FORTRA

Do You Know Where Your Data Is?

Three Common Data Management Problems & How To Fix Them

Knowing the Location of Your Data Plays a Crucial Role in Keeping It Secure.

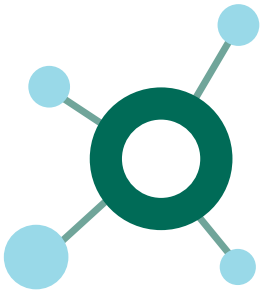
When you find yourself jumping through order to protect, manage, monitor, analyze, or report on your data, then you're not getting the most out of your IT infrastructure. Is your current IT infrastructure helping you—or hurting you?

This eBook evaluates three common data management problems that make life difficult for an organization's IT team. Keep reading for insight on how you can achieve crucial balance through proper data management techniques and a proper data management solution that helps you achieve increased security and overall operational efficiency.

Your IT infrastructure can be severely weakened when core IT requirements are not being met. If you don't know where your data is at all times, then your IT infrastructure is getting in your way. An agile, efficient, secure, and compliant IT infrastructure provides operational visibility, control, and governance.

Legacy or homegrown systems, disparate applications and systems, and shadow IT interfere with the secure and efficient management of your data and IT infrastructure.

Leaving your organization vulnerable to data breaches, compliance violations, and a wide range of operational inefficiencies.



Your IT infrastructure can be the catalyst to your success...

or it can be an endless project that depletes your employees' time and your organization's budget.

In the face of today's highly regulated and fast-paced business environment, an **organization must be able to rely on the security and efficiency** of their IT infrastructure – or they may quickly fall behind.

Three common IT infrastructures that lack the optimal level of data management and can adversely affect your security, compliance, and efficiency goals include the following:

Legacy and homegrown data exchange systems

When an old or homegrown data exchange system slows down your business growth

Disparate applications and systems

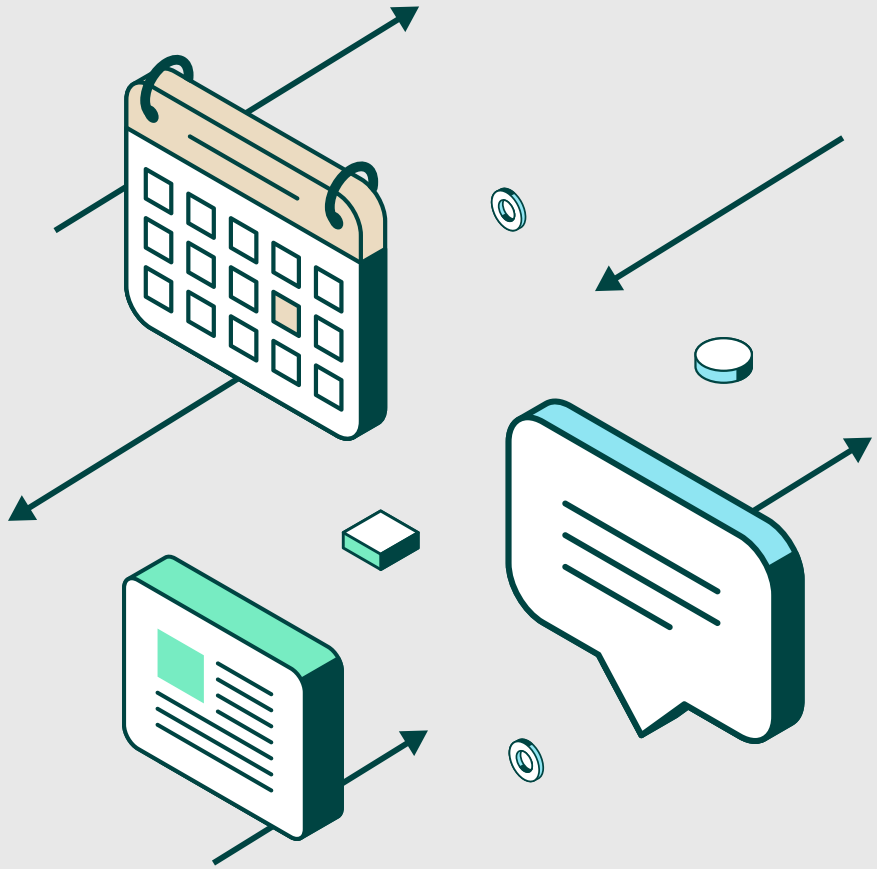
When you have multiple systems or applications moving your data, leaving you lacking a single platform to manage, protect, and track your data movement

Shadow IT

When employees use unsanctioned applications and tools that limit IT control or governance, and in turn expose an organization to security vulnerabilities

Getting Getting ahead of these common IT infrastructure challenges will require a proactive data management strategy that enables full operational visibility, control, and governance over your data exchange environment.

With the right data management strategy and tools in place, security, compliance and efficiency will always be at the forefront.



HOW TO GET OUT OF YOUR OWN WAY WITH A DATA MANAGEMENT STRATEGY

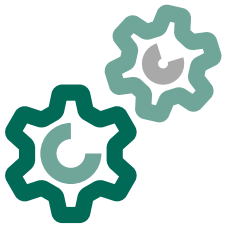
Implementing a comprehensive data management strategy means that you will valways have the upper hand and you will be able to address security or efficiency concerns before they become a serious problem. Achieving your security, compliance, and efficiency requirements means you need a comprehensive data management strategy AND a strong data management platform.

THREE COMMON IT INFRASTRUCTURE CHALLENGES THAT GET IN THE WAY

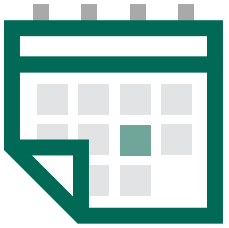
WHEN AN OLD SYSTEM SLOWS BUSINESS GROWTH

Why Legacy File Transfer Systems Are Hurting You

Not Secure



Inflexible



Time-Consuming

Legacy file transfer processes can haunt an organization with the ghosts of yesterday's codes and scripts, and languages that may no longer be current or used with today's technologies.

Legacy file transfer systems and processes often force an organization to spend excessive time training employees on how to use antiquated technologies. You're also left at the mercy of your employees and their availability to manage and maintain these systems and all that goes along with the processes they run.

Long story, short: Legacy file transfer systems get in your way because they are not secure, inflexible, and time-consuming.

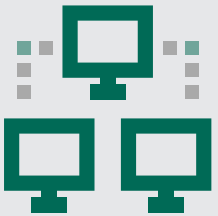
Legacy file transfer systems can be insecure
AA data breach can cost an organization
$4 million to remediate.
– Ponemon, "2016 Ponemon Cost of Data Breach Study"

Often comprised of multiple insecure FTP servers or an inflexible and haphazard home-grown file transfer system, legacy file transfer systems can expose weaknesses in an organization's IT infrastructure.

AMONG THOSE WEAKNESSES INCLUDE:

FTP SERVERS
do not secure or encrypt data in transit

FREQUENT SSL UPDATES
that likely were written after an organization's legacy file transfer scripts



DESIGNED FOR A SPECIFIC TASK,
legacy file transfer scripts may not be focused on security

Legacy file transfer systems can compromise your security efforts, risking non-compliance with industry regulations and the security of your sensitive or proprietary data, complicating business-critical workflows, and ultimately taxing your IT department.

Scalability Is Limited

Legacy file transfer systems are often inflexible and outdated, making it difficult to quickly adapt to a business and its evolving data transfer needs.

If the volume of data increases and the data transfer workflows become more complicated, a legacy file transfer system may not have the capacity to handle the change in workload.

Legacy file transfer systems lack the foundation for growth, which ultimately can slow down business growth.

Outdated Systems Complicate Data Management

Legacy systems can cost an organization an infinite amount of time and effort, which could be better spent on other IT projects.

Some outdated systems require skills that an organization's current IT staff may not have, which can limit visibility into your data, making the management of that data overly time consuming. At the same time, even when a staff member does have the scripting skills required for a legacy system, the process can be extremely time-consuming—making up an employee's entire job.

Non-integrated legacy healthcare systems that shift to an interoperable system can save taxpayers more than $30 billion usd a year on wasteful spending.
– Health IT News, "System Interoperability Provides Massive Benefits"

Troubleshooting Is More Challenging

Determining where a failed transfer went wrong can be next to impossible without visibility.

WHAT'S THE END RESULT?

FAILED FILE TRANSFERS CAN LEAD TO:

A decrease in productivity

Wasted time

Lost business opportunities

Missed SLAs

Ultimately, failed file transfers can adversely affect your overhead and profitability.

WHEN YOUR DATA IS EVERYWHERE AND NOWHERE

The Problem With Disparate Applications and Systems

Sometimes disparate systems arise as a result of a merger or an acquisition. Other times, they evolve based on the needs of the organization due to unexpected growth or a change in business direction, and the disparity between applications and systems is an end result.

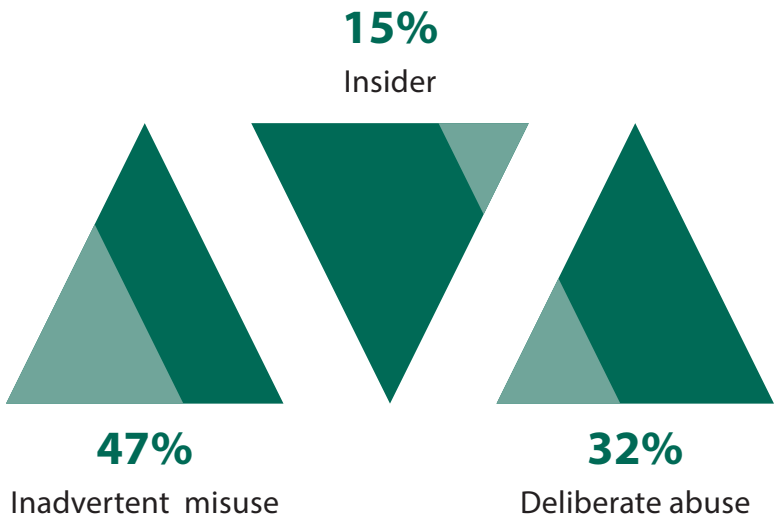
The business risk of disparate systems is just that, they are not connected and therefore interfere with operational visibility.

Without full operational visibility, your organization may be required to spend more time creating workarounds and chasing security or productivity problems. The amount of time spent trying to accomplish these tasks will not always provide you with the answer or resolution you need, but will ultimately cost your organization more money in overhead costs.

Disparate Applications and Systems Increase Your Business Risk

This lack of visibility and control has serious consequences. Disparate systems need to be unified to mitigate your business risk.

47% of security breaches were caused by either inadvertent misuse (32%) or deliberate abuse (15%) by an insider. The problem can be traced in part to a lack of control over data sharing with conventional strategies such as email, FTP and consumer-grade cloud services like Dropbox and YouSendIt.
– Network World, "Combatting Security Breaches with Managed File Transfer Technology"



Given that nearly half of all security breaches originate with an insider, points to a critical need to decrease your security risks with an IT infrastructure that enables your organization to maintain full operational visibility and control. This ensures that your organization take a proactive and preventative approach to securing your IT infrastructure and data.

Do You Want To Reduce Your Business Risk?

Consider consolidating your applications and systems into one unified platform.

Consolidation will put you back in control, ensuring that you can see and manage all data activity within your IT infrastructure. It can save you time, and help you catch productivity and security risks before they become a problem.

System Upgrades Cost Money

If your business is older than a few years, you've likely had some turnover in the IT department, meaning different IT professionals have introduced their own methods, custom coding, and software into your environment.

These scripts need to be maintained. Each piece of software must be updated regularly, and as employees and contractors move on, their knowledge of those tools moves on with them.

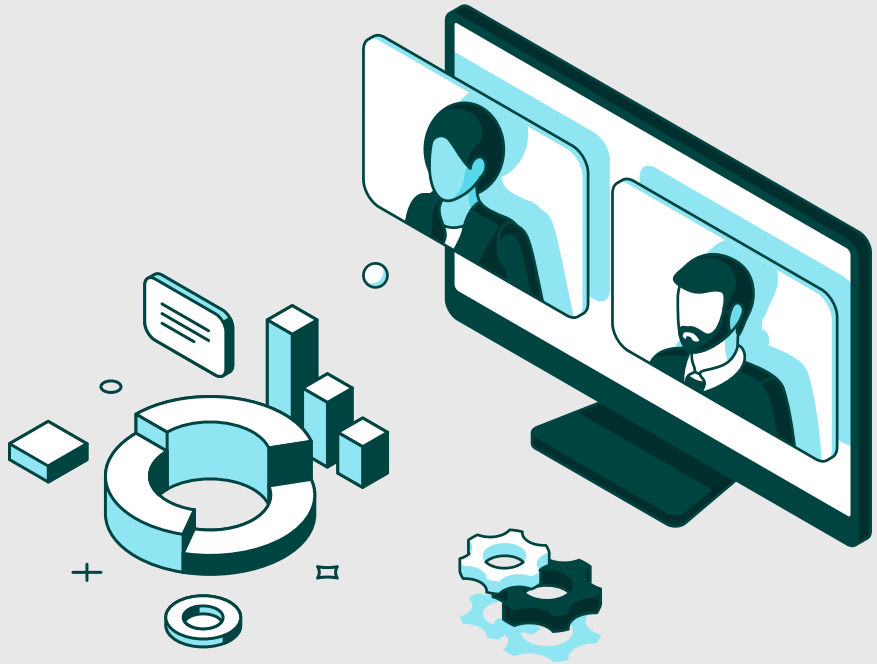
Much of the software in use might have the very same purpose, but it's installed on different systems and you may have to pay for upgrades to them. In turn, the system upgrades will not only cost you more money for the software upgrade, but also the time spent updating your system, along with the time spent by your team implementing and learning the new software.

Poor Connection With Business Partners

Data transfer requirements often vary between business partners, and vendors.

Flexibility within your IT infrastructure is crucial to accommodating to the needs of your business. When you need to connect with new partners, your system needs to have the capability to interface with their systems. Perhaps their security rules require SFTP, while your system only connects with FTP or FTTP. In that scenario, you would need another new system or piece of software to enable that communication with your new partner.

When a disparate system gets in the way of your current business needs, it can interfere with your future business opportunities.



Managing Disparate Systems Is Expensive

Managing and maintaining a disparate system is a 24/7 job that can quickly overextend your resources. Disparate systems and applications can require multiple software upgrades and platform logins. At the same time, there may also be multiple streams of data and workflows to manage.

Quite simply, sustaining a disparate system is expensive because it requires a great deal of time from your IT department.

Are your employees taxed on time? For some, outsourcing may seem like a viable option; however, that would mean incurring an additional expense outside of our budget. Aside from cost, a move to an outsourced vendor may involve moving sensitive data through a third-party vendor or partner, which may complicate your compliance and data management goals.

Do You Want To Reduce the Cost of Maintaining Your Data and It Infrastructure?

Reduce your costs and simplify the management of your data and IT infrastructure by consolidating your disparate system into one manageable platform.

Consolidation will enable you to save money in overhead, allowing your employee to use his or her time more efficiently. At the same time, you'll be able to avoid the need to use an outside vendor, which could also drive up your overhead costs.

WHEN GOOD INTENTIONS GO WRONG

The Problem With Shadow IT

On one hand, shadow IT points to the resourcefulness of an employee doing his or her very best to the get the job done and get it done quickly.

On the other hand, shadow IT exposes vulnerabilities within your organization. What are these vulnerabilities?

Shadow IT may:

Increase your risk of a data breach

Increase your overhead costs

Disrupt your IT processes and policies

Interfere with your compliance objectives

SHADOW IT IS A SECURITY RISK

"70% of unauthorized access to data is committed by an organization's own employees."
– Gigaom, "Shadow IT: Data Protection and Cloud Security"

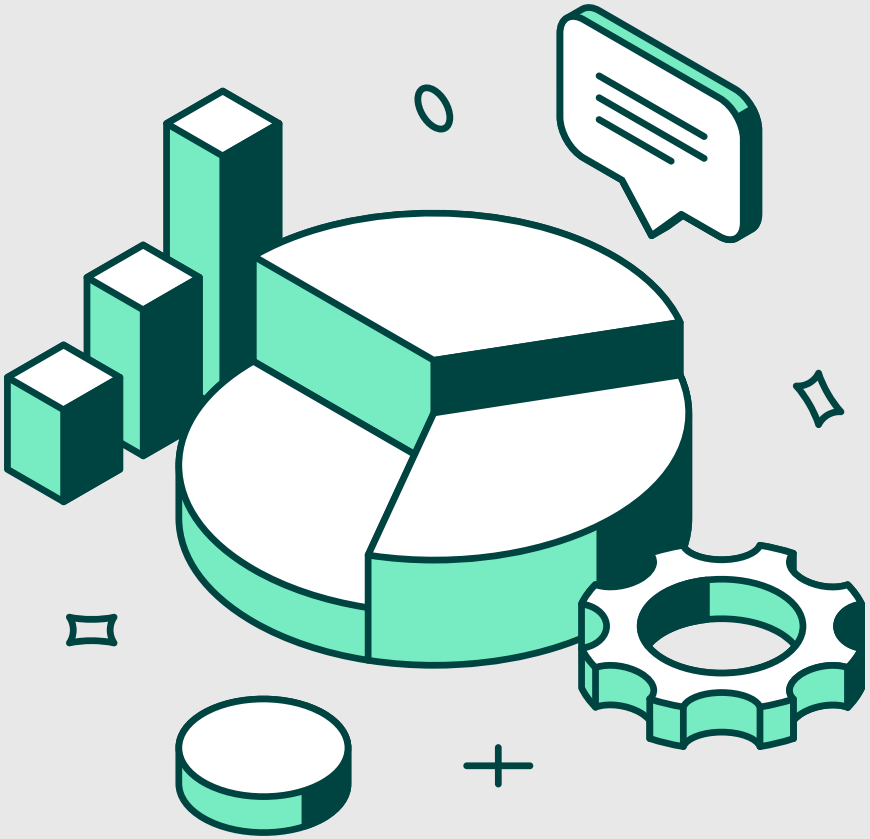
The practice of shadow IT involves the use of unsanctioned methods that employees use to move data inside and outside of an organization, outside the purview of your IT department. Common ways this happens include flash drives, unapproved web services or devices, consumer-grade file sharing services, laptops or smart devices.

Unprotected apps are often easy targets for cybercriminals looking for security vulnerabilities or new ways to target an organizations data.

Shadow IT Increases Costs

"Shadow it management accounted for 35% of total it expenditures in 2016."
– Gartner Research, 2016:
"The State of Shadow IT"

When employees provision their own IT resources there can be some degree of duplication. Collaboration with IT can eliminate duplication issues and help ensure that employees get a user friendly, secure, and compliant tool.



How Can You Prevent the Increased Shadow IT Costs?

Encourage cross-department communication and collaboration with your IT department to prevent employees from working in a silo. Doing so will ensure that employees know about existing tools and security policies. At the same time, it will help ensure that they know what to ask for and who to ask when they need new tools. As a result, you can help reduce your overhead costs and protect your bottom line.

Shadow It Disrupts Your IT Processes and Policies

Shadow IT can be very intrusive on the consistency and reliability of your organization's processes and procedures. It only takes one person to expose an organization to a data breach or compliance violation. When shadow IT interferes with business critical IT processes and policies, an organization's IT staff may quickly lose time chasing fixes for problems caused by shadow IT methods.

Communicate with employees and provide clear training and information on your security policies, the tools you have available, and the processes required when a new solution is needed.

Shadow IT Interferes With Your Compliance Objectives

Similar to disparate systems and homegrown, legacy systems, shadow IT can greatly reduce OR eliminate IT's operational visibility and control – this can increase your risk of data loss and lead to compliance violations if you manage regulated data.

Four Signs That Shadow It Is a Problem What Are the Red Flags?

A Drop in Requests or Complaints

A decline in troubleshooting tickets or requests may mean that your system is perfect, but it could also indicate that employees are seeking alternative – less secure ways of accomplishing their daily business objectives.

Regular Security Training isn't Standard

Securing your IT infrastructure must be a collaborative effort, and should involve the entire company. Ignorance is not bliss when it comes to protecting your organization's data. Most employees do not keep tabs on the latest security vulnerabilities. Keeping your employees informed and offering security training on a regular basis will ensure that everyone is on the same page.

An Overly Complex Security Policy

If the language within your security policy is overly complex, then it will be harder to implement and even harder for employees to follow. Use plain English and steer clear of technical jargon. Make it easy for your employees to comply with your security policy.

Employees are Unaware of Unsanctioned Tools and Applications

While employees may just be doing what they can to get their jobs done, they may not actually know that what they are doing puts your organization's data and IT infrastructure at risk. At the same time, they may not know about available tools and how to use them.

How To Get Ahead of Shadow IT

Evaluate Existing Processes

Evaluating your existing tools and processes will help you discover any potential shortcomings where your users are being enabled to create a shadow IT infrastructure.

Communicate with Employees

Survey or audit your employees' data management processes. Understanding why they are using work-arounds can help you determine a better route, such as more training or new tools to prevent any further shadow IT problems.

Keep it Simple

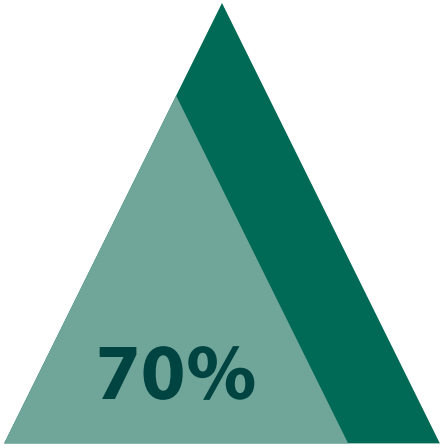
Keep communications simple, clear, and direct. Make it easy for employees to follow your security policy. Provide end-user training on the policy annually, and to all new employees.

Be sure to update the entire company on system security risks.
communicating their role in preventing those risks.

THE ULTIMATE DATA TRANSFER HEADACHE

Legacy or homegrown file transfer systems, disparate systems and applications, and shadow IT take away from your ability to provide the very best IT infrastructure for your organization, because they all may lead to failed data exchanges.

Out of the more than $78 billion total technology budget for the fiscal year 2015, 26 federal agencies spent $60 billion on legacy investments. over the past six years, this amount has continued to increase.
– U.S. Government Accountability Office (GAO)

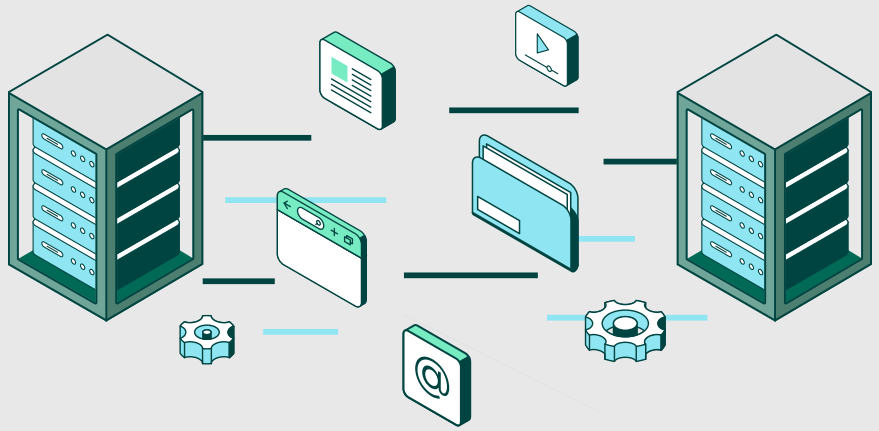


"Each year, public and private sector organizations devote around 70% of their average it budget to legacy software maintenance."
– Former US Airforce CIO and Ret. Lieutenant General William Lord
"Breaking the Cycle of Legacy IT Investment"

Failed Data Transfers Interfere With Daily Business Operations

Organizations need to securely and efficiently move data in order to operate to meet their business and compliance requirements. Any interference in their daily processes can be damaging for a business.

Without secure and efficient file transfers, employees or business partners may not be able to collaborate in a timely fashion. Medical facilities may not be able to exchange crucial and protected patient information. Organizations may not be able to process tax or payroll information.



What Happens When Data Transfers Fail

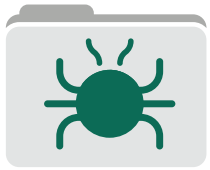
When legacy or homegrown file transfer systems, disparate applications and systems, shadow IT, latency or downtime affects your business critical data transfer processes more problems can arise, including the following:

DATA LOSS

MISSED SLAS

DATA TRANSFER INTERCEPTION

LOST REVENUE



DATA CORRUPTION

FINES DUE TO NON-COMPLIANCE

MFT to the Rescue

The managed file transfer (MFT) technology enables organizations to securely and efficiently move data within the IT infrastructure and between systems. More robust than the insecure FTP server, MFT is a powerful and secure solution that can move a high volume of data and a complex set of workflows.

Simplify and strengthen your data management capabilities with a customized managed file transfer (MFT) solution.

With a MFT solution, your IT infrastructure will better support your data transfer requirements, from a proactive and preventative data security strategy to stringent compliance regulations, in addition, to complex processes or workflows.

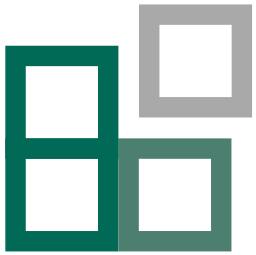
Overcome Data Transfer Challenges With a MFT Solution

The challenges that follow legacy or homegrown file transfer systems, disparate systems and applications, and shadow IT require an advanced data management solution that is inherent in a MFT technology.

With the centralized platform of a MFT solution, you can maintain full visibility and control over your IT infrastructure and move beyond the traditional IT considerations to create real opportunities to achieve:

Greater operational efficiency

An enhanced security posture



Data management integration capabilities

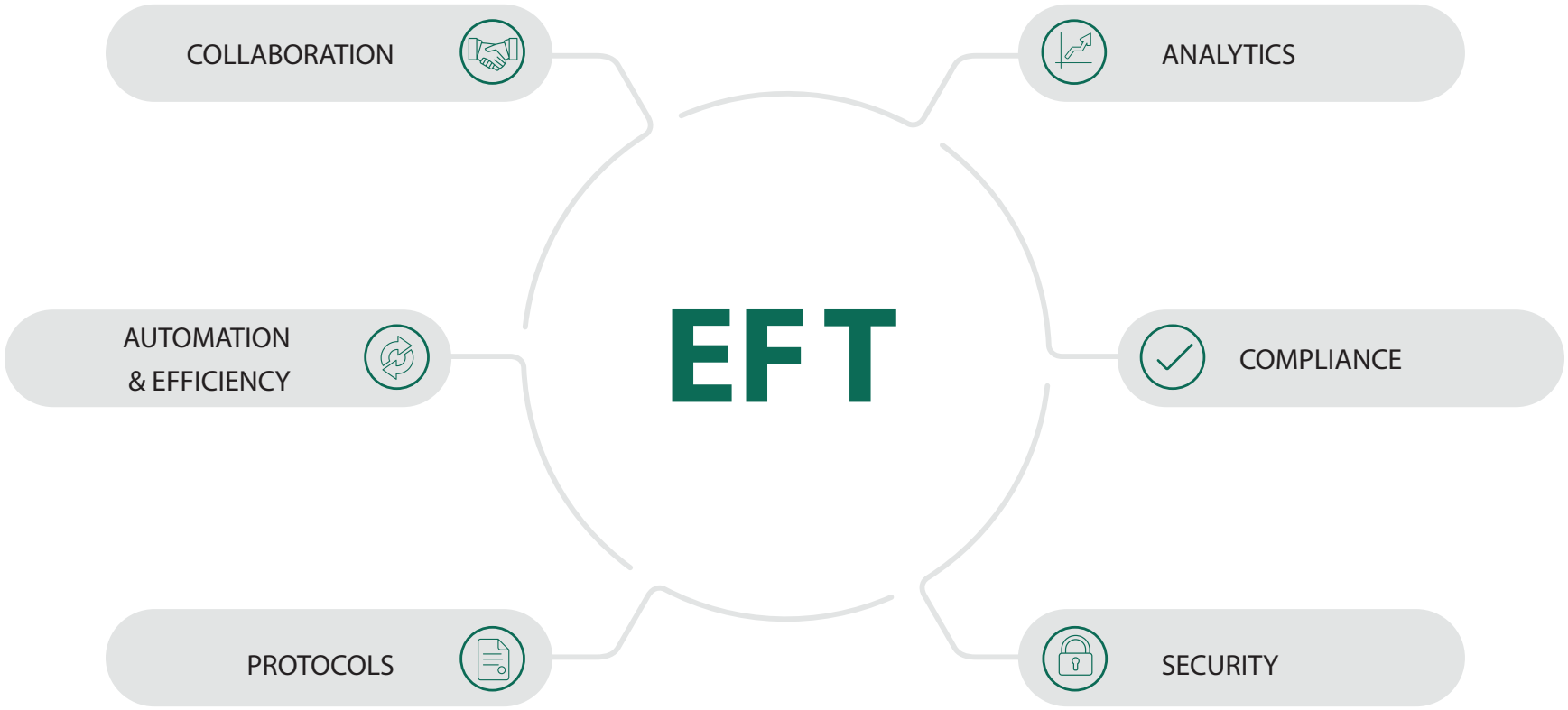
At the same time, you can produce measureable effects on ROI within your organization.

GLOBALSCAPE HELPS ORGANIZATIONS PROTECT THEIR SENSITIVE DATA AND IT INFRASTRUCTURE IN THE MOST TRANSPARENT AND PREVENTATIVE WAY.

Enhanced File Transfer™ (EFT™) is Globalscape's awardwinning MFT platform that was designed to manage data transparently, efficiently, and within the parameters of control and accessibility that you require.

EFT provides enterprise-level security for collaboration with business partners, customers, and employees, while automating the integration of back-end systems.

Built-in regulatory compliance, governance, and visibility controls help keep your data safe, while outstanding performance and scalability help boost operational efficiency and maintain business continuity. Administration is easy, yet granular enough for complete control of your file transfer system.



With EFT, You Can

- Use industry-standard secure protocols to secure your file transfers
- Monitor file movement and user activities on your network
- Create a multi-layered security solution for data storage and retrieval, authentication, and firewall traversal with Globalscape DMZ Gateway®
- Use malware and IDP tools to prevent malware from entering the network and prevent sensitive data from leaving the network
- Use data wiping to thoroughly delete data
- Encrypt stored data
- Securely access your data on any device without the cloud
- Merge or replace legacy file transfer systems
- Automate workflows and integrate systems

CONTACT US TODAY TO LEARN MORE.

www.globalscape.com

210.308.8267

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-gs-gd-1022-r1-79d