

OPSWAT.

METADEFENDER™

Drive Series

Transient and Stationary Device Threat Scanning



Protecting the World's Critical Infrastructure

Table of Contents

- 01 The Challenge
- 02 Our Mission
- 03 OPSWAT Solution
- 04 MetaDefender™ Drive Series - Benefits
- 05 MetaDefender™ Drive with Digital Display
- 06 Case Study 1, Case Study 2, Cast Study 3, Case Study 4
- 07 Strengthen Your Cybersecurity Posture
- 08 MetaDefender™ Cyber Asset Security
- 09 Which Drive is Right For you? Compatibility



01

The Challenge

Transient devices pose special challenges for OT air-gapped environments

- Compliance Requirements
- Sensitive Data Leakage
- Device Technological Complexity
- End-to-End Supply Chain Security

02

OPSWAT MISSION

Protect Your Supply Chain

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

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.

03


OPSWAT SOLUTION

Helping Meet Compliance

Failing an audit is often one of the largest concerns of an organization.

Negative outcomes:


- Large fines
- Forced halts in operations
- Losses in production
- Loss of reputation
- On-demand audit reports



Global
Manufacturing

ISO/IEC 27001


Global standard to manage information security and cybersecurity practices



United States
All Sectors

US Executive Order 14028

United States presidential decree to improve the nation's cybersecurity and protect federal networks



NATO Countries, United States
Government, Defense, Public Sector

NIST SP 800-53 and 800-82

United States standard governing computer security of all federal information systems

NIST FIPS 140-2


United States standard governing security requirements for cryptographic modules



Canada, United States
Oil & Gas, Energy, Nuclear

CIP-003-7 and CIP-010-4

Electric reliability standards governing respectively: removeable media & TCA, and configuration change management & vulnerability



France
All Sectors

ANSSI

French cybersecurity agency for defense and national security requires a minimum two AV engines for removeable media scanning

04

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.

Benefits



Zero-Trust



Easy-to-use



No Software Installation Required



End-to-End Supply Chain Security



Self-Checking Secure Firmware



Support for UEFI, GPT, Legacy BIOS



Security Compliance Ready



Threat Removal



File-Based Vulnerability Assessment



Multilingual Support in 12 Languages



05

METADEFENDER™

Drive with Digital Display

Stationary Device Threat Scanning



Scan servers, engineering workstations, and other stationary devices



Review server scan results without an external display

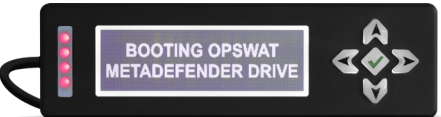


Easy decision-making based on results

1

Plug In

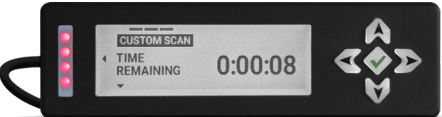
Secure boot your device directly from MetaDefender Drive



2

Scan

MetaDefender Drive performs bare metal scan of the system



3

Review

Review the results of the scan directly on MetaDefender Drive



06

CASE STUDY 1

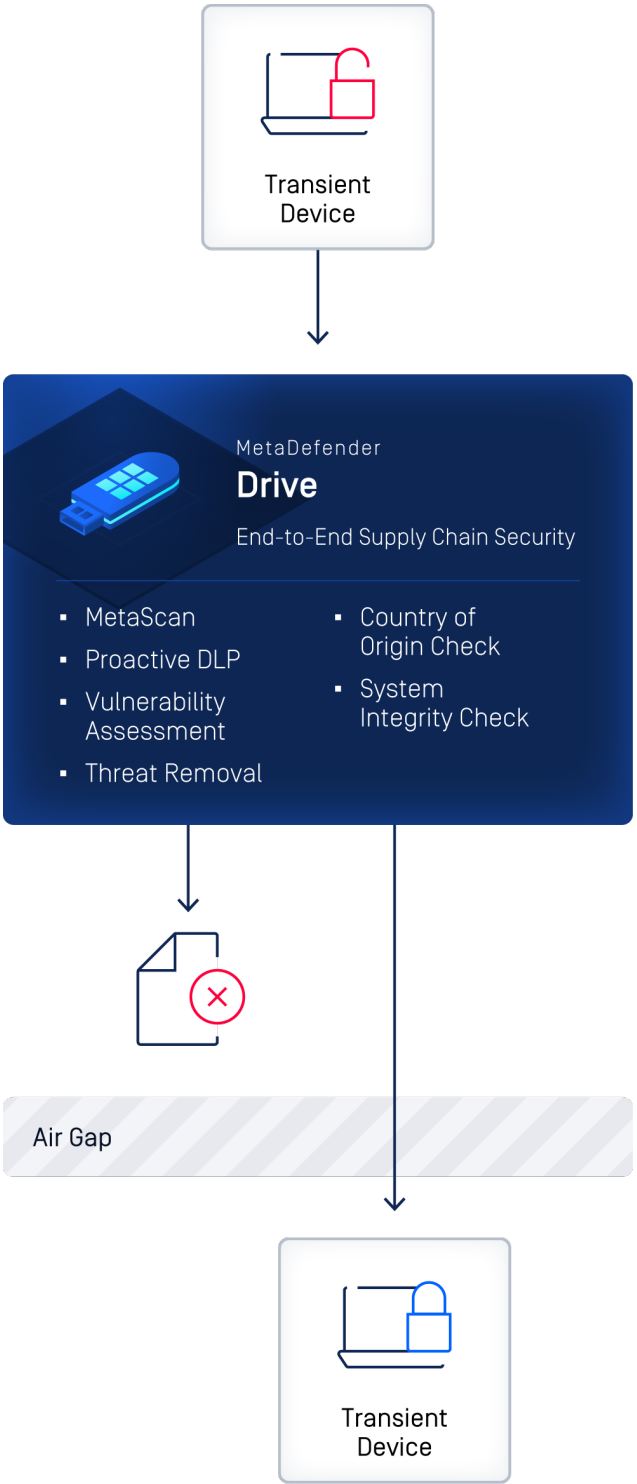
Critical Air Gap Network Protection from Transient Devices

Challenge

- Allowing vendors, contractors, or employees to use their laptops within a secure air-gapped network introduces security risks.
- Performing upgrades and maintenance on PLCs, HMIs, or SCADA machines required specialized applications preinstalled on vendor laptop.

Solution

- Secure Boot MetaDefender Drive
- Perform a bare metal scan in kernel level to detect vulnerabilities and prevent threats
- Transient device protection reduces risk of OT network propagation



CASE STUDY 2

Centralized Drive Management That Delivers Real-Time Insights

Challenge

- Managing multiple systems across sites is inefficient and leads to inconsistent reporting.
- Limited real-time reporting and visibility.

Solution

- Real-time monitoring and seamless centralized management for all connected MetaDefender Drives.
- Automated report syncing ensures instant data availability for audits and actionable insights.
- Simplify operations with large-scale deployments and unified management

CASE STUDY 3

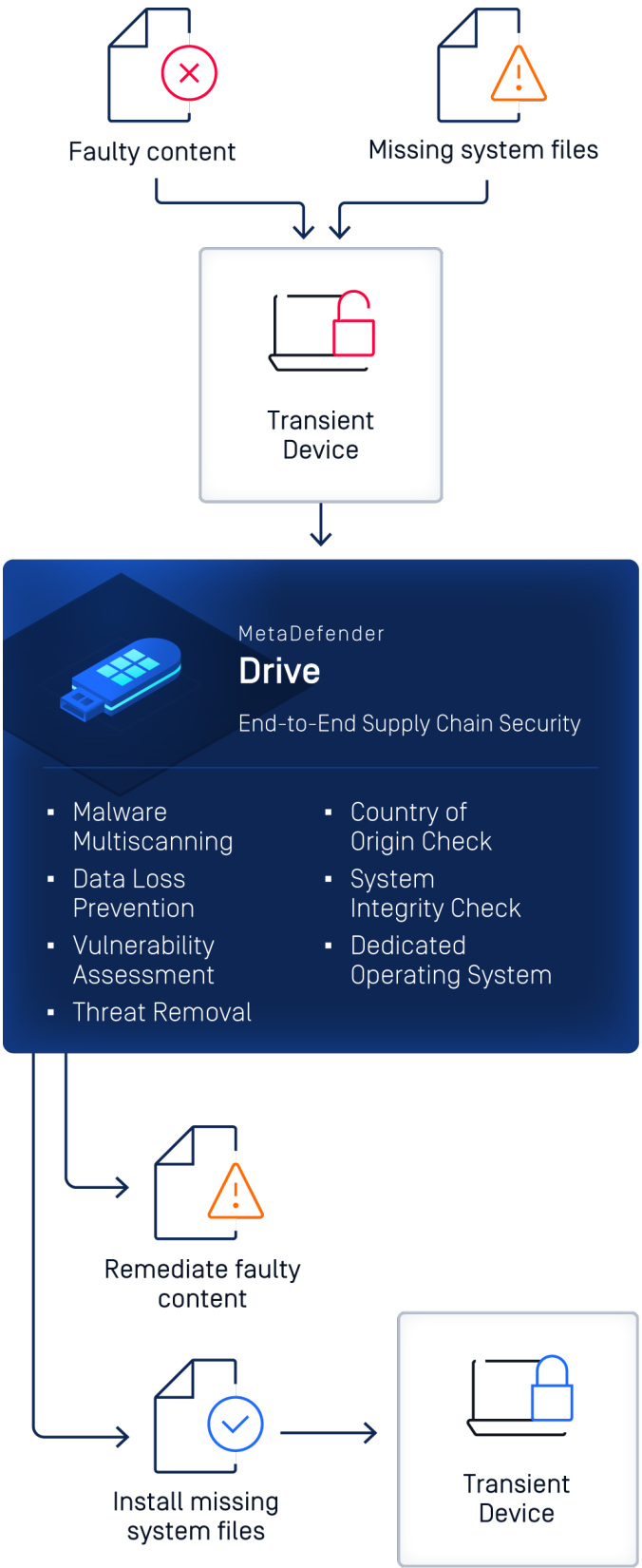
Recover Inoperable Operating System* to Minimize Downtime

Challenge

- System failures caused by corrupt firmware updates, missing critical files, or OS crashes lead to operational disruptions.
- Missing or damaged critical system files prevent laptop's OS from booting.

Solution

- Boot from MetaDefender Drive's dedicated OS on the target device.
- MetaDefender Drive automatically scans all non-encrypted disks to detect issues and perform remediation steps if necessary.



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



CASE STUDY 4

Centralized Scanning Profile for Policy Consistency

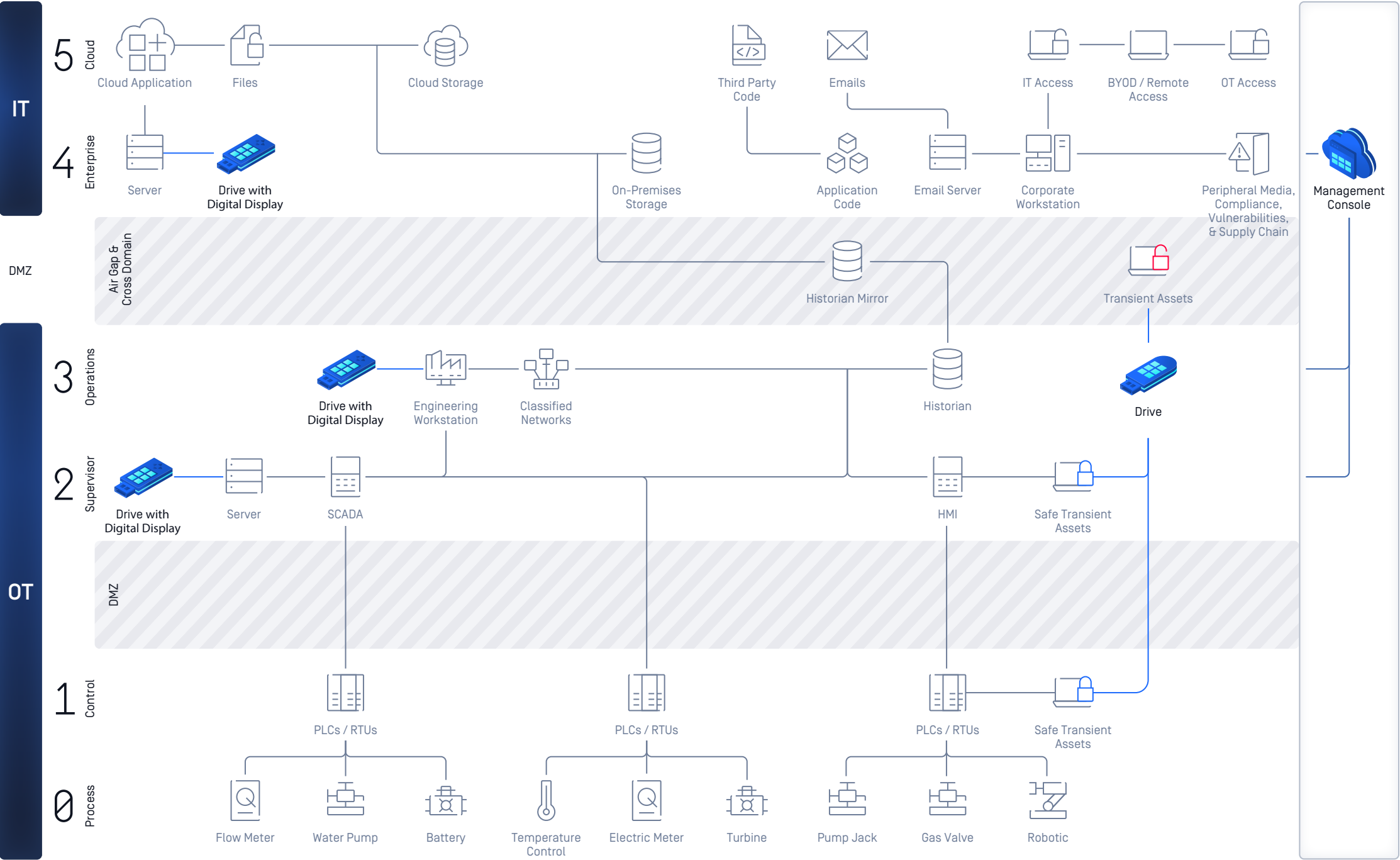
Challenge

- Unauthorized scan configuration changes may compromise the OT network.
- Inconsistent scan policies increase non-compliance risk and potential fines.

Solution

- Securely lock MetaDefender Drive to prevent unauthorized scan configuration changes.
- Enable real-time local policy modification with remote one-time-password approval.
- Streamline scan policy enforcement at scale.

Strengthen Your Cybersecurity Posture




Cyber Asset Security




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

Which Drive is Right For You?

USB
TAA Compliant
64GB



Digital Display
TAA Compliant
1TB NVME



Configuration	Professional	Enterprise	Advanced
Metascan Engines	3 Engines Ahnlab, Avira, ClamAV	5 Engines Ahnlab, Avira, Bitdefender, ESET, K7 or K7, Quick Heal, Emsisoft, Avira, Bitdefender	7 Engines Ahnlab, Avira, Bitdefender, ESET,K7, CrowdStrike, McAfee
Metascan Detection of top 10000 threats	86.3%	87.6%	88.9%
Legacy Laptop Support	Yes	Yes	Yes
Technologies	<p>All configurations include:</p> <ul style="list-style-type: none">• Proactive DLP: Detects sensitive and confidential data such as credit card and social security numbers in documents, images, and videos.• File-Based Vulnerability Assessment: Detects known vulnerabilities in over 20,000 software applications with a patented file-based approach.• Country of Origin Detection: Checks the device's software and flags anything that may violate country of origin compliance.		

Compatibility

	Windows	MacOS	Linux
Platform	x86 or x64 Intel- or AMD-based		
Operating System	XP [support embedded version] 7 [support embedded version] 8 8.1 10 11 Server 2012 Server 2016 Server 2019 Server 2022	Intel-based from 2006-2017	Debian 5-based or newer RHEL 6-based or newer
File System	FAT16 FAT32 NTFS exFAT*	HFS HFS+ APFS	EXT2 EXT3 EXT4 XFS BTRFS Reiserfs UFS*** ZFS (non-encrypted)
Security	BitLocker (user password and recovery key)**	FileVault for APFS	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

GET STARTED

Are you ready to put MetaDefender Drive on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:

opswat.com/get-started

sales@opswat.com



OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and

device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.