OPSWAT.

SOLUTION BRIEF

Secure File Movement from Kiosk Intake to Controlled Delivery

Move files from physical media intake into governed, auditable delivery workflows across the DMZ

Value Proposition

Fast intake screening. Governed transfer. Deeper analysis before delivery.

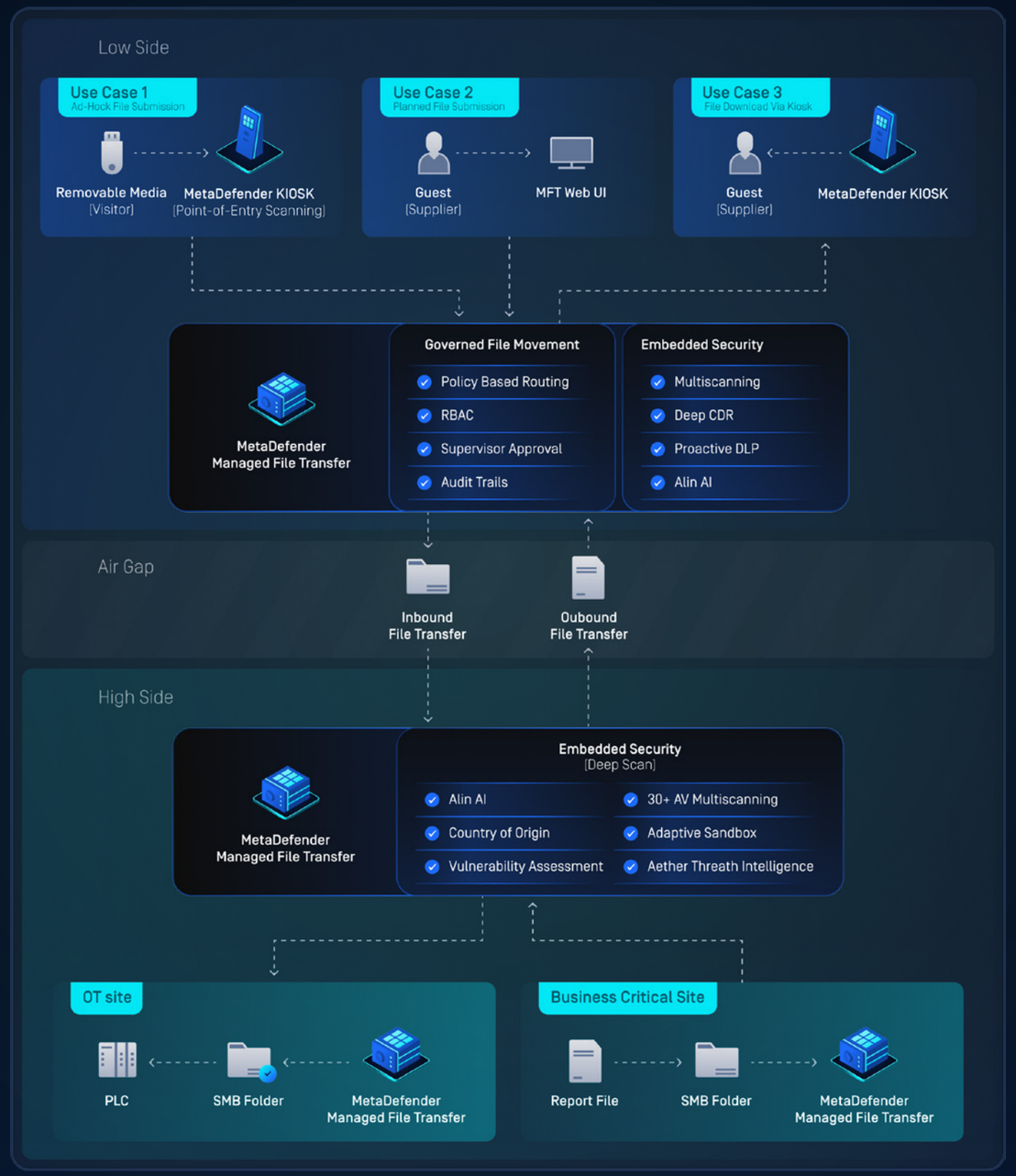
MetaDefender Kiosk solution gives organizations a controlled point of entry for files introduced through portable media or walk-up workflows. MetaDefender Managed File Transfer solution then pulls approved files into a governed workflow where routing, RBAC (Role-Based Access Control), automation, auditability, and deeper built-in inspection help ensure files reach the right destination under the right policy.

The Challenge

Critical file movement often happens outside standard enterprise workflows:

- Contractors arrive with files on USB drives or optical media
- Vendors need to deliver patches, firmware, updates, or engineering files
- Operators need files quickly to maintain equipment or restore service
- Security teams need time to inspect files before they reach sensitive systems
- IT and OT teams need visibility into who submitted a file, where it went, and what happened to it
- Manual handoffs and unmanaged shared folders create audit gaps
- Uncontrolled sneakernet increases operational, security, and compliance risk

The problem extends beyond mere file scanning to controlling the full journey, from intake to approved delivery.



Integration Use Cases

Point-of-Entry Scanning

For contractors, field engineers, operators, or visitors who arrive with portable media and need to deliver files into a controlled environment:

- MetaDefender Kiosk provides the first controlled intake point
- Built-in file security performs rapid screening with multiscanning and Alin AI-assisted analysis
- Approved files are pulled into MetaDefender Managed File Transfer
- Files are routed to the correct department, folder, or destination workflow
- Deeper analysis can run before release while the user moves toward the plant, workstation, tool, or operational system

Planned File Submission

For suppliers, vendors, partners, or guest users who can submit files before an operational window:

- Users submit files through the MetaDefender Managed File Transfer web interface
- Policy-based routing sends files to the right workflow
- Built-in security performs deeper inspection, including sandboxing and threat analysis where configured
- Approved files are delivered to the target folder, OT system, business-critical workflow, or partner exchange
- Blocked or suspicious files are held, quarantined, or escalated based on policy

Controlled Internal Data Release

For operations, engineering, or plant teams that need to share production reports, logs, analytics, or other approved files with suppliers or partners:

- Files generated in OT or production environments are saved in an SMB or SFTP folder
- MetaDefender Managed File Transfer picks up the file through scheduled automation and applies DLP (Data Loss Prevention) to help prevent sensitive data violations
- Files that meet policy requirements enter a supervisor approval workflow to help ensure confidential data does not leave the organization without authorization
- An automated job delivers the file to another MetaDefender Managed File Transfer instance integrated with MetaDefender Kiosk
- Non-guest suppliers can retrieve approved files through MetaDefender Kiosk without direct access to internal OT or production folders

Key Benefits

Keep Operations Moving While Security Runs Deeper

Give contractors, vendors, field teams, and operators a controlled way to submit files without waiting on manual handoffs or bypassing security. Rapid intake screening helps users move forward, while deeper analysis can continue before files are released to the destination.

Reduce the Cost of Manual File Movement

Replace unmanaged sneakernet, shared folders, and one-off transfer processes with policy-driven delivery. IT, OT, and security teams spend less time coordinating file movement, validating destinations, chasing approvals, or reconstructing what happened after the fact.

Lower the Impact of File-Borne Threats

Apply inspection at intake and before delivery to reduce the chance that malware, suspicious content, or unverified files reach OT, production, partner, or business-critical environments. Blocking one unsafe file can help avoid downtime, incident response effort, compliance exposure, and reputational damage.

Make Every File Journey Accountable

Maintain a clear record from media insertion or file submission through inspection, routing, approval, quarantine, or delivery. Teams can see who submitted the file, what policies were applied, where it went, and whether it was approved, held, or blocked.

Govern Delivery Across Critical Environments

Move approved files into the right department, folder, system, or partner workflow using policy-based routing, RBAC, encrypted transfer, notifications, and audit controls. This gives CISOs, IT leaders, operations teams, and administrators a repeatable way to control file movement across IT, OT, and business-critical environments.

MetaDefender Kiosk and MetaDefender Managed File Transfer solutions help organizations turn risky file movement into a controlled workflow. Files are screened at intake, moved through governed transfer paths, analyzed before release, and delivered with policy, visibility, and auditability.

Talk to an Expert

OPSWAT.
Protecting the World's Critical Infrastructure