FORTRA MFT
Globalscape

WHITEPAPER

One Organization. Different Security Needs.

Establishing a shared framework for secure data exchange across the enterprise

Executive Summary

Every department moves sensitive information, but the information they handle, the risks they manage, and the demands placed on them differ.

Sensitive information takes many forms across an organization. From employee and financial data to contracts, customer information, supplier records, and logistics data, each department has its own requirements for keeping information secure and moving it where it needs to go.

These activities support different business objectives, yet they rely on a shared foundation: information must move securely, reliably, and with appropriate visibility and control.

As departments adopt tools and workflows to meet immediate needs, organizations can accumulate a fragmented mix of email attachments, shared folders, FTP servers, scripts, cloud-sharing services, and application-specific exchanges. Each workflow may serve a legitimate purpose, while the overall environment becomes harder to monitor and govern.

$4.99M GLOBAL AVG. COST DATA BREACH

The implications of ineffective governance continue to grow. According to IBM's *2026 Cost of a Data Breach Report*,[1] the global average cost of a data breach reached USD 4.99 million, a 12% increase over the previous year. The average cost for U.S. organizations reached $11.5 million.

An enterprise Managed File Transfer (MFT) strategy helps organizations address this challenge. It provides a common framework for security, automation, visibility, and governance while supporting different departmental requirements.

This whitepaper explores those requirements and outlines a practical approach to bringing sensitive and business-critical file exchanges under more consistent control.

Different Departments. Different Business Priorities.

Every department moves information, but each evaluates risk through a different business lens. For IT and security leaders, the challenge is not supporting a single file transfer process. It is managing numerous business workflows, each with its own data, stakeholders, schedules, regulatory obligations, and operational consequences.

Human Resources

Employee Privacy and Trust

Human Resources exchanges employee records, payroll files, benefits information, recruitment documentation, and onboarding materials. These files often contain personally identifiable information (PII) and may move between internal teams and external service providers.

The priority is to protect employee privacy while keeping essential processes on schedule. Manual handling and uncontrolled sharing can expose sensitive information, delay payroll or benefits administration, and make it difficult to establish who accessed or transferred a file. HR needs controlled access, secure exchanges, and traceable activity across employee-data workflows.

Finance

Accuracy, Accountability, and Timing

Finance teams exchange payment instructions, banking files, invoices, tax documents, and financial reports. Many transfers support recurring processes with specific deadlines.

A delayed or failed transfer can interrupt payment cycles, create reconciliation work, and require urgent manual intervention. Limited visibility can make it difficult to confirm delivery or provide evidence during an audit.

Finance needs reliable exchanges, automation, delivery visibility, and clear records of transfer activity.

Legal

Confidentiality and Control

Legal departments exchange contracts, regulatory filings, intellectual property, litigation documents, and privileged information with internal stakeholders, external counsel, regulators, and other parties.

Their priority is to maintain confidentiality and appropriate control over sensitive exchanges. Disconnected sharing methods can make access management and traceability more difficult, increasing the effort required to investigate an issue or demonstrate how information was handled.

Legal needs restricted access, secure transfer methods, and records that support accountability and governance.

Sales

Customer Confidentiality and Commercial Agility

Sales teams exchange proposals, pricing documents, agreements, and customer information with prospects, customers, partners, and internal stakeholders.

These exchanges often combine commercially sensitive information with time-sensitive commitments. Ad hoc sharing practices can expose confidential files, reduce traceability, and delay exchanges that support customer relationships and the sales cycle.

Sales needs secure, practical ways to exchange sensitive files while keeping commercial activity moving.

Procurement

Supplier Confidentiality and Purchasing Continuity

Procurement teams exchange purchase orders, supplier contracts, banking details, onboarding documentation, and other purchasing information.

Their priority is to keep supplier exchanges secure, controlled, and on schedule. Manual processes, inconsistent permissions, and limited visibility can expose sensitive supplier information and create purchasing delays or additional follow-up.

Procurement needs controlled supplier access, repeatable transfer workflows, and an auditable record of exchanges.

Operations & Supply Chain

Scale and Continuity

Operations & Supply Chain teams depend on information moving among manufacturing systems, warehouses, distributors, logistics providers, customers, and internal applications.

These exchanges may be automated, high-volume, and closely tied to production schedules, stock availability, or shipment deadlines. A failed or delayed transfer can prevent downstream processes from completing their work.

Operations & Supply Chain teams need reliable automation, delivery monitoring, and timely alerts when intervention is required.

IT & Security

Enterprise Visibility and Oversight

IT & Security supports these departments while overseeing the broader file transfer environment.

The team needs visibility across workflows, systems, users, and external connections.

Responsibilities may include access management, monitoring, operational support, incident investigation, auditability, and policy enforcement.

A shared MFT approach helps IT & Security apply consistent controls while working with business owners to address the requirements of individual workflows.

Different Departments. Different Consequences.

Department	Sensitive information	Business impact if exchanges fail or are insecure	Priority requirements
Human Resources	Employee records, payroll, benefits, and recruitment data	Exposure of employee information; payroll or benefit delays	Access control, encryption, and auditability
Finance	Payments, banking information, invoices, and financial reports	Delayed payments, reconciliation work, and financial disruption	Reliability, automation and traceability
Legal	Contracts, regulatory filings, intellectual property, and privileged information	Exposure of confidential information; increased legal and compliance risk	Restricted access, secure delivery, and governance
Sales	Proposals, pricing, agreements, and customer information	Exposure of sensitive information; delayed commercial exchanges	Access control, secure delivery, and traceability
Procurement	Purchase orders, supplier contracts, banking details, and onboarding files	Exposure of supplier information; purchasing delays and manual follow-up	Controlled access, automation, and auditability
Operations & Supply Chain	Supplier, manufacturing, logistics, inventory, and customer data	Production delays, shipment disruption, or downstream operational impact	Automation, reliability, and monitoring

The Enterprise Challenge: Fragmented Exchanges, Fragmented Oversight

File transfer environments often develop one workflow at a time. A department introduces a sharing tool, an administrator creates a script, or a business application establishes a connection with an external provider.

Over time, these exchanges can become distributed across technologies and teams.

Controls may vary. Monitoring may be incomplete. Ownership and escalation procedures may be unclear.

When a transfer fails, teams may need to check several systems before understanding the cause and business impact. When an audit or investigation requires evidence, relevant records may be scattered across tools and stakeholders.

The challenge is to establish consistent protection, accountability, and oversight across the different ways information moves through the organization.

Four Shared Requirements for Enterprise Data Exchange

1. Security

Sensitive files require controls appropriate to their content, destination, and business purpose.

Encryption, authentication, access permissions, and secure transfer protocols help protect exchanges between users, systems, and external parties. Organizations also need clear processes for granting, reviewing, and removing access.

The data differs by department, but every workflow needs an appropriate level of protection.

2. Automation

Manual file handling creates repetitive work and opportunities for delays and errors.

Automation helps teams schedule recurring transfers and process files according to defined business rules. Finance may automate banking exchanges, HR may automate payroll-provider transfers, and Operations & Supply Chain may automate inventory or logistics feeds.

Each workflow has different dependencies, but reducing unnecessary manual intervention can improve consistency and operational efficiency.

3. Visibility

Business and technical teams need to understand whether files reached their intended destinations and when action is required.

Monitoring, notifications, and reporting help teams identify failed transfers, investigate issues, and establish what happened.

Visibility also supports business owners who need confirmation that a time-sensitive exchange completed successfully.

Effective oversight connects technical transfer status with the business process that depends on it.

According to IBM's *2026 Cost of a Data Breach Report* (lifecycle findings), organizations took an average of 247 days to identify and contain a data breach.

4. Governance

Governance establishes ownership, expectations, and accountability.

Common policies, access controls, audit trails, and reporting help organizations manage file transfer as an enterprise capability. Defined responsibilities and escalation procedures help teams respond when an exchange fails or requirements change.

Consistent governance supports departmental flexibility within an agreed framework.

Together, security, automation, visibility, and governance create a shared foundation.

Departments can continue to operate according to their business needs, while the organization maintains greater confidence in how sensitive information is exchanged.

MFT in Practice: A Shared Foundation for Different Workflows

Consider an organization exchanging payroll files with an HR provider, payment files with banks, confidential documents with external counsel, proposals with customers, purchase orders with suppliers, and inventory data with logistics partners.

Each of these workflows differ in timing, sensitivity, volume, and operational dependencies.

However, a shared MFT framework helps the organization answer consistent questions across them:

- Who is authorized to send, receive, or access the files?
- How is the information protected?
- Did the transfer complete successfully?
- Who is notified when something fails?
- Can the organization retrieve a reliable record of activity?
- Who owns the workflow and its business outcome?

When answered and addressed, business functions retain processes suited to their responsibilities, while IT & Security gains a more consistent way to oversee those exchanges.

Building an Enterprise MFT Strategy

Developing an enterprise MFT strategy begins with understanding how information moves through the organization. In many environments, file transfer practices have evolved department by department, resulting in a mix of technologies, manual processes, custom scripts, and individual solutions.

The following steps can help organizations assess their current approach and prioritize improvements:

1

Map the workflows

Identify participating departments, business owners, data types, systems, external parties, transfer methods, schedules, and dependencies.

Include both automated exchanges and processes that still rely on individual employees.

2

Prioritize business impact

Focus first on workflows that involve sensitive information, critical deadlines, significant manual handling, limited monitoring, or unclear ownership.

Ask what would happen if a transfer was delayed, failed, or reached an unauthorized recipient.

3

Involve business owners and IT & Security

Business stakeholders understand the operational consequences. And IT & Security can assess technical requirements, access controls, integration needs, monitoring, and governance.

Together, they can define practical success criteria and select an appropriate starting point.

4

Establish and measure the first use case

Begin with a manageable workflow where improvement can be assessed. Relevant measures may include manual effort, transfer success, time to detect failures, and effort required to retrieve audit records.

5

Extend the approach

Use the lessons from the initial workflow to evaluate additional departments, sites, systems, and external relationships. Assess each new use case against its own business and technical requirements.

Conclusion

Different departments will continue to have different security, operational, and compliance priorities. A shared MFT framework helps organizations support those differences while improving consistency in how sensitive information is protected, automated, monitored, and governed.

The opportunity is enterprise-wide: protect employee and customer information, support reliable financial and operational processes, strengthen supplier exchanges, and give IT & Security clearer oversight.

One organization. Different security needs. One shared foundation for secure data exchange.

Build a More Unified Approach to Secure Data Exchange

Talk to a Fortra MFT expert about your departmental workflows and how Globalscape EFT can help improve security, automation, visibility, and governance across your organization.

CONTACT US

Sources
1. IBM, Cost of a Data Breach Report 2026.
   The report states that the global average cost of a data breach reached $4.99 million, a 12% year-over-year increase and a record high. IBM's associated announcement states that $4.99 million was the global average; the U.S. average of $11.5 million is also reported in the 2026 findings. View IBM's 2026 report.
2. IBM, Cost of a Data Breach Report 2026, lifecycle findings.
   The reported mean time to identify and contain a breach increased to 247 days, reversing five consecutive years of improvement. Review the documented 2026 findings.

FORTRA. MFT
Globalscape®

About Globalscape MFT

Fortra's Globalscape is recognized for consistently providing Windows-centric organizations with top-notch solutions for securing and automating file transfers. For more than 25 years, organizations around the globe have continued to rely on us to support their mission-critical business processes, enabling them to securely transfer millions of files a month between systems, trading partners, databases and more.

globalscape.com

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.