OPSWAT.

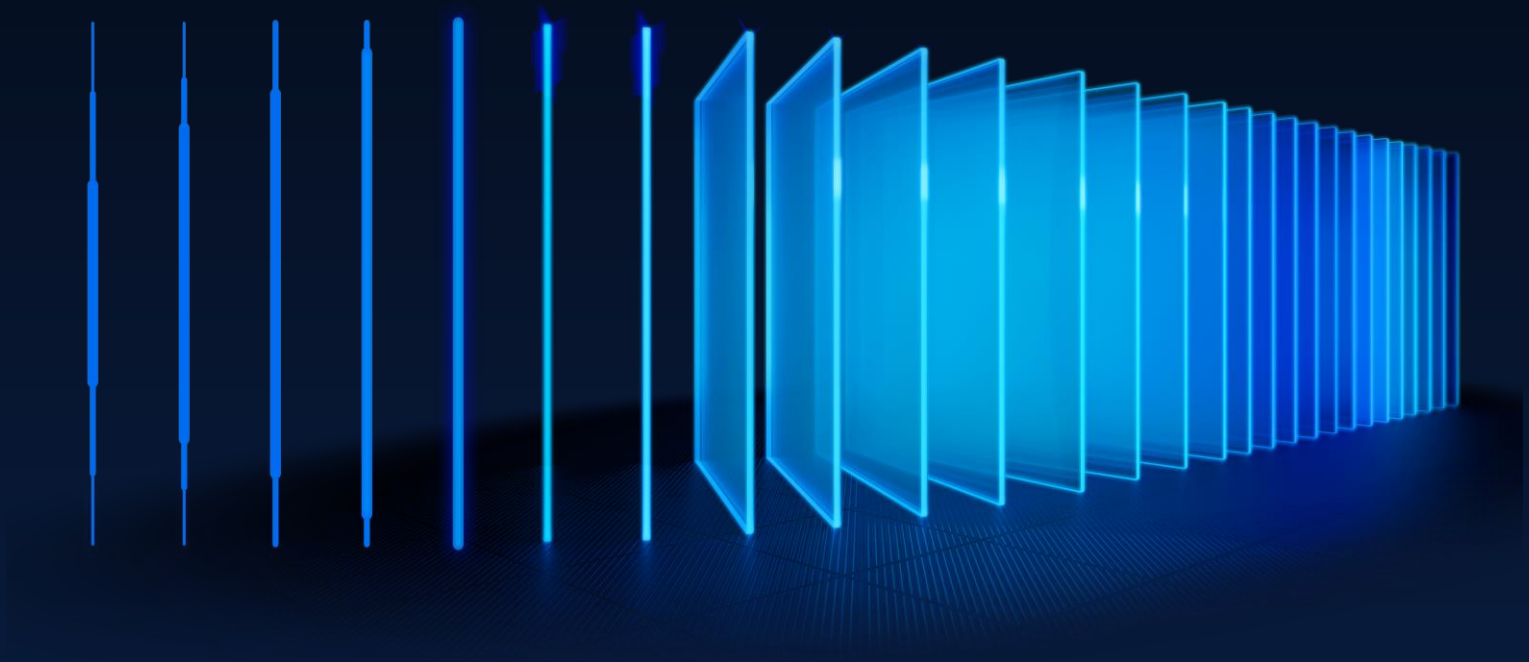
SDK News

OESIS Framework Update

April 2026

Announcement Date

2026/04/14



OPSWAT.

Contents

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

OPSWAT.

OESIS Framework Release Announcement
April 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 Improved Readability for raw_json.js in compliance.zip

FEATURE: COMPLIANCE

ENHANCEMENT, ALL PLATFORMS, DATA UPDATE NEEDED

We have updated the raw_json.js file in our Compliance data (for all platforms including Windows, macOS, Linux) to use a pretty-printed JSON format. This improves readability for customers who inspect or troubleshoot this datafile manually.

As a result, the Compliance package (compliance.zip) is slightly larger (from ~13 MB to ~14 MB), but no changes are required for existing integrations that programmatically consume this file.

1.2 Real-time monitoring on macOS

FEATURE: COMPLIANCE

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

Real-time monitoring (RTM) has been expanded to macOS. Unlike the previous compliance checks, which are on-demand audits, RTM is dynamic, adapting to live events and status changes as they occur.

In this delivery, the engine now provides initial macOS support for GetRealtimeProtectionState of "Bitdefender Antivirus for Mac", enabling customers to detect real-time protection state changes on macOS endpoints through OESIS.

This update is delivered in SDK from version 4.3.5280.0 (mac native).

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

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

1.3 Support for Patching Multiple App Instances on macOS

FEATURE: PATCHING

ENHANCEMENT, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

OESIS Framework Patch Management on macOS now better supports patching when multiple instances of the same app exist, even when they are renamed or installed outside the standard Applications folder.

This enhancement allows customers to patch the intended instance without leaving confusion regarding the patching status or vulnerability reporting.

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

1.4 Per-Instance CVE Visibility in GetProductVulnerability for Linux

FEATURE: VULNERABILITY ASSESSMENT

NEW FEATURE, LINUX, ENGINE UPDATE NEEDED, CODE CHANGE

We have extended the OESIS Framework on Linux to properly handle multiple instances of the same application and show which instances are affected by each CVE.

What has changed:

- DetectProduct detects and returns multiple instances of the same application on a single Linux endpoint.
- GetVersion will now return the version for each detected instance.
- GetProductVulnerability will:
    - Scan all application instances for a given signature, and
    - Return CVEs enriched with a new affected_app_instances field, for example:

```
"affected_app_instances": [
  {
    "id": "string",    // matches instance ID from DetectProduct
    "path": "string"
  }
]
```

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

1.5 HubStaff 32-bit auto-patching support removed in OESIS

FEATURE: PATCHING

BEHAVIOR CHANGE, WINDOWS, DATA UPDATE NEEDED

We have updated our patch data to reflect HubStaff ending support for 32-bit Windows from its 1.8.x releases.

On 64-bit Windows, InstallFromFiles, GetLatestInstaller, and GetProductPatchLevel continue to work as expected and will install or report the latest release of HubStaff.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

On 32-bit systems, fresh install and auto-patching using InstallFromFiles for the latest version of HubStaff has been blocked to avoid vendor-side failures. However, GetLatestInstaller and GetProductPatchLevel will resolve to the last version of HubStaff that supports 32-bit: 1.7.8, rather than returning any installer newer than version 1.8.x that cannot run on x86.

1.6 Delta File Architecture for Linux Vulnerability Data

FEATURE: VULNERABILITY ASSESSMENT

NEW FEATURE, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

To help customers reduce bandwidth usage and improve update performance, we have extended our delta file architecture to additional Linux vulnerability data files in OESIS Framework.

Instead of downloading the full 130 MB file, customers can now retrieve smaller baseline and delta files (liv_baseline.dat, liv_delta.dat), which are packaged in analog.zip and supported by OESIS data pipeline.

This change helps large-scale deployments avoid full large-file downloads on every update while preserving data integrity. Integrators might need to update their data delivery logic to take advantage of the new delta architecture.

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

1.7 Optional CPE-enriched Vulnerability Payload for v2mod-vuln-oft

FEATURE: VULNERABILITY ASSESSMENT

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

To help customers get CPE data on the endpoints, the OESIS Framework introduces a new optional supplemental payload, v2mod-vuln-oft-extra.dat, alongside the existing v2mod-vuln-oft.dat vulnerability dataset.

The extra file, delivered under analog/client and available individually or via analog.zip on VCR Gateway, contains the additional CPE information.

When placed in the same folder as v2mod-vuln-oft.dat, OESIS automatically loads both files and returns CVEs enriched with their CPEs. If the extra file is absent, the SDK behavior and dataset size remain unchanged, so other customers continue using the lean v2mod-vuln-oft.dat flow without impact.

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

1.8 Add detection support for VMware Workstation 17.x

FEATURE: COMPLIANCE

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

We've extended the OESIS Framework to fully support VMware Workstation 17.x on Windows, with verified coverage for version 17.5.2 under normal user, admin, and service modes. The core VMware Workstation methods now work as expected for this product line, while actions like Run and TerminateProcesses continue to require admin privileges by design.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

In addition, the ListSnapshots method (WAAPI_MID_LIST_SNAPSHOTS – method ID 1018) has been updated to accept an optional password field in the input JSON, enabling snapshot retrieval for password-protected VMs.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

OPSWAT.

2 – Upcoming Changes

2.1 Clearer Windows Defender Real-time Protection Status when managed by Third-Party AV

FEATURE: COMPLIANCE

ENHANCEMENT, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

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

Today, 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 current 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.


```
{
  "result": {
    "code": 0,
    "details": {
      "antispyware": false,
      "antivirus": false
    },
    "enabled": false,
    "managed_by_3rd_party_products": [
      {
        "displayName": "CrowdStrike Falcon",
        "pathToSignedProductExe": "C:\\Program Files\\CrowdStrike\\CSFalconService.exe",
        "signature": 2866
      }
    ],
    "method": 1000,
    "signature": 477,
    "timestamp": "1765255198",
    "timing": 16
  }
}
```


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.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo 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

2.2 Remove “method_status” hive from patch_status.json

FEATURE: PATCHING

BEHAVIOR CHANGE, ALL PLATFORMS, DATA UPDATE NEEDED, CODE CHANGE

To ensure that *patch_status.json* is dedicated solely to indicating the patching status of applications, and to consolidate application capabilities into a single data file (*products.json*), the “method_status” hive will be removed from *patch_status.json* starting in May.

As a replacement for the “method_status” hive, we have introduced a new field called “useable_download_link” in *products.json*. This field serves the same purpose as the “method_status” hive, indicating whether the *GetLatestInstaller* method can return a download link when the “download” field is set to 0.

2.3 Support for Patching Multiple App Instances on Linux

FEATURE: PATCHING

ENHANCEMENT, LINUX, ENGINE UPDATE NEEDED, CODE CHANGE

OESIS Framework will support patching when multiple instances of the same app exist on Linux devices, even when they are renamed or installed outside the standard Applications folder.

This enhancement allows customers to patch the intended instance without leaving confusion regarding the patching status or vulnerability reporting.

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

2.4 Integration between OESIS Framework and WinGet

FEATURE: ALL MODULES

NEW FEATURE, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

Starting in May, we will introduce integration between the OESIS Framework and WinGet. With this integration, the number of applications supporting detection, vulnerability assessment, and patch management will increase rapidly.

Data from WinGet will be returned when the new “data_source” flag is defined in the JSON input of the DetectProducts, DiscoverProducts, and GetLatestInstaller methods with the appropriate value (“opswat” and/or “winget”). When the “data_source” flag is enabled, the JSON output will include products/patches covered by the WinGet integration. Users can distinguish between data from OPSWAT and WinGet by using the “data_source” field with the value “opswat” or “winget.”

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

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

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.

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

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 opswat-support@opswat.com

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.

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

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.