OPSWAT.

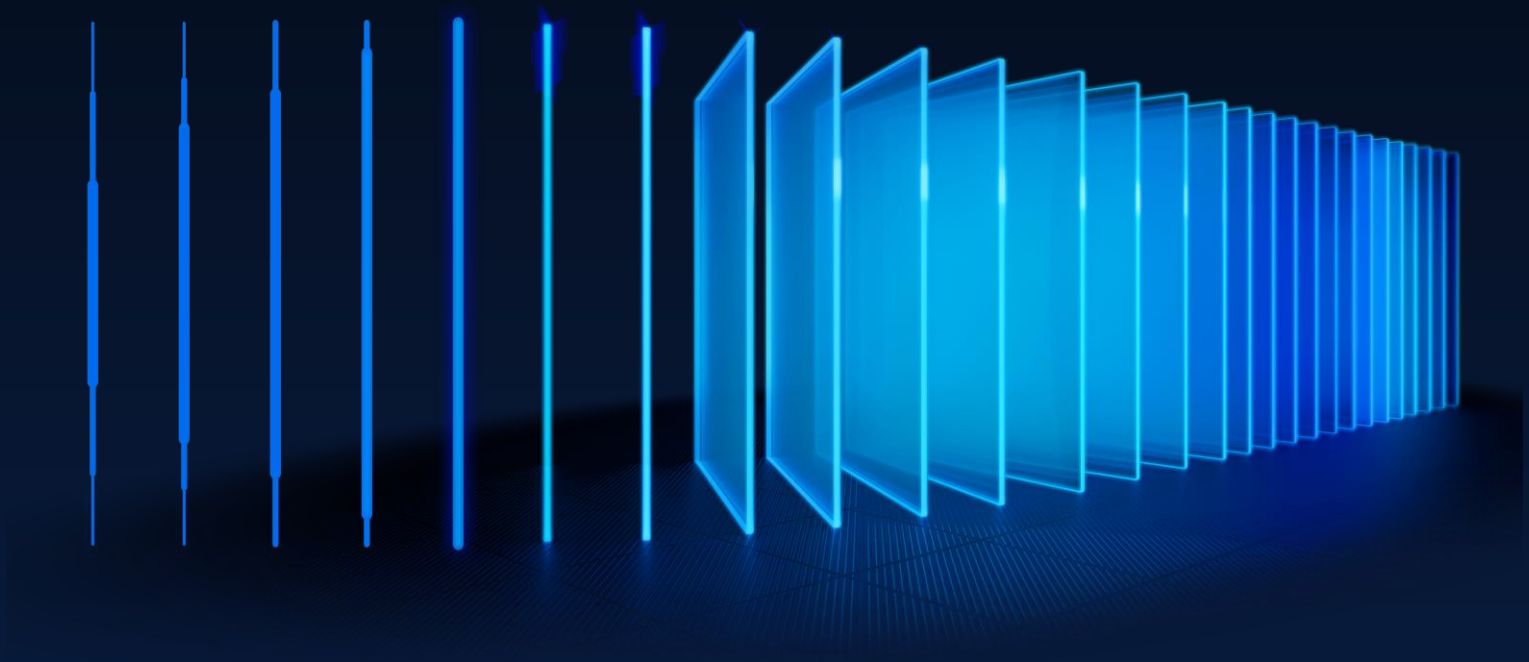
SDK News

OESIS Framework Update

June 2026

Announcement Date

2026/06/09



OPSWAT.

Contents

OPSWAT.

OESIS Framework Release Announcement
June 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 Support for Ubuntu 26.04 LTS

FEATURE: COMPLIANCE, VULNERABILITY ASSESSMENT, PATCHING

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We've expanded our Linux coverage to include the upcoming Ubuntu 26.04 LTS release in OESIS Framework.

Ubuntu 26.04 LTS is now supported across OESIS modules, including Compliance, Patching, and VA. All applicable functionalities will behave consistently with other supported Ubuntu versions, even during the early period where no CVEs have yet been published for 26.04.

1.2 Support phased updates in GetMissingPatches for Ubuntu apt

FEATURE: COMPLIANCE, PATCHING

ENHANCEMENT, LINUX, DATA UPDATE NEEDED

We've developed an enhancement to the GetMissingPatches method for **apt** (Advanced Package Tool - the primary package management system on Debian-based systems such as Ubuntu), adding visibility into Ubuntu's phased updates.

Ubuntu uses "phased updates" for some apt packages, where updates are gradually rolled out to a percentage of endpoints. Our GetMissingPatches (*WAAPI_MID_GET_MISSING_PATCHES* – ID 1013) API will detect those and return a new optional field, patches.phased.

- If the package is in a phased rollout, patches.phased returns the rollout percentage (e.g., value 10 means 10% of endpoints are targeted for the update).
- If no phased information is found, patches.phased field is omitted from the response.

1.3 Support Vulnerability Assessment and Patching for Windows Drivers

FEATURE: VULNERABILITY ASSESSMENT, PATCHING

NEW FEATURE, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We have extended OESIS Framework Vulnerability Assessment (VA) and Patch Management (PM) capabilities to cover Windows drivers. This enhancement enables customers to detect, assess, and remediate vulnerabilities at the driver level.

With this update, customers can leverage OESIS to identify outdated or vulnerable Windows drivers, evaluate risk exposure, and apply available patches.

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

1.4 Version-specific Patching for 3rd-Party Applications

FEATURE: PATCHING

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

OESIS Framework previously patched third-party applications to the latest available version.
Now we are excited to introduce Version-Specific Patching, a comprehensive set of enhancements that give you full control over which version of a third-party application gets downloaded and installed, including:

- A new optional ***requested_version*** parameter to both GetLatestInstaller and InstallFromFiles, allowing customers to download and install an exact application version. When specified, the SDK verifies the installer's integrity by comparing its SHA-256/MD5 hash against the SDK checksum database before proceeding.
- A new patch-centric database (**patchv2.dat**) to store version metadata that supports multiple versions per product instead of only the latest. Both GetLatestInstaller and InstallFromFiles can be used with patchv2.dat.

When requested_version is omitted, the SDK behaves exactly as before, defaulting to the latest version. The requested_version parameter in GetLatestInstaller only works when patchv2.dat is loaded. If using patch.dat, GetLatestInstaller will silently ignore the requested_version field and return the latest version as usual.

This feature is now available on Windows (SDK 4.3.6110.0) and macOS (SDK 4.3.5527.0). Linux support is coming soon this June.

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

1.5 Improved Uninstall handling for newer application versions

FEATURE: UNINSTALL

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED

We are pleased to announce an improvement to how the OESIS Framework handles application uninstallation for versions beyond the currently validated range. This update removes unnecessary version-lock restrictions and introduces clearer error reporting when issues occur.

Previously, attempting to uninstall an application version that had not yet been explicitly validated by OESIS Framework would immediately fail without making any attempt. The SDK now takes a more practical approach: it automatically falls back to the uninstall method from the closest validated version and attempts the operation.

- If the uninstall succeeds: returns success as normal.
- If the installed version cannot be determined at all: exits early with the new WAAPI_ERROR_FAILED_TO_GET_PRODUCT_VERSION error code.
- If the fallback uninstall is attempted but fails: returns the new error code WAAPI_ERROR_UNINSTALL_UNVALIDATED_VERSION, clearly indicating the failure occurred on an untested version.

Behavior for versions within the validated range remains unchanged.

1.6 Linux 3rd-party patch data now available in Server-Side data files

FEATURE: PATCHING

ENHANCEMENT, LINUX, ANALOG UPDATE NEEDED, CODE CHANGE

We are pleased to announce that Linux 3rd-party patch data is now included in the server-side Analog data files: ***patch_aggregation.json***, ***patch_associations.json***, and ***os_info.json***.

Previously, Linux patch information was only available on the client side via patch_linux.dat and was excluded from the server-side JSON files used for offline validation. With this update, customers who rely on these data files can now validate patch availability for Linux endpoints using the same workflow they already use for Windows and macOS.

No breaking schema changes, so there is no action required from customers who do not consume Linux patch data.

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

1.7 Duplicate CVE References Removed

FEATURE: VULNERABILITY ASSESSMENT

ENHANCEMENT, ALL PLATFORMS, ANALOG UPDATE NEEDED

We've cleaned up duplicate reference URLs across our vulnerability assessment data feeds, improving data quality, and reducing download sizes.

Our CVE data (vmod.dat, v2mod.dat) contained duplicate reference URLs for certain vulnerabilities, the same advisory link appeared multiple times under different sources or URL encodings. We identified and removed these duplicates across 377 affected CVE records covering third-party applications (e.g., Oracle Java, Apache Tika, ExifTool, radare2) and Windows system packages (e.g., Windows NTFS, CLFS, Internet Explorer components).

If you have any questions about this change or notice unexpected behavior in your vulnerability scans, please contact OESIS Support Team.

1.8 Integration between OESIS Framework and WinGet

FEATURE: ALL MODULES

NEW FEATURE, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

Since May, we introduced integration between the OESIS Framework and WinGet, expanding the catalog of applications supported for detection and patch management.

To enable WinGet-sourced products, customers can pass the new optional *enable_winget_source* boolean flag in the JSON input of DetectProducts. By default, this flag is false, meaning existing integrations will continue to behave exactly as before with no changes required.

When *enable_winget_source* is set to true, the method will return both OPSWAT-curated and WinGet-sourced products in its results. Every entry in the output will include a *data_source* field, allowing customers to distinguish between "opswat" and "winget" sourced products.

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

2 – Upcoming Changes

2.1 Clearer Windows Defender Real-time Protection Status when managed by 3rd Party AV

FEATURE: COMPLIANCE

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We are enhancing the GetRealTimeProtection method for Windows Defender to make it more clear when Windows Defender is being managed (and effectively disabled) by a third-party antivirus product.

Today, customers sometimes see Windows Defender protection state reported as ON or OFF inconsistently, which is expected when a third-party AV is in control. But the current output does not explain why.

With this change, when Windows Defender is managed by another AV, JSON output of GetRealTimeProtection will include a new *managed_by_3rd_party_products* array listing the managing product's information. If Windows Defender is not managed by any third-party AV, this field will be omitted.


```
{
  "result": {
    "code": 0,
    "details": {
      "antispyware": false,
      "antivirus": false
    },
    "enabled": false,
    "managed_by_3rd_party_products": [
      {
        "displayName": "CrowdStrike Falcon",
        "pathToSignedProductExe": "C:\\Program Files\\CrowdStrike\\CSFalconService.exe",
        "signature": 2866
      }
    ],
    "method": 1000,
    "signature": 477,
    "timestamp": "1765255198",
    "timing": 16
  }
}
```


This additional context helps customers understand that Windows Defender's state is no longer the primary indicator of protection and that they should rely on the third-party AV's real-time protection state for posture and compliance decisions.

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

2.2 Bulletin Support for Patching

FEATURE: PATCHING

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

We are introducing Bulletin-based patch organization in the OESIS Framework, enabling customers to view and sort patches by Bulletin ID — consistent with how major software vendors publish and communicate their updates, which may include security fixes, bug resolutions, and general software improvements.

With this update, customers can now filter and retrieve patch information by Bulletin ID (e.g., Adobe's APSB25-14), making it easier to align remediation workflows with vendor-issued advisories.

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

2.3 Release Note Download Links in OesisPackageLinks.xml

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS

Starting in July, each release entry in OesisPackageLinks.xml will include a new download link for its corresponding release note file. Customers will be able to download release notes directly from the URL in the manifest, no portal login required, giving you a single, consistent location to access all release artifacts.

This is an additive change. Existing fields in OesisPackageLinks.xml remain unchanged, so no action is required unless you want to consume the new release note links. If your integration uses strict XML schema validation, please verify it tolerates the new element. Please contact the OPSWAT team if you need assistance adopting this change.

3 – Required Actions

3.1 Engine Release Cadence Change (Starting October)

RELEASE SCHEDULE UPDATE, ALL PLATFORMS

Starting in October, we will update our Engine Package release cadence from weekly to bi-weekly. Under this new schedule, releases will occur twice per month, once in the second week and once in the fourth week of each month. This change aligns with our new development framework, enabling more accurate estimations, clearer updates, and more reliable on-time releases. We believe this adjustment will help us deliver higher-quality updates more consistently.

** The initial rollout timeline has been revised from April to October. If you have any concerns or need clarification on this update, please contact the OPSWAT team to assist with this**

3.2 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.

As of January 1, 2026, the OSX package has been removed. We recommend upgrading to AppRemover OSX V2 to ensure your system receives all new updates and comprehensive technical support for the AppRemover module.

3.3 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 previously 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