OPSWAT.

SOLUTION BRIEF

Secure Forensic Investigation for Law Enforcement

OPSWAT.

Products

- MetaDefender Core™
- MetaDefender Threat Intelligence™
- MetaDefender Sandbox™

Key Advantages

Reliable and secure acquisition of evidence

Seamless digital investigation workflow

Enhanced threat detection

Preserved chain of custody

Real-time threat intelligence

Secure inter-agency collaboration

Shorter time to investigation

SIEM, SOAR & EDR integration

Combating Malware Risks in Digital Forensic Processes

As digital transformation accelerates, law enforcement agencies increasingly rely on digital evidence to solve cases. This evidence is crucial for modern investigations but demands rigorous handling to avoid contamination, ensure admissibility, and preserve the chain of custody. When devices are seized, law enforcement often creates “images” of the data—such as Encase (EOL) or UFDR images—which must be thoroughly checked for malware or tampering before analysis. Sophisticated malware like Emotet, ransomware, and other evolving threats pose severe risks to the integrity and security of digital evidence.

The entire cycle of collecting, processing, and storing digital evidence introduces potential vulnerabilities that could impact chain of custody and, ultimately, case outcomes. To maintain evidentiary value, digital forensics typically involves a three-step process:

01

Seizing the Media

Securing and acquiring digital devices while ensuring that they are not tampered with or contaminated. Proper protocols are essential to uphold the integrity of the evidence from the point of seizure.

02

Acquiring the Media

A forensic image of the media is created. This involves making a bit-by-bit copy of the original data, which investigators use for analysis. The original media remains untouched to preserve its integrity and legal admissibility.

03

Analyzing the Forensic Image

Examining the forensic image allows for in-depth analysis while leaving the original media unchanged. This approach preserves the probative value of the evidence and mitigates risks of data alteration.

Each step in this process requires advanced tools and techniques for detecting and analyzing malware, ensuring that potential threats are identified and contained. OPSWAT’s MetaDefender suite offers multi-layered threat detection, prevention, analysis, and real-time threat intelligence capabilities essential for forensic teams to securely handle and analyze digital evidence.

Key Capabilities

Detects threats with MetaScan™ Multiscanning using 30+ commercial anti-malware engines to identify both known and emerging threats.

Provides real-time threat intelligence with up-to-date insights on malware sources and threat actors via Threat Intelligence feeds.

Facilitates secure collaboration by enhancing inter-agency cooperation with Standardized Threat Data Formats(e.g., STIX, MISP).

Enhances investigation by facilitating inter-agency cooperation, uncovering advanced malware behaviors, and supporting detailed forensic analysis.

Uncovers hidden malware behavior, such as data exfiltration, through behavioral analysis with emulation-based sandbox.

Maintains detailed forensic records, thorough documentation of potential threats, while preserving evidence security and admissibility.

Why OPSWAT MetaDefender?

Enhanced Threat Detection and Containment

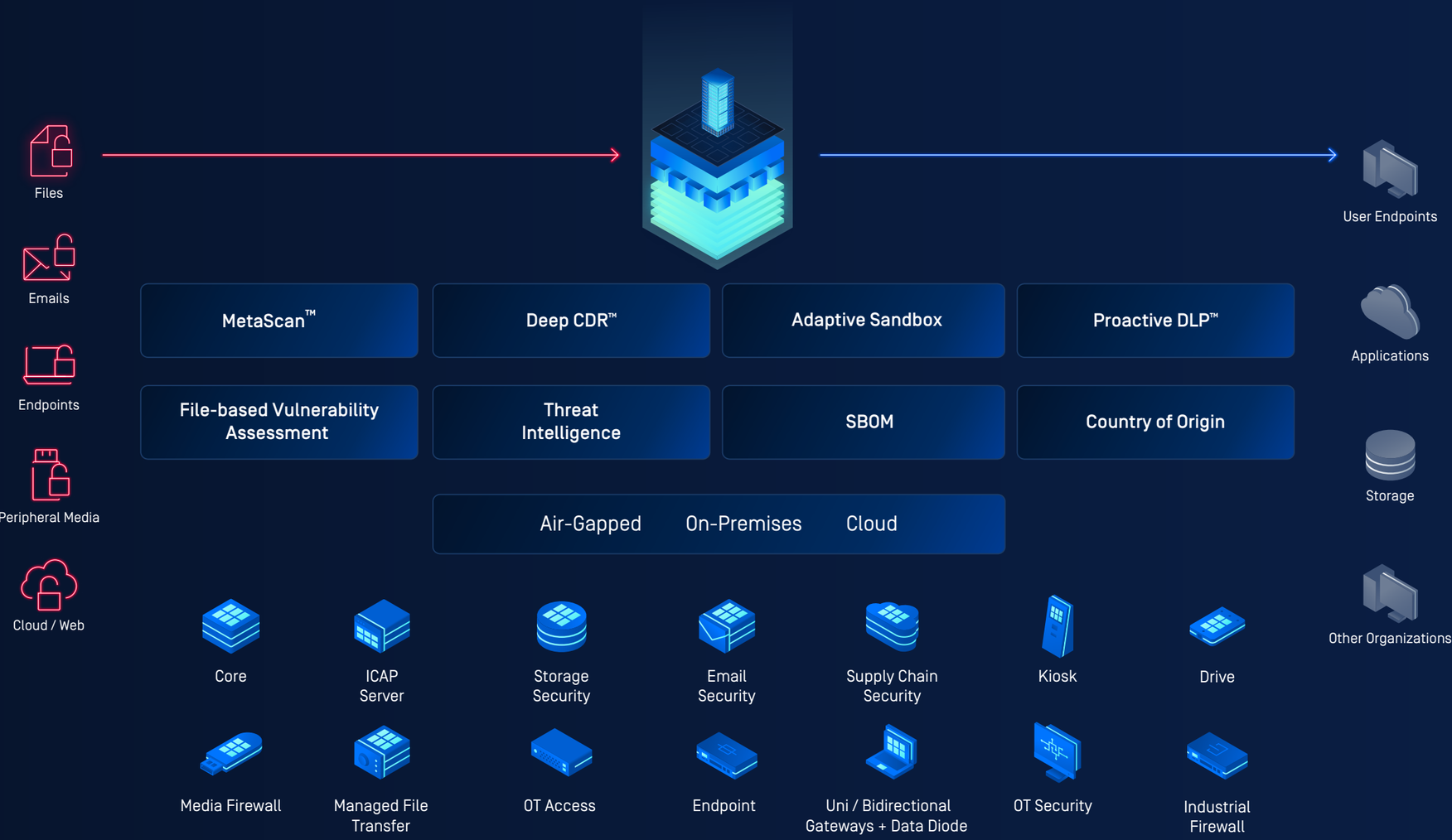
Neutralizes malware threats embedded within seized digital assets, ensuring these assets remain uncontaminated and unaltered.

Improved Intelligence and Collaboration

Facilitates secure, inter-agency threat intelligence sharing in standardized formats, supporting cross-jurisdictional investigations and enhancing the value of digital evidence.

Protection of Digital Evidence and Chain of Custody

Secures digital evidence from threats and unauthorized access from the point of collection through the entire investigation process.



GET STARTED

Are you ready to put OPSWAT MetaDefender solutions 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.