OPSWAT

DATASHEET

METADEFENDER

FileTAC

File Triage, Analysis and Control

Close the end-user security gap by stopping file-borne breaches and incidents with technology that takes the risk out of the end-users' hands.

Today's biggest security threats are malware, ransomware, phishing campaigns, impersonation, scams, fraud, and data loss violations. These threats typically have two things in common: an end user and a file.

Other detection and response solutions (XDR, NDR, EDR) are ineffective against file-borne attacks. Our FileTAC solution is purpose-built for file analysis at scale. No one analyzes files - in more depth, faster, or across time- better than InQuest®.

Core Competencies

- Threat Prevention
- Data Loss Prevention
- Powered by our Deep File Inspection® (DFI) Technology
- Threat Hunting via RetroHunting

Features

- Dissects common carriers to expose embedded logic, semantic context, and metadata
- Typically results in 4X the amount of analyzable content relative to original file size

Differentiators

- Streamlines attack and incident identification with its effective recognition of malicious documents and extraction as well as submittal of IOCs to other tools
- Easily integrates into any SecOps infrastructure and tooling via robust APIs as well as the ability to automate workflows
- Automates the costly and intensive manual process of document reverse engineering and analysis
- Easy to deploy without giving the bad guys any indication of its presence in the environment

opswat.com/get-started

Our Technology

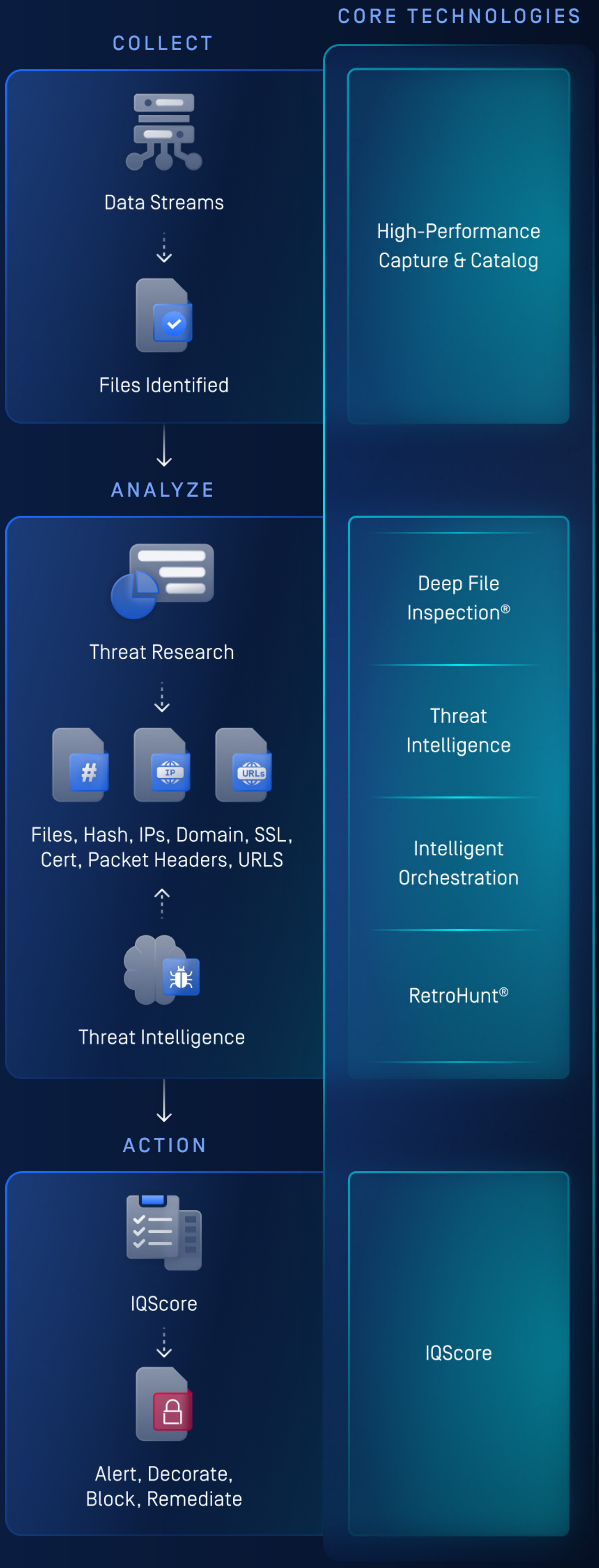
Our unique Deep File Inspection (DFI) technology automates human, analyst-grade file dissection - exposing 4x more content in an average of three seconds. These outputs are then analyzed through a combination of proprietary systems that include a Data Loss Prevention (DLP) engine, machine learning models, YARA signatures, malware detection engines, a variety of heuristics, and then finally enriched with threat intelligence, both third-party external IOCs as well as IOCs extracted within your environment by our DFI. This results in the rapid identification of files with sensitive, suspicious, or malicious characteristics.

Benefits

First and foremost, DFI saves organizations from the costs associated with file-borne malware, ransomware, exploits, phishing campaigns, impersonation, scams, fraud, and data loss breaches and incidents.

DFI also relieves staff from countless hours of work, reduces cybersecurity capital spend and operating costs, and drives up the efficacy and value of adjacent security solutions.

Attack Type	Average Total Cost
Ransomware Breach	$4.54M
Data Breach	$4.35M
Business Email Compromise (BEC)	$4.89M
Phishing	$4.89M
Compromised Credentials	$4.50M



CORE TECHNOLOGIES

COLLECT

Data Streams

Files Identified

High-Performance Capture & Catalog

ANALYZE

Threat Research

Files, Hash, IPs, Domain, SSL, Cert, Packet Headers, URLS

Threat Intelligence

Deep File Inspection®

Threat Intelligence

Intelligent Orchestration

RetroHunt®

ACTION

IQScore

Alert, Decorate, Block, Remediate

IQScore

OPSWAT.

Protecting the World's Critical Infrastructure

opswat.com/get-started