OPSWAT.

Deep File Inspection for Security Operations Teams

Reduce Alert Fatigue. Stop File-Based Threats Before They Execute.

The average SOC team processes hundreds, often thousands, of alerts per day. Most do not require action. Many are wrong. Meanwhile, the threats keep coming, and the tools built for a different era cannot keep up.

OPSWAT File Security solutions inspect files before they reach systems or users: blocking known malware, flagging zero-day risks, and eliminating the noise that buries real threats. The result: fewer alerts, higher-confidence verdicts, and bandwidth for the threats that matter.

01 THE CHALLENGES

The SOC Alert Overload

Alerts fall into three categories:

Commodity alerts are low-value noise — repetitive, low-confidence detections that clog investigation queues and erode analyst focus over time.

False positives consume real investigation hours without producing outcomes; chasing them is expensive and demoralizing.

True positives — the threats that actually require a response — are buried beneath both. Accurately identifying them, and quickly, is the core of what a SOC exists to do.

The problem is not analyst capability. It is that detection tools generate alerts reactively after a file has already entered the environment.

OPSWAT.

SOLUTION BRIEF

02 THREAT SURFACE

How Threats Have Evolved

The attack surface has grown: more entry points, more alerts, more triage burden. SOC teams need prevention at the point of entry to filter threats early before they ever reach the queue.

PAST STATE

File-based threats were dangerous, but slow enough that detection could keep pace.

- Malware hidden inside Office macros and scripts
- Malicious hyperlinks embedded in PDFs and documents
- OLE (Object Linking and Embedding) objects used to trigger payload execution on open
- Images carrying hidden code via steganography
- Sensitive data exposed through file metadata
- Vulnerabilities in file parsers exploited at the point of opening
- Ransomware delivered via email attachments
- Spoofed file extensions masking executable content

CURRENT STATE

AI has collapsed the cost and skill required to create file-based threats.

- All legacy file-based threats persist — now generated and deployed at machine speed
- LLMs (Large Language Models) produce convincing phishing documents indistinguishable from legitimate ones
- AI-generated invoices, contracts, and wire instructions are weaponized for financial fraud
- Supply chain attacks embedded inside trusted, legitimate-looking files
- Every cloud upload, web form, and API transfer is a potential entry point beyond just email

FUTURE STATE

As AI capabilities scale, the threat trajectory accelerates.

- File creation volume continues to explode — more files mean exponentially more attack surface
- Zero-days are discovered and weaponized faster: dwell time shortens and response windows shrink
- Adversarial AI iterates on evasion techniques continuously, outpacing signature-based detection
- Autonomous attack pipelines generate, test, and deploy file-based payloads at scale with no human involvement

Understanding the prior state of the threat landscape allows us to navigate modern threats with historical context, allowing for better decisions and outcomes.

The File is the Weapon

Phishing is the delivery mechanism. People are the weakest link. But the file is the weapon.

Thousands of files move through an organization every day. Wire transfer instructions. KYC (Know Your Customer) documents. Trade confirmations. Email attachments. Build artifacts. Any of them can carry a payload, and users do not need to install anything. They only need to open the file.

OPSWAT treats every file as a potential threat and inspects it before it becomes one. Every detected threat is mapped to MITRE ATT&CK, so SOC teams get immediate context for hunt campaigns, TTP investigation, and risk prioritization, backed by threat intelligence at opswat.com/technology-center/research-center.

Key Benefits

Arrives
Email attachment, web upload, storage, transfer, or removable media — the number one threat vector for malicious intent.

Evades
Signatures don't flag it; EDR (Endpoint Detection and Response) finds no known behavior; the file lands in storage with a clean verdict.

Dwells
The file is inactive, profiles the environment, and fires no behavioral anomaly.

Executes
Reaches a command-and-control server; ransomware begins encrypting; data begins exfiltrating.

Detected
Too late — the SOC alert fires after the breach has started.

03 WHY OPSWAT

From Alert Fatigue to True Positive

OPSWAT meets your SOC where it is today and scales as your program matures. Whether you're starting with standalone sandbox detonation or deploying a full file lifecycle platform, the goal is the same: eliminate the noise, surface the threats that matter, and let your analysts focus on what they were hired to do.

Key Benefits

Advanced Threat Detection and Prevention	High Performance and Scalability	Simple and Flexible Deployment	Proven at Scale
OPSWAT File Security integrates multi-layered detection and prevention technologies in a single platform. Achieved a 100% protection score from SE Labs.	Files are processed and regenerated in milliseconds. Built-in high-performance architecture and load balancing scale to any volume.	Deploy on-premises, in the cloud, or air-gapped via REST API or ICAP. Integrates with SOAR platforms to automate incident response and reduce false positives.	OPSWAT protects 2,000+ organizations across 16 critical infrastructure sectors, including Tier 1 banks, insurers, and payment processors.

Build the Right Program for Your SOC

OPSWAT supports organizations at every stage of maturity. Start with targeted deployment. Expand as the program grows.

GOOD: DETECT	BETTER: ACCELERATE	BEST: PREVENT
MetaDefender Aether™ Standalone ▪ Detects zero-days that bypass signature-based tools ▪ Reduces false positives — only flags what truly executes maliciously	**MetaDefender Aether + OPSWAT Predictive Alin AI** AI-Accelerated Detection ▪ Pre-filters and triages files with ML-based scoring before malware detection and analysis ▪ Faster verdicts, lower analyst burden ▪ Shift-left: catch threats earlier in the file lifecycle	**OPSWAT File Security Platform** Full file lifecycle coverage across uploads, transfers, storage, and sharing channels ▪ Multi-engine detection (30+ AV engines) ▪ Deep CDR™ technology sanitizes files before they reach systems ▪ MetaDefender™ ICAP Server prevents malicious files at the network perimeter ▪ MetaDefender™ Storage Security scans files at rest, continuously ▪ MetaDefender™ Managed File Transfer secures every transfer channel
Optimize your SOC. Stop zero-days before they execute.	**Faster triage. Smarter detection. Less analyst fatigue.**	**Eliminate the work the SOC shouldn't have to do in the first place. Prevent, don't just detect.**

99+%
Malware Detection Rate
Metascan™ Multiscanning

<0.1%
False Positives
Predictive Alin AI:
Zero-Day Prediction

20x
Faster than Traditional Tools
MetaDefender Aether:
Zero-Day Detection

Get Started

Are you ready to put MetaDefender solutions on the front lines of your cybersecurity strategy?
Talk to an Expert: opswat.com/get-started

OPSWAT.
Protecting the World's Critical Infrastructure