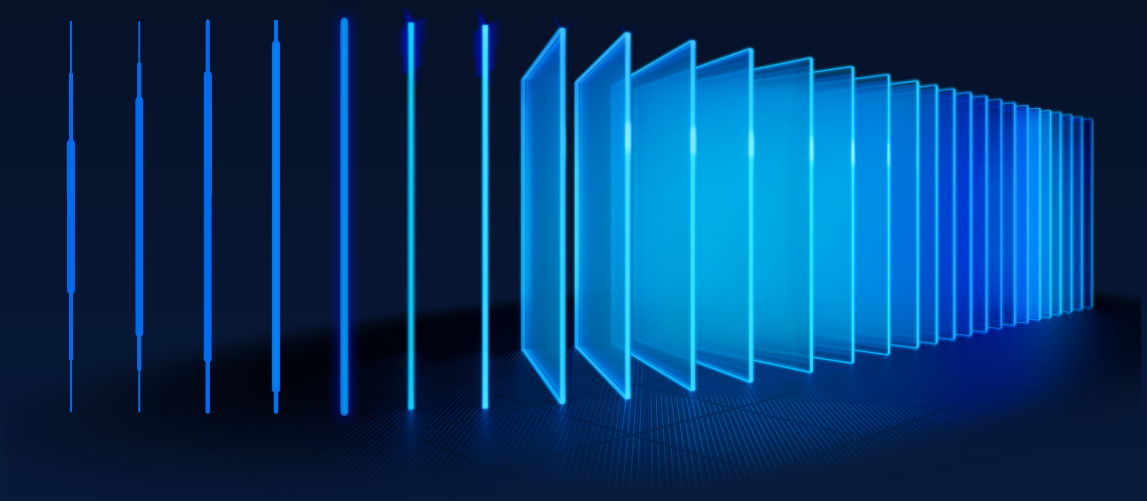
OPSWAT.

SDK News

OESIS Framework Update
November 2026

Announcement Date
2026/11/03



Contents

OESIS Framework Release Announcement November 2026 3
1 – All Components 3
1.1 Bearer Token Authentication for VCR Gateway Downloads 3
1.2 x64 SDK Support on Windows on Arm through x64 Emulation 4
1.3 Engine Release Cadence Change 4
1.4 End of Support for Windows 7 & Windows 8 4
2 – Compliance 6
2.1 Change Logs for Compliance Data 6
2.2 Compliance Module Support for Ubuntu 26.10 6
2.3 New EDR/XDR Product Category 6
2.4 Trusted Platform Module (TPM) Detection on Windows 7
2.5 Secure Enclave Detection on macOS 7
3 – Patch 8
3.1 Restart Type for Third-Party Patches (OS Restart vs. Application Restart) 8
3.2 data_source Field in products.json 8
3.3 Patch Windows Updates by KB ID with InstallMissingPatches 9
3.4 Restart Type for OS Patches 9
3.5 InstallFromFiles Will No Longer Block Installers by OS Architecture 9
4 – Vulnerability 11
4.1 CVSS v4 Scores in Vulnerability Data 11
4.2 Vulnerability Assessment for Windows Drivers on Lenovo Devices 11
4.3 Per-Instance CVEs on Windows and macOS with detect_affected_instances 12
4.4 MetaDefender Tri Integration for OESIS Vulnerability Data 12
5 – AppRemover 13
5.1 End of Support for AppRemover package with the old engine on macOS 13
6 – Detailed SDK Information 13
7 – Contact 14

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

OESIS Framework Release Announcement November 2026

There are no new Required Actions this month. Previously announced actions remain in effect and are listed under the relevant component.

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.

Changes are grouped by component, so you can go straight to the modules you license. Items that apply to more than one component are repeated in each relevant section.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

1. All Components

Changes that apply across every OESIS Framework module.

WHAT'S NEW?

1.1 Bearer Token Authentication for VCR Gateway Downloads

Enhancement, all platforms, no SDK update needed, code change

SDK version: Server-side change on the VCR Gateway, no SDK update required.

The VCR Gateway download API (GET https://vcr.opswat.com/gw/file/download/{filename}) now accepts your download token in an Authorization: Bearer <token> request header, in addition to the existing token query parameter. Passing the token in a header keeps it out of URLs, which tend to end up in proxy and CDN access logs, browser history and Referer headers.

The change applies to every file served by the endpoint, including analog.zip, analog.zip.sig and the SDK public key. The token, how it is issued, and the type parameter are unchanged, and the token query parameter remains supported, so existing integrations keep working while you migrate. Send the token in one place only: a request that carries both the header and the query parameter, or more than one Authorization header, is rejected with HTTP 400.

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

1.2 x64 SDK Support on Windows on Arm through x64 Emulation

Enhancement, Windows, engine update needed

SDK version: Windows 4.3.6788.0

The x64 build of the SDK now runs on Windows 11 on Arm devices under Microsoft's x64 emulation. Previously, x64 SDK modules could fail to initialize on Arm devices, so method calls returned an error. The SDK now detects when it is running under emulation and adjusts an internal integrity check that was not compatible with it, so modules load and methods execute normally.

No integration change is needed: update to this engine version and deploy your existing x64 package to Windows on Arm endpoints.

UPCOMING CHANGES

No upcoming changes for All Components this month.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

REQUIRED ACTIONS

1.3 Engine Release Cadence Change

Release schedule update, all platforms

We have updated our Engine Package release cadence from weekly to bi-weekly. Releases occur twice per month, once in the second week and once in the fourth week. The mid-month release focuses on bug fixes, and the end-of-month release can also include new features. This change aligns with our new development framework, enabling more accurate estimations, clearer updates, and more reliable on-time releases.

1.4 End of Support for Windows 7 & Windows 8

End of support, Windows

OESIS Framework support for Windows 7 and Windows 8 (server versions included) will end on January 1, 2027. Here is what this means for your integration:

- Nothing is removed. Existing Windows 7 and Windows 8 data stays in the data files, and your current integration keeps working on these endpoints as it does today.
- From January 1, 2027, Windows 7 and Windows 8 will no longer actively receive fixes or updates, such as bug fixes, new application support or data updates.
- No changes to your integration are required.

To keep receiving OESIS Framework fixes and updates on these endpoints, simply upgrade them to a newer Windows version supported by the OESIS Framework. No other change is needed.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

2. Compliance

Product detection, security posture and device information.

WHAT'S NEW?

2.1 Change Logs for Compliance Data

Enhancement, all platforms, data update needed

SDK version: Windows 4.3.6706.0, macOS 4.3.6098.0, Linux 4.3.5726.0

Compliance data packages (libwaresource) now include change logs in JSON format, generated per platform (macOS, Windows, and Linux). For the engine package release, a changelog folder is placed under offline_resource with a separate change log for each platform, covering the changes since the last successful release, hotfixes included. For daily compliance data updates, the change log is bundled inside compliance.zip, covering the changes since the last successful compliance.zip publish.

This is an additive change to the package structure, so no action is required unless you want to consume the change logs.

2.2 Compliance Module Support for Ubuntu 26.10

Enhancement, Linux, data update needed

SDK version: Linux 4.3.5785.0

Following Canonical's release of Ubuntu 26.10, the Compliance module now supports it in production. The Ubuntu 26.10 operating system identifier and end-of-life values are live in production data, so endpoints on the latest Ubuntu interim release are detected and assessed the same way as earlier Ubuntu versions.

2.3 New EDR/XDR Product Category

NEW feature, all platforms, engine update needed

SDK version: Windows 4.3.6669.0, macOS 4.3.6063.0, Linux 4.3.5670.0

The SDK now has a dedicated EDR/XDR category, 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 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.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

The EDR/XDR category is available in the SDK on all platforms. Today it is assigned to EDR/XDR products on Windows, and we will extend it to the EDR/XDR products we detect on macOS and Linux in upcoming data updates, so each product reports the same category on every platform.

UPCOMING CHANGES

2.4 Trusted Platform Module (TPM) Detection on Windows

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

2.5 Secure Enclave Detection on macOS

NEW feature, MacOS, engine update needed, code change

We are adding detection of the Apple Secure Enclave on macOS, the hardware security subsystem built into Apple silicon and T2-equipped Macs. You will be able to include Secure Enclave presence in your device posture checks.

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

REQUIRED ACTIONS

No required actions for Compliance this month.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

3. Patch

Patch detection, installation and patch data.

WHAT'S NEW?

3.1 Restart Type for Third-Party Patches (OS Restart vs. Application Restart)

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

SDK version: Windows 4.3.6788.0, macOS 4.3.6181.0, Linux 4.3.5785.0

We are adding a new restart_type field so you can tell, before installing a third-party patch, whether it needs a full operating system restart or only an application restart. Until now, requires_reboot in patch_aggregation.json and requires_restart in patch_aggregation_v2.json only said whether a restart was needed, so integrations that skip every patch with a restart flag also skipped patches that only need the application to be restarted.

The field is a string with four values: os_restart, application_restart, none, and unspecified. It is present on every entry in patch_aggregation.json and patch_aggregation_v2.json, alongside requires_reboot and requires_restart, and in the GetLatestInstaller result alongside reboot_required. The existing fields are unchanged. unspecified means the scope depends on endpoint conditions at install time, so rely on the InstallFromFiles return code (1003 for an OS restart, 1005 for an application restart) in that case.

In this release the field carries a determined value for third-party patches only, and OS update results (Windows Update and Linux package-manager flows) return unspecified. Restart classification of existing catalog entries is being improved over time, so expect unspecified for some patches that advertise a restart.

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

3.2 data_source Field in products.json

Enhancement, all platforms, data update needed

SDK version: Data update only, no SDK update required.

Every signature in products.json now includes a data_source field that tells you where the signature's support data originates. Permitted values are opswat and winget, and more sources may be added in the future. This lets you determine data provenance offline from products.json alone, without calling the SDK.

The value matches the signature-level data_source already published in moby.json, and is consistent with the patch-level data_source in patch_aggregation.json. This is an additive change, so existing integrations continue to parse the file without modification.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

UPCOMING CHANGES

3.3 Patch Windows Updates by KB ID with InstallMissingPatches

Enhancement, Windows, engine update needed, code change

We are adding an optional kb_id input to each patches[] entry of InstallMissingPatches (method 1014) for Windows Update Agent (signature 1103). You will be able to remediate a vulnerability by passing its Microsoft KB number directly, without having to parse the patch title and product. Existing title and product input continues to work unchanged, and if an entry carries both, kb_id takes priority.

When a KB matches more than one applicable missing update, all matched updates are installed, and the result reports the normalized kb_id of each entry. A malformed or missing selector returns WAAPI_ERROR_INVALID_JSON, and kb_id on a signature other than 1103 or a non-Windows platform returns WAAPI_ERROR_NOT_SUPPORTED.

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

3.4 Restart Type for OS Patches

Enhancement, Windows & Linux, data update needed, engine update needed

Building on the new restart_type field for third-party patches, we plan to extend the same pre-install signal to OS patches. patch_system_aggregation.json and patch_system_aggregation_v2.json will carry restart_type, and the GetLatestInstaller result for Windows Update (signature 1103) will return a value derived from the system catalog instead of unspecified. Until then, continue to rely on the InstallFromFiles return code for OS update flows.

3.5 InstallFromFiles Will No Longer Block Installers by OS Architecture

Enhancement, Windows, engine update needed, code change

Today InstallFromFiles refuses some patch packages on certain OS architectures, for example a number of x64 installers on Windows ARM64, and returns WA_VMOD_ERROR_OS_ARCHITECTURE_NOT_SUPPORTED (-1046). Because GetLatestInstaller still returns those installers, an integration that calls both methods on the same endpoint can receive a patch that InstallFromFiles then rejects.

We have decided to remove this SDK-side architecture check. InstallFromFiles will run the installer that GetLatestInstaller returns and let the vendor installer apply its own architecture checks, as x64 applications commonly run on ARM64 through emulation. When a vendor installer rejects the architecture, the error response will carry the installer's native error in the error_message field, including the vendor error code and message when the installer returns them, so you can see why it failed. Applications with

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

known vendor architecture limitations are listed in the KB article Applications Observed Failing to Patch on Windows ARM64.

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

REQUIRED ACTIONS

No required actions for Patch this month.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

4. Vulnerability

Vulnerability assessment and CVE data.

WHAT'S NEW?

4.1 CVSS v4 Scores in Vulnerability Data

Enhancement, all platforms, engine update needed, data update needed

SDK version: Windows 4.3.6669.0, macOS 4.3.6063.0, Linux 4.3.5670.0

Vulnerability data now carries CVSS v4 scores, the latest version of the Common Vulnerability Scoring System published by FIRST, alongside the existing CVSS v2 and v3 data. GetProductVulnerability (method 50505) returns a new cvss_4_0 object inside cves[].details, next to cvss_2_0 and cvss_3_0, and the server-side cves.json feed carries the same object for third-party CVEs.

The object includes the vector string, base score and base severity, the exploitability and impact metrics, and the threat and supplemental metrics when the source provides them. CVSS v4 adoption varies by vendor, so cvss_4_0 is present only for CVEs that have CVSS v4 data. Client-side support uses v2mod.dat. This is an additive change, so existing integrations continue to parse the response unchanged.

4.2 Vulnerability Assessment for Windows Drivers on Lenovo Devices

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

SDK version: Windows 4.3.6788.0

The SDK now reports CVEs for installed Windows drivers. A new method, GetDriverPatchVulnerabilities, identifies the CVEs associated with the drivers on an endpoint, including the CVE ID, severity and affected driver version, and links each CVE to the driver patches that remediate it, so you can assess and remediate driver exposure the same way you do for applications. Driver CVE data is available for the Lenovo devices supported by driver patching (DetectDriverFirmwarePatches), and Dell coverage will follow in a future release.

Driver vulnerability data is available for both endpoint and server-side use. On the endpoint it ships in driv.dat, which is loaded with LoadDriverFirmwareDatabase (method 50900), the same method used for driver patching. On the server side, driver CVEs are included in cves.json with the existing schema, and the new vuln_driver_associations.json maps each driver CVE to its driver identifiers. DetectDriverFirmwarePatches also accepts a new detect_type value, installed, which returns the catalog patches that are already installed or up to date.

Some driver CVEs may be reported without a remediating patch when the vendor does not publish one for that driver version. Driver vulnerability assessment and driver patching are both covered under the VAPM license.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

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

4.3 Per-Instance CVEs on Windows and macOS with detect_affected_instances

Enhancement, Windows & MacOS, engine update needed, code change

SDK version: Windows 4.3.6788.0, macOS 4.3.6181.0

GetProductVulnerability (method 50505) now supports the optional detect_affected_instances input on Windows and macOS, matching its existing behavior on Linux. When an application is installed more than once on an endpoint, for example system-wide and per user, or by several users at different versions, setting the flag to true makes the SDK evaluate every instance, for active and inactive users, and report which instances each CVE affects in cves[].affected_app_instances[].

Without the flag, the method keeps its current behavior and evaluates a single instance resolved from the active user session, so it returns one user's results and fails with WAAPI_ERROR_NO_ACTIVE_USER_SESSION when no user is logged on. For service deployments, we recommend calling DetectProducts with detect_all_users_products: true, then GetVersion for each instance, then GetProductVulnerability with detect_affected_instances: true, and mapping affected_app_instances[].id back to the detected instances.

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

UPCOMING CHANGES

4.4 MetaDefender Tri Integration for OESIS Vulnerability Data

Enhancement, all platforms, data update needed

Planned release: End of November 2026.

We are integrating MetaDefender Tri into the OESIS Framework as our primary vulnerability data source. MetaDefender Tri provides AI-based vulnerability intelligence, which lets OESIS unify CVE data and publish new CVEs to customers more quickly.

MetaDefender Tri will be the primary source behind the server-side and client-side vulnerability data files that OESIS generates. The change is delivered through the existing OESIS data files, so no change to how you call vulnerability methods is expected. Keep consuming the vulnerability data files as you do today, and you will receive newly published CVEs faster.

REQUIRED ACTIONS

No required actions for Vulnerability this month.

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

5. AppRemover

Application removal.

WHAT'S NEW?

No new changes for AppRemover this month.

UPCOMING CHANGES

No upcoming changes for AppRemover this month.

REQUIRED ACTIONS

5.1 End of Support for AppRemover package with the old engine on macOS

End of support, Mac

Two packages of the AppRemover module on macOS have been 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 continue receiving updates and full technical support for the AppRemover module.

6. Detailed SDK Information

This is just the tip of the iceberg! You can view all the supported applications on our support charts:

6.1 Windows Support Charts

6.2 Mac Support Charts

6.3 Linux Support Charts

6.4 SDK API Documentation

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.

7. Contact

Are you a customer and have questions about this list? Please contact our trusted support team at support_sdk@opswat.com

©2026 All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.