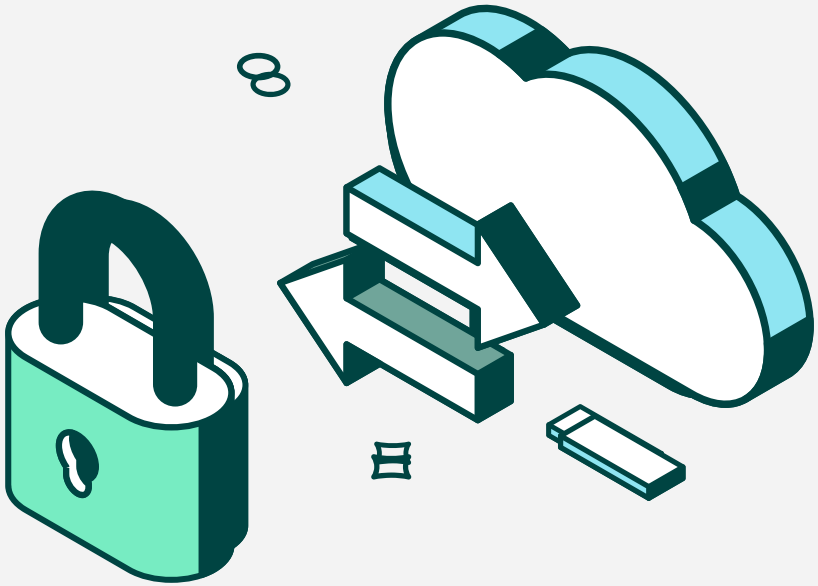
FORTRA MFT
GoAnywhere

Beyond Checkbox MFT

Security That Actively Protects Your Data Transfers

A Buyer's Guide for Evaluating Real Security, Operational Control, and Risk Reduction

Table of Contents



Purpose of This Guide

Most Managed File Transfer (MFT) platforms claim to be “secure.” Encryption is enabled, certifications are in place, and audit logs are available on demand. On paper, these MFT environments look well protected.

But experienced practitioners know that security failures rarely stem from missing encryption. They stem from everyday operational realities: misrouted files, over-permissioned users, and one-off scripts that quietly become critical workflows and environments where enforcement depends more on institutional knowledge than on system design.

This guide is intended to help organizations move beyond checkbox security—controls that satisfy audits—and examine whether their MFT environment actually **reduces risk in daily operations**. It focuses on whether a platform **prevents mistakes** as transfers occur, limits the blast radius when something goes wrong, and **enforces policy automatically**, rather than relying on after-the-fact reviews.

Executive Summary

From "Secure Transfers" to Controlled Data Movement

Most MFT platforms can secure files during transmission. They emphasize foundational capabilities such as:

- Why MFT has become a primary attack surface
- Encryption in transit and at rest
- Regulatory alignment (GDPR, HIPAA, PCI, SOC, ISO, FIPS)
- Audit logging and reporting

These are **necessary**, but they are **foundational controls**, not sufficient.

Where many platforms fall short is in controlling how data moves through real-world environments—where files are routed through multiple systems, handled by different teams, and exchanged with external partners. In those conditions, security is less about protecting packets on the wire and more about ensuring transfers behave correctly every time.

Platforms that enable real risk reduction are able to:

- Ensure files go to approved destinations
- Enforce least-privilege access by default and apply policies automatically as workflows execute
- Reduce risk before incidents occur, not just document them afterwards

Key takeaway

The security of an MFT platform should not be judged solely by encryption standards or the richness of its audit logs. It should be judged by how consistently it:

- **Prevents mistakes** instead of documenting them
- **Enforces policy in real time** instead of relying on reviews
- **Scales securely** without increasing operational burden

To understand why this gap persists, it helps to look at how MFT platforms are typically evaluated—and where those evaluations fail to reflect real operational risk.

1 The gap between security controls and security outcomes

Most MFT evaluations begin with a familiar checklist: encryption protocols (TLS, PGP), compliance claims (GDPR, HIPAA, PCI, etc.), and reporting capabilities. These controls are important—but they don't directly answer the question security teams wrestle with in practice:

Will this platform protect us from the mistakes we haven't anticipated yet?

In production environments, risk is rarely driven by missing controls. It's driven by how those controls are applied—or bypassed—once systems scale.

Common sources of risk include:

- **Files sent to the wrong partner or environment**
- **Users granted access "temporarily" that never gets revoked**
- **Partner onboarding that grows faster than governance**
- **Script-heavy automation with limited oversight**
- **Configuration drift as teams, integrations, and requirements change**

Reality in many environments:

- ✓ Controls exist
- ✗ Enforcement is inconsistent
- ✗ Detection happens after the event
- ✗ Security depends on administrator discipline

Does the platform prevent incorrect actions at runtime, or only record them after they happen?

2 Compliance does not equal protection

Compliance frameworks play an important role. They help organizations answer questions such as who accessed data, when an action occurred, and whether required safeguards were in place.

What they do not do is stop problems from happening.

Compliance reporting alone cannot:

- **Block unauthorized transfers**
- **Dynamically enforce least-privilege access**
- **Prevent human error in automated workflows**
- **Reduce reliance on manual checks and reviews**

That distinction matters. Auditability provides visibility. Active security provides protection. One does not replace the other.

auditability = visibility | active security = prevention

Platforms that conflate audit reporting with security controls often leave enforcement gaps that only become visible during an incident, or an investigation.

Does the platform enforce policy during execution, or does it rely on post-event review to surface issues?

3 What to look for: "Active MFT Security" in practice

Active security means controls are applied as transfers occur across the entire workflow lifecycle. It's the difference between ***discovering* a violation** and ***preventing* it from happening** at all.

In practice, this requires security to be embedded directly into how the platform operates, not bolted on as an external layer.

Platforms that deliver active security typically share these characteristics:

- **Policy enforcement at runtime**
  Transfer rules are applied automatically and consistently—without manual checks.
- **Security embedded in workflows**
  Controls are built into automation logic, not delegated to external tools or scripts.
- **Reduced script dependency**
  Centralized, auditable logic replaces fragile custom scripts.
- **Unified control plane**
  Policies are defined and enforced in one place, not fragmented across components.
- **Real-time operational visibility**
  Insight is tied to behavior and execution, not just log aggregation.

Are security controls intrinsic to how workflows execute, or simply layered on top?

4 Where Risk Actually Occurs: Before and After the Transfer

Encryption protects data in transit. But most operational risk exists outside that narrow window.

Incidents commonly originate:

- Before transfer, during data preparation, routing, and access decisions
- After transfer, during storage, processing, or downstream distribution

Few MFT incidents are caused by broken encryption. Far more stem from:

- **Uncontrolled partner onboarding**
- **Credential reuse and weak access controls**
- **Script-driven workflows that outgrow their original design**
- **Limited visibility across pre- and post-transfer steps**

Many large MFT environments expand into multi-component architectures, often deployed independently over time. While having some flexibility, this fragmentation increases operational complexity and makes consistent enforcement harder to achieve.

Does the platform provide end-to-end control across the entire workflow or does it focus primarily on the protocol layer?

5 Operational complexity is a security risk

Security doesn't fail all at once. Rather, it erodes gradually as systems become harder to manage.

Environments that rely heavily on **manual configuration, periodic hardening, and script maintenance** tend to accumulate risk as they scale. Over time, this leads to:

- Inconsistent policy enforcement
- Increased human error
- Higher operational overhead
- Slower response to emerging risks

Common indicators of growing operational risk include:

- **Frequent reliance on custom scripts for automation**
- **Ongoing manual security reviews to "double-check" configurations**
- **Security knowledge is heavily siloed in a few administrators**
- **Difficulty scaling without adding headcount (or vendor services)**

These pressures are often what prompt organizations to reassess legacy MFT platforms—not because they failed outright, but because control didn't scale with complexity.

Does the platform reduce operational dependency, or does security depend on continuous manual effort?

6 Critical Capabilities to Validate Before Selection

When evaluating MFT solutions, technical breadth matters—but so does how those capabilities work together.

Rather than assessing features in isolation, **validate whether the platform delivers cohesive control** across these areas:

Security & Control

- Policy enforcement at transfer time
- Centralized access control and governance
- Integrated threat protection (e.g., scanning, inspection)
- Strong key and certificate management

Automation & Orchestration

- Native workflow engine (not script-dependent)
- Event-driven triggers and scheduling
- API access for automation and integration

Architecture

- Unified platform vs loosely coupled components
- Consistent enforcement across DMZs, gateways, and external services
- Designed support for high availability and disaster recovery

Visibility & Audit

- Real-time operational visibility
- Centralized audit logs tied directly to workflows
- End-to-end traceability of data movement

Cloud & Integration

- Native support for cloud storage and services
- Prebuilt integrations that reduce custom effort
- Consistent policy enforcement across environments

7 Questions that reveal real capability

Well-designed demos can often hide operational friction. The fastest way to surface it is by asking questions that **probe enforcement, scaling, and day-to-day management**:

- Can policies be enforced without **modifying scripts or workflows**?
- What percentage of automation depends on **custom scripting**?
- How does the platform prevent **human error**, not just detect it?
- Are security controls **consistent across all components**?
- Does scaling increase **administrative overhead**?
- How are **pre- and post-transfer risks controlled**?
- Is visibility **centralized across the full workflow lifecycle**?

8 Common pitfalls in MFT evaluations

Organizations often underestimate:

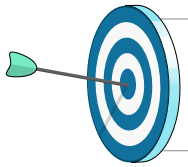
- **The long-term impact of script-based automation**
- **The operational burden and enforcement gaps of multi-component architectures**
- **The gap between audit visibility and real protection**
- **The complexity of scaling secure environments**

Most of these issues don't surface during evaluation. They appear months or years **after deployment**, once complexity sets in.

9 The path forward to modern MFT

Your MFT environments today must do more than only move files securely. They must:

- Enforce security **automatically**
- Drastically **limit manual processes**
- Provide true **end-to-end control**
- **Scale** without increasing operational risk
- Treat security as an **operational system**, not a checklist



The goal is not to simply transfer files securely.
It's to ensure that every transfer behaves correctly by design.

What's Next?

Evaluate your current MFT environment against these criteria—any one of them should be considered a red flag.

If your platform

- Relies on manual enforcement
- Depends heavily on scripts
- Separates security from operations

It is time to reassess

Look for solutions that embed security into workflows, centralize control and visibility, and reduce operational risk at scale.

Turn insight into action. Explore how modern MFT platforms enforce security as part of every transfer, not after the fact.

BOOK A DEMO

FORTRA® MFT

GoAnywhere®

About GoAnywhere

GoAnywhere MFT is an award-winning cybersecurity product line that helps more than 4,000 organizations safely connect to their trading partners, automate their IT processes, protect their data, and keep their sensitive information out of the DMZ.