OPSWAT.

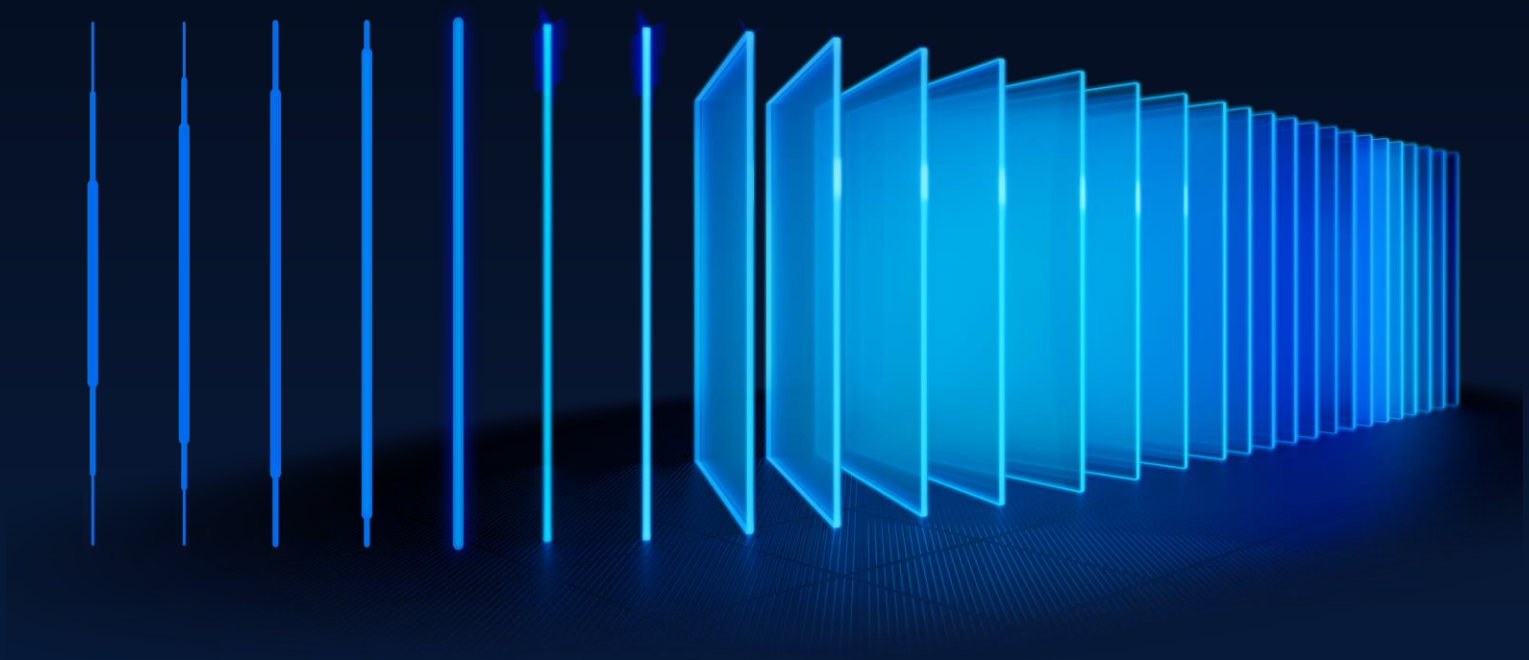
SDK News

OESIS Framework Update

September 2026

Announcement Date

2026/09/01



OPSWAT.

Contents

OPSWAT.

OESIS Framework Release Announcement
September 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 EPSS Score in Vulnerability Data

FEATURE: VULNERABILITY

NEW FEATURE, ALL PLATFORMS, DATA UPDATE NEEDED

The Exploit Prediction Scoring System (EPSS) score is now included in 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 includes 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.

1.2 Scan Products Across All Users on macOS

FEATURE: COMPLIANCE

ENHANCEMENT, MACOS, ENGINE UPDATE NEEDED, CODE CHANGE

DetectProducts on macOS now supports 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, including when no user is logged in. When omitted or set to false, detection remains scoped to the active user as before.

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.

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

1.3 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.

1.4 New data_source Field in moby.json

FEATURE: ALL MODULES

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

Every signature object in moby.json now includes a *data_source* field, 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.

1.5 GetVersion Returns Language Name on macOS

FEATURE: ALL MODULES

ENHANCEMENT, MACOS, ENGINE UPDATE NEEDED

GetVersion (method 100) on macOS now returns the product's language name in the *language.name* field, which previously always returned "n/a". Both short and full language formats are supported (for example, *en* and *en-EN*), and the value feeds server-side JSON mapping and patch-centric workflows that rely on language information.

When the language cannot be retrieved, the field still returns "n/a", consistent with the existing Windows behavior, and the *language.code* field is unchanged, continuing to return "n/a". This is an additive change, existing integrations continue to work without modification.

1.6 Trend Micro Products Rebranded to TrendAI

FEATURE: COMPLIANCE

ENHANCEMENT, WINDOWS & MACOS, DATA UPDATE NEEDED

Following the vendor's rebranding from Trend Micro to TrendAI, our detection data now carries new signatures under the TrendAI product names as following:

- TrendAI™ Deep Security Agent, from 20.0.31108 on Windows (including the market name "TrendAI 服务器深度安全防护系统客户端") (signature 4380)

- Apex One Security Agent, from 14.0.20842 (also 14.0.20898 and 14.0.20957) on Windows (signature 4381)
- TrendAI™ Security Agent, from 3.7.2050 on macOS (signature 100656)

1.7 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 13 additional applications (15 signatures in total). The newly supported applications are:

Product	Signature
3DF Zephyr Free	4287
Arelle	4294
BurnAware Free	1614
BurnAware Pro	1917
HWMonitor	1939
PeaZip	268, 3558
Go	3789
PowerShell	3504, 3503
Notion	4175
Endstate	4246
Markdown Studio	4247
Writ	4288
Hardware Visualizer	4244

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.

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.

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