OPSWAT.



SOLUTION BRIEF

Secure Digital Evidence for Law Enforcement

Protect digital evidence from malware contamination and strengthen chain-of-custody controls across collection, transfer, analysis, and storage.

Protecting the World's Critical Infrastructure

Table of Contents

01 Rapidly Evolving Digital Forensics

02 Every Stage of Digital Evidence Handling Introduces Risk

03 How OPSWAT Secures the Digital Evidence Workflow

04 Secure Every Stage of the Investigation

05 Why OPSWAT



01

Rapidly Evolving Digital Forensics

Digital evidence is a pervasive element in modern criminal investigations, with smartphones appearing in 97% of cases. The escalating volume and complexity of digital data, encompassing everything from personal devices to cloud services and IoT ecosystems, demand highly secure and efficient forensic investigation processes.

Traditional security measures, often focused on securing communication channels rather than content, leave law enforcement agencies vulnerable to malware, data corruption, and compromised evidence. The increasing sophistication of cyberthreats, including AI-generated manipulated evidence, further complicates the critical task of maintaining evidentiary integrity and a verifiable chain of custody.

02

Every Stage of Digital Evidence Handling Introduces Risk

Digital evidence changes hands dozens of times between the crime scene and the courtroom. Each handoff is a chance for something to go wrong.



Contamination Risk

Seized devices and files can carry malware that spreads the moment they reach a forensic workstation. A single infected file can corrupt analysis environments, and derail active investigations.

Evidence Integrity

Digital evidence traverses multiple stages: without stringent protocols for hashing, audit trails, and controlled transfers, the risk of errors, tampering, and incomplete documentation increases.

Sensitive Data Exposure

Case files and seized media often contain highly sensitive information, such as credit card numbers, national IDs, personal data, and confidential case details.

Investigation Efficiency

Digital forensics labs frequently face backlogs of six months to a year or more, delaying investigations and justice. Manual scanning and validation eat into the time investigators need for the case itself.

Data Volume and Complexity

Analyzing vast datasets efficiently to identify relevant information is a major hurdle. Investigations typically involve two to five devices per case, significantly increasing data volume and complexity.

Legal and Regulatory Constraints

Balancing comprehensive searches with privacy rights and adhering to evolving legal frameworks requires careful navigation and strict adherence to guidelines.

03

How OPSWAT Secures the Digital Evidence Workflow

OPSWAT provides a comprehensive solution suite for secure digital evidence handling. It integrates advanced inspection, sanitization, and transfer capabilities to protect sensitive data and the integrity of evidence.



Solution Components



MetaDefender™ Drive

Primary Function

Securely collect digital evidence using trusted portable media in field operations.

Key Capabilities

- Entry points to secure facilities
- Before data enters classified or OT networks
- As a controlled data ingestion point for removable media entering secure environments



MetaDefender™ Kiosk

Primary Function

Scan and validate removable media before evidence enters police stations or forensic environments.

Key Capabilities

- Peripheral media protection
- Automated evidence intake workflow
- File-based Vulnerability Assessment



MetaDefender™ Endpoint

Primary Function

Protect investigator workstations and endpoints during evidence acquisition and handling.

Key Capabilities

- Peripheral media protection
- Peripheral device control
- File-based Vulnerability Assessment
- Secure file download



MetaDefender™ Managed File Transfer (MFT)

Primary Function

Securely transfer digital evidence between field locations, police stations, forensic labs, prosecutors, and courts.

Key Capabilities

- Secure collaboration and file sharing
- Encrypted file transfer
- Policy-enforced file exchange
- Automated transfer workflows
- Intelligent routing



MetaDefender™ Optical Diode
(Optional)

Primary Function

Enable one-way secure data transfer into highly secure forensic or classified environments without exposing them to external networks.

Key Capabilities

- Secure and compliant unidirectional data transfer
- Air-gap protection
- High-assurance evidence movement



MetaDefender™ Core

Primary Function

Inspect, scan, and sanitize digital evidence before forensic analysis to prevent malware from compromising investigation systems.

Key Capabilities

- Multi-AV scanning
- Deep CDR™
- File type verification
- Vulnerability assessment
- AI Content Inspector
- Data loss prevention
- Adaptive threat analysis



MetaDefender Aether™

Primary Function

Detect sophisticated and unknown threats using AI-powered analysis before investigators access suspicious evidence.

Key Capabilities

- Zero-day detection
- Emulation sandboxing
- Threat intelligence
- Threat reputation
- Machine-learning similarity search



How Evidence Moves Safely, Step by Step:

01 Secure Data Intake

Create a controlled entry point for physical media, endpoints, field collection devices, laptops, and file uploads using MetaDefender Kiosk, MetaDefender Drive, and MetaDefender Endpoint.

02 File-borne Threat Inspection

Analyze evidence with MetaDefender Core using multi-AV scanning, emulation-based sandbox, file-based vulnerability assessment and AI Content Inspector to flag AI-generated images, manipulated visual evidence, and fraudulent documents before they reach investigative environments.

03 Data Sanitization

Remove or rebuild risky elements including macros, scripts, and embedded objects with Deep CDR™ Technology to produce clean, usable evidence files when policy allows.

04 Sensitive Data Discovery

Use Proactive DLP™ to inspect documents, images, archives, and video for credit card numbers, national IDs, personal data, and confidential case information so agencies can classify, redact, route, or restrict evidence by policy.

05 Secure Data Movement

Move evidence to forensic labs, case management systems, prosecutors, partner agencies, and air-gapped repositories with encryption, approval workflows, and audit logs through MetaDefender Managed File Transfer and MetaDefender Optical Diode.

Connect Secure Digital Evidence Workflows Across Your Ecosystem

Forensic & Case Workflows

REST APIs and ICAP connect scanning and transfer to forensic tools, case management systems, and evidence repositories.

Security Operations

Malware detections, threat intelligence and analysis results feed into SIEM, SOAR, EDR, and SOC workflows.

Threat Intelligence Sharing

Exchange threat indicators and investigation-relevant intelligence using standardized formats such as STIX and MISP to support cross-agency collaboration.

MetaDefender Platform: Purpose-Built for Investigative Environments

Secure Evidence Intake

Malware hidden in seized devices and files is caught before it reaches investigative environments.

Strengthen Chain of Custody

Hashing, audit trails, and policy enforcement that flag AI-generated or manipulated content.

Streamline Investigations

Automated scanning, transfer and analysis workflow to improve efficiency.

Sensitive Data Protection

Find and control regulated, sensitive and confidential data within evidence.

Preserve Operational Continuity

Reduce malware risk without slowing down operations.

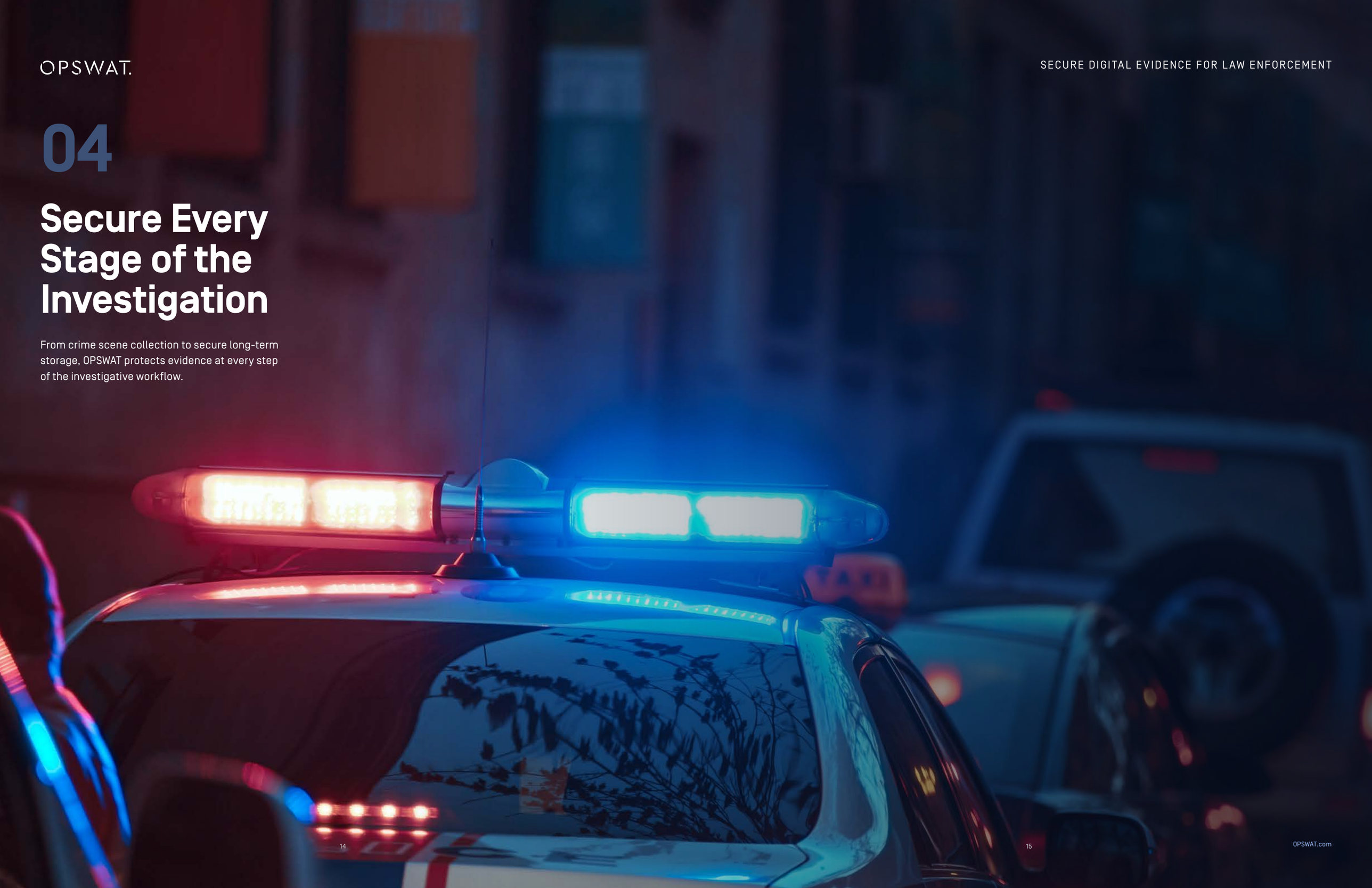
Resolve Multi-Device Dilemma

Bring kiosks, portable scanning, endpoint collection, and secure transfer together in one evidence workflow across field sites and forensic labs.

04

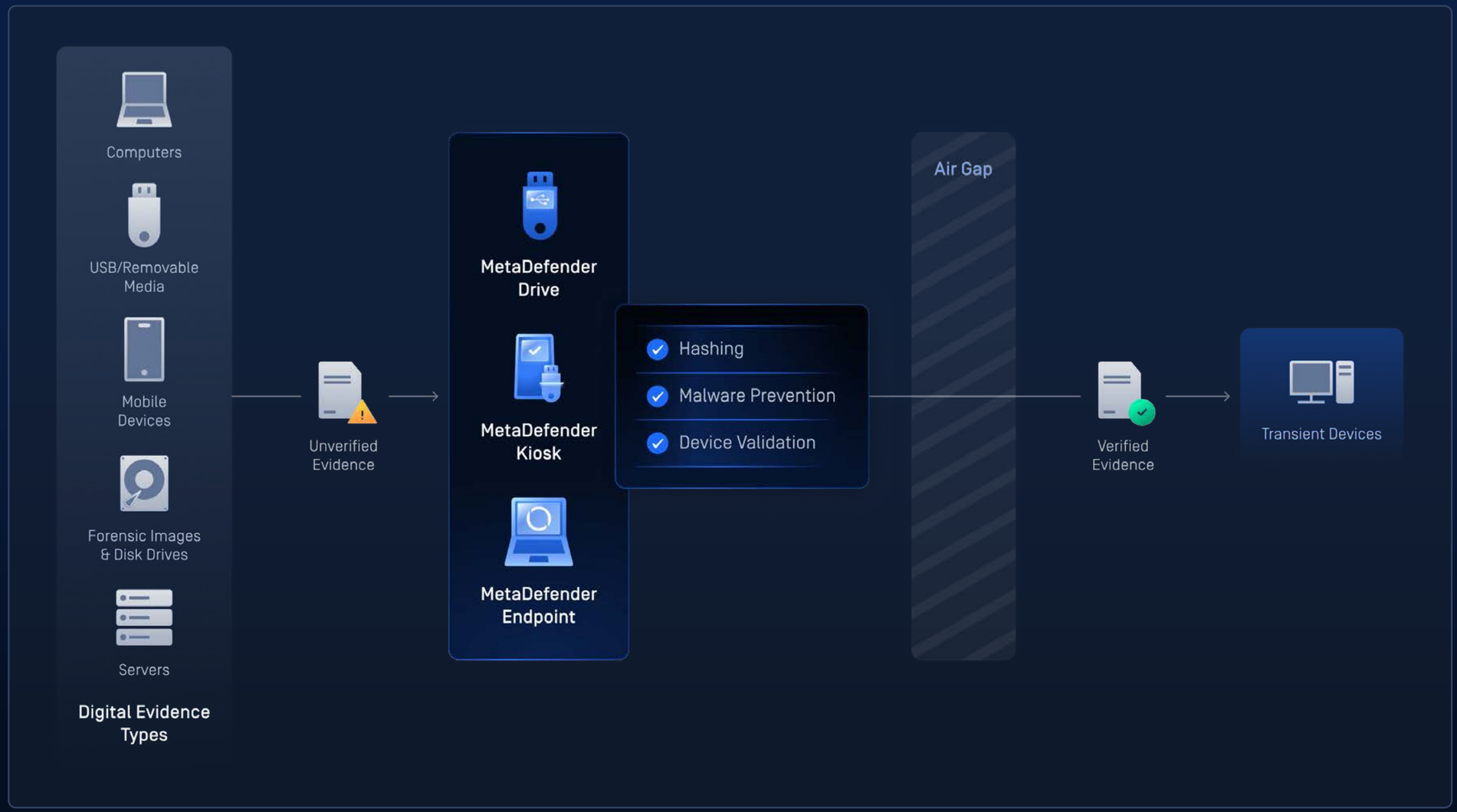
Secure Every Stage of the Investigation

From crime scene collection to secure long-term storage, OPSWAT protects evidence at every step of the investigative workflow.



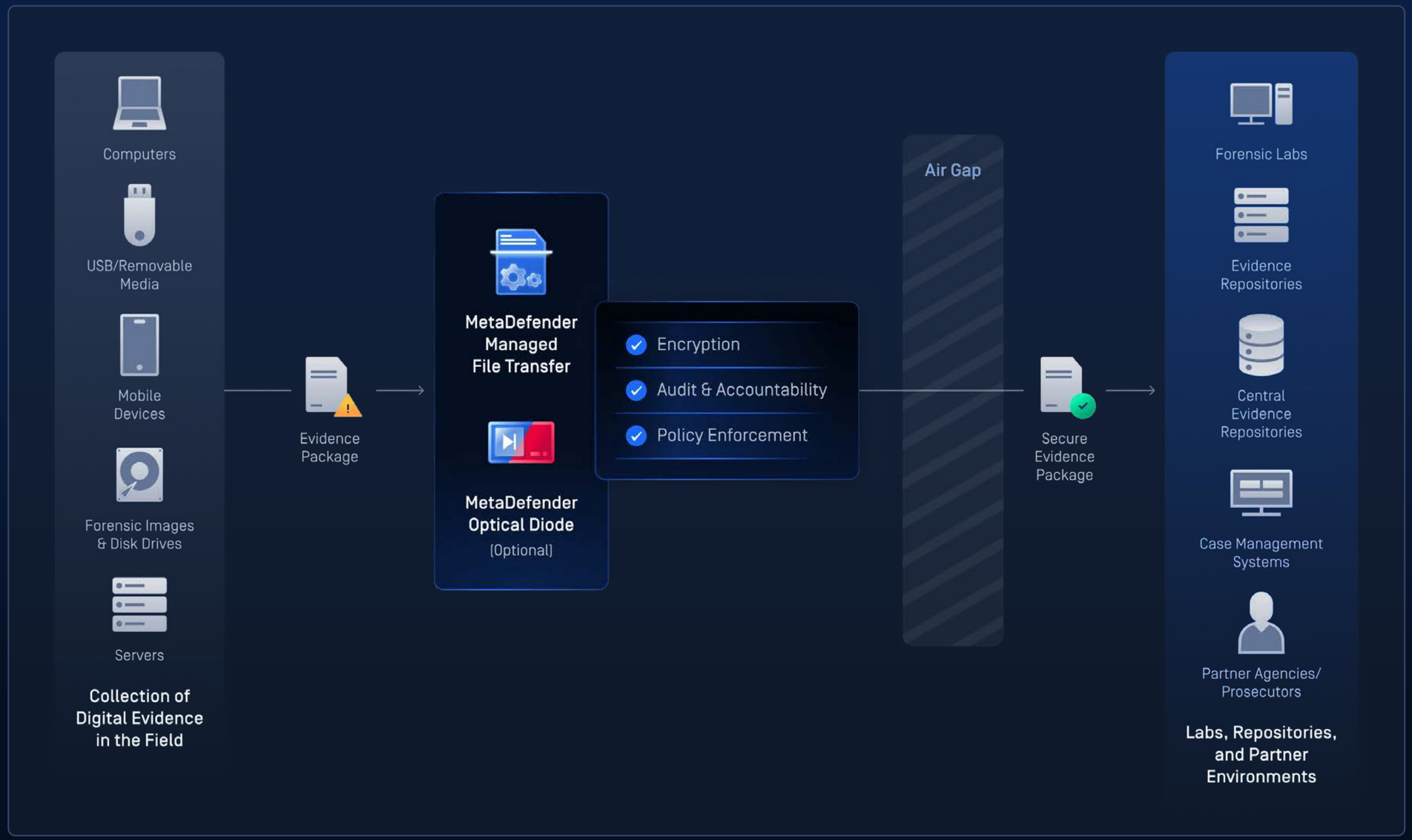
Crime Scene Evidence Collection

Investigators frequently encounter seized laptops, removable media, mobile devices, and external storage that may contain malware. OPSWAT helps teams safely access, scan, and validate evidence before it enters investigative environments.



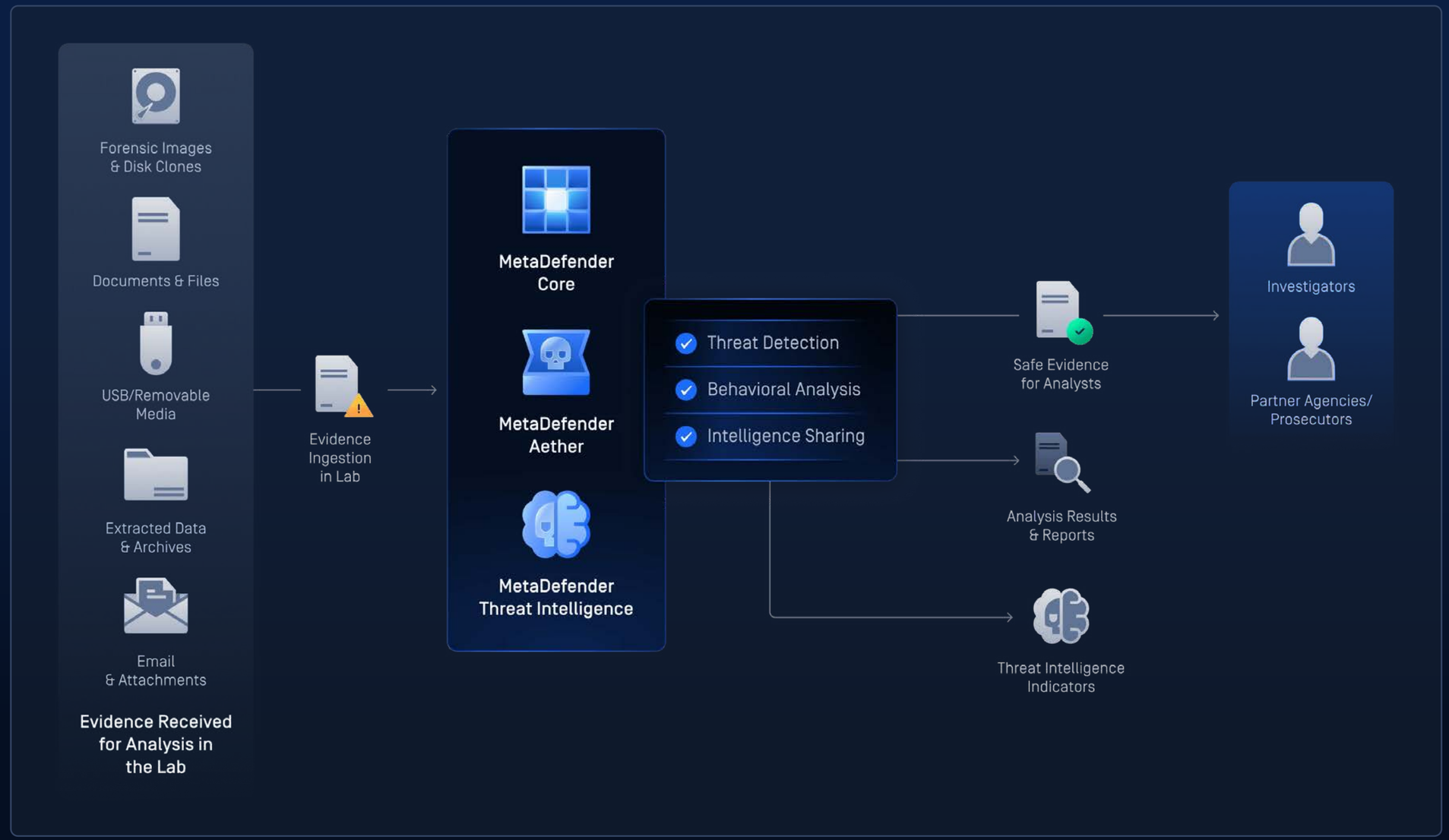
Evidence Transfer Between Locations

Secure evidence transfers with encryption, sensitive data detection, policy enforcement, and tamper-evident audit logs, including one-way delivery into air-gapped forensic environments.



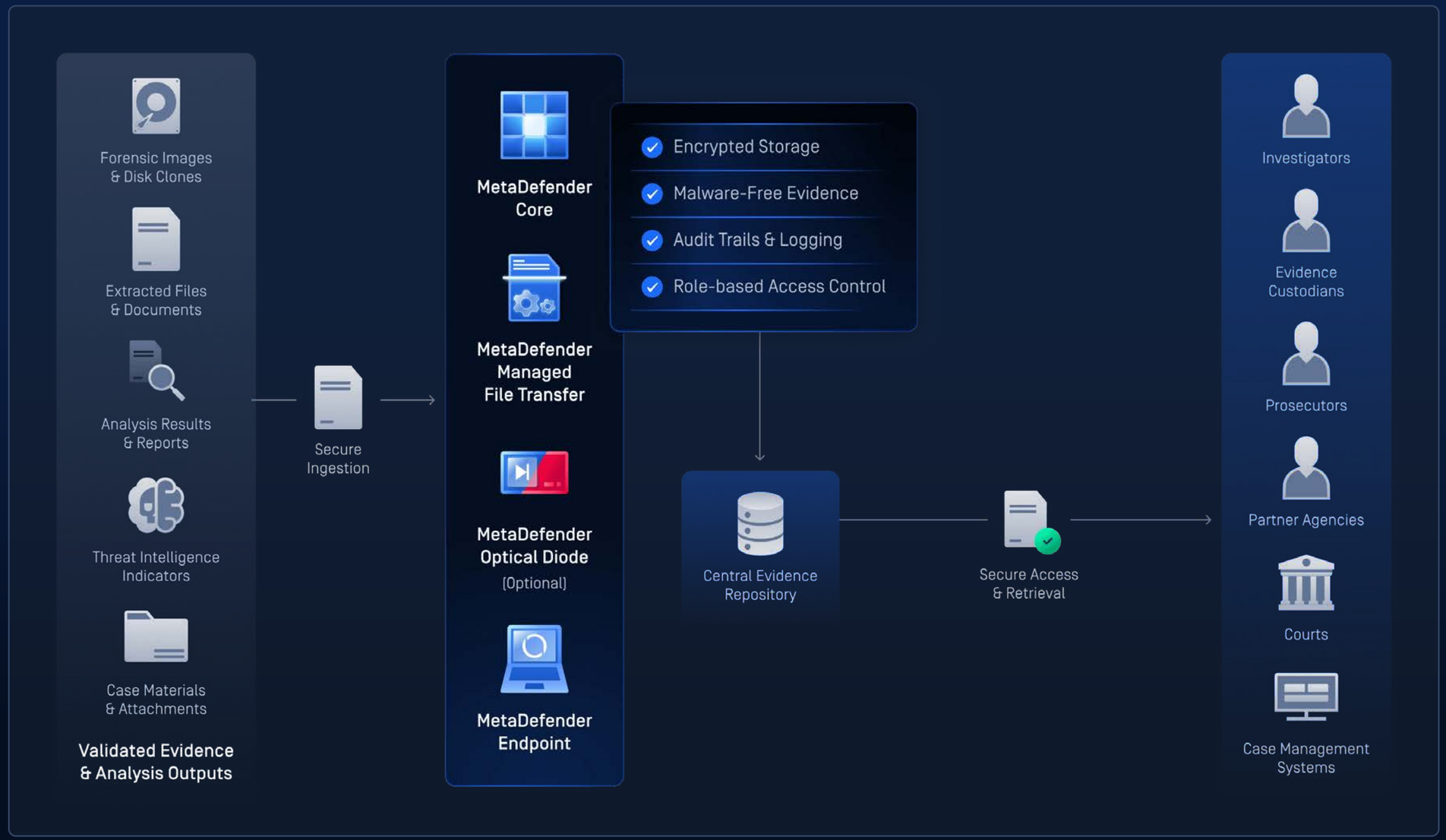
Forensic Lab Analysis

Files and forensic images are analyzed and sanitized before investigators or prosecutors open them, without exposing internal systems.



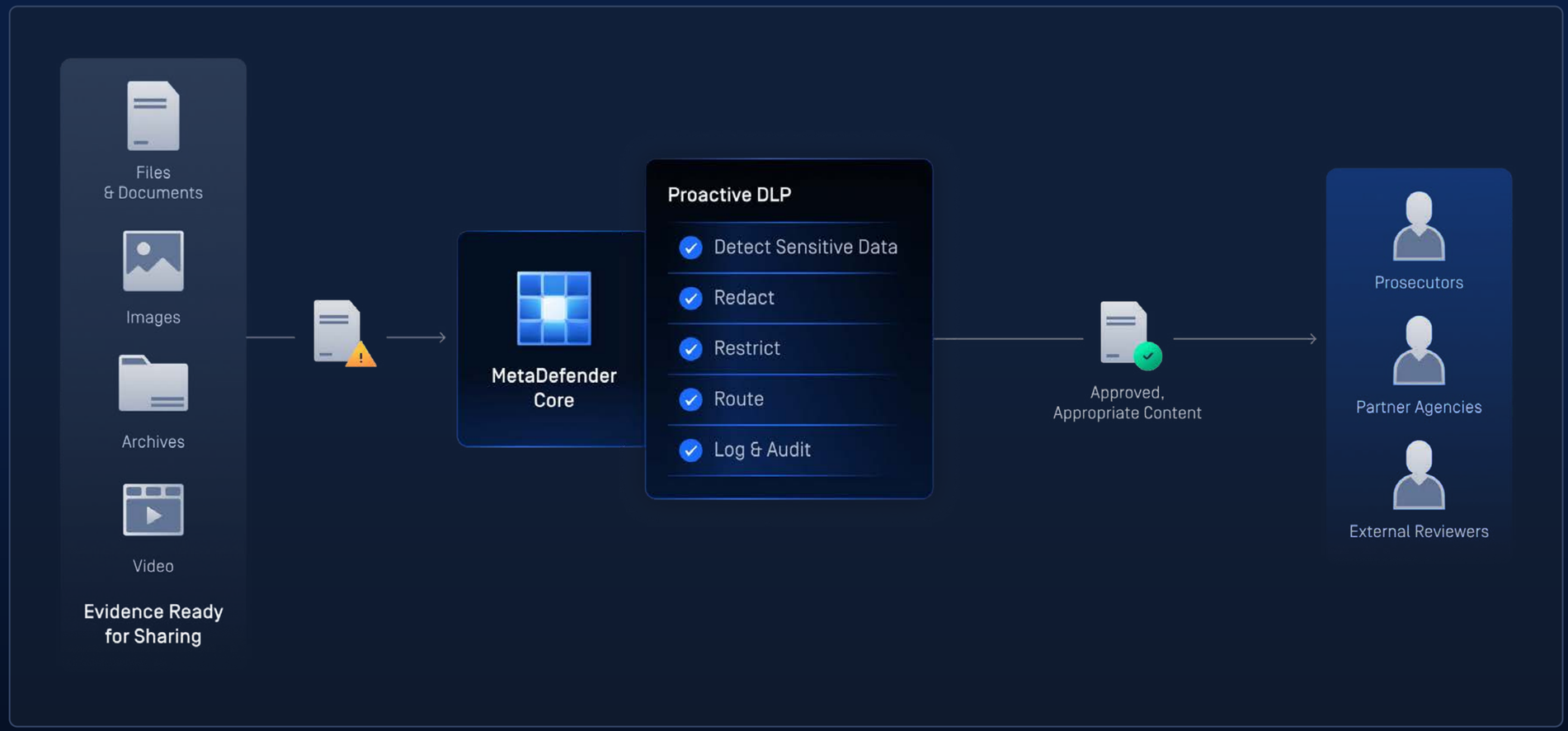
Secure Evidence Repository

Protect digital evidence repositories with continuous malware scanning, secure transfer controls, access validation, and real-time monitoring to support secure long-term storage and retrieval.



Sensitive Data Detection Before Sharing

Documents, archives, images, and video are checked for regulated data before release, so agencies can redact or restrict what shouldn't go out.



05

Why OPSWAT

Zero Trust Evidence Handling

Every device and file is verified before it can reach sensitive evidence environments.

End-to-End Protection

One platform secures evidence from the crime scene through final disposition.

Built for Scale

Automation keeps pace with growing caseloads without adding headcount.

Proven in High-Security Environments

Trusted by over 2,100 organizations worldwide to protect their critical data, assets, and networks from device and file-borne threats.

Support Security and Evidence Handling Requirements

CJIS Security Policy

Protect criminal justice information with malware prevention, access controls, audit logging, and secure transfer.

NIST SP 800-53

Support the security and privacy controls required in federal and government environments.

ISO 27001

Strengthen information security management through monitoring, access control, and secure transfer.

CMMC

Support the cybersecurity practices required of defense contractors and organizations handling sensitive government data.

Trusted by Governments and Critical Infrastructure

> With OPSWAT's multiscanning capabilities and emulation-based sandbox, we get both depth and speed. Files are cleared or flagged in minutes, not hours.
>
> Cybersecurity Specialist, Regional Government Forensic Agency

> A single weak link in this chain could open the door to cyberthreat with immediate and severe consequences: leaked evidence, derailed investigations, and the risk of suspects evading justice.
>
> Public Institution, Law Enforcement & Public Safety

> Handling external files is a major risk for law firms. That's why we use OPSWAT Kiosk... keeping sensitive case data secure from day one.
>
> Cybersecurity Specialist, FISCHER (FBC & Co.)

GET STARTED

Law enforcement evidence workflows run on speed, control, and trust. OPSWAT helps protect all three.

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 over 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 2,000 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.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, Metascan, MetaDefender, MetaDefender Managed File Transfer (MFT), MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. 2026-08