

OPSWAT.



USE CASE GUIDE

MetaDefenderTM Cluster

Scaling advanced threat prevention across the
MetaDefender portfolio with MetaDefender Cluster

Protecting the World's Critical Infrastructure

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.

This guide shows how MetaDefender Cluster works together with other products in the MetaDefender portfolio to deliver scanning capacity, resilience, and consistent policy enforcement at scale.

Use this guide to identify which pairing fits a customer's environment, to support a technical conversation, or to plan an internal architecture that grows with demand.

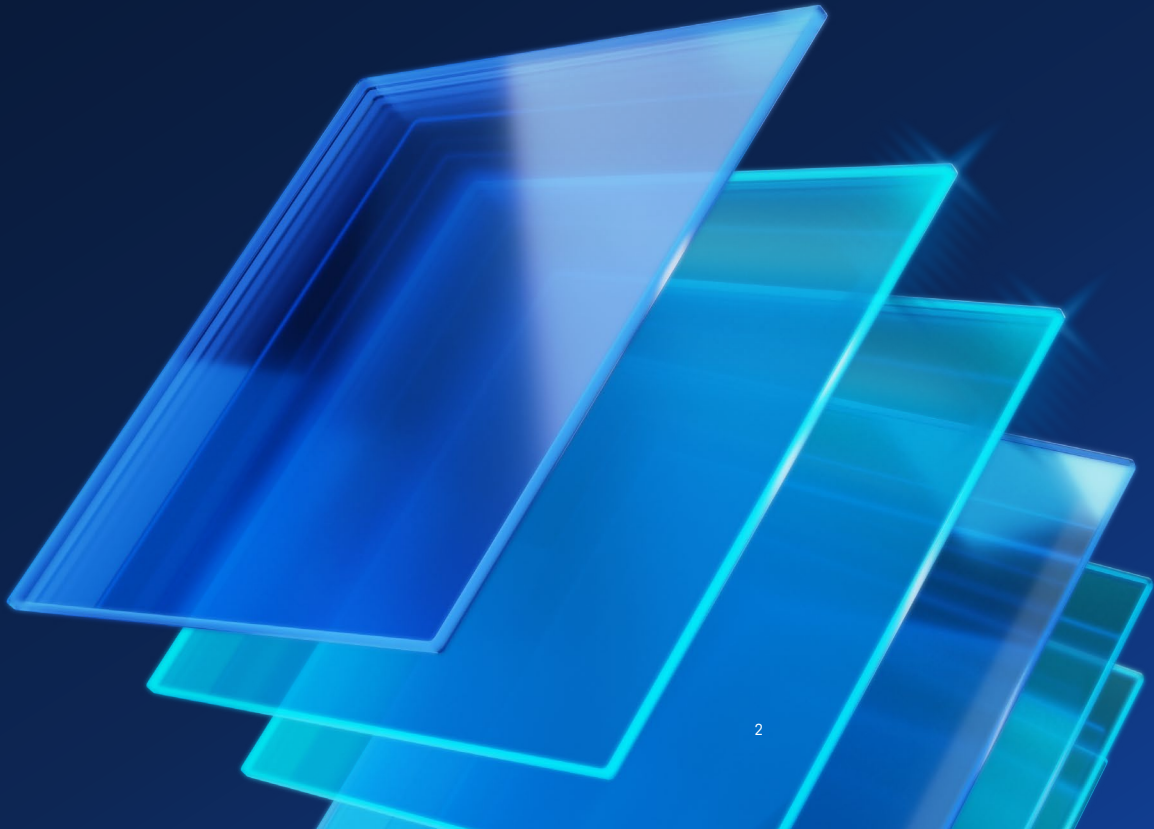


Table of Contents

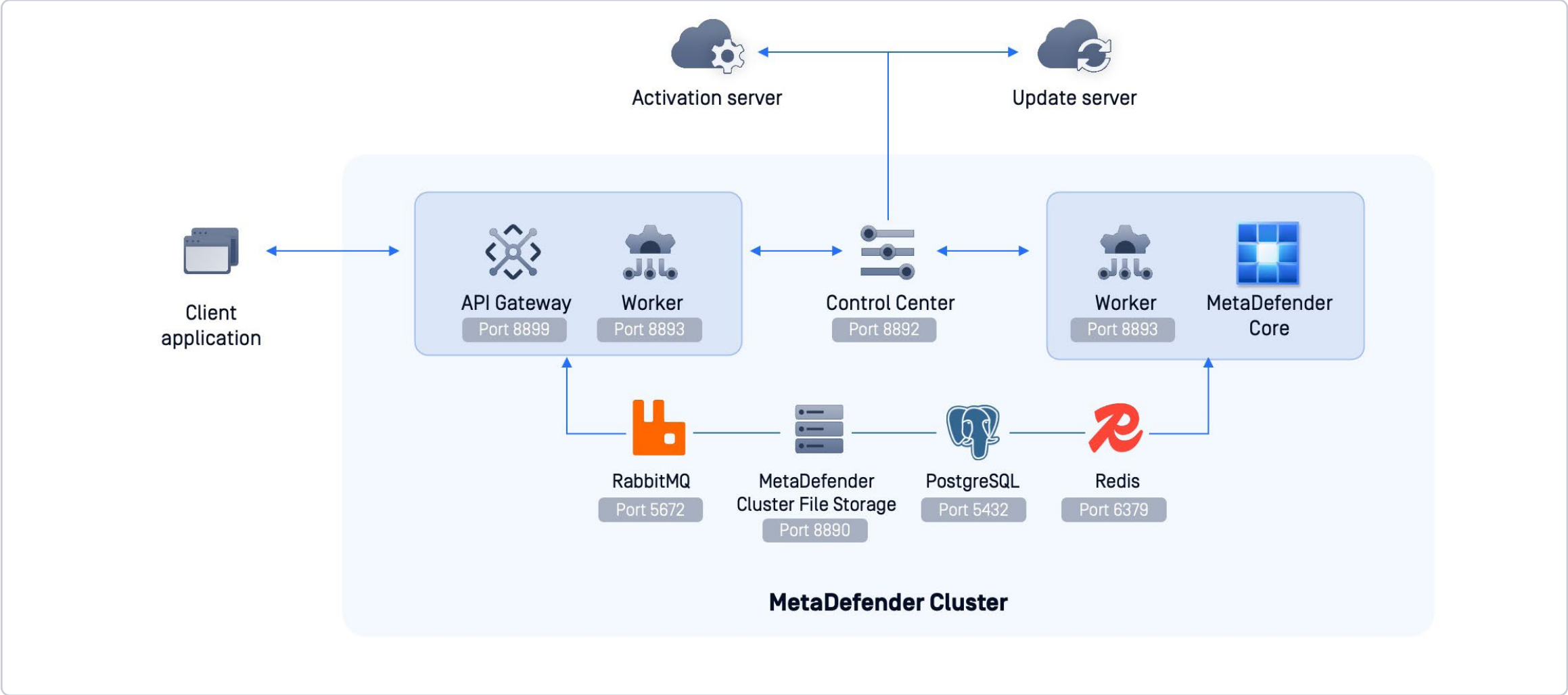
01	How Does MetaDefender Cluster Work?
02	Use Cases
	1. Distributed Extraction for Large and Nested Archives
	2. Keeping Pace with Everyday Endpoint File Activity
	3. Protecting Backup and Recovery Repositories Continuously
	4. Ensuring Email Security at Scale
	5. Maintaining Throughput for Bulk File Transfers
	6. IT/OT Security Across the Trust Boundary
03	Conclusion

01

How Does MetaDefender Cluster Work?

MetaDefender Cluster distributes scan workloads across multiple MetaDefender Core instances, accelerates archive processing through parallelization, and ensures operational continuity even during component outages. Its centralized Control Center provides orchestration, monitoring, and policy enforcement across deployments. Combined with support for API Gateway integration, secure file storage, and dynamic scaling, MetaDefender Cluster redefines how file security is deployed and managed at scale.

This deployment option is ideal for organizations prioritizing performance, resilience, and operational efficiency in high-demand environments.



Scalable File Security

Scale with confidence. Handle high-throughput file traffic without bottlenecks.

- Horizontal scaling of MetaDefender Core instances
- Parallel processing of archive file contents
- RabbitMQ-based task distribution
- Redis caching for in-memory result access

Resilient, Distributed Architecture

Built for resilience. Maintain uptime and availability even under failure or load.

- High availability across distributed components
- Fault-tolerant design with decoupled services
- Automated load sharing across nodes
- Health monitoring through Control Center

Centralized Control & Operational Visibility

Orchestrate with ease. Unified visibility and control across deployments.

- Centralized Control Center for deploying and upgrading Core and API Gateway
- License, workflow, and certificate management
- Executive dashboards, audit logs, and processing history
- HTTPS enablement for secure communication

02

Use Cases

USE CASE 01

Distributed Extraction for Large and Nested Archives

Business Requirement: Organizations that regularly scan large or deeply nested archive files and need scanning performance that keeps pace with file size and complexity.

Best For: Technology, Banking & Finance, Public Sector

The Use Case

Archive files are deceptively simple on the outside. A single archive can contain thousands of nested files, each of which needs to be extracted and inspected before anything inside can be trusted. The deeper the nesting and the larger the archive, the more that inspection work compounds, and a scanning setup that handles everyday files just fine can slow to a

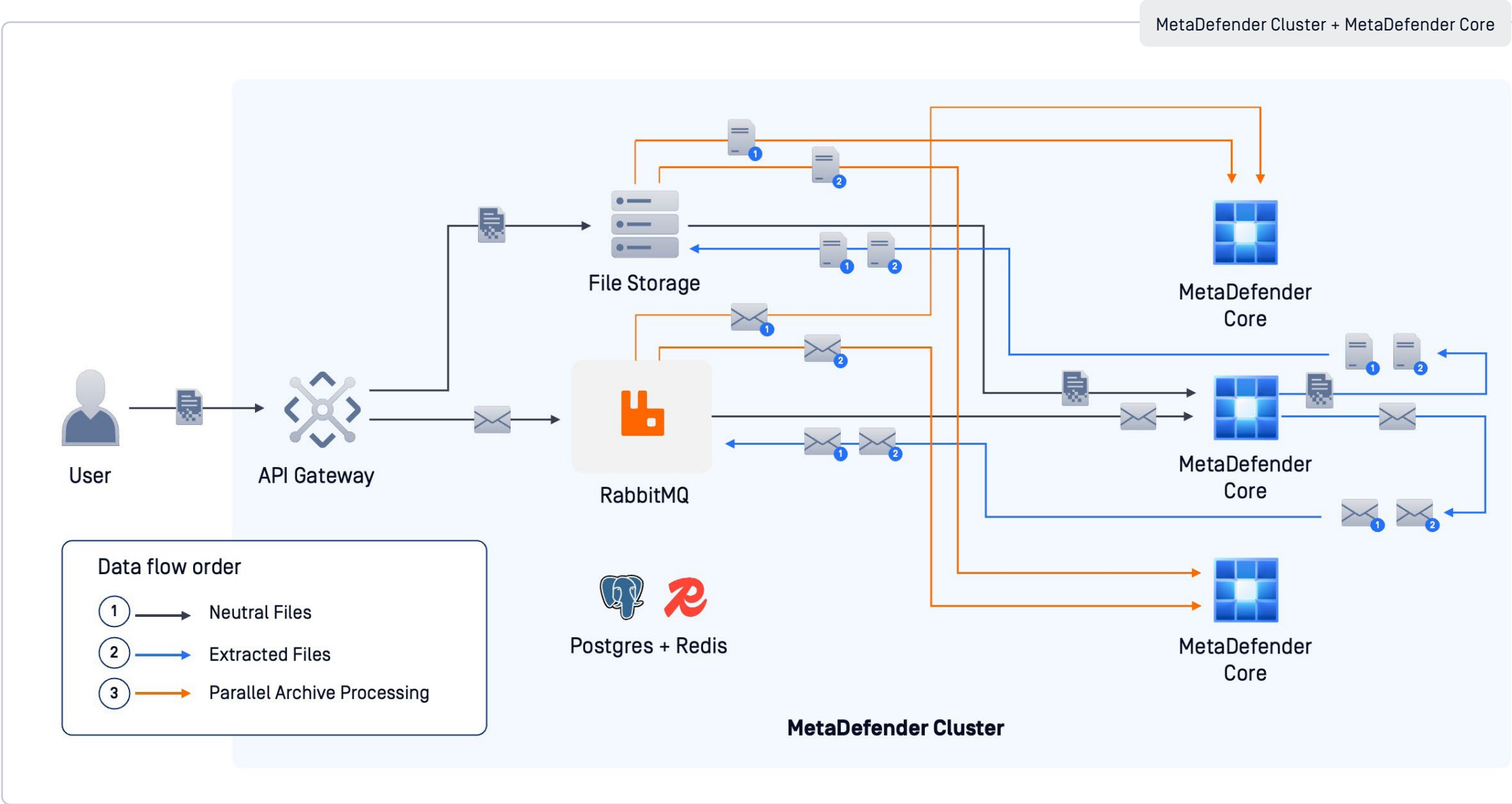
crawl the moment someone submits a multi-gigabyte archive with folders inside folders. The problem isn't whether the content can be scanned. It's whether it can be scanned without holding up everything else waiting behind it in the queue.

How the Products Work Together

- MetaDefender Cluster breaks a large or nested archive apart for simultaneous processing and distributes its contents across MetaDefender Core instances
- Workflow, updates and reporting are managed once and applied instance-wide, keeping every node consistent
- Built-in failover keeps an in-progress archive scan moving even under downtime or failure

Business Outcome

Large and nested archives scan significantly faster, with the added capacity and resilience that come from a distributed architecture.



USE CASE 02

Keeping Pace with Everyday Endpoint File Activity

Business Requirement: Enterprises with large, distributed device fleets that generate constant file activity, cloud downloads, removable media, file syncs, and need that volume inspected without becoming a point of failure.

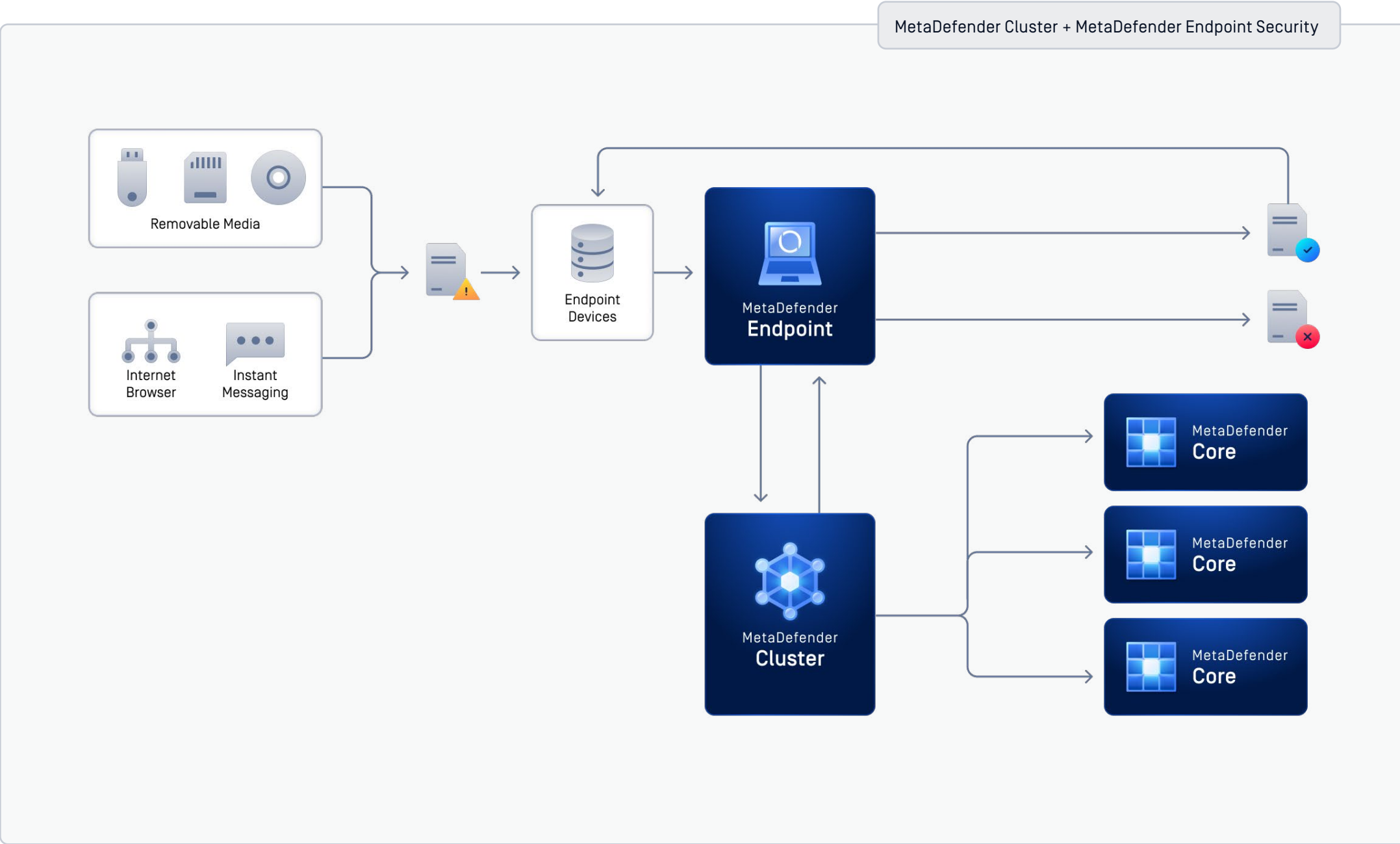
Best For: Banking & Finance, Healthcare, Professional Services

The Use Case

Across large organizations, everyday work generates a constant stream of files that need to be checked before they're trusted: staff downloading files from cloud storage and collaboration platforms, opening documents from removable media, pulling attachments off email, syncing folders between devices. Individually, none of it looks like much, but multiplied across thousands of employees doing normal work at the same time, the volume adds up fast. A scanning setup built for a lighter workload can stall entirely under added pressure, and when the scanning layer has a single point of failure, everyone downstream waits, or work grinds to a halt across the organization all at once.

How the Products Work Together

- MetaDefender Endpoint Security forward files requiring inspection to MetaDefender Cluster
- MetaDefender Cluster distributes incoming requests across every available MetaDefender Core instance, so a spike from thousands of endpoints is met with matching capacity. MetaDefender Core instances can be added to MetaDefender Cluster as file processing requests grow, so scanning capacity keeps pace with fleet size
- Verdicts return to MetaDefender Endpoint Security quickly enough to inform file inspection results in real time



Business Outcome

File security check at each endpoint stays fast and consistent, even during organization-wide sweeps or onboarding surges.

USE CASE 03

Protecting Backup and Recovery Repositories Continuously

Business Requirement: Organizations that need to protect large backups or file repositories without scanning becoming a gap in recovery readiness.

Best For: Banking & Finance, Healthcare, Managed Service Providers

The Use Case

A backup repository is the thing an organization falls back on when everything else goes wrong, which makes it a strange place to leave scanning as an afterthought. But backup and archive repositories are also where file counts get largest, millions of files, growing continuously, and a scan of that volume can take long enough that running often stops being practical. The risk amounts to a scanning process too slow to keep the backup itself trustworthy.

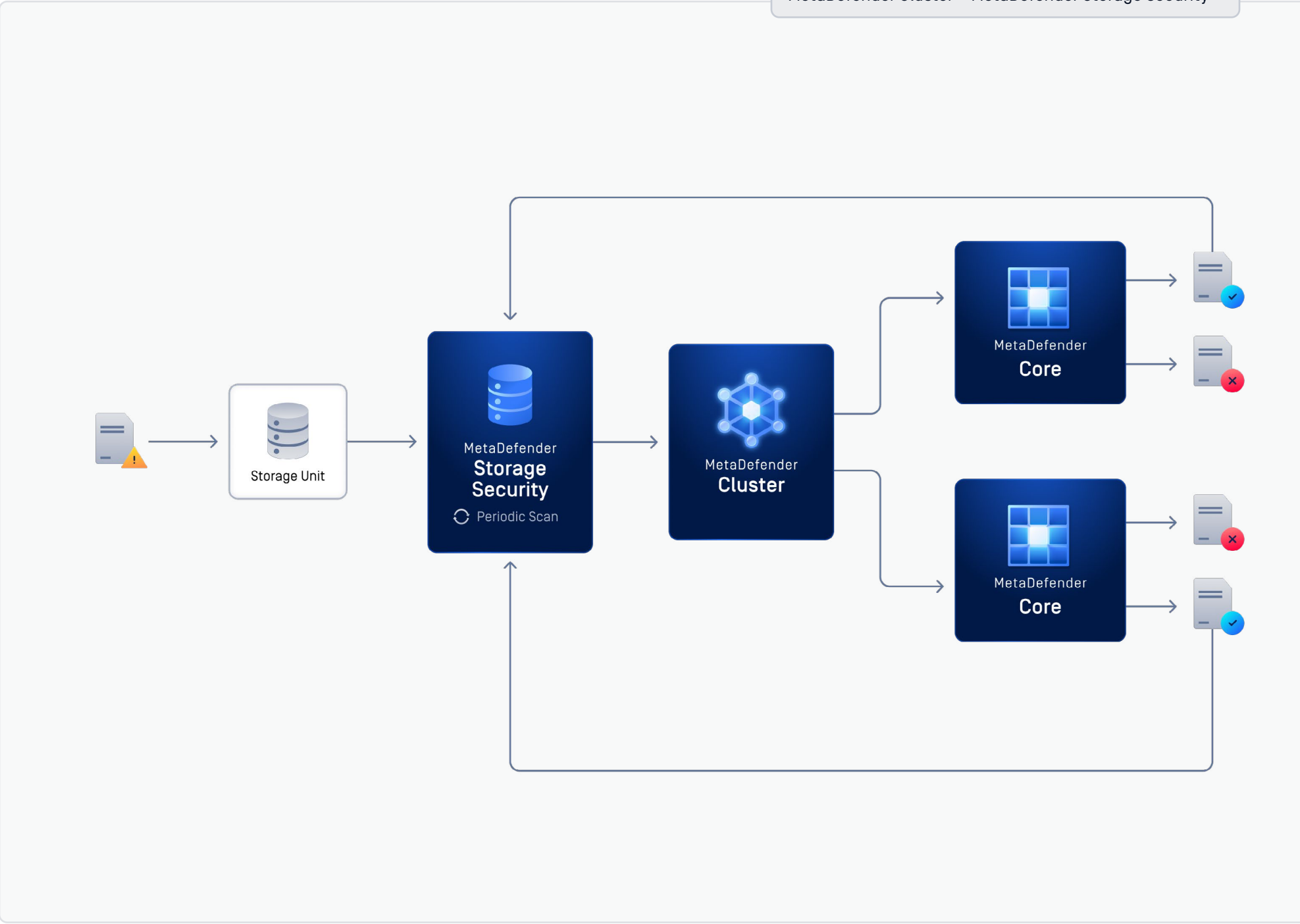
How the Products Work Together

- MetaDefender Storage Security centralizes new or existing files across the connected backup or storage repositories
- Files are sent to MetaDefender Cluster, which distributes them across MetaDefender Core instances for inspection
- File scanning and remediations happen in parallel across MetaDefender Core instances
- Clean, infected, or sanitized files are tagged and moved to assigned destinations according to pre-determined workflow in MetaDefender Storage Security
- Admin can set periodic scans in MetaDefender Storage Security to automatically check your files at rest for zero-day or vulnerabilities at a pre-determined time and frequency.

Business Outcome

Large backup repositories and continuous ingestion scan quickly and reliably, keeping recovery data clean and trustworthy.

MetaDefender Cluster + MetaDefender Storage Security

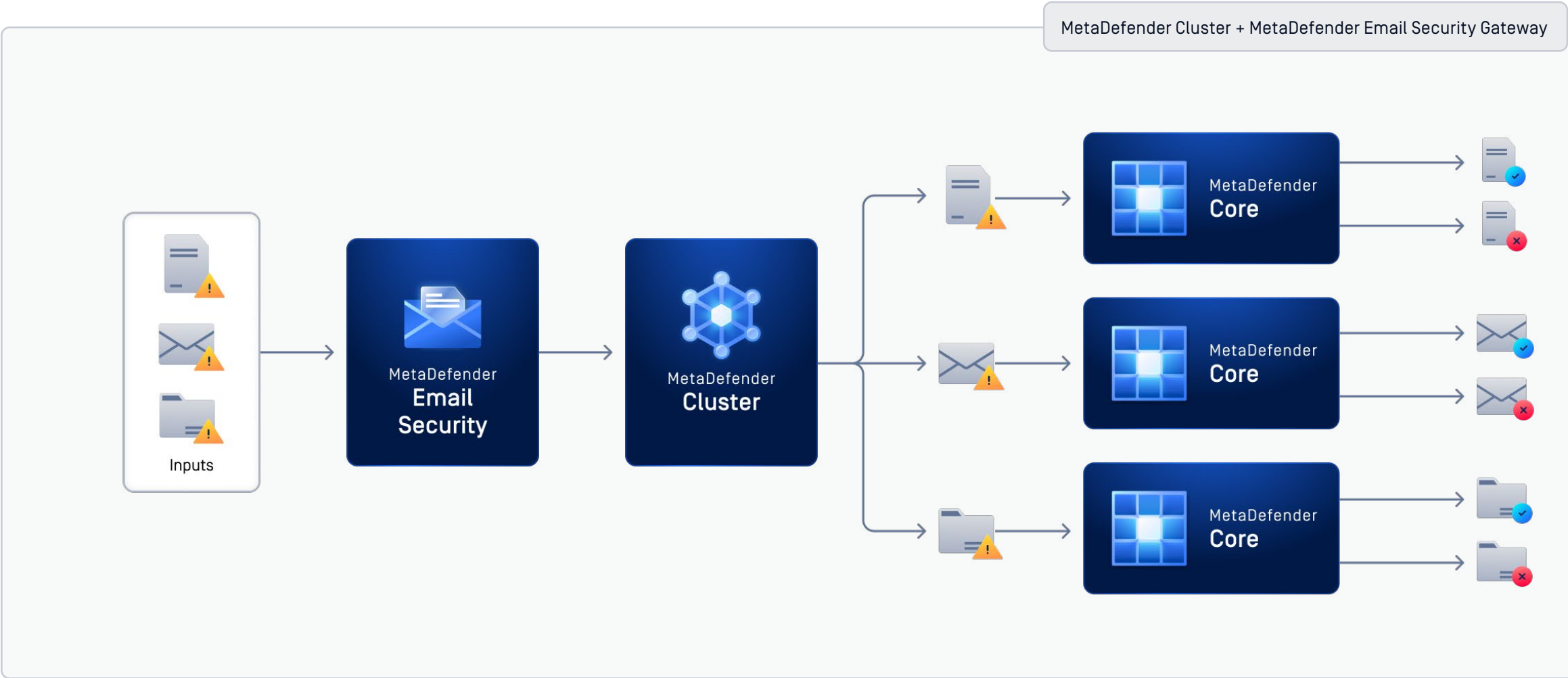


USE CASE 04

Ensuring Email Security at Scale

Business Requirement: Organizations with over a thousand end users relying on email as a primary channel for document exchange, where large attachments and high daily volume make single-node scanning impractical.

Best For: Banking & Finance, Professional Services, Education, Public Sector



The Use Case

Organization that needs to scan daily inbound and outbound email traffic for over a thousand end users. The primary file types moving through that traffic are attached documents, including email, PDF, and Office formats, as well as archives, often at large file sizes. Email volume at this scale, combined with large or complex attachments, requires scanning capacity that keeps pace with traffic without slowing mail delivery.

How the Products Work Together

- MetaDefender Email Security Gateway handles routing, quarantine policies, and allow/block rules for every inbound and outbound message
- Attachments requiring inspection, documents, PDFs, Office files, and archives, are sent to MetaDefender Cluster
- MetaDefender Cluster distributes attachment scanning across MetaDefender Core instances for parallel processing
- High availability capability across MetaDefender Cluster keeps email scanning running continuously, even during maintenance or unexpected load
- Verdicts return to MetaDefender Email Security Gateway to inform quarantine, allow, and block decisions in real time

Business Outcome

Inbound and outbound email keeps moving at the pace a large user base requires, with consistent scanning of every attachment regardless of size or volume.

USE CASE 05

Maintaining Throughput for Bulk File Transfers

Business Requirement: Organizations that move and inspect very large volumes or very large , complex files and need scanning capacity that scales to match throughput.

Best For: Critical Infrastructure, Public Sector, Banking & Finance

The Use Case

When file volume or file size crosses a certain threshold, the question stops being whether a file can be inspected and becomes whether inspection can keep up without turning into the bottleneck. That's compounded when files are also crossing a transfer boundary, where the requirement isn't just speed, it's guaranteeing data only moves in one approved direction.

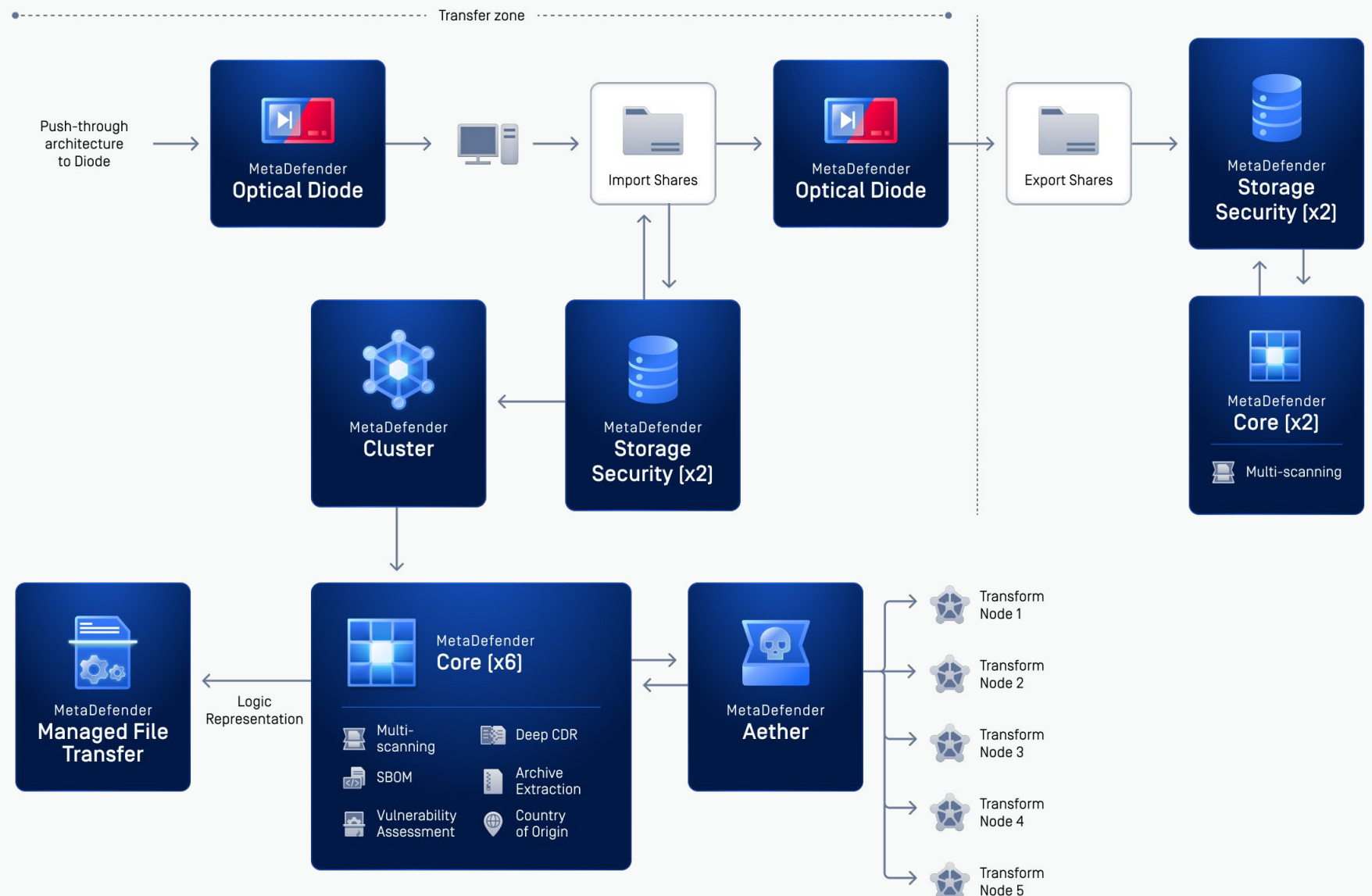
How the Products Work Together

- MetaDefender Optical Diode enforces one-way data flow at the transfer zone boundary, physically preventing any data from moving back across once it has been imported, so files can only pass in the approved direction after inspection.
- Files are received via SMB Shares and picked up by MetaDefender Storage Security
- Then MetaDefender Storage Security sends files to MetaDefender Cluster.
- From here, MetaDefender Cluster distributes files across multiple MetaDefender Core instances - each runs a full inspection stack, so every file gets deep file inspection without slowing throughput
- Scanned files are forwarded to MetaDefender Aether for deeper analysis, keeping overall time-to-verdict low
- Based on the scan and behavior analysis outcome, MetaDefender Storage Security tags and moves files to destinations according to the pre-determined workflow
- MetaDefender Managed File Transfer orchestrates release with automatic failover, so a transfer keeps moving even while downtime or single failure

Business Outcome

High volumes of large files move through deep inspection quickly, with capacity that scales to match throughput requirements.

MetaDefender Cluster + MetaDefender Core, MetaDefender Storage Security, MetaDefender Managed File Transfer, MetaDefender Aether, MetaDefender Optical Diode



USE CASE 06

IT/OT Security Across the Trust Boundary

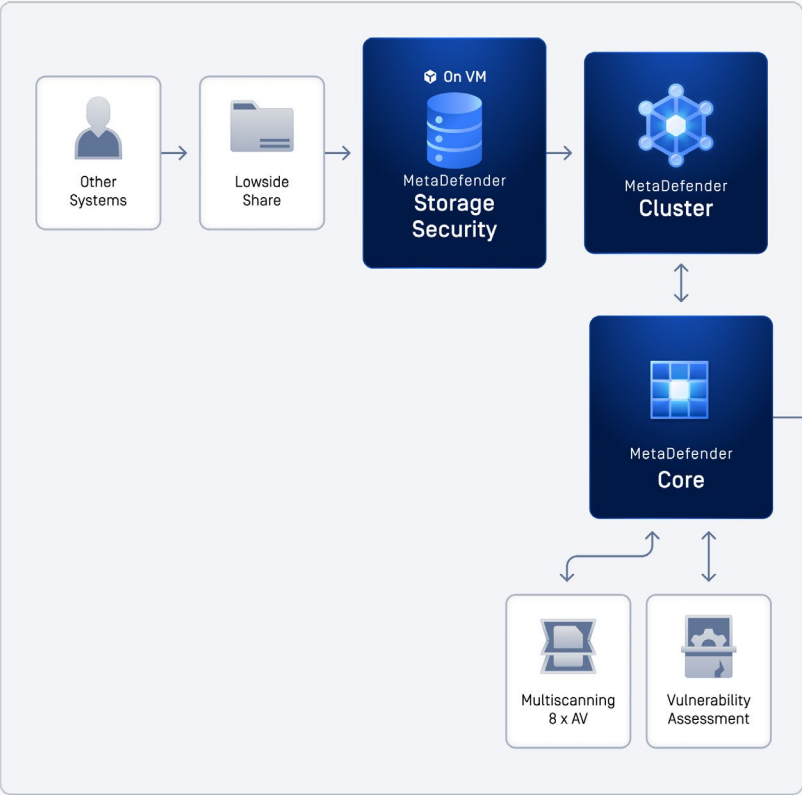
Business Requirement: Organizations operating regulated or industrial environments that need consistent, policy-enforced file security across the IT/OT boundary.

Best For: Manufacturing, Energy & Utilities, Critical Infrastructure, Government & Defense

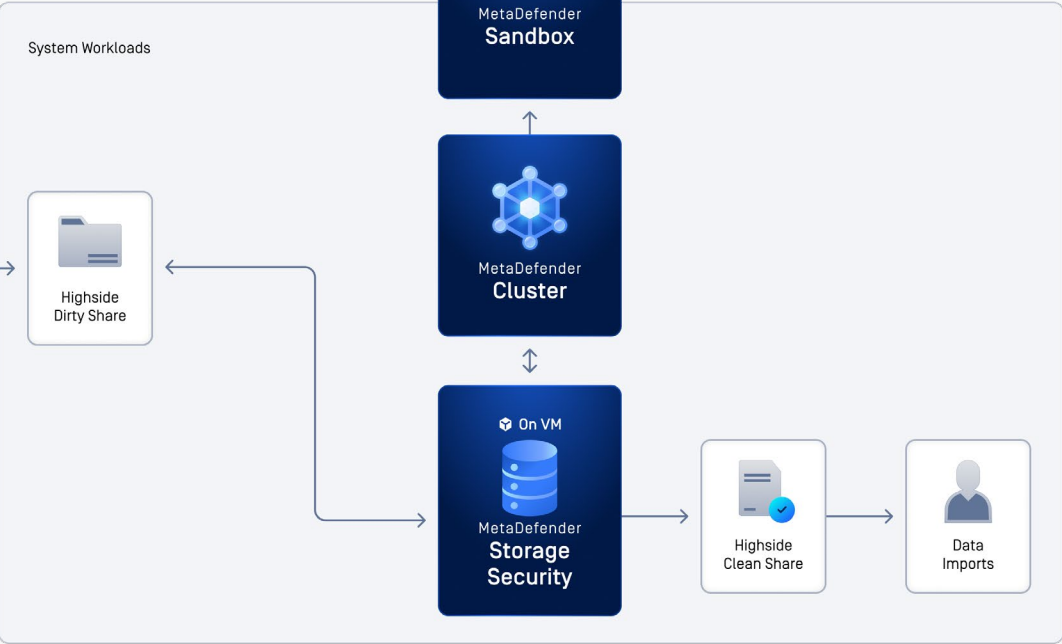
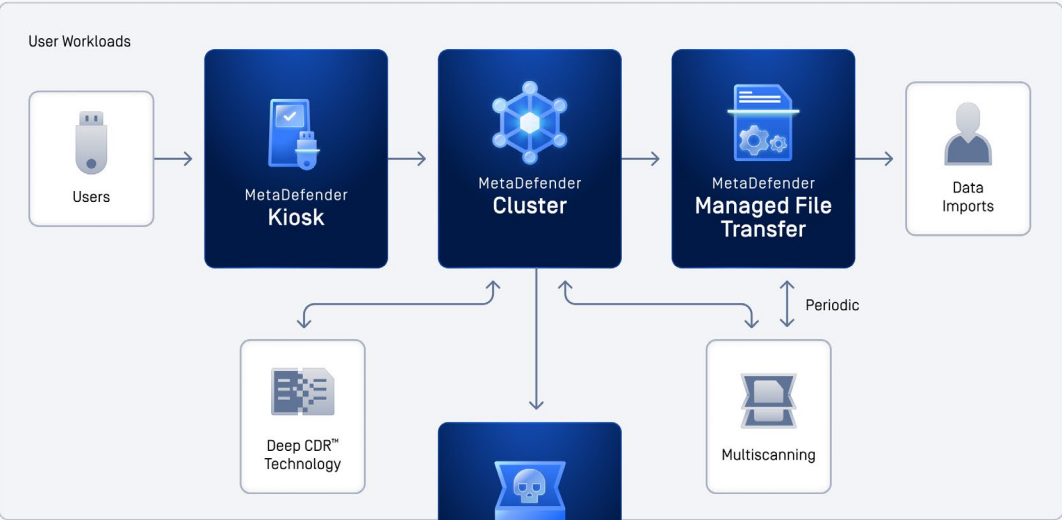
The Use Case

IT and OT environments are kept separate for good reasons: a compromise on the OT side doesn't just risk data, it risks physical processes, safety systems, and uptime that can't be undone after the fact. But that separation was never meant to be absolute. Patches, engineering files, vendor updates, and production data still must move between the two sides, and every one of those movements, whether it arrives on a removable device or a scheduled transfer, is a potential way in. The challenge is making sure every path into the production environments is held to the same standard, without adding enough friction that people start looking for shortcuts around it.

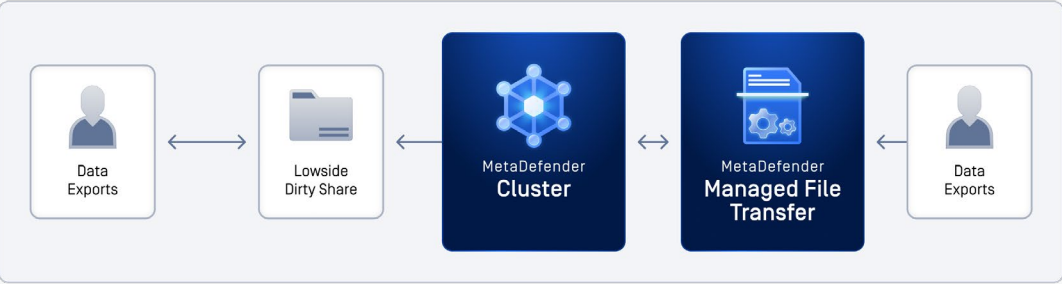
Import Flow



MetaDefender Cluster + MetaDefender Kiosk, MetaDefender Storage Security, MetaDefender Managed File Transfer, MetaDefender Aether



Export Flow



How the Products Work Together

- MetaDefender Storage Security sends files to MetaDefender Cluster. MetaDefender Cluster distributes this workload across MetaDefender Core instances to scan and check for file-borne threats and file-based vulnerabilities
- MetaDefender Optical Diode enforces strict one-way data flow between import and export shares, physically preventing return traffic across the transfer zone boundary
- From user workload side, MetaDefender Kiosk scans removable media before a device connects to any system, sending files to MetaDefender Cluster so every checkpoint enforces the same workflow. Files that meet escalation criteria are routed to MetaDefender Aether for behavioral analysis, reserving deep inspection for what actually needs it
- MetaDefender Managed File Transfer automates policy-driven file transfers and enhances operational efficiency. MetaDefender Cluster helps MetaDefender Managed File Transfer ensure high availability with its fault-tolerant design and distributed architecture.

Business Outcome

Files move across the IT/OT boundary only after consistent, policy-enforced inspection, with scanning capacity that scales to match the environment.

03
Conclusion

MetaDefender Cluster gives organizations the flexibility to grow their file security posture in step with their environment, whether that growth comes from more files, more devices, more integrated products, or more complex infrastructure.

The use cases in this guide illustrate different starting points, but they all draw from the same underlying capability. As file security needs evolve, MetaDefender Cluster provides the foundation to scale confidently, without compromising on performance, resilience, or control.

GET STARTED

For help scoping MetaDefender Cluster deployment alongside any MetaDefender products in this guide, reach out to your OPSWAT account team.

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 1,800 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