

MetaDefender® Drive

Trust you can hold in your hand

Even the most isolated, air-gapped networks provide access to external devices. Any transient device, like a laptop, is a prime target for malicious attacks. Security procedures can utilize a MetaDefender Drive before a device enters a facility to inspect the device for malware before the device boots.

Isolate. Analyze. Address.

MetaDefender Drive creates a portable perimeter, anywhere maintaining an air-gap is critical. Once plugged into a USB port, the computer is booted safely from MetaDefender Drive, by running off of MetaDefender Drive's own operating system. This separation allows analysis without software installation, scanning the entire device for malware, vulnerabilities, and overall integrity. Deep forensic analysis is conducted on every possible file, and detailed threat reports pinpoint which files need to be removed and remediated.



Highlights

Multiscanning

Scans with multiple anti-malware engines using signatures, heuristics, and machine learning to proactively detect known and unknown threats.

Flexible workflow

Full system or custom scan for specific file path. Supports scanning while target system is online or offline.

Encrypted disk support including Microsoft BitLocker

Detects encrypted volumes and prompts for a password, confirming that encrypted files are scanned. Supports LUKS-based encryption and macOS FileVault.

File-based Vulnerability Assessment

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

Multiple operating system support

Microsoft Windows, macOS and Linux.

Robust support for file systems

Supports NTFS, FAT32, APFS, or Linux ext2, ext3, ext4.

Central manageability

Options to connect to OPSWAT Central Management for reports and configurations from a single platform.

Tamper Proof

Device firmware is protected by a digital signature. The ruggedized housing is waterproof and tamper proof.

Data Privacy

Run on-premises for maximum privacy. No data is sent to the cloud.

OPSWAT.

MetaDefender Drive

Specifications

MetaDefender Drive Enterprise

MetaDefender Drive Advanced

Security Features

Advanced Malware Scanning	Kaspersky, Ahnlab, Bitdefender, Avira, and K7	McAfee, ESET, Bitdefender, Avira, and K7
File-based Vulnerability Assessment	Included	Included
Proactive DLP	-	Included

Hardware Security

Digital Security	Digitally Signed Trusted Secure Firmware (RSA-2048 Bit)	Digitally Signed Trusted Secure Firmware (RSA-2048 Bit)
Physical Security	FIPS 140-2 Level 2 compliant physical epoxy security encapsulation	FIPS 140-2 Level 2 compliant physical epoxy security encapsulation

Hardware Performance

USB Write Speed	170MB/s	170MB/s
USB Type	USB 3.0	USB 3.0
USB Connector	USB Type A	USB Type A

Hardware Specification

Physical Dimensions	2.9" x 0.8" x 0.4" 71mm x 19mm x 9mm	2.9" x 0.8" x 0.4" 71mm x 19mm x 9mm
TAA Compliant	Yes	Yes
Package Weight	38 g	38 g
Storage Temperature	-25°C to +85°C	-25°C to +85°C
Operating Temperature	0°C to 70°C	0°C to 70°C
Operating Humidity	20% to 90%	20% to 90%
Material	Aluminum	Aluminum
Shock Resistance	1000G maximum	1000G maximum
Vibration Resistance	15G maximum, peak-to-peak	15G maximum, peak-to-peak

Compatibility

Computer Hardware Platform	Linux, Intel-based Macs from 2006-2017, Windows
System Requirements	Windows® 7, 8, 8.1, 10 macOS X 10.8 Mountain Lion [or newer] Linux Debian 5 based [or newer], RHEL 6 based [or newer] Minimum 4GB RAM

OPSWAT.

Trust no file. Trust no device.