

OPSWAT.

# MetaDefender ICAP Server<sup>TM</sup> Deployments Guide





MetaDefender ICAP Server is a plug-and-play solution that protects organizations against file-borne attacks at the network perimeter. Multi-layered security technologies detect and prevent malicious files as they traverse through your load balancer, WAF (web application firewall), or any other ICAP-enabled network security device.

As a result, suspicious files traveling through your network traffic are automatically blocked or sanitized before they reach your end users. Sensitive data is redacted, removed, or blocked to help organizations meet data protection and security compliance standards.

# Table of Contents

- 01 Overview
- 02 Usage Scenarios
- 03 Explore Deployment Options
- 04 Design the Right Deployment Strategy
- 05 Selection Guidelines
- 06 Resources

# 01

## Overview

Every enterprise IT infrastructure is unique, with distinct underlying architectures and varying security and compliance needs. This diversity in design and implementation influences the method of integrating new software into your existing systems.

To address these varied requirements, MetaDefender ICAP Server offers flexible deployment options which work for businesses of all sizes and industries. Whether you seek on-premises control, hybrid flexibility, or the simplicity of cloud infrastructure, our solutions are easy to manage, offering advanced security without compromising performance.

MetaDefender ICAP Server offers various deployment options for your organization’s specific security demands:

### On-Premises

In this model, organizations can seamlessly integrate MetaDefender ICAP Server software with their existing data systems using VMs or physical hardware. This provides complete control over the infrastructure and data handling.

### Cloud

In a SaaS model, MetaDefender ICAP Server instances and all file scanning processes happen in the cloud, managed by OPSWAT. This deployment method requires less setup time and fewer local resources, which helps organizations reduce operating expenses.

### Hybrid

This model combines both on-premises and cloud deployments, where certain components of MetaDefender ICAP Server are managed by the organization while others are managed in the cloud by OPSWAT. This integration allows for flexibility in operations and resource management.

# 02

## Usage Scenarios

### Challenges

Consider MetaDefender ICAP Server if your organization has one or more of these concerns:

- 1

You have a web application portal that receives file uploads, which can be a major attack vector for malware, ransomware, and data theft.
- 2

Traditional solutions (such as WAFs) may not prevent file-borne malware for web traffic security or offer adequate file content inspection.
- 3

Managing the security of file transfers and stored files can be challenging in complex file storage systems.
- 4

Integrating new technology into your existing IT infrastructure introduces compatibility and security challenges, while increasing costs and time to implement.

### Solution

MetaDefender ICAP Server (on-premises and cloud) protects network and application servers by inspecting files for embedded threats before they reach your systems.

### Example

Integrate MetaDefender ICAP Server to an existing load balancer, WAF, or any ICAP-enabled network security device. This helps secure your business data and prevents compromised servers from distributing malware or being exploited for zero-day and ransomware attacks.

### What’s in It for Customers?

Scalable protection for file uploads ensures business continuity and data integrity without the need for extensive overhead implementation.

### Industries at Risk

Public sector and government, banking and financial services, insurance and healthcare providers, and more.


03


# Explore Deployment Options


Regardless of the deployment model chosen, you can still benefit from the same advanced threat prevention capabilities from MetaDefender ICAP Server.


Files are transferred from the internet, passed through a network security device (such as a load balancer, WAF, or MFT), and routed to MetaDefender ICAP Server. Based on your deployment and configuration setup, these files are either directed to MetaDefender Core (on-premises) or MetaDefender Cloud to be analyzed, sanitized, or blocked, before being securely returned to your corporate environment.


All deployments are secured by our suite of MetaDefender technologies.

- 

MetaScan™ Multiscanning
- 

Deep CDR™
- 

Adaptive Sandbox
- 

Proactive DLP™
- 

Country of Origin

| Capabilities                                | On-Premises | Hybrid | Cloud |
|---|-------------|--------|-------|
| VMs (Virtual Machines)                      | ✓           |        |       |
| Locally Hosted                              | ✓           |        |       |
| Workload Isolation                          | ✓           |        |       |
| Full Customization                          | ✓           |        |       |
| Back End Flexibility: Cloud and On-Premises | ✓           | ✓      |       |
| Kubernetes-Based                            | ✓           | ✓      |       |
| Containerized Workloads                     | ✓           | ✓      |       |
| Scalable and Automated                      | ✓           | ✓      |       |
| Flexible Architecture                       | ✓           | ✓      |       |
| High Availability                           | ✓           | ✓      | ✓     |
| Saas (Software-As-A-Service)                |             |        | ✓     |
| Cost Efficient                              |             |        | ✓     |
| Subscription-Based                          |             |        | ✓     |
| Reduced Operational Overhead                |             |        | ✓     |
| Dynamic Scaling                             |             |        | ✓     |



On-Premises Deployment via VMs [Virtual Machines]

For Organizations with Traditional IT Infrastructure

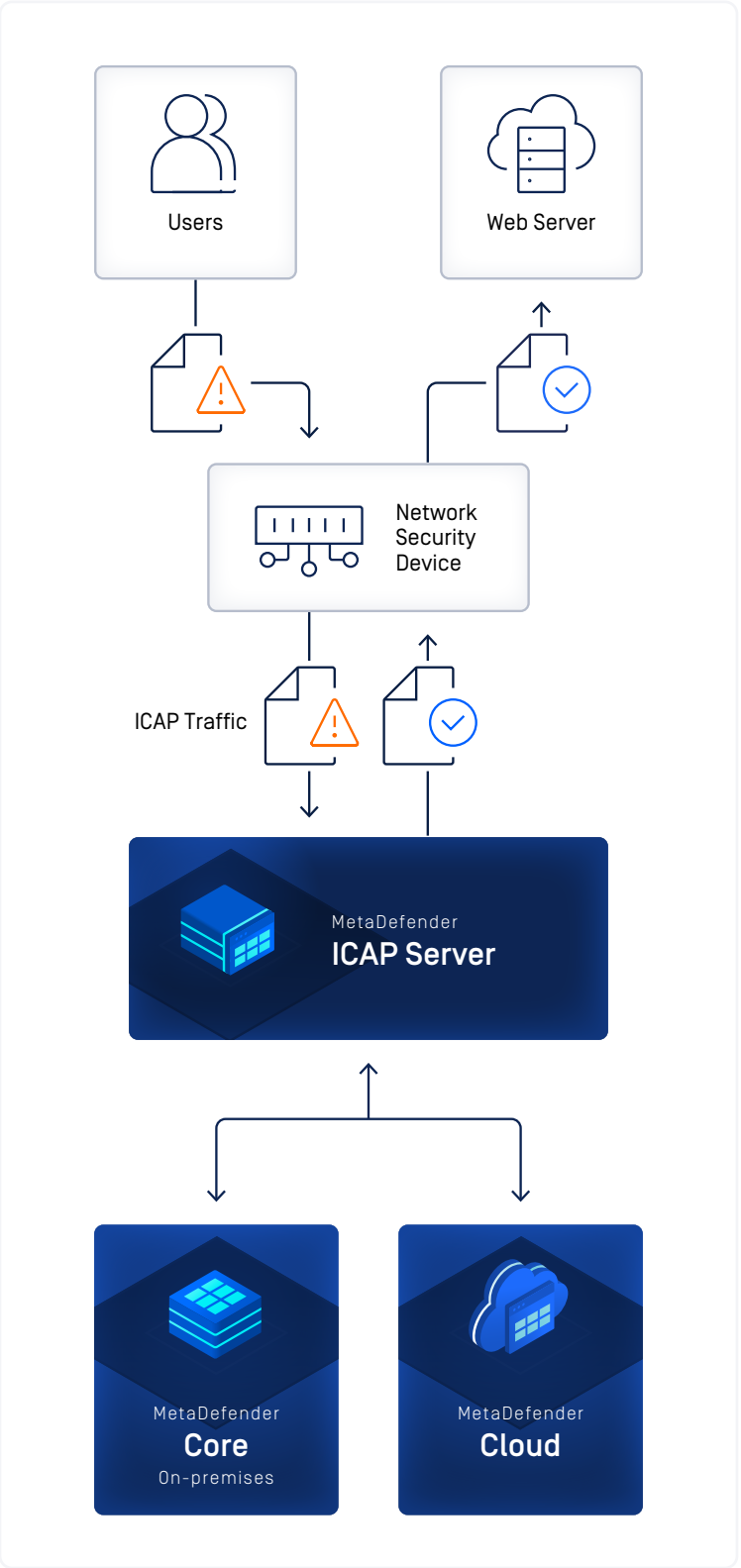
For organizations with traditional IT setups that need to virtualize existing physical servers, or applications that are not easily containerized, on-premises deployment through virtual machines is an ideal solution.

Customers have the flexibility to run multiple MetaDefender ICAP Server instances on the same hardware. This allows users to enable better resource control, strengthen security through network and data isolation, and customize security protocols to meet the unique demands of their network and data flow.

This option is particularly suitable for environments with a need for security transparency or with strict data protection requirements. Sensitive data can be processed locally, which helps reduce latency and strengthens compliance with industry regulations.

Key Features

- High level of control over infrastructure and data.
- Fulfills certain aspects of data sovereignty and compliance requirements.
- Reduced latency through local data processing.
- Capability to run legacy applications or custom OS environments.
- Customizability to align with organizations' specific operational requirements.



Cloud Deployment via SaaS

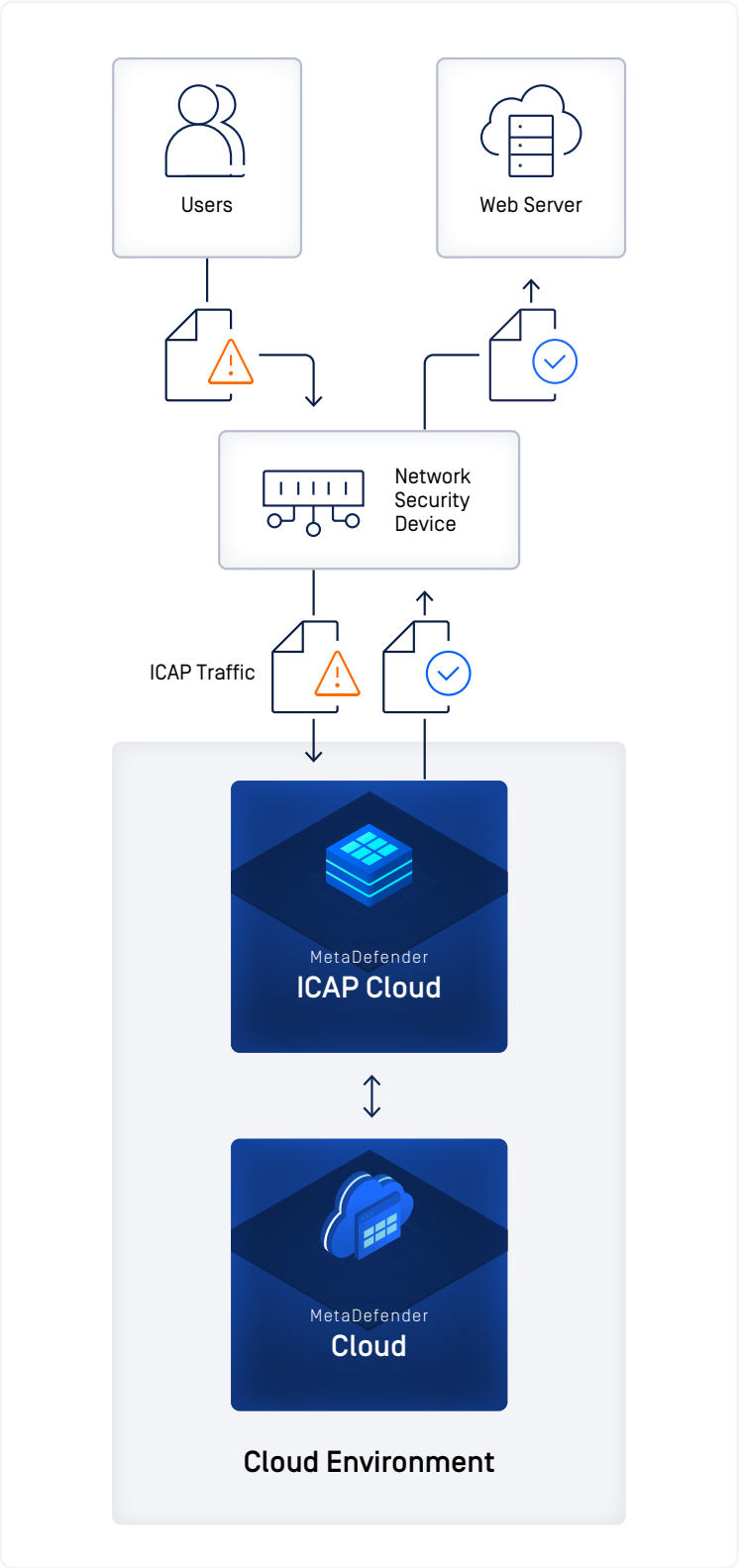
For Small-to-Medium Businesses and Organizations Shifting to Cloud-Native Solutions

Cloud deployment of MetaDefender ICAP Server is ideal for organizations looking for a fully managed, cost-effective security solution. This option eliminates the need for complex infrastructure management while implementing robust security measures, so that businesses can focus on their core competencies.

With SaaS deployment, businesses can reduce overhead costs associated with maintaining hardware. Because the infrastructure is managed in the cloud by OPSWAT, this option comes with capabilities such as automatic updates, disaster recovery, and global accessibility. This model is ideal for organizations with limited IT resources, as it provides rapid deployment for faster time to value and minimizes operating expenses.

Key Features

- Instant access to security services with minimal configuration.
- Reduced infrastructure overhead and IT management burdens.
- High availability, disaster recovery, and automatic updates.
- Cost-effective solution, especially for small-to-medium businesses and global collaboration.
- Regional Coverage: Deployments in EU, USA, Canada, Australia, and APAC.



On-Premises and Hybrid Deployment via Kubernetes

For Enterprises with Modern Architecture and Distributed Workloads

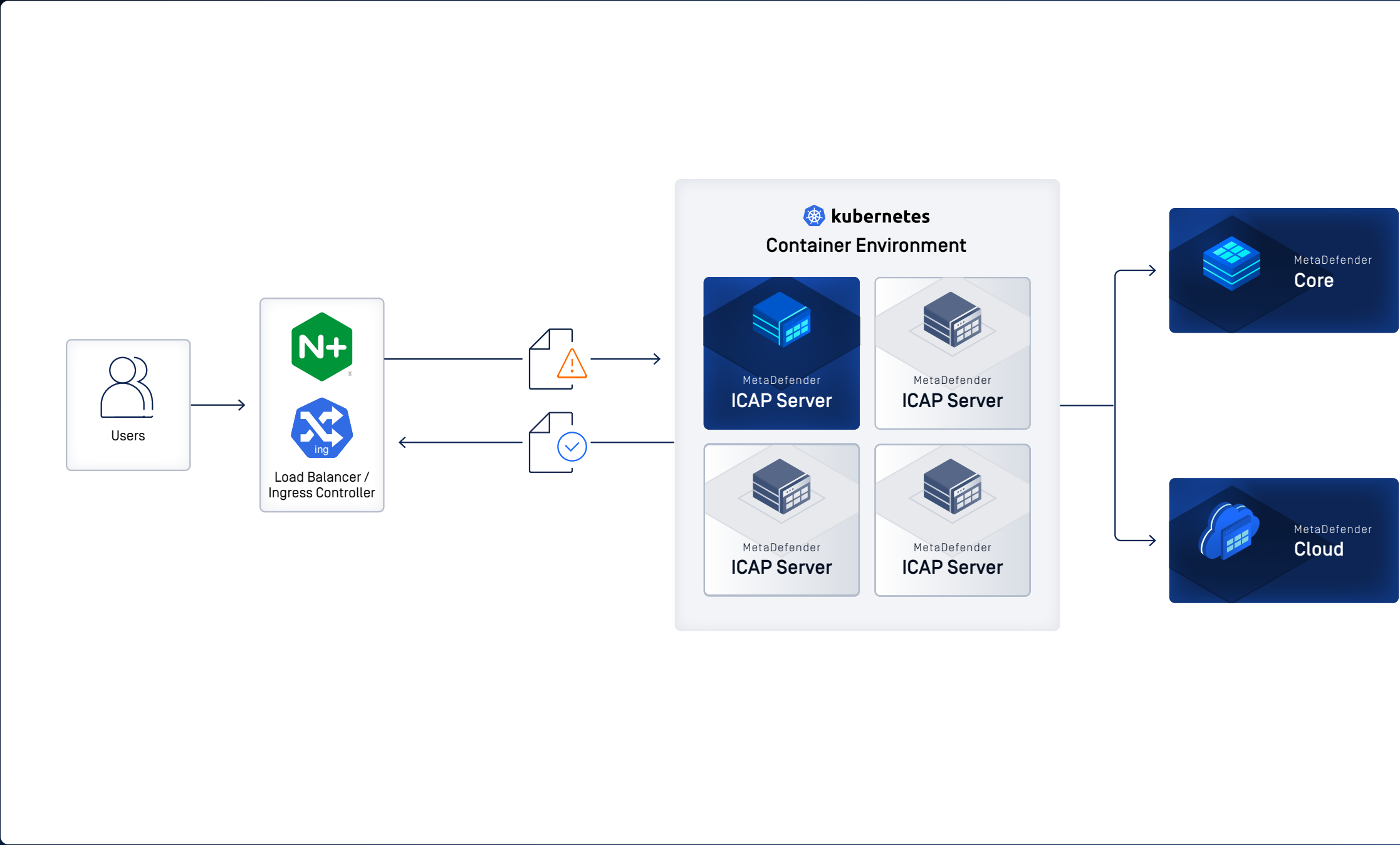
Kubernetes allows dynamic scaling of security services to match the needs of your microservices architecture. For organizations that are managing distributed microservices or are looking to modernize their applications, Kubernetes deployment is a highly scalable and flexible solution.

In this model, MetaDefender ICAP Server instances can be deployed as containerized applications across various cloud platforms or hybrid environments. The benefits of containers provide the added benefits of high availability, horizontal scalability, and automation.

MetaDefender ICAP Server supports deployment on major container orchestration platforms, including AWS EKS (Elastic Kubernetes Service), AKS (Azure Kubernetes Service), and GKE (Google Kubernetes Engine), ensuring compatibility with leading cloud environments.

Key Features

- High availability and scalability for modern distributed architectures.
- Seamless integration with AWS EKS, AKS, and GKE.
- Automation capabilities for efficient workload management.
- Ideal for businesses with containerized applications requiring flexibility.
- Self-healing, as Kubernetes provides disaster recovery mechanisms to ensure reliable file scanning uptime.



04

# Design the Right Deployment Strategy

Choosing the right deployment model for MetaDefender ICAP Server depends on your organization's infrastructure, compliance requirements, and operational goals.

Each deployment model—whether on-premises, hybrid, or cloud—offers its own distinct advantages, from full control over data to ease of use and scalability. Customers may also determine their level of ownership and management of MetaDefender ICAP Server deployments. This means they may opt for full management and ownership, or offload partial or full management responsibilities to OPSWAT, depending on their needs.

By understanding your business's specific needs, you can select the deployment model that best aligns with your security strategy and long-term objectives. Incorporating internal stakeholders early in the decision making process (including IT, security, and compliance teams) is crucial to ensure successful deployment and seamless integration with your existing systems.

|                        | On-Premises  | Hybrid  | Cloud  |
|------------------------|--|---|--|
| Environment            | Virtual Machines   | Containers via Kubernetes   | Software-as-a-Service  |
| Ideal for              | Organizations prioritizing full control over infrastructure and data   | Enterprises managing containerized workloads and complex distributed systems  | Small-to-medium businesses or those with limited IT resources  |
| Key Features           | <ul style="list-style-type: none"><li>• Data compliance</li><li>• Reduced latency</li><li>• Full control</li><li>• Customization</li></ul>   | <ul style="list-style-type: none"><li>• High availability</li><li>• Scalability</li><li>• Automation</li><li>• Flexible architecture</li></ul>  | <ul style="list-style-type: none"><li>• Ease of use and maintenance</li><li>• High availability</li><li>• Cost efficiency</li></ul>  |
| Technical Benefits     | <ul style="list-style-type: none"><li>• Direct management of hardware resources.</li><li>• Complete isolation of workloads.</li><li>• Ideal for sensitive data storage and regulated industries.</li></ul> | <ul style="list-style-type: none"><li>• Orchestrates containerized MetaDefender ICAP Server instances</li><li>• Self-healing and auto-scaling features for resilience</li><li>• Ideal for microservices and CI/CD pipelines</li></ul> | <ul style="list-style-type: none"><li>• Reduces operational overhead with automatic scaling and updates</li><li>• Accessible from anywhere with internet connectivity</li><li>• Subscription-based pricing for cost predictability</li></ul> |
| MetaDefender Offerings | MetaDefender ICAP Server (on-premises) + MetaDefender Core (on-premises)<br><br>#2 (cloud backend): MetaDefender ICAP Server (on-premises) + MetaDefender Cloud  | #1: MetaDefender ICAP Server + Kubernetes + MetaDefender Core (on-premises)<br><br>#2 (cloud backend): MetaDefender ICAP Server + Kubernetes + MetaDefender Cloud   | MetaDefender ICAP Cloud + MetaDefender Cloud   |

# 05

## Selection Guidelines

Cloud (SaaS) is recommended if you need:

- ❑ Less than 100,000 file scans per day
- ❑ Rapid deployment with minimal setup
- ❑ Global collaboration capabilities
- ❑ Built-in disaster recovery features
- ❑ Whether you decide to host our file security solution on-premises or in SaaS, we can help you meet your specific needs for security and compliance.

On-Premises is recommended if you need:

- ❑ High file volumes (more than 100,000 scans per day)
- ❑ Data sovereignty and strict control over your infrastructure
- ❑ Cost-efficient scanning for large files

# 06

## Resources

[Deployments Webpage](#)

[Use Case](#)

[MetaDefender ICAP Server Webpage](#)

- [Brochure](#)
- [Datasheet](#)

[MetaDefender ICAP Cloud Webpage](#)

- [Datasheet](#)



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](https://opswat.com/get-started)

[sales@opswat.com](mailto: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](https://www.opswat.com).