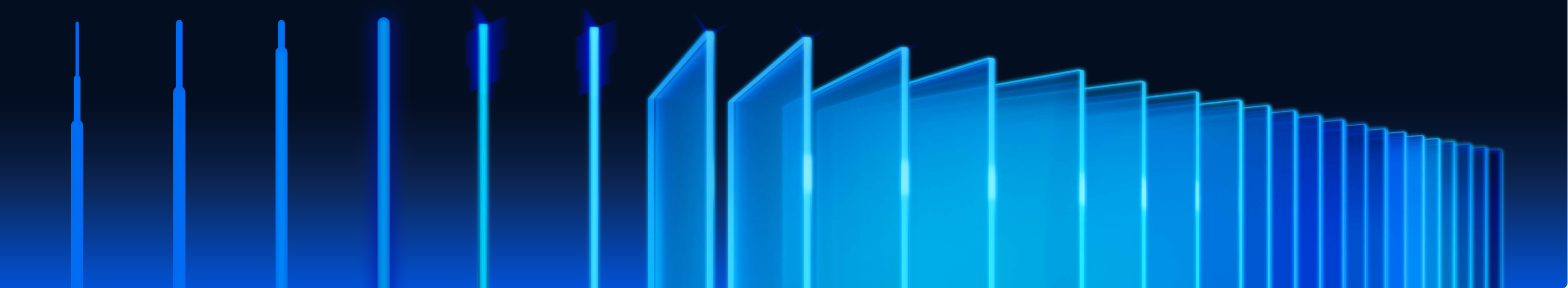


OPSWAT.

MetaDefender ICAP Server™

Secure Files at the Network Perimeter



Introduction

MetaDefender ICAP Server is designed to protect organizations against file-borne cyberattacks at the network perimeter. Comprehensive, multi-layered security technologies detect and prevent malicious files as they pass through your load balancer, WAF (web application firewall), or any other ICAP-enabled network security device.

All suspicious files traveling through your network traffic are blocked or sanitized **before** they are accessible to end users to protect against evolving cyberthreats. Sensitive data is redacted, removed, or blocked to help organizations meet stringent security compliance standards.

Table of Contents

01	Challenges
02	MetaDefender ICAP Server™
03	Comprehensive, Secure, and Efficient All-in-one Platform
04	Use Cases
05	Deployments
06	Powered by Proven, Globally Trusted, and Market-Leading Technologies
07	Integrations
08	Specifications

01

Challenges



File-Borne Malware

Malware can easily bypass a single AV (antivirus) engine and put organizations at risk. Different AV vendors have different response times to outbreaks. False positives in AV detection are common in any malware scanning solution.



Zero-Day and Advanced Evasive Malware

Malware continues to evolve and becomes more successful at evading traditional anti-malware solutions. Zero-day malware can easily defeat signature-based AV engines, which only detect known threats.



Data Breaches and Regulatory Compliance

Confidential information can be maliciously or accidentally disclosed to unauthorized parties. Data breaches are costly and damaging to an organization's reputation and business continuity.



Lack of File Security Capabilities

Network security devices like load balancers and WAFs focus on malicious network traffic and typically do not have native anti-malware capabilities, which can allow malware to slip through otherwise seemingly secure traffic.



Network Traffic Blind Spots

Traditional and advanced security measures often fall short, allowing malware to bypass AI/ML-based solutions, sandboxes, WAFs, and next-gen firewalls.



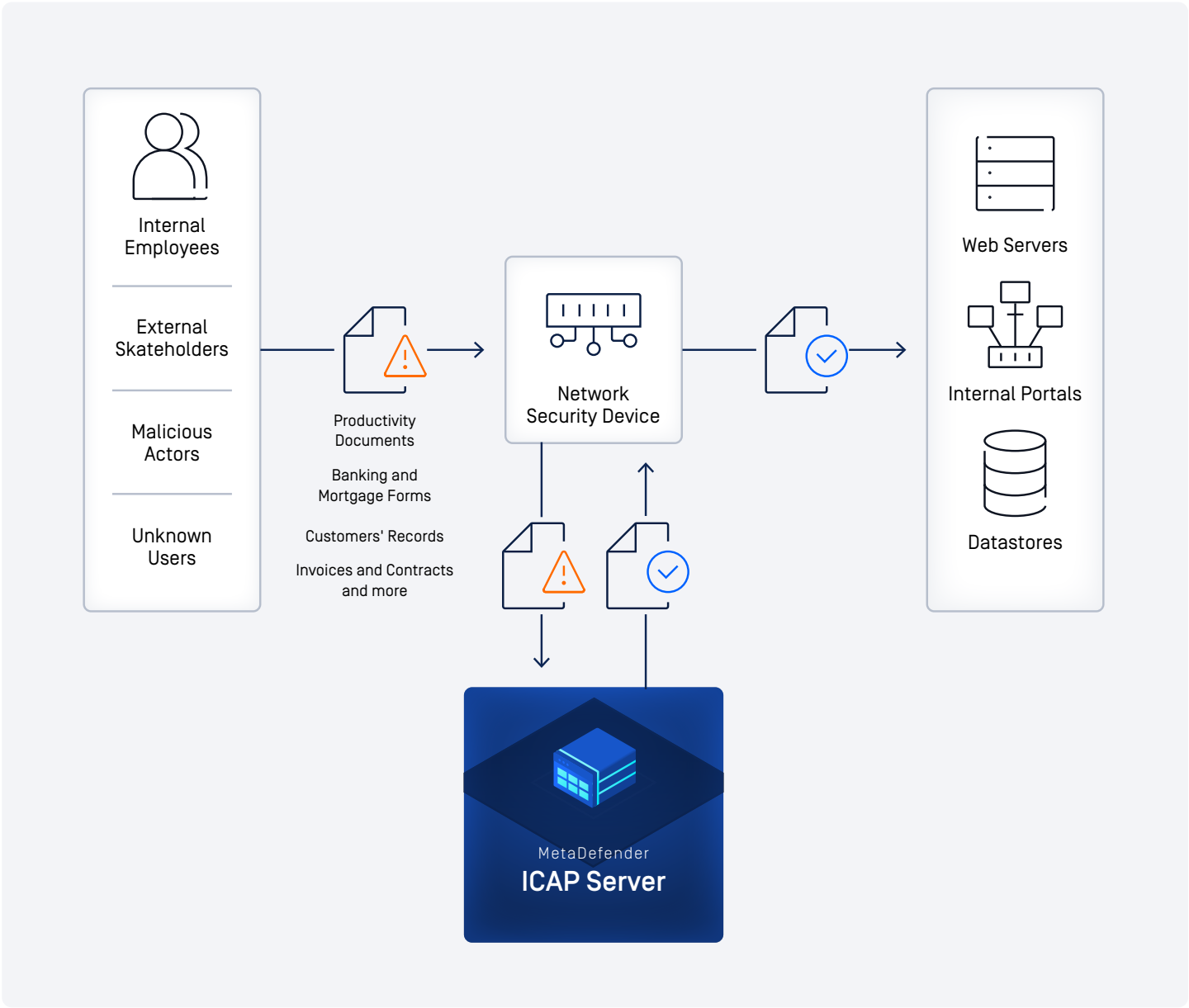
Integration Complexities

Security integration can be complex, with numerous considerations such as compatibility, complexity, cost, scalability, regulatory compliance, and time consumption.

02






MetaDefender ICAP Server™

Trust Your Network Traffic



03

Comprehensive, Secure, and Efficient All-in-one Platform

	Multi-layered File Security	Threat detection and prevention to protect web applications from malicious file uploads, zero-day attacks, sensitive data loss, and file-based vulnerabilities. Real-time multi-layered defense with OPSWAT proprietary technologies, including MetaScan®, Deep CDR™, Proactive DLP™, and our emulation-based Adaptive Sandbox.
	Compliance Adherence	OPSWAT helps organizations meet compliance regulations – such as PCI-DSS, HIPAA, GDPR, ISO 27001, and more – by preventing sensitive or out-of-policy data breaches, helping organizations avoid legal and financial penalties and maintain customer trust.
	Simple Integration	Reduce overhead with seamless integration via the lightweight ICAP (Internet Content Adaptation Protocol). With setup taking less than 10 minutes, organizations can allocate resources towards file security capabilities, so that they can focus on their core competencies and other business priorities.
	Extensive Compatibility	Wide range of integration support with OPSWAT technology partners and a multitude of network security devices, including load balancers, WAFs, next-gen firewalls, MFT (managed file transfer), ADCs (application delivery controllers), ingress controllers, reverse proxies, forward proxies, and more.
	Versatile and Scalable Deployments	Fits with all IT infrastructure with flexible deployment support for on-premises, hybrid, and cloud systems. This adaptability ensures organizations can easily scale their security solutions to meet their unique requirements, while also enabling a smooth transition between deployment models and change of business needs.

04

Use Cases

File Upload Security Protect network and application web servers by inspecting file uploads for malware and malicious content before they reach your application.	Enterprise Secure File Transfer and Storage Prevent malicious files from spreading through mass transfers of business documents across organizations or via SRA-protected connections into air-gapped environments.	Web Traffic Security and SSL Inspection Prevent malicious files from being downloaded by internal employees or users. Screen web traffic before it reaches your secure network.
---	---	---

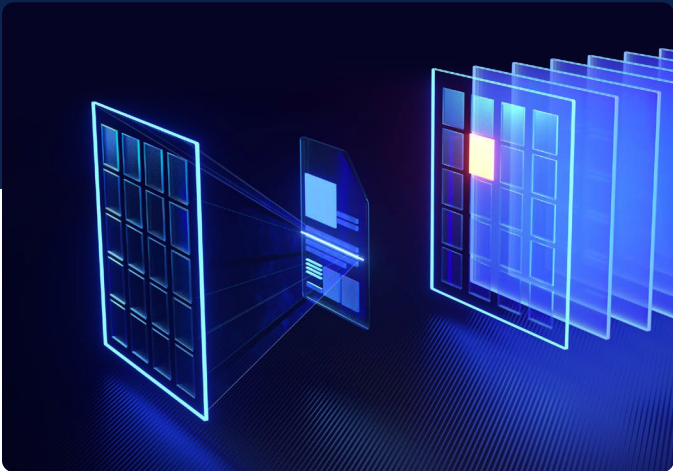
05

Deployments

Flexible deployment options across on-premises, hybrid, and SaaS IT infrastructures.

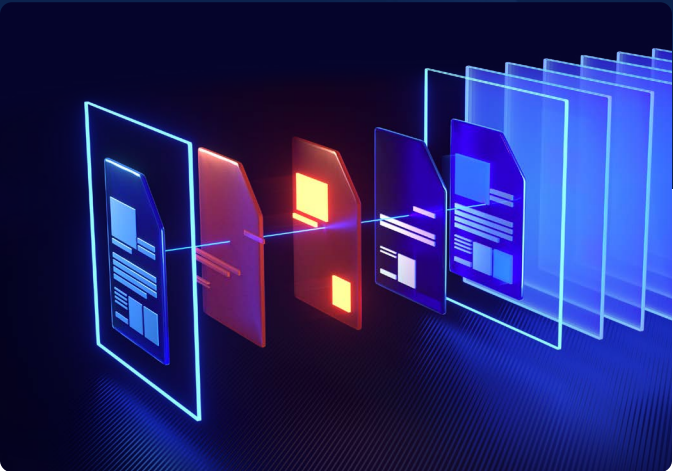
Virtual Machines On-premises	Kubernetes On-premises and Hybrid	Cloud Software as a Service (SaaS)
--	---	--

Powered by Proven,
Globally Trusted,
and Market-Leading
Technologies



MetaScan®

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



Deep CDR™

Deep CDR is the first and only CDR solution to achieve a 100% accuracy rating from SE Labs.* 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 malicious behaviors and provides 100x more resource efficiency than other sandboxes.



Proactive DLP™

Utilizes AI-powered models to locate and classify unstructured text into predefined categories, and automatically redacts identified sensitive information in files.

*recognized by SE Labs <https://info.opswat.com/report/se-labs>

07

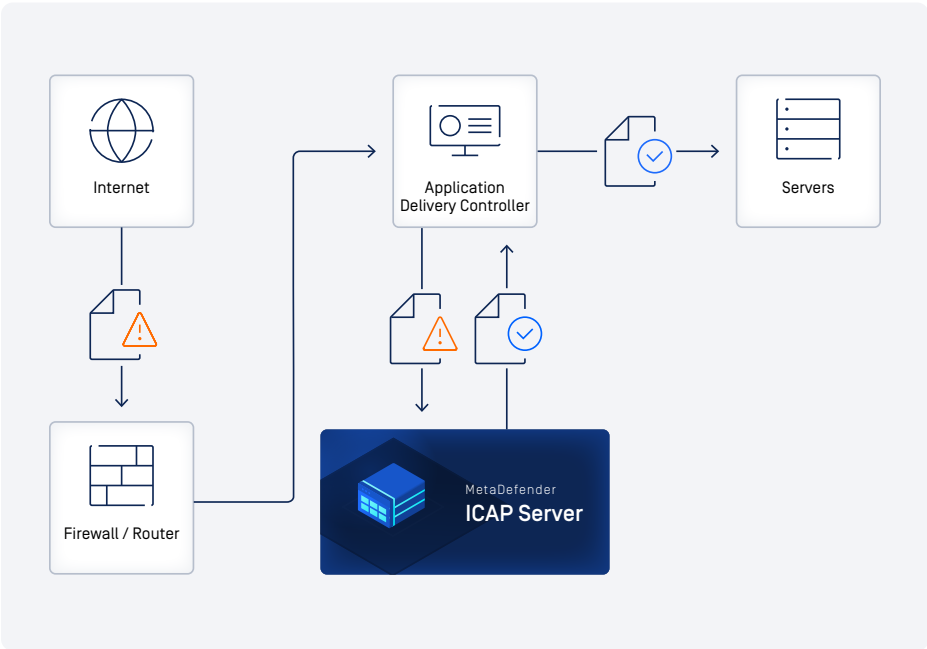
Integrations

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.

ADC (Application Delivery Controller)

Ensure web applications are optimized to run smoothly while all files uploaded through the application are secured.

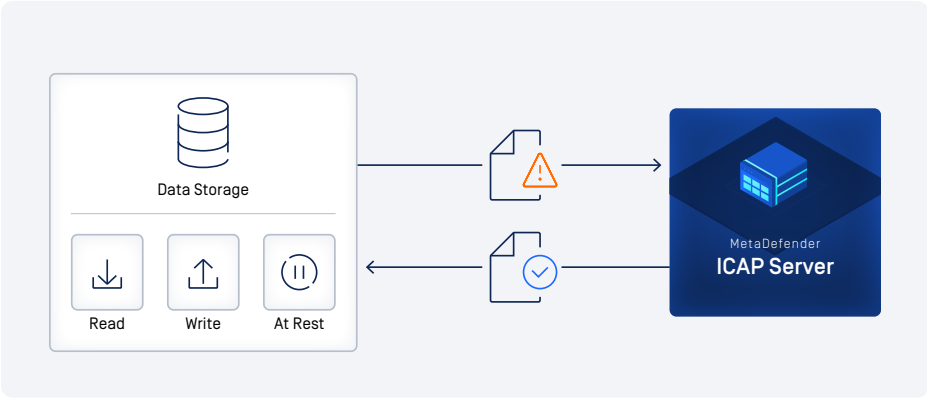
- Supports:**
- F5 BIG-IP LTM (Local Traffic Manager)
 - NetScaler ADC



Storage Solutions

Consistently scan files in repositories on read, write, or at rest to ensure the integrity and security of stored data.

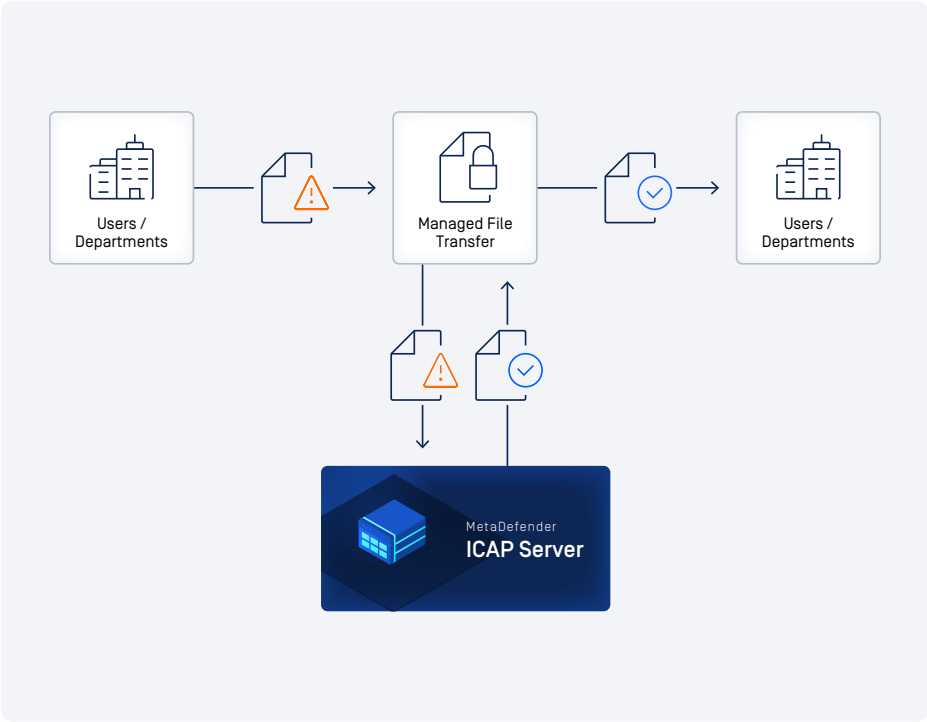
- Supports:**
- Dell EMC Isilon OneFS
 - Nutanix Files
 - Huawei Oceanstor



MFT (Managed File Transfer)

Scan all file traffic as it moves through your data repositories.

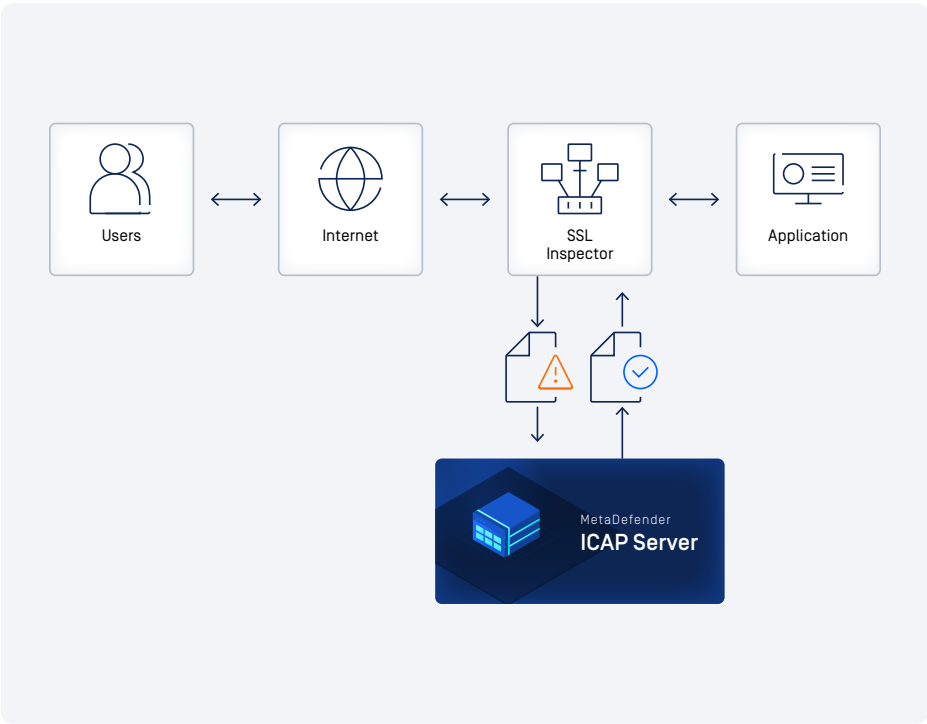
- Supports:**
- GoAnywhere MFT
 - Progress MOVEit
 - Axway B2Bi
 - GlobalScape EFT
 - FileCloud Server



SSL (Secure Sockets Layer) Inspector

Integrate MetaDefender ICAP Server at the point of decryption to ensure protection against malicious files and visibility into SSL/TLS traffic.

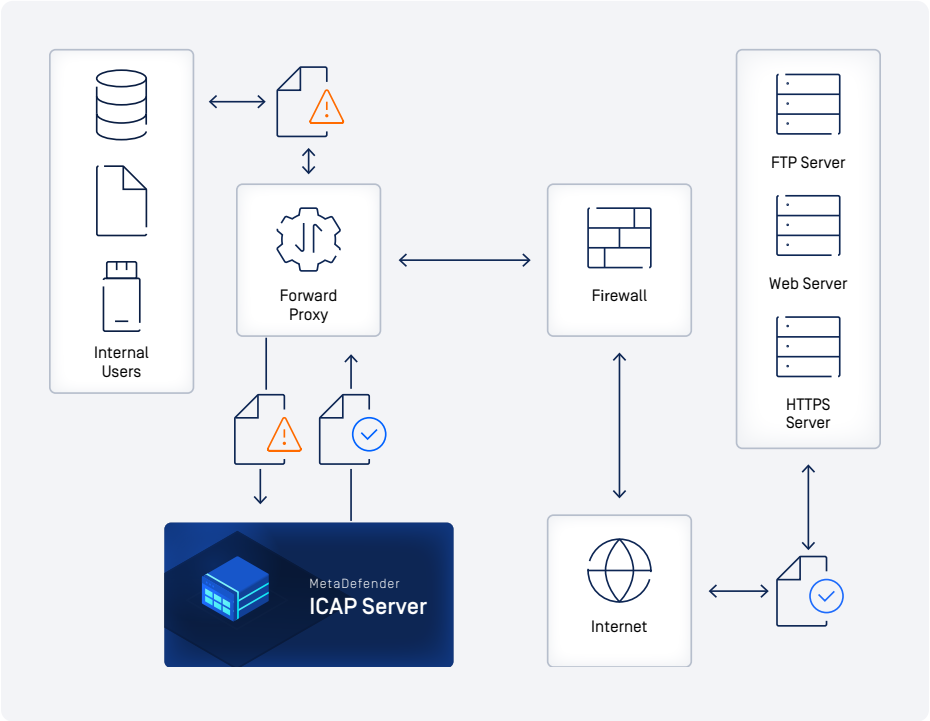
- Supports:**
- F5 BIG-IP SSL Orchestrator
 - A10 Networks Thunder SSLi



Forward Proxy

Set up any forward proxy that implements ICAP to automatically send HTTP requests to MetaDefender ICAP Server.

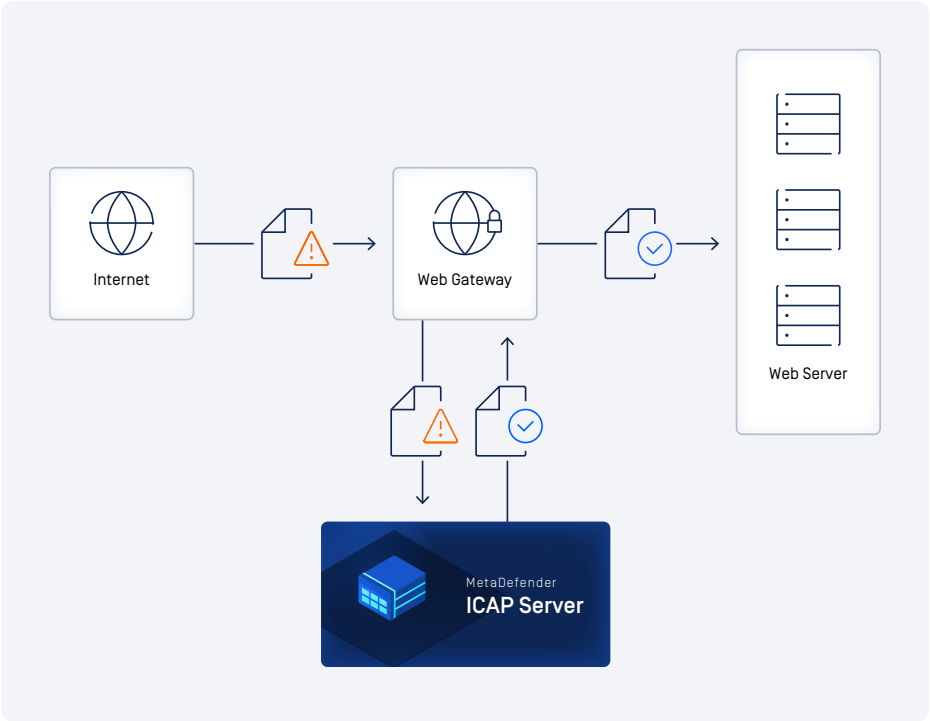
- Supports:**
- Squid Open Proxy
 - Symantec ProxySG [Blue Coat]
 - Forcepoint



Web Gateways

Screen file content in web traffic before it reaches secured networks.

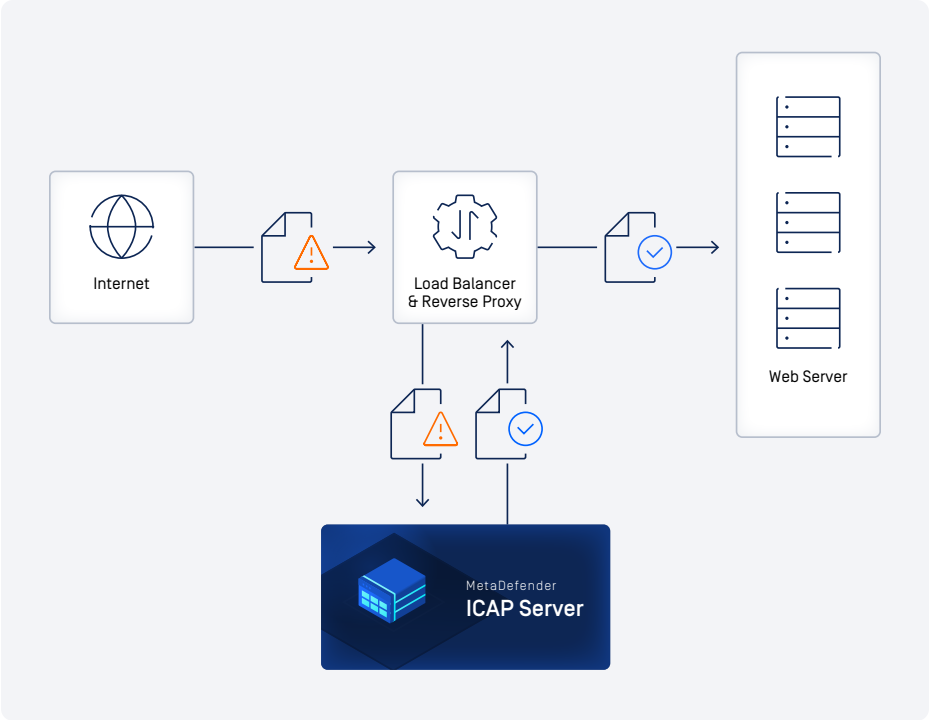
- Supports:**
- ARA Networks JAGUAR5000
 - McAfee Web Gateway
 - Symantec ProxySG [Blue Coat]
 - Squid Web Gateway
 - Forcepoint Secure Web Gateway
 - Airlock Secure Access Hub Gateway
 - Cyolo Secure Remote Access [SRA]



Reverse Proxy and Load Balancer

Set up any reverse proxy or load balancer to automatically forward any uploaded files to MetaDefender ICAP Server.

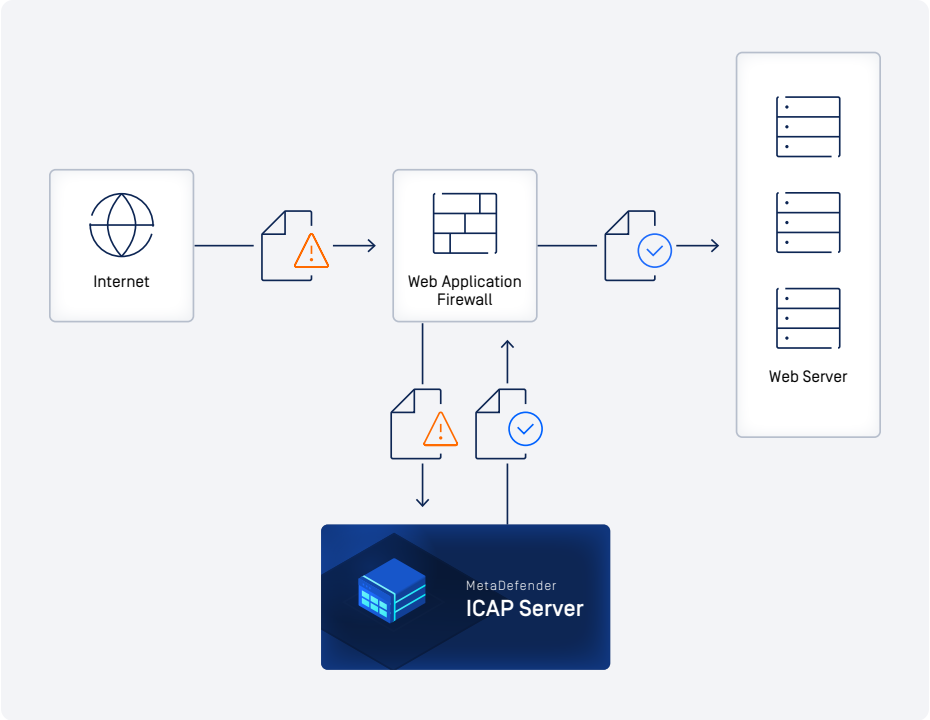
- Supports:**
- F5 BIG-IP Local Traffic Manager [LTM]
 - NGINX Plus
 - Symantec ProxySG [Blue Coat]
 - Squid Web Gateway



WAF [Web Application Firewall]

Strengthen defense mechanisms against cyber threats by combining the threat prevention capabilities of both MetaDefender ICAP Server with a WAF.

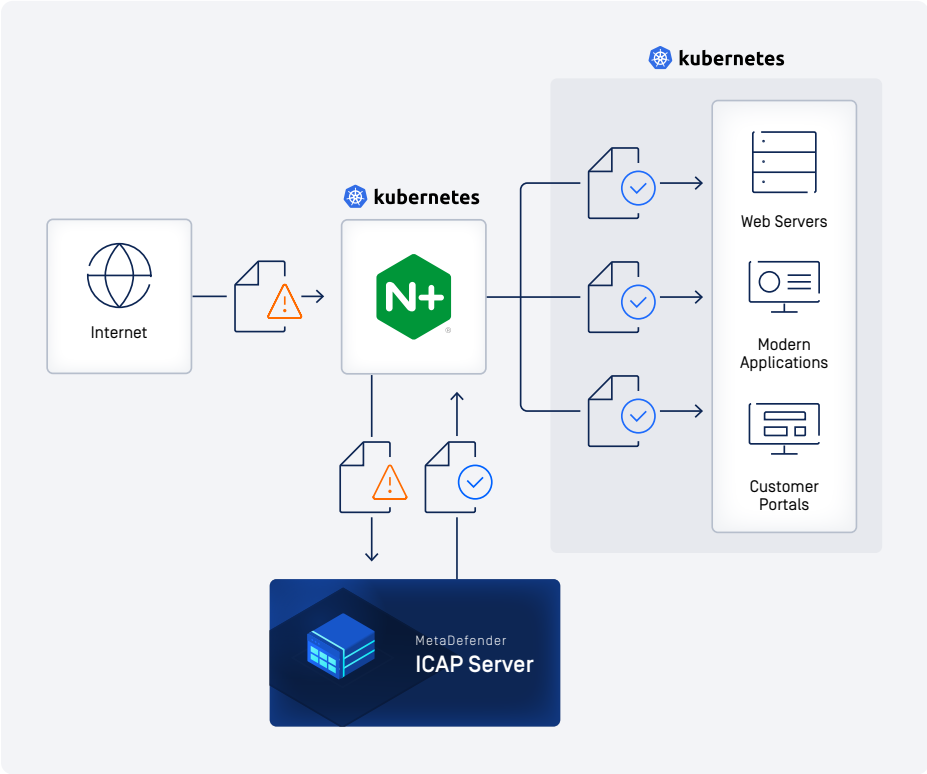
- Supports:**
- F5 BIG-IP AFM [Advanced Firewall Manager]
 - F5 BIG-IP ASM [Application Security Manager]
 - NGINX App Protect
 - Fortinet Fortigate NGFW [Next Generation Firewall]
 - Vmware Avi Vantage



Ingress Controller

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

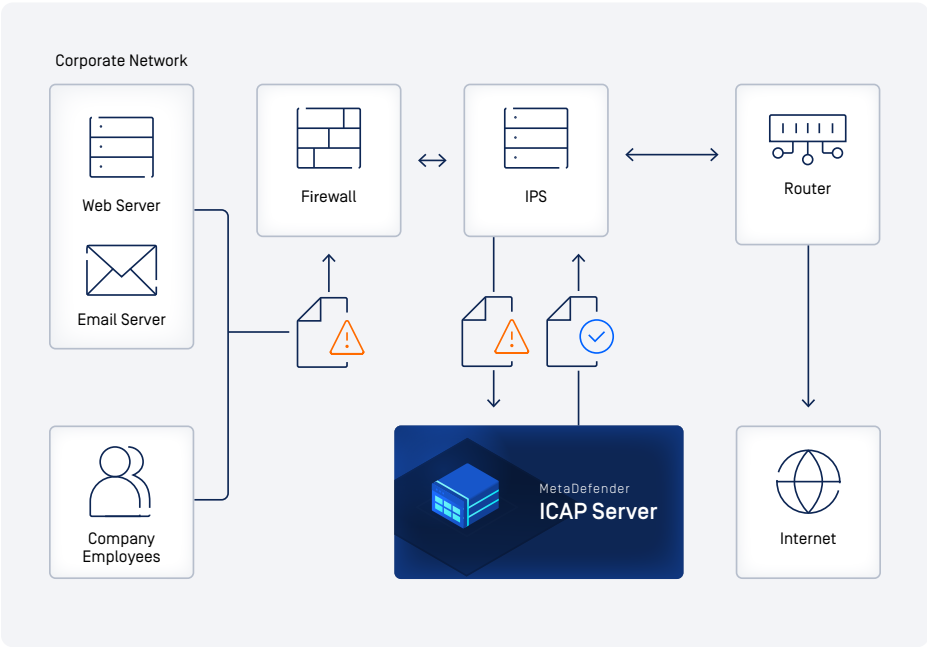
- Supports:**
- NGINX Plus
 - NGINX Open Source



IPS (Intrusion Prevention Systems)

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



08

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

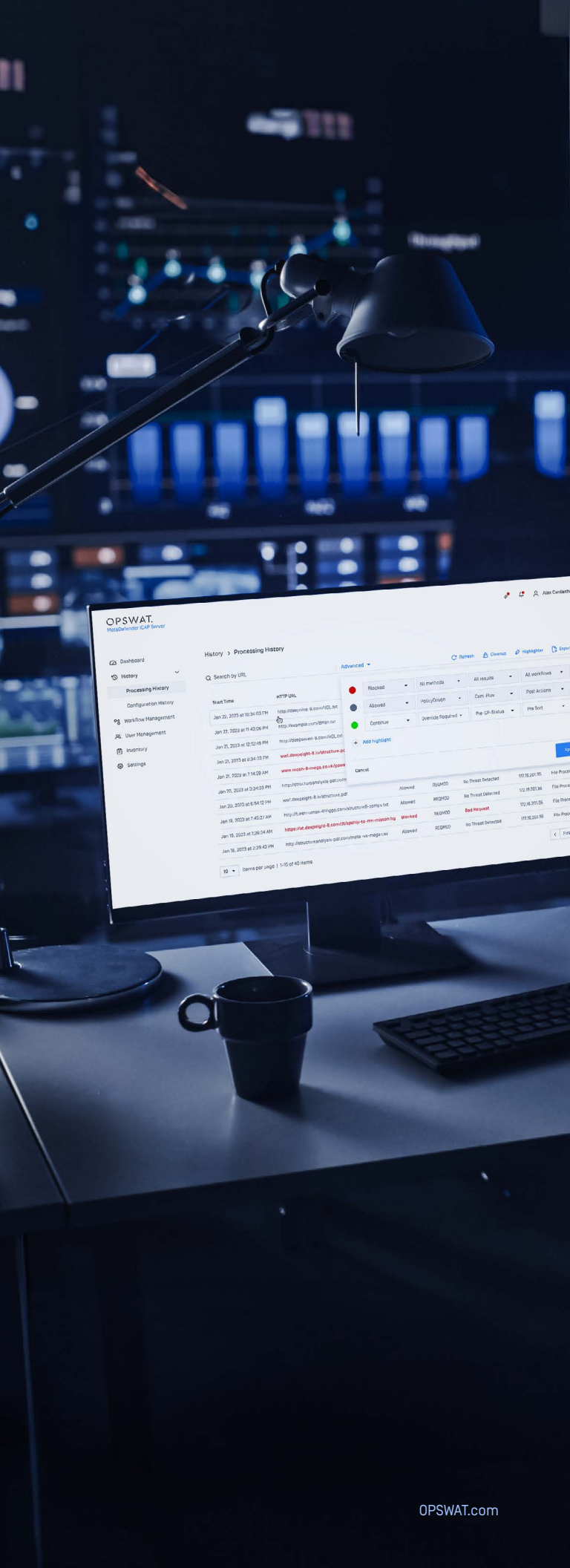
Chrome, Firefox, Safari, Microsoft Edge

Ports

Inbound	1344 (ICAP), 8048 (Web Management Console and REST interface), 8043 & 8443 (NGINX)
Outbound	8008 (only if MetaDefender Core is 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)



GET STARTED

Are you ready to put MetaDefender ICAP Server™ on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:

opswat.com/get-started

sales@opswat.com



OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and

device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.