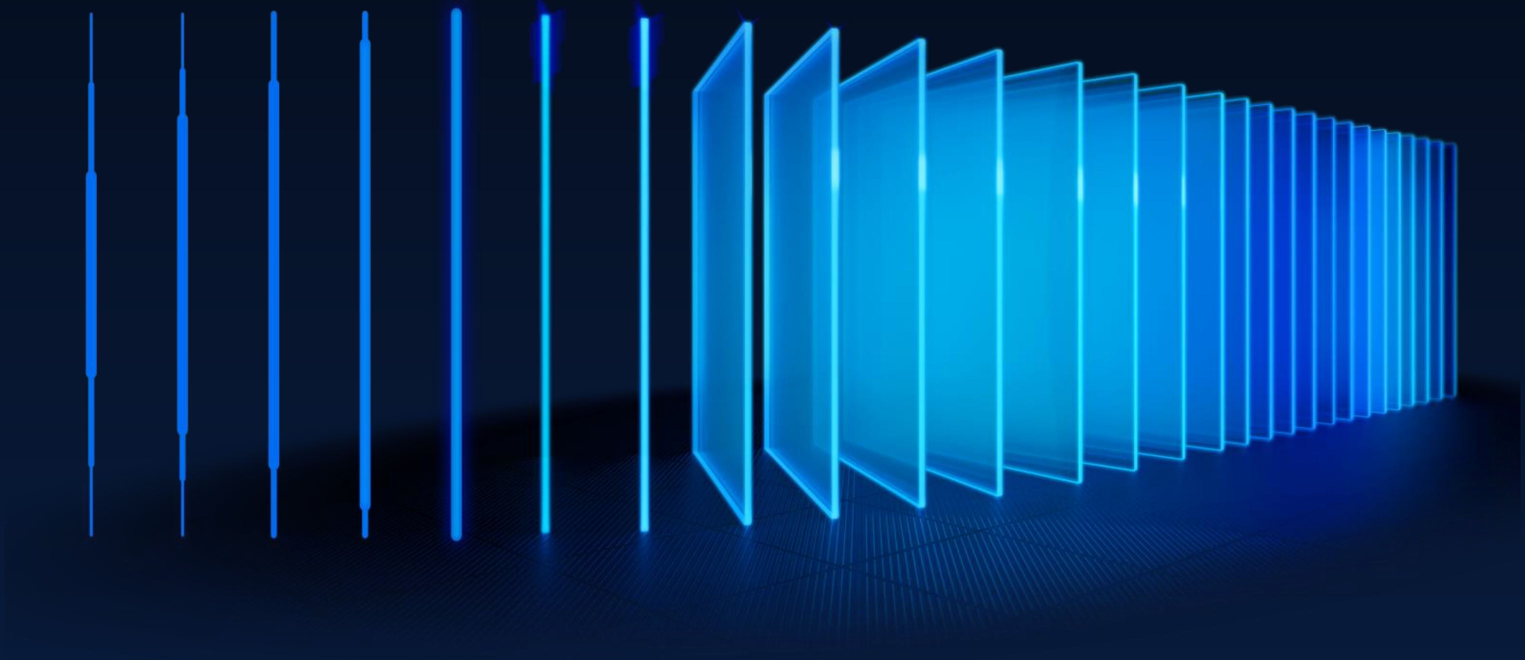
SDK News

OESIS Framework Update

December 2025

Announcement Date

2025/12/09



Contents

OESIS Framework Release Announcement
December 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 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 Behavior change in InstallFromFiles's default Signature Check

BEHAVIOR CHANGE, MAC, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We have updated the default behavior of the skip_signature_check parameter in InstallFromFiles method for both Windows and macOS platforms. Starting from SDK versions 4.3.5218.0 (Windows) and 4.3.4677.0 (macOS), our SDK will now skip digital signature validation **by default** when installing third-party applications.

Customers do not need to specify the skip_signature_check parameter to skip signature checking. If omitted, unsigned installers will be allowed as before.

If you require signature validation for enhanced security, please explicitly set skip_signature_check=0 when invoking InstallFromFiles. This will block unsigned or invalidly signed installers.

Please review your integration and security requirements accordingly.

1.2 Support Adjustment for VMware Player Patching

BEHAVIOR CHANGE, ANALOG PACKAGE, DATA UPDATE NEEDED

Due to recent changes by Broadcom, OPSWAT will no longer support patching for VMware Player 16 and 17.

The standalone installers for these versions are no longer available from the vendor, and all patching attempts for VMware Player 16/17 will now return a "WA_VMOD_ERROR_PRODUCT_NOT_SUPPORTED" error (code -1026) in our SDK. The SDK's product feeds and patching APIs have been updated to reflect this change.

Instead, customers are encouraged to upgrade directly to VMware Workstation Pro 17, which is now free for all users, including commercial environments.

For more details and guidance, please refer to our updated knowledge base article: Broadcom changes affect patching support for VMware products.

1.3 Enhanced Vulnerability Data for Microsoft Product

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We're excited to announce improvements to our vulnerability assessment data.

First, CVE associations for Microsoft SharePoint Server are now included, giving customers greater visibility into vulnerabilities affecting SharePoint 2016, 2019, and Subscription Edition.

Second, Windows KB CVE associations have been refined: only those relevant to products supported by our vulnerability engine (as defined in wiv-lite.dat) are now included. Most KB articles from the Extended Security Update (ESU) product family have been removed, except for those related to Windows Server 2008 R2, Windows 7, and Internet Explorer 9, which remain supported.

These changes help ensure you receive focused, relevant, and up-to-date vulnerability information for your patch management and security workflows.

1.4 New Brand, Same Mission!

REBRANDING, ALL PLATFORMS, ENGINE UPDATE NEEDED

We are pleased to announce that MetaDefender Endpoint Security SDK has been rebranded as **OESIS Framework**.

This update will be reflected across all technical documentation, API references, and support materials for a more unified experience.

The MyOPSWAT Portal page has also been updated, and you can now access it at https://my.opswat.com/portal/home/oesis-framework. Any previous links or bookmarks to the old portal URL (https://my.opswat.com/portal/home/metadefender-endpoint-security-sdk) will automatically redirect to the new page.

All schemas and integrations remain fully compatible, so no action is required on your part. If you have any questions or need assistance, please contact our support team. Thank you for your continued partnership with OPSWAT.

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

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 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 New "usable_download_link" field in products.json

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We will add a new "usable_download_link" boolean field to each product entry in analog/server/products.json. This field will indicate whether the installer download link from GetLatestInstaller(download=0) will be valid.

- 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.

2.5 Detect Per-User Applications for All Users

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

We are enhancing our SDK to enable detection of per-user applications across Windows, MacOS, and Linux platforms. By the end of 2025, a new flag, detect_all_users_products, will be introduced 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

2.6 Distro-specific files for Linux vulnerability data

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

To address file size limitations and improve efficiency, the current liv.dat file will be split into smaller, distribution-specific files such as liv_ubuntu.dat, liv_debian.dat, and others.

This update allows customers to specify only the data relevant to their environment, reducing storage and bandwidth requirements. The new files will provide the same vulnerability coverage as before.

Implementation of this enhancement is already underway, with completion targeted by December. We appreciate your feedback and partnership as we continue to improve our Linux vulnerability management capabilities.

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

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

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> 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