

OPSWAT.

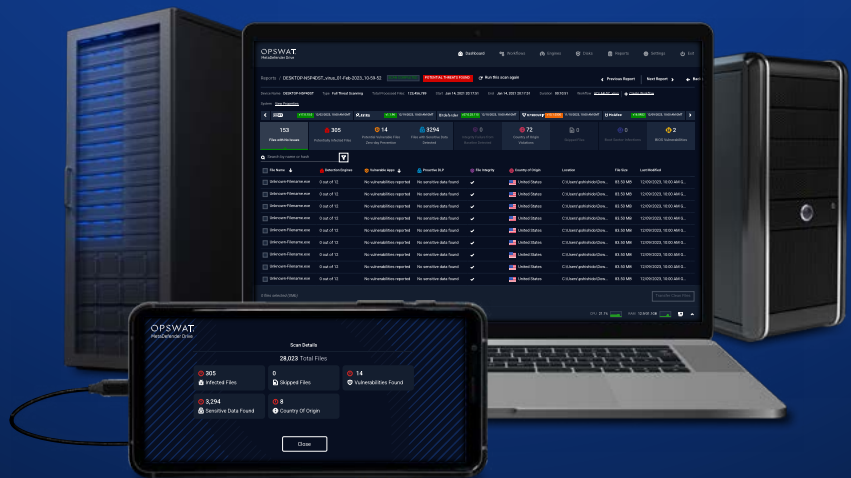
METADEFENDER™

Drive

WITH SMART TOUCH

MetaDefender Drive with Smart Touch delivers portable malware and compliance scanning, enabling organizations to inspect laptops, desktops, and servers before they power on and during system operations—even in isolated or air-gapped environments.

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.



Scan Across All Devices Including Servers, Desktops, and Laptops
With Ease Before They Enter Secure Environments

Built for remote and isolated environments where internet access is limited, MetaDefender Drive with Smart Touch operates fully standalone, with the capability to update applications, reports and engines directly on the device using Wi-Fi or cellular networks. With three hardware kill switches that physically disable wireless connectivity, MetaDefender Drive with Smart Touch ensures total control and zero risk to air-gapped networks and environments.

Key Features



Pre-Boot Scanning

Scans devices from bare metal to user space 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.



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.



Configurable Smart Scan

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



Centralized Scanning Profiles

Ensures policy consistency while enabling remote real-time access and usage policy modifications with approvals using a one-time password.



Proactive DLP™

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



Country of Origin Detection

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



File-Based Vulnerability Assessment

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



Enterprise Central Management

Securely integrates with My OPSWAT Central Management to provide automated report syncing, real-time monitoring, configuration, and actionable security insights.



Plug and Update

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

Smart Touch Only



Secure File Storage

Acts as a safe storage device, securely transferring files from any system that supports FAT32 or NTFS, with the transferred files remaining hidden until they are scanned and verified using a MetaDefender Kiosk.



Wireless Updates and Reporting

Easily update reports, engines, and applications over Wi-Fi or cellular networks.

METADEFENDER DRIVE WITH SMART TOUCH

Specifications

Hardware	
Screen	5.7" IPS TFT screen with a 720x1440 resolution
Dimensions	152 mm [5.98 in] x 74 mm [2.91 in] x 15 mm [0.59 in]
USB	USB C: USB 3.0 data, [power delivery dual-role port]
Weight	262g [0.58 lb]
Hardware Warranty	1 year
Wi-Fi	802.11a/b/g/n/ac/ax, 2.4GHz/5GHz
Cellular	4G/LTE
Country of Origin	Made in the U.S.A [U.S. Model] Manufactured outside of the U.S.A [Standard Model]

System Requirements	
Minimum	Intel i3 or equivalent dual-core 64-bit processor HDD or SSD (PATA/IDE, SATA, NVMe, SCSI, USB) 1024x768 display
For Full Engine Scan	4 GB RAM or higher USB 2.0 port or higher
For Engine & Software Updates	8 GB RAM or higher USB 3.0 port or higher
For In-Session Scan	Windows 10 or newer 4 GB RAM or higher 4 CPU
Secure File Storage	File Systems: FAT32, exFAT, or NTFS Operating System: Windows XP or higher, Ubuntu (16.04+ NTFS), RHEL, Debian, macOS, and Embedded OS using FAT32 Storage Capacity: 32GB

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 3, ZFS ³ , LUKS/LVM2

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 ⁴

MetaDefender Drive Professional	Ahnlab, Avira, Predictive Alin AI
---------------------------------	-----------------------------------

Regulatory Compliance			
NERC CIP 003-7 and 010-4	NIST 800-53 and 800-82	US Executive Order 14028	ISO/IEC 27001

Environmental Compliance			
CE Mark	FCC, Part 15, Class B	WEEE	RoHS
1 Wireless update requires a separate 4G/LTE cellular data plan [not included]. 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). 4 Made in India engine package.			