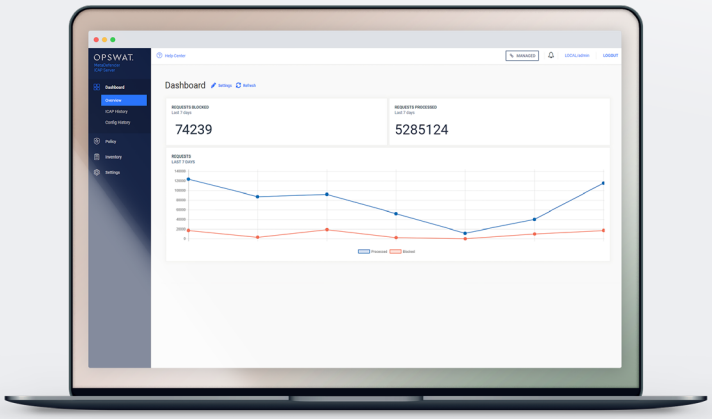
OPSWAT.

DATASHEET

MetaDefender® ICAP Server

Trust your network traffic



Protecting your network from malware is more challenging than ever before due to the commercialization of cybercrime as well as its evolution and further sophistication.

Right this moment, malicious or sensitive files might be intentionally or unintentionally transferring through your network by both internal and external users. The files can be intercepted by web application firewalls and sent to a web gateway antivirus. But what if the file contains advanced evasive malware or zero-day threats? And what if the files contain confidential data or unexpected PII?

"We've used OPSWAT technology for several years, in multiple integrations and in various products. Their reputation in the industry has just been stellar. I've worked in the industry for 30 years, and OPSWAT is a company I've always trusted and worked well with."

Joe Peck
Senior Director of Product Management, F5®

Configure. Analyze. Address.

By inspecting all files traveling through your network with MetaDefender ICAP Server and MetaDefender Core, your users and systems are comprehensively protected from malicious internet content.

MetaDefender ICAP Server provides ICAP interface between MetaDefender Core with any client application that supports the ICAP protocol, such as secure gateway, proxies, web application firewall, etc. Every file is processed with best-in-class threat detection and prevention technologies.

As a result, all suspicious files are blocked or sanitized before they are accessible to end user. Sensitive data is redacted, removed or blocked, helping enterprises meet security compliance standards.

Benefits

- Real-time comprehensive threat detection and prevention for your network
- Protection against zero-day and advanced targeted attacks
- File-based vulnerability detection before installation
- No more sensitive data entering or leaving your organization
- Custom policies, workflow and analysis rules to meet your unique security needs
- Simple integration with any ICAP enabled devices

OPSWAT.

MetaDefender ICAP Server

Integration

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 transfers.

Typical MetaDefender ICAP Sever integrations are illustrated below:

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

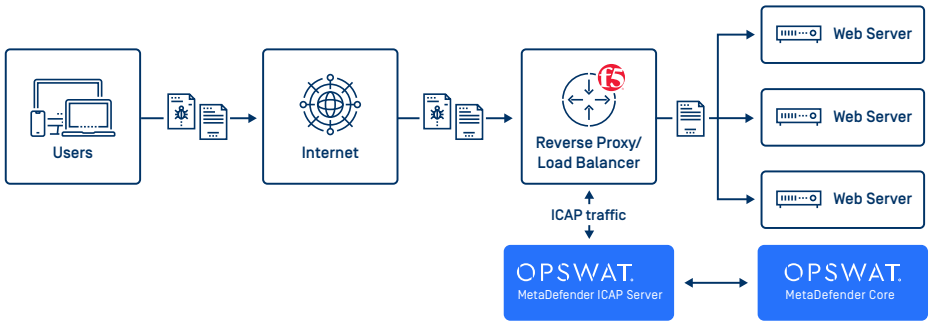
Ports
Inbound (1344, 8048), Outbound (8008)

Supported File Systems
NTFS, FAT32, AFS, Linux EXT2, 3 & 4

Deployment Model
Online/Offline, Physical/Virtual

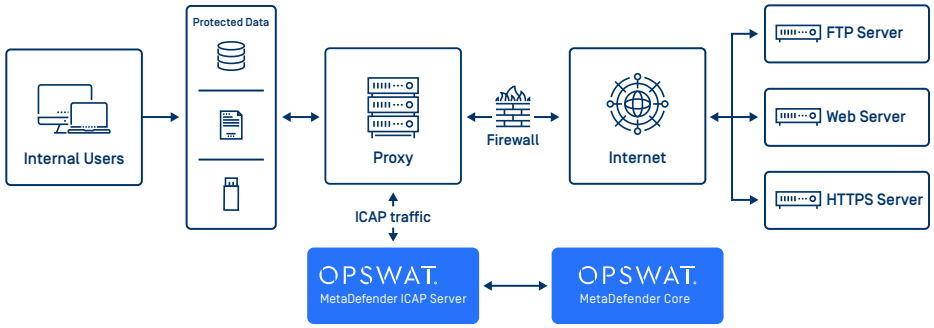
Reverse Proxy/ Web Application Firewall/ Load Balancer
Protect application web servers from malicious file upload

Supports: F5® Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP® LTM™, Symantec™ Blue Coat ProxySG



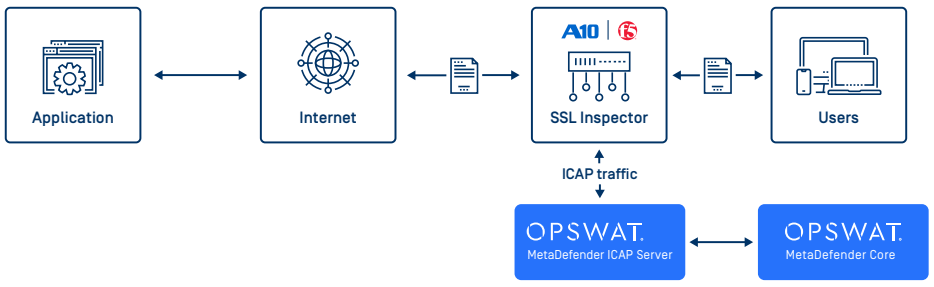
Forward Proxy / Web Gateway / Firewall
Screen web traffic before it reaches a secured network

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



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

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



OPSWAT.
Trust no file. Trust no device.

For further information about MetaDefender ICAP Server visit www.opswat.com/products/metadefender/icap

OPSWAT.com/contact