FORTRA

Using Managed File Transfer to Secure Your Cloud Data

Are you considering the move from on-premise operations to an external platform in the cloud?

Maybe you're just dipping your toes into the waters of this vast infrastructure. Maybe you've started moving pieces of your business to the cloud, and it's time to assess the security measures that best cater to your new environment. Or perhaps you're interested in deploying your business in a hybrid environment.

Whatever stage you're at, one thing's certain: you're not alone.

Many companies worldwide are shifting to cloud computing in order to minimize their reliance on in-house IT infrastructure and finicky business processes. However, the current state of cloud security is a real concern. 91% of organizations are concerned about cloud security, according to the 2018 Cybersecurity Insiders Cloud Security Report. When asked about the biggest barriers holding back cloud adoption, 39% of respondents mentioned general security risks.

Which begs the question: how confident are you that your data is secure? **Is your organization at risk in the cloud?**

What if we told you there's a way to improve the security of your cloud data, both in transit and at rest, so you don't have to worry about storing sensitive company information off-premises?

This white paper examines the pulse of the cloud, from why companies are leaving on-premise perations to the state of today's cloud security and file transfers. Use our guide to explore how a strong managed file transfer solution can help protect your data transfers, in transit and at rest, without compromising the convenience or cost-effectiveness of moving your business to a cloud-based environment.

Today's Cloud Adoption Practices

In a technology outlook survey from accounting firm BDO, 74% of tech-related Chief Financial Officers said cloud computing would have the most measurable impact on their business in 2017. In addition, nearly half of organizations expect cloud security budgets to increase in the next 12 months, according to the 2018 Cybersecurity Insiders Cloud Security report.

Despite this high percentage of investment, few companies are expected to move 100% of their business processes to the cloud. Industry analyst Gartner predicts that "90 percent of organizations will adopt hybrid infrastructure management capabilities" and "hybrid will be the most common usage of the cloud" in the next three years.

Cloud File Transfers

Most organizations oversee dozens (if not hundreds or thousands) of in-house file transfers a day. Whether it's sending files to employees, transferring reports to trading partners, receiving data from thirdparty vendors, or collecting sensitive information from customers, it's all part of the exchange of information that is regularly processed.

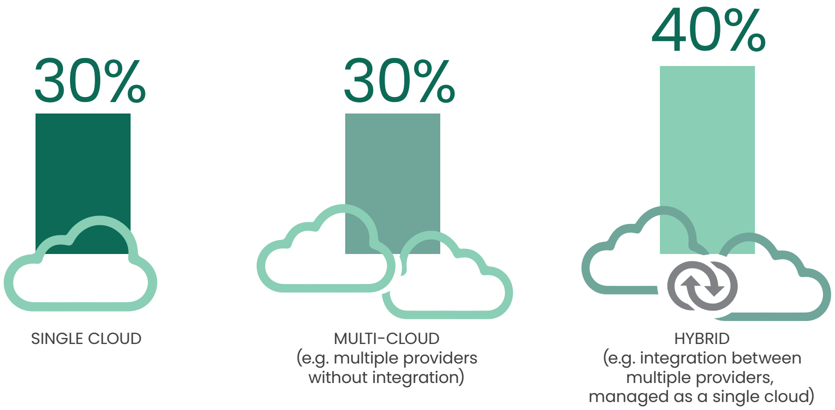
But what about cloud-based file transfers?

Cloud infrastructure can give companies a lot of leeway. Some data can be managed in the cloud, or all of it can be—the choice is entirely up to you. Moving data to the cloud is as simple as transferring files and folders to whatever storage platform you have with your provider. And with proper encryption and security policies in place, you can control who has access to that data in the cloud.

Data that's been entrusted to the cloud is kept in physical servers and data centers managed by cloud computing services. Almost all file movement between a business, its employees, its trading partners, and its remote locations can happen through the cloud.

Sensitive information can move quickly and efficiently between the business and wherever it's stored (often on servers around the world), which gives organizations the ability to operate smoothly and access their data from anywhere. Because everything is stored off-site, local outages and user errors are minimized, bettering the chances that important scheduled transfers will complete successfully.

What is your primary cloud deployment strategy?



Source: 2018 Cybersecurity Insiders Cloud Security Report

Security in the Cloud

The benefits of the cloud have enticed many organizations to adopt, or at least consider, some sort of cloud environment. Gartner forecasts that cloud-deployed organizations will experience fewer security incidents in upcoming years, and in general, cloud-stored data is often considered more secure than data kept on company-run servers.

Sadly though, data loss can (and does) affect those who move to a cloud environment. Take the 2017 RNC data breach, for example. The data firm they used placed an unencrypted database containing the information of 198 million American voters on an equally unsecured AWS server. If the firm had routinely monitored the cloud for vulnerabilities, the breach could've been prevented. But it wasn't.

The reality is, the cloud isn't 100% safe. Because of events like the RNC data breach, companies are wary of relinquishing their data to public, hybrid, and private cloud servers. In fact, a good majority of cybersecurity teams identify data loss, threats to data privacy, and breaches of confidentiality as their top three cloud security concerns, followed by regulatory compliance and data sovereignty.

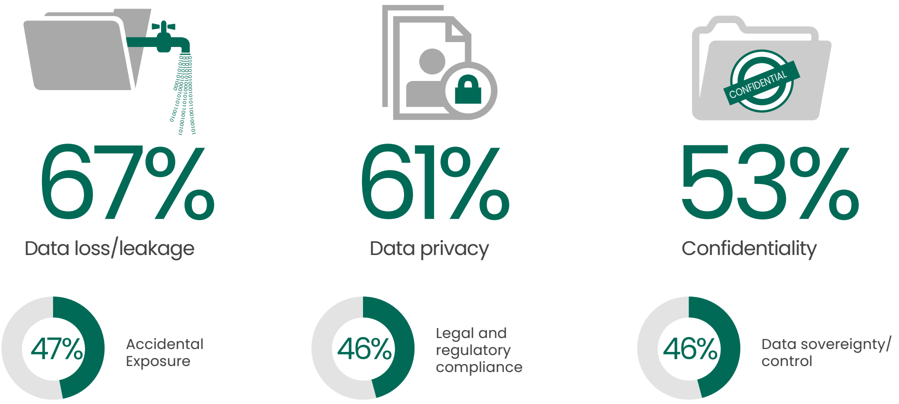
Furthermore, Forbes reports that over 40% of businesses surveyed have delayed cloud deployment due to a gap in their team's cybersecurity skills, and only 23% fully trust public cloud platforms to keep their data secure.

The Current State of Cloud Data Security

For cloud computing platforms like Amazon Web Services, Microsoft Azure, and Google Cloud, security of customer data is one of their highest priorities. They have a variety of resources in place to protect their clients' privacy, but despite their best attempts, these measures don't always stop data loss, compromised information, or unexpected cloud server outages.

Cloud security is a two-way street. Researching each cloud provider's cybersecurity methods and selecting the best one for your organization is imperative—a positive step toward ensuring your data's integrity. But it's not the only step. IT teams are just as responsible for the security of their sensitive business data as the cloud platforms that hold it.

What are your biggest cloud security concerns?



Source: 2018 Cybersecurity Insiders Cloud Security Report

Whether your organization is thinking of deploying to the cloud or already has, it needs to perform due diligence for its processes and policies. Start by asking questions like these:

- What are our top security considerations?
- How will our IT processes change?
- What vulnerabilities have been introduced or addressed from moving to the cloud?
- Do we have points of failure that should be planned for?
- Are cloud file transfers properly encrypted to minimize risk of data breaches?

Protecting Your File Transfers

Many of these questions are subjective, of course. Each IT team is likely to answer them in different ways, based on your company policies and processes. But to achieve the best possible cloud security, don't overlook the state of your file transfers.

Encryption is often the last line of defense between a malicious user and sensitive information. If data is properly secured during file transfers and when sitting on a server, a successful breach of the cloud is less likely to end in exposure.

For those that must be in compliance with regulations like HIPAA and the GDPR, following encryption requirements in the cloud comes with extra benefits—as long as the keys for encrypted data are safe, breached information can't be read, preventing hackers from selling or otherwise exploiting sensitive data.

File Transfers and the Cloud

When moving your data between your network and the cloud, it's considered best practice to always encrypt your files and protect your communication using secure network protocols like SFTP, FTPS, or SCP. Your files, databases, and even entire folders should be encrypted at rest, too, despite whether the cloud platform you've chosen already secures it.

A common approach to file transfers consists of using custom scripts created by internal programmers. The scripts often include commands for encryption, which may or may not be simple to modify depending on your given skillset.

This process for transferring and securing files can work for a while. It addresses basic company needs initially. But as the number of file transfers rise, so does the difficulty of maintaining a homegrown solution—and that's not including other possible roadblocks, like an inability to handle logging capabilities or alerts when a file transfer fails.

Managed file transfer (MFT) solutions provide organizations with helpful features that allow them to grow with their data exchange requirements, which is especially beneficial when moving to a cloud environment.

GoAnywhere Managed File Transfer

GoAnywhere MFT eliminates the need for homegrown scripts and multiple programs by streamlining the file transfer process. It can be installed in a cloud-based environment or on-premises via a variety of platforms, giving you full control of deployment.

Transfers can be scheduled and automated with custom workflows (projects), and data can be sent between systems, employees, customers, and trading partners. Meanwhile, administrators are given a single point of control with extensive security settings, audit trails, and reports, greatly reducing the possibility of user errors and oversights.

GoAnywhere also provides high return on investment by reducing the time spent on manual labor, improving the quality of file transfers, making security more cost-effective, and helping organizations meet a variety of requirements including PCI DSS, HIPAA, GDPR, and FISMA.

MFT Security and Encryption

All file transfers are protected with popular encryption protocols, including SFTP, FTPS, AS2, and HTTPS, in the GoAnywhere Managed File Transfer solution. A built-in key manager allows administrators to create, import, export, and manage Open PGP keys, SSH keys, and SSL certificates.

And for those who must comply with FIPS 140-2, validated encryption ciphers can be enabled for SSL and SSH protocols. GoAnywhere offers connections to a variety of servers and guarantees file delivery by using connection retries and file auto-resume. Admins can monitor transfer success, review account activity, and authenticate user access from anywhere via GoAnywhere’s browser-based interface.

Beyond basic encryption practices and features, GoAnywhere also addresses several business requirements for the cloud.

Cloud Requirement	Corresponding GoAnywhere Feature
Activity Alerts Your organization needs to know the exact moment a file is added, removed, or changed in the cloud.	**File Monitoring** GoAnywhere's file monitoring feature allows IT teams to watch folders on cloud-based systems and receive an email alert whenever an event is triggered.
Deployment to Cloud Computing Platforms Your organization wants to interface with an external application, like a trading partner's cloud-based portal, to send and retrieve important business files, schedule automated file transfers, and run advanced workflows.	**Commands, APIs, and Web Service Protocols** GoAnywhere provides commands and APIs for integration with external applications: system command lines, scripts, programming languages, third party schedulers, and more. Web service protocols like SOAP and REST are also supported, allowing easy interface with cloud computing platforms AWS and Microsoft Azure.
Connecting to Trading Partners Your organization needs to connect to internal and external trading partners in the cloud, while protecting the integrity of subsequent file transfers.	**Cloud-based File Systems** Internal and external trading partners can connect to your organization through folders on cloud-based file systems like Amazon S3 buckets. GoAnywhere also secures inbound cloud transfers from key stakeholders with SFTP, FTPS, HTTPS, and AS2 protocols.
Automated File Processing Your organization wants files in the cloud to be moved and processed automatically, instead of manually, to save time and labor costs.	**Scheduled Workflows** File transfers and workflows are easily configured to move and process files in your cloud environments and private networks. You can schedule these to run anytime using GoAnywhere's built-in scheduler.
Itegration with Cloud Applications Your organization needs an easy, safe way to transfer data to and from web and cloud-based applications and services.	GoAnywhere Cloud Connectors give you out-of-the-box integration with popular web and cloud applications and services, including Salesforce, JIRA, SharePoint, Microsoft Dynamics CRM, Box, and Dropbox, as well as an easy-to-use Cloud Connector designer where you can build your own integrations.

GoAnywhere and Amazon EC2

For organizations that use AWS as their cloud provider, GoAnywhere MFT easily integrates with Amazon Elastic Cloud Computing (EC2). You can find, and quickly install, GoAnywhere MFT on Amazon's AWS Marketplace.

You can use GoAnywhere's secure FTP technology to protect sensitive file transfers with strong encryption technology and modern authentication methods. This creates encrypted tunnels between client and server systems and provides confidentiality and integrity to critical transmissions. Secure FTP also protects any user credentials that flow over the connection.

Want to address high volumes of file transfers in your organization? With GoAnywhere's clustering technology, file transfers and other processes can be distributed across multiple Amazon EC2 instances for load balancing. And when an instance is taken offline, file transfers and jobs will be auto-routed to other installations in the cluster.

GoAnywhere and Microsoft Azure

For organizations that use Microsoft as their cloud provider, GoAnywhere integrates with Azure to provide IT teams with secure file transfers between all active parties.

Installing and running GoAnywhere MFT on Azure is an effortless process, as everything you need is included, reducing the need for additional third-party solutions. You can install GoAnywhere on your choice of Azure-supported Windows or Linux operating systems, then set up your trading partner accounts and file transfer processes.

GoAnywhere's intuitive design and modular features allow you to be up and running on Azure quickly.

If you want to scale GoAnywhere on Azure, file transfers and other processes can be distributed across multiple Azure VM instances for load balancing. Connections to a variety of databases including Microsoft SQL Server through GoAnywhere, and user accounts can be authenticated against Microsoft Active Directory to simplify user management for your file collaboration needs.

Conclusion

Organizations worldwide are turning their focus to the cloud. In fact, many have partially made made the transition and feel positive about its future. But security is still an issue, and moving to the cloud isn't without risk. To avoid data loss, IT teams must do due diligence and take steps to protect their data—starting with their cloud file transfers.

Implementing a managed file transfer solution like GoAnywhere MFT lets businesses control how their data is protected, in transit and at rest. Through strong encryption protocols, file monitoring, and integration with Amazon EC2 and Microsoft Azure, IT teams can rest assured that their data is safe in a variety of environments without running expensive, time-consuming scripts and programs.

Are you ready to enhance the security of your cloud data?

Get a free 30-day trial of GoAnywhere MFT.

Start A Free Trial

FORTRA

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.