OPSWAT

DATASHEET

METADEFENDER™

ICAP Server

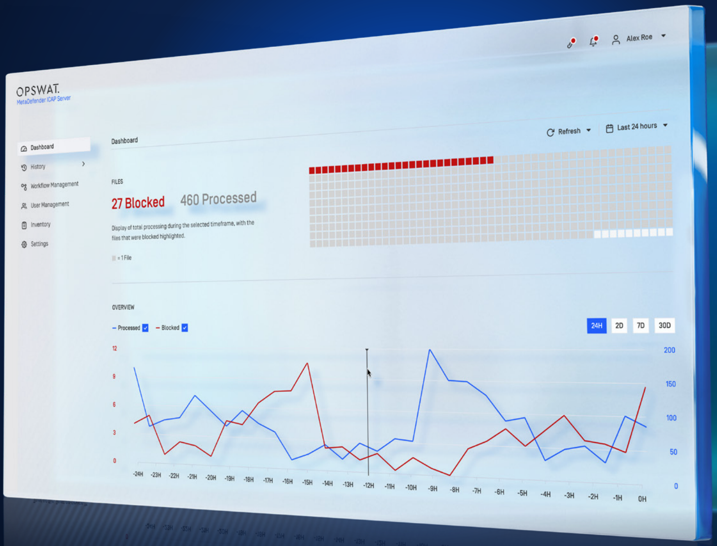
Secure Files at the Network Perimeter

MetaDefender ICAP Server integrates into your existing network devices to provide an additional layer of security for file uploads, file downloads, and file transfers.

With multi-layered threat detection and prevention technologies integrated via the lightweight internet content adaptation protocol (ICAP), MetaDefender ICAP Server can analyze files for potentially malicious content and sensitive data before they reach end users, helping organizations meet security and compliance requirements.

Benefits

- Real-time comprehensive threat detection and prevention to protect web applications from malicious files.
- Reduce overhead with simple plug-and-play integration via any ICAP-enabled network devices.
- Protect against malware, zero-day threats, advanced targeted attacks, and sensitive data leakage.
- Fits with all IT infrastructure with flexible deployment support for on-premises, hybrid, and cloud systems.
- Integrate in less than 10 minutes without infrastructure changes or system overhauls.
- Customize policies, workflow and analysis rules to meet your unique security needs.



Dashboard

FILES

27 Blocked 460 Processed

Display of total processing during the selected timeframe, with the files that were blocked highlighted.

Key Technologies

MetaScan™ Multiscanning

Detects nearly 100% of malware by scanning with 30+ leading AV engines simultaneously.

Deep CDR™

Zero-day exploits are neutralized by removing any potentially harmful and out-of-policy objects in files and regenerating new, safe-to-use files.

Adaptive Sandbox

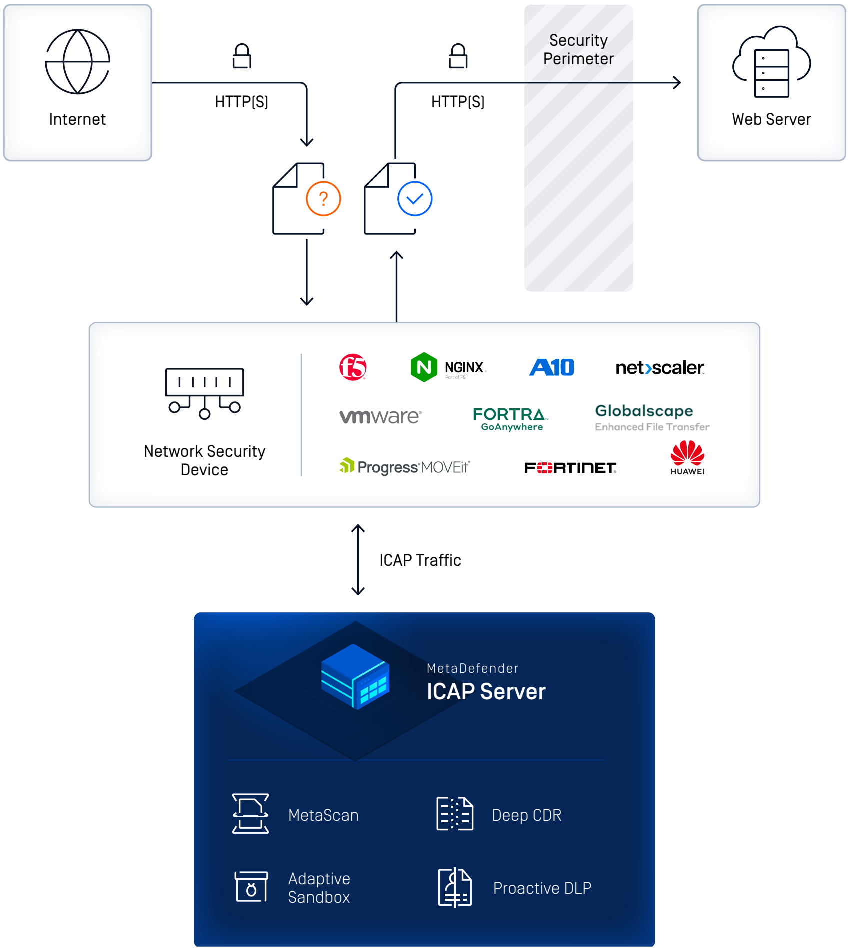
Dynamically detects complex and evasive malware threats using threat agnostic analysis of files and URLs, emulation of targeted applications, IOC (Indicator of Compromise) extraction, and Rapid Dynamic Analysis.

Proactive DLP™

Detect and block confidential or out-of-policy data, then automatically redacts the identified sensitive information in 110+ file types. Supports image-to-text recognition.

Industry-Leading Technologies

File Type Verification, Archive Extraction, Reputation Engine, InSights Threat Intelligence, File-Based Vulnerability Assessment, Country of Origin, and SBOM (Software Bill of Materials).



Integrations

As the most broadly compatible ICAP Server in the market, MetaDefender ICAP Server adapts to your infrastructure. Our solution can be installed at various intersection points and integrated with any network security devices that supports ICAP:

- Load balancers
- Web application firewalls
- Application delivery controllers
- Managed file transfers
- Ingress controllers
- Storage solutions
- Web gateways
- Reverse proxies
- Forward proxies
- Intrusion prevention systems
- Other ICAP-enabled devices and services

OPSWAT.
Protecting the World's Critical Infrastructure

Specifications

Supported Operating Systems

Windows	Windows 11 Windows Server 2019, 2022 or newer (64-bit)
Linux	CentOS 8.x, 9.x Red Hat Enterprise Linux 8.x, 9.x Rocky Linux 9 Debian 11.x , 12.x Ubuntu 18.04, 20.04, 22.04, 24.04

Hardware Requirements

RAM	Minimum 2GB free
SSD	2 GB + (Max size per scan request* [number of scan request in parallels])
CPU	Minimum 4 CPU cores

Supported Browsers

Chrome, Firefox, Safari, Microsoft Edge

Ports

Inbound	1344 (ICAP), 8048 (Web Management Console and REST interface), 8043 & 8443 (NGINX)
Outbound	8008 (only if MetaDefender Core in installed on a remote system)

Deployment Models

On-premises	
Cloud	
Physical/ Virtual deployment	Amazon Machine Images (AMI) Azure VMs
Containers	Kubernetes Helm support is available for Amazon EKS (Elastic Kubernetes Service), AKS (Azure Kubernetes Service), and GKE (Google Kubernetes Engine)

For more information on MetaDefender ICAP Server, visit opswat.com/products/metadefender/icap

Schedule a demo with a cybersecurity expert at opswat.com/contact