OPSWAT.

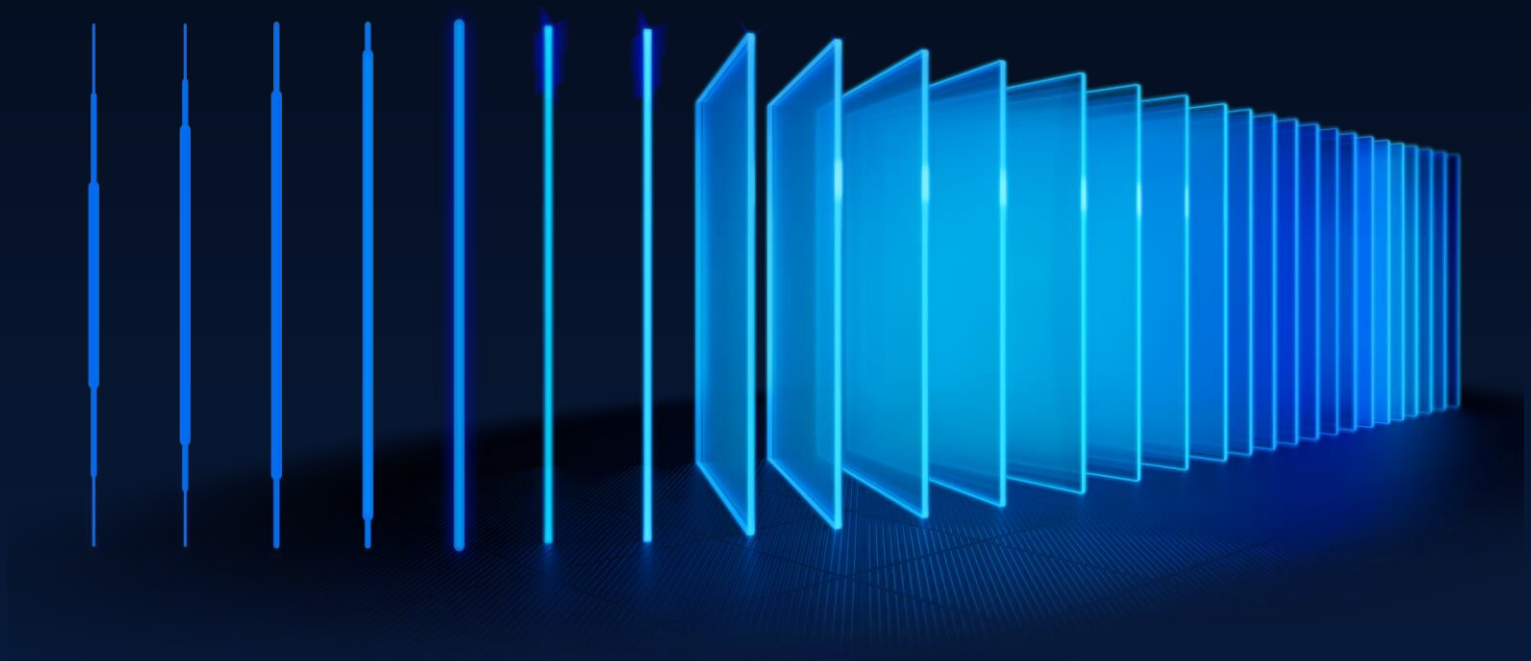
SDK News

MetaDefender Endpoint Security SDK Update

July 2025

Announcement Date

2025/07/08



OPSWAT.

Contents

OPSWAT.

MetaDefender Endpoint Security SDK Release Announcement
June 2025

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 MetaDefender Endpoint Security SDK 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 projects. Prepare for an epic upgrade that'll take your security to the next level.

1.1 Differentiate Ubuntu Resolutions in GetProductVulnerability

NEW FEATURE, LINUX, DATA UPDATE NEEDED

We've enhanced GetProductVulnerability method to provide clearer insights into Ubuntu vulnerability resolutions by distinguishing between Ubuntu Pro and Community fixes.

This only affects Ubuntu packages; standard APT packages are not impacted.

A new overlay field is now included in the resolution data, but only when a matching association exists and the value is not empty. This field clearly indicates whether a given fix belongs to Ubuntu Pro or Community, helping you understand what's available for your system more accurately.

This update helps improve clarity for end-users and supports customer requirements for more transparent security insights.

1.2 Query CrowdStrike ZTA Scores via GetAgentState

NEW FEATURE, SDK UPDATE NEEDED

We've added support for retrieving Zero Trust Assessment (ZTA) scores from CrowdStrike Falcon directly through the GetAgentState SDK method — enabling integrated, real-time device trust evaluation.

By including the assessment_queries field in your request, you can now query ZTA scores (ranging from 0 to 100) for a target endpoint, helping strengthen your Zero Trust decision-making.

Sample input:

```
{
  "input": {
    "signature": 2866,
    "method": 1012,
    "assessment_queries": [
      {
        "data_type": "zta_score",
        "credentials": {
          "base_url": "<string>",
          "client_id": "<string>",
          "client_secret": "<string>"
        }
      }
    ]
  }
}
```

Sample result:

```
{
  "result": {
    "assessment_results": [
      {
        "data_type": "zta_score",
        "value": <int>
        "return_code": <int>, // 0 for a successful query
      }
    ]
    ...
  }
}
```

This new feature is now available, providing a streamlined way to include trusted risk scoring within your agent state checks.

1.3 InstallMissingPatches for Software Update now works on macOS Apple Silicon

FIX, MAC, DATA UPDATE NEEDED

We've resolved a major issue affecting the InstallMissingPatches method for Software Update on macOS with Apple Silicon chips. The method now works reliably with administrative (privileged) permissions, allowing successful patch installations in most scenarios.

While this fix significantly improves functionality, there are still known limitations — such as failure when running in Service mode. We're actively working on these and will continue to enhance support in upcoming updates.

1.4 Deprecation Notice: GetSystemVulnerabilities - Method ID: 50509

DEPRECATION

We’d like to inform that method 50509 - GetSystemVulnerabilities, which checks for potential system vulnerabilities based on product version, is now deprecated and will be removed in a future update.

The method will remain temporarily available but will no longer receive updates or enhancements. While it still works for now, we recommend planning for its removal in a future release and migrating to supported alternatives.

OPSWAT.

2– Upcoming Changes

2.1 Support Differential Update for Windows Update Offline data

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

In the July release, the SDK will introduce a new feature that enables customers to distribute smaller Windows Update Offline data to endpoints using a differential update mechanism.

This feature will include a new Analog package, named analogv2.zip, which contains two new files: wuo_baseline.dat and wuo_delta.dat. These files allow customers to implement differential updates by distributing both files to endpoints initially. After that, for up to one year, customers will only need to distribute the smaller wuo_delta.dat file to keep the Windows Update Offline data up to date.

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

2.2 V3V4 Adapter to use libc++ instead of libstdc++

ENHANCEMENT, MAC, LIBRARY UPDATE

Soon, all Mac V3V4 Adapter libraries will be built via libc++ instead of libstdc++. This shift will bring better support for modern C++ standards, faster compilation, and better optimizations.

You will need to change your compile process for the macOS to add support for the libc++ library.

2.3 New value for requires_reboot field in patch_aggregation.json file

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

Due to the specific behavior of certain products that require updating the Microsoft Visual C++ Redistributable, two different restart scenarios may occur:

- If the machine already has the up-to-date version of Microsoft Visual C++ Redistributable, the installation of the target product does not require a restart.
- If the machine has an outdated version of Microsoft Visual C++ Redistributable, the installation of the target product does require a restart.

This behavior impacts how the MDES SDK handles the requires_reboot field. Since this condition is environment-dependent and cannot be predicted, we are introducing a new value called "conditional" to represent such cases. The "conditional" value allows the SDK to recognize and respond appropriately to these dynamic restart requirements.

2.4 Non-security Microsoft patch support

NEW FEATURE, WINDOWS, DATA UPDATE NEEDED, CODE CHANGE

In the September release, the SDK will be able to detect and install Microsoft non-security patches when using the Windows Update Offline functionality.

Currently, the Microsoft categories supported by the SDK are Security Updates, Service Packs, and Update Rollups.

The Microsoft categories we will be adding are Regular Updates and Critical Updates.

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

2.5 Realtime monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

This autumn, the SDK will provide **Real-time monitoring** on Mac operating systems. Unlike the current compliance checks, which are on-demand audits, real-time monitoring is dynamic, adapting to live events and rule changes as they occur.

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

2.6 Introduce new server data in the Analog package

NEW FEATURE, ANALOG, DATA UPDATE NEEDED

We introduced new patch-related information that contains hash string of patches in the server files of Analog package as follows:

In patch_system_aggregation.json:

```
"analog_id": {
    ...
    "download_link": {
        ...
        "sha1": <string>
    },
    "optional": <bool>
    ...
}
```

In patch_aggregation.json:

```
"analog_id": {
    ...
    "download_link": {
        ...
        "sha256": <string>
        },
    ...
}
```

2.7 Introduce new patch-related information in GetLatestInstaller

NEW FEATURE, DATA UPDATE NEEDED

We introduced new patch-related information that contains vendor name, description, required restart information of patches in the json out of GetLatestInstaller method as below:

```
result: {
  ...
  "description": <string>,
  "vendor": <string>,
  "reboot_required": <bool>,
  "optional": <bool>
}
```

OPSWAT.

3 – Required Actions

3.1 CVE-2025-0131

VULNERABILITY, WINDOWS

An incorrect privilege management vulnerability in the OPSWAT MetaDefender Endpoint Security SDK used by the Palo Alto Networks GlobalProtect™ app on Windows devices allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY\SYSTEM. However, execution requires that the local user also successfully exploits a race condition, which makes this vulnerability difficult to exploit.

To address CVE-2025-0131, please upgrade your MDES SDK to version 4.3.4451 or later.

3.2 We moved the OesisPackageLinks.xml behind the VCR gateway

SECURITY UPDATE, VCR GATEWAY

Starting December 31st, 2024, the OesisPackageLinks.xml file are relocated behind the VCR Gateway for enhanced security, replacing its currently public location.

Since September 1st, 2024, the file can be accessed via the VCR Gateway. You can download the file by following these steps: copy and paste this URL: https://vcr.opswat.com/gw/file/download/OesisPackageLinks.xml?type=1&token=<authorization_token> into your browser and replace **<authorization_token>** with your unique token. If you don't have a unique token, please contact support.

This update ensures continued and secure access, and users should have updated their systems to accommodate this change.

3.3 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.

Starting January 1, 2026, the OSX package will be removed. We recommend upgrading to AppRemover OSX V2 to ensure your system receives all new updates and comprehensive technical support for the AppRemover module.

3.4 End of Support for Windows 7 & Windows 8

END OF SUPPORT, WINDOWS

Starting January 1, 2026, support for Windows 7 and Windows 8 (server versions included) will be removed from the SDK. To ensure security, compatibility, and optimal performance with MDES SDK, 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 opswat-support@opswat.com.

OPSWAT.

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