

## MetaDefender<sup>®</sup> ICAP Server

Trust your network traffic

Cybercrime is a multibillion-dollar business. Criminals use files to sneak malware into otherwise secure systems. Negligent users may download innocent-looking files meant to steal or encrypt data. Right now, files containing threats or sensitive data might be unknowingly moving through your network traffic and into your organization's infrastructure.

To best secure network traffic from malicious file upload attacks and data leakage, organizations need a comprehensive solution that defends against malware and mitigates risks from data theft.

### Our Solution

MetaDefender ICAP Server addresses issues before they are a problem. It integrates into your existing network devices to provide an additional layer of security.

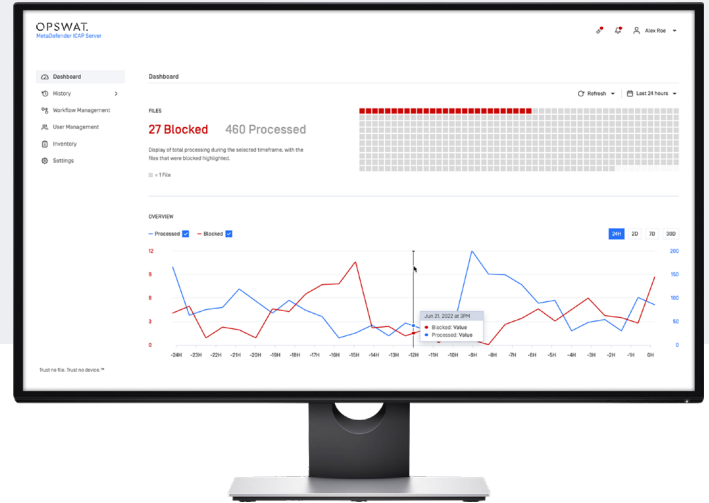
By combining multiple threat detection and prevention technologies, MetaDefender ICAP Server can analyze every file for malware, potentially malicious content, and sensitive data.

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

### Key Features

**Deep CDR (Content Disarm and Reconstruction)** prevents known and unknown file-borne threats and mitigates zero-day attacks

**Proactive DLP (Data Loss Prevention)** content-checks files for sensitive, private, and confidential data



### Benefits

- Leverage real-time comprehensive threat detection and prevention for network traffic
- Increase cost-efficiency with simple plug-and-play integration via any ICAP-enabled network devices
- Protect against zero-day threats and advanced targeted attacks
- Prevent sensitive data from entering or leaving the organization to mitigate data breaches and compliance violations
- Detect vulnerabilities in files before they are installed
- Customize policies, workflow and analysis rules to meet your unique security needs

**Multiscanning** detects over 99% of malware using more than 30 anti-malware engines

**File-Based Vulnerability Assessment** technology detects application and file vulnerabilities before they are installed

# OPSWAT.

## MetaDefender ICAP Server

### Integration

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

### Forward Proxy / Web Gateway / Firewall

Screen web traffic before it reaches a secured network

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

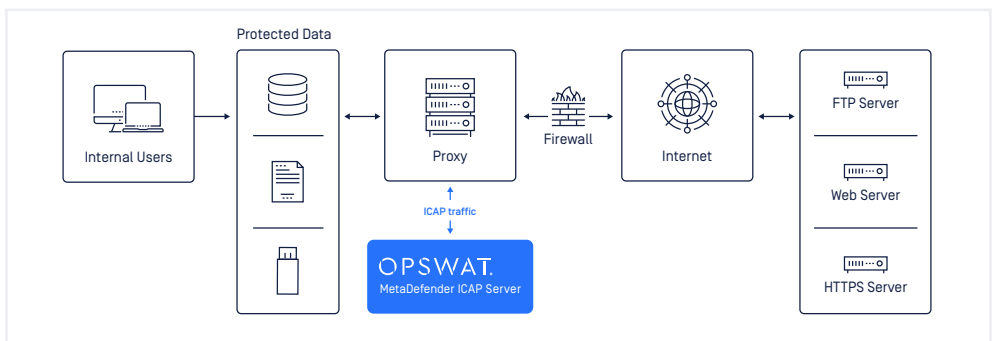
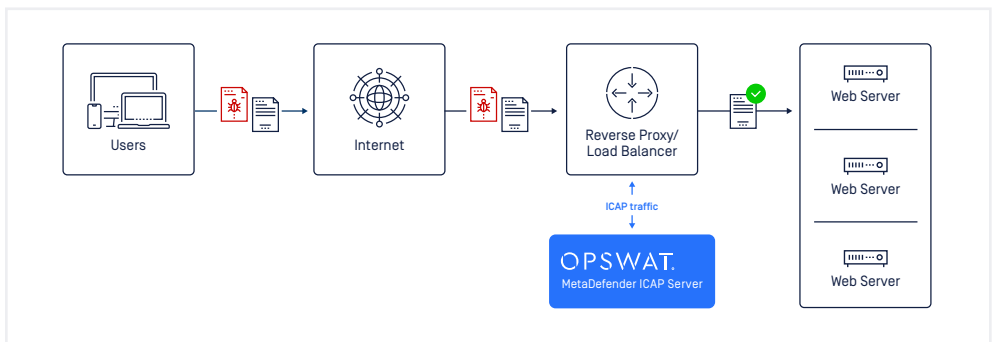
### Reverse Proxy / Web Application Firewall / Load Balancer / Application Delivery Controller

Protect application web servers from malicious file upload

**Supports:** F5® Advanced WAF™, F5 Big-IP® ASM™, F5 Big-IP® LTM™, Citrix ADC, Avi Vantage [VMware], Symantec™ Blue Coat ProxySG

### Specifications

<b>Deployment Model</b>	<b>Windows</b> Windows 10; Windows Server 2012, 2016, 2019 or newer (64-bit)	<b>Linux</b> Red Hat (7.x, 8.x); Ubuntu (18.04, 20.04); CentOS (7.x, 8.x); Debian (9.x, 10.x, 11.x)
<b>Hardware Requirements</b>	Minimum RAM: 2GB Minimum SSD: 2 GB + ~500MB x [number of managed scan engines]	
<b>Supported Browsers</b>	Chrome, Firefox, Safari, Microsoft Edge	
<b>Ports</b>	Inbound (1344, 8048), Outbound (8008)	
<b>Supported File Systems</b>	NTFS, FAT32, AFS, Linux EXT2, 3 & 4	
<b>Deployment Model</b>	Online/Offline, Physical/Virtual	



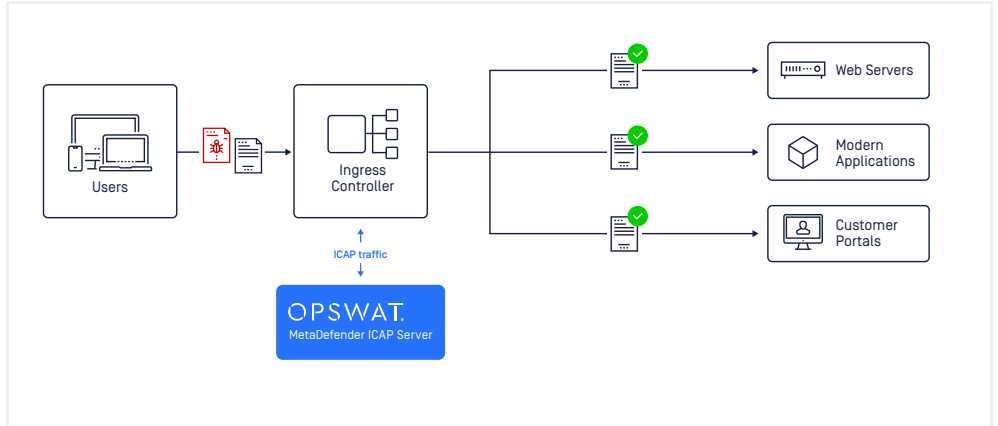
# OPSWAT.

## MetaDefender ICAP Server

### Ingress Controller

Inspect all incoming files for potential malicious files before they are admitted to applications deployed in containerized environments.

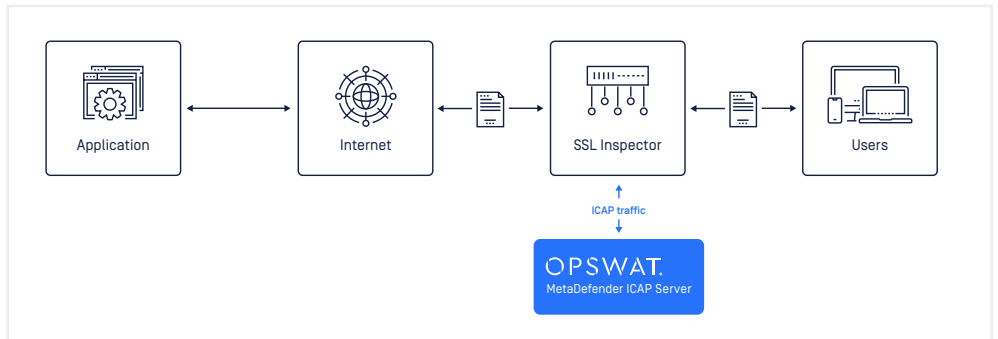
**Supports:** NGINX Plus, NGINX Open Source



### SSL Inspection

Integrate multiple security features at the point of decryption for efficient file-based threat prevention.

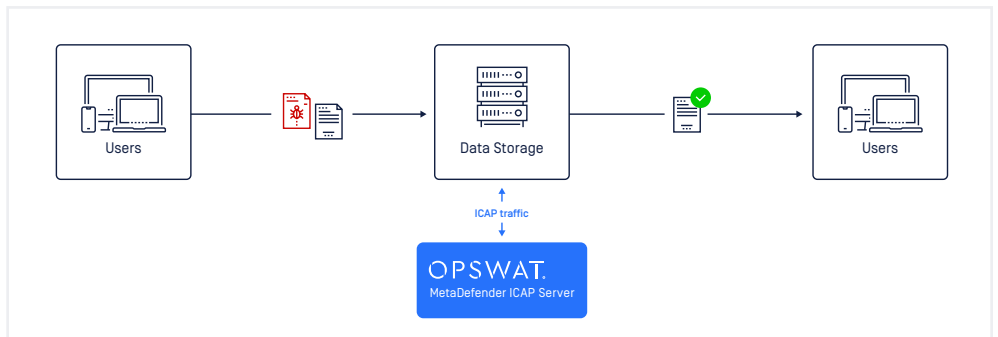
**Supports:** F5® SSL Orchestrator™, A10 Networks Thunder® SSLi®



### Managed File Transfer (MFT)

Scan all file traffic as it moves through your data repositories

**Supports:** GoAnywhere MFT, Progress MOVEit, Axway B2Bi, Axway SecureTransport



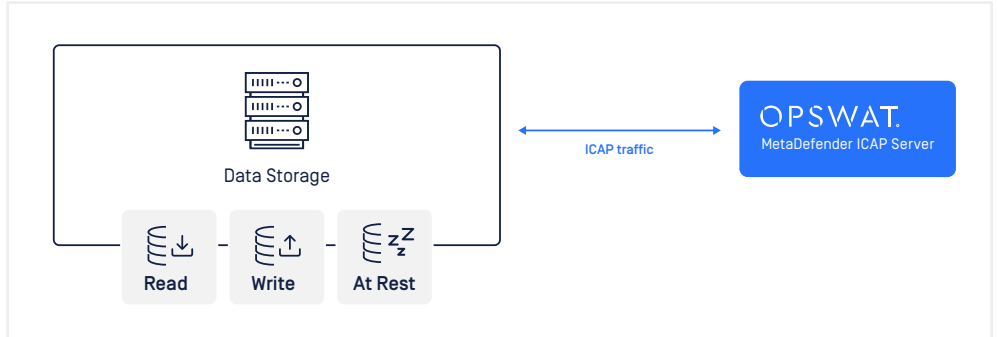
# OPSWAT.

## MetaDefender ICAP Server

### Storage Solutions

Quickly scan files in repositories on read, write, or at rest

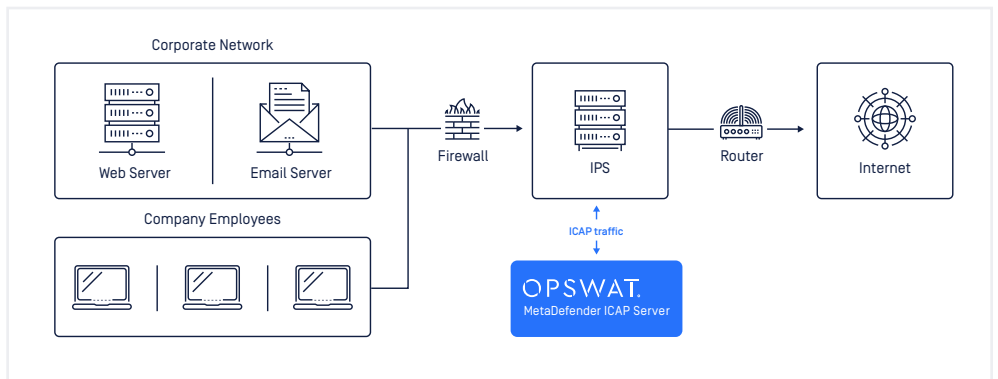
**Supports:** Dell EMC Isilon OneFS, Nutanix Files, Huawei Oceanstor



### Intrusion Prevention Systems (IPS)

Enhance the effectiveness of Intrusion Prevention/Detection Systems (IPS/IDS) by adding advanced threat prevention and vulnerability detection

**Supports:** Any IPS/IDS with ICAP client functionality



# OPSWAT.

Protecting the World's Critical Infrastructure

©2023 OPSWAT, Inc. All rights reserved. OPSWAT, MetaDefender, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT, Inc. Revised 2023-March-20

Visit [opswat.com/products/metadefender/icap](https://opswat.com/products/metadefender/icap) for more information on MetaDefender ICAP Server. Schedule a demo with a cybersecurity expert at [opswat.com/contact](https://opswat.com/contact).