OPSWAT.

DATASHEET

METADEFENDER™

Drive Series

Transient and Stationary Device Threat Scanning

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 MetaDefender Drive before a device enters a facility to inspect the device for malware before the device boots.

Scan an offline x86 server within your IT or OT network before deploying it to ensure no malicious software is embedded within the server kernel space, user space, firmware and drive installs and upgrades.

Features

Bare Metal Laptop or Server Multiscanning
Scan 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
Full system or custom scan for specific file path.

Central Manageability
Option to connect to My OPSWAT for reports and configurations from a single platforms.

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

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

Country Of Origin Detection
MetaDefender Drive checks the device's software and flags anything that may violate country of origin compliance.

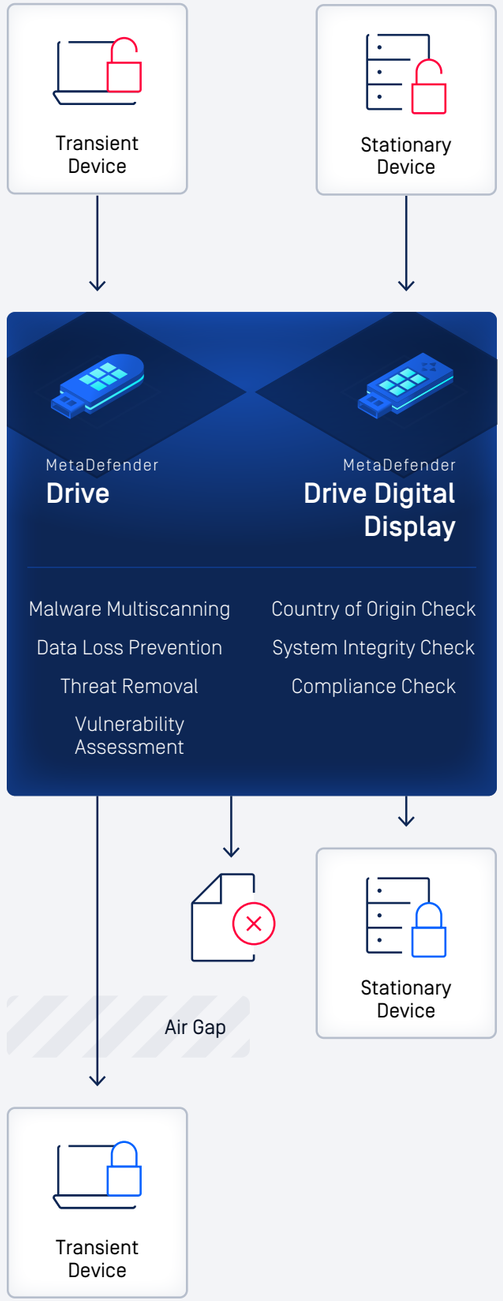
Encrypted Disk Support (Including Microsoft BitLocker)
Detects encrypted volumes and prompts for a password, confirming that encrypted files are scanned. Supports LUKS-based encryption and macOS FileVault.

Backup
Ability to backup unit to the same state before scanning or threat removal

Threat Removal
Ability to remove files with threat after scan is completed.

Digital Display and LED Indicator Components
The scanning report and detailed alerts show on the LCD and LED light, enhancing the overall user experience.

OPSWAT.

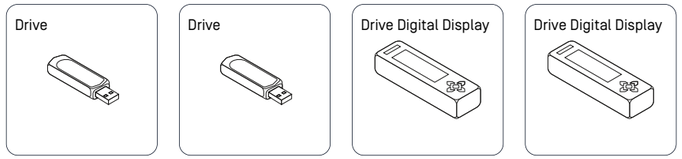


Isolate. Analyze. Address.

MetaDefender Drive securely boots from the USB port of a laptop or server. MetaDefender Drive provides operating system separation that allows analysis without software installation, scanning the entire device for malware, vulnerabilities, and overall integrity. Deep forensic analysis is conducted on every possible file, memory boot sectors, peripheral drivers, kernel space and user space and detailed threat reports pinpoint which files need to be removed and remediated.

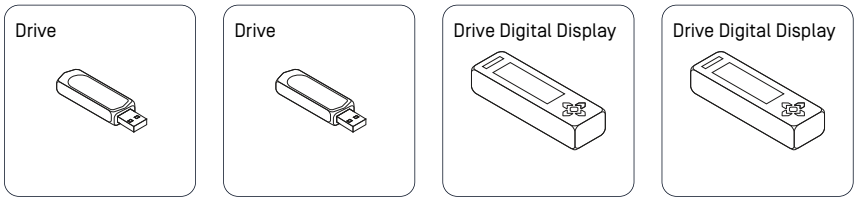
- Zero-Trust Secure Bare Metal Boot Scan
- No Software Installation Required
- Support for UEFI/GPT Legacy BIOS
- Scan Stationary and Transient Assets
- Advanced Threat Removal Technology
- Security Compliance Ready

Specifications



	Enterprise MD-DRIVE-ENT	Advanced MD-DRIVE-ADV	Enterprise MD-DRIVE-ENT-LCD	Advanced MD-DRIVE-ADV-LCD
Features				
Advanced Malware Scanning	Ahnlab Avira Bitdefender ESET K7	Ahnlab Avira Bitdefender CrowdStrike ESET K7 McAfee	Ahnlab Avira Bitdefender ESET K7	Ahnlab Avira Bitdefender CrowdStrike ESET K7 McAfee
File-Based Vulnerability Detection	✓	✓	✓	✓
Proactive DLP	✓	✓	✓	✓
Country of Origin Check	✓	✓	✓	✓
Security				
Firmware	Digitally signed trusted secure firmware (RSA-2048bit)			
Body	FIPS 140-2 Level 2 compliant physical epoxy security encapsulation			
Hardware				
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 & LED indicator	✗		✓	
Ports	1x USB 3.0 Type-A		1x USB 3.2 Gen 1x2 Type-A 1x USB 3.2 Gen 1x2 Type-C	
Body	Aluminum			
Weight	38g		450g (±10g)	

METADEFENDER DRIVE



Enterprise MD-DRIVE-ENT	Advanced MD-DRIVE-ADV	Enterprise MD-DRIVE-ENT-LCD	Advanced MD-DRIVE-ADV-LCD

Hardware	
Storage temperature	-25°C to +80°C
Operating temperature	0°C to 70°C
Operating humidity	10% to 90%
Shock resistance	1000G max.
Vibration resistance	15G peak-to-peak max.
Hardware warranty	1 year
Country of origin	United States of America

Regulatory	
Compliance	NERC CIP 003-7 NIST 80053 and 800-82 U.S. Executive Order 14018 ANSSI FIPS 041-2 ISO/IEC 27001

Compatibility	
Platform	x32 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* BitLocker (user password and recovery key)**
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 (non-encrypted) LUKS/LVM2

* ReFS support is planned
** does not yet support hardware-based disk encryption (known to come as default on some Windows Home laptops)
***Encrypted ZFS support is planned

OPSWAT.
Protecting the World's Critical Infrastructure

opswat.com/get-started