OPSWAT.

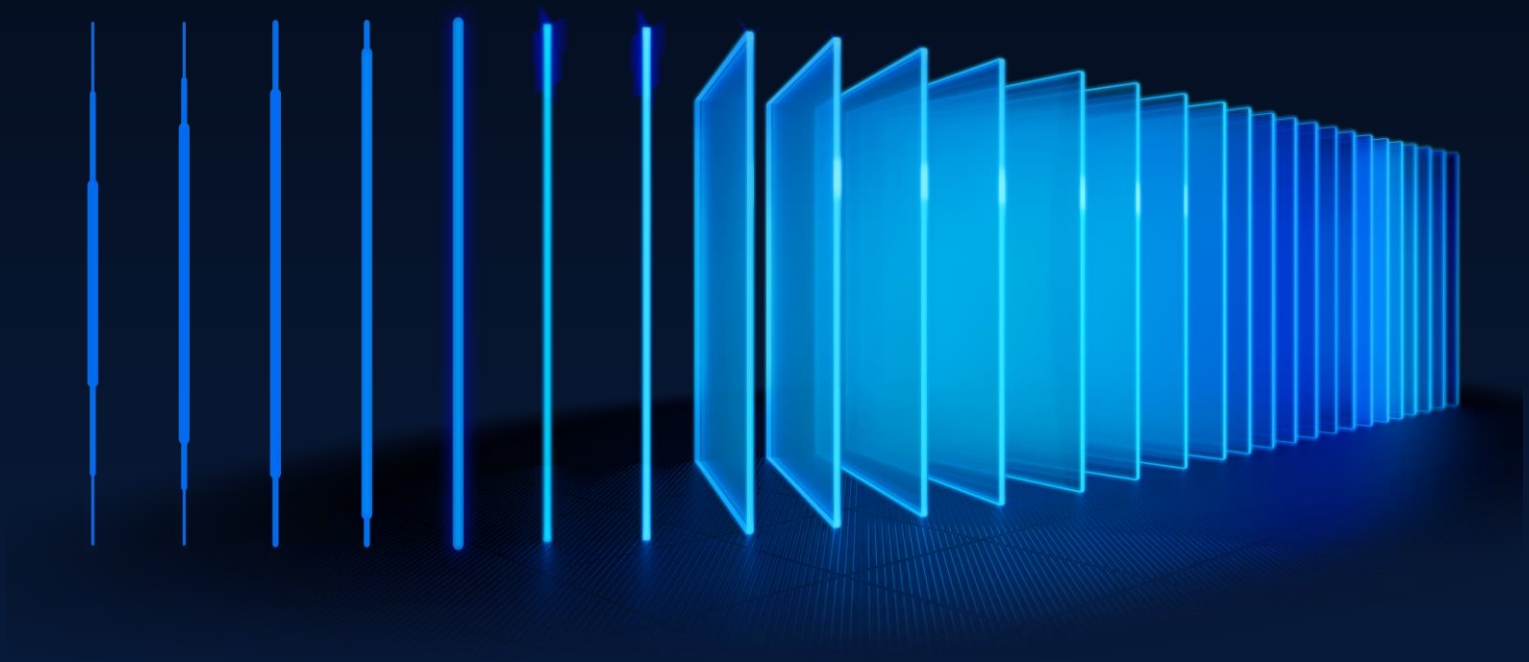
SDK News

OESIS Framework Update

August 2026

Announcement Date

2026/08/04



OPSWAT.

Contents

OPSWAT.

OESIS Framework Release Announcement
August 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 Clearer Windows Defender Real-time Protection Status when managed by 3rd Party AV

FEATURE: COMPLIANCE

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

We have enhanced the GetRealTimeProtection method for Windows Defender to make it clearer when Windows Defender is being managed (and effectively disabled) by a third-party antivirus product.

Earlier, 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 previous 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

1.2 New has_static_download_link Field in products.json

FEATURE: PATCHING

ENHANCEMENT, ANALOG PACKAGE, 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.

1.3 Full Disk Access Requirement Exposed in Patch Data (macOS)

FEATURE: PATCHING

NEW FEATURE, ANALOG PACKAGE, DATA UPDATE NEEDED

To improve the reliability of patch management on macOS, we have added a new attribute, *requires_full_disk_access*, to help administrators identify applications that require Full Disk Access (FDA) permissions for successful installation or updates.

Some macOS applications require the OESIS Agent to have Full Disk Access to perform patching operations. Without this, update attempts might fail silently or with permission errors if the necessary rights haven't been granted.

requires_full_disk_access is now available in *patch_aggregation.json*, specific to macOS product entries only; non-macOS patches remain unaffected. The field returns “yes” for applications requiring FDA and “no” otherwise.

By exposing this requirement directly in OESIS, integrators can have the technical insights needed to build more robust and user-friendly patch management workflows for macOS environments.

1.4 Regulatory Compliance (Generic Mode + PCI-DSS 4.0.1)

FEATURE: COMPLIANCE

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

A new *GetComplianceReport* method is available on Windows, macOS, and Linux, returning a device-state compliance report with no pass/fail verdict, so you can map endpoint posture directly to a regulatory framework. Currently we support two modes: Generic Mode (*framework_id*: "generic", *framework_version*: "1.0") and PCI-DSS 4.0.1 (*framework_id*: "pci_dss", *framework_version*: "4.0.1"), the latter returning each control with its requirements[] mappings.

- Generic Mode currently covers 12 controls: *anti_malware, firewall, anti_phishing, backup, encryption_at_rest, dlp, vpn, patch_management, vulnerability_management, remote_control, public_file_sharing, web_conference*
- PCI-DSS 4.0.1 currently covers 6 controls: *anti_malware, encryption_at_rest, firewall, vpn, dlp, patch_management*

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

1.5 Specific Error Code for Insufficient Disk Space During KB Installation

FEATURE: PATCHING

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED

InstallFromFiles no longer reports a generic *WA_VMOD_ERROR_INSTALLATION_FAILED (-1034)* when a Windows KB installation fails because the disk ran out of space mid-install. The SDK now returns a new, specific error, *WAAPI_ERROR_INSUFFICIENT_DISK_SPACE*, so callers can distinguish a disk-space failure from other installation failures and remediate accordingly, for example by prompting the operator to free up space before retrying.

This addresses the case where free space looks sufficient at install start but drops below what DISM requires at peak activity, causing the installer to abort. A small number of KB installer types do not follow the Windows disk-space error convention and may still return -1034 in this scenario.

1.6 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 patching support for 67 additional applications (81 signatures in total). The newly supported applications are:

Product	Signature
Backupper	297
Partition Assistant	299
Exact Audio Copy	1969
Resource Hacker	915
Find and Mount	2496
Azul Zulu JDK 23	3972
Azul Zulu JRE 8	4009
Reg Organizer	1456
Registry Life	2237
Lightscreen	2874
CloneSpy	1518
Convertilla	2401
Cppcheck	1572
AnyToISO	1073
Uninstall Tool	1594
Secure IT	1169
Doxygen	292
EaseUS Todo Backup	120
Eclipse Temurin JDK with Hotspot 17	3588
Eclipse Temurin JDK with Hotspot 19	3657, 3652
Eclipse Temurin JRE with Hotspot 19	3653, 3654

Eclipse Temurin JDK with Hotspot 25	4087
Eclipse Temurin JDK with Hotspot 8	3578
Flock	3238
Gajim	718
Geany	1906
AusweisApp	4270
Chromium	4172
VeraCrypt	2334
Advanced SystemCare	242
Jabra Direct	3324
PyCharm Community	1133
PyCharm Professional	1132
JetBrains WebStorm	1104
Karen's Replicator	451
Microsoft ASP.NET Core Runtime 6.0	3751, 3740
Microsoft ASP.NET Core Runtime 9.0	3994, 4093
Microsoft .NET Runtime 6.0	3737, 3745
Microsoft .NET Runtime 7.0	3746, 3736
Microsoft .NET Runtime 9.0	3993, 3991
Microsoft .NET SDK 6.0	3735, 3749
Microsoft .NET SDK 7.0	3747, 3734
Microsoft .NET SDK 8.0	3876, 3877
Microsoft .NET SDK 9.0	3989, 3990
Power Automate for desktop	4056
MKVToolNix	2900
ExtractNow	799
Wireless Network Watcher	917
OBS Studio	4174
Obsidian	4177
foobar2000	1358
AnyBurn	2031
ExamDiff	1067
Rclone UI	4274
Lightshot	2878
Softros LAN Messenger	773
Splashtop Streamer	3901
010 Editor	1931
UrBackup	1091
Wise Game Booster	981
Wise JetSearch	980
Kodi	1948
Angry IP Scanner	3909
NetSpeedTray	4268
MyPhoneExplorer	2064

Vim	4171
Everything	2890, 3560, 3844, 3845

2 – Upcoming Changes

2.1 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.

2.2 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

2.3 New error_message Field in Error Responses

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS, ENGINE UPDATE NEEDED

We are adding a new *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.

2.4 New data_source Field in moby.json

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

We are adding a *data_source* field to every signature object in *moby.json*, indicating where the signature's support data originates. The field sits at the signature level, alongside *signature_name*, *signature_id*, and *vendor_name*, and carries exactly one value from a supported source enum, currently *opswat* and *winget*, extensible to other sources in the future.

Existing OPSWAT-curated signatures are backfilled with *data_source: "opswat"*, and WinGet-sourced signatures carry *data_source: "winget"*, so consumers can distinguish OPSWAT-curated support data from WinGet-sourced data directly in the file.

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