AN AXWAY REALLY USEFUL SECURE FILE TRANSFER GUIDE:
Part 2

How to move your Secure File Transfer Application without losing your cool.

INTRODUCTION

Congratulations, you’ve done it. You’ve decided to move your Secure File Transfer to a new provider, or as we like to say – **your forever home.**

While you might be relieved that the decision has been made, we suspect you might also feel a little anxious. And that’s understandable. It’s like moving to a new (and better) house. While it always seems like a much-needed fresh start, you’re also saddled with packing and sorting out the old place as well as setting up the new place just how you like it.

Hopefully, you’ve also identified a guide to help you with the journey.

It’s one thing to decide on software but having the right partner to help and ideally deliver the outcome for you can make your life so much easier.

And here, you generally have two options. If you’re keen on DIY, a professional services partner can drive the deployment of the software and get you setup with your own instance in your own tenant even on premises if you want. Or, easier still, you can select a provider that builds the software, provides the cloud service and also offers all the professional services you need to get you to your new home for secure file transfer.

One other important item to keep in mind is something we touched on briefly in the first paper in this series: How much do you want to do yourself? (Why’s that an important consideration right now? Because now’s the time to be sure exactly how much help you want or need.)

The reality is that there’s little point in moving if you’re not improving something (or better still, multiple things). If you’re not going to enhance where you are now and what you’re doing, you may as well stay put. However, you’re here, so we’ll take it as a given that you have your heart set on getting better.

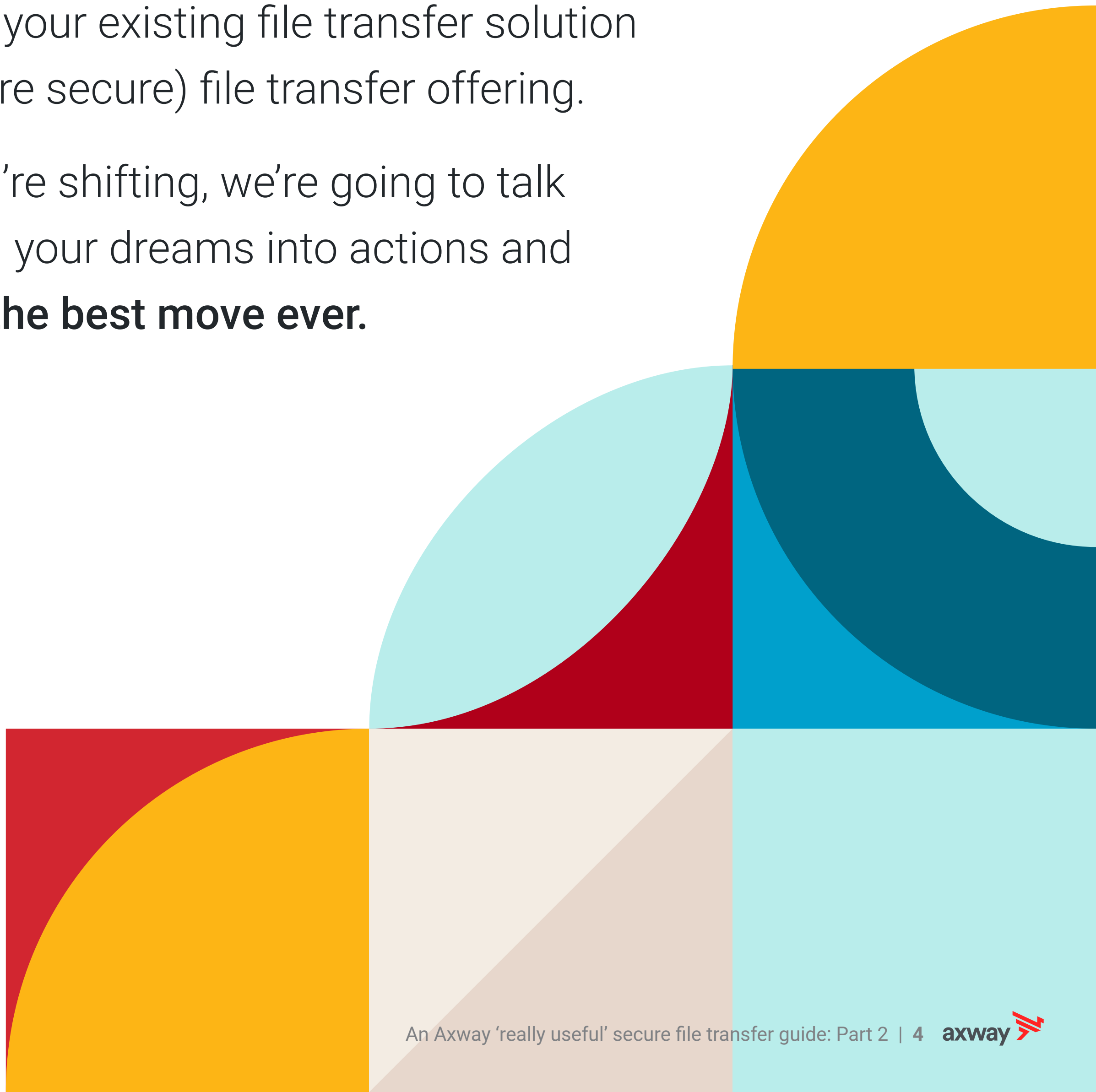
So, we’re going to guide you through how to make the most of your move.

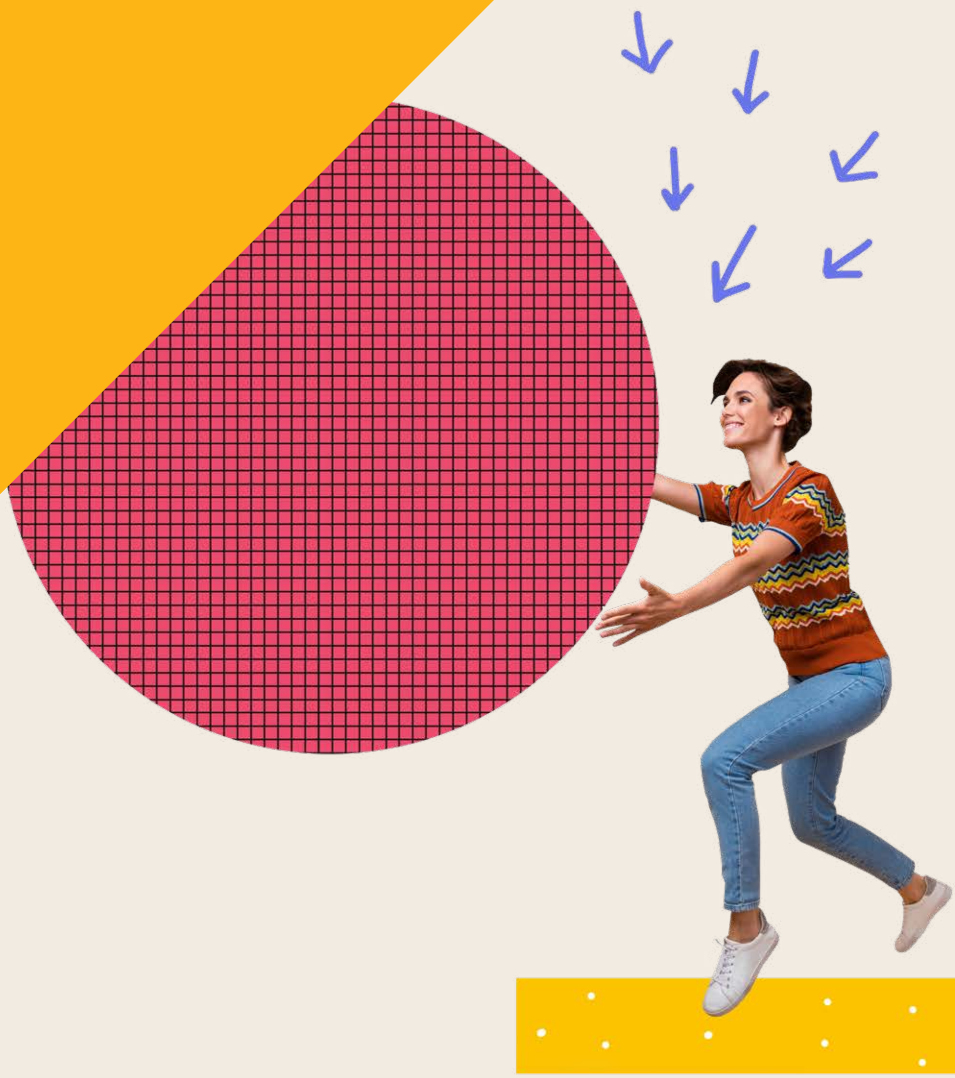
And in no time, you’ll be sitting back on your new sofa and chilling out with a pizza and Netflix. And just in case you are not a fan of a lot of reading (and because we’re really nice, helpful people), you can check out our upcoming video series that contains useful tips and thoughts around the execution and move of a secure file transfer process into the cloud.

WHAT YOU MAY HAVE MISSED SO FAR

In the first part of our guide (***Thinking about shifting your Secure File Transfer application? Here are 8 things to think about first***), we covered what you needed to keep in mind when moving from your existing file transfer solution to a new (more secure) file transfer offering.

Now that you're shifting, we're going to talk about turning your dreams into actions and **making this the best move ever.**





YOUR TO-DO LIST

We know you're probably a bit of an old hand at this, so we won't go on at too much length about the typical activities you already know about (like deciding where you are going to install the app, setting up the right security and access controls for your personnel, configuration, etc.). We know you've got this part down cold, and hey, those are generic activities no matter what the application.

Instead, we're going beyond the basics and will focus on the other mission-critical tactics – that, when done correctly, will turn your posh new place into a bit of a Secure File Transfer (SFT) fortress.

So, here goes.

START AS YOU MEAN TO GO ON - SECURITY IS EVERYTHING!

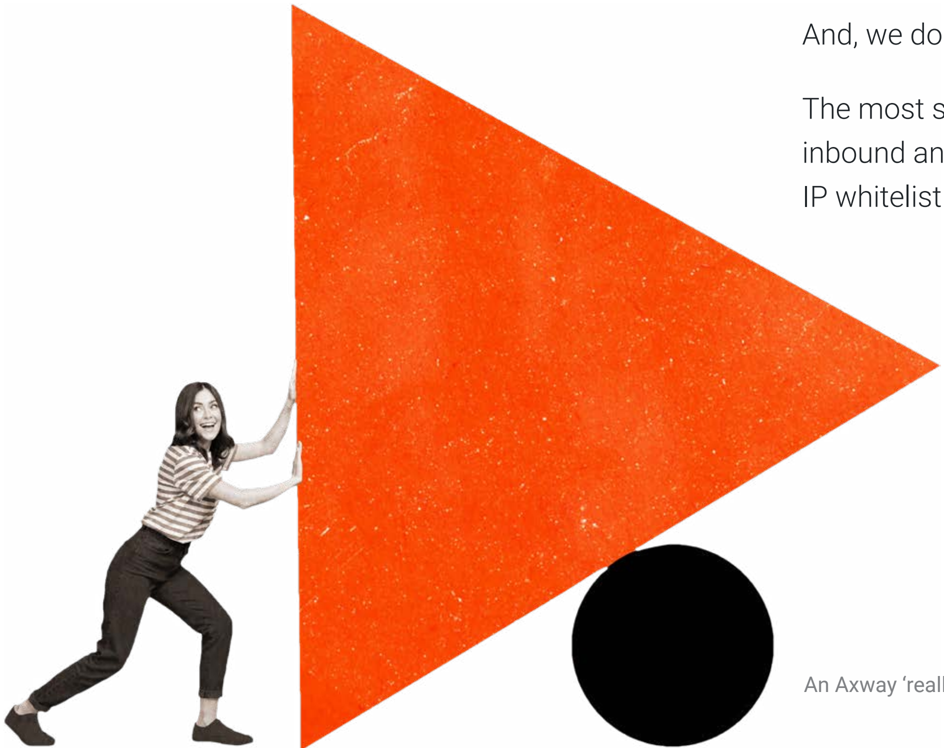
One of the most common reasons for shifting is better and proven security.

Sadly, as those persistent cybercriminals seek to hack the file transfer pattern, you end up with more and more reasons to:

1. Find and move to a more secure and robust file transfer application with a greater focus on security, and
2. Step up your management and flexibility game.

Enhancing your security posture is considerably easier in a house that's not only a quality build but also comes with all the mod cons. When the architect and builders are hyper-aware of the risks, they invest in a much higher standard of in-built security as their reputation - and yours - depends on it.

Let's assume you have made sure your vendor is focused on both your security and theirs. How can you now leverage what's on offer to safely enjoy your new home more than your last one without sacrificing the speed and flexibility you love?



1. Set up role and responsibility-based security

It probably goes without saying, but we'll say it anyway. **You need to configure the roles and responsibilities in your SFT solution correctly.**

This includes every person who will play a part in managing the system, as well as those users and systems who might trigger or receive bulk file transfers, or the end users who have the ability to transfer files on an ad-hoc basis. If they interact or impact the SFT solution, you need to lock down what they can and can't do – no exceptions. Hopefully, you're on your way to a more powerful solution, so you will likely also want to look at business unit-level security and security for all integration connectivity.

(Yes, we know you knew this, but it would be irresponsible if we didn't call it out just in case.)

2. Protect your data-in-transit

Safeguard your data as it travels from A to B to Z by deciding which protocol to use for encryption in transit. Let your partners know as well as those you're going to hand out keys or secrets.

And, we don't need to say it, but we will:

The most secure approach is to encrypt both inbound and outbound communications and IP whitelist on both sides. **Always**.

3. Leveraging a proxy

Now, getting a little more advanced. Think of the proxy as that little room before entering your home, where you ask your guests to leave their shoes. Not part of the outside, but not inside either. Proxies are placed in the DMZ and serve multiple security purposes: from connection encapsulation (such as IP addresses and port numbers) to ensuring network segmentation, keeping the dirty separate from the clean.

Connection to the network from cloud

If you've chosen to move to the cloud, make sure you are clear on whether you will connect your new secure file transfer home to the SaaS environment using a VPN, VPC, or use multiple approaches to facilitate a smooth interaction between the cloud application and your endpoints on premises and in other clouds.

4. Check out every payload

Make sure you turn on your anti-virus scanning option. It's like installing a 'Ring' video doorbell, allowing you to eyeball and check out everyone who arrives at your front door asking to be let in – even when you're not home. This adds yet another layer of protection when transferring file-based workloads.

5. Encryption at rest

Many people and organisations think about encryption as a function of security between two points (i.e., the transfer itself), but encryption with a premium file transfer solution can do much more, including encrypting beyond the transfer process itself. You will also likely want to encrypt data at rest (i.e., on the database and the file system while the file workloads are being utilised).

6. Integration with a DLP

If you're already using a DLP, you may want to make sure that your secure file transfer process is connecting to the policies and rules related to files and whether they can even be transferred at all (based on the requirements of your organisation).

MAKE YOUR MOVE RUN LIKE CLOCKWORK

We know that shifting can be a nightmare, but in truth, it doesn't have to be!

If you're a first-time home buyer (in other words, you don't already have a secure file transfer solution), then migration is usually a little more straightforward. There's far less to pack, no old appliances and furniture to try to squeeze into new spaces, and you have all the benefits of a clean start in your lovely new place, where you can set all the rules anew. Nice one!

However, if you're moving out of your home of several years and are taking all your furniture and appliances with you (i.e., all of those historical integration patterns), your migration plan should include a couple of key activities:

1. Configuring your new transfers in your new application

Getting up and running smoothly without introducing new headaches or customisations makes all the difference. Luckily, with an SFT SaaS application, it's extremely easy to get onboarded rapidly, including rapid testing of the initial file transfers and any incremental changes, so that everyone involved in the shift can relax at the end of the day and enjoy a cold beer. So here is what you need to be ready for:

a. **Upload details** –account parameters including authentication

b. **Routing details** – where it's coming from to where it is going (i.e. the target or many targets that are the destinations and any workflow functions to be executed between

c. **Security provisions** – who can do it was discussed before but now we are talking about the protocols to be used

d. **Destination** – where the files are going

e. **Scheduling** – with a new file transfer app, hopefully you are in a better place on scheduling and the flexibility in the app. But in some cases, you may need to be thinking about synchronising jobs between what your file transfer application and a job scheduling tool if that is what you want to do.

f. **Connectivity** – this is usually the piece that takes the longest time in most cases because while the setup is easy, multiple teams are usually involved.

It's important to reuse wherever possible, rather than creating customisations in job scheduling tools or flows that are one-to-one. In other words, build your base flows that follow common patterns and set the foundation for how you will perform file transfers. Then, reuse those flows wherever possible. While it's always possible and likely you may have some flows that will require unique configuration, by reusing wherever possible, you lift the burden of effort from your admin team and facilitate secure automation and participation by the wider team.

2. Identifying and configuring the movement to and from the transfer process

You expect your new solution to do what it says, right? And quite rightly so.

Secure File Transfer is designed to securely move files between locations that are already secured and hardened. You can think of SFT as the control that orchestrates the flow of files, determining how many to which destination, and then dispersing the data from the files as appropriate – or even collecting it via an integration or application to send to the next destination.

Realistically, this movement should be able to be accomplished without customisation and change beyond the core of what can be configured with a premium file transfer application. What you don't want, though, is to introduce complexity by relying on customisations in third-party applications or within the file transfer process. In short, the fewer moving parts, the better. Something, somewhere in the overall process will be responsible for the "packing" and "unpacking" of the data in the file transfer process so it can be consumed by other applications. However, ideally you want this packing and unpacking process to be executed utilising standard capabilities of the application(s) instead of creating custom point to point capabilities.

3. Orderly movement vs. the chaotic, move as fast as possible approach

There are two types of shifting strategies: **Orderly and measured** and **move as fast as possible**. The later tends to be more chaotic and drives opportunities for errors but there are times where the move to a new solution just has to happen and there's no time for a more measured approach.

And it's probably no surprise that avoiding a chaotic approach is best when you want to identify and execute an orderly flow of movement of your current file workloads to the new application. While it doesn't have to be absolutely, perfectly designed, **the migration process should follow a structured approach**. Doing so will ensure easy communication and preparation with your internal participants and external partners.

When considering how to make this orderly transfer where there is a real concern about business impact, start with lower-value transfers and ensure they work, then shift your focus to the highest-value transfers or the most critical transfers. Finally, move back to the "long tail" of lower value or less meaningful transfers to the business operations. Alternatively, when working with a guide or professional services partner that mitigates your risk, you could take a variety of different approaches, such as a business unit-based, partner-led, customer-led, incremental process or geography-based approach. Ultimately, the prioritisation approach isn't primarily about the SFT application but rather about what your business is most comfortable with executing, aligned with the plans for the migration itself.

Regardless of the approach you take, you need a plan that is clearly documented and communicated to all.

4. Build your communication plan early and use it often

Secure file transfer is all about movement and timing – so communicating about what's where and when is critical.

With a new file transfer offering, your communication plan ensures an orderly shift from your current integration to the new one. Your communication plan should focus on:

- Overview of the change, including a short briefing on the benefits of the change, what your internal and external customers should expect and when the changes are occurring.
- Structure of the migration team, including the key points of contact for the internal aspects of the migration as well as the external aspects. Typically, the team that deals with partners, customers and suppliers will be different and a different level of specialisation or expertise so both internal and external need to be addressed.
- The order of migration for which file workloads (between external partners and you, and vice versa) will be moved in which order, including key dates when workloads will move, when they will be tested, and when they will be live in the new application.
- Security and integration expectations, including key contacts for additional details on the details related to the workloads for the parties that will move.
- Information about the future state including responsible parties, logging support cases, and where to find additional info.

A communication plan also reflects any work that needs to be done by your partners, so they, too, are aware of what they need to execute and by when, including a clear series of contacts and resources available to assist. Again, the partner we recommended you select earlier can really help here because they can provide a template for FAQS and other details to be provided to external partners. Failing to notify your internal and external partners creates an opportunity for delays in the process, as other parties must securely connect with you, and their process might take a little time to complete. It's essential to note that you don't absolutely "have to" IP whitelist and secure between partners, but you will likely want to as a matter of best practice.

5. What am I keeping, what am I throwing away, and when?

One of the many questions to ask when you plan your move is, **'Do I really need all that storage?'**

When it comes to shifting, it's never a great idea to move everything first – lock, stock, and barrel – with the intention of sorting it out later. Instead, use the impending move as an opportunity to consider what you truly need and will keep, for how long, and what you can discard. Then determine if you are going to move everything at once based upon a business need that justifies doing so, or if you are going to winnow out the elements that don't need to be moved first.

By its very nature, file transfer is transient, meaning you may not need to retain file transfer workloads forever. Interestingly, due to the growing number of security risks, there's a trend to remove file transfer workloads once they've been processed. In some cases, your security and privacy team and/or your business may insist on removing file transfer workloads "on success." In other cases, a regulatory body may mandate that you must keep file transfer workloads in storage for a prolonged period of time. A strong and powerful file transfer application like Axway will allow you to make these decisions on a very granular level (i.e., the type of files being moved can determine the duration and type of storage).

While deploying, it's essential to ensure that these requirements are well understood and executed so that you are as procedurally secure as possible. When configuring your file transfer process flows, consider the storage you're using and reuse it wherever possible. And, as we mentioned before, if you configure the application to store file transfer workloads for a time, it's an excellent idea to ensure that this storage "at rest" is encrypted.

6. Make your new file transfer operationally efficient and optimised

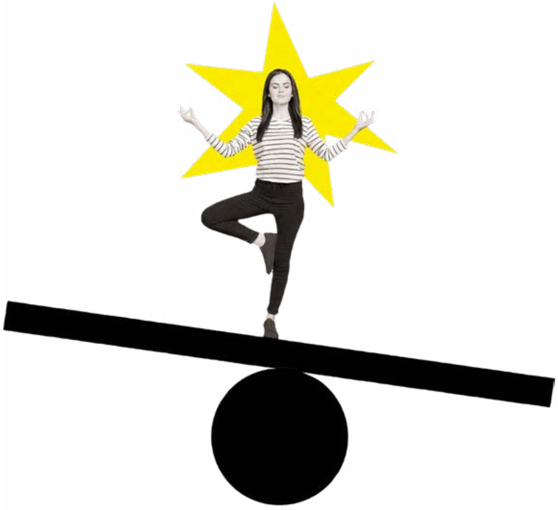
You now have an application and some flows that have been tested. You've got a clear plan for moving new file transfer flows, and a clear communication plan to securely inform everyone who needs to know where you 'are.' Great job so far!

However, you'll want to exercise caution before moving everything into your new file transfer application. In other words, take a little time to make sure that you have an optimised setup.

What does that really mean?

Well, you want to optimise the energy and effort you put into the application and its associated management and use. Now, if you've chosen to move the whole thing to the cloud, that becomes easier, especially if you have a managed service running the whole thing, and all you have to do is submit an ITSM request or similar to see things done on the cloud

Whether you are running with a SaaS offering or your own deployment, you're running the application yourself. So here are some considerations to keep in mind to ensure efficiency:



1. Reuse. (Yes, again!)

We know we've already mentioned this, but we'll repeat it: Wherever possible, opt for reuse! In other words, ensure that you're taking as much of the application's core functionality as possible, executing configurations and integrations to the endpoints on either side with standard functionality vs. customisations (like the earlier plumbing example) and connecting them in a way that facilitates reuse for your IT and management teams. Additionally, you'll want to configure file transfer flows that can support multiple types of file transfer workloads coming from multiple secure sources using a common flow.

A powerful and secure file transfer application will give you the ability to configure the file transfer flows in a way that will allow for a secured endpoint (i.e., an application, external partner, internal person, etc.) to interact with different files of different types where the file transfer application itself can direct traffic utilising a core set of capabilities.

2. Onboarding

Maybe, just maybe, there's an area you may want to look at upgrading the existing "wiring" a little bit more. For example, when you want to bring a new partner or internal user on board.

In this instance, you can utilise connectivity to your existing and in-place security application via a common protocol, such as LDAP, and then automatically set up the flow. If your onboarding process is configured and set up under your current ITSM tool, you can utilise the integration tools of your new secure file transfer application to build this type of configuration.

3. Efficiently managing upgrades and changes

Moving to a SaaS offering? In that case, you can move along; there's nothing for you to see (or worry about) here.

However, if you're going to run it yourself, you'll need a clear plan to stay up to date with the latest vendor releases. After all, the rapid rise in file transfer vendor security breaches over the last few years is probably the reason you're moving to start with!

If you've opted to manage the application internally, maintaining currency with your vulnerability scans and version upgrades is essential to maintain a secure environment.

The most efficient way to achieve this is to have a clear and consistent upgrade plan - one that you've established at the point of deployment and adhered to over time.

4. Monitoring and reporting

Just as with all your other applications, monitoring, alerting and reporting are key aspects of an efficient file transfer application – regardless of whether it runs in the cloud or your own tenant. A powerful file transfer application should securely deliver configurable actions that require monitoring for success, alert you to incidents or failures and report on overtime using the observability or monitoring and reporting framework that you've already got in place as a company.

The best tools come with their own capabilities and user interfaces for monitoring, alerting, and reporting. But you don't necessarily want to add more views, right? However, ideally, you should be able to choose between using what's available or having all the data about how the application is operating seamlessly pushed into your existing tools – thereby creating a more efficient overall operation.

Now, answering one of the most asked questions: "Can the monitoring and management application go one step further to help us identify what's missing?" (The answer here should be **yes!**).

For example, you may want to configure the system to handle the most frequently asked question of IT from users: "Where is my file?" The good news is that this request can be tailored to your own environment, introducing a whole new level of efficiency.

Yes, it's critical to deploy the application as 'vanilla' (non-customised) as possible to make your life easier in the future. However, having the ability to tailor the solution to meet specific needs (those that don't adversely impact upgrades or the core of the application) can give you the best of both worlds.

And here is another place you want to get ready for AI. The reality is that AI should be able to help you with identifying what's happening and what should be happening.

5. Be ready for the regulator

In many cases, your organisation may have to adhere to certain requirements of the regulator that oversees your industry. It's good to know these requirements in advance, but before going live and launching the application, you want to ensure that you have incorporated any regulatory-specific requirements into your testing regime.

Regulatory requirements are typically incorporated to address business continuity of service, security, compliance and testing. You'll want to execute these respective tests and receive any necessary documentation from the vendor before going live.

6. Get geared up for AI

When you think about it, the real goal of moving (and doing a good job of it) is to deliver an application to your business that's more secure and as cost effective and as efficient as possible - from the initial onboarding of new partners or integrations through to secure file transfer movements, to the alerting, monitoring and reporting that occurs throughout.

What else can you improve, though?

Returning to our moving home analogy, it's a great idea to get out and explore the neighbourhood and local amenities. And then, work out which ones you can take advantage of to improve your lifestyle.

And this is where AI comes into play. It's not hype - it's reality, and realistically, you should expect to be able to enable some key elements of the application without impacting the security of the offering. This can include onboarding new file transfer flows and enabling the monitoring and understanding of utilisation with the file transfer application using natural language. (And, oh yeah, that "where's my file?" question from users, you should be able to get answers to that as well. This is just the tip of the iceberg in terms of what AI can do.)

You may find that you can see the activities we discussed in Part 1 of this really useful guide, or in the benefits and measurements we discuss in Part 3 - stay tuned!

Many organisations find that when they move to a new secure file transfer solution, such as Axway, they discover room for improvement in other processes, as well as areas where they can finally meet other business requirements that have long been on their wish list.

Some examples?

- **User-based file collaboration.**
  If you'd like to track and trace what's happening with your files securely, Axway enables user-based file collaboration. This can include introducing a DLP.

- **Cloud-to-cloud transfers.**
  Moving to a cloud environment can increase demand for cloud-to-cloud file transfers. You'll be pleased to know that managing these structured and time-based file-based workloads between applications can be accomplished with a flexible file transfer application.

- **ETL-based transfer.**
  File transfer applications have been evolving! Today's SFT solutions can, either independently or when integrated with an iPaaS' lite" capability, address some of the most complex challenges traditionally handled by ELT applications.

- **Job scheduling.**
  When working with the application and deploying it in your operation, have you ever thought how nice (and helpful) it would be to have a handy job scheduling tool to orchestrate your file transfer flows? You'll be pleased to know that file transfer solution vendors, including Axway, can provide this capability. A tip here, though: Make sure you ask and answer this question: *"Do I really need the job scheduling tool, or can the file transfer application handle this?"* If the answer is yes, you do need that scheduling and orchestration, then you may want to look to an iPaaS 'lite' capability instead of a job scheduling tool.

WHAT NEXT?

While this guide uses many analogies about moving house (and you probably felt a bit exhausted thinking about it), you can rest assured that moving files is less complex and a lot less hard work.

By committing to some prior planning, there's no need to get caught short and end up staying in an over-furnished single-room apartment rather than relocating to a luxurious new family home with a pool. And when your SFT vendor offers cloud delivery capabilities, the move is even easier.

In our next really useful guide, we'll share what improvements you can expect after you transition to a new cloud environment - and how to measure them.

Missed the really useful Guide Part 1? **Check it out here.**

Get started with your move. **Contact us here.**