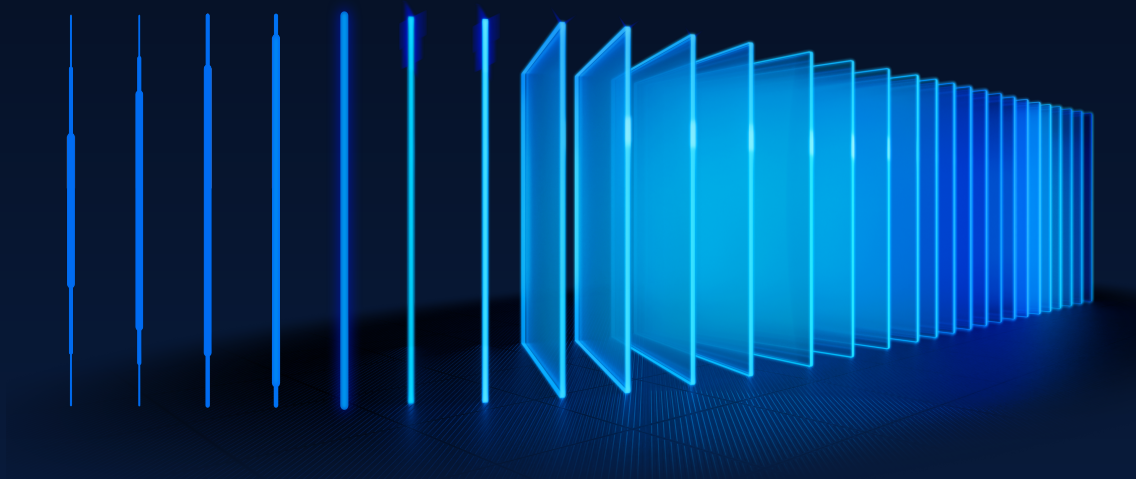


OPSWAT.

SDK News

OESIS Framework Update
October 2026

Announcement Date
2026/10/06
Document Version
1.0



Contents

OESIS Framework Release Announcement October 2026.....	3
1 – What’s New?.....	3
1.1 New state Field in Real-Time Protection Results.....	3
1.2 Application Rollback to a Previous Version	4
1.3 Skip the Connectivity Pre-Check on UpdateDefinitions.....	4
1.4 Non-Security and Out-of-Band KBs in patch_system_aggregation.json	5
1.5 Native Error Detail on Linux Patch Installation Failures	5
1.6 macOS 27 Support.....	6
1.7 Expanded Patching Coverage through WinGet Integration	6
2 – Upcoming Changes	9
2.1 Vulnerability Assessment for Windows Drivers & BIOS	9
2.2 CVSS v4 Support in Vulnerability Data	9
2.3 New EDR/XDR Product Category	9
2.4 Trusted Platform Module [TPM] Detection on Windows	10
3 – Required Actions.....	11
3.1 Engine Release Cadence Change (Starting October)	11
3.2 End of Support for AppRemover package with the old engine on macOS.....	11
3.3 End of Support for Windows 7 & Windows 8	11
3.4 SDK Public Key Rotation	11
4 – Detailed SDK Information	12
4.1 Windows Support Charts	12
4.2 Mac Support Charts	12
4.3 Linux Support Charts	12
4.4 SDK API Documentation	12
5 – Contact.....	12

OESIS Framework Release Announcement

October 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 New state Field in Real-Time Protection Results

Feature: compliance

Enhancement, [Windows](#), engine update needed

GetRealTimeProtectionState [method 1000] now returns a new string field state alongside the existing enabled boolean, so callers can tell a security product that is genuinely off from one that is still starting up. Posture checks that run right after boot or login previously saw enabled: false for an agent whose services had not finished initializing, and had no way to distinguish that from real-time protection being switched off.

The state field carries exactly one of four values, and is never null or empty:

- enabled — real-time protection is on
- disabled — real-time protection is off, or the backing services are stopped
- initializing — the backing services are still starting
- unknown — the service state could not be queried

state is returned for every product that supports method 1000. The computation and meaning of enabled and of the details object are unchanged, so this is an additive, backward-compatible change. We recommend treating initializing as a signal to wait and retry rather than to block, and applying a short retry before treating disabled as final during the boot window.

1.2 Application Rollback to a Previous Version

Feature: patching

NEW feature, **Windows & MacOS**, engine Update needed, **Code change**

You can now roll an installed application back to an earlier version through `InstallFromFiles`, so a version that turns out to be faulty after patching can be reversed in a single call, without chaining a separate uninstall and reinstall.

`InstallFromFiles` accepts a new optional boolean input, `enable_rollback`, which defaults to false. Set it to true together with `requested_version`, and the SDK uninstalls the currently installed version and then installs the version you requested. The SDK checks that the application can be rolled back to that version before it touches the endpoint, and returns an error without making any change if it cannot:

- `WAAPI_ERROR_INVALID_INPUT_ARGS [-20]` — `enable_rollback` is true but `requested_version` was not supplied
- `Wa_vmod_error_product_not_supported [-1026]` — the application does not support removal or fresh installation
- `Wa_vmod_version_lock_not_supported [-1052]` — the requested version is not recognized, or no version-specific installer is available for it

If the uninstall step fails, the SDK returns `WAAPI_ERROR_UNINSTALL_SERVICE_FAILED [-89]` and does not proceed to install. If the install step fails, it returns `WA_VMOD_ERROR_INSTALLATION_FAILED [-1034]`, and the application may be left uninstalled. Requesting the version that is already installed runs the same flow without error, so one code path covers both cases. The output of `InstallFromFiles` is unchanged.

To let you determine which versions are valid rollback destinations ahead of time, every package entry under each patch in `patch_aggregation_v2.json` now carries a boolean `is_rollback_target`. It is true when the application can be rolled back to that version, and false or absent when it cannot. This requires using `patchv2.dat` on the endpoint and `patch_aggregation_v2.json` on the server side.

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

1.3 Skip the Connectivity Pre-Check on UpdateDefinitions

Feature: compliance

Enhancement, **all platforms**, engine update needed, **code change**

`UpdateDefinitions` (method 1003) now accepts an optional `skip_connection_check` boolean input. Before running a definition update, the method checks that the endpoint has internet connectivity, and on endpoints that block general internet access while still allowing security vendor update traffic, that check failed even though the update itself would have succeeded.

Pass "skip_connection_check": true in the 1003 json_in to bypass the connectivity check and proceed directly to the update. When the flag is omitted or set to false, the method behaves 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 Non-Security and Out-of-Band KBs in patch_system_aggregation.json

Feature: patching

Enhancement, [Windows](#), data update needed

The server-side patch_system_aggregation.json now includes non-security and out-of-band Windows updates, which were previously missing from the file even though they were supported on the endpoint side. Existing records are unchanged, and the file schema is unchanged.

The addition takes the file from 42,911 to 58,269 records, an increase of roughly 35%, and the new records cover 2,040 distinct KB articles. Consumers should plan for the larger file and should not assume every record carries CVE or severity data: most non-security KBs have no associated CVEs, carry a severity of unknown, and report requires_reboot as maybe.

1.5 Native Error Detail on Linux Patch Installation Failures

Feature: patching

Enhancement, [Linux](#), engine update needed

InstallMissingPatches (method 1014) on apt-based Linux distributions now returns specific error codes with native detail in error.error_message, instead of a bare WAAPI_ERROR_GENERAL [-1]. Download and installation failures previously collapsed into a single generic code, so the underlying cause was not visible to the integrator.

The following codes are now returned with accompanying detail:

- WAAPI_ERROR_ACCESS_DENIED [-22] — the operation requires administrator privileges
- WAAPI_ERROR_INVALID_INPUT_ARGS [-20] — the patches array is missing or empty, auto_repair is invalid, patches.product or patches.title is missing or empty, or patches.version is present but empty
- Waapi_error_resource_busy [-70] — the package manager resource is currently busy

error_message is not encrypted even when encrypt_sensitive_info is set to true. The scope is JSON-level error responses. We recommend logging and surfacing error.error_message for triage.

1.6 macOS 27 Support

Feature: all modules

Enhancement, [MacOS](#), data update needed

Following Apple's general release of macOS 27, the SDK now supports it in production for detection and compliance, and for vulnerability assessment. The macOS 27 operating system identifier is live on production data, and the compliance modules that were previously validated against the beta, including Gatekeeper, the built-in firewall, FileVault, Packet Filter and iCloud, now report against the general release.

Vulnerability assessment reports CVEs for the installed macOS 27 version. Note that macOS 27 runs only on Apple Silicon, so Intel-based Macs stay on their current macOS release and are unaffected by this update.

1.7 Expanded Patching Coverage through WinGet Integration

FEATURE: compliance & Patching

Enhancement, [Windows](#), data update needed

Building on our WinGet integration, we have expanded the catalog of applications supported for patching. This release adds patching support for 31 additional applications (31 signatures in total). The newly supported applications are:

Product	Signature
Accident Reconstruction Professional	4432
Antigravity	4213
Anytype	4396
AutoHotkey	4390
Azure Connected Machine Agent	4384
balena-cli	4397
CyberHive Connect	4403

DiscoverWorthy Scratchpad	4434
Ditto	4435
DMMGamePlayer	4442
Duo Desktop	4345
Envarly	4466
Executor	4531
FastTube Pro	4470
fullfetch	4273
KakaoTalk	4393
Karuzip	4515
memoir	4544
Microsoft Azure Storage Explorer	4372
nu	4404
Password Safe	4347
PW Auto Login	4415
qbPortWeaver	4533
SASM	4440

SnippingTool	4428
Tenebra	4437
ToeRings	4296
VSCodium	4365
Wazuh Agent	4363
Zotero	4421
znote	4210

2 – Upcoming Changes

2.1 Vulnerability Assessment for Windows Drivers & BIOS

Feature: vulnerability assessment

NEW feature, **Windows**, engine update needed, **code change**

We are adding vulnerability assessment for Windows drivers & BIOS, closing the gap where detected driver patches carry no vulnerability context. The SDK will identify and report the CVEs associated with installed drivers, including severity and affected driver version, for the same device models supported by driver patching.

Driver CVEs will also be linked to the patches that remediate them, so you can correlate the exact vulnerabilities present on a device with the available fixes, and the driver vulnerability data will be available for both endpoint and server-side use cases. Driver vulnerability assessment and driver patching are both covered under the VAPM license.

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

2.2 CVSS v4 Support in Vulnerability Data

Feature: vulnerability assessment

Enhancement, **all platforms**, data update needed

We are adding support for CVSS v4, the latest version of the Common Vulnerability Scoring System published by FIRST, to our vulnerability data. CVSS v4 refines how exploitability and impact are measured and provides a more accurate severity signal than earlier scoring versions.

CVSS v4 scores will be carried alongside the existing scoring data where available, so customers can adopt v4-based prioritization without losing current behavior.

2.3 New EDR/XDR Product Category

Feature: compliance

NEW feature, **all platforms**, engine update needed

We are adding a dedicated EDR/XDR category to the SDK, so an EDR/XDR product can be identified directly from its category in DetectProducts results rather than reconstructed from the individual antimalware, firewall and other components it installs.

Products can belong to more than one category, so adding the EDR/XDR category does not remove or replace any existing category assignment, and the existing edrxdr label continues to work unchanged for integrations that rely on it. A support chart will accompany the new category, covering the methods available for EDR/XDR products.

2.4 Trusted Platform Module [TPM] Detection on Windows

Feature: compliance

NEW feature, Windows, engine update needed, code change

We are adding a new Device Info method, `GetTrustedPlatformModuleInfo`, that reports whether a Windows endpoint has a Trusted Platform Module and what state it is in. This gives you a direct way to include TPM presence and configuration in device posture checks.

The response will report:

- Whether a TPM is present on the endpoint
- The TPM specification version, for example 2.0 or 1.2
- The TPM manufacturer and firmware version
- Whether the TPM is enabled, activated and owned

An endpoint with no TPM returns a successful result with the TPM reported as not present. Querying TPM information requires elevated privileges. The method is Windows only.

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 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.

3.4 SDK Public Key Rotation

Public key rotation, [all platforms](#)

The SDK public key is valid for one year, and the current key expires on October 22, 2026. A new key is available now. If you use Digital Signature Verification to confirm that downloaded SDK packages are authentic, download the current sdk_pubkey_YYYY-MM-vD.gpg file and import it before that date, following

the steps in [How can SDK packages be verified using a public key and specific signatures?](#). The new key is valid until October 22, 2027.

During the transition, packages are signed with both the outgoing and the incoming key, so `gpg --verify` may report "Can't check signature: No public key" for one signature alongside a good signature for the other. Importing the current key file resolves this, and once the outgoing key expires only the new key applies.

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