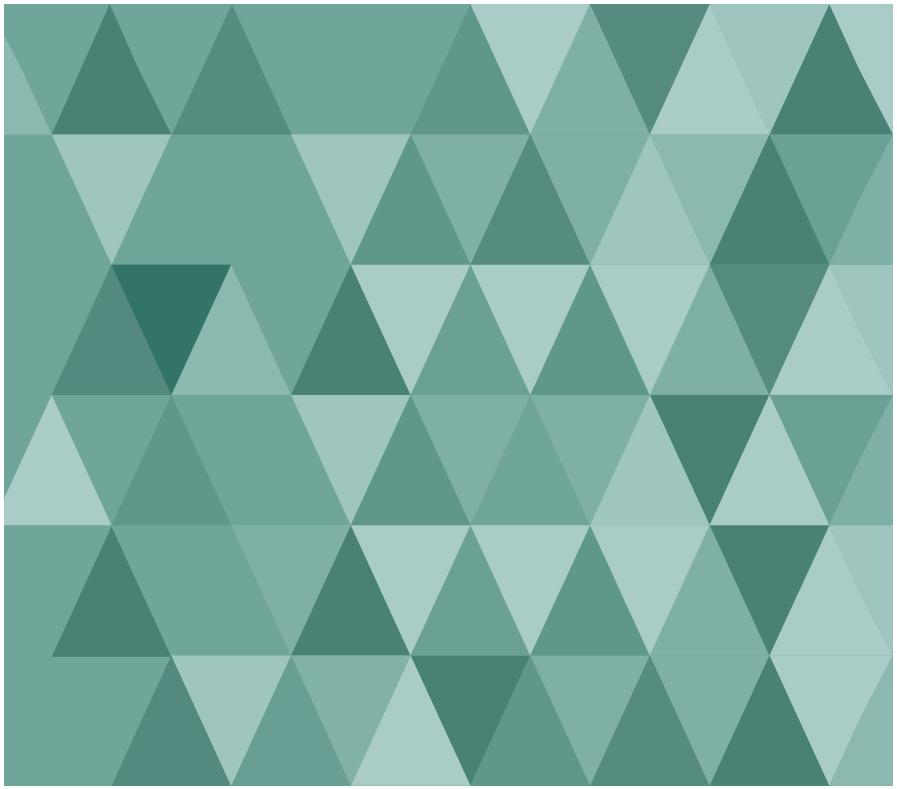
FORTRA MFT Globalscape

Industry-Ready MFT:

Secure, Govern, and Optimize Data Exchange Across Sectors

Reduce manual work, improve compliance, and streamline workflows across your sector.

Table of Contents



Executive Summary

Managed File Transfer (MFT) has become a core part of how organizations move sensitive, business-critical data. Yet across many industries, IT teams still rely on fragmented tools, legacy FTP servers, manual scripts, and disconnected workflows to support their growing data exchange demands.

This approach is not only inefficient; it increases operational costs and risk.

Independent research from firms such as Deloitte, Accenture, and IDC shows that consolidating infrastructure, automating processes, and modernizing legacy systems can significantly reduce IT operating costs.

MFT solutions help organizations replace these fragmented processes with a more controlled, efficient approach by replacing disconnected data transfer processes with a centralized, secure platform tailored to their workflows, compliance requirements, and partner ecosystems.

But cost efficiency is only part of the story. As organizations modernize how data moves, they also reshape their risk exposure, as the threat landscape continues to evolve.

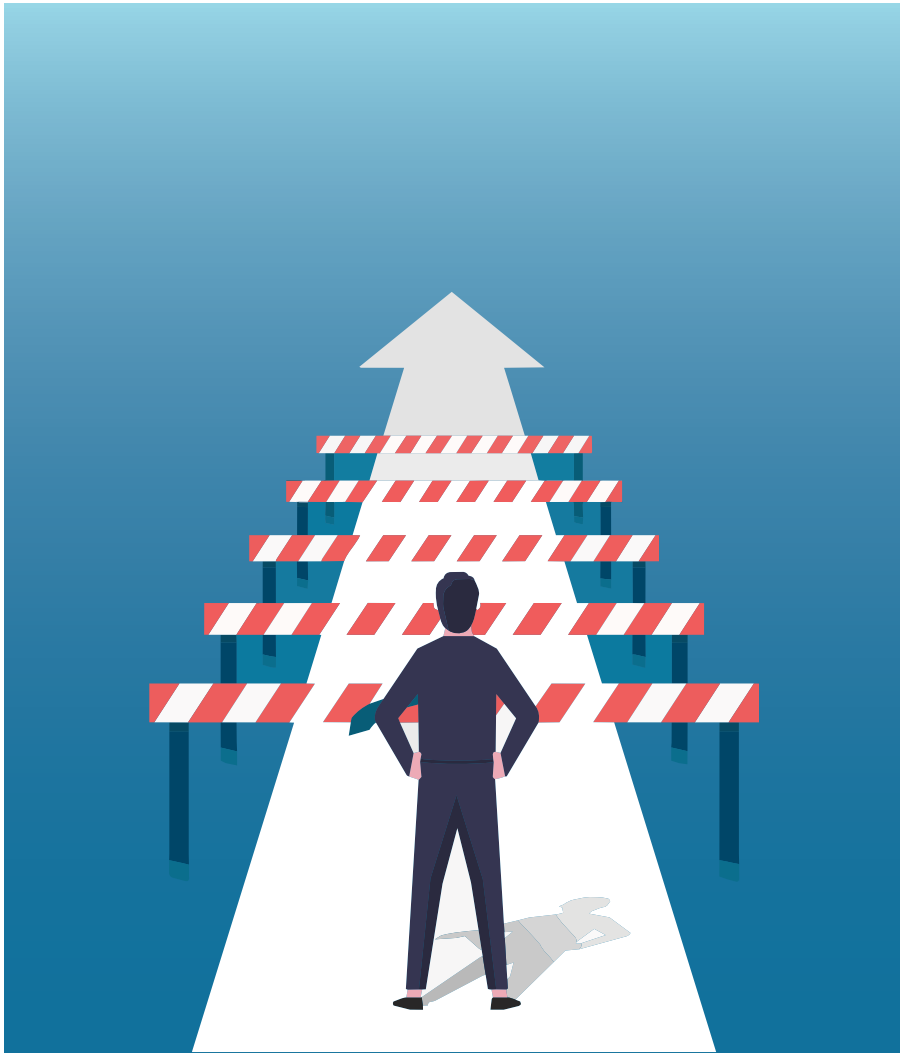
According to IBM's *2024 Cost of a Data Breach Report*, the average global cost of a data breach rose to US$4.88 million—up from US$4.45 million the previous year. For industries where sensitive data is constantly exchanged, such as with financial transactions, healthcare records, supply chain data, or citizen information, unsecured or poorly governed file transfers remain a hidden source of operational and regulatory risk.

Modern MFT platforms reduce that exposure by combining encryption, automated controls, access policies, audit trails, and secure workflows to meet the demands of each sector. Instead of relying on email attachments, legacy systems, or ad hoc solutions, organizations gain a more resilient and controlled way to manage data movement.

This guide explores how MFT delivers measurable value across a range of industries, including:

Each of these industries face unique challenges—from regulatory compliance and audit pressure to high-volume transfers and complex partner ecosystems. By aligning MFT capabilities to sector-specific requirements, organizations can improve security, streamline operations, and better support business growth.

This guide looks at how modern MFT solutions go beyond simple file transfer to serve as a foundation for secure, efficient, and scalable data exchange across industries.



Where MFT Makes the Difference:

Industry-Specific Challenges and Outcomes

MFT plays an important role in how organizations manage sensitive data, but its impact varies by industry. Each sector operates under different regulatory, operational, and data requirements which shape how file transfer is implemented and managed in practice.

As a result, the challenges and the resulting value of MFT look different in practice, depending on the environment.

The following sections break down how MFT supports specific industries, highlighting where common approaches fall short and where a more modern, purpose-built strategy can make a measurable difference.

Where MFT Delivers Value to Financial Services, Banking, and Insurance

Financial services, banking, and insurance organizations rely on the constant exchange of highly sensitive data, from payment transactions and loan documentation to claims processing and regulatory reporting. These environments are also defined by strict compliance requirements, high transaction volumes, and the need for absolute accuracy and traceability in every data exchange.

In this sector, Managed File Transfer (MFT) acts as a critical control layer for both operations and security. In lieu of manual processes or fragmented tools, financial institutions use MFT to centralize and standardize how data moves across systems, partners, and networks.

Common use cases include:

- ✓ **Secure payment and transaction processing**, including settlement files and financial records
- ✓ **Loan and mortgage workflows**, from applications to underwriting and approvals
- ✓ **Regulatory reporting** with automated, audit-ready delivery
- ✓ **Claims and policy administration** across internal teams and external providers
- ✓ **Secure data exchange** between banks, fintech partners, clearinghouses, and third parties.

These workflows typically involve high-frequency, high-volume transfers that must be completed on time and be error-free.

Specific Industry Requirements

While many industries require secure data transfer, financial services environments place unique emphasis on:

- ☐ **Auditability and traceability:** Every transfer must be fully documented (who accessed the data, when it was moved, and under what controls).
- ☐ **Data integrity and non-repudiation:** Financial data must remain accurate and tamper-proof throughout its lifecycle.
- ☐ **High availability and operational continuity:** Downtime or failed transfers can directly impact transactions, settlements, and customer trust.
- ☐ **Complex partner ecosystems:** Financial institutions operate within interconnected networks of banks, regulators, and third-party providers, requiring standardized yet flexible exchange mechanisms.

Compliance and Regulatory Alignment

Robust MFT platforms can help financial organizations meet a range of regulatory requirements by embedding security and governance directly into file transfer workflows.

Key compliance frameworks supported include **PCI DSS, SOX, GDPR, and SOC 2** as well as internal governance standards that enforce access controls, auditing, and reporting.

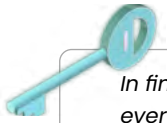
These requirements depend heavily on capabilities such as encryption, detailed logging, role-based access control, and consistent policy enforcement—all of which are central to modern MFT platforms.

Where Risks May be Found

When legacy file transfer methods, such as FTP servers, manual scripts, or disconnected point tools, financial organizations can see several critical areas of concern:

- › **Limited visibility:** Logs may exist, but they are often fragmented across systems, making audits time-consuming and incomplete.
- › **Inconsistent controls:** Security policies are applied manually or unevenly, increasing the risk of misrouted files or unauthorized access.
- › **Heavy reliance on scripting:** Custom scripts create operational complexity, are difficult to maintain, and introduce ongoing risk.
- › **Reactive security models**: Some solutions focus primarily on protocols or perimeter defenses rather than embedding controls directly into workflows.

As environments grow more complex, these gaps become harder to manage. They also are more likely to result in compliance issues or operational failures.



In financial services, secure file transfer solutions need to ensure every transaction, report, and exchange is controlled, traceable, and compliant from end to end.

Where MFT Delivers Value to Healthcare Organizations

In healthcare, MFT plays a critical role in securely moving sensitive patient and operational data across a highly interconnected ecosystem. In place of manual processes or siloed systems, healthcare organizations use MFT to centralize and standardize how data is exchanged between providers, payers, internal systems, and third-party applications.

Common use cases include:

- ✓ **Secure transfer of patient records**, including electronic health records (EHRs) and imaging files
- ✓ **Data exchange** between healthcare providers, laboratories, and insurers
- ✓ **Claims processing and billing workflows** across systems and partners
- ✓ **Secure sharing of clinical data** with external specialists and care teams
- ✓ **Integration of healthcare applications**, including EHR, ERP, and third-party platforms

In many cases, these transfers include high volumes of sensitive data that must be transferred quickly, accurately, and securely to support timely patient care.

Specific Industry Requirements

While secure data transfer is important across all industries, healthcare environments place unique emphasis on:

- ☐ **Patient data protection:** Healthcare organizations must safeguard Protected Health Information (PHI) at every stage of its lifecycle.
- ☐ **Strict access controls:** Only authorized users should have access to sensitive patient data, following "minimum necessary" access principles.
- ☐ **Data availability and timeliness:** Delays in data transfer can impact clinical decisions and patient outcomes.
- ☐ **Interoperability across systems:** Healthcare environments depend on seamless integration between a wide range of systems and providers.

Compliance and Regulatory Alignment

MFT platforms help healthcare organizations meet stringent regulatory requirements by embedding security and governance directly into file transfer processes.

Key compliance frameworks include **HIPAA, HITECH, and GDPR** — requirements that rely on capabilities such as encryption in transit and at rest, detailed audit logs, and role-based access control — to ensure data is handled securely and compliantly.

Where Risks May be Found

In healthcare environments still dependent on older tools such as FTP servers, manual processes, or disconnected systems, several risk areas can emerge:

- › **Limited visibility:** Difficulty tracking who accessed patient data and how it was transferred
- › **Manual handling of sensitive data:** Increased risk of human error and exposure
- › **Fragmented systems:** Inconsistent controls across different applications and environments
- › **Delayed detection of issues:** Problems may not be identified until after data has been exposed or misrouted

And as healthcare environments become more complex and data-driven, these gaps can directly impact both compliance and patient trust.

In healthcare, secure file transfer should ensure that sensitive patient data is protected, accessible, and fully auditable to support both compliance requirements and the timely delivery of care.

Where MFT Delivers Value to Manufacturing Organizations

In manufacturing environments, MFT supports the secure and reliable movement of operational data across highly distributed systems. In place of manual processes or disconnected tools, manufacturers use MFT to centralize and standardize how data flows between production systems, suppliers, logistics partners, and business applications.

Common use cases include:

- ✓ **Secure exchange of production data**, including CAD files, design specifications, and engineering documentation
- ✓ **Supply chain coordination**, including orders, shipping notices, and inventory updates
- ✓ **Integration** between ERP, MES, and warehouse management systems
- ✓ **Data exchange** with suppliers, distributors, and logistics providers
- ✓ **Automated transfer** of operational reports and performance data across facilities

In many cases, this involves large file sizes and time-sensitive transfers that must be completed reliably to avoid production delays or downstream disruptions.

Specific Industry Requirements

While secure data transfer is essential across industries, manufacturing environments place unique emphasis on:

- ☐ **High-volume and large-file transfers:** Engineering files, product designs, and operational data can be large and complex, requiring efficient and reliable transfer mechanisms.
- ☐ **Always-on operations:** Manufacturing environments often run continuously, requiring file transfers to support production schedules without interruption.
- ☐ **Supply chain visibility:** Data must move seamlessly across a wide network of suppliers, partners, and logistics providers.
- ☐ **System integration:** Manufacturing relies on tightly connected systems (ERP, MES, PLM), requiring consistent and automated data exchange across platforms.

Compliance and Regulatory Alignment

Manufacturing organizations may not always be governed by a single overarching compliance framework like finance or healthcare, but they still face a range of regulatory and operational requirements depending on their sector and geography.

MFT platforms help support data protection and privacy regulations (such as **GDPR**, where applicable), as well as **industry-specific requirements** around quality, safety, or export controls. In addition, there are often **internal governance standards** for secure data handling and traceability.

These requirements depend on data transfer capabilities such as encryption, centralized logging, role-based access control, and consistent policy enforcement to help ensure sensitive intellectual property and operational data are protected.

Where Risks May be Found

When manufacturing organizations rely on legacy file transfer methods such as FTP servers, manual workflows, or fragmented tools, several risks can emerge:

- › **Limited visibility across the supply chain:** Difficulty tracking where data is moving and who has access
- › **Manual and inconsistent processes:** Increased risk of delays, errors, or misrouted files
- › **Siloed systems:** Gaps in control between production, IT, and partner environments
- › **Operational disruption:** Failed or delayed transfers can directly impact production timelines and downstream delivery

As manufacturing ecosystems become more interconnected, these risks can scale quickly across systems and partners.

In manufacturing, secure file transfer requires critical operational data to move reliably, at scale, and without disruption to support continuous production and complex supply chain coordination.

Where MFT Delivers Value to Government and Public Sector Entities

In government and public sector environments, MFT plays a critical role in securely managing the exchange of sensitive data across agencies, departments, and external stakeholders. To replace fragmented tools or manual processes, public sector organizations use MFT to centralize and standardize how information is shared to improve both security and operational efficiency.

Common use cases include:

- ✓ **Secure exchange** of citizen records, tax data, and case management information
- ✓ **Interagency data sharing** between federal, state, and local entities
- ✓ **Automated reporting and data submission** to oversight bodies
- ✓ **Secure communication** with contractors, vendors, and partner organizations
- ✓ **Transfer of large datasets** supporting public services, research, or infrastructure programs

In practice, this involves high volumes of sensitive or regulated data that must be transferred accurately, securely, and on schedule to support operations and public services.

Specific Industry Requirements

While many sectors require secure data transfer, government and public sector environments place unique emphasis on:

- ☐ **Data sovereignty and control:** Sensitive information must remain within authorized boundaries and jurisdictions.
- ☐ **Auditability and transparency:** Agencies must demonstrate full visibility into how data is accessed, shared, and managed.
- ☐ **Interagency collaboration:** Data must move securely across diverse systems and organizational structures.
- ☐ **Operational resilience:** Systems must support continuity of essential services, even during high demand or disruption.

Compliance and Regulatory Alignment

MFT platforms support government organizations by embedding security and governance directly into data transfer workflows, helping meet both regulatory and internal policy requirements.

Relevant frameworks and expectations may include data privacy regulations (e.g., **GDPR or regional equivalents**, where applicable), **public sector security standards** and **internal governance policies**, and **audit and reporting requirements** tied to transparency and accountability mandates.

These demands depend on core capabilities such as encryption, detailed logging, role-based access control, and consistent enforcement of data handling policies to ensure that sensitive information is protected and traceable throughout its lifecycle.

Where Risks May be Found

When public sector organizations scale, gaps can emerge when relying on older file transfer methods—such as FTP servers, manual processes, or siloed systems:

- › **Limited visibility across agencies:** Difficulty tracking how and where data is shared
- › **Inconsistent policy enforcement:** Security controls applied unevenly across departments
- › **Manual and fragmented processes:** Increased potential for human error or delays
- › **Exposure of sensitive data:** Higher risk of misrouted files or unauthorized access

As government environments grow more interconnected and data-driven, these challenges can impact both compliance obligations and public trust.

In government and the public sector, secure file transfer should ensure that sensitive data is shared responsibly, transparently, and in full alignment with regulatory and public accountability requirements.

Where MFT Delivers Value to Defense Organizations

In defense environments, MFT is not just about enabling data exchange—it is a critical component of protecting national security information and maintaining operational control across highly restricted environments. Defense organizations use MFT to enforce strict governance over how data moves between classified systems, secure networks, and external partners.

Common use cases include:

- ✓ **Secure transfer** of classified and sensitive mission data across systems and environments
- ✓ **Exchange** of intelligence, operational reports, and situational data
- ✓ **Coordination** with defense contractors and supply chain partners under strict controls
- ✓ **Movement of large datasets** for simulation, engineering, and weapons systems development
- ✓ **Controlled transfers across network boundaries**, including cross-domain and air-gapped environments

These processes involve highly sensitive data that must be handled with precision, ensuring strict enforcement of policies at every stage of transfer.

Specific Industry Requirements

While public sector organizations focus on transparency and interagency collaboration, defense environments are uniquely defined by:

- ☐ **Data classification and compartmentalization:** Information must be handled according to strict clearance levels, with access tightly restricted based on need-to-know.
- ☐ **Cross-domain security:** Data often needs to move between environments with different classification levels without exposing protected systems.
- ☐ **Zero-trust enforcement:** Every transfer, user, and endpoint must be verified—there is no implicit trust within the environment.
- ☐ **Mission assurance and resilience:** Systems must operate reliably under all conditions, where disruption can impact mission readiness and national security.

Compliance and Regulatory Alignment

Defense organizations operate under highly specialized and stringent regulatory frameworks focused on protecting controlled and classified information.

MFT platforms support requirements such as:

- **ITAR** (International Traffic in Arms Regulations) — Controlling access to defense-related technical data
- **CMMC** (Cybersecurity Maturity Model Certification) — Enforcing cybersecurity practices across the defense supply chain
- **NIST frameworks** (e.g., NIST 800-53) — Defining security controls for federal information systems
- **Internal defense policies governing classified data** handling, access control, and auditability

Meeting these requirements relies on capabilities such as strong encryption, granular access controls, detailed auditing, and consistent policy enforcement throughout every transfer.

Where Risks May be Found

If defense organizations rely on legacy or fragmented solutions, several critical risks can emerge:

- › **Breakdown at security boundaries:** Inadequate controls when moving data across classified environments
- › **Limited control over data flow:** Inability to enforce consistent policies across systems and networks
- › **Manual or script-driven processes:** Increased likelihood of misconfiguration or unintended exposure
- › **Gaps in auditability:** Difficulty proving how sensitive or classified data was accessed and transferred

Given the sensitivity of defense operations, even minor gaps in control can have significant consequences.

In defense environments, secure file transfer must enforce strict classification, control, and boundary protection—ensuring sensitive data is governed with precision across every system, network, and partner.

Where MFT Delivers Value to Retail and Logistics Organizations

In retail and logistics environments, MFT supports the fast, secure, and reliable movement of data across highly dynamic and interconnected ecosystems. Moving beyond manual processes or fragmented tools, organizations use MFT to centralize and standardize data exchange across suppliers, distribution networks, eCommerce platforms, and internal systems.

Common use cases include:

- ✓ **Order processing and fulfillment data** between eCommerce platforms, warehouses, and partners
- ✓ **Inventory and supply chain updates** across suppliers, distributors, and retail locations
- ✓ **Shipment tracking and logistics coordination** across transportation networks
- ✓ **Secure exchange** of customer, payment, and operational data across systems

These processes often operate in near real time and at high volume, where delays or errors can quickly impact fulfillment, delivery timelines, and customer experience.

Specific Industry Requirements

While many industries depend on secure file transfer, retail and logistics environments place unique emphasis on:

- ☐ **Speed and timeliness:** Data must move quickly to support order fulfillment, shipping, and real-time inventory visibility.
- ☐ **High transaction volume:** Systems must handle large numbers of transactions daily, especially during peak periods (e.g., holidays or promotions).
- ☐ **End-to-end supply chain visibility:** Data must flow consistently across suppliers, warehouses, carriers, and retail endpoints.
- ☐ **System interoperability:** Retail and logistics operations rely on tight integration across eCommerce, ERP, warehouse, and transportation systems.

Compliance and Regulatory Alignment

Retail and logistics organizations must meet data protection and payment security requirements while maintaining operational efficiency.

Relevant frameworks include **PCI DSS**, data privacy regulations (e.g., **GDPR**, where applicable), as well as **internal governance standards** designed to enforce secure data handling, access control, and reporting

MFT platforms support these requirements through encryption, audit logging, role-based access control, and automated workflows that require consistent policy enforcement across high-volume operations.

Where Risks May be Found

When legacy file transfer methods or disconnected systems are still in place for retail and logistics organizations several key risks can emerge:

- › **Lack of visibility across the supply chain:** Difficulty tracking data movement between partners and systems
- › **Transfer delays or failures:** Disruptions that affect order fulfillment, shipping, and inventory accuracy
- › **Manual processes and workarounds:** Increased likelihood of errors and inefficiencies at scale
- › **Inconsistent security controls:** Exposure of customer or payment data due to uneven policy enforcement

As operations scale and supply chains become more complex, these issues can quickly impact both operational performance and customer satisfaction.

In retail and logistics, secure file transfer must ensure fast, reliable, and fully controlled data movement to keep supply chains running smoothly and customer experiences consistent.

Where MFT Delivers Value to Utilities Organizations

In utilities environments, MFT enables the secure and reliable exchange of operational data across critical infrastructure systems, field operations, and partner networks. Instead of relying on fragmented tools or manual processes, utilities organizations use MFT to centralize and standardize how data moves between control systems, enterprise applications, and external stakeholders.

Common use cases include:

- ✓ **Secure transfer** of operational data from SCADA and field systems
- ✓ **Data exchange** between generation, transmission, and distribution systems
- ✓ **Integration** between operational technologies (OT) and IT systems (e.g., ERP, analytics platforms)
- ✓ **Reporting and data submission** to regulatory bodies
- ✓ **Secure coordination** with contractors, service providers, and partner organizations

These exchanges are often continuous, high-frequency data flows that must remain accurate and uninterrupted to support critical infrastructure operations.

Specific Industry Requirements

While many industries require secure data transfer, utilities environments are uniquely defined by:

- ☐ **Operational continuity:** Systems must support always-on services where disruptions can impact power, water, or energy delivery.
- ☐ **IT/OT integration:** Data must move securely between operational systems (e.g., SCADA) and enterprise IT environments without introducing risk.
- ☐ **Infrastructure resilience:** Transfers must be reliable even across distributed, remote, or bandwidth-constrained environments.
- ☐ **Controlled data flow:** Sensitive operational data must be carefully managed to prevent unauthorized access or disruption.

Compliance and Regulatory Alignment

Utilities organizations operate under strict regulatory and security frameworks designed to protect critical infrastructure and sensitive operational data.

MFT platforms help support requirements such as **NERC CIP, regional and national cybersecurity regulations** for utility providers, **data privacy regulations** (e.g., **GDPR**, where applicable), and **internal governance** and **audit requirements** for data handling and system access

These requirements rely on capabilities such as encryption, centralized logging, role-based access control, and consistent enforcement of policies across IT and OT environments.

Where Risks May be Found

In utility environments still dependent on older tools or disconnected systems, several risks can emerge:

- › **Breakdowns between IT and OT systems:** Gaps in visibility and control across environments
- › **Operational disruption:** Failed or delayed transfers impacting real-time operations
- › **Limited auditability:** Difficulty tracking how sensitive operational data is shared
- › **Manual or inconsistent processes:** Increased risk of human error and misconfiguration

As infrastructure becomes more interconnected and data-driven, these risks can affect both system reliability and regulatory compliance..

In utilities, secure file transfer needs to ensure continuous, controlled, and resilient data movement across critical infrastructure—supporting reliable service delivery and regulatory compliance.

Where MFT Delivers Value to Telecommunications Organizations

In telecommunications environments, MFT supports the secure, high-speed movement of data across vast, distributed networks. In place of fragmented tools or manual processes, telecom providers use MFT to centralize and standardize how data is exchanged between network systems, business platforms, partners, and customers.

Common use cases include:

- ✓ **Secure transfer** of network data, including performance metrics, logs, and usage records
- ✓ **Data exchange** between billing systems, customer platforms, and operational systems
- ✓ **Automated delivery** of subscriber data, invoices, and service records
- ✓ **Integration** between OSS/BSS systems, cloud platforms, and external partners
- ✓ **Secure sharing of large datasets** supporting analytics, reporting, and network optimization

These processes often operate at extremely high volumes and speeds, where delays or failures can impact service delivery, billing accuracy, and customer experience.

Specific Industry Requirements

While many industries depend on secure data transfer, telecommunications environments are uniquely defined by:

- ☐ **High-volume, real-time data exchange:** Telecom networks generate continuous streams of data that must be processed and transferred without delay.
- ☐ **Distributed infrastructure:** Data must move securely across geographically dispersed systems, including edge, cloud, and on-prem environments.
- ☐ **Network reliability and uptime:** Transfers must support always-on services where interruptions can affect connectivity and customer experience.
- ☐ **System interoperability at scale:** Telecom providers rely on complex ecosystems of OSS, BSS, and partner platforms that must exchange data seamlessly.

Compliance and Regulatory Alignment

Telecommunications organizations must meet a range of regulatory and data protection requirements while maintaining performance and reliability.

Relevant frameworks may include data privacy regulations (e.g., **GDPR**, where applicable) governing subscriber data, **telecom-specific regulations** varying by region and provider, and **internal governance** and **audit requirements** for data handling, billing accuracy, and service operations

MFT platforms help meet these requirements through encryption, centralized visibility, detailed audit logging, and policy-driven controls that ensure consistent and secure data movement at scale.

Where Risks May be Found

Legacy file transfer methods can expose several risks to telecom organizations, including:

- › **Inconsistent data flow across systems:** Gaps between network, billing, and customer platforms
- › **Limited visibility into high-volume transfers:** Difficulty tracking and auditing large-scale data movement
- › **Performance bottlenecks:** Legacy systems may struggle with the scale and speed required
- › **Manual processes and scripts:** Increased risk of errors, delays, and operational inefficiencies

As telecom environments scale and become more distributed, these challenges can impact both operational efficiency and service reliability.

In telecommunications, secure file transfer must handle high-volume, real-time data movement with consistency and control—ensuring reliable service delivery across complex, distributed networks.

Where MFT Delivers Value to Big Technology Companies

In larger technology organizations, MFT supports the secure, scalable movement of data across complex, cloud-driven ecosystems. Replacing ad hoc tools or custom scripts, tech companies use MFT to centralize and standardize how data flows between applications, platforms, development environments, and partners.

Common use cases include:

- ✓ Secure exchange of application data between microservices, APIs, and backend systems
- ✓ Integration across cloud, hybrid, and on-prem environments
- ✓ Automated data pipelines for analytics, AI/ML models, and reporting
- ✓ Secure sharing of software builds, updates, and deployment artifacts
- ✓ Data exchange with partners, customers, and third-party platforms

These processes often operate continuously and at scale, where performance, reliability, and automation are essential to maintaining development velocity and service delivery.

Specific Industry Requirements

While many industries require secure data transfer, technology companies are uniquely defined by:

- ☐ **Speed and agility:** Data movement must support rapid development cycles, continuous integration, and frequent deployments.
- ☐ **Cloud and hybrid environments:** Data flows across distributed infrastructure, including multi-cloud and containerized environments.
- ☐ **Automation at scale:** File transfers must integrate seamlessly into automated workflows without manual intervention.
- ☐ **Developer and system integration:** MFT must align with APIs, DevOps pipelines, and modern application architectures.

Compliance and Regulatory Alignment

Technology companies must balance speed with strong data governance and compliance, particularly as they handle customer, application, and platform data at scale.

Relevant frameworks may include **GDPR, CCPA,** and **SOC 2** as well as **internal governance standards** for access control, auditability, and data protection

MFT platforms help meet these requirements through encryption, centralized visibility, automation, and policy-driven controls that help ensure consistent governance across fast-moving environments.

Where Risks May be Found

As systems scale in technology organizations, gaps emerge when relying on fragmented or legacy approaches:

- › **Over-reliance on custom scripts:** Increased maintenance burden and potential for security gaps
- › **Lack of centralized control:** Difficulty governing data flow across distributed systems
- › **Inconsistent security enforcement:** Policies not applied uniformly across environments
- › **Limited visibility:** Challenges tracking data movement across cloud, APIs, and services

As systems scale and architectures become more complex, these risks can slow development, increase exposure, and create operational inefficiencies.

In technology organizations, secure file transfer must support fast, automated, and scalable data movement—enabling innovation without sacrificing control, visibility, or security.

Conclusion

Across industries, the role of Managed File Transfer has evolved from a background IT function into a critical layer of security, control, and operational efficiency.

As this guide has shown, the value of MFT is not one-size-fits-all. Each sector—from financial services and healthcare to manufacturing, utilities, and telecommunications—faces distinct challenges shaped by regulatory requirements, data sensitivity, system complexity, and operational demands.

Yet a common thread remains: organizations are under increasing **pressure to move sensitive data faster, more securely, and with greater accountability**. Legacy approaches built on fragmented tools, manual processes, or script-heavy workflows often struggle to keep pace with these expectations.

Modern, industry-aligned MFT solutions address this gap by centralizing control, enforcing consistent policies, and providing the visibility needed to manage risk proactively—not just respond to it after the fact.

A sampling of companies that already trust our MFT solutions

FINANCIAL & BANKING	HEALTHCARE	TELECOMMUNICATION
BARCLAYS, Santander, HSBC, citi, LONDON STOCK EXCHANGE An LSEG Business	Cedars Sinai, DELTA DENTAL, COVIDIEN, AdventistHealth	AT&T, verizon, bouygues
MANUFACTURING	**RETAIL**	**INSURANCE**
DELL, JOHN DEERE, AIRBUS AN EADS COMPANY, SHARP, life.augmentec	pepsi, Pizza Hut, El Corte Inglés, MANGO, TOUS	MetLife, GENERALI, MAIF

What's Next?

Understanding how MFT applies to your industry is only the first step. The next is evaluating whether your current approach is built to meet today's requirements and tomorrow's demands.

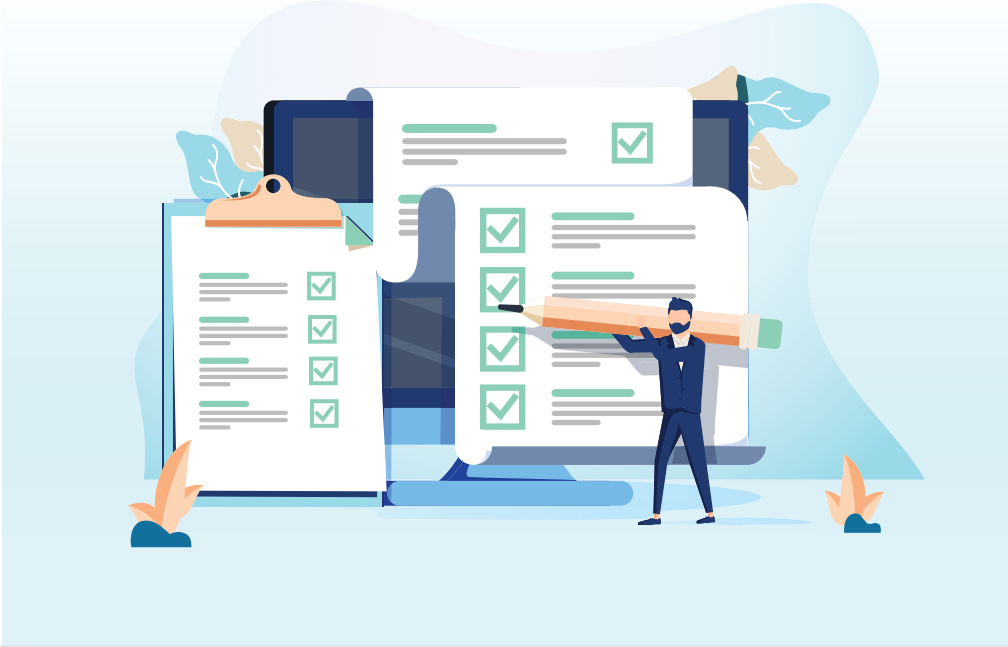
As you assess your environment, consider:

- ☐ Where are file transfer processes still fragmented, manual, or difficult to govern?
- ☐ How easily can you track, audit, and enforce policies across all data movements?
- ☐ Does your current solution reduce risk or simply document it?
- ☐ Can your file transfer strategy scale with growing data volumes, partners, and compliance needs?

The answers to these questions will help determine whether your organization is simply maintaining file transfer or actively managing it as a strategic capability.

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

Globalscape®

About Globalscape

Globalscape Enhanced File Transfer (EFT) is an enterprise MFT platform that streamlines and encrypts the exchange of data between systems, employees, customers, and trading partners. Administration is easy yet detailed enough for complete control of your file transfer system.