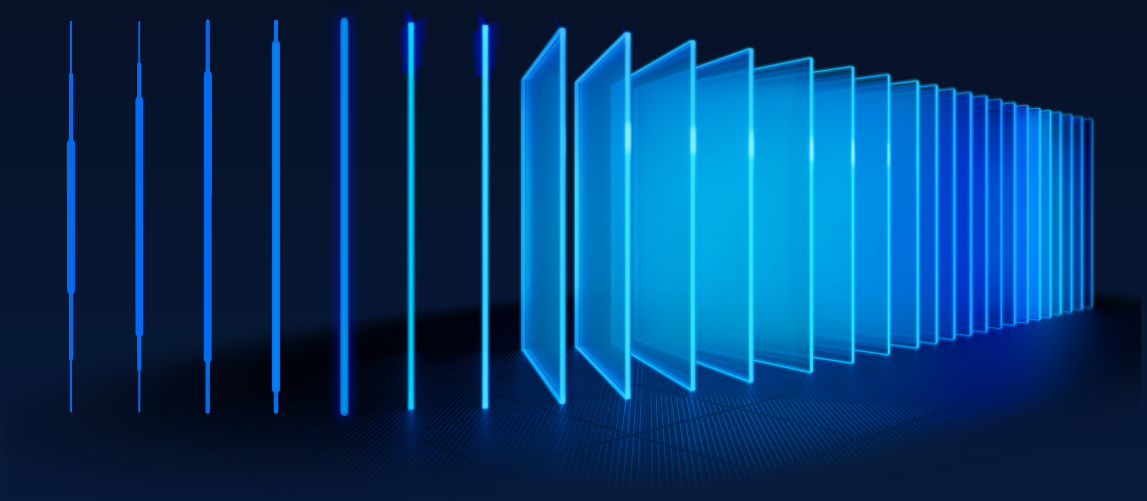
OPSWAT.

SDK News

OESIS Framework Update
December 2026

Announcement Date
2026/12/01



Contents

OESIS Framework Release Announcement December 2026 3
1. All Components 4
1.1 Self-Service OESIS Application and OESIS OK Certification Submissions 4
1.2 Engine Release Cadence Change 4
1.3 End of Support for Windows 7 & Windows 8 5
2. Compliance 6
2.1 Separate Per-User and Per-Machine Mozilla Firefox Installations on Windows 6
2.2 Tamper-Resistant Security Product State Reporting on Linux 6
2.3 Trusted Platform Module (TPM) Detection on Windows 7
2.4 Secure Enclave Detection on macOS 7
2.5 Detection of Rebranded TrendAI Products 7
2.6 OESIS Framework Support for iOS and Android 8
3. Patch 9
3.1 Patch Windows Updates by KB ID with InstallMissingPatches 9
3.2 Expanded Patching Coverage on Windows ARM64 9
3.3 InstallFromFiles No Longer Blocks Installers by OS Architecture 9
3.4 Specific Error Codes and Messages for Third-Party Installer Failures 10
3.5 Per-Patch Result Codes for Windows Update in InstallMissingPatches 11
3.6 Restart Type for OS Patches 11
3.7 Non-Security Windows Updates in patch_system_aggregation_v2.json 11
3.8 Signing Certificate Information for Patch Installers 12
4. Vulnerability 13
4.1 MetaDefender Tri Is Now the Primary OESIS Vulnerability Data Source 13
5. AppRemover 14
6. Detailed SDK Information 14
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 December 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 Self-Service OESIS Application and OESIS OK Certification Submissions

New feature, All platforms, No SDK update needed

SDK version: Server-side change in My OPSWAT Portal (version 2026.4.3.0), no SDK update required.

You can now request that an application be added to the OESIS Framework, or submit it for OESIS OK Certification, directly through the My OPSWAT Portal. You can track each submission's progress in real time and download the verified certification report once testing is complete.

To submit an application:

- Sign in to the My OPSWAT Portal, or sign up if you don't have an account yet.
- Go to **OEM Portal** > **OESIS Submission** > **Add Submission** and choose the submission type, for example "Add Application to OESIS Framework".
- Upload the installer or provide a download link, then enter the application name, version and operating system.
- Select the application category and the capabilities you would like supported (Detection, Patch, Vulnerability, App Removal), and add a license key if one is needed to test all features.
- Add any additional information and the technical contacts we should reach out to.

Create one submission per product version and operating system. You receive email updates as your submission progresses, and the OPSWAT team contacts you through the portal and by email if anything else is needed, such as access to your console.

UPCOMING CHANGES

No upcoming changes for All Components this month.

REQUIRED ACTIONS

1.2 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

©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.

development framework, enabling more accurate estimations, clearer updates, and more reliable on-time releases.

1.3 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 Separate Per-User and Per-Machine Mozilla Firefox Installations on Windows

Enhancement, Windows, Data update needed, Engine update needed

SDK version: Windows 4.3.6960.0

When Mozilla Firefox is installed both per-machine and per-user on the same Windows endpoint, the SDK now reports each installation as its own product, so both copies are versioned, assessed for vulnerabilities and patched independently.

Per-user installations are reported under three new signatures, and per-machine installations stay on the existing Mozilla Firefox signatures:

- 5145 Mozilla Firefox User (x86)
- 5146 Mozilla Firefox User (x64)
- 5147 Mozilla Firefox User (arm64)

Mozilla Firefox ESR follows the same model: per-user installations are reported as 5376 Mozilla Firefox ESR (User) (x86) and 5377 Mozilla Firefox ESR (User) (x64), separately from the per-machine signatures.

Detection, patching (**GetProductPatchLevel**, **GetLatestInstaller** and **InstallFromFiles**) and vulnerability assessment for the per-user signatures are delivered through the latest compliance and Analog data packages, and the browser-specific methods for these signatures come with the engine version above. Patching a per-user installation runs in that user's session, while the user is logged on. This change also applies to the Patch and Vulnerability modules.

2.2 Tamper-Resistant Security Product State Reporting on Linux

Enhancement, Linux, Engine update needed

SDK version: Linux 4.3.5843.0

GetRealTimeProtectionState and **DetectProducts** on Linux now read the service state of security products from system commands through a protected channel, so other programs on the endpoint cannot influence the results. The security posture you report for Linux endpoints is more reliable, with no change to your integration.

©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

2.3 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

2.4 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

2.5 Detection of Rebranded TrendAI Products

Enhancement, Windows & macOS, Data update needed

Trend is renaming several of its endpoint products in its December release as part of the TrendAI rebranding. We are updating detection so these products are reported under their new names, and releases under the previous names continue to be detected. Installation paths and macOS bundle IDs stay the same.

On Windows:

- Apex One becomes TrendAI Apex One
- TrendAI™ Deep Security Agent becomes TrendAI Vision One agent
- TrendAI™ Endpoint Basecamp becomes TrendAI Vision One Endpoint Basecamp
- TrendAI™ Cloud Endpoint becomes TrendAI Vision One Cloud Endpoint

©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.

- TrendAI Vision One™ Zero Trust Secure Access becomes TrendAI Vision One AI Gateway User Access

On macOS:

- Apex One (Mac) Security Agent and Endpoint Sensor becomes TrendAI Vision One agent for Mac
- TrendAI Vision One™ Zero Trust Secure Access becomes TrendAI Vision One AI Gateway User Access

2.6 OESIS Framework Support for iOS and Android

New feature, iOS & Android, Engine update needed, Code change

We are adding iOS, iPadOS and Android as platforms of the OESIS Framework. The same methods and the same JSON contract you use on desktop will run on mobile devices, delivered as iOS and Android builds of the OESIS package, so you can reuse your existing integration to assess the posture of mobile endpoints.

The first release will cover:

- Operating system information with **GetOSInfo**
- Product detection and product information with **DetectProducts** and **GetProductInfo**
- Installed application discovery with **DiscoverProducts** (Android)
- Encryption state with **GetEncryptionState**
- Device information with **GetDiskSpace**, **GetCpuAndRamInfo** and **GetPowerOptions**
- Compliance reporting with **GetComplianceReport**

Supported operating systems will be iOS and iPadOS 26 and 27, and Android 12 through 16. Mobile runs under its own license, loaded through the same mechanism as the current license, and writes V4 debug logs the same way as the desktop SDK.

For details, early access or a proof of concept, please contact your OPSWAT Product Manager, Sales representative or Customer Support team.

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 Patch Windows Updates by KB ID with InstallMissingPatches

Enhancement, Windows, Engine update needed, Code change

SDK version: Windows 4.3.6852.0

InstallMissingPatches (method 1014) for Windows Update Agent (signature 1103) now accepts an optional **kb_id** input in each **patches[]** entry. You can 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

3.2 Expanded Patching Coverage on Windows ARM64

Enhancement, Windows, Data update needed

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

We have reviewed the applications that were excluded from patching on Windows ARM64 and enabled patching for 62 of them. Each application was validated through the full patching flow on Windows 11 ARM64, including download, installation and patch level, so these applications now patch on ARM64 endpoints the same way they do on x64 endpoints.

The change is delivered through the production Analog data, and the ARM64 entries on the support charts grow accordingly. Applications with known vendor architecture limitations are listed in the KB article Applications Observed Failing to Patch on Windows ARM64.

3.3 InstallFromFiles No Longer Blocks Installers by OS Architecture

Enhancement, Windows, Engine update needed, Code change

SDK version: Windows 4.3.6960.0

©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.

InstallFromFiles (method 50301) now runs the installer that **GetLatestInstaller** returns and lets the vendor installer apply its own architecture checks, as x64 applications commonly run on ARM64 through emulation. Previously the SDK refused some packages on certain OS architectures with **WA_VMOD_ERROR_OS_ARCHITECTURE_NOT_SUPPORTED** (-1046), so an integration could receive a patch from **GetLatestInstaller** that **InstallFromFiles** then rejected.

When a vendor installer rejects the architecture, the error response carries 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 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

3.4 Specific Error Codes and Messages for Third-Party Installer Failures

Enhancement, Windows & macOS, Engine update needed, Code change

SDK version: Windows 4.3.6960.0, macOS 4.3.6348.0

When a third-party installer fails during **InstallFromFiles** (method 50301) or **InstallPackage** (method 50305), the SDK now forwards the installer's own error in the **error_message** field of the error response. You can see the cause of a failed installation, for example a prerequisite the vendor installer requires, without opening the vendor's installer log.

When the cause is clear, the SDK also returns a specific error code instead of the generic **WA_VMOD_ERROR_INSTALLATION_FAILED** (-1034):

- Installer file or folder not found: -28
- Archive cannot be extracted (macOS): **WA_VMOD_ERROR_EXTRACT_FAILED** (-1036)
- Disk image cannot be opened (macOS): **WAAPI_ERROR_INVALID_INSTALLER** (-1082)
- Disk image busy (macOS): **WAAPI_ERROR_RESOURCE_BUSY** (-70)
- Copy or install denied (macOS): **WAAPI_ERROR_ACCESS_DENIED** (-22)
- File access blocked by a macOS protection such as System Integrity Protection, a privacy setting or an MDM policy: **WAAPI_ERROR_FILE_ACCESS_BLOCKED** (-1085), a new code
- Disk full (macOS): **WAAPI_ERROR_INSUFFICIENT_DISK_SPACE** (-1072)

Other installer failures keep returning -1034, now with the installer's message in **error_message**.

See InstallFromFiles and InstallPackage in the OESIS API documentation for the **error_message** field and the return codes.

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

©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.

3.5 Per-Patch Result Codes for Windows Update in InstallMissingPatches

Enhancement, Windows, Engine update needed, Code change

SDK version: Windows 4.3.6960.0

InstallMissingPatches (method 1014) for Windows Update Agent (signature 1103) now returns a **return_code** for every entry in **patches[]**, as it already does on Linux. The SDK maps the Windows Update HRESULT reported in **patches[].code** to an OESIS error code, so you can handle patch results the same way on Windows and Linux without per-platform parsing.

For example:

- Update installed: 0
- Update not found, **0x80240008:** -28
- Update cancelled, **0x8024000B: WAAPI_ERROR_WUA_CALL_CANCELLED** (-1100)
- Access denied, **0x80070005: WAAPI_ERROR_ACCESS_DENIED** (-22)

The SDK error code list now includes the **WAAPI_ERROR_WUA_*** codes for Windows Update results. The existing **state** and **code** fields and the top-level result code are unchanged.

See Return Codes in the OESIS API documentation for the full list of return codes.

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

UPCOMING CHANGES

3.6 Restart Type for OS Patches

Enhancement, Windows & Linux, Data update needed, Engine update needed

Building on the **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.

3.7 Non-Security Windows Updates in patch_system_aggregation_v2.json

Enhancement, Windows, Data update needed

patch_system_aggregation_v2.json will include the non-security and out-of-band Windows updates, such as Critical Updates and Updates, that **patch_system_aggregation.json** already lists. Both files will describe the same set of OS patches, so every KB that an endpoint reports as missing through **wuov2.dat** can be found and downloaded from either file.

©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 schema and structure of **patch_system_aggregation_v2.json** stay the same, and the file grows by more than 15,000 entries.

3.8 Signing Certificate Information for Patch Installers

Enhancement, All platforms, Data update needed, Code change

We are adding the signing certificate identity of patch installers, such as the certificate subject (Issued To) and thumbprint, to the patch data alongside the SHA-256 hash we publish today. This gives you a second way to confirm that an installer comes from its genuine publisher, including installers whose file changes behind a fixed download link.

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 MetaDefender Tri Is Now the Primary OESIS Vulnerability Data Source

Enhancement, All platforms, Data update needed

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

The OESIS Framework now uses MetaDefender Tri as its 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 is 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 needed. Keep consuming the vulnerability data files as you do today, and you receive newly published CVEs faster.

You can also explore this vulnerability intelligence on the MetaDefender Tri OESIS dashboard. Sign in through the My OPSWAT Portal with single sign-on to use notifications, tracking, watch lists and the APIs.

UPCOMING CHANGES

No upcoming changes for Vulnerability this month.

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

No required actions for AppRemover this month.

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

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.