OPSWAT.

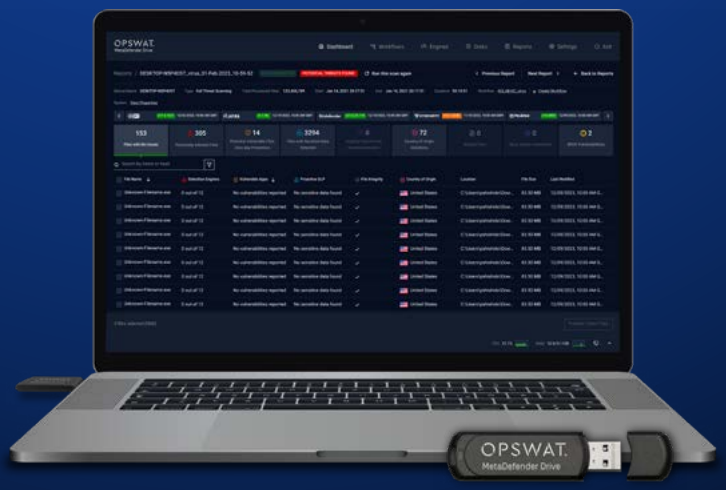
METADEFENDER™

Drive 2

Pre-Boot and In-Session Threat Scanning for Laptops and Desktops

MetaDefender Drive scans and verifies all devices before they connect to critical systems, with secure pre-boot and support for in-session scanning when uptime is required.

Pre-boot scanning enables verifying hardware outside the host operating system to uncover hidden threats before devices enter secure networks. For uptime-critical systems that cannot be powered down, in-session scanning enables malware detection without interrupting operations.



Key Features

Pre-Boot Scanning
Scans laptops, desktops, and critical devices from bare metal to user space files and directories with up to 8 anti-malware engines by securely booting from a built-in OS to uncover hidden malware, vulnerabilities, and risks at the hardware level.

In-Session Scanning
Scans devices while the system remains operational, ideal for critical environments where downtime is not acceptable, detecting threats using 3 anti-malware engines including ESET, Bitdefender, Predictive Alin AI.

Read-Only Scanning
Scans devices in read-only mode to prevent tampering and ensure file integrity.

Device Inventory Collection
Captures hardware, software, and system configuration details during In-Session scans, syncing device inventory to My OPSWAT™ Central Management for enterprise-wide visibility.

Central Manageability
Can optionally connect to My OPSWAT Central Management to manage reports and configurations from one place.

File-Based Vulnerability Assessment
Detects known vulnerabilities in over 20,000 software applications with a patented file-based approach.

Country of Origin Detection
Checks the device's software and flags anything that may violate country of origin compliance.

Encrypted Disk Support
(Including Microsoft BitLocker)
Detects encrypted volumes and prompts for a password. Supports LUKS-based encryption and macOS FileVault.

Multilingual Support
MetaDefender Drive comes with localization support, covering key interface elements in the following 12 languages: English, Dutch, German, Vietnamese, Korean, Chinese, French, Italian, Japanese, Arabic, Hebrew, and Polish.

Configurable Smart Scan
Configure a one-click Smart Scan, including anti-malware engines, security technologies, target directories, and operator guidance. It also includes custom dashboard button name and instructions for a single, purpose-built operational workflow.

Direct Threat Removal
Ability to remove unsafe files directly after scanning completion.

Plug and Sync
Automatically syncs approved policies, engine updates, and scan reports with My OPSWAT Central Management by plugging into MetaDefender Kiosk, no workstation or internet required.

Proactive DLP™
Detects sensitive and confidential data such as credit card and social security numbers in documents, images, and videos.

Centralized Scanning Profile
Ensuring policy consistency while allowing real-time local policy modifications with remote approval using a one-time password.

Specifications

Hardware

Dimensions	2.9 x 0.8 x 0.4” 71 x 18 x 9mm
Ports	1x USB 3.0 Type-A
Body	Aluminum FIPS 140-2 Level 2 compliant physical epoxy security encapsulation
Weight	1.34oz (38g)
Storage Capacity	1TB
Operating Temperature	32°F to 158°F | 0°C to 70°C
Operating Humidity	10% to 90%
Shock Resistance	1000G maximum
Hardware Warranty	1 year
Country of Origin	United States of America

Regulatory

Supports Regulatory Requirements	NERC CIP 003-7 and 010-4 NIST 800-53 and 800-82 US Executive Order 14028 ISO/IEC 27001
Trade Compliance	Trade Agreements Act
Cryptography Compliance	FIPS 140-2
Environmental Compliance	RoHS REACH

Software

MetaDefender Drive Advanced	Ahnlab, Avira, Bitdefender, ESET, K7, CrowdStrike, Trellix, Predictive Alin AI
MetaDefender Drive Enterprise	Ahnlab, Avira, Bitdefender, ESET, K7, Predictive Alin AI or K7, Quick Heal, Ahnlab, Avira, Bitdefender, Predictive Alin AI[1]
MetaDefender Drive Professional	Ahnlab, Avira, Predictive Alin AI

System Requirements

Minimum	Intel i3 or equivalent dual-core 64-bit processor HDD or SSD (PATA/IDE, SATA, NVMe, SCSI, USB) 1024×768 display
For Full Engine Scan	4 GB RAM or higher USB 2.0 port or higher
For In-Session Scan	Windows 10 or newer 4 GB RAM or higher 4 CPU
For Engine & Software Updates	8 GB RAM or higher USB 3.0 port or higher

Compatibility

Platform	x86-64 Intel- or AMD-based
Windows	XP, 7, 8, 8.1, 10, 11, Server 2012, Server 2016, Server 2019, Server 2022, Server 2025 FAT16, FAT32, NTFS, exFAT BitLocker[2]
Windows Embedded	XP, 7
Mac	Intel-based from 2006-2017 HFS, HFS+, APFS FileVault for APFS
Linux	Debian 5-based or newer, RHEL 6-based or newer EXT2, EXT3, EXT4, XFS, BTRFS, ReiserFS, JFS, ZFS[3] LUKS/LVM2

1 Made in India engine package
2 Supports BitLocker (using user password and recovery key).Does not yet support hardware-based disk encryption (default on some Windows Home laptops).
3 Supports ZFS (non-encrypted)

OPSWAT.
Protecting the World’s Critical Infrastructure

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.