FORTRA MFT
GoAnywhere

What is Missed When Using Other MFT Solutions

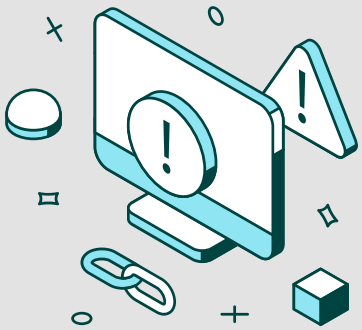
Table of Contents

In many IT environments, MFT solutions such as Axway SecureTransport or Progress MOVEit are already in place to handle file transfer needs. However, as audits become more complex, automation does not scale effectively, nor security expectations get elevated, “it works” simply isn’t enough.

Based on what we consistently see across IT teams running other MFT solutions, our experience providing solutions, and leading migrations for over 6,000 organizations globally, here is a practical overview of areas that can surface over time.

Modern file transfer risk isn’t solved by protocols alone. The difference is whether your MFT is **properly governed, automated, and audit-ready** in production.

The Hidden Gaps Exposed in MFT Deployments



In many environments, critical gaps in architecture, identity, automation, auditing, and security can typically remain unnoticed during initial implementations and only surface as environments scale or become more complex. These gaps often emerge during periods of change, such as cloud migrations, increased data volume, or with heightened security scrutiny.

At that stage, teams frequently discover that addressing these gaps requires additional components, specialized expertise, and ongoing operational effort. This is often the inflection point where operational risk, limited visibility, and rising total cost of ownership (TCO) become impossible to ignore, prompting organizations to reassess whether their current MFT approach is still sustainable.

Let's look at the gaps and what can help close them >

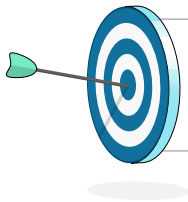
1 **Perimeter architecture difficult to standardize across business units** (DMZ patterns, proxies, trust boundaries)

WHAT CUSTOMERS OFTEN HAVE TODAY:

- A DMZ component (like Axway SecureTransport Edge or MOVEit Gateway) is deployed correctly, but **inconsistently** across teams or regions
- Different protocol handling, firewall rules, and operational processes per business unit
- Perimeter security that depends heavily on **external controls** (network firewalls, addon tools) rather than MFT-native governance

WHAT TO LOOK FOR AND WHY IT MATTERS:

- Look for a single, repeatable DMZ reverse-proxy model that works the same way across all teams and protocols, not a perimeter design that changes by region, business unit, or transfer type.
- When each team implements the DMZ differently, security reviews get harder; firewall rules multiply, and risk accumulates quietly over time. Platforms that provide a **consistent gateway** pattern make it easier to standardize controls, onboarding, and audits across the organization.



Solutions designed around a dedicated, protocol-aware MFT gateway tend to scale more cleanly than deployments that rely on custom or environment-specific perimeter setups.

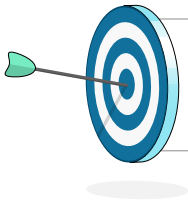
2 Identity configuration surprises that change how users can transfer files (SSO/MFA edge cases)

WHAT CUSTOMERS OFTEN HAVE TODAY:

- SSO and MFA are supported but may include **important configuration considerations** that are not always obvious.
- Example:
  - In some configurations, enabling SSO for end users can impact or restrict HTTP(S) transfer methods.
  - MFA setups may introduce constraints or limitations for OpenSSH or batch-based workflows.

WHAT TO LOOK FOR AND WHY IT MATTERS:

- Identity controls (SSO, MFA, RBAC) that behave consistently across user access, automation, APIs, and batch transfers—with clear documentation on any constraints
- In many environments, tightening identity security later introduces unexpected tradeoffs. (For example, certain transfer methods no longer working with SSO or MFA). A modern MFT platform should let security teams strengthen identity controls without breaking business workflows.



Platforms that apply identity uniformly and automatically across users reduce the risk of security improvements unintentionally disrupting file transfers.

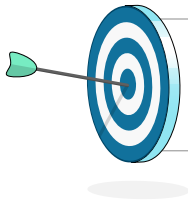
3 Automation that scales operational work instead of reducing it (scripts, manual exceptions, inconsistent standards)

WHAT CUSTOMERS OFTEN HAVE TODAY:

- Automation exists, but is frequently built with **scripts, custom jobs, or loosely governed APIs**.
- Over time, this creates:
  - Manual exceptions
  - Inconsistent error handling
  - Limited visibility into who or what triggered a transfer
- API access is often broad, making it harder to enforce least-privilege policies.
- Script-based automation often increases hidden operational risk: undocumented dependencies, inconsistent error handling, and limited audit visibility.

WHAT TO LOOK FOR AND WHY IT MATTERS:

- Policy-driven workflow automation with governed APIs, not scattered collections of scripts, ad-hoc jobs, or broadly permissioned integrations.
- Governed automation platforms to reduce manual exceptions and enforce standards by design.



Solutions that support scoped API access and centralized workflow orchestration help automation become easier manage as the organization grows, not harder.

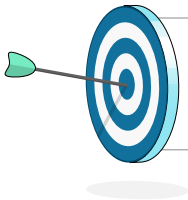
4 Audit evidence that exists, but isn't "clean"
(hard to prove integrity or correlate to workflows)

WHAT CUSTOMERS OFTEN HAVE TODAY:

- Logs do exist, but are often:
  - Stored separately from workflows
  - Difficult to correlate across systems
  - Hard to prove have not been altered
- During audits, teams spend a significant amount of time **manually assembling evidence** instead of producing it directly.
- This creates difficulties and delays in investigating and identifying security-related issues.

WHAT TO LOOK FOR AND WHY IT MATTERS:

- Tamper-evident audit evidence that is directly tied to workflows, users, and outcomes, not just raw logs.
- Platforms that produce tamper-evident, workflow-aware audit trails, as they significantly reduce audit preparation time and risks. During audits or investigations, teams need to prove not only what happened, but that records haven't been altered.



This readily available proof is especially important in regulated environments where auditors increasingly expect integrity controls, not just activity logs.

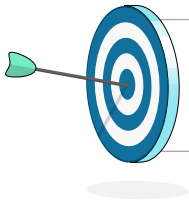
5 Security controls that are bolted on late
(e.g., adding a WAF after exposure concerns arise)

WHAT CUSTOMERS OFTEN HAVE TODAY:

- Core MFT functionality is deployed first; **additional security layers are added later**, as requirements evolve or risks become more visible. This can increase complexity and operational overhead over time.
- Example: MOVEit positions a purpose-built WAF as an option to help protect MOVEit Transfer servers from malicious traffic.

WHAT TO LOOK FOR AND WHY IT MATTERS:

- Security controls that are designed into the MFT platform—including traffic controls and content inspection—rather than added later as external compensating layers.
- Platforms that integrate security controls directly into the transfer flow reduce tool sprawl and simplify ongoing operations When security is layered on after deployment, complexity and operational overhead increase.



Native support for content scanning and traffic filtering allows security teams to manage risk inside the MFT platform instead of stitching together multiple point solutions and adding complexity.

Modern MFT Capabilities Buyers Should Demand

(Regardless of Vendor)

Use this as your internal requirement baseline to guide both evaluation and decision-making. It should help ensure consistency across teams and prevent critical capabilities from being overlooked. In our experience, organizations that formalize these requirements early are better positioned to avoid gaps and rework later in their MFT lifecycle.

Governance & Proof

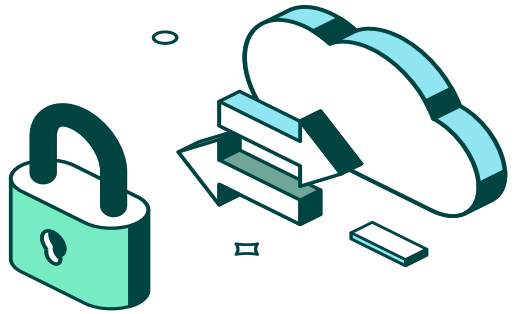
- Tamper-proof audit evidence (not just "logs exist")
- Clear, centralized admin model (browser-based admin can reduce operational friction for distributed teams).

Governance is only as strong as the evidence behind it. Clean, provable audit trails and centralized administration reduce compliance friction and operational risk.

Perimeter & Segmentation

- A documented DMZ gateway or reverse-proxy architecture, with clarity on supported proxied protocols (FTP/FTPS/SFTP/HTTP/HTTPS).
- Clear protocol support through the perimeter component

A standardized perimeter model simplifies security reviews and makes it easier to apply consistent controls across the enterprise.



Automation That's Safe

- API keys/tokens with scope control (and optional source IP restriction where available)
- Workflow automation designed to replace scripts, not coexist with them; remote execution options for distributed environments (agents)

Automation should reduce risk and effort, not create new blind spots.

Security Controls That Scale

- Content scanning (ICAP) integrated into AV/DLP content workflows
- IP reputation/traffic filtering to reduce exposure before threats reach core systems

Security controls are most effective when they're embedded directly in the data flow.

Deployment Flexibility

- On-prem + SaaS options, and modern deployment support (e.g., Docker)
- Modern deployment options that align with cloud and platform strategies

MFT often outlives infrastructure decisions. Flexibility reduces future migration pressure.

A Simple, Easy, and Low-Friction Next Step

For your MFT Security and Automation Environment

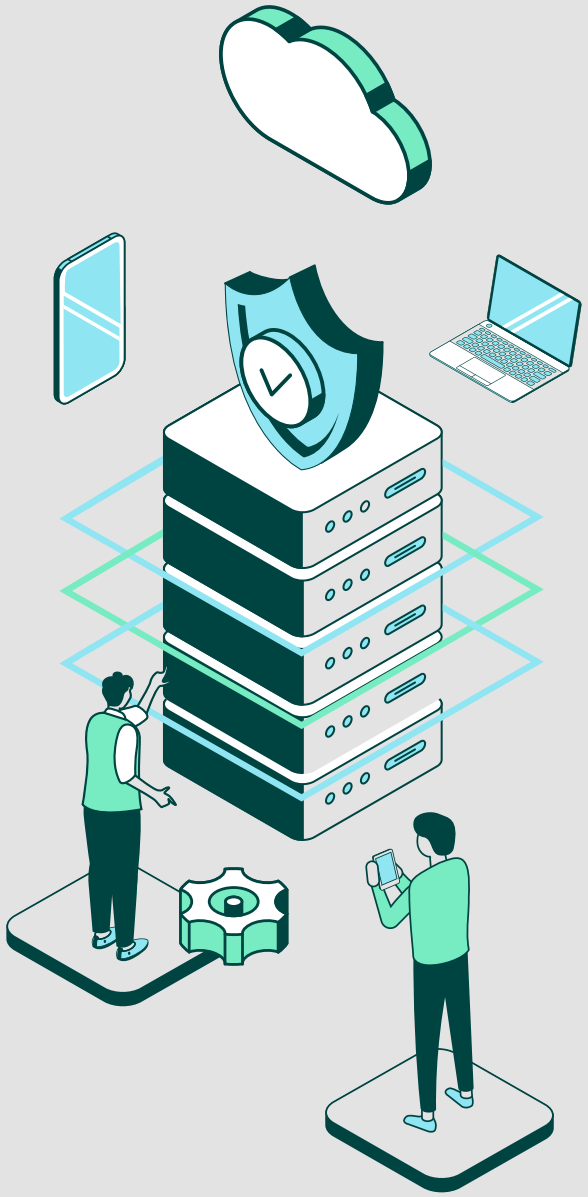
Schedule an Assessment Call (20–30 minutes)**:**

We'll map your current environment to a **modern evaluation checklist**, covering:

- Protocols actually in use + future needs (AS2/PeSIT/Connect:Direct/SharePoint, etc.)
- DMZ architecture (Edge/Gateway), supported flows, and operational model
- Audit evidence requirements (including tamper-evident options)
- API governance and automation controls (scoped keys, optional IP restrictions)
- Optional controls: ICAP scanning + IP reputation filtering

Outcome: You will get a short list of gaps, risks, and modernization options (with no rip-and-replace assumptions).

SCHEDULE TODAY



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.