OPSWAT.

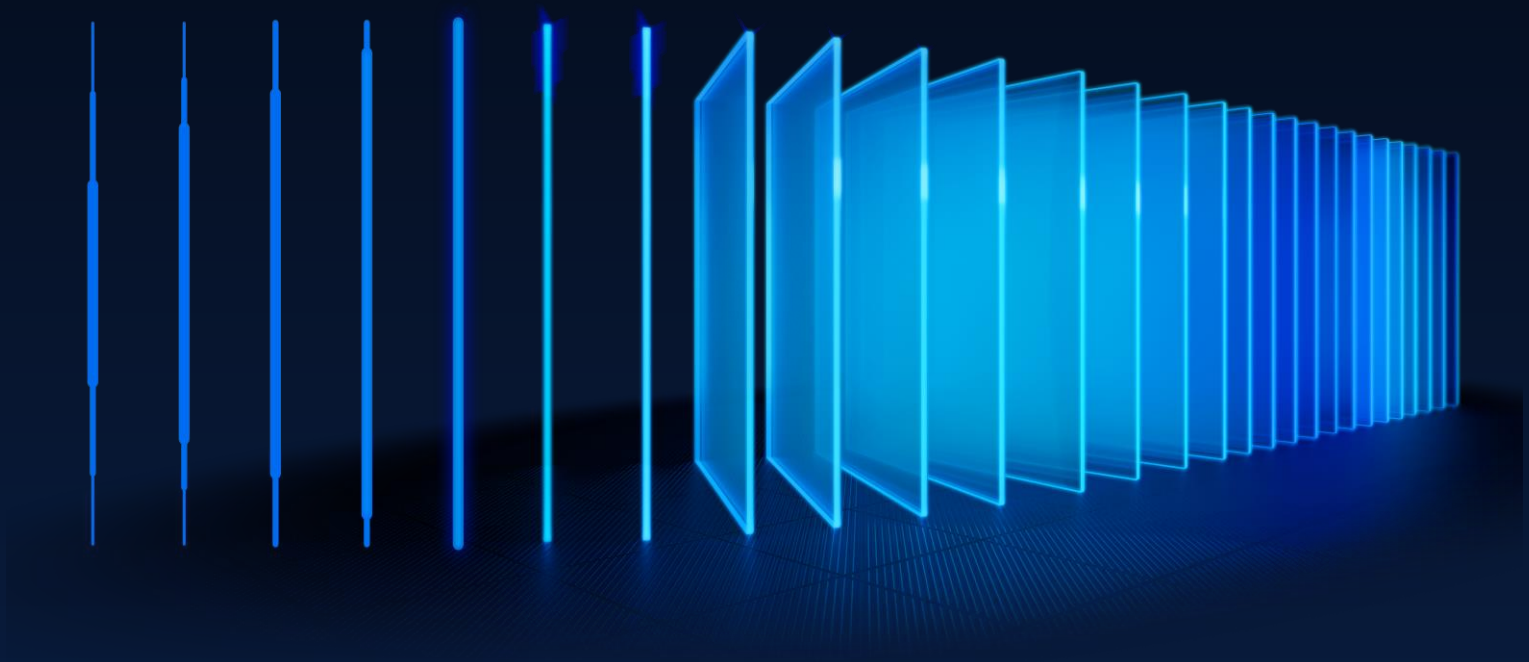
SDK News

OESIS Framework Update

July 2026

Announcement Date

2026/07/14



OPSWAT.

Contents

OPSWAT.

OESIS Framework Release Announcement
July 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 Patching Support for Dell and Lenovo BIOS/Firmware

FEATURE: PATCHING

NEW FEATURE, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We have extended OESIS Framework patching capabilities to cover hardware-level updates on Windows. Customers can now detect outdated BIOS and firmware, assess exposure, and apply OEM updates through the same workflow used for software patching. This release covers BIOS updates for both Dell and Lenovo, plus firmware updates for Lenovo.

To protect endpoints during the update, BIOS pre-flight checks are enabled by default and validate power state, BitLocker status, and administrator privileges before the OEM installer runs, returning a clear error if a condition is not met. A reboot is required to apply a BIOS update, the SDK reports when one is needed, and rollback is not supported, consistent with OEM installer behavior.

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

1.2 Bulletin Support for Patching

FEATURE: PATCHING

NEW FEATURE, ALL PLATFORMS, DATA UPDATE NEEDED

We are introducing Bulletin-based patch organization for server-side use cases, enabling customers to group and retrieve patches by Bulletin ID, consistent with how major vendors publish and communicate their updates. The new bulletin.json feed is served alongside the existing data feeds, while patch_aggregationv2.json and patch_system_aggregationv2.json carry the bulletin IDs that link each bulletin to its patches, so consumers can resolve which patches belong to a bulletin without engine-side tooling.

Two bulletin types are supported, determined by the patch delivery channel. Vendor bulletins cover Microsoft at the KB level (format MS<YY>-<MMDD>-<KB>) and Adobe using the upstream APSB number directly, while all other third-party applications are grouped under OPSWAT-authored bulletin IDs. Bulletins with no patches are never published.

1.3 Patch-Centric Structure for Patch Management

FEATURE: PATCHING

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

We are applying a patch-centric data model to OESIS Patch Management, where a patch is the unit of update and a package is the environment-specific installer (per OS, architecture, and language) that delivers it. The new patch_aggregationv2.json server file follows this model, holding every application version OESIS recognizes rather than only the latest and adding the bulletin_id and data_source fields. The pattern now also covers Microsoft KB data through patch_system_aggregationv2.json.

The following methods are now promoted to production:

- GetPackages(patch_uuid): returns all packages for a patch, with download URLs and hashes.
- InstallPackage(package_uuid, path): installs a pre-downloaded package, verifies its hash, and reports whether a reboot is required (supports system patching via wuo.dat).
- GetLatestInstaller and InstallFromFiles: now accept the requested_version parameter to install a specific version, or omit it to install the latest as before.

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

1.4 Expanded Patching Coverage through WinGet Integration

FEATURE: PATCHING

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

Building on our WinGet integration, we have expanded the catalog of applications supported for patching. This release adds detection and patching support for 23 additional applications (25 patches in total).

The newly supported applications are: Azul Zulu JDK 17 (x86 and x64), Azul Zulu JDK 8, Python 3.9 (x86 and x64), Microsoft ASP.NET Core Runtime 7.0, Blender, SMPlayer, TechSmith Snagit 2025, AirDroid, Sync Breeze, Sync Breeze Ultimate, Sync Breeze Enterprise, DiskBoss, IZArc, UltraISO, PowerISO, IsoBuster, ImgBurn, jetAudio, CPU-Z, BitComet, mIRC, FlashFXP, and Internet Download Manager.

1.5 Release Note Download Links in OesisPackageLinks.xml

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

Each release entry in OesisPackageLinks.xml now includes a download link for its corresponding release note file. Customers can download release notes directly from the URL in the manifest with 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.

1.6 Support Change for Microsoft Teams Classic

FEATURE: PATCHING

NEW FEATURE, ALL PLATFORMS, DATA UPDATE NEEDED

Microsoft has ended availability of the Teams Classic client, so OESIS Framework now marks Microsoft Teams Classic (signature 3089) as defunct. In addition, because the x64 installer for Teams Classic is no longer available from Microsoft, OESIS Framework no longer supports auto-patching for Microsoft Teams Classic x64.

For reference, Microsoft's end-of-availability notice is published here. If you have any questions about this change, please contact the OESIS Support Team.

OPSWAT.

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.

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 Regulatory Compliance (Generic Mode + PCI-DSS 4.0.1)

FEATURE: COMPLIANCE

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

We are introducing Regulatory Compliance support in the OESIS Framework across Windows, macOS, and Linux. This capability delivers a Generic Mode along with mapping to the PCI-DSS 4.0.1 standard, enabling customers to evaluate endpoint posture against recognized regulatory requirements.

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

2.3 EPSS Score in Vulnerability Data

FEATURE: VULNERABILITY ASSESSMENT

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

We are adding the Exploit Prediction Scoring System (EPSS) score to our vulnerability data, giving customers an exploitability-based signal to prioritize remediation alongside CVSS severity. EPSS estimates the likelihood that a vulnerability will be exploited in the wild.

The GetProductVulnerability (method 50505) response will include a new optional “epss” object nested inside each cves[].details, containing three fields: “score” (probability from 0 to 1), “percentile” (rank from 0 to 1), and “date” (the EPSS model date, in YYYY-MM-DD format). The object is present only when EPSS data is available for the CVE and is omitted otherwise. This is an additive change, so existing integrations continue to parse the response without modification.

2.4 Scan Products Across All Users on macOS

FEATURE: COMPLIANCE

ENHANCEMENT, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

We are extending DetectProducts on macOS with a new optional detect_all_users_products boolean flag, matching the existing Windows behavior. When enabled, DetectProducts enumerates installed products across all user accounts on the endpoint, active and inactive, regardless of session state. When omitted or set to false, detection remains scoped to the active user as it is today.

Detecting all users' products requires elevated privileges (running as a root daemon); without sufficient permissions the SDK returns WAAPI_ERROR_ACCESS_DENIED, consistent with Windows. This gives customers a complete inventory on shared and multi-user macOS endpoints, including scenarios where no user is logged in.

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

2.5 New native_error_message Field in Error Responses

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS, ENGINE UPDATE NEEDED

We are adding a new native_error_message field to the error response, surfacing the underlying native error detail alongside the existing OESIS error code. This makes it easier to diagnose failures during integration and support investigations. This is an additive change.

2.6 Updated Manual and Auto-Patching Definitions

FEATURE: PATCHING

ENHANCEMENT, ALL PLATFORMS

We are correcting the definitions used to classify how an application is patched, so they accurately reflect the SDK methods each application supports:

- An application supports manual patching when GetProductPatchLevel and InstallFromFiles are supported.
- An application supports auto-patching when GetProductPatchLevel, InstallFromFiles, and GetLatestInstaller are all supported.

Once the corrected definitions roll out to the support charts, the number of supported applications will change to reflect the accurate classification, with a notable decrease in the manual-patching count. We are sharing this in advance so customers who reference the support charts are aware of the change.

2.7 New has_static_download_link Field in products.json

FEATURE: PATCHING

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

We are adding a new boolean field, has_static_download_link, to each object in the signatures[] array of products.json. This field indicates whether a patch ships a static download link stored in patch_aggregation.json, which helps customers who use their own downloader identify exactly which patches provide a usable static URL.

This is distinct from the existing usable_download_link field, whose meaning is unchanged. Some products generate links dynamically at runtime (for example, FileZilla and TortoiseSVN), so usable_download_link can be true while has_static_download_link is false.

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 support_sdk@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