OPSWAT.

DATASHEET

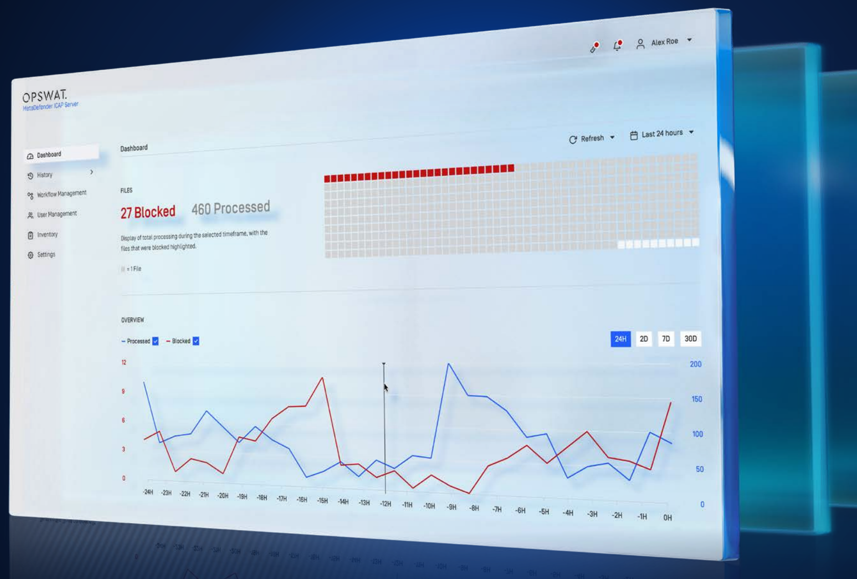
METADEFENDER™

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 multiple threat detection and prevention technologies integrated via the lightweight internet content adaptation protocol (ICAP), MetaDefender ICAP Server can analyze every file for potentially malicious content and sensitive data, helping organizations meet security and compliance requirements.



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

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.
- Customize policies, workflow and analysis rules to meet your unique security needs.

Key Technologies

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.

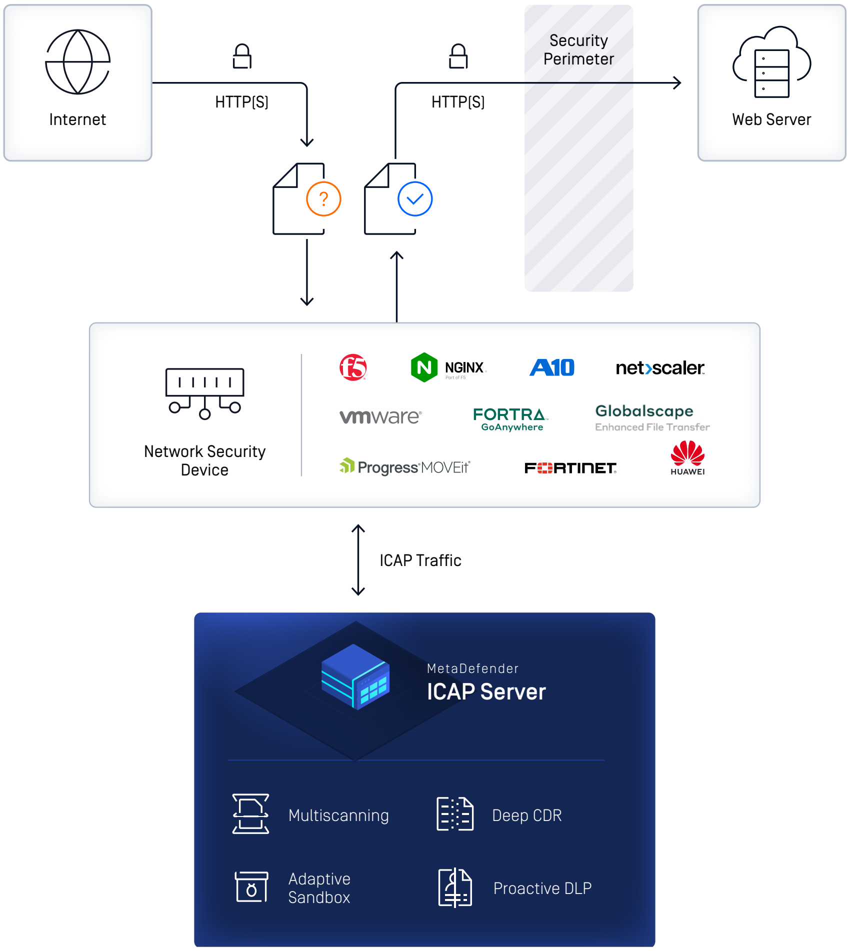
Adaptive Sandbox

Uses static and dynamic analysis to detect malicious behavior with 100x more resource efficiency than traditional sandboxes.

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.

opswat.com/get-started



Integrations

MetaDefender ICAP Server integrates with any product that supports ICAP and can be installed at various intersection points to secure your network traffic.

Supported network security devices include:

- Load balancer
- Web application firewall
- Application delivery controller
- Managed file transfer
- Ingress controller
- Storage solutions
- Web gateway
- Reverse proxy
- Forward proxy
- Intrusion prevention systems
- Other ICAP-enabled devices and services

Specifications

Supported Operating Systems

Windows	Windows 10 Windows Server 2016 or newer (64-bit)
Linux	CentOS 7.x, 8.x, 9.x Red Hat Enterprise Linux 7.x, 8.x, 9.x Debian 10.x, 11.x Ubuntu 18.04, 20.04, 22.04

Hardware Requirements

RAM	Minimum 2GB free
SSD	Minimum 5GB free

Supported Browsers

Chrome, Firefox, Safari, Microsoft Edge

Ports

Inbound	344 (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

OPSWAT.
Protecting the World's Critical Infrastructure