OPSWAT.

Removable Media Protection Overview

OPSWAT Central Management together with OPSWAT Client manages removable media on endpoint devices, preventing the endpoint from connecting to any unexamined portable media, including flash drives, memory cards, SIM cards, CDs, DVDs, and smart phones. It monitors endpoints for any removable media that end users insert and enables your organization to manage how each endpoint treats the media, based on preconfigured security policy.

Block. Protect. Secure.

OPSWAT Client can block any connection the media tries to make with an endpoint, and it can block all connections, except those processes your organization specifies. It blocks all access to themedia, while allowing this service to pass the content through advanced content security technologies, which verifies and sanitizes the data.

The OPSWAT Client is the endpoint agent that runs on Windows devices and enforces the Removable Media Protection features.

Removable Media Access Protection

To provide this protection, OPSWAT (as a member of the Microsoft Intelligent Security Association and a participant in the Microsoft Virus Initiative), uses a signed driver that loads into the Windows OS and hooks into the file system on the device.

There is a load-order and access-order among all the file system drivers, and Microsoft enforces the load-order and access-order by a guaranteed ID (the Altitude Number). As the Windows OS is booted, Windows will enforce the load/access order, as provided by Microsoft and agreed-to with their partners (such as OPSWAT).

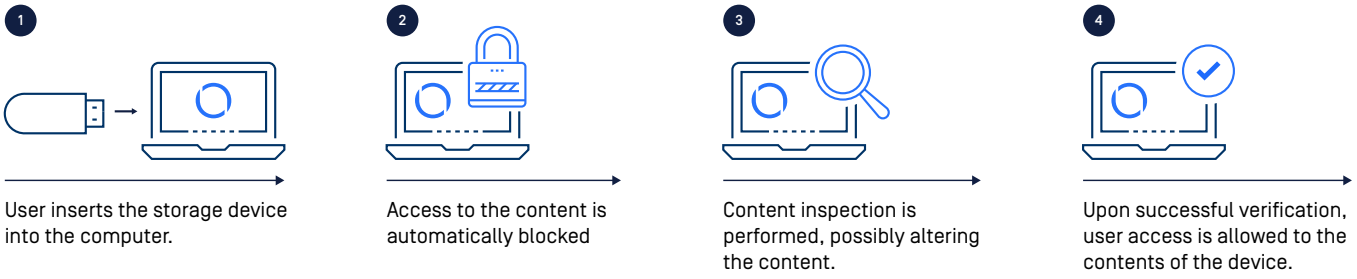
The OPSWAT driver loads high enough into the OS to ensure that the Removable Media Protection feature can intercept and block accesses to the files on the removable media, with only a few exceptions by the most critical processes running on the machine.

OPSWAT.

Removable Media Protection Overview

Removable Media Protection Features

Multiscanning
The Removable Media Protection feature undergoes a rigorous testing process to ensure that the OPSWAT Client can block all access to the removable drives until the drive is scanned by 20 anti-virus engines and deemed threat-free.



Removable Media Protection in action

Deep CDR
This feature also has the capability to sanitize files within removable media devices using OPSWAT's Deep CDR technology. Users can select the option to upload only sanitized files into local storage or into MetaDefender Vault, ensuring that data at rest will not cause any harm to your organization.

Media Validation
If the removable media devices have been scanned by MetaDefender Kiosk before, the Media Manifest feature makes sure that you don't have to scan the data again. This feature will leave behind a manifest file on the device, enabling it to bypass the next scans, saving time and resources.

Straight-to-Vault Storage
Our removable media protection solution has also integrated MetaDefender Vault, allowing quick and secure data storage. With this feature enabled, users can move data from removable devices directly to MetaDefender Vault after the scans, creating a streamlined work process.

The OPSWAT client supports Windows 10 and Windows 11 OS versions.

Resources

https://www.opswat.com/products/metaaccess/advanced-endpoint-protection
https://www.opswat.com/partners/microsoft