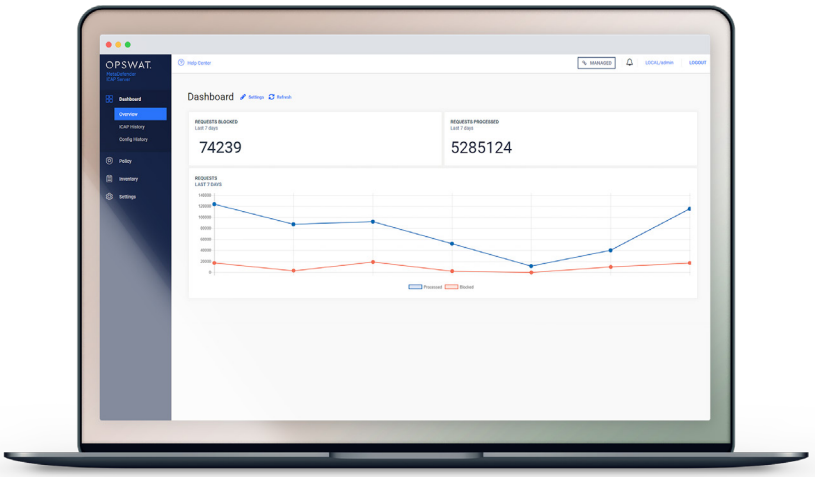
OPSWAT.

DATASHEET

MetaDefender® ICAP Server

Trust your network traffic



Hackers relentlessly attempt to upload malware to your systems. Employees accidentally visit malicious websites. External users submit files containing sensitive information.

MetaDefender ICAP Server enhances your network traffic security, while maintaining productivity.

Configure. Analyze. Address.

When a customer uploads a file to your website, it is scanned by anti-virus software. But what if it contains an undetected threat? What if it contains unexpected sensitive information, like a social security number?

MetaDefender ICAP Server protects your systems by inspecting every file traveling through your network. Every file is scanned for malware and vulnerabilities. Suspicious files can be blocked or sanitized. Sensitive files can be redacted. Files are remediated, before they are accessible to the end user.

MetaDefender ICAP Server protects your users from malicious internet content.

Benefits

Industry-Leading Multiscanning
Integrated multiscanning of 30+ engines

Sanitize Suspicious Files
Disarm unknown content and output clean, usable files

File-Based Vulnerability Assessment
Finds exploits before they reach your environment

Prevent Sensitive Data Leakage
Detect, redact, or block sensitive data

Customizable Policies & Role Functions
Configure workflow and analysis rules, based on file source

OPSWAT.

MetaDefender ICAP Server

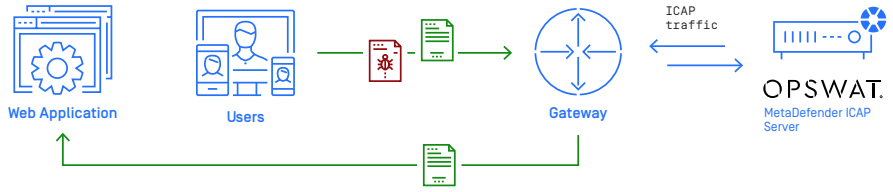
Configurations

MetaDefender ICAP Server integrates with any product that supports Internet Content Adaptation Protocol (ICAP) and can be installed at various intersection points to secure file transfer. For example:

Reverse Proxy / Web Application Firewall / Load Balancer

Protect application web servers from malicious file uploads.

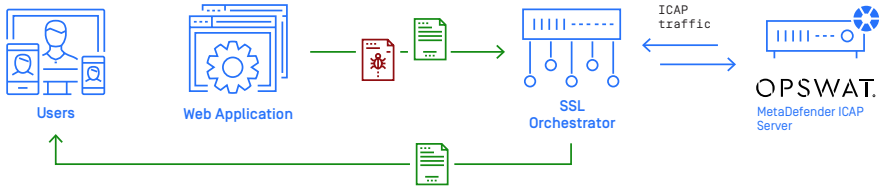
Supports: *F5 Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP LTM™, Symantec BlueCoat ProxyAG™*



SSL Inspection

Integrate multiple MetaDefender features at the point of decryption for simplicity and agility.

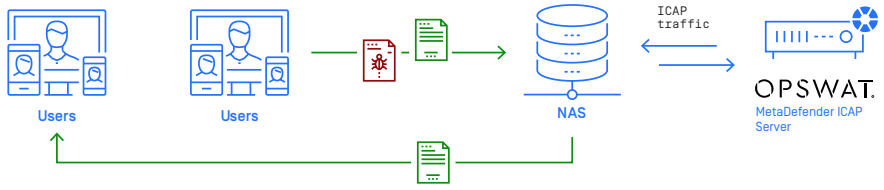
Supports: *F5 SSL Orchestrator™, A10 Networks Thunder® SSLi®.*



Network Attached Storage (NAS)

Scan retrieved files from NAS to avoid the spread of sensitive information or malware.

Supports: *Dell EMC® Isilon.*



Forward Proxy / Web Gateway / Firewall

Screen web traffic before it reaches a secured network.

Supports: *Squid, ARA Networks JAGUAR5000, McAfee Web Gateway™, Fortinet FortiGate®.*

Specifications

Supported Operating Systems

- **Windows**
  Windows 7, 10, Server 2012, Server 2016, Server 2019
- **Linux**
  Red Hat (6.6+, 7.0+), Ubuntu (16.04, 18.04), CentOS (6.6+, 7.0+), Debian (8.0+, 9.0+)

Hardware Requirements

Minimum RAM: 2GB,
Minimum HDD space: 20GB

Supported Browsers

Chrome, Firefox, Safari,
Microsoft Edge, Internet Explorer 11

Ports

Inbound (1344, 8048),
Outbound (8008)

Supported File Systems

NTFS, FAT32, AFS, Linux EXT2, 3 & 4

Deployment Model

Online/Offline, Physical/Virtual

OPSWAT.

Trust no file. Trust no device.