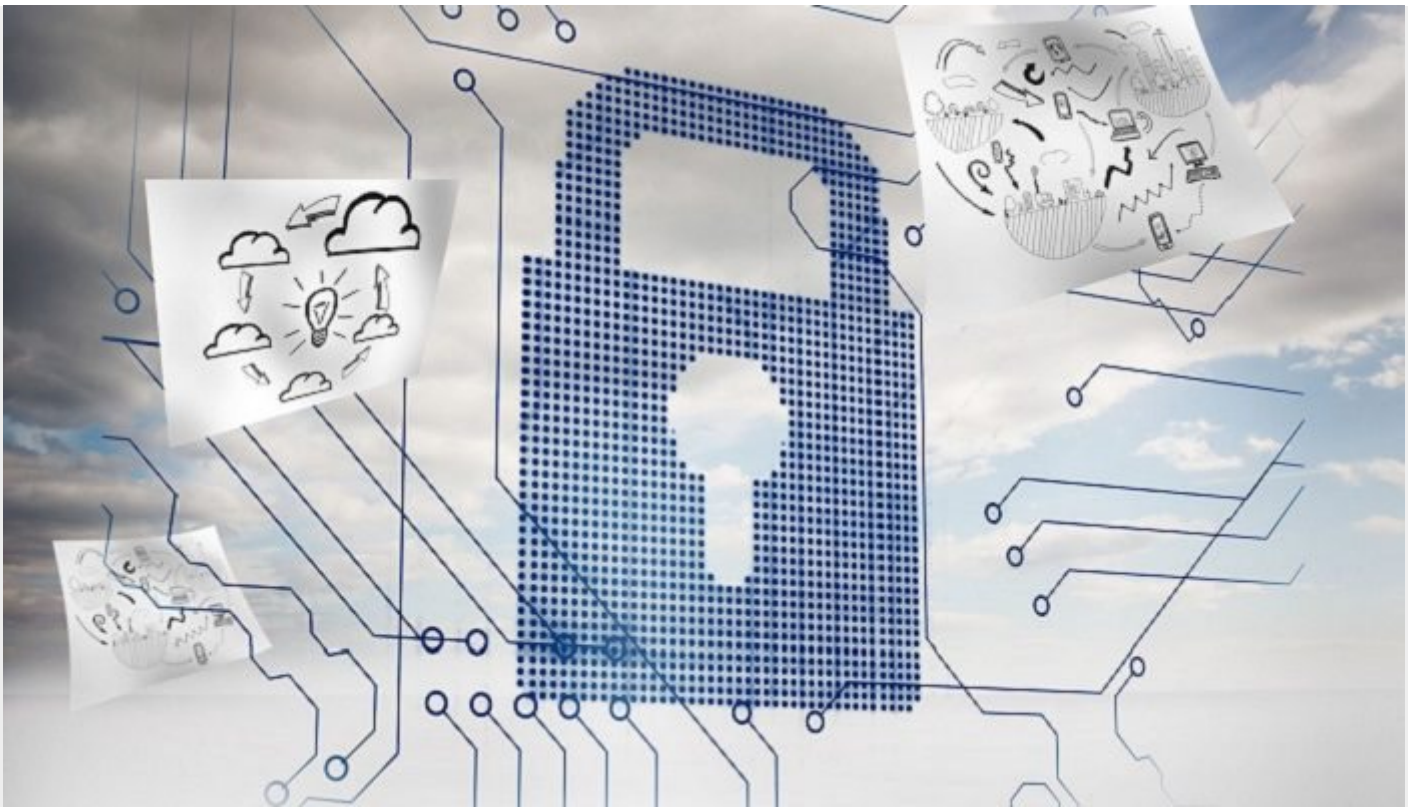
3 TIPS FOR EFFECTIVE CLOUD SECURITY



Cloud computing has revolutionized the way we do business. The cloud allows for increased productivity, making sure employees and stakeholders can access the files they need from anywhere at any time. This is particularly helpful in the event of a global emergency that requires people to stay in their homes and limit face-to-face interactions. The cloud also allows companies to reduce cost, stay agile with certain functions, and try out new products easily.

Most businesses keep at least a portion of their data in the cloud. Despite the innovations in cloud security, no cloud service can be completely immune from security threats such as:

- Hacked accounts
- Malware
- Loss of data
- Accidental changes or deletions
- Abuse of privileges

Losing important data can have severe, long-lasting effects for business owners, employees, and customers. While these threats will always be present, it is possible to minimize them, ensuring your organization's data remains secure while enjoying the benefits of cloud computing. Follow these tips to further protect your business from potential security breaches.

Back up your backup

Any system can fail—even those from Amazon, Microsoft, and Google—but your business doesn't have to. It is vital that an organization plan for the eventuality of a server crashing, a disk being damaged, or a security breach. It's always wise to back up important files in more than one location. Much like building reliability and resiliency into your systems for dependability, you can also build this dependability into your data.

When you store important data on the cloud, a best practice is to securely back up your *original* backup. Here are the two most common ways of backing up your data:

Local backup

Using a local/on-prem storage solution as a backup is great for prompt access. If something goes wrong on the cloud or with the network, recovering data from a local server is much faster than waiting for a virtual system to make the connection. (And we know how vital speed is for customer satisfaction during incidents.) This is especially true if you need to recover a significant amount of data.

Backing up your organization's data locally can require more of an up-front investment in hardware and office space, but it does provide piece of mind for those who like to keep their important files close and in their control. While a local server may be quicker and easier to access in a pinch, it is still susceptible to the unexpected. On-site storage can fall prey to environmental factors such as a loss of power, a fire or flood, or something as simple as overheated equipment. This is why it is critical to diversify your back up plans.

Cloud-to-cloud backup

Cloud-to-cloud (C2C) backup solutions are becoming increasingly popular. Utilizing a second cloud to back up your data often offers more comprehensive protections than a local storage option. If the office network is attacked, data backed up on a C2C server is immune. Of course, C2C ensures that your backed-up data is accessible from anywhere. Plus, restoring from C2C is more flexible because it is possible to customize the back up to specific machines.

Overall, the initial cost of C2C is lower as there are no costly hardware expenditures, but it is important to note that services are scalable and costs can rise easily as the volume of data increases. Additionally, certain third-party providers charge a fee to recover data lost on their systems. It would be wise to assess these costs *before* choosing a provider. With C2C storage, security measures are twofold, coming from both the provider and any in-house strategies you may apply. However, having your data on two different cloud servers does add another opportunity for internet-based breaches.

Double encrypt your data

When it comes to data security, encryption is a known best practice. Even if the wrong person gains access to your documents, their login attempt will fail without the decryption code to unscramble it. When shopping for cloud providers for your organization, be sure to choose services that offer encryption services.

Furthermore, you should be encrypting your own files before you upload them to the cloud. This provides an extra layer of security, and it protects your data from the service provider and its administrators. There are third-party encryption tools that will encrypt and add a password to your files before you upload them anywhere. If you encrypt at the file level before uploading, and then use a service that encrypts as well, you will be doubly protected.

Manage user access

The biggest risk to cloud data security is the unpredictability of its users. The cloud is an essential way to keep employees connected and to maintain up-to-date files. However, giving employees access to vital documents from a variety of access points increases the risk of something going wrong.

Organizations need to be strategic when planning how to manage the way users utilize the cloud. Here are two common ways to control user access:

Implementing permissions

Most employees don't need access to every file or application. One way to limit risk is to set levels of authorization. Only allow access to what is needed for an employee to do their job. This prevents users from accidentally causing damage, and it protects from hackers who may have acquired the employee's login credentials.

In addition to controlling who can access data, focus on who has permission to edit and share. In many cases, someone may only need to view the pertinent information. To do this, your IT department can define groups and assign privileges. This limits the odds of data being accidentally changed, deleted, or shared to the wrong party.

As important as it is to manage the access of current employees, it is also vital to have a plan for departing employees. Organizations should have a clear and comprehensive off-boarding process in place to ensure that former employees can no longer access customer information, systems, intellectual properties, and other data.

The more humans that have access to your information, the more at risk you are. Even if a user isn't purposefully trying to harm the company, they can fall prey to a phishing scam or log on using an insecure network. Limiting downloads to pre-approved networks and devices also goes a long way.

Educate and promote transparency

With all the above regulations in place, it is impossible to control the behavior of every user at every moment. For example, employees may access their own cloud storage providers over the company network.

This shows the importance of regulating which cloud providers employees are using for company business as well as communicating with complete transparency *why* these regulations are in place. Stay updated on trends and safety statistics of third-party cloud storage services and communicate this to staff.

Furthermore, scammers and so-called "social engineers" are consistently refreshing the tactics they use to acquire information. In order to keep data secure and to cut down on the opportunities for human error, organizations should provide anti-phishing training regularly. If employees are

informed, they will be better prepared when, not if, they are targeted.

Cloud security protects your business

Cloud computing allows businesses to increase productivity and connectivity. While most providers have security measures in place, it is important for organizations to take initiative in protecting their own data. Utilizing these methods in addition to keeping anti-virus software up to date, using multi-factor authentication, and encouraging the use of strong passwords can help to ensure the security of your data and, ultimately, your business. Of course, for the utmost in cloud security, a cloud management tool with a focus on minimizing cost and maximizing security might be exactly what you need.

Learn more about cloud strategy and security with these BMC Blogs:

- How to Secure Your Public Cloud
- The Cloud: Here, there and everywhere
- Getting Started With a Multi-Cloud Strategy
- Advantages of Cloud Computing: 5 Benefits
- Best Practices for Cloud Ops Success