SUNDOG

YOUR STRATEGIC IT PARTNER

Overcoming the Challenge of Cloud Security

WAYS TO SECURE YOUR DATA IN THE CLOUD

OVERCOMING THE CHALLENGE OF CLOUD SECURITY

TABLE OF CONTENTS

Cloud computing is a shared responsibility

Also known as cloud technology or just “the cloud,” cloud computing allows users to store, host, and access computer system resources through an online connection. Third-party cloud service providers (CSPs) own, operate, and maintain the data centers and servers where your data is stored.

When it comes to data security, CSPs adhere to a shared responsibility model whereby protecting the clients’ data is a responsibility shouldered by both the CSP and the client. To illustrate, the CSP takes all the steps needed to protect physical servers and data centers from damage and compromise. The CSP also handles all necessary software patches and updates and bears the cost of hardware upgrades.

However, CSPs have little to no control over their clients’ behavior, including the cybersecurity risks that may result from said behavior. For instance, downloading content that’s potentially laden with malware can compromise your data’s security despite the defensive measures implemented by your CSP. Customers must, therefore, be especially proactive in fulfilling their share of the responsibility in securing their cloud environments.

In this eBook you will learn the best practices you need to follow, as well as the behaviors you need to avoid, to ensure that your data remains secure in the cloud.

Best practices for cloud data protection

In his book *Secrets and Lies: Digital Security in a Networked World*, Bruce Schneier regards people as “the weakest link in the security chain.” This is because many instances of cybersecurity failure can be attributed to user error or bad habits. In fact, most types of malware require some kind of user input to be activated or downloaded onto a system.

Conversely, it’s also this need for input that makes users possibly your strongest first line of defense against cyberthreats. As long as you and your team know how to consistently identify, manage, and prevent unauthorized access to your cloud servers, you can keep your business’s data as safe as can be.

Here are best practices to follow:

1 Use strong passwords

Almost all cloud services require users to input a password to access or modify files. While passwords are generally a reliable authentication factor, weak passwords can be easily cracked and misused. In fact, over 80% of data breaches in 2019 were caused by compromised passwords.

Here are password-related mistakes many users commit:

- Using common and predictable patterns (e.g., “password” and “abcd1234”)
- Assigning personal information, such as their name or birthday, as their password
- Using the same password across several online accounts
- Not changing or updating their passwords regularly

These mistakes are, of course, understandable. A password shouldn’t be forgotten, so people make them as simple and memorable as possible. Unfortunately, passwords that are easy to remember also tend to be easy to guess.

Ideally, your password should be:

- **Long –** Most platforms require an eight-character password, while others require at least 12 characters.
- **Unpredictable –** If the platform permits passwords with special characters, you can use these to substitute some letters in your passcode. For example, you can use “7” and “$” as replacements for “L” and “S,” respectively.
- **Unrecognizable –** Try to avoid passwords that use known terms, such as your name or words one can find in the dictionary. You’re free to make up any random combination of characters, so take full advantage of that.
- **Mixed –** If the platform uses case-sensitive passwords, it's advantageous to use a combination of upper- and lowercase letters.
- **Unique –** Each of your accounts must have a unique password. Otherwise, crooks will only need to guess or break one passcode to access several of your accounts.

We recommend two methods of creating strong but memorable passwords. The first method entails coming up with a random sentence you can easily recall, ideally one that includes numbers and special characters. As an example, we'll use "At my first summer job, I earned $10."

Take the first letter of every word and the special character in the sentence, and combine these to get "Amfsjie$10." Switch up the cases of some letters and replace others with numbers and special characters. By doing so, you can get a 10-character complex password like: "amF$jiE$10."

The second method is called the Diceware method. This involves using ordinary dice to generate a memorable phrase composed of three or more random words from a word list like the Diceware List. The key here is randomness, so phrases like "winner takes it all" and "rock paper scissors" won't be as effective.

For example, in using the Diceware method, you spawn the phrase "red chocolate plastic belt." You can then switch up some of the letters' cases and replace the rest, including the spaces, with special characters. You can end up with a finished password like "rEd&chOc0laTe&p7Ast1c&BeLt."

Alternatively, you can use a password manager like Roboform. A password manager lets you store and secure multiple passwords behind a single master password. Your individual passwords are encrypted, so unauthorized users cannot read or use them. The app also remembers which passwords are for which platform, letting you create multiple unique passcodes without the risk of forgetting them and getting locked out of your account.

2 Employ multifactor authentication (MFA)

You can say MFA is an upgrade of the traditional username-password login requirement. True to its name, MFA requires users to input two or more authentication factors before they can access an account. To illustrate, after you provide your password, a system protected by MFA may ask you for:

Something you know	Information only you are aware of or have access to	• Personal identification number (PIN) • Answer to a security question • One-time code
Something you are	Biometrics or other information unique only to you	• Facial patterns • Iris pattern • Fingerprint
Something you have	An item, physical or digital, that only you have in your possession	• Physical key • ID or smart card • Software certificate

Should cybercriminals crack your password through either credential stuffing, social engineering tactics, or brute force attacks, MFA frustrates them by requiring something only you are likely to have. According to Microsoft, MFA effectively stops 99.9% of automated hacking attacks.

3 Secure data in transit

One common misconception is that cybersecurity measures should only focus on endpoints — devices that are connected to and communicate with a network. Endpoints range from the servers where your data is stored to the laptop computers or mobile devices you use to access said data.

The reality is much more complex than that. Data in transit is especially vulnerable to man-in-the-middle (MITM) attacks , which occur when cybercriminals intercept communications to either steal information or disrupt the traffic between the parties involved. With MITM, attackers can eavesdrop on transmitted data and access or steal sensitive information such as login credentials and personal details. They can also perform dangerous alterations, including injecting malware into your traffic.

These are what you can do to block MITM attacks and other threats to data in transit:

- **Avoid connecting to unsecured networks –** If you're accessing your cloud data outside the office, do not do so while connected to public Wi-Fi networks, such as those found in cafes, public libraries, or airports. These networks are not protected from malicious third parties who can easily hijack the connection, position themselves between you and your connection point, and steal data or plant malware.
- **Beef up your router's security –** Your office connection may not be safe either; crooks can hack into your router and do anything from bogging down your bandwidth to spying on your traffic and stealing sensitive information. Here's how you can prevent these from happening:
    - Update your router's admin credentials and assign a strong password.
    - Use a different service set identifier (SSID), which is the name of your network. The default SSID usually shows the router's brand and other details, which hackers can use to guess your password.

  - Enable WPA-2 or, if possible, WPA-3 encryption. These versions of the Wi-Fi Protected Access (WPA) security protocol are designed to keep unauthorized users from accessing your router's data.
  - Disable the remote administration function, which allows users to access the router using a PIN and not the password.
  - Keep the router's firmware updated. This ensures that the device is shielded from the latest known threats.
  - Install solutions designed to protect your Wi-Fi connection. If your anti-malware program has this feature, make sure to take advantage of it.

- **Encrypt your data –** Encryption renders data unreadable to any party that does not possess the encryption key. An encryption solution makes any data unreadable as it moves from one endpoint to another, making it a vital defense against eavesdroppers.
- **Use a virtual private network (VPN) –** A VPN lets you access data securely, even on a public network. It's like a tunnel that connects you to your intended destination in cyberspace, protecting you from threats such as hackers and malware. A VPN also grants you anonymity by masking your IP address and encrypting your data.

4 Manage permissions properly

The ability to control who has access to your files in the cloud is a powerful defense against data breaches. After all, if everyone in your team has access to the same level of information and privileges, all a hacker has to do is steal anyone's login credentials. Then they'd be able to do as they please to any files in your cloud server.

According to the zero trust security model, users must have access to only the files and privileges they need to perform their tasks. Your interns, for instance, are not likely to need access to cash flow figures unless their job description says so specifically. Moreover, your HR team does not need the same privileges that your IT department has over matters that concern your IT network.

It's best to pair access controls with a verification measure like MFA. This way, if a cybercriminal is able to obtain the password of an admin account, they still need to supply other credentials to successfully gain access.

5 Be wary of online scams

Cyberattacks are very rarely a frontal assault in which hackers openly barge in and try to get into your system. In most cases, they employ deceitful tactics and take advantage of human emotions, such as fear, uncertainty, and even impatience, to get users to do as cybercriminals please. These are what make online scams so dangerous and effective.

! Most common types of online scams

Phishing scams

These usually take the form of emails that look like they come from entities you do business with, such as your bank, vendor, or customer. Many phishing emails trick victims into providing sensitive information, like login credentials and payment details. Others fool victims into visiting malicious websites or downloading malware-infested attachments.

Social media scams

In these scams, a hacker may take control of a friend's or a co-worker's social media profile and use it to send you a link via personal message. Clicking on the link automatically downloads malware onto your computer.

Fake apps

These are apps that imitate legitimate applications in an attempt to steal personal information. Banking apps are a frequent target by cybercriminals who want access to victims' bank accounts.

Of these fraudulent schemes, phishing is perhaps the most concerning. For the past several years, phishing attacks have been among the leading causes of data breaches. The trend isn't likely to change anytime soon.

Here are tips to avoid online scams:

- **Educate your staff –** Online scams cannot harm your business as long as no one in your organization interacts with them. One of your best defenses, therefore, is an educated workforce. Train your staff not to open suspicious emails. On the off chance that they do, they should not click on links or download attachments. They must also learn how to detect phishing emails.

Signs of a phishing email

Sender

- Phishing emails look like they come from an important person or organization. They may even look like they come from an executive in your own company.
- The email comes from a different, unfamiliar email address.
- The sender's address may also be a rip-off of a legitimate domain (e.g., xx@gnnail.com instead of xx@gmail.com).

Links or attachments

- Phishing emails instruct users to visit a website through a provided URL.

Links or attachments

- The link may be unrelated to the content of the email (e.g., a link to a coupon in an email that's supposedly from your bank).
- The email contains an attached file that you have to download.
- The attached file is usually an executable file (i.e., ending in .exe), a Microsoft document, or a PDF, although other file types may be used.

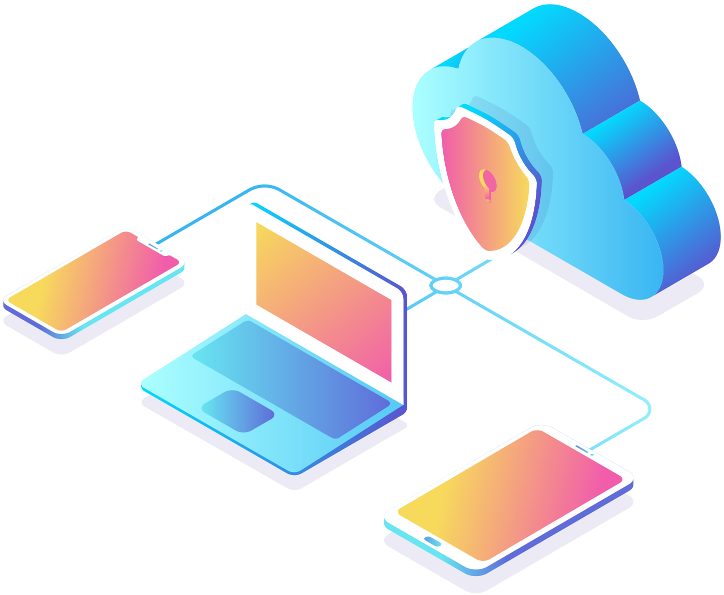
Contents

- Phishing emails usually have a catchy subject.
- The content, including the subject, likely has misspellings and grammatical errors.
- The subject and the content of the email may be unrelated to each other.
- If you're familiar with the purported sender, you may notice words or phrases in the email that they won't normally use.

Tone

- Phishing emails are designed to evoke human emotional responses.
- The email usually demands urgency by threatening negative consequences, including lawsuits or loss of money.
- The email may also promise something good, like freebies or exclusive knowledge.

- **Be mindful of your social media behavior –** Your social media posts offer hackers plenty of clues about your preferences, the issues that matter to you, and even how they can reach out to you. All these indicate your susceptibility to scams and can be used to your detriment. Avoid posting private information and make sure your profile is secure.
- **Be careful who you trust –** Just because you're seeing your friend's profile photo doesn't mean you're actually talking to them. If you feel that the other person is asking for information they normally wouldn't inquire about, don't hesitate to confirm with them through a different medium, such as a call or text.
- **Download apps only from official app stores –** Installing apps from anywhere but the Apple and Android app stores is extremely risky. While several malicious apps have been found in these app stores in recent years, they remain among the safest sources of applications nowadays.
- **Update your passwords regularly –** Should you fall victim to a scam, rotating passwords will prevent crooks from accessing your cloud data using your old passcode.



6 Use a private cloud

A private cloud is a cloud environment built exclusively for your organization. In this arrangement, it's possible for you to own and maintain the servers yourself, or a third-party CSP can do it for you. The servers may also be located on-premises or off-site. In any case, the private cloud's hardware and other resources are solely for your company's use.

Advantages of a private cloud

Security Because the cloud's resources are dedicated to your company, you're free to implement higher levels of security to protect your data. Your files are also less likely to be exposed to online threats.

Control You can customize your private cloud according to your business's specific needs.

Scalability A private cloud caters only to your organization, so you can scale resources up or down as needed, add new software, or implement updates.

Disadvantages of a private cloud

Cost

A private cloud is bound to be pricier than a conventional public cloud. Depending on how the cloud environment is set up, you may have to pay for hardware and all the needed software.

Maintenance

Keeping a private cloud running is also costlier than doing so with a public cloud. In many cases, companies need an IT department to handle the cloud's maintenance.

Take these pros and cons into account before deciding whether or not to invest in a private cloud. Alternatively, you can consider investing in a hybrid environment, which offers the security benefits of a private cloud but at a potentially lower cost.

7 Choose the right cloud provider

CSPs are not created equal. How secure your cloud data is has much to do with your choice of CSP. For this reason, as you search for the right provider to partner with, examine how secure your candidates' systems are. You must also investigate the methods and tools they employ to guard their clients' data.

A provider whose services are worth looking into must utilize these security measures:

- **Artificial intelligence (AI) –** The cybersecurity applications of AI can be leveraged in cloud security. AI can be used to scour historical cyberattack data, and learn and identify patterns and tactics used by cybercriminals. In this way, an AI security tool can detect attacks before they cause lasting damage to the cloud servers and the files stored within.
- **Firewalls –** CSPs employ both internal and advanced firewalls that check incoming traffic and confirm they're safe. Firewalls are among the go-to technologies for keeping malicious and unauthorized parties from gaining access to your data.
- **Event logging –** The provider's system must maintain a record of security "events." These events could be something as mundane as normal traffic to something as suspicious as a failed login attempt. Events can be used to identify vulnerabilities in the system as well as determine attack patterns.
- **Intrusion detection system (IDS) –** An IDS monitors the provider's system with the goal of identifying policy violations and suspicious behaviors in network traffic. Any anomalous activity detected is reported to the system administrator and recorded for future reference.
- **Encryption –** The CSP must have their own encryption solutions to protect your files from unauthorized access. These solutions can vary depending on the needs of their customers or the nature of data they aim to protect.
- **Redundancies –** The provider must have more than one server spread across multiple locations. Additionally, they must save multiple copies of your files. These redundancies ensure that should your files or server be compromised, you would still have access to your data.
- **Security testing –** A good provider tests their current security measures, preferably with the assistance of a third-party security company. Testing uncovers possible vulnerabilities and ensures that systems are protected against changing threats.

How can Sundog help?

If you're searching for technology that can empower your business, but haven't considered investing in the cloud, then now is the best time to get started. Storing your files in the cloud is convenient and efficient, and can save you a lot of money. It's also one of the best tactics to keep your data out of cybercriminals' reach.

At Sundog, our cloud services do not just cover storage — we protect your data too. We keep ourselves updated on the latest threats and ensure that our systems are more than adequately defended against them.

As we have discussed in this eBook, cloud security is a partnership between client and provider. We can also help you in that regard. Our team is composed of cybersecurity specialists — we'll be more than glad to set you up with best-in-class solutions, answer your questions, and offer recommendations on how to protect your organization's data.

CONTACT US TODAY!

Phone: **(815) 991-2400** Email: **yourteam@sundogit.com**

SUNDOG

YOUR STRATEGIC IT PARTNER

www.sundogit.com