FORTRA

EBOOK (GoAnywhere)

Control in the Cloud: Using MFT to Solve Your Data Challenges

Intro

In the last couple of years, the rapid, unexpected shift in business operations revealed new security challenges. While many were scrambling with the logistics of keeping data safe in their adoption of cloud technologies, others recognized the value of a good Managed File Transfer solution. We spoke with a group of subject matter experts from various companies and industries who shared their stories with us so that your cloud initiative can be as smooth, secure, and effective as possible.

Digital transformation has fundamentally changed how we manage a business. Much of this transformation is occurring in the cloud ecosystem. Cloud implementations are taking place in all sectors across all industries. With the cloud, we started understanding the benefit of value-added services implemented in the cloud ecosystem through efficient data management. Many other advantages of managing and storing data in a cloud environment include cost savings, flexibility, mobility, improved information security, increased collaboration, and new insights within an enterprise data asset.
(Reza Alavi | Senior Manager, Technology and Digital Risk | LinkedIn)

Working from home has accelerated the adoption of cloud technology, but while there is an increase in cloud-based collaborative applications, file transfer methods haven't really changed so much. That seems to be driven more by the need to upgrade or replace a certain system and moving that to the cloud. That was definitely the catalyst for us. We were moving a business-critical system from an on-premises model to a cloud system, and we needed to make sure that the data was secure. Managed File Transfer lets us move files with the flexibility and control that we need.
(Matthew Hankinson | Infrastructure manager | LinkedIn)

Question 1: On-prem challenges

What are some of the key challenges when it comes to data transfer on-prem, and in the cloud? How does having the right technology help when it comes to productivity, security, and compliance?

Funso Richard | Information Security Officer | LinkedIn

The major challenge organizations face is the ineffective management of data. The use of on-prem protocols to transfer files across the organizations and to external parties poses major challenges such as lack of security, lack of mobility, performance issues, maintenance cost, productivity impact, and poor user experience. An alternative has been to migrate data transfer to the cloud. However, ineffective planning, financial cost, misconfiguration, and poor user experience are some of the challenges with cloud data transfer. As a result of poor user experience, employees use unapproved file transfer solutions to move files around. This is a serious risk that exposes businesses to data loss, exfiltration, and data breaches.

To ensure data protection and optimized productivity, investment in the right file transfer technology is crucial in keeping the business operating effectively and efficiently. With the increase in remote work adoption and dependence on the supply chain, organizations need a dynamic, dependable, and flexible file transfer technology to move data across multiple protocols, platforms, and environments. Such technology is Managed File Transfer (MFT). MFT is built with security controls, without undermining productivity and performance. The benefits of using MFT include cost reduction, centralized data management, scalability, integration, compliance, timely data access, enhanced decision-making, and positive user experience.

Gary Hibberd | Security Consultant | LinkedIn

There is a fundamental challenge with data transfer, whether it is on-prem or in the cloud – and that is one of control; who has access to the data, and how it is transferred. Of course, the amount of data we are processing is increasing, and safely sharing it across our infrastructure is of key importance to any organization.

The challenges we face come down to the management and control of these transfers, and where they happen, we should implement appropriate technical solutions, like Managed File Transfer (MFT.) Having a Managed File Transfer capability ensures that data is managed and monitored to ensure it arrives safely at its destination. A good MFT solution reduces compliance risks by ensuring data integrity is maintained. Beyond compliance, it will also increase productivity, as it reduces the overload on the network, and increases transfer speeds, along with the reliability of the transfer.

Michael Barford | Solutions Engineer | LinkedIn

For on-prem data transfers, we still see the high complexity associated with developing and maintaining custom solutions to handle high-volume and highly complex transfers as the top challenges. Yet today, lots of organizations rely on scripting or in-house developed solutions to handle internal transfers. This comes with big associated maintenance and operating cost. Usually, a big cost is associated with errors. When one file is lost, many realize it days afterward, and different IT resources need to be mobilized just to diagnose what happened, where the file is, process it manually, and fix the “script” so the issue does not repeat in the future. The problem gets worse when the people that developed the custom solution move to another role or company, or when this custom solution needs to be expanded to handle new use cases, with more and more cases involving the cloud.

Another challenge is typically associated with security or compliance requirements. It is hard and costly to comply without a purpose-built solution that is up to date with the latest security protocols, and that provides comprehensive encryption, auditing, reporting, and roles segregation.

When moving to the cloud, an important consideration is to check if the MFT can interact with many cloud platforms, as well as REST APIs, which are constantly being evolved to cover future use cases.

Due to the numbers of platforms and interfaces companies work with today, security, auditing, and maintainability of data transfers are growing ever more difficult. Traditionally, file transfer processes are configured and then left to run which worked quite nicely in an era of just SFTP or just FTP transfers since you can use the same process for multiple trading partners. The times when it gets difficult is when there's a requirement to adapt the process; this is commonly the turning point for when customers look towards an MFT solution.

Using the right technology allows companies to more easily adapt to the ever-changing file transfer requirements that they may face.

Ray Sutton | Technical Consultant | LinkedIn

There are numerous challenges when you are looking at data transfer, mainly about exposing these services to external parties, perhaps across the internet. These challenges are around keeping a good and secure environment, and in most cases having to over-engineer the solution to protect the networks and systems within your organization. It's probably fair to say, however, that this challenge also exists in the cloud too, where you have to look at the security of the cloud-based data center where you connect and protect the data even more. Having the right balance is key to ensuring that employee productivity, security, and compliance requirements are met. Anyone who interacts with your systems also needs to be sure that you have met all the security requirements, but also have an easy process to follow for transferring data. This is crucial to maintain a high level of security. Missing this step, or putting in difficult processes or systems, could cause some people to perhaps look for quicker alternatives, which, in turn, could cause you more risk in the way you support your cloud or on-prem solutions.

Matthew Hankinson | Infrastructure manager | LinkedIn

The challenge with secure data transfer is that fine balance between achieving what the business requires, and asking for, and meeting the cybersecurity requirements. It has to meet the business needs, while also being compliant. Secure data transfer needs to address everyone's concerns, and cybersecurity is required, not only from a practical standpoint but also from a regulatory perspective.

Historically, the key differences between moving files on-premises, and in a cloud environment had always centered on control. With the cloud, there's that unknown territory of having to trust a third party in some regard. You need to make sure that the cloud service provider is meeting your security standard. You also need to be cognizant of the type of data that you're sending. If the data contains Personally Identifiable Information (PII), you need to make sure you have extra protections in the process. Too often, people don't ask the question about what is being transmitted. They're just asked to move a file from one location to another, but what is actually in that data? Is it something that will cause the business more of an issue if it gets leaked? It's important to have a reliable Managed File Transfer solution that puts those security features in place. A lot of the challenge comes from breaking old habits. People have been freely transferring information for many years, but now, they have to think about the data that is contained in those files, or they can violate privacy laws. We are working to educate the users, to make them consider what they are sending. We try to have a standard process and initial checkpoints about what is being requested.

Soulos Panagiotis | Global Information Security Manager | LinkedIn

Some of the key challenges when it comes to data transfer on-prem, are:

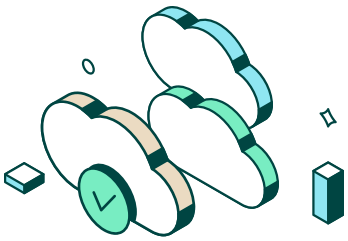
Security weaknesses: Traditional on-premise file transfer solutions, such as FTP and SFTP/FTPS, do not cover all current business needs for security. FTP was not even designed with security in mind, lacking basic security controls, such as an encrypted authentication channel. Encryption, such as transfer and storage encryption to protect data-in-transit and data-at-rest, is an afterthought requiring additional steps and IT expertise, making it difficult, expensive, and time-consuming to send and store files safely. Also, the exchange of user credentials is not managed by these solutions and should be performed with external and usually manual procedures, which may lack security measures, increasing the possibility of exposing credentials.

Automation: Traditional solutions do not offer automation or scheduling of file transfer operations. Usually, manual scripting or additional solutions are required to address such needs, leading to increased costs and expertise of IT staff.

Automated alerts: Traditional solutions do not offer automated notifications and should be combined with other solutions to notify users when a file transfer has failed.

Business Continuity: Disaster Recovery Plans should be designed and implemented manually, as traditional solutions do not embed automated DRP mechanisms. Also, recovery procedures when service fails are done manually.

Capacity issues: On-premise solutions may have issues transferring large files, which can happen due to minor network outages and errors.



Key challenges when it comes to data transfer in the cloud are:

Compliance: Depending on the type of organization, specific regulations and/or industry standards may need to be adhered to. Data sovereignty should also be considered when storing and transferring data in the cloud.

Data leakage/breaches: Data leakage or breaches may happen if the cloud provider is compromised.

Access/Denial-of-Service: Access to services may be prohibited if the cloud provider is under a Denial of Service attack, or if the organization's access to the internet is down.

Malware infection: Anti-malware controls should be in place to minimize the risk of files stored and transferred in the cloud being infected by malware.

Vendor lock-in/lock-out & Service portability: The use of cloud services should be assessed to avoid vendor lock-in/lock-out and be as much as possible easily portable to another vendor/cloud service provider. Vendor lock-in refers to the situation when the cost of changing vendors is so high that the organization is stuck with the current vendor. Vendor lock-out refers to the situation when the vendor goes out of business and shuts down provided services.

By having the right technology, an organization can address these challenges by making sure that its chosen technology can improve the organization's productivity and efficiency. Cloud solutions leverage cloud characteristics such as resource pooling, rapid elasticity, and measured service. Also, cloud solutions are designed and implemented with security in mind, providing appropriate encryption mechanisms to protect data-in-transit and data-at-rest. Some aspects of compliance are achieved, as appropriate certifications, audit capabilities, and transparent procedures are built into the cloud solutions.

Use Cases

It's easy to speak in theoretical terms about the benefits of a superior managed file transfer system. However, there are some great success stories for deploying GoAnywhere MFT into the cloud that breathe life into the narrative. The following 3 use cases illustrate the point.

Major Global Healthcare Company

One of the major IT efforts for this international healthcare organization was to migrate services into the cloud to design a more hybrid model.

When we first spoke with them, they had a long-term requirement to update MFT which were littered with out-of-date and unmanageable processes that, if left alone, could pose a potential security threat in the near future. They also wanted to mature their cloud infrastructure, which remained a priority project for them over the next 12 months.

Their current MFT solution was end-of-life and out of support which made updating existing tasks difficult. Along with this, cloud support was limited and posed a real issue with their strategy of migrating more services into the cloud, so, earlier this year, we finalized implementing GoAnywhere into their private cloud environment.

Natural Gas Distributor

When we spoke with this organization, they shortlisted GoAnywhere MFT as their chosen MFT solution simply because we had an offering for the cloud.

They had an internal objective to keep as many services as possible integrated into their DevOps workflows, which meant that any new service they deployed had to be compatible with their containers or AWS infrastructure.

Our container offering was, at the time, a bit undeveloped, with a lack of knowledge and understanding in the UK, so we decided to go with deployment within AWS.

One of the key values of using AWS for them was that it allowed them to automate a substantial amount of the deployment with existing processes.

International Product Distributor

Another organization was looking to minimize the footprint of its own hardware and wanted to go with a SaaS approach using MFTaaS.

They made great use of GoAnywhere Agents to adopt a hybrid model by creating a trusted link between on-premises and the cloud, which helped complement their long-term strategy of sunsetting on-premise services.

They had a key requirement around security, which we managed to fulfill with MFTaaS, thanks, in part, to the SOC-2 Type 1 certification we've attained.

Most demonstrations with customers seriously consider MFTaaS or deployment into their private cloud.

Question 2: Cloud challenges

What are the implications for managed file transfer when moving to the cloud? What areas of the business do you need to consider?

Funso Richard | Information Security Officer | LinkedIn

Adopting a cloud strategy requires thorough planning to avoid business disruption. It is no different when organizations are considering moving managed file transfer (MTF) to the cloud. A poorly implemented MFT migration to the cloud could lead to data loss, breaches, regulatory fines, significant financial cost, ineffective decision-making due to delay in data access, performance and productivity loss, supply chain disruption, and negative user experience. To avoid these adverse effects, it is important to have a well-thought strategy in place.

Moving data to the cloud is more of a business decision than an IT process. Though IT owns the underlying technology, there are business implications that must be considered before data migration. A key consideration is the business need. Yes, data is the fuel running the business engine, but to have optimized performance, that fuel must be the right grade. From data collection, storage, protection, transmission, access, management, and destruction, the business objective must be factored into the selection of an MTF and data migration strategy. This is non-negotiable. There is no question that cloud MFT proffers data scalability, mobility, visibility, interoperability, and usability in a highly mobile and interconnected business ecosystem. However, implementation cost and resources are important business considerations. For highly regulated organizations, compliance requirements play a significant role in moving data to the cloud. To address compliance concerns, organizations should select MFT solutions with built-in compliance and security controls.

Soulos Panagiotis | Global Information Security Manager | LinkedIn

When moving to a managed file transfer solution in the cloud some key points should be considered. Data security – at rest and in transit – along with compliance, are at the top of the list. There should be no chance that the introduction of a cloud-managed file solution would lead to legal, regulatory, or any compliance non-conformities. The performance of the service should also be considered. Interoperability and portability are key factors for adopting the cloud solution. You should ensure that the service migration will have the least operating impact on the organization, and if possible, no impact at all, including any current communication channel with collaborating organizations and customers. Service Level Agreements (SLAs) should be reviewed thoroughly, included in the contract, and cover all business needs.

Training of users, whether these are business users or IT personnel should also be considered to minimize the risk of operational failures due to a lack of personnel skills and be able to utilize the cloud service at its full potential.

Business end-users of the service, information security personnel, operational risk personnel, compliance and legal, information technology personnel should be involved to ensure that the cloud service will cover all business needs.

Gary Hibberd | Security Consultant | LinkedIn

For MFT to work effectively, the organization must understand what data it holds, and how it is used. Once this is understood, then a strategy to implement MFT must be developed and communicated to the whole business, because the likelihood is that all areas of the business need to be considered.

Areas of the business which are currently transferring large quantities of personal or sensitive data via email or FTP should be prioritized as they will see the benefits, and the controls being employed. A good MFT solution will improve the security of the data, and also its privacy.

By implementing MFT, organizations can consolidate and manage data transfers using a centrally controlled and monitored platform. This offers visibility of what data is being transferred, when and by whom. Because this monitoring is in place, MFT systems help provide evidence that can be used as part of the internal audit process.

Ray Sutton | Technical Consultant | LinkedIn

When you migrate services to the cloud, you need to be mindful of risk, security, and performance. If by moving to the cloud, the system performs poorly or has timeout issues, this could cause your customers and users of that service to not use it, or in the worst case, find alternate means of copying files. This would potentially cause some issues around security and perhaps confidential information being exposed. Migration to cloud solutions is not a "lift and shift" exercise, especially when we are talking about personal or confidential data. Just recently, we have seen some security breaches which – perhaps with planning and understanding the risk factors – could have been avoided.

Some key areas which you will need to address are understanding your data, and what safety precautions need to be in place. This doesn't matter if you are migrating to the cloud or storing data on-premises; the rules are the same. Putting together a security framework for data and being able to manipulate and secure that data is vital. For example, look for a solution that encrypts in transit and offers the ability to encrypt at rest. Look at protecting that data when it reaches the end destination. Also, look beyond the end-point, and perhaps how to apply a lifecycle to your data where you can control who can view, edit and perhaps, even print.

Cloud offers a world of possibility, but it's important to understand the nature of your data and how you need to protect this very valuable commodity.

Q&A: Michael Barford | Solutions Engineer | LinkedIn

Migrating to the cloud is not a simple project. There are varying factors that will influence this business-enabling event. Part of the due diligence that is required is to ask the right questions to find the best solution to fit your business vision:

- **Where do our most critical workflows happen, on-prem or cloud?**
  That might help you decide on MFT hosted in the cloud or on-prem, hybrid, or both.

- **Do we need an MFT solution that is "transparent," whether information flows happen on-prem, cloud, or hybrid?**
  It is more common today that automated workflows mix traditional technologies like SFTP, and FTPS, with common cloud service providers. You probably want to be able to create complex automations abstracting from the technology stack that is involved, so it doesn't require IT resources with low-level knowledge of each.

- **Are we moving to a pure cloud infrastructure, or will we still be operating hybrid mid/long term?**
  The vast majority of companies will have use cases that interconnect on-prem and cloud. In those cases, being able to deploy MFT whenever we want (on-prem/cloud,) and having agents automate processes on systems whenever they are deployed, can be a critical capability. MFT with agents will allow automating workflows involving systems on-prem, cloud, and even in customer/partner networks in a transparent manner. This strategy allows for a smooth migration to the cloud, which doesn't happen in one day.

- **Do we need an MFT as a cloud service, or should we operate one ourselves?**
  In case you decide to operate it yourself, you might want to evaluate if the solution will fit your existing deployment strategy, i.e., that it can be deployed in containers/dockers, can escalate, load balance, and others.

- **What kind of data are we going to process?**
  You will need to check that information transfers happen with appropriate security/compliance levels. In the cloud, this can be more challenging, so you might benefit from providers offering certifications, as well as features like encryption at rest, and other characteristics that meet your business requirements.

Good and bad practices

As with all security initiatives, there is a way to meet compliance without actually being secure. Sometimes, it is easy to satisfy a compliance checklist but has the potential to leave the organization vulnerable. To take the right steps, our experts offered advice, including both what to avoid, as well as what to aim for.

✗ BAD PRACTICES: Christos Syngelakis | Chief Information Security Officer | LinkedIn

There are a lot of challenges to overcome when working with secure file transfers. The challenge is not so much within an individual corporation, but when the corporation must conduct activities outside of its environment. For example, a medical facility that needs to transfer large files to patients, or a marketing company that must share files outside the organization.

Many companies do not have dedicated IT staff, or someone responsible for this kind of operation. In a lot of cases, the recipient only has a public account for mail transfer, and nothing else. The corporate tools that you have in order to manage this kind of transaction that will also adhere to your organizational policies don't fit well into this scenario.

Sometimes, you may have the ability to create an account to give the recipient access to the security products that you use, but generally, these on-the-spot communication tools are not affordable. They entail not only human costs, but perhaps the license cost for this kind of activity. Big, corporate collaborative tools can support corporate-to-corporate file transfers because there are established mechanisms between the two parties, but, the on-demand capacity can be a huge problem.

Another challenge occurs with disparate powers between corporations. Sometimes, the other party may be a government authority who wants to transfer data, and they don't have a secure way of communicating all this data, but they insist on proceeding to move sensitive data. Sometimes, you have problems with time limitations, and the business leaders just want the information transferred now. The end-user is going to use any kind of publicly available software to accomplish the task.

There is a huge need for a solution that is easy to deploy and use without the need for the end user or the other party to do anything. There are some solutions, but they are unaffordable, and often not easy to manage. Every company needs this because there are so many different documents that contain information that you don't want to be available to everyone.

✓ GOOD PRACTICES: Chris Hodgson | Business Development Manager | LinkedIn

There are lots of protocols and methods of transferring data with customers and trading partners, all with their benefits, and drawbacks. Having such disparate methods of sharing data can become confusing, and hard to manage, maintain, and keep compliant. What a solution like GoAnywhere provides is a centralized Secure File Transfer solution that can help move data from any endpoint to any endpoint, be this on-prem to the on-prem, cloud to cloud, or a hybrid of the two. GoAnywhere provides users and administrators, with a role-based security framework for logging into and accessing the system, with two-factor authentication, and encryption of all files and data while in transit and at rest. This helps enterprises automate and streamline their exchanges of sensitive data while maintaining compliance with industry standards.

Moving to the cloud is often the catalyst for people to look at a Secure File Transfer solution. Cloud platforms have some really good tools for moving data around within their own environment, but what they lack is the ability to send data between different cloud tenancies. A solution like GoAnywhere can help streamline the exchange of data between disparate cloud platforms, all from one centralized user interface. There's also a strong use case for Finance teams to explore the benefits of Secure File Transfers, as they migrate to new cloud-based ERP systems, and need a secure way of integrating files and data with remaining downstream systems, or trading partners.

Conclusion

File transfer is a deep subject. We have so many ways now that we can transfer data. Having oversight of that is particularly challenging. We've moved away from the days of File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP), and embraced new methods and products where all providers are cloud-based. This creates disparate elements; some organizations are using older tactics; still using SFTP, and others are using APIs, which are pulling and pushing data all the time to different third parties and different cloud solutions and SaaS. With the sheer complexity of all these different facets and the different ways of working, there is no one-size-fits-all. Maintaining a consistent method is a big challenge because each organization has its own way of doing what they feel is right.

Then, the ability to check the integrity of the files that are being transmitted is also important. There are some good solutions out there that can validate the files. If you ingest a lot of data and you take a lot of data from different web services that you provide, you can scan them before they're transferred using an in-line scanning tool.

Transferring files isn't always a simple case of moving a file from location A to location B. You need to ensure security at each step of the transaction. If the CEO says that he needs you to send the budget sheets to another location, you're not going to send that via email. There are some good tools that allow you to classify the file and lock those down.
(Goher Mohammad | Head of InfoSec | LinkedIn)

"File transfer is complex, regardless of whether it's in the cloud, on-prem, or hybrid. Do you restrict based on extension, or do you scan every piece of data that comes in for malware to ensure the integrity of your data, amongst other components? As well as enforcing a set of security controls on how this should take place, it's also important to have re-useable patterns so you have consistency in implementation across projects and initiatives that need to develop such file-transfer solutions. Whether it's traditional SFTP, or using a vendor's SDK and API suite to drop to something like an S3 bucket with strict access controls, no implementation is a simple move function. Classification of that data, where it resides, and the security controls around that implementation are all equally important."
(Lidia Guiliano | Information Security Professional | LinkedIn)

Whether your organization is just embarking on its cloud journey or has already established a strong cloud presence, security should be an overarching business concern. Security is more than making sure that your data is not exposed to the internet. Data is not a static entity, nor is it isolated to a single area. It needs to move in order for the business to function. The importance of a managed file transfer solution cannot be overstated. Our experts have presented many thought-provoking ideas to help your business thrive and grow, securely, in the cloud.

About BlueFinch-ESBD

Organisations rely on BlueFinch-ESBD to make IT lives easier and keep business running smoothly. We specialise in data protection and compliance by encrypting and securing data, and provide easy access to the information people need. BlueFinch-ESBD is Diamond certified implementation and support partner of Fortra.