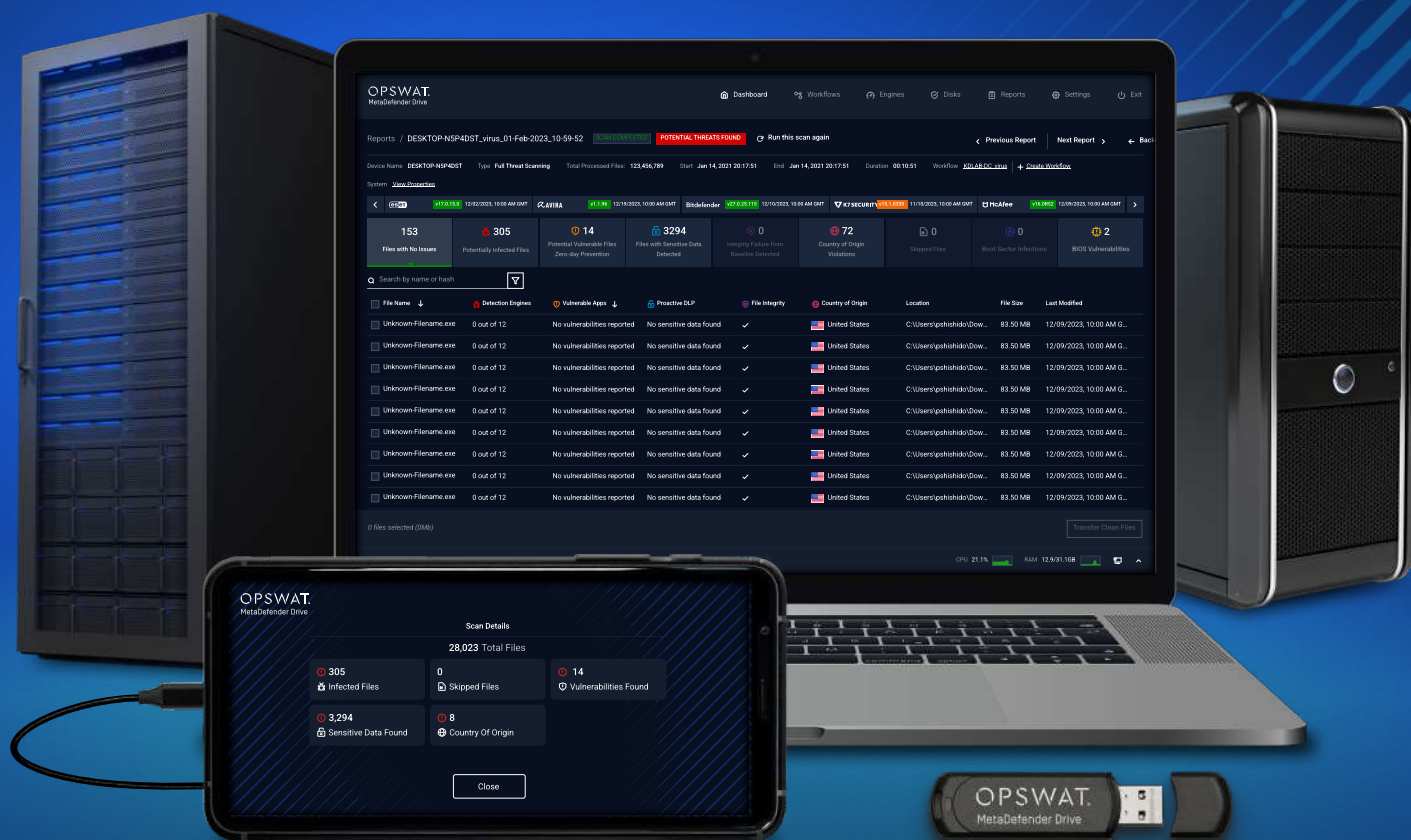


OPSWAT.

METADEFENDER™

Drive Series

Portable Malware and Compliance Scanning



Protecting the World's Critical Infrastructure

Table of Contents

- 01 Protect Your Supply Chain
- 02 Helping Meet Compliance
- 03 MetaDefender Drive Series
- 04 MetaDefender Drive 2
- 05 MetaDefender Drive with Smart Touch
- 06 In-Session Scanning
- 07 Stay Protected Anywhere
- 08 Enterprise Central Management at Scale
- 09 Case Study
- 10 Strengthen Your Cybersecurity Posture
- 11 Portable Malware and Compliance Scanning Security
- 12 Which Drive is Right For You?



01

Protect Your Supply Chain

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 to scan devices before they power on, ensuring malware detection and compliance checks are performed before the device enters secure environments.

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.

For critical systems that can't be powered down, in-session scanning enables portable malware detection while the OS remains operational.



02

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
- Reputational damage
- High remediation costs for future audits



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

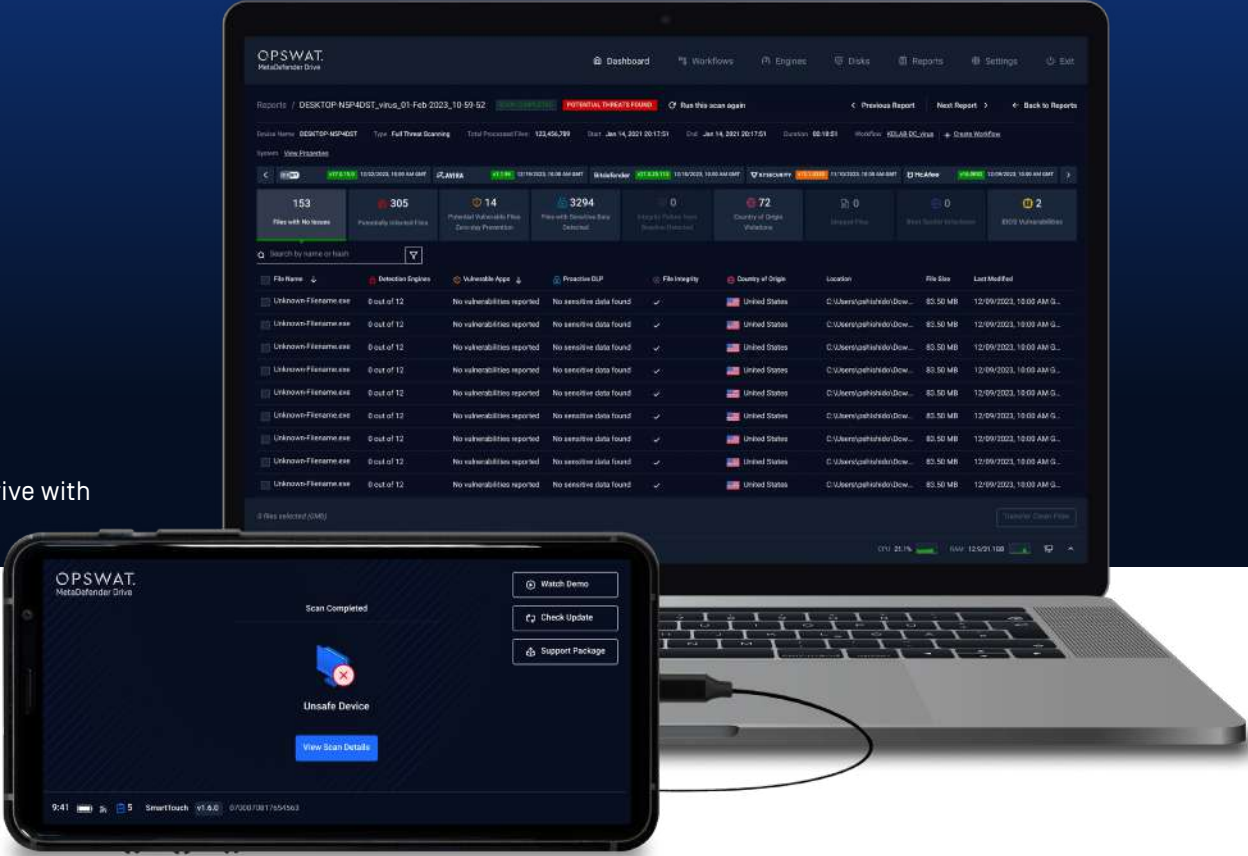
CIP-003-7 and CIP-010-4
Electric reliability standards governing respectively: removeable media & TCA, and configuration change management & vulnerability



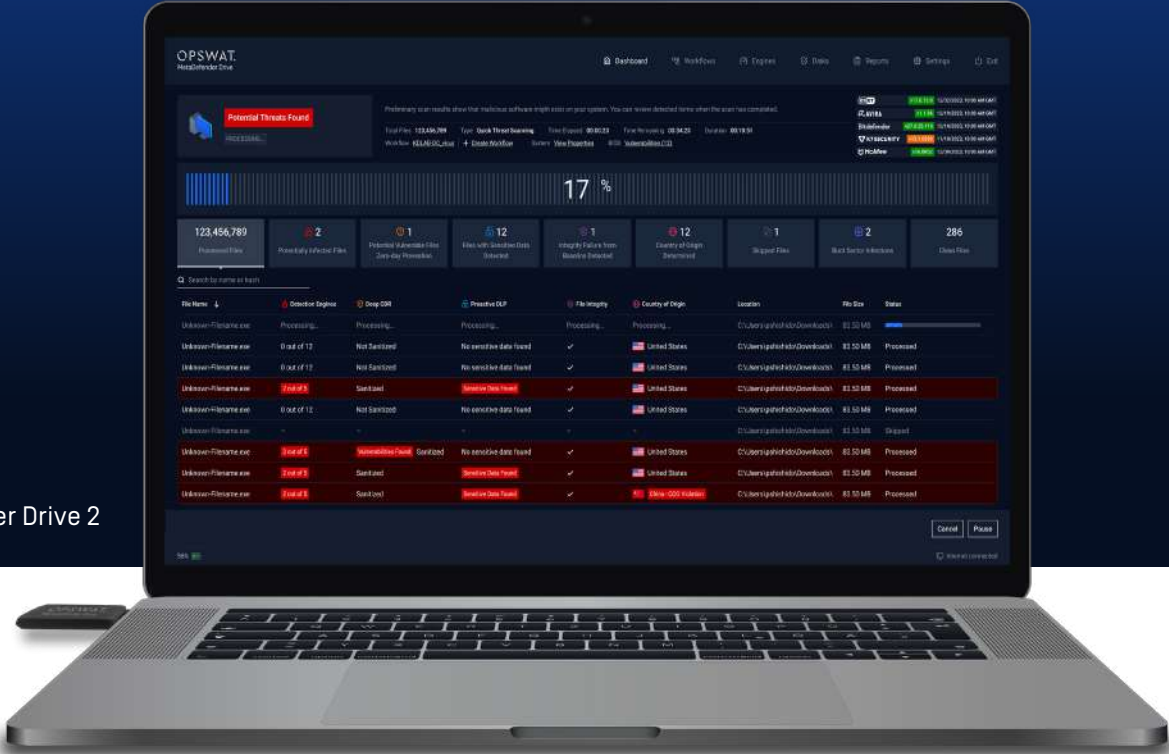
France
All Sectors

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

MetaDefender Drive with Smart Touch



MetaDefender Drive 2



03

METADEFENDER™ Drive Series

Portable Malware and
Compliance Scanning



Boots From a
Built-in OS



Performs pre-boot scanning
with up to 8 trusted
anti-malware engines



Zero Risk of
Network Compromise
During Operation



Made In the U.S.A.



No Software Installation
on Asset Required



1TB Storage Offering
Expanded Archive Capacity
and Improved Performance



Enterprise Central
Management



Supports in-session scanning
for systems that can't be
powered down using 3
anti-malware engines

04

METADEFENDER™

Drive 2

Portable Pre-Boot Malware Scanning for
Transient and Stationary Devices

Scan Before You Trust

- 

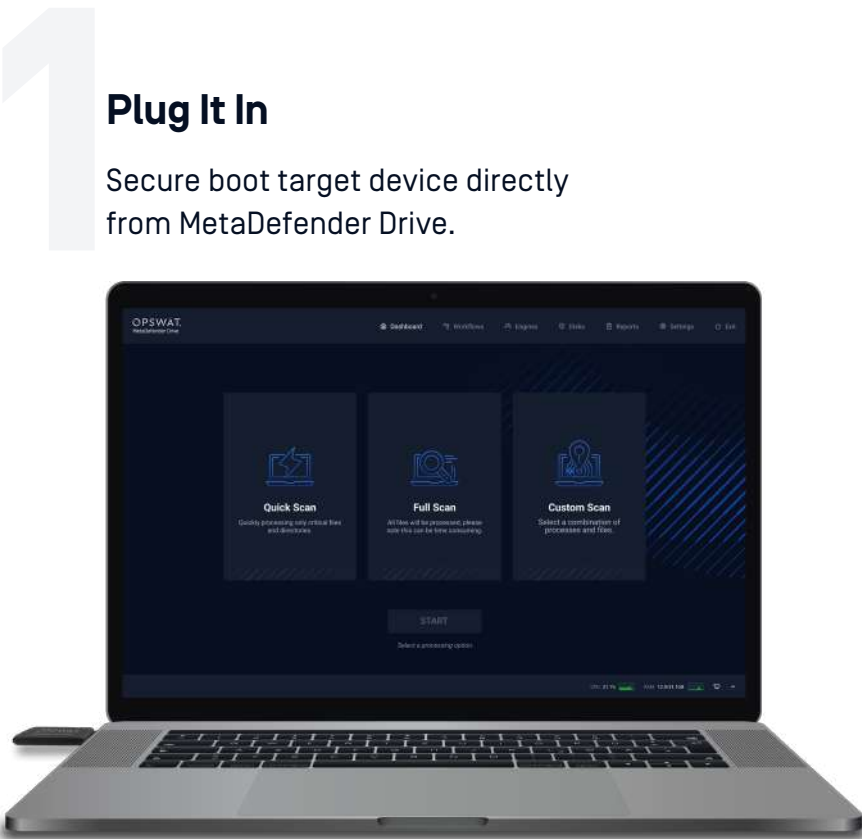
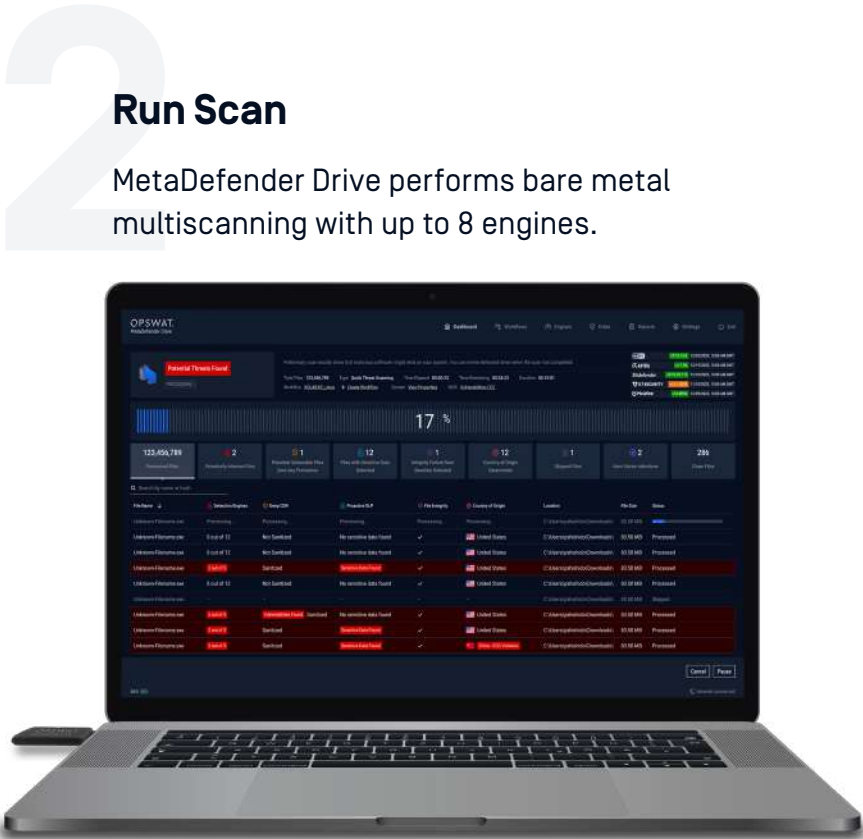
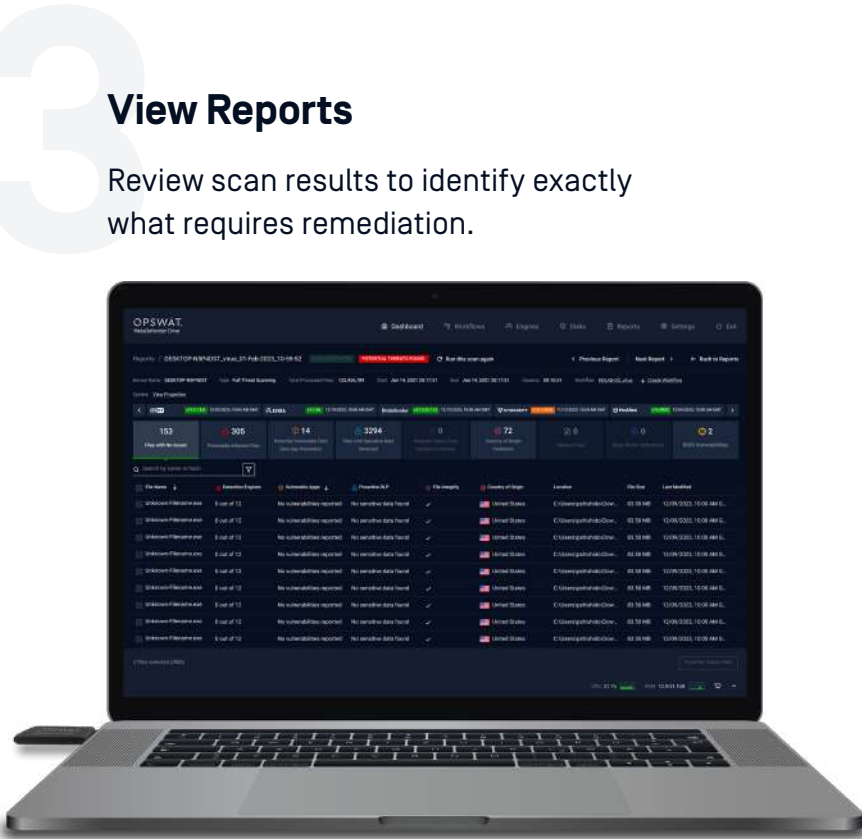
Bare Metal Multiscanning
with Up to 8 Engines
- 

No Software
Installation Required
- 

Plug and Scan Solution
- 

Compliant with
FIPS 140-2 & TAA

Scan and Verify Laptops Before They Power On



05

METADEFENDER™

Drive with Smart Touch

Portable Pre-Boot Multi-Device Scanning
at the Touch of a Finger

Security On the Move



Automated Reports,
Engines and Application
Updates via Cellular
or Wi-Fi



Physical Network
Kill Switches



Secure File
Storage Between
Critical Systems



No Software
Installation Required



Made In the U.S.A.



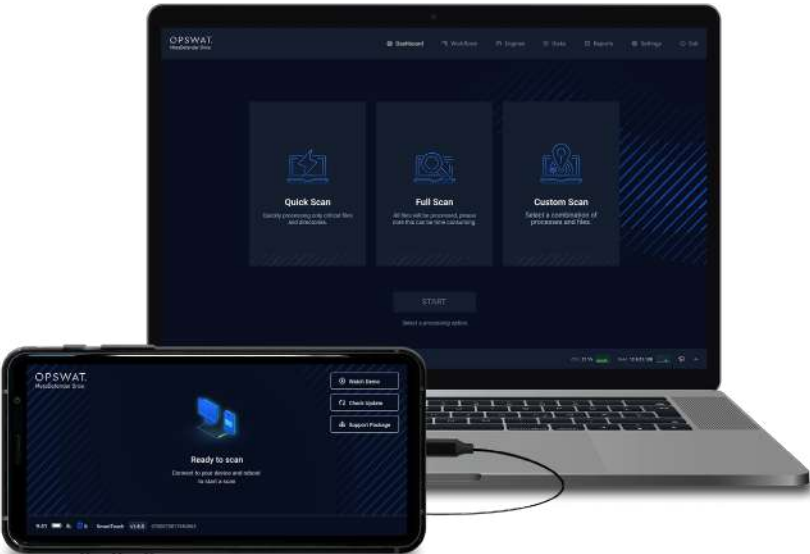
Enterprise
Central Management

Verify Servers, Desktops, and Laptops Before They Power On

1

Connect and Boot

Use Wi-Fi or cellular to update engines and security on MetaDefender Drive with Smart Touch, then connect to the target device and securely boot from the Drive.



2

Run Scan

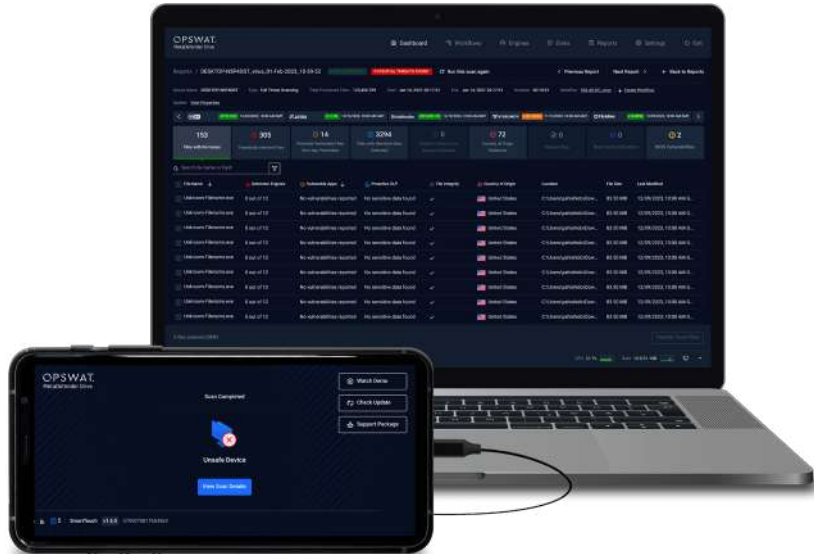
With physical kill switches for air-gapped environments, securely boot your device directly from the MetaDefender Drive with Smart Touch for a full bare metal multiscanning with up to 8 engines. Includes 1TB of Storage for large archive scanning.



3

View Reports

5.7" screen to view scan results, directly on the MetaDefender Drive with Smart Touch interface. Streamlined, automated report syncing with My OPSWAT Central Management.



06

In-Session Scanning

Uninterrupted Device Inspection Without Downtime*

MetaDefender Drive also supports in-session scanning, enabling devices to be scanned with multiple anti-malware engines during live system operations, ideal for critical environments where downtime is not acceptable.

Security On the Move



Multiscanning: Scanning with up to 3 trusted engines including ESET, Bitdefender, and Predictive Alin AI



BitLocker Accessibility: Enables scanning even when BitLocker keys are not accessible to the user.

1

Connect

MetaDefender Drive connects to the system while the operating system is running. No software installation or system restart is required.

2

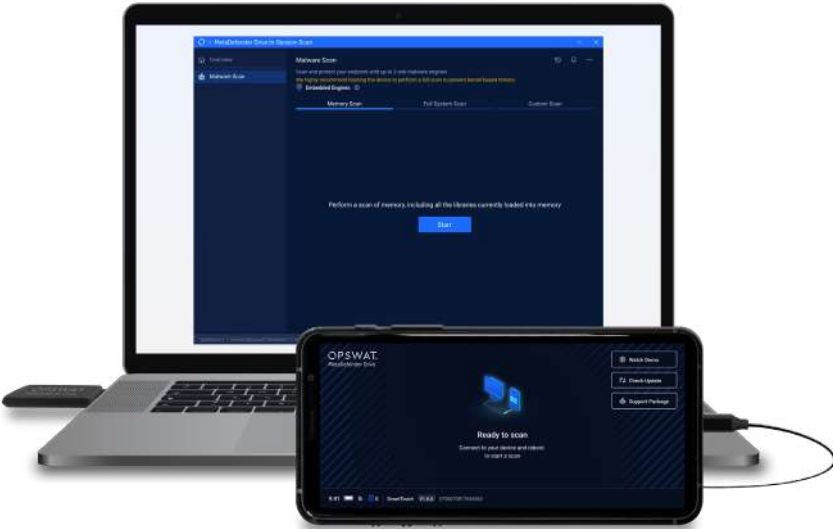
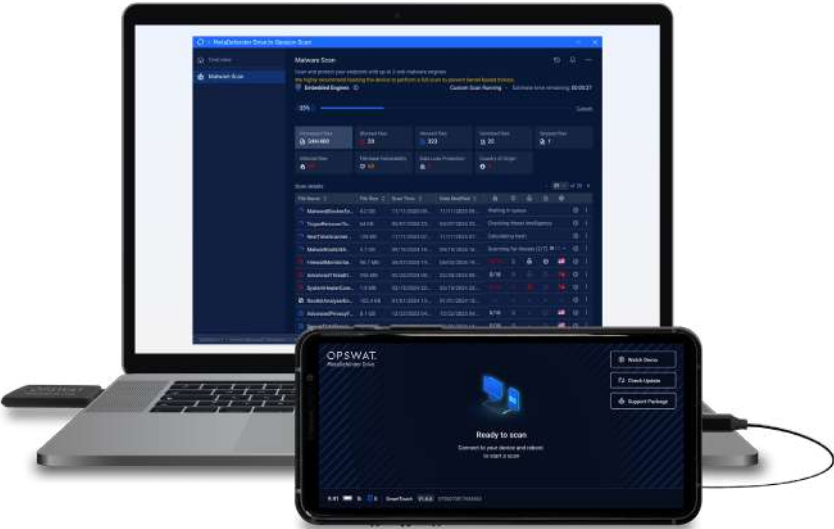
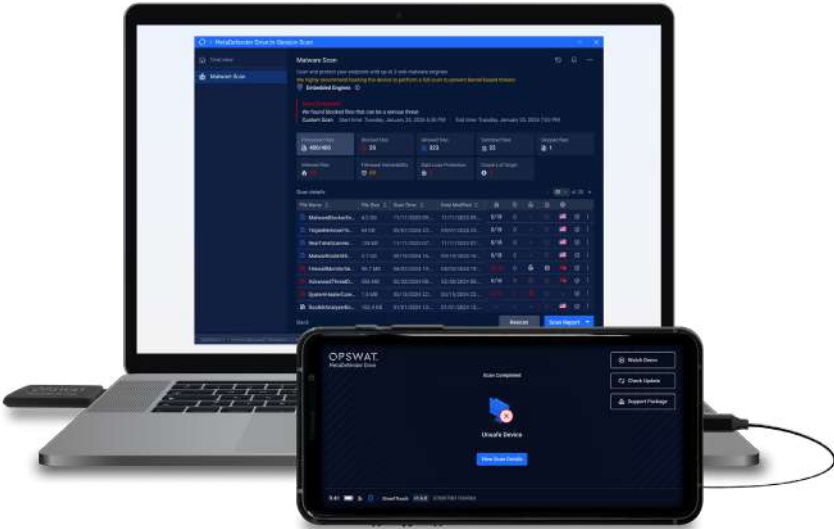
Scan During Live Operation

MetaDefender Drive performs in-session scanning on system memory and local drives using up to 3 engines, including ESET, Bitdefender, and Predictive Alin AI.

3

View Reports

Scan results clearly identify threats and system risks on the built-in touchscreen, enabling fast and informed remediation decisions.

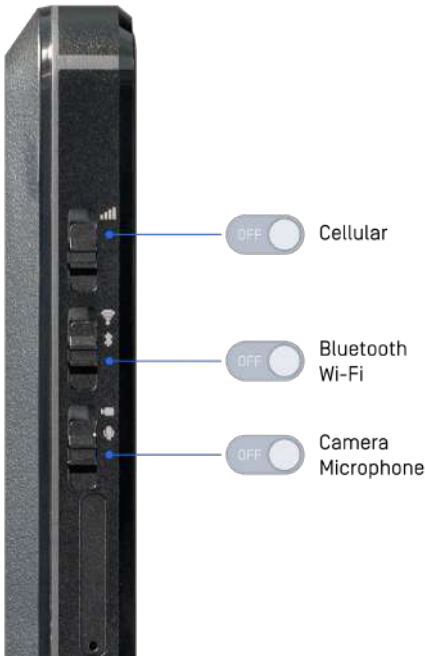
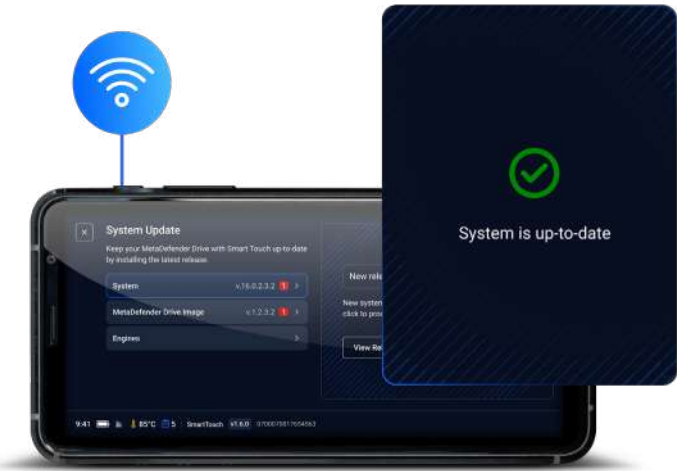


07

Stay Protected Anywhere

Purpose-Built, Mobile Form Factor, Physical Control

Physical kill switches ensure zero risk of network compromise during scans



Stay Updated Anywhere with Wireless Connectivity

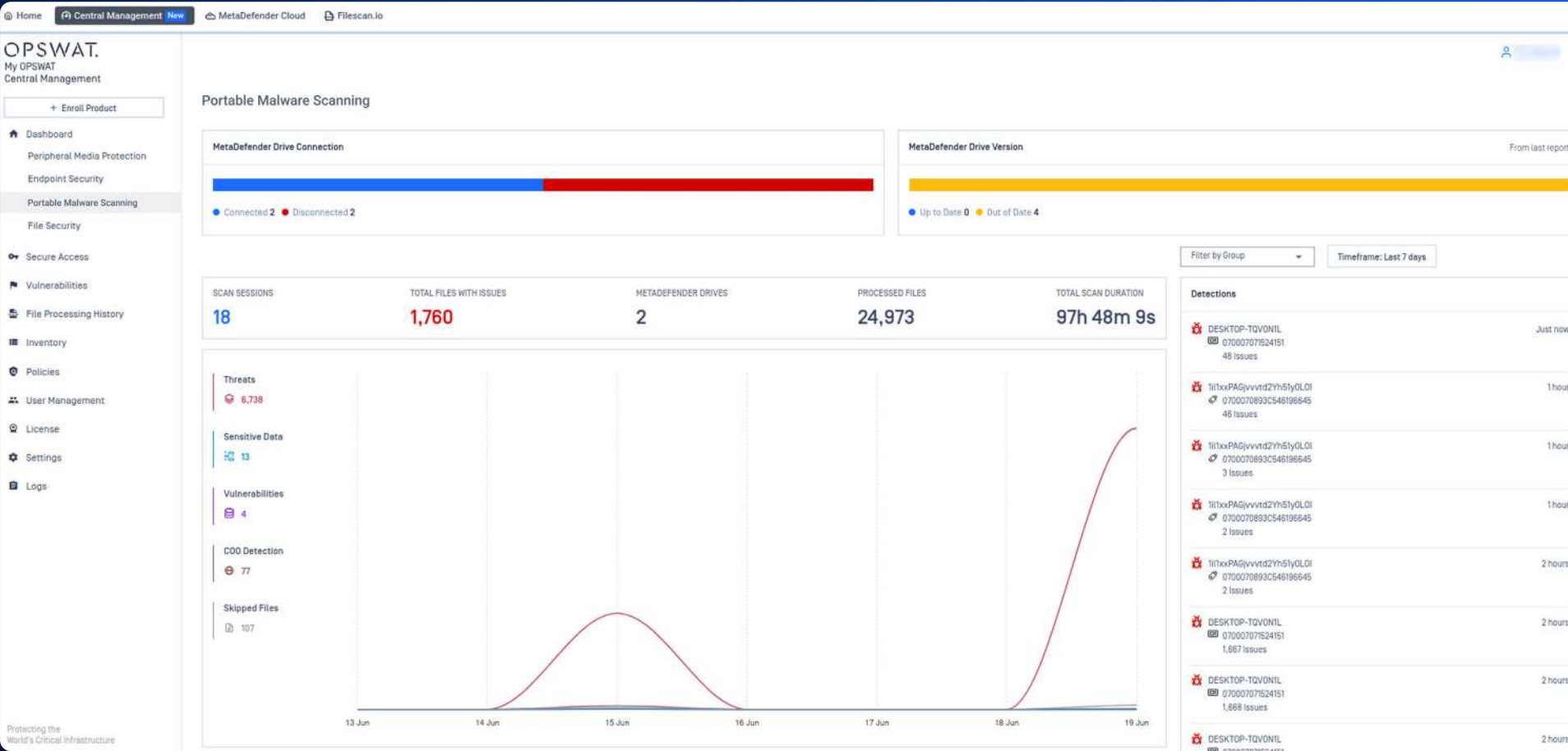
Engines, applications, and reports sync instantly over Wi-Fi or cellular. Save time and keep protection seamless, even on the move.

08

Enterprise Central Management at Scale

Gain Comprehensive Visibility and Control Across All Scanned Devices

MetaDefender Drive with Smart Touch securely integrates with My OPSWAT™ Central Management so every scan result is instantly documented, every risk is tracked, and compliance reporting is effortless — even from remote or isolated environments.



09

CASE STUDY 1

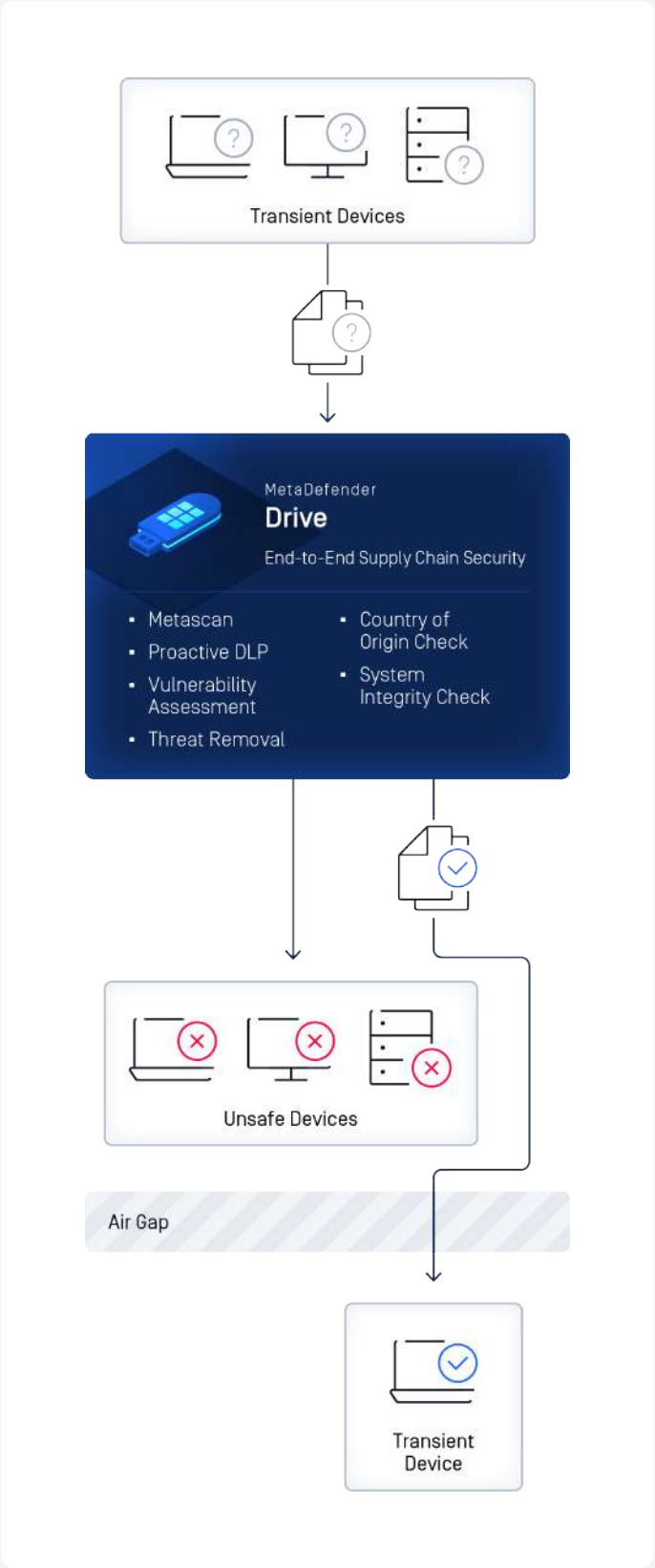
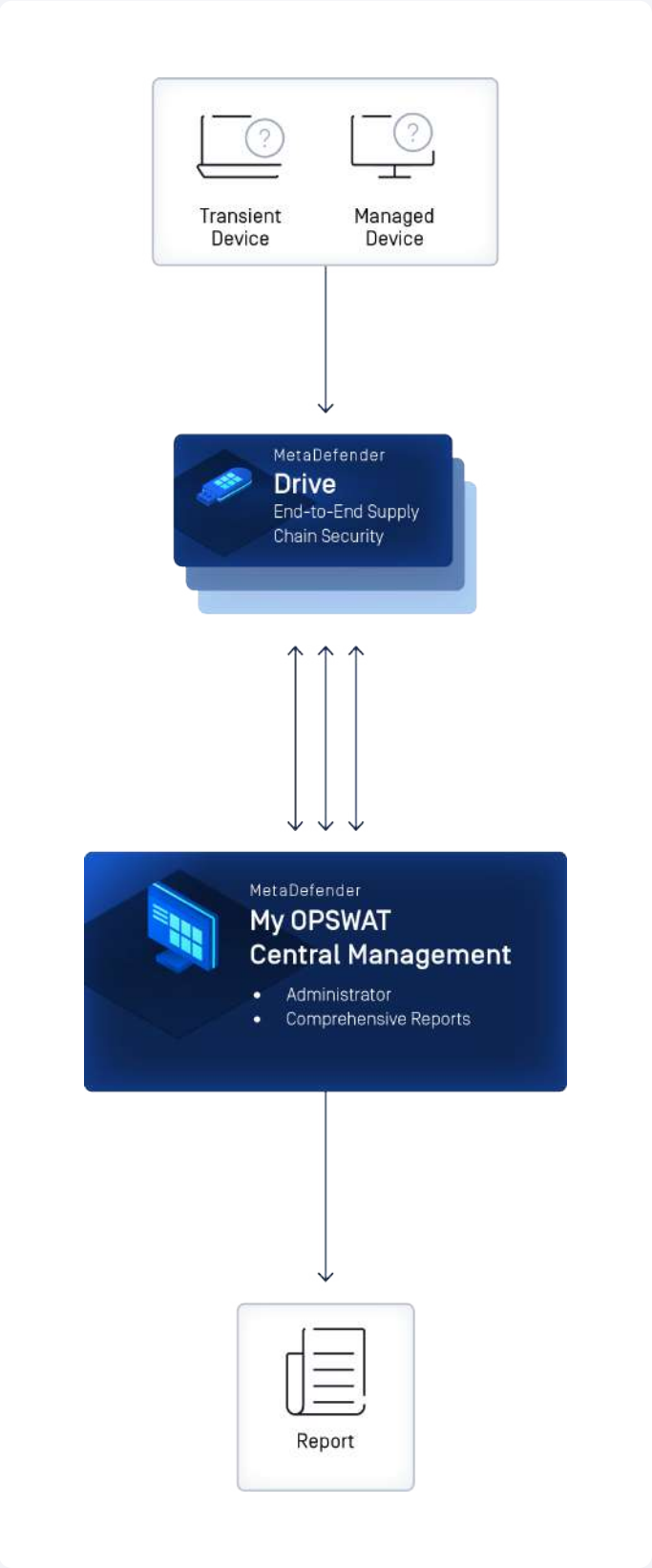
Critical Air-Gapped Network Protection from Transient Devices

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
- Simplified operations with large-scale deployments and unified management of all MetaDefender Drives

CASE STUDY 3

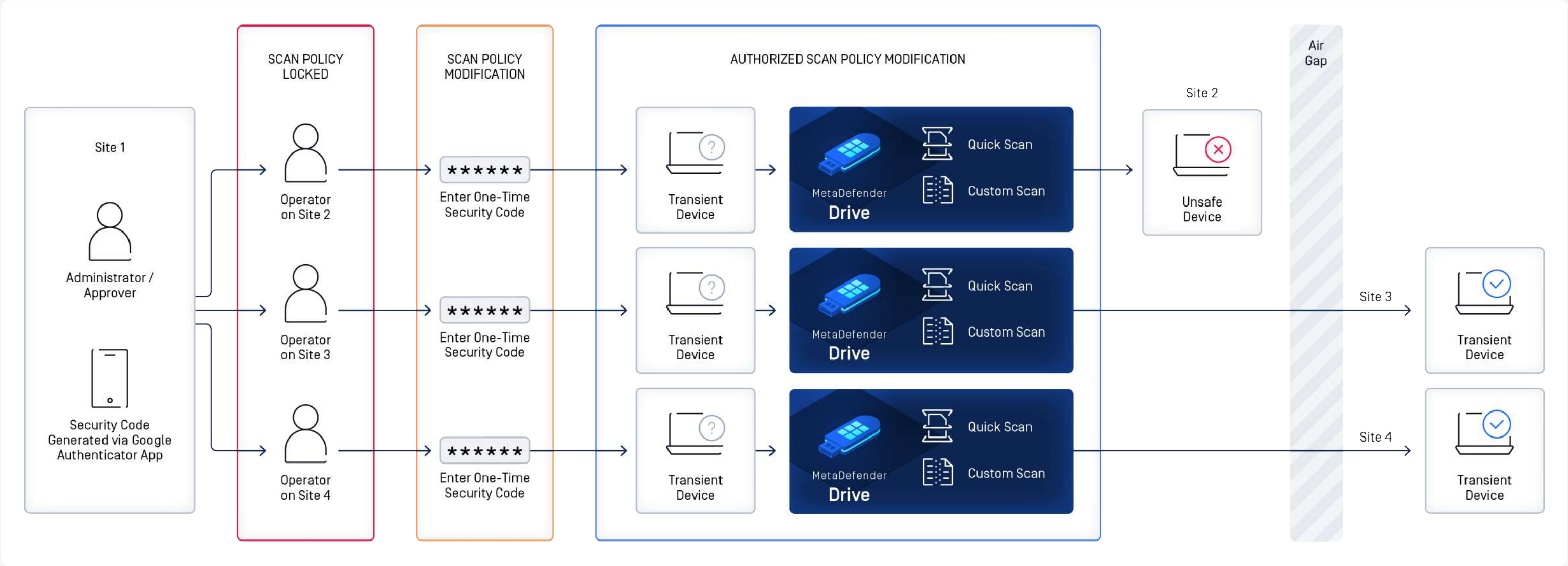
Centralized Scanning Profile for Policy Consistency

Challenge

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

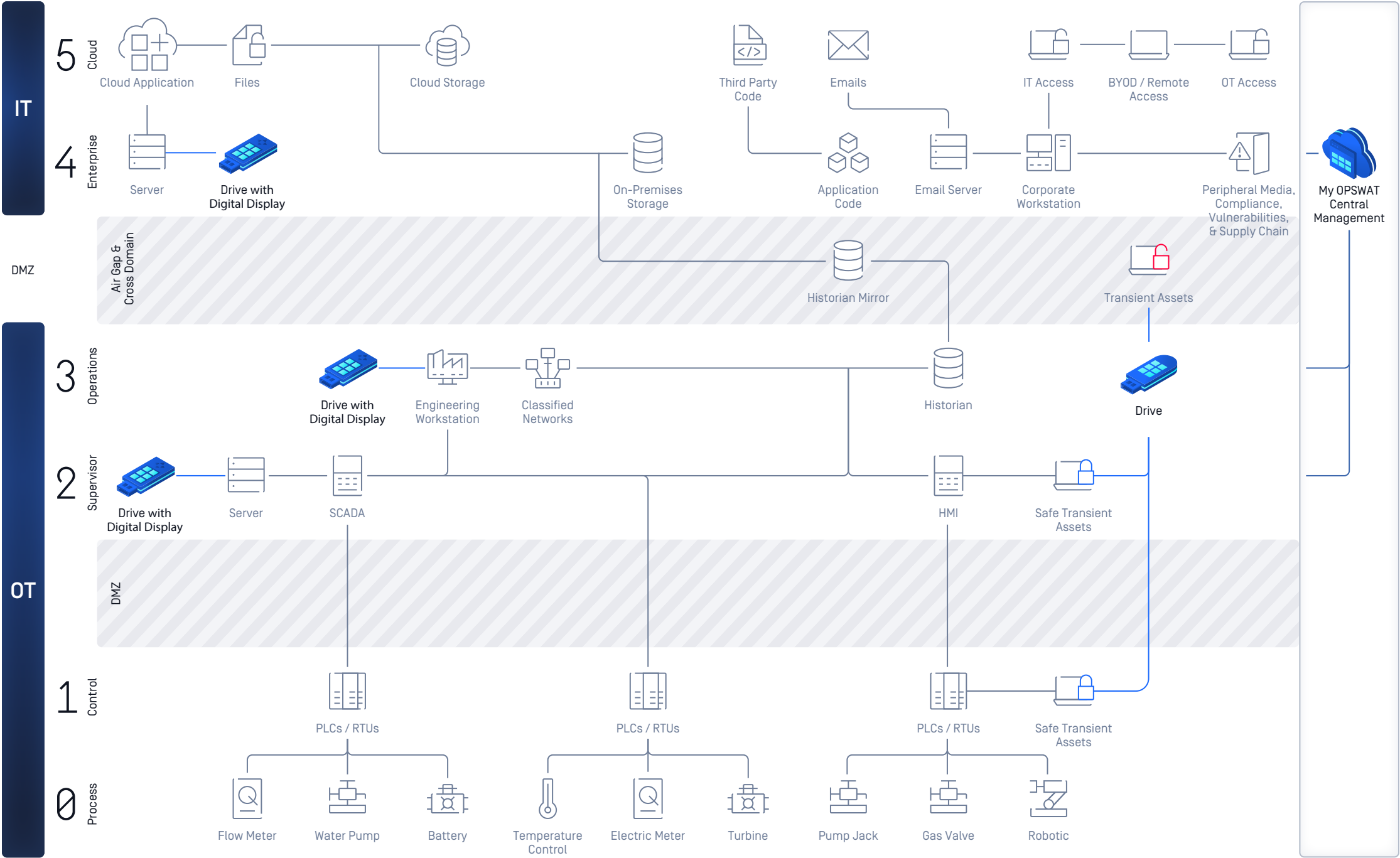
Solution

- 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

The MetaDefender platform protects critical infrastructure against modern cyberthreats, from IT to OT and everything in between. MetaDefender Drive secures transient assets before granting them access to air-gapped OT environments. It integrates with other products, such as MetaDefender™ Managed File Transfer for safe data transfers, and MetaDefender™ Kiosk for report syncing and maintenance.



11

Portable Malware and Compliance Scanning Security



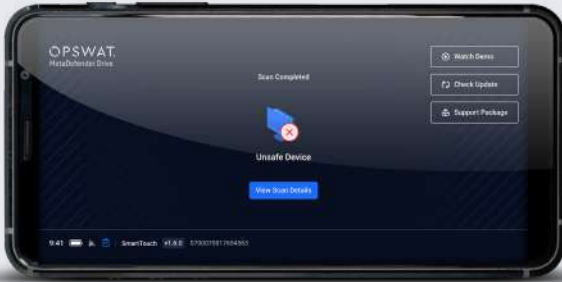
Which Drive is Right For You?



USB

Made in U.S.A

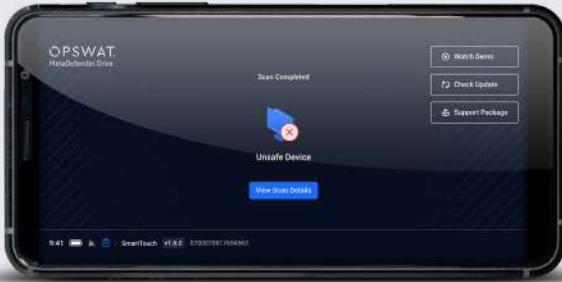
- ✓ TAA, FIPS 140-2, RoHS and REACH



Smart Touch [U.S. Model]

Made in U.S.A

- ✓ CE Mark, WEEE, RoHS, and FCC, Part 15, Class B



Smart Touch [Standard Model]

Manufactured outside U.S.A

- ✓ CE Mark, WEEE, RoHS, and FCC, Part 15, Class B

	Edition Engine Packages		
	Professional	Enterprise	Advanced
	Metascan™ Multiscanning 3 Engines Ahnlab, Avira, Predictive Alin AI	6 Engines Ahnlab, Avira, Bitdefender, ESET, K7,Predictive Alin AI or K7, Quick Heal, Ahnlab, Avira, Bitdefender, Predictive Alin AI ¹	8 Engines Ahnlab, Avira, Bitdefender, ESET, K7, CrowdStrike, Trellix, Predictive Alin AI
	Detection of top 10000 threats	94%	98.7%
	Legacy Laptop Support	✓	✓
	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 ²
Security	BitLocker ³	FileVault for APFS	LUKS/LVM2

1 Made in India engine package

2 Supports ZFS [non-encrypted]

3 Supports BitLocker [using user password and recovery key]. Does not yet support hardware-based disk encryption [default on some Windows Home laptops].

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 1,900 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.