# OPSWAT.

METADEFENDER™

Drive

WITH SMART TOUCH

MetaDefender Drive helps to secure your hardware supply chain by performing a bare metal scan to detect threats that traditional scanning methods miss.

Built for remote and isolated environments where internet access is limited, MetaDefender Drive with Smart Touch supports central management with automated report syncing. The applications, reports, engines and MetaDefender Drive software
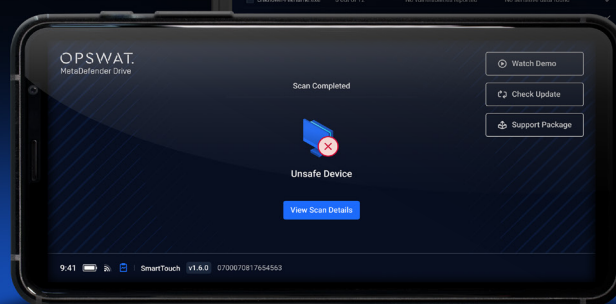
Scan target laptop with real-time results on Smart Touch screen

can be updated over Wi-Fi and cellular networks to overcome the limitations of air-gapped environments. Equipped with three hardware kill switches that physically disable wireless connectivity, Bluetooth, camera, microphone, and the cellular, MetaDefender Drive with Smart Touch ensures total control and zero risk to air-gapped networks and environments.

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 laptops and critical devices from bare metal to user space files and directories with multiple anti-malware engines.

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.

Wireless Updates
Easily update software, engines, and applications over Wi-Fi or cellular networks.[1]

Enterprise Central Management
Securely integrates with My OPSWAT™ Central Management to provide automated report syncing, real-time monitoring, configuration, and actionable security insights. Reports can also be sent over Wi-Fi and cellular networks.

Plug and Update Engines
Supports seamless engine updates by plugging it into a MetaDefender Kiosk™ — noworkstation required.

Plug and Sync Reports
Automatically syncs scanning reports in isolated environments via MetaDefender Kiosk and My OPSWAT Central Management with on-premises integration — no internet required.

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

Specifications

Hardware

Screen	5.7" IPS TFT screen with a 720x1440 resolution
Dimensions	152 x 74 x 15 mm (5.98 x 2.91 x 0.59 in)
USB	USB-C with USB 3.0 Data Transfer Power Delivery (Dual-Role Port)
Weight	262g (0.58lb)
Hardware Warranty	1 year
Wi-Fi	802.11a/b/g/n/ac/ax, 2.4GHz/5GHz
Cellular	4G/LTE
Country of Origin	United States of America (select model) China

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

Supports Regulatory Requirements

NERC CIP 003-7	NIST 800-53	ISO/IEC 27001
Executive Order 14028	NIST 800-82	ANSSI

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 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, ZFS (non-encrypted), LUKS/LVM2

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 Engine & Software Updates	8 GB RAM or higher USB 3.0 port or higher

Environmental Compliance

CE Mark
FCC, Part 15, Class B

[1] Wireless update requires a separate 4G/LTE cellular data plan (not included).
[2] Does not yet support hardware-based disk encryption (default on some Windows Home laptops).

OPSWAT.

Protecting the World's Critical Infrastructure

opswat.com/get-started