OPSWAT.

DATASHEET

METADEFENDER™

Drive

SERIES

Transient and Stationary Device Threat Scanning

MetaDefender Drive boots from a contained, secure OS and performs a bare metal scan on the device to detect threats that traditional scanning methods miss. Deep forensic analysis is conducted on every possible file, memory boot sector, peripheral driver, kernel space, and user space. Then, detailed threat reports pinpoint which files need to be removed or remediated.

From the manufacturer to your air-gapped zone, ensure all transient and stationary cyber assets are safe to use.

Key Features

Bare Metal Multiscanning
Scans a laptop or server from bare metal to user space files and directories with multiple anti-malware engines using signatures, heuristics, and machine learning to proactively detect known and unknown threats.

Flexible Workflow
Can perform full system or custom scans for specific file paths.

Digital Display and LED Indicator Components
Shows scanning status and results on the LCD with LED light alerts, enhancing the overall user experience.

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

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.

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

Threat Removal
Ability to remove files with threats after scans.

MetaDefender Drive Toolkit
Includes tools for firmware updates, configuration, and report management to streamline on-premises deployment and provisioning.

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

Inoperable OS Recovery*
Recovers inoperable operating systems by first booting from MetaDefender Drive.

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.

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

*The Inoperable OS Recovery feature is an on-demand capability, custom-built based on specific case, forensic reports or incident.

Specifications

	METADEFENDER Drive	METADEFENDER Drive with Digital Display
Physical		
Dimensions	2.9 x 0.8 x 0.4" 71 x 18 x 9mm	6.1 x 1.77 x 1.18" 155 x 45 x 30mm
LCD Screen with LED Indicator	✕	✓
Ports	1x USB 3.0 Type-A	2x USB 3.2 Type-C Type-A adapters included
Body	Aluminum FIPS 140-2 Level 2 compliant physical epoxy security encapsulation	Aluminum
Weight	1.34oz (38g)	15.87oz (450±10g)
Storage Temperature	-13°F to 176°F | -25°C to 80°C	
Operating Temperature	32°F to 158°F | 0°C to 70°C	
Operating Humidity	10% to 90%	
Shock Resistance	1000G maximum	
Vibration Resistance	15G peak-to-peak maximum	
Hardware Warranty	1 year	
Country of Origin	United States of America	
Regulatory		
Compliance	NERC CIP 003-7 NIST 80053 and 800-82 US Executive Order 14028 ANSSI FIPS 140-2 ISO/IEC 27001 Trade Agreements Act (TAA)	

	METADEFENDER Drive	METADEFENDER Drive with Digital Display
Software		
MetaDefender Drive Advanced	Ahnlab, Avira, Bitdefender, ESET, K7, Crowdstrike, McAfee	
MetaDefender Drive Enterprise	Ahnlab, Avira, Bitdefender, ESET, K7 or K7, Quick Heal, Emsisoft, Avira, Bitdefender	
MetaDefender Drive Professional	Ahnlab, Avira, ClamAV	
Compatibility		
Platform	x86 or x64, Intel- or AMD-based	
Windows	XP, 7, 8, 8.1, 10, 11, Server 2012, Server 2016, Server 2019, Server 2022 FAT16, FAT32, NTFS, exFAT [1] BitLocker (user password and recovery key) [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 (non-encrypted) LUKS/LVM2	

1. ReFS support is planned.
2. Does not yet support hardware-based disk encryption (default on some Windows Home laptops).
3. Encrypted ZFS support is planned.

OPSWAT.

Protecting the World's Critical Infrastructure