OPSWAT.

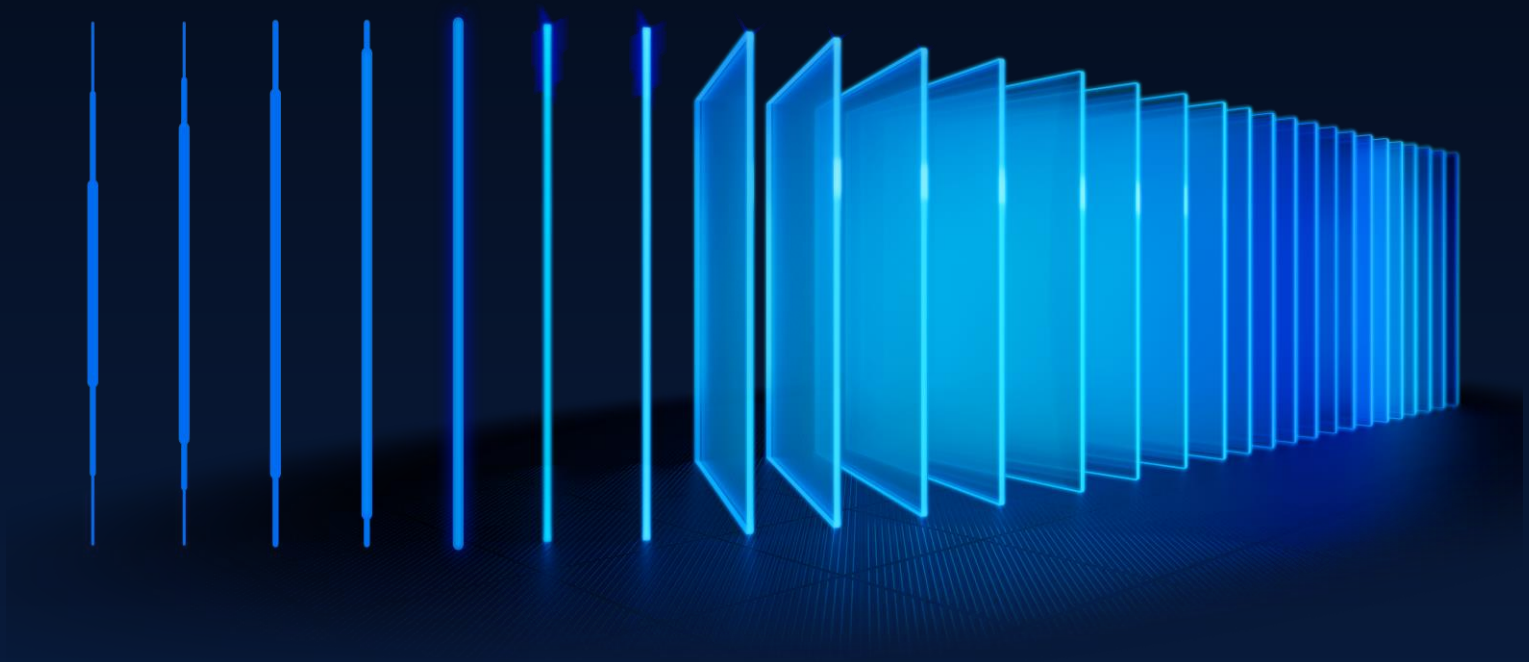
SDK News

MetaDefender Endpoint Security SDK Update

November 2025

Announcement Date

2025/11/10



OPSWAT.

Contents

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

1.1 Vulnerability Assessment support for SUSE 15.6 & 15.7

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED

We're excited to announce that our SDK now supports vulnerability assessment for SUSE Linux Enterprise Server versions 15.6 and 15.7. This update brings enhanced detection of CVEs for these latest SUSE releases, ensuring your Linux environments remain secure and compliant.

Stay protected with the latest vulnerability intelligence!

1.2 Ability to input the expected SHA-256 when installing patches

ENHANCEMENT, ALL PLATFORMS, ENGINE UPDATE NEEDED, CODE CHANGE

We've enhanced the InstallFromFiles method to support passing an expected SHA-256 hash for installer verification.

If the installer's hash does not match, our SDK will now return a WAAPI_ERROR_HASH_MISMATCH error, preventing potential tampering or corruption. This enhancement ensures greater integrity and security during patch installations.

This update is live and production-ready across all supported platforms.

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

1.3 Last Server Connection Time for CrowdStrike Falcon

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

Our SDK now supports retrieving the "last connection time to server" attribute from CrowdStrike Falcon agents on Windows, macOS, and Linux.

This update empowers administrators to monitor when endpoints last communicated with the CrowdStrike Falcon cloud, strengthening visibility and security management.

By including the assessment_queries field in your request, you can now retrieve the last server connection time as a numeric epoch value.

Sample input:

```
{
  "input": {
    "signature": <number>,
    "method": 1012,
    "assessment_queries": [
      {
        "data_type": "last_server_connect_time",
        // credentials is only needed to query last_server_connect_time for macOS
        "credentials": {
          "base_url": <string>,
          "client_id": <string>,
          "client_secret": <string>
        }
      }
    ]
  }
}
```

Sample result:

```
{
  "result": {
    "assessment_results": [
      {
        "data_type": "last_server_connect_time",
        "value": <number>,
        "return_code": <number>, // 0 for a successful query
        "message": <string>
      }
    ]
    ...
  }
}
```

This release marks just the first step, plans are already underway to extend this capability to additional EDR products soon.

1.4 Flexible Patch Installation for macOS

ENHANCEMENT, MAC, DATA UPDATE NEEDED, CODE CHANGE

We're excited to announce a significant enhancement in InstallMissingPatches method of macOS Software Update. The update enables patch installation using any user account on the device, not just the currently active one.

To apply this update, simply ensure your SDK version is updated to the latest release. When calling InstallMissingPatches method on macOS for Software Update, include the optional username and password fields in your request payload to specify the desired user account for patch installation. If these fields are omitted, our SDK will default to using the currently active user as before.

This enhancement added flexibility is especially valuable for managed environments, allowing administrators to specify the username and password for patch installation, regardless of which user is logged in. Both standard and admin accounts are supported (with some limitations on Intel-based Macs), making patch management more adaptable and compliant with diverse organizational policies.

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

1.5 Behavior change in the Installer Signature Check feature

BEHAVIOR CHANGE, MAC, WINDOWS, ENGINE UPDATE NEEDED, CODE CHANGE

Starting **November 1, 2025**, a behavior change will be applied to the Installer Signature Check feature to enhance security maturity. When the digital signature of an installer is checked during the patching process:

- (no change) If the installer's digital signature is valid and passes the check, the installer will be verified by the SDK, and the patching process will continue as normal.
- (no change) If the installer's digital signature is invalid and fails the check, an appropriate error message will be returned, and the installation process will be aborted.
- (NEW) If the installer's digital signature is missing, an appropriate error message will be returned, and the installation process will also be aborted.

Tips: If you receive an error due to a missing or invalid digital signature, you can use the skip_signature_check flag of the InstallFromFiles method to bypass the Installer Signature Check feature.

2– Upcoming Changes

2.1 New Software Categories for Compliance

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

We are pleased to announce that our Q1-2026 release will introduce three new software categories: Vulnerability Management, Artificial Intelligence, and Gaming.

All new categories will include comprehensive support methods such as version detection, running state, installation directories, and more.

Stay tuned for further details as we approach the release date.

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

2.2 Support for the Windows 10 Extended Security Updates (ESU) program

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

After October 14, 2025, Microsoft will no longer provide security patches, feature updates, or technical support for Windows 10. Windows 10 systems will still function, but become progressively vulnerable to security threats and software compatibility issues.

Therefore, Microsoft is introducing the Windows 10 Extended Security Updates (ESU) program, which gives customers the option to receive security updates for PCs enrolled in the program.

To extend support for Windows 10 and ensure the MDESDK remains compatible with future updates of Windows 10, we have decided to continue supporting Windows 10 via the Windows 10 Extended Security Updates (ESU) program. This support will be applied to devices running Windows 10, version 22H2 with KB5046613, or a later update installed, and having an active ESU subscription.

2.3 Support for Patching Multiple App Instances on macOS

ENHANCEMENT, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

We are pleased to inform you that our team is actively investigating ways to improve patching support on macOS.

In the future release, our SDK will support patching multiple instances of applications, even when they are renamed or installed outside the standard Applications folder.

This enhancement ensures that after patching, only the latest version remains, eliminating unpatched or vulnerable duplicates across all locations.

2.4 New "usable_download_link" field in products.json

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We will add a new "usable_download_link" boolean field to each product entry in analog/server/products.json. This field will indicate whether the installer download link from GetLatestInstaller(download=0) will be valid.

- If "usable_download_link" is true, agents will be able to use the download link.
- If "usable_download_link" is false, agents should not attempt to use it.

This update will help improve reliability by providing clear guidance to agents. To reduce failed download attempts, please plan to update your integration logic to check this field before fetching installer links.

2.5 Detect Per-User Applications for All Users

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

We are enhancing our SDK to enable detection of per-user applications across Windows, MacOS, and Linux platforms. By the end of 2025, a new flag, detect_all_users_products, will be introduced to the DetectProducts method.

By default, this field is false and detection is limited to only applications installed for the active user and those available to all users (system-wide). When detect_all_users_products is set to true, this field enables detection of all applications installed on the device, including those specific to other user accounts.

On Windows, when detect_all_users_products is enabled, the output will include a new installed_for_users field for each detected product. This field lists all users (by SID and username) who have the product installed in per-user mode.

This enhancement provides a comprehensive view of software inventory across all user profiles on a device.

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

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> in to 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

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 previous planned).

To ensure security, compatibility, and optimal performance with MDES SDK, we recommend upgrading endpoints to a supported Microsoft operating system.

OPSWAT.

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 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