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

Law enforcement relies on digital evidence to solve cases, but handling it securely is critical to maintaining its integrity and admissibility. Malware threats like ransomware and advanced attacks can compromise forensic processes, risking contamination and chain-of-custody breaches. OPSWAT's MetaDefender suite provides forensic teams with powerful tools for multi-layered malware detection, prevention, and threat intelligence, ensuring digital evidence remains secure at every stage—from collection and imaging to analysis.

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. With its multi-layered approach to threat detection and prevention, MetaDefender not only safeguards digital evidence but also secures the critical steps of forensic analysis.

Key Capabilities

MetaDefender provides forensics teams cutting-edge capabilities tailored to meet their security and data integrity needs, ensuring evidence can be thoroughly examined without risk of exposing law enforcement to file-borne threats.

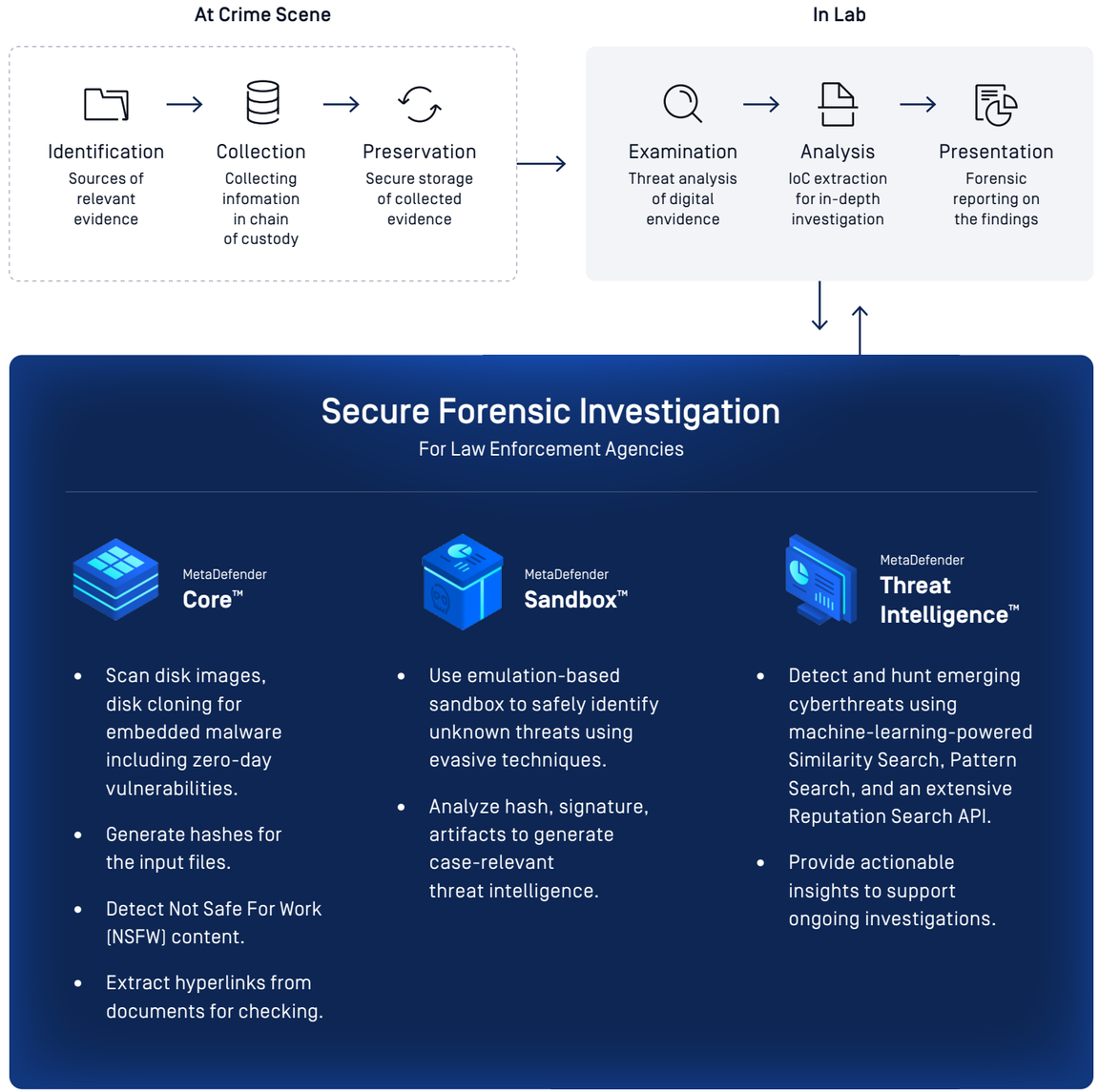
MetaScan™ Multiscanning uses 30+ commercial AV engines, as well as heuristics and machine learning, to identify known and unknown threats.

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

Standardized Threat Data Formats (e.g., STIX, MISP) are supported to enhance and fortify inter-agency cooperation.

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

Emulation-based Adaptive Sandbox uses behavioral analysis to uncover hidden malware behavior, such as data exfiltration, and valuable IOCs (indicators of compromise).



Why OPSWAT MetaDefender?

Enhanced Threat Detection and Containment

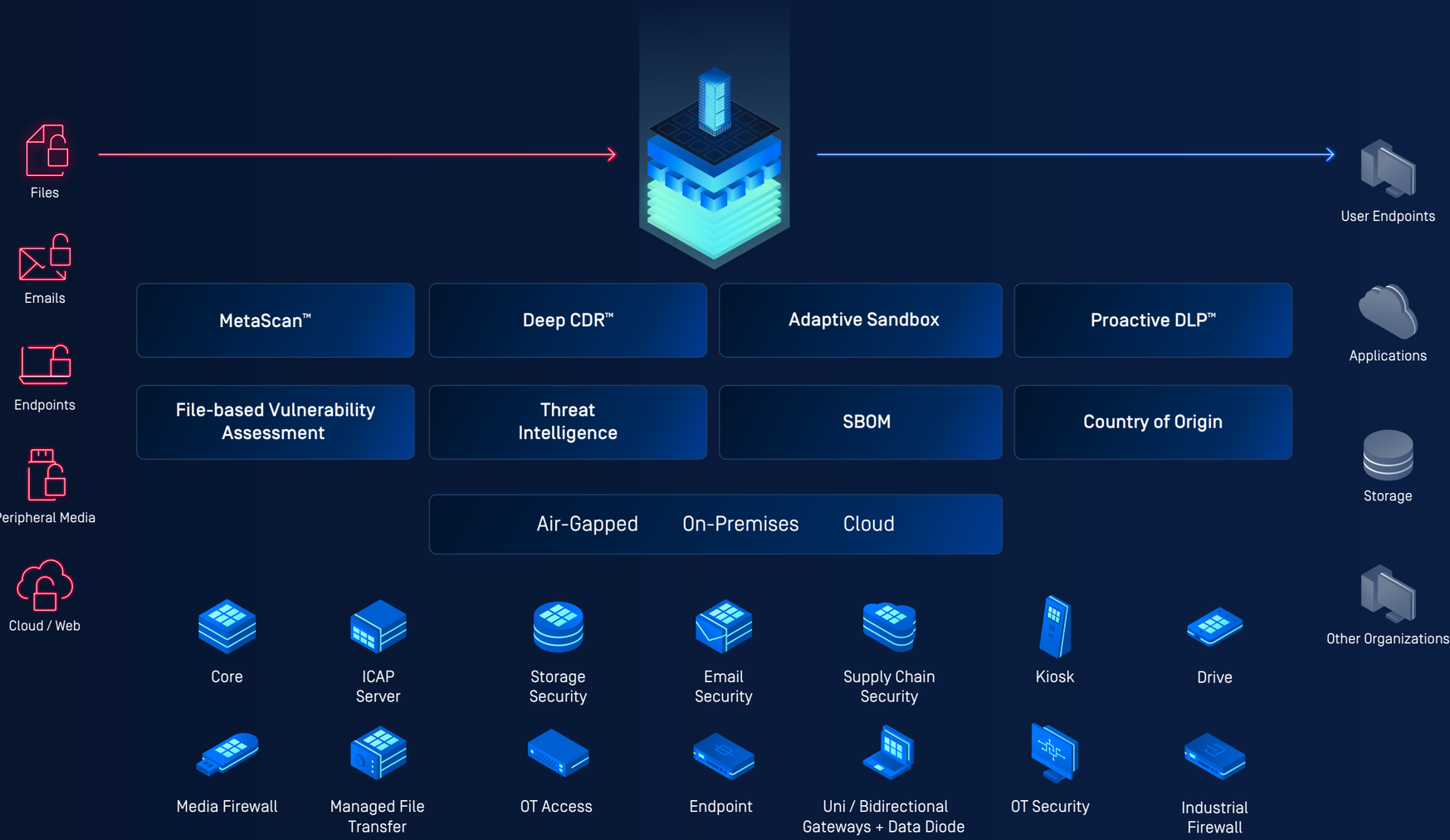
Neutralizes malware threats embedded within seized digital assets, ensuring these assets remain uncontaminated, without altering the file structure or integrity—a crucial requirement for the analysis of digital evidence.

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 Law Enforcement Infrastructure

Secures digital evidence from malware and unauthorized access, ensuring law enforcement officers can conduct safe and accurate forensic analysis without exposing their infrastructure to embedded threats.



GET STARTED

Are you ready to put OPSWAT MetaDefender solutions on the front lines of your Digital Forensic Process?

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.