eBook

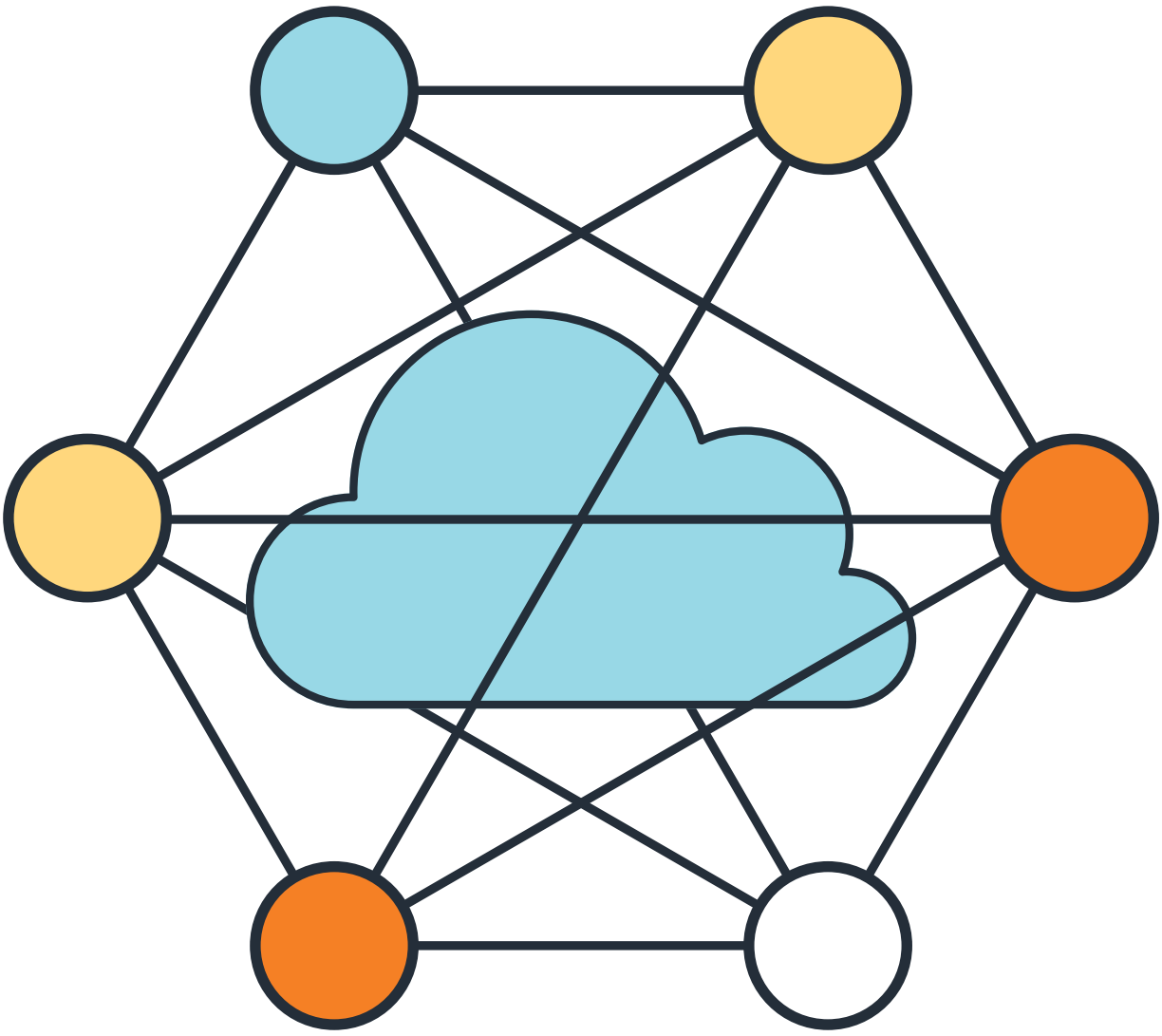
SECURITY IN THE CLOUD

Tips on How to Protect Your Data

PROCORE®

It's been around for years, but the concept of the cloud is still a difficult one for many to grasp. The name itself, simply a metaphor for the Internet, conjures up visions of important and private data floating around in the ether, which doesn't evoke a strong sense of security. However, cloud storage is much safer and secure than many on-site servers and hard drives.

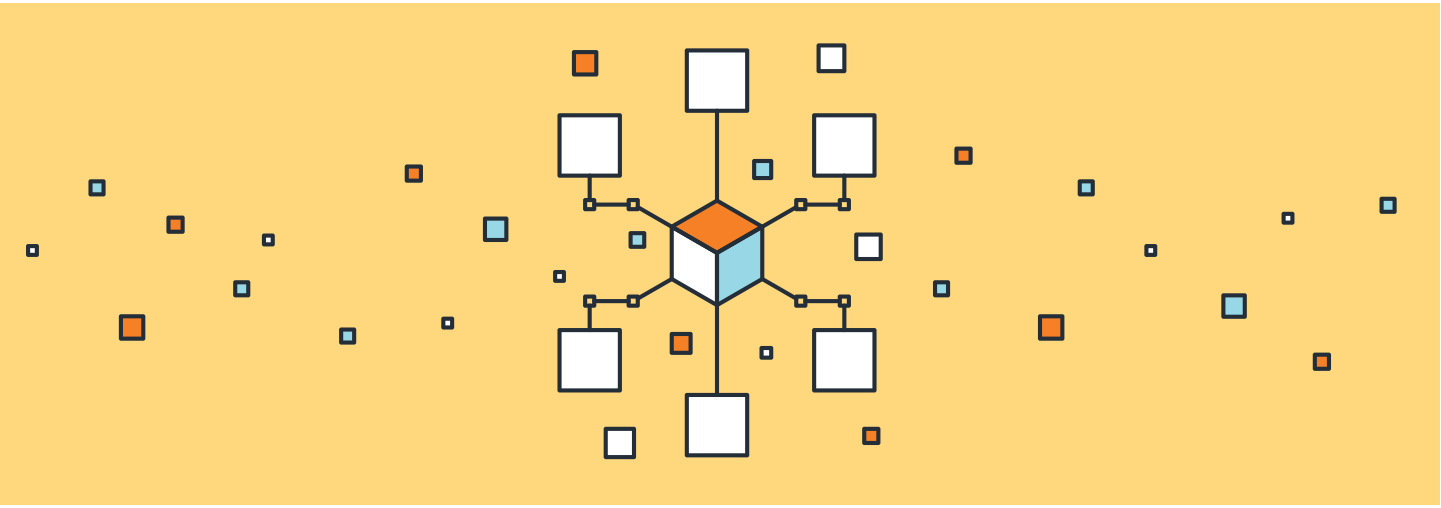
Though you ultimately leave the cloud storage service in the hands of skilled professionals, it doesn't hurt to understand how it works. Find out how the cloud is changing the technological landscape for businesses and what to look for when choosing a provider.



SO WHAT IS THE CLOUD?

It may sound like just one more buzzword that will soon pass out of our collective vernacular but, in reality, the concept of cloud computing has been around for decades. It's hard to pinpoint exactly when the word "cloud" was first used, but its origins lie in the early days of network design.

A network is basically a collection of computers and other devices (e.g., printers, servers, etc.) that share data over a wireless or cable connection. The best-known example of a computer network would be the Internet, but you likely have one in your home (connecting your personal computer, modem, router, printer, etc.) and office (connecting your computer, your coworkers' computers, printers, scanners, servers, modems, and routers).



In earlier years of network design, when engineers charted out their networks, it involved mapping nodes (the devices that originate, route, and terminate the data on the network). While a simple network such as the one you use in your home might involve three or four nodes, a larger network could feasibly have millions. In this scenario, when drawing lines to represent single links between nodes, the diagram can easily become a nebulous blur of connections, with much of the represented activity happening outside of the home or office. Many engineers grouped those external connections together inside a bubble or other similar shape, which led to its eventual designation as "the cloud."

THE CLOUD AS WE KNOW IT TODAY

These days, the term is understood as signifying data that is accessed online via the Internet. It's very likely that you've been using websites that use cloud storage without even knowing it—social media, email companies, and banks are just some of the many businesses that utilize the cloud when storing your photographs, emails, files, and other data. Cloud-based companies offer the following benefits:

Fast access: Cloud storage services have devices that are immensely powerful, which allows them to quickly locate and access the data you need. Think of the last time you went on social media and shared your vacation photos. Thanks to the cloud, your pictures were almost immediately accessible to those people with whom you wanted to share them.

Nearly infinite storage space: Your computer may have a lot of storage space, but the companies offering cloud storage services have vastly more. You don't need to worry about filling up your computer's disk drives, which slows its processes down—the cloud can handle it for you (without losing processing speed).

Shareability: Storing something on the cloud allows you to share it with anyone else who has access to the same service. If your coworker is several states away and needs an updated PowerPoint presentation, no one needs to hop on the next plane—just upload it to your shared drive on the cloud and they will have immediate access.

Think of cloud storage as a self-storage facility. When your belongings get to be too much for the home you live in, it clutters your space, making it difficult to move around and even harder to find something you're looking for. The perfect solution is an off-site storage unit, where you take all of your extra furniture and boxes, freeing up your home and making it easier to find the things you need. If you want to access your storage unit, simply make a trip over to the facility and grab whatever it is you need. Cloud storage is the same concept—move your excess data to an off-site storage facility, where it is easily and quickly accessible, freeing up space on your computer so it can handle more important tasks.

WHY CAN'T I JUST DO IT MYSELF?

Perhaps you've been storing your company's data locally on your company computers or on a server maintained by your IT department. Or perhaps you have outsourced it to an IT company. Even if you're pleased with how it has been working so far, there are several distinct advantages to utilizing cloud storage.

The most important of these advantages is security. It is likely that any client data you store contains contact and payment information, including addresses, phone numbers, credit cards, or other account numbers—information you absolutely do not want falling into the wrong hands.

Even if you have virus and malware protection on your company computers, computer viruses change so rapidly that protection can become obsolete if not updated frequently enough, (and even when it is, sometimes a new virus can pop up and proliferate before antivirus software engineers can provide updated protection for their product). A particularly nasty virus can completely corrupt your hard drive and wipe out all the data you have saved, which is disastrous for a business of any size.

There is also a threat of hard drive failure, which can occur randomly without any outside influence. A study done by Google shows that 8.6 percent of three-year-old drives fail; many small businesses rely on technology older than that, which only increases the odds of failure. While no one is truly safe from a natural disaster occurring, your office is likely to be much less prepared to handle earthquake, tornado, fire, or flood damage than a reinforced data center.

Cloud storage provides additional layers of security that, while not 100 percent guaranteed to keep your data safe, comes much closer than a local storage option. Most cloud storage services house their servers (where your data is stored) in highly secure data centers that are monitored by surveillance and multi-factor access control systems. An ideal data center is staffed around the clock by trained security guards and authorization to access the server area is extremely limited; in fact, much of the security tasks are performed by automation, eliminating the opportunity for unwarranted accessibility and potential errors. Additionally, many data centers require that personnel be screened when leaving areas that house customer data.

Cloud storage services not only provide security against physical theft or damage of your files, but also against intangible threats (e.g., corrupted files, server failure, etc.) by making frequent backups of your data in multiple locations, a process called “redundancy.”

GOOD STORAGE: CHEAP AT TWICE THE PRICE

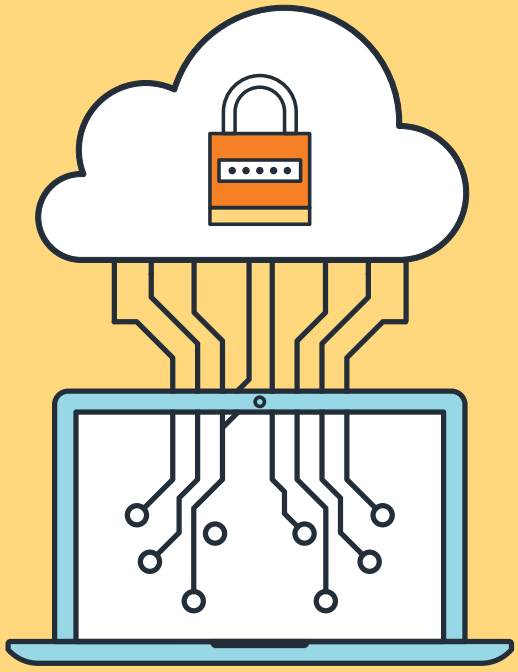
Think of the bills you pay in your personal life—electric, water, cable, Internet, gas, etc. For the non-necessities, you likely pay a flat rate for the entire month, whether or not you watch any TV or browse the Internet. For the public utilities that are necessities, you likely pay a scalable rate; the more you use, the more you pay. The majority of cloud storage solutions offer the same set up, making them work for most organizations regardless of their size and storage needs, from an individual all the way up to a mega-corporation.

Security features can also affect the price of a service. A business with sensitive data might be willing to spend a little more to ensure there are certain precautions in place, such as a remote wipe (the ability to delete files off of a stolen computer by using another device connected to the same cloud service or geo-redundant storage (copies of your data are stored at various data centers spread across a region in order to protect it in the event that physical damage, such as a fire, occurs at one data center). Enterprise cloud storage often comes with much more stringent security, better access to support, team management tools, and a price that covers all users, not just individuals.

SECURITY FEATURES TO LOOK FOR IN A PROVIDER

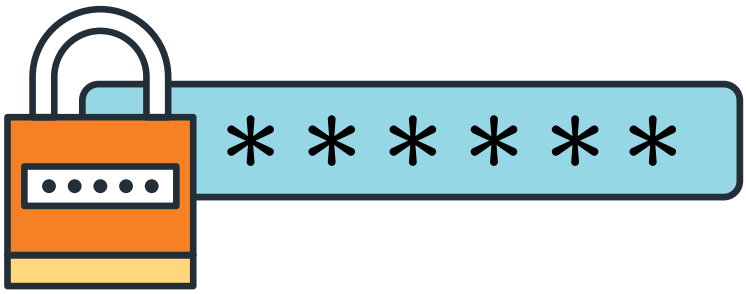
It can be overwhelming to look at the long list of cloud storage service providers and select one to store and protect your business data. Not only are there hundreds of companies with dozens of features to choose from, but many of the features are terms that the average layperson might not be familiar with. In fact, a study done in 2013 indicated that roughly 50 percent of cloud storage users didn't know what security measures their provider had in place, which means their private data could be at risk if they chose a company with weaker security.

One of the most common security features is encryption. This process converts electronic data into another form, called ciphertext, which makes it difficult to be deciphered by unauthorized parties. Think of the cryptogram word puzzles in the newspapers: these simple encrypted texts can be solved by hand by replacing the puzzle's letters with their correct corresponding letter. Many websites use sophisticated encryption to keep your sensitive data safe—including credit card information, Social Security numbers, bank account passwords, and other information you don't want anyone to see.



There are two main methods of encryption that websites utilize: symmetric-key and public-key (also referred to as asymmetric). In symmetric-key encryption, each computer has a secret key that it uses to encrypt data before it sends it over the network to other computers. The computers on both ends must have the key installed in order to be able to decode the contents of the encryption. To use the cryptogram example above, it would be as if you wrote a note to a coworker that said, "RTQVGEV AQWT FCVC." You and the coworker had both previously discussed that the key to your code could be solved by moving two letters up the alphabet, so they would know that your message was "PROTECT YOUR DATA." However, to outside individuals who might have seen the note, all they would see is indecipherable gibberish. This is the same process as symmetric-key encryption, though on a much smaller scale.

When the first major symmetric-key algorithm (Data Encryption Standard, or DES) was developed in the 1970s, it used a 56-bit key, which offers more than 70 quadrillion possible combinations. DES has since been replaced by Advanced Encryption Standard (AES), which uses 128-, 192-, and 256-bit keys, each exponentially harder to crack than the last. Data encrypted by AES-256, which the National Security Agency (NSA) uses for its top secret information, has 1.1 x 1077 possible key combinations that would take 3.31 x 1056 years—literally billions of billions of years—to crack via brute force.



Public-key encryption uses a public key to encrypt the data and a separate private key to decrypt, adding another level of security on top of what symmetric-key already offers. Another security feature found in cloud storage is [LC2] zero-knowledge password policy. Only the client knows the password to access their data—not the service provider. The provider can't even see the details of your files, except for how many you have and how much storage space they're taking up. If the government were to come knocking with a valid demand for your data, the service provider could hand it over, but it would be impossible for either side to decrypt it without the key (which only you as the client have knowledge of).

Security doesn't only mean protecting your private data from prying eyes, it also includes ensuring that data is safe from damage and your access to it remains uninterrupted. A provider should offer exceptional security at their data centers, including guards, strict guidelines about who can enter the building, redundancy across multiple locations, and protection against natural disasters (such as preventative steps against flooding, fires, or other small-scale disasters). Your provider should also have a continuity plan in place in the event that one data center goes down—a client should never lose access to their data in the cloud.

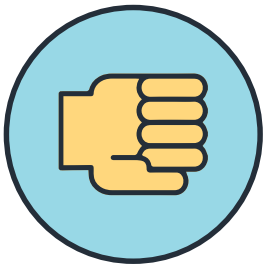
In summary, look for these security features in a provider:

- At least AES-128 encryption (or a comparable level)
- Redundant storage with scheduled backups
- Providers that offer proof of ongoing security testing against vulnerabilities
- Different encryption keys used for different customers
- Providers that allow you to create your own encryption key so that no one outside your company has it
- Providers that are transparent about the security measures in place at their data centers
- Expiration dates on private links shared (limits access to sensitive data)

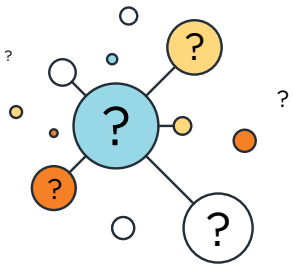
TAKE CHARGE ON YOUR END

While a cloud storage provider will handle all the maintenance, security, and other important tasks when managing your data, that doesn't mean that you shouldn't also be taking steps to protect yourself, your company, and your clients.

The first and most important step in protecting any sensitive information is having a secure password. A recent study has shown that 90 percent of passwords can be cracked in mere seconds, even if their creator thought it was complex enough. There are a variety of ways that passwords can be broken, including:



Brute force: Technology has developed to the point where some hackers rely solely on their device's computational powers to deduce your password. A brute force attack uses the incredibly fast processing speed of a computer to try millions of options for a password—for example, it will start with the assumption that the password begins with aaaaaa; when that doesn't work, it tries aaaaab, then aaaaac, and so on until it finds the right password. With modern computers as powerful as they are, a desktop PC could crack the password "lucky" in less than a second. Even the combination of upper and lowercase letters and numbers in "Lucky99" would take a computer only 14 minutes to crack.



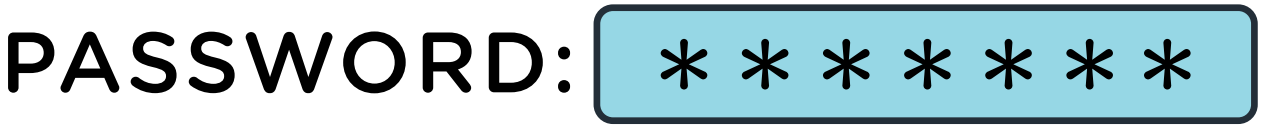
Simple guessing: With all we have to remember in our day-to-day lives, coming up with a complex password can be a headache. It's much easier to type 123456 to access your accounts than it is to type C0Mpl3xPhr4$e!, for example. A criminal who doesn't have access to any of your personal information or software that can do the job for him or her will generally be able to access your data by guessing if you have a simple password. Other no-nos include "password", "qwerty", or any other string of keys that sit in a row.

Social engineering: The next step up from simple guessing is someone who socially engineers their way into your account by already knowing something about you. If your beloved dog's name is Pookie, your anniversary is June 17th, you were born in 1978, and your favorite football team is the Cowboys, those are four pieces of information that can be used to guess your password (Pookie617, GoCowboys78, etc.). Try not to use special dates, names, or other identifying terms in your password; someone who knows you might use them against you.

Phishing: We've all heard of the "Nigerian prince" who offers you millions of dollars if you'll share your bank account information. This is phishing, where a malicious individual will masquerade as a trustworthy entity in order to get your password or other private information from you. If you receive any emails that are remotely suspicious, talk to your IT staff to discern if it's legitimate or not.

Spear phishing: This is a form of phishing that targets a specific organization or individual by pretending to come from a trusted source—for example, the "IT person" of your company, using a strange email address (e.g. enabduvh22@ixmx.ru), asks for your password in a message rife with errors. Most IT professionals make it abundantly clear that they will never ask for your password, so if you have any inkling that it might be a scam, delete it and let your IT person know. As technology advances, so do the scams; you can even receive a spear phishing attempt from what looks like someone you know, but make sure to look at the actual email address. If the message sets off any alarm bells, contact that person to make sure they were the ones who sent it.

To ensure a secure password on your end, which will in turn protect the data on the cloud storage end, use the following guidelines:



- Use at least 12 characters in your password
- Use a mix of upper and lowercase letters, symbols, and numbers
- Add random words to your password—they are easy for you to remember, and the longer your password, the more secure it is (BicycleEmbroidery4# would take a modern computer almost five quintillion years to brute force)
- Rotate passwords frequently
- Don't use the same password across multiple accounts (once they break into your Facebook account, for example, it's basically opening the door to your email password, bank account, and more)
- Develop a password "algorithm"—pick a word that you're guaranteed to remember and use it as the base for each password. For a particular website you use the password for, pull out an element of its name to add to your base word (such as the third letter, or the first and last). Finally, add a mix of numbers and characters to greatly increase the strength of your password. For example, say your base word is Pumpkin and your numbers and characters are derived from the last four digits of your old phone number (hitting the shift key for some of the numbers to add an extra element of security). Your password for Facebook, for example, could then look like FPumpkin48#@k; for Yahoo! email, YPumpkin48#@o; and so on.
- Check your password strength on a trusted website like https://howsecureismypassword.net/

SHARE THIS eBOOK!

Another step towards security is using multiple cloud storage service providers to spread your sensitive data across multiple services. If one provider faces a security issue, you avoid having all of your data compromised. If data loss is more your concern than sensitivity, consider doing your own backups.

Lastly, be alert when browsing the Internet. Some websites, even trusted ones, can be hiding malware or viruses, especially in their ads. Be aware of what computers you log in to; some browsers offer to remember your username and password, and if you accept that on a public computer, then anyone can log into your accounts. Even on your personal computer it can be risky—your usernames and passwords are saved in a place in your browser that can be easily accessed by anyone who uses your computer. Also, when downloading software or files, be sure they come from a trusted source, and read every text box that pops up on your screen during the installation. If you click "Continue" and breeze through all the alerts without paying attention, you might inadvertently give the software permission to install something you don't want on your computer.

CONCLUSION

Armed with the above knowledge, it should be easier than you initially thought to pick a cloud storage service provider, should your company be moving in that direction. Many major corporations, financial institutions, social media powerhouses, and even the U.S. government are using cloud storage, confident in its security and benefits.

SHARE THIS eBOOK!

PRODUCED BY
Procore Technologies, Inc.

Procore Technologies, Inc., the world's number one most widely used construction management software, helps firms drastically increase project efficiency and accountability by streamlining and mobilizing project communication and documentation. Hundreds of thousands of registered Procore users manage all types of construction projects including industrial plants, office buildings, apartment complexes, university facilities, retail centers, and more.

For more information about Procore, or for a free online demo, visit http://www.procore.com.

Schedule a Demo

WOULD YOU LIKE MORE RESOURCES?

Construction Blog > YouTube Channel > Resources >

If you have any questions, please give us a call at 1.866.477.6267 or email us:
sales@procore.com | support@procore.com

PROCORE

6309 Carpinteria Ave. | Carpinteria, CA 93013
866.477.6267 www.procore.com