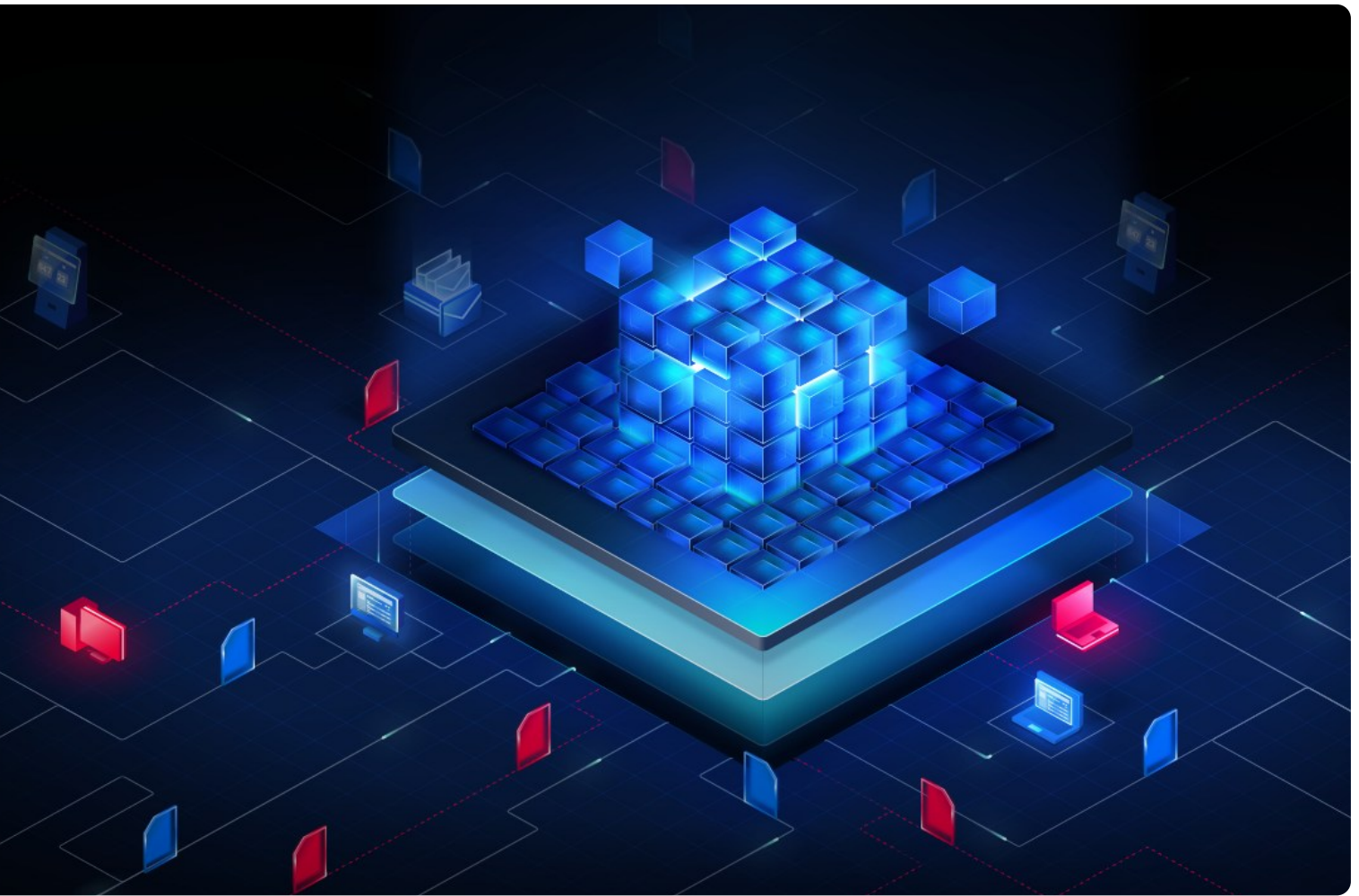




Deployment Options

MetaDefender™ Core: Understanding Deployment Options

MetaDefender Core at a Glance

MetaDefender Core is an advanced threat detection and prevention platform that proactively analyzes, detects and neutralizes file-borne threats before they can breach your security perimeter.

What It Does

- Scans files using 30+ commercial anti-malware engines simultaneously.
- Sanitizes and reconstructs files using CDR (Content Disarm and Reconstruction) to neutralize embedded threats.
- Leverages AI and machine learning to optimize threat detection and prevention engines for faster, smarter, and more adaptive protection.
- Detects, redacts, and anonymizes sensitive data, aiding compliance and enforcing data handling policies.
- Integrates easily with existing IT and OT systems through APIs, ICAP, and SDKs, adapting to complex infrastructure without disrupting operations.

01

Overview: Deployment Challenges

Securing file-based threats is only part of the challenge. Getting a file security platform deployed, scaled, and maintained across complex, mixed infrastructure is where organizations most often struggle.

- **Diverse Infrastructure:** From air-gapped on-premises environments to multi-cloud architectures, no two organizations look the same. Security tools must adapt to the infrastructure, not the other way around.
- **Data Residency and Compliance:** Regulations dictate where data can reside and how it must be processed. Many organizations cannot allow files to leave their perimeter under any circumstances.
- **High Throughput Demands:** Elastic, high-performance scanning with no single point of failure is non-negotiable for critical environments. A bottleneck at the file inspection layer creates downstream risk.
- **Limited IT Resources:** Mid-market and resource-constrained organizations need security that deploys fast and manages itself, not tools that require a dedicated team to operate.

MetaDefender Core addresses these challenges by offering multiple flexible deployment options, giving every customer a path to deploy advanced threat prevention exactly where and how they need it.

02

Explore the Options

MetaDefender Core supports various deployment categories. MetaDefender Cluster extends MetaDefender Core with a scalable, disruption-resistant architecture that distributes workloads, accelerates processing, and centralizes control across environments.

Virtual Machines [VM] On-Premises · IaaS	Containers On-Premises · IaaS	SaaS Fully Managed · Zero Ops
Run MetaDefender on any cloud or on-premises VM. Scale from a single node to elastic Auto Scaling Groups without changing your workflow. • Single Instance • Multiple Instances • Auto Scaling Group • MetaDefender Cluster	Helm-based deployment across every major K8s flavor, cloud-managed or self-hosted. One chart, any cluster. • Amazon EKS • Azure AKS • Google GKE • Red Hat OpenShift • K8s Local Cluster • Docker Swarm • MetaDefender Core Container • MetaDefender Cluster	Flexible managed deployment options that scale with your needs, with minimal setup and no infrastructure overhead. • MetaDefender Cloud

MetaDefender Cluster: Resilient, High-Throughput File Security for Enterprises

MetaDefender Cluster enables enterprise-grade scalability and resilience for MetaDefender Core. With distributed architecture, parallel file processing, and centralized orchestration, it supports high-throughput scanning environments while ensuring uptime and operational control. Ideal for organizations that need to process large volumes of content with performance and confidence.

03

Deployment Comparison

Choose the model that matches your security posture, operational maturity, and infrastructure strategy.

	Virtual Machines	Containers	SaaS
Infrastructure Control	Full control	High control	Managed by OPSWAT
Setup Complexity	High	≈ Medium	Minimal
Time to Deploy	Hours to days	≈ Minutes to hours	Fast, minimal setup
Elastic Scaling	≈ Manual / ASG [Auto Scaling Group]	Auto Scaling / HPA [Horizontal Pod Autoscaler]	Automatic
Self-Healing	Not native	Native pod restart	Platform-managed
Air-gap / Offline Support	Fully supported	Fully supported	Requires connectivity
Ops and Maintenance	Customer-managed	Customer-managed	Fully managed
Engine / Signature Updates	≈ Manual / scheduled	≈ Manual / scheduled	Continuous automatic
Data Residency	Customer-controlled	Customer-controlled	≈ Depends on plan
Best For	High-security, regulated, air-gapped environments	Cloud-native teams, CI/CD pipelines, DevSecOps	Fast integration, low operation overhead, SaaS-first organizations

04

How to Find the Right Deployment Option

Use this table during customer conversations to match their environment and priorities to the right deployment model.

Deployment Option	Environment	Ideal For	Key Benefits
Virtual Machines	- On-Premises - IaaS	Organizations requiring full infrastructure control, data residency, or air-gapped environments	- Full control over infrastructure and data - Air-gap and offline deployment ready - Terraform templates included - Horizontal scale with Auto Scaling Group
Containers	- On-Premises - IaaS	Enterprises managing containerized workloads and complex distributed systems	- Horizontal scaling and auto-scaling - Self-healing with native pod restart - Automated rollouts and rollbacks - Ideal for microservices and CI/CD pipelines
MetaDefender Cluster	- On-Premises - IaaS - Kubernetes	Enterprises requiring continuous high-volume file inspection with zero downtime and built-in redundancy	- Horizontal scaling via additional MetaDefender Core instances for high-throughput peaks - Automated failover mechanisms avoiding single points of failure - Parallel archive file processing - Unified monitoring and management across worker nodes

Deployment Option	Environment	Ideal For	Key Benefits
MetaDefender Cloud	SaaS	Organizations with limited IT resources wanting fast, low-overhead deployment	• Zero infrastructure overhead, OPSWAT manages everything • Start processing files within minutes • Continuous engine and signature updates • Global availability and built-in redundancy
Cloud Images	IaaS	Teams who want to spin up MetaDefender Core fast to test capabilities or run a PoC first before hardening it into a production-ready deployment.	• Available on AWS, Microsoft Azure, and GCP Marketplace. Launch in your existing cloud environment in minutes • Pre-configured quick-start image gets you from zero to a working instance without manual install steps • Serves as a baseline you can harden and scale for production once validated

05

Discovery Questions

Walk through these questions with the customer. Follow the Yes path to reach a recommended deployment. Multiple Yes answers pointing to the same option strengthen the recommendation.

Discovery Question	If Yes	If No
Security and Data Control		
Does the customer require all file data to stay within their own network perimeter?	→ Recommend: Virtual Machine or Container Data never leaves the customer environment. Fully air-gappable. No cloud dependency	Continue to next question ↓
Can the customer operate in an air-gapped or fully offline environment?	→ Recommend: Virtual Machine or Container or MetaDefender Cluster Both VM and Container deployments are designed to operate fully offline. MetaDefender Cluster is also fully air-gap compatible and adds high availability within the isolated environment, which is often critical in defense and government deployments where uptime requirements are strict.	Continue to next question ↓
Is the customer integrating MetaDefender Core with existing ICAP, or SIEM tools?	→ Recommend: Virtual Machine or Container Both integrate natively via ICAP and REST API. VM is often simpler for legacy infrastructure.	
Do MetaDefender Core deployment options support compliance needs?	Yes, MetaDefender Core provides audit logs, monitoring, and reliable workflows that support enterprise compliance standards. MetaDefender Cluster additionally provides unified audit logging across all worker nodes, consolidated through the Cluster Control Center.	

Discovery Question	If Yes	If No
Infrastructure and Architecture		
Is the customer running Kubernetes or Docker containerized workloads?	→ Recommend: Container or MetaDefender Cluster Deploy on-premises or IaaS with Helm. Auto-scaling, self-healing, CI/CD integration.	Continue to next question ↓
Is the customer running a traditional VM environment (VMware, Hyper-V, or bare metal)?	→ Recommend: Virtual Machine or MetaDefender Cluster On-premises or IaaS. Full hardware control. Terraform templates, auto scaling groups for IaaS environment.	Continue to next question ↓
Does the customer want to avoid managing any infrastructure entirely?	→ Recommend: SaaS (MetaDefender Cloud) No infrastructure to manage. OPSWAT hosts, scales, and maintains everything.	Continue to next question ↓
Does the customer operate across multiple data centers or regions and need consistent deployment?	→ Recommend: Container (K8s) or MetaDefender Cluster K8s Helm chart ensures uniform config across regions. MetaDefender Cluster centralizes policy management across instances.	Continue to next question ↓
Is the customer currently evaluating or migrating to a cloud-native architecture?	→ Recommend: Container or SaaS or Virtual Machine IaaS (Cloud) Container deployment scales with cloud-native patterns. SaaS eliminates the infrastructure transition entirely. VM IaaS deployment can be provisioned on IaaS platforms.	Continue to next question ↓
Does MetaDefender Core support a hybrid environment — some on-premises and some clouds?	→ Recommend: Container (K8s) or Virtual Machine The Container deployment via Kubernetes is the most natural fit for hybrid environments. A single Helm chart can be used consistently across on-premises clusters and managed cloud clusters like EKS, AKS, or GKE. Alternatively, VM deployment can be provisioned both on-premises and on IaaS platforms and managed through the same policy layer.	

Discovery Question	If Yes	If No
Workload and Scalability		
Does the customer need to scan high volumes of files continuously with no downtime tolerance?	→ Recommend: MetaDefender Cluster Distributed nodes with load balancing, built-in redundancy, and horizontal scalability.	Continue to next question ↓
Does the customer require zero single points of failure in their file security stack?	→ Recommend: MetaDefender Cluster High availability architecture. Automated failover mechanisms avoiding single points of failure. Add nodes without service interruption.	Continue to next question ↓
Does the customer expect scan demand to spike significantly at certain times (peak hours, release cycles)?	→ Recommend: Container [K8S] or MetaDefender Cluster K8s HPA auto-scales pods during spikes. MetaDefender Cluster provides pre-provisioned capacity across dedicated nodes.	Continue to next question ↓
Does the customer need to scan files as part of a CI/CD pipeline or DevSecOps workflow?	→ Recommend: Container Native integration with artifact repositories and CI/CD tools. Helm chart deployment keeps it consistent.	Continue to next question ↓
Does the customer want to minimize CapEx and pay based on usage rather than fixed infrastructure?	→ Recommend: SaaS [MetaDefender Cloud] No infrastructure investment. Subscription-based pricing. OPSWAT scales capacity automatically.	

Discovery Question	If Yes	If No
Operational Readiness		
Does the customer have a dedicated DevOps or platform engineering team to manage deployments?	→ Recommend: Container or Virtual Machine or MetaDefender Cluster Container for modern DevOps teams. VM for traditional ops teams. Both are customer-managed.	Continue to next question ↓
Is the customer looking for a deployment that requires minimal ongoing maintenance from their team?	→ Recommend: SaaS (MetaDefender Cloud) SaaS: fully managed by OPSWAT.	Continue to next question ↓
Is the customer currently evaluating multiple vendors and needs a proof-of-concept quickly?	→ Recommend: Cloud Image Launch a pre-configured MetaDefender Core instance on AWS, Azure, or GCP for instant deployment and on-demand file scanning.	

How to use:

Work through each category with your customer. The more Yes answers pointing to a single option, the stronger the fit. If multiple options appear, consider combining them, for example MetaDefender Cluster deployed via Containers (K8S) for customers who need both high availability and CI/CD integration.

06

Objection Handling

Use these responses when customers raise common concerns during the sales conversation.

Objection	Response
"We process millions of files a day. We are worried that a single deployment won't keep up. Also, we can't afford any downtime on our file security infrastructure."	This is the core use case for MetaDefender Cluster. Rather than scaling a single node vertically, MetaDefender Cluster distributes scan requests horizontally across multiple MetaDefender Core instances. As volume grows, additional instances are added without service interruption. The MetaDefender Cluster Control Center handles load balancing and worker health monitoring automatically. Customers with multi-million file-per-day requirements have successfully deployed MetaDefender Cluster without throughput degradation.
"Deploying MetaDefender Core sounds complex and time-consuming."	• VM deployment uses ready-made Terraform templates that provision the environment in a few hours. • Container deployment runs from a single Helm chart and are live within minutes. • SaaS requires no deployment at all. OPSWAT provides documentation and professional services support for every deployment path.
"The cost seems high compared to simpler tools."	MetaDefender Core consolidates Predictive Alin AI, Deep CDR, Metascan Multiscanning, AI Content Inspection, Proactive DLP, Adaptive Sandbox, Threat Intelligence, File-based Vulnerability Assessment, SBOM, and Country of Origin into one deployment instead of separate tools - resulting in significantly lower TCO [Total Cost of Ownership] • The SaaS option eliminates infrastructure costs entirely and runs on a predictable subscription. • For on-premises, MetaDefender Cluster allows the customer to handle massive file volumes with horizontal scaling and parallelized archive processing, ensuring performance even under peak loads.

"We are concerned about scan performance and added latency."	For organizations with high scan volumes, MetaDefender Cluster distributes scan requests intelligently across MetaDefender Core instances using RabbitMQ and Redis, ensuring throughput without bottlenecks.
"Our team does not have the resources to manage this deployment."	• SaaS requires zero deployment expertise. • For on-premises, MetaDefender Cluster provides a single management interface for all worker nodes, reducing operational surface area compared to managing multiple independent MetaDefender Core instances. Container deployment benefits from Helm chart automation and integrates with existing Kubernetes tooling the team already operates.
"We need this to work in an air-gapped environment."	• Virtual Machine and Container deployments both supports fully offline operation. A local signature update server distributes engine and definition updates within the air-gapped network with no internet connectivity required. MetaDefender Cluster is also fully air-gap compatible and adds high availability within the isolated environment.
"We are concerned about licensing costs as our scan volume grows."	MetaDefender Core licensing is structured to scale with your deployment rather than purely on scan volume. For high-throughput environments, MetaDefender Cluster licensing is based on the number of MetaDefender Core instances rather than a per-scan fee, which provides cost predictability as volume grows. Speak with your OPSWAT Sales Engineer about the licensing structure for your expected volume tier. There are options designed to avoid unpredictable cost increases as usage scales.
"How do we know this will perform at our scale before we commit?"	OPSWAT supports proof-of-concept deployments scoped to your environment and file volume. A PoC [Proof of Concept] can be stood up quickly and run against your actual file types and volumes to demonstrate throughput and latency under real conditions. This gives you measured data rather than theoretical benchmarks before making a purchasing decision.

07

Resources

Deployment Page: <https://www.opswat.com/products/metadefender/core/deployment>

MetaDefender Core: <https://www.opswat.com/products/metadefender/core>

MetaDefender Cluster: <https://www.opswat.com/products/metadefender/cluster>

Documentation Page: <https://www.opswat.com/docs/mdcore>

Need Help?

Contact your OPSWAT Sales Engineer for a technical deployment assessment.