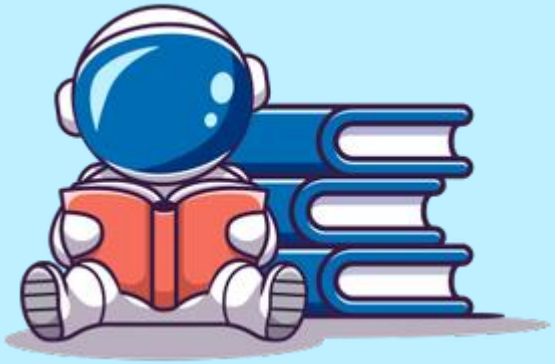
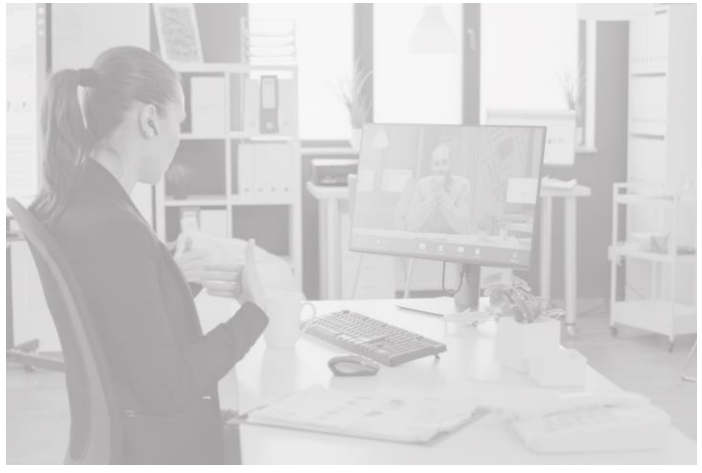
BlueFinch ESB

HYBRID CLOUD GUIDE

Table of Contents





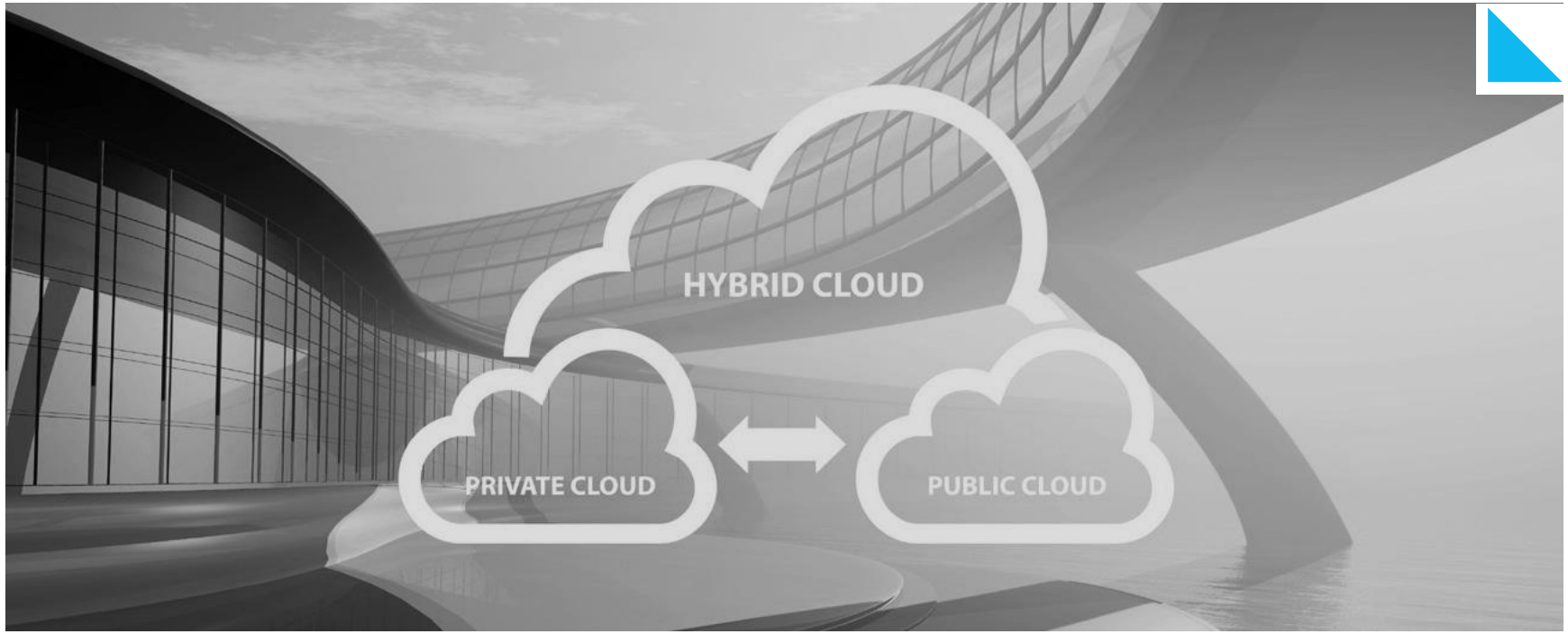
Introduction

Is Hybrid Cloud the Future?

You can't go far in any industry without running into discussions on the cloud. Organizations are increasingly integrating cloud solutions into their operations, so it's clear cloud use is here to stay. But what about hybrid cloud, when organizations combine on-premise and cloud environments or multiple cloud environments? When considering moving portions of your on-premises environment to the cloud, when should you consider hybrid cloud scenarios?

Statista expert analysts, found that as of 2023, 72% of organizations use hybrid cloud as their chosen cloud strategy. Hybrid is becoming a major component of cloud business.

If you're considering a move to a hybrid cloud environment, this guide is for you. Read on to learn all about planning for a secure hybrid cloud, including IT buying considerations, how the hybrid cloud works, and which tools can keep your cloud data secure.



What is the Hybrid Cloud, Anyway?

According to ISO 17788, hybrid cloud is a deployment model that uses two different cloud deployment models bound by appropriate technology that allows for interoperability, data portability, and application portability. A hybrid cloud could be owned and operated by the organization or a third party, and it can exist on or off premises.

The following scenarios identify three ways a hybrid cloud environment could take form:

Scenario #1:

A manufacturing organization needs to exchange files with trading partners in the cloud. They keep everything on-premises except for their secure file transfer solution, which they operate on instance within their chosen cloud-computing platform for easier trading partner connectivity.

Scenario #2:

A state university moves several data processes, including class materials and course schedules, to a private cloud.
However, sensitive student data remains on a secure internal server to help the university remain compliant with industry data security standards.

Scenario #3:

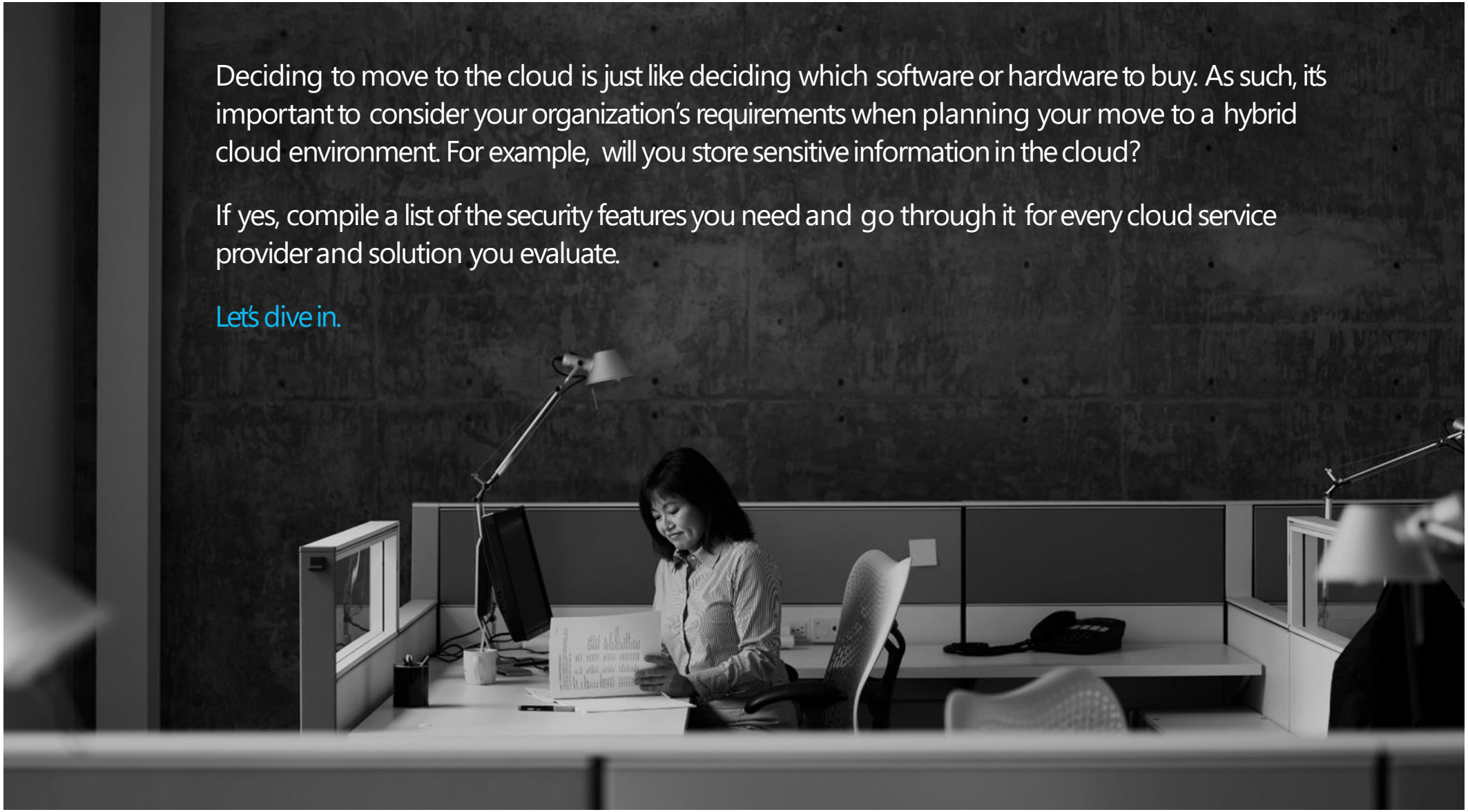
An information technology business wants to reduce the amount of hardware in their server room. They spin up a virtual machine on Amazon Web Services, then move their file transfers to a mix of private and public cloud platforms. Cloud integrations are then used to automate processes between on-premises servers and the cloud (for example, updated user data is pushed from the sales team to popular web services like SharePoint or Microsoft CRM).

Multi-cloud

Most organizations today use a multi-cloud and on-premises split for their requirements. If you're still not sure if a hybrid cloud deployment is right for you, here are a few considerations:

	HOW IT WORKS	WHAT IT COSTS	HOW DATA IS PROCESSED	KEY BENEFITS	DOWNSIDES
HYBRID CLOUD	Hybrid cloud environments use cloud solutions in tandem with on-premises systems located at your organization. Some processes kept on-premises connect occasionally to folders in the cloud, while others are run 100% in the cloud.	May require a mix of capital expenditure (for on-premises processes) and "pay as you go" methods (for cloud processes) to fund activities.	Data is split between local servers and internet-based servers. When working with trading partners or clients, data shared to a cloud-based storage location can be pulled down and processed by on-premises workflows if required.	The organization retains control over most aspects of the environment. Other key benefits include the flexibility to continue development and freedom to keep certain data under strict organizational control.	Running a mix of on-premises and cloud environments may require a larger budget to keep things running. Equipment failure and asset management are also of concern, as is the time commitment required to monitor both on-premises and cloud servers for security risks.
CLOUD	All organizational processes operate on remote internet servers hosted by a third-party service. These servers can be located worldwide and are used to store and manage data. No processes are kept on-premises.	Requires a "pay as you go" method dependent on the scale and licensing needs of the organization, with a low-entry-point advantage over a long-term on-premises investment.	Data is processed using cloud solutions or cloud-based applications, with a remote endpoint that provides processing and encryption functions.	The cloud is easy to scale. It offers fast and controllable upgrades and contributes to lower energy costs. Most cloud environments are simple to set up.	Entrenched operations in the cloud leave your organization with little control over increased monthly pricing. Security is a concern when relying on a third-party to ensure data security. Support can also be expensive, and the cloud can be susceptible to connectivity downtime.

Moving to the cloud



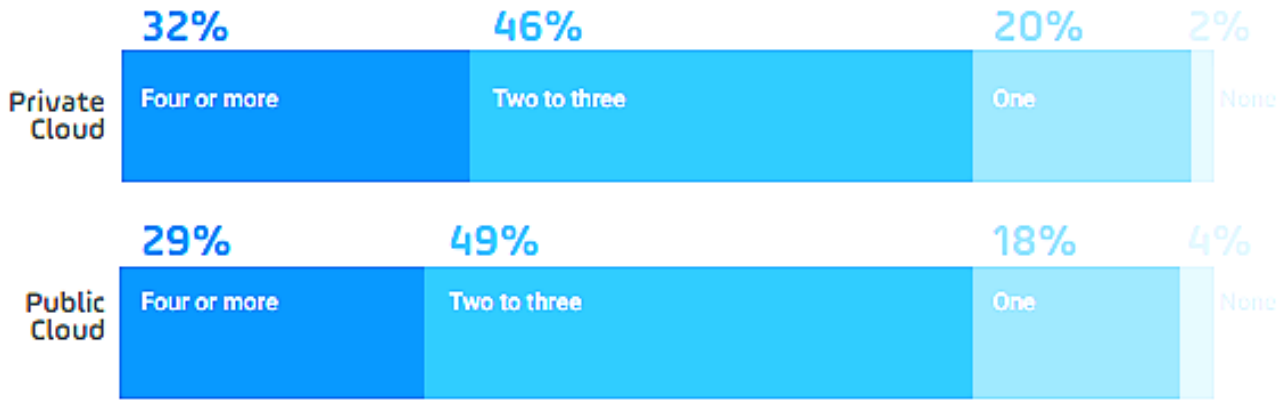
Deciding to move to the cloud is just like deciding which software or hardware to buy. As such, it's important to consider your organization's requirements when planning your move to a hybrid cloud environment. For example, will you store sensitive information in the cloud?

If yes, compile a list of the security features you need and go through it for every cloud service provider and solution you evaluate.

Let's dive in.

Who Uses a Hybrid Cloud?

Number of Private and Public Cloud Providers Used in 2023



Hybrid cloud use can be found across all industries and favors certain data types. According to the Stonebranch report 2023, 78% of companies use multiple public clouds, 79% uses multiple private clouds.

Hybrid cloud is arguably the most popular cloud environment strategy for organizations today. Full adoption of the cloud is rare, mainly due to the cost and the time requirements for a complete transition. Another concern is the risk of failure – for instance, if an organization runs key business processes on premises, and moving those processes to the cloud fails, the health of the business will be immediately affected. Furthermore, many organizations cannot
move to a full cloud due to security concerns and requirements from trading partners, industry standards, and government regulations. These concerns make hybrid cloud a perfect choice for most. With a hybrid cloud deployment, organizations can decide which data stays on-premises and which processes are migrated to the cloud.

Hybrid cloud deployments make it easier for workloads and projects to run seamlessly between cloud platforms and an organization's on- premises environment. Simplified integration to and from different setups is useful when working with trading partners that operate in varying cloud environments. For example, an organization may set up a hybrid cloud environment to exchange files with one third-party vendor in Amazon Web Services and another third-party vendor in Microsoft Azure.

When to Use a Hybrid Cloud

So, when is moving to a hybrid cloud environment appropriate? Let's take a look.

GO HYBRID IF…

You're just wetting your toes with the cloud.

A move to a hybrid cloud might be a good middle ground if you're still deciding whether a full cloud environment is appropriate for your business. It is also, arguably, easier to return to an on-premises environment from a hybrid cloud than a full cloud, as there are fewer pieces in play.

You want to maintain maximum availability for business continuity.

A move to a hybrid cloud environment is a good option if you're looking to keep secure backups of sensitive data somewhere that's less likely to be afflicted by natural disasters, power outages, or other avenues that cause server downtime. Most cloud computing platforms run remote servers in multiple regions, so even if one location goes down, your organization can rest assured knowing your data is available and safe elsewhere around the globe.

You work with trading partners that have migrated to the cloud.

Being in a hybrid cloud allows you to work with trading partners and exchange data securely between your on-premises environment and their cloud buckets or folders. You'll get all the benefits of simplifying and automating your file transfers and other business processes while refraining from a full cloud move.

Cloud Cybersecurity

Cybersecurity is an important consideration for any area of IT—cloud included.

If you plan on storing customer or business data in the cloud, including credit card numbers, physical addresses, birthdates, intellectual property, employee data, health records, personal identifiers, or even backups of software code, you'll want to make sure you're following cloud security best practices long before making the move to a hybrid cloud.

Here are a few cybersecurity tips to keep in mind:

1. Maintain a strict policy for customer data retention and deletion.

Certain organizations need to store information indefinitely. This applies to the healthcare industry, for example; keeping patient data over a period of decades helps practitioners provide patients with high quality care. But for those who aren't in healthcare, it's helpful to know what data retention laws apply to you and when you should keep, or even delete, sensitive information. With this knowledge, you'll know exactly how long data should be preserved in the cloud
… and how to get rid of it safely when the retention period is over.

2. Conduct frequent security audits for your hybrid cloud environment.

You can quickly find and correct pain points in the cloud by conducting audits of your environment. Each cloud service provider has examples of what you should look for when running an audit.

Undertaking an audit may not seem like a walk in the park. But the benefits of doing so on a frequent basis far outweigh the temporary inconvenience to an organization's resources. Not only can you get ahead of the curve by spotting problem areas before they occur, you can review your third-party vendors and cloud integrations to make sure the integrity of your data is upheld on both ends.

3. Keep your data safe with cloud-specific security tools.

Organizations rely heavily on cloud applications. A study from KPCB estimates there are 893 to 1,206 cloud apps in use per enterprise—and growing. Imagine how much data is shared between these off-site applications and your business!

To keep your data safe, we recommend protecting them with tools in these four categories: DDoS Protection, Cloud Access Security Broker, Data Loss Prevention, and Cloud Backup.

Looking for more cybersecurity tips for a hybrid cloud? The good news is, any cybersecurity tips that apply to a full cloud environment should apply to the hybrid cloud as well.

Cloud File Encryption

With the concerning increase we've seen in data breaches over the years, it's never been more crucial for organizations to ensure their information is properly secured. Is your data encrypted in transit to and from internal systems? Most organizations say yes, but while this may seem obvious, the secondary encryption practice—to protect data at rest with OpenPGP or AES encryption —is less frequently enforced. Full disk encryption methods (or the equivalent) are readily available in popular cloud environments.

According to the 2021 Thales Data Threat Report for healthcare, a large percentage of health organizations use the cloud without following strong encryption or cybersecurity strategies that will keep them protected. This invites risk into the organization. Remember: even if the files are stored in a secure folder, there's no guarantee that your server won't be compromised by external or internal users.

Statistics from Thales, Digital Guardian, and other industry leaders prove that the best advocate of data security isn't your chosen cloud service provider or third-party applications. It's the one who stands between an organization and the outside world—and that person is you.

If you're moving to the cloud, even to a hybrid cloud, encryption is nonnegotiable. Securing data in transit and at rest is a must and should be on your planning checklist long before data is ever stored in the cloud.

Cloud Automation and Cloud Data Compliance

Automation is a hot topic for IT professionals. It reduces manual tasks and user errors, streamlines and simplifies complicated business processes, and helps eliminate repetition so employees can reprioritize their focus onto other areas of the business.

File transfer automation is especially important for organizations looking to migrate to the cloud. File transfer automation aligns with cost-saving strategies by eliminating a need for several separate file transfer tools, replaces manual processes, and gives you more control over your data movement and trading partner connections.

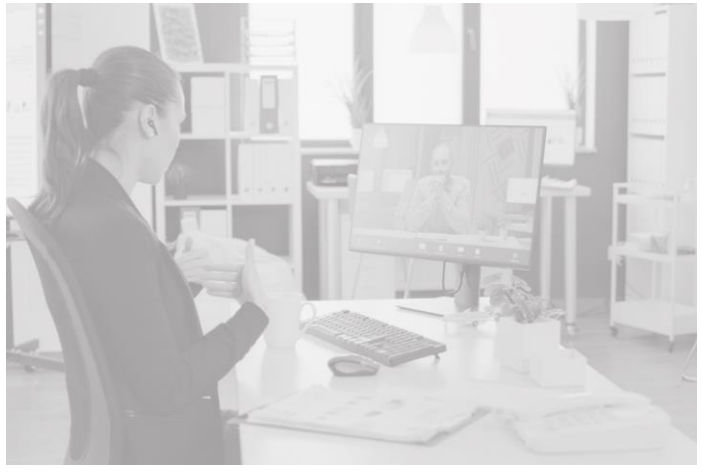
HOW IT WORKS:

A robust, secure cloud file transfer solution allows IT professionals, like system admins, network engineers, and programmers to create file transfer workflows. These projects can easily be configured to move and process files around the cloud, between environments, and within private networks. Certain tasks can be automated (e.g., moving a file from one folder to another) or, if you prefer, the entire process, including encryption, can be automated end to end.

With hundreds of tasks, resources, and triggers to choose from, file transfer automation is flexible, simple, and powerful. Paired with a built-in scheduler, workflows can be scheduled to run at any time, and the files can be monitored in folders on cloud-based or internal file systems. If a workflow fails, you have the option to be alerted immediately through email or by text message.

So, if you have a plethora of processes to handle, including web integrations and file transfers, cloud automation should be a consideration as you design your new environment.

Data stored in the cloud must follow compliance requirements that apply to your organization. Credit card data must be processed and transmitted in the cloud following guidelines handed down by PCI DSS. Medical information should be secured in accordance with HIPAA and HITECH. And if you handle the personal data of EU citizens (whether your organization is located in Europe or not), your cloud data must meet GDPR stipulations. Organizations that do not maintain compliance with applicable regulations, standards, or laws could face hefty fines and penalties.



How to use Hybrid Cloud

Today's Cloud Marketplace

Today's cloud marketplace gives organizations a lot of options to choose from. The largest and most popular contenders for the cloud are Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud, and Oracle Cloud, but there are others that provide public and/or private access to your data.

Which option you choose will depend on the size of your organization, your budget, your business requirements, and the data security standards you must comply with.

There are also several types of "service models" to evaluate. Each model comes with different services that are handled directly by the cloud service provider.

Infrastructure as a Service (IaaS):

The IaaS service model offers organizations a place to install and run cloud-supporting software 100% in a hybrid or cloud environment. In this model, the cloud service provider takes care of managing the infrastructure, while the customer is responsible for running, managing, and maintaining any deployed operating systems, databases, or applications.

Integration Platform as a Service (iPaaS):

The iPaaS service model helps IT integrate software applications that are deployed in different environments. For organizations that use a multiple-cloud approach for a hybrid environment, iPaaS can keep software and services connected between several on-premises and cloud locations.

Platform as a Service (PaaS):

The PaaS service model is a solid option for developers who want to create applications without purchasing the hardware, software, and other services required to do so. With PaaS, the cloud service provider hosts resources, including an operating system, server, programming toolkit, and more. Many also offer storage, so application developers can build, test, store, and run their creations completely in the cloud.

Software as a Service (SaaS):

The SaaS service model allows IT professionals to use the built-in software and databases that are provided by the cloud computing platform. This is a very hands-off approach to software; the provider downloads and hosts the software in the cloud and also provides infrastructure, which reduces the overall amount of management, support, and maintenance required to run the software.

Getting Started in the Cloud

At this point, you may be ready to deploy some of your processes to a hybrid cloud.

If you aren't sure how to get started, we suggest talking to your chosen cloud service provider. Explain your situation and see what they'd suggest. Any software vendors you use that you want to move to the cloud could also help; they may have cloud documentation, guidelines, or best practices to share with you.

Here are a few remaining things to consider as you migrate to a hybrid cloud:

Do you want to migrate only certain services in the cloud, or are you planning to make a full transition eventually?

If you have legacy applications that must remain on-premises, will they continue to be interoperable with the applications you run in the cloud? If not, what do you plan to do with them?

Where do you want your cloud applications to sit? Who

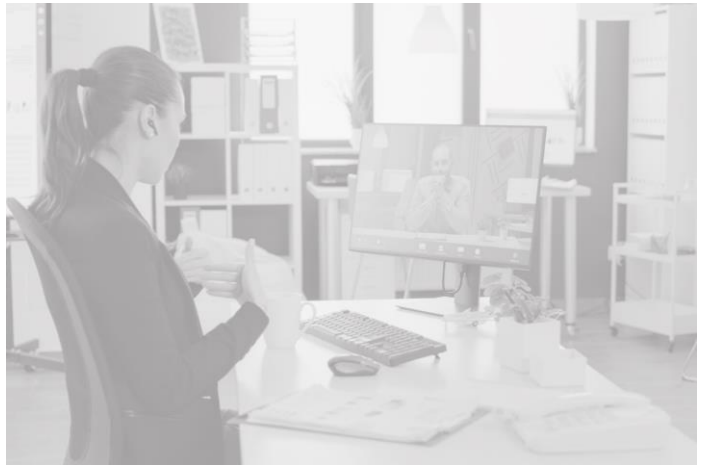
should have access to your cloud data?

Note: Ensure database and folder permissions are configured correctly!

Secure your hybrid Cloud data:

Regardless of the storage location and whether your databases and folders are encrypted, you should always make sure to encrypt your information at the file level, too. This ensures protection for internal and external data at every layer, reducing the overall risk from vulnerabilities or data breaches.

If you use the cloud to store data, it's an inevitable fact that many parties will have access to that information, including trading partners, third-party vendors, and key stakeholders. This can be beneficial—cloud storage allows these parties to connect and retrieve the information they need from anywhere, without being limited to physical locations or internal networks. All cloud solutions offer basic authentication requirements and security controls. You can also use a secure file transfer solution that can encrypt your information in transit and at rest, no matter where it resides.



Introducing MFT for the Cloud

Hybrid Cloud for File Movement & Storage

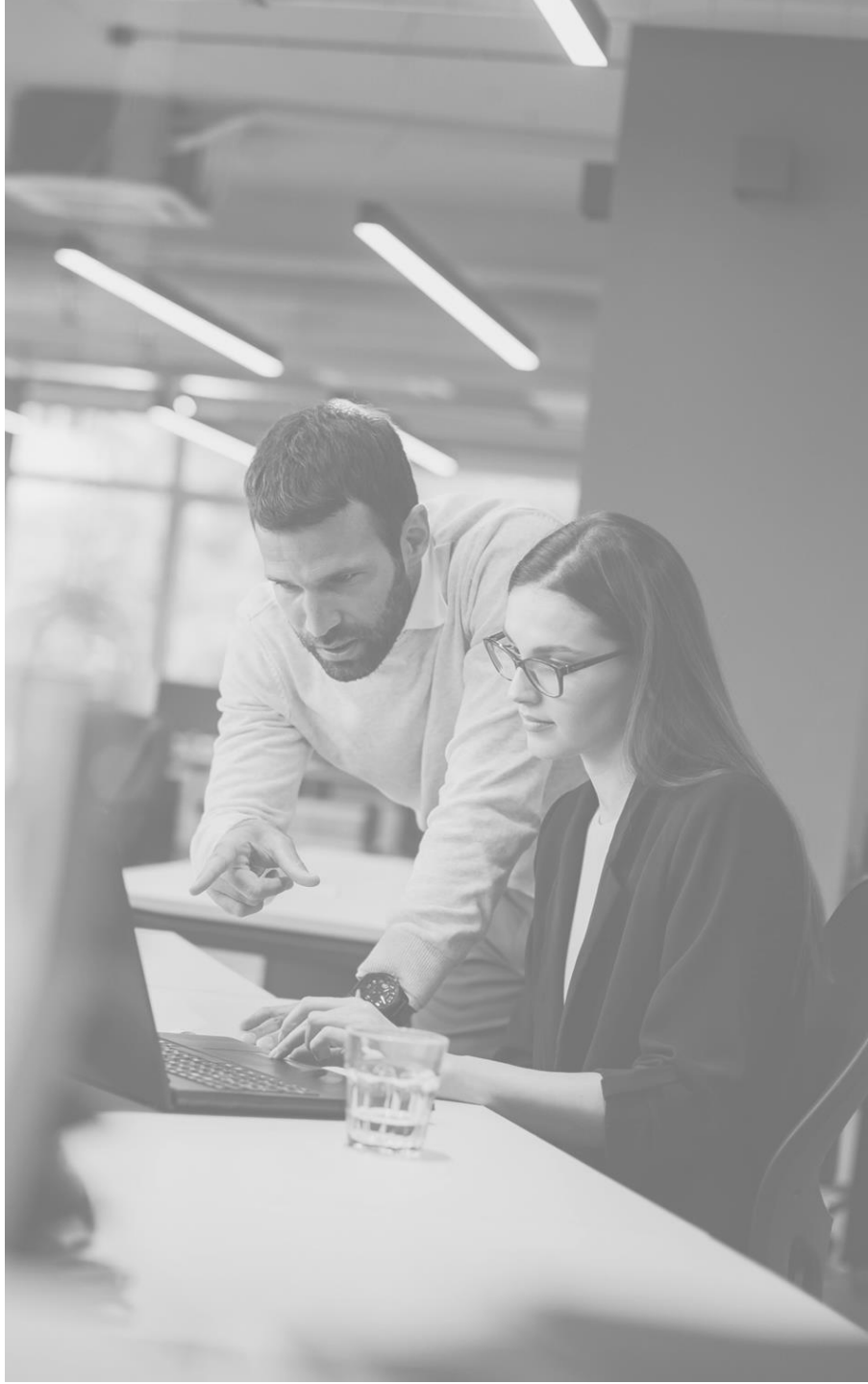
When the hybrid cloud is paired with a secure file transfer solution, organizations can deploy their file transfer processes (including workflows and automation, encryption/decryption, granular security controls, and data translation) to a variety of hybrid environments. This allows the business to keep a portion of their resources on-premises and run the rest via a cloud service provider like Amazon Web Services or Microsoft Azure.

The right file transfer solution should provide popular file transfer and encryption protocols that are supported in a hybrid cloud environment. These protocols include SFTP, FTPS, SCP, AS2, and HTTPS, as well as OpenPGP, ZIP with AES encryption, and FIPS 140-2 validated encryption ciphers for protecting confidential information and sensitive data. Using that secure functionality, files that are shared with cloud trading partners will be protected by a secure connection, and data stored in the cloud will be encrypted at rest.

What is managed file transfer?

Managed file transfer (MFT) is a secure solution that automates file transfers, encrypts data, and streamlines process development using a centralized enterprise-level approach. MFT software can move and protect files that reside on-premises, in the public/private cloud, or within a hybrid environment, making scaling or migrating to different environments a simpler task. It delivers the security and control you need to transmit and store data safely between systems, locations, users, and trading partners.

Most MFT solutions in the marketplace today are all-in-one offerings, meaning they include everything you need for your file transfers—thus eliminating the need for supporting software, insecure free software solutions, or manual scripts. MFT software typically comes with industry-leading features: automation, security controls, secure email sharing, cloud and web integrations, advanced auditing and reporting, and the ability to improve the overall compliance stance of your organization.



Managed File Transfer for the Hybrid Cloud

How MFT works with the cloud

As you implement a managed file transfer solution, you'll want to consider how and where you want it to operate. First, it's generally easy to set up an MFT instance in the cloud. Installation is fast, and there's no need to set up a third-party solution; everything should be included for you. After running through a quick installation wizard, you will simply need to set up your trading partner accounts and file transfer processes.

Regarding implementation, there are a few directions you can take in a hybrid cloud environment:

1 Run your MFT solution completely in the cloud

Some MFT vendors offer their solution as part of your chosen cloud platform's marketplace. For example, Amazon Web Services and Microsoft Azure both allow organizations to download and run an instance of the vendor's software in their cloud environment. This approach reduces the need to use servers, legacy tools, or other processes on-premises. A full cloud MFT solution can also help you comply with compliance audits, internal policies, and business requirements.

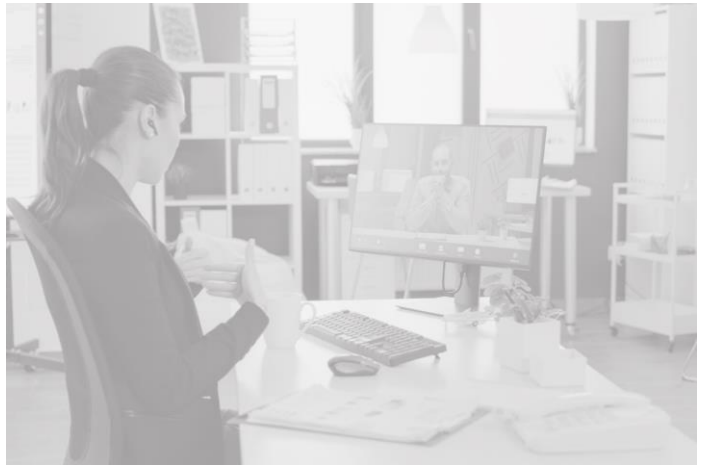
2 Run a DMZ gateway solution in the cloud and point it to on-premises servers

You can choose to keep your MFT solution implemented on-premises but run a reverse and forward proxy (DMZ gateway) solution in the cloud. This solution can point to on-premises servers and help keep file sharing services safely in your private network when exchanging data with cloud trading partners. A DMZ gateway will also not require inbound ports to your network and make connections to external systems on behalf of local users.

3 Run your MFT solution completely on-premises but connect to cloud users

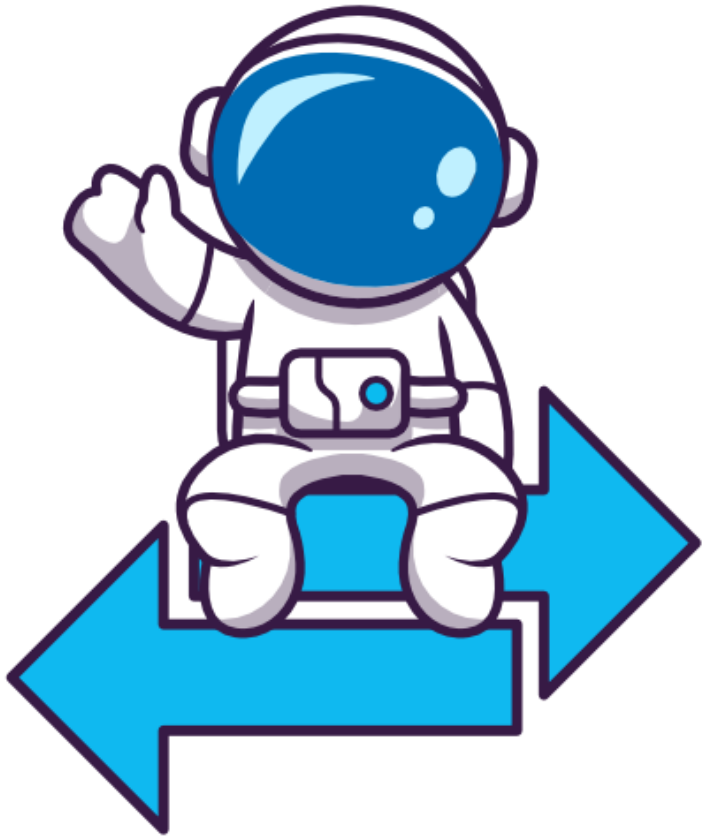
If you decided to keep your MFT solution 100% in an on-premises environment, you can still integrate parts of it with the cloud. For example, you could decide to only connect to specific folders in the cloud. Your solution would then make connections via secure file transfer protocols (SFTP, FTPS, HTTPS, or AS2) to the cloud so files can be exchanged and retrieved with cloud trading partners. Cloud-based file systems, like Amazon S3 buckets, can also be used in this instance. Your MFT solution would then automatically pull files shared this bucket into your private network.

One thing to keep in mind: your MFT solution will operate consistently across environments no matter which implementation option you choose. Where you keep your solution should depend on other aspects of the business—time, resources, hardware, required cost-savings, and compliance requirements—rather than on the solution itself. **Note:** This only applies if your MFT solution is truly platform agnostic.



GoAnywhere MFT and the Cloud

What is GoAnywhere MFT?



GoAnywhere MFT is a cybersecurity solution developed by Fortra that automates and secures file transfers using a centralized enterprise-level approach. Incorporating GoAnywhere in your organization and a hybrid cloud environment will save you time and money, improve security, simplify file transfers, and help you meet compliance requirements.

Protecting sensitive data is of paramount importance in today's environment. GoAnywhere provides a safe and secure method for automatically transferring information inside and outside your enterprise. File transfers and related business processes will be streamlined with GoAnywhere without requiring your team to have prior knowledge of programming or scripting.

Using GoAnywhere for your Hybrid Cloud Needs

The benefits of using GoAnywhere in a hybrid cloud

Most managed file transfer admins choose to run their solution in a hybrid cloud environment. By using GoAnywhere in the cloud, your business can benefit from:

- ✓ Secure file movement and connectivity
- ✓ Automated file transfer workflows and projects
- ✓ Comprehensive audit logs and audit reduction capabilities for file transfer and user activity
- ✓ Detailed reports for sending to stakeholders and partners
- ✓ A high level of interoperability to seamlessly integrate with popular web and cloud services
- ✓ Simplified interaction with internal and external trading partners
- ✓ Assists in meeting data security requirements derived from GDPR, PCI DSS, HIPAA, and more
- ✓ Granular security controls, including a role-based access model for users and trading partners
- ✓ Built-in data translation for various formats, including Excel, XML, and EDI X12/EDIFACT
- ✓ User-friendly administration with a browser-based interface

GoAnywhere MFT is flexible, scalable, highly available, and offers fast, controllable upgrades. Operating GoAnywhere in a hybrid cloud environment can help your organization lower costs and protect key business data in the event of unexpected downtime or disaster.

Integration with cloud applications and services

GoAnywhere's cloud connectivity provides you with the flexibility to partially or completely migrate to cloud infrastructure such as Microsoft Azure or Amazon Web Services. You can also interact with web and cloud services like SharePoint, Salesforce, and Dropbox using GoAnywhere's easy cloud integrations.

These integrations, called Cloud Connectors, are enabled through connections with APIs like SOAP and RESTful web services. Cloud Connectors seamlessly support the automation of data exchanged between on-premises and cloud-based environments.

To learn more about GoAnywhere MFT in the cloud, request a 15-, 30-, or 60-minute specialized demonstration with one of our product experts.

We'll discuss your hybrid cloud requirements, walk through the benefits and features that apply to your organization, and spin up an instance of GoAnywhere in the cloud to show you how easy it is to get started.

Request a Demonstration

BlueFinch ESBD

FRANCE : +33 (0)9 70 75 61 13

NETHERLANDS : +31(0)8 82 58 33 46

sales@bluefinch-esbd.com

www.bluefinch-esbd.com

Make an appointment