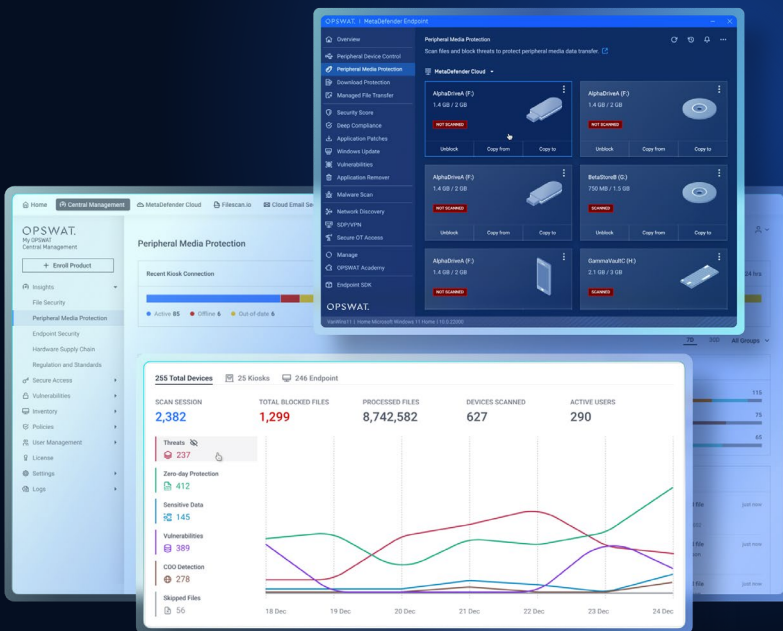
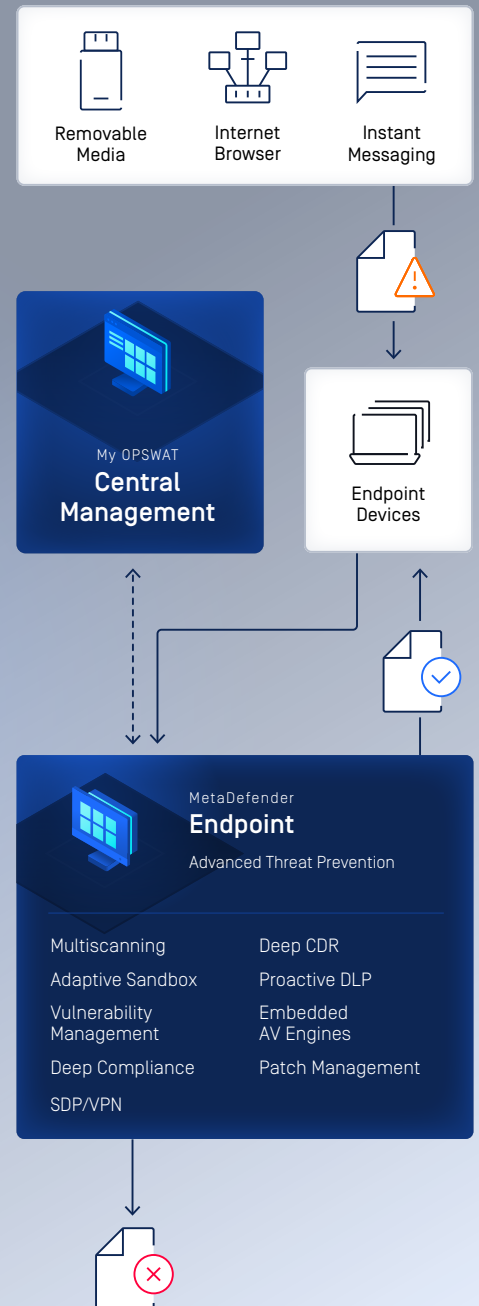


METADefENDER™

Endpoint

Seamless Defense Against Peripheral and Removable Media Threats

Traditional endpoint protection solutions, including single antivirus engines and dedicated device control tools, fall short of providing adequate protection against evolving threats. With advanced threat prevention technologies, including MetaScan™ Multiscanning and Deep CDR™ to scan and sanitize files, MetaDefender Endpoint secures assets from peripheral and removable media-borne threats and enables monitoring and auditing of usage in alignment with your organization's security and compliance standards. MetaDefender Endpoint additionally scans files downloaded from the internet.



MetaDefender Endpoint provides a layer of security for your assets to protect devices from the threats presented by removable media.



Your First 500 Scans Are On Us
Download a fully functioning trial valid for 500 scans.

DOWNLOAD

Key Features



Peripheral Media Protection

Scan peripheral media before they are made accessible and only grant permission for those with no detected threats.



BadUSB Protection

Safeguard endpoints from malicious removable media threats, including BadUSB, rubber ducky, and other USB-based attacks.



Peripheral Device Control

Monitor and manage all ports and connected media with full visibility.



Patch & Vulnerability Management

Detect vulnerabilities in 900+ applications with recommended fixes, enable patching for 1100+ third-party applications and OS updates, manage unwanted applications and ensure system compliance.



Download Protection

Scan files downloaded from web browsers and instant messaging apps to ensure they are malware-free.



Advanced Malware Prevention

Detect over 99% of known malware by scanning with 30+ leading anti-malware engines simultaneously.



Prevent Unknown & Zero-Day Exploits

Recursively sanitize 200+ file types with Deep CDR technology and remove 100% of potential threats.



Internet Connected & Air-Gapped Support

Support for both online and air-gapped environments.



Admin File Management

File management administration via cloud and block file types according to extension. Support for encrypted and unencrypted archives.



Central Management

Manage and enforce policies with granular control using My OPSWAT™ Central Management (Cloud/On-premises).



Industry-Leading Technologies

Deep CDR, MetaScan MultiScanning, File-Based Vulnerability Assessment, Proactive DLP™, Adaptive Sandbox, Country of Origin.



Compliance Assurance

Assists with NERC CIP 003-7, HIPAA, SOC 2, ISO 27001, and more applicable frameworks to best monitor security controls on the endpoint.

Windows

Minimum Version

Windows 7/8/8.1/10/11;
Windows Server
2008 R2/2012/2012
R2/2016/2019/2022
R2/2012/2012
R2/2016/2019/2022/2025

Minimum System Requirements

CPU: 1 GHz
Hard disk space: 500MB

macOS

Minimum Version

OSX 10.15 /11/12/13/14/15/26

Minimum System Requirements

CPU: 1 GHz
Hard disk space: 500MB

Linux v3

Minimum Version

CentOS 7
Ubuntu 14.4

Minimum System Requirements

CPU: 1 GHz
Hard disk space: 500MB

Debian-based Linux v4

Minimum Version

Ubuntu 16 or newer
Mint 18 or newer
Debian 8 or newer

Minimum System Requirements

CPU: 1 GHz
Hard disk space: 500MB

Red Hat-based Linux v4

Minimum Version

CentOS 7.14 or newer
Red Hat Enterprise 7
or newer
openSUSE 11.4 or newer
SUSE Enterprise 12x
or newer
Fedora 27 or newer

Minimum System Requirements

CPU: 1 GHz
Hard disk space: 500MB

iOS

Minimum Version

iOS 15/16/17/18/26

Minimum System Requirements

iPhone 6s; iPad (4th generation) iPad Air; iPad mini

Android

Minimum Version

Android 8.0/9/10/11/12
/12.1/13/14/15/16

Minimum System Requirements

Memory: 2GB

OPSWAT.

Protecting the World's Critical Infrastructure