Synchrony Connect

synchrony

5 THINGS TO KNOW

ABOUT CLOUD STORAGE

Cloud storage is a common way for businesses to back up their data. A cybersecurity breach on average costs a business $4.24 million,[1] so it's essential to be prepared and backed up. **Here's five things to know about what cloud storage is, what to store in the cloud, how to evaluate a provider, and most importantly, how to ensure business-critical data is protected.**

1. DEFINING CLOUD STORAGE

Cloud storage is simply data storage managed as a service. Business owners or individuals pay for data storage according to how much they use, usually on a monthly basis, accessing it from any internet-connected device. Data is encrypted to protect it against physical failures and cybersecurity breaches.

Most people already use cloud storage for personal use, from saving images on Google Photos or Apple iCloud to sharing documents on Microsoft 360 or Google Docs.

Cloud storage can often scale from personal storage accounts by upgrading to an enterprise or business subscription to provide added security and collaboration, as well as the ability to store more data.

Synchrony experts highlight **Microsoft Azure**, **Google Cloud**, and **Amazon Web Services (AWS)** as the three major public cloud providers that allow for the customization, security, and added data needs of businesses of all sizes, with a variety of cloud storage products and integrations.

Using cloud storage to solve more complex challenges or handle more data can mean an investment in something like **Amazon Simple Storage Service (Amazon S3)** as one piece of a larger business solution. More focused cloud storage solutions **focused cloud storage solutions** like iDrive Team or Dropbox can solve for business with less data.

2. CLOUD STORAGE AS BACKUP

Whether or not a business has a physical location, data is likely stored locally. Cloud storage can act as a second storage backup, because it meets the data security requirement of redundancy, that the copy is physically separated from the original. If customer data is stored on a computer in a location that suffers fire or water damage, data can be restored as long as the second copy wasn't also stored at the same location.

All cloud storage providers have their own redundancy built in, with data centers located strategically around the world. If one site goes down or is compromised, the redundancy means the uptime and security of the data with a storage provider will always be higher than any system a small business could create on their own.

Products like **network attached storage (NAS)** can also be used if a business has files that are too big to access via the cloud quickly but need to be redundant. NAS automatically archives a backup of a local computer onto a local, on-premises cloud for easy access.

3. WHAT TO STORE IN THE CLOUD

From customer data to raw media files to internal confidential documents, cloud storage can be used for an organization's financial, operational, logistical, and employment departments.

Customer preferences, full customer profiles, customer service data, and payment information can be stored in the cloud, along with employee records, inventory, and other types of sensitive data. Public data, or non-sensitive data like large source files for a product video or photo shoot should also be stored on the cloud.

Documents and files that employees share or collaborate on can also be stored in the cloud for quick access, allowing multiple people to edit and comment at once.

4. HOW TO SELECT A CLOUD STORAGE PROVIDER

Start with research. Publications like **PC Mag** and **Consumer Reports** collect and evaluate cloud storage providers and will give advice on which new and existing providers are worth investigating.

Synchrony experts recommend considering not only security, cost, collaboration capabilities, and file size limits, but also how devices can access stored data and how many of them will have what kind of access.

> **Be sure a cloud storage provider is routinely and transparently audited for compliance across a number of security and redundancy protocols and that all encryption standards are met.**

Scalability is another key factor when selecting a cloud storage provider, letting businesses upgrade the amount of storage easily as they grow. Some providers also charge for accessing, using, or transferring data, so considering how often data access is needed is also important. A stable, fast internet connection will also be necessary to ensure there's no lag when accessing cloud-stored data.

A consideration with a small business working with a large provider like Google or Amazon is tiered customer support, with 24 to 48 hour email response rates at the lowest tier. Big providers publish their SLA (service-level agreements) publicly for anyone to review as part of cloud storage research, but the larger value to the business by bundling solutions might be worth it.

It's also important to consider whether a cloud provider offers *at-rest encryption* in addition to *in-transit encryption*. In many cases, providers charge more to encrypt data when it is at rest. The extra cost can be evaluated if it's worth it to protect business-critical data.

Capability research and cost considerations will narrow provider options, and the top choices can be tested with a demo or trial period before a final decision is made

5. HOW TO STAY SECURE IN THE CLOUD

Staying secure means first knowing the capabilities of a cloud provider's encryption, uptime, and authentication documentation. Google products, even the free versions, have high-grade encryptions that are more secure than any locally stored hard drive.

> **Other potential weak points in data security can include point of sale (POS) systems, laptops and other mobile devices, other technology vendor integrations, as well as employees themselves.**

Business owners should keep a log of who is accessing their data and if it's appropriate. Create an audit trail of access to keep track of who is accessing what and when, so data theft doesn't occur if employees leave with the data or if there's a cybersecurity hack. Keep passwords on lockdown, keep local storage physically and digitally secure, and ensure no single employee has the only copy of anything. Security in the cloud is about redundancy as much as identifying entry and exit points, keeping data (and the business) safe.

For more information or to connect with an expert, contact us at **synchronyconnect@synchrony.com**.

Synchrony Connect is a value-added program that lets Synchrony partners tap into our expertise in areas beyond credit. It offers knowledge and tools that can help you grow, lead and operate your business.

This content is subject to change without notice and offered for informational use only. You are urged to consult with your individual business, financial, legal, tax and/or other advisors with respect to any information presented. Synchrony and any of its affiliates (collectively, "Synchrony") makes no representations or warranties regarding this content and accepts no liability for any loss or harm arising from the use of the information provided. Your receipt of this material constitutes your acceptance of these terms and conditions.

[1] **Cost of a Data Breach** IBM, 2021