Best Practices for Backing Up Your Data

Innovation and change are what drives almost everything we do in the digital world. But for more than a half-century one imperative has remained constant — backing up your data. While the reasons for doing so have evolved over time from protection against natural and man-made disasters to today's ever-increasing risk of cyberattacks, having a robust data backup process in place continues to be a must for any organization.

While it may require a considerable investment of time and resources, the cost is far less than the burdensome task of re-creating data for which no backup exists. Frequent and well-executed backups are vital assurance against a data-loss catastrophe that could cripple your organization at any moment. Although having a robust backup strategy is an integral part of a healthy security posture, it should never be a replacement.

How important are data backups?

The backup landscape has changed dramatically in recent years. It used to be that managing a robust and effective backup process was an expensive proposition — with storage capacity requiring external hard drives, magnetic tape, and other costly equipment, as well as the personnel to carry it out. Today, however, storage is much cheaper, largely because organizations can now back up their data externally with any of a number of cloud services offering automated, seamless, and faster solutions. At the same time, however, the movement of backed up data into the cloud has created new opportunities for threat actors to gain access to it and steal it.

Ransomware: An old threat gets new life. The reemergence of ransomware as a threat is reason enough that any organization should have a robust process to keep stored data backed up and safe. Some would argue that performing regular backups is among one of the best ways to be fully protected against ransomware.

Threat actors are upping their game — and getting nastier. In Crypsis's 2020 Incident Response and Data Breach Report, we reported that a growing percentage of the incidents we handle include the deletion or disablement of backups, which can be potentially crippling to an organization. Treat your backups as mission critical data in case you are struck with ransomware that makes live data unusable. There should be a physical or logical barrier between your computing environment and your backup environment.

TOP OPTIONS FOR BACKING UP DATA

Remote Backup via the Cloud

The cloud offers an easy, fast, efficient, and scalable option, particularly for small and medium size companies. Unfortunately, it offers those same advantages to threat actors who want to steal or destroy data. Restoring backed up data in a disaster also requires that you have an internet connection.

Local Backup via Internal Hard Drives

Local hard drives can be reused, solid-state hard drives are inexpensive, and both can be easily secured through encryption. Plus, organizations maintain direct control of their data. This option may work well for smaller organizations, but its limited scalability is the key reason many look elsewhere for backup solutions.

Removable Storage via Magnetic Tape or Optical Drive

These scalable solutions enable organizations to store backup data offsite and protect it from damage. They are also easily secured in case of theft. However, they are costly, particularly for small and mid-sized organizations, many of which use SnapShot software instead.

What are the latest best practices for backing up data?

While stories of how just one crucial backup saved a victimized organization from unmitigated disaster exist, this is no longer the norm. In today's environment, threat actors have many clever ways to either corrupt your data (ransomware), steal your data (data exfiltration) and use it, or misuse your data (fraud) once exfiltrated. To increase your chances of ensuring your data's confidentiality, integrity, and availability, you need a multifaceted approach that focuses not just on the backup process itself but also on how your backed-up data may one day be used.

The ultimate best practice in backups.

Following the U.S. Department of Homeland Security's **3-2-1 rule** is perhaps the greatest defensive stance you can take.

Keep **3** copies of any important file: 1 primary and 2 separate backups.

Keep the files on **2** different media types to protect against different types of hazards — from among cloud, hard-drive, and removable storage options.

Store **1** copy offsite and away from your main facility.

Consider your recovery strategy.

Too many organizations take a blanket approach to backing up, treating all their data the same. If and when they experience a cyberattack, they can face significant challenges in locating the data they need to quickly get systems back online. They may also discover that critical, dynamic information was being backed up with the same frequency as old files that hardly ever change.

To avoid such a dilemma, you should proactively plan out the steps you would need to take to quickly restore systems under emergency circumstances, with your files wiped out and your operations at a standstill. These considerations will help you develop the right approach to backing up your data and, if attacked, to recover your data and resume full operations.

- **Assess retention span.** The more data you back up, the more you will have to deal with under trying circumstances if you need to restore data after an attack. Avoid information bloat by eliminating from the data process data that will never change — and thereby can be taken out of the backup process and permanently stored.
- **Practice good data hygiene.** In the vast majority of cases, an organization does not have to spend an enormous amount of time and resources backing up all its operative data on a frequent, priority basis. A data loss prevention (DLP) solution can enable you to easily classify your data and separate that which needs to be backed up monthly from other files (like financial records) that should be backed up weekly, or even daily.

Be cloud conscious.

Cloud backup solutions offer enormous scalability, efficiency, and ease of use, particularly for small and medium sized businesses. However, they also create new opportunities for cyber criminals. It is important to remember that ransomware and other forms of malware can spread into your cloud backup and continue to cause an array of problems. Taking the following measures will help keep threat actors out of your cloud drives:

- **Carefully check the security practices of your cloud backup provider.** Ensure that they follow established network security recommended practices, such as the use of firewalls and measures to prevent your data from leaking to its other customers. Consider requesting third party validation of security practices or any statements made by the vendor about their compliance, such as SOC 1 and SOC 2 documentation.
- **Encrypt your backup.** No method or approach to backup is going to keep your data 100 percent safe. Encryption will not protect your data from an attack but it can protect it from exfiltration. For that reason alone, you should always run an encryption tool with all your backup solutions, especially those that back up to the cloud.

Other best practices to consider.

- **Stagger your backup schedule.** Scheduling your backups at different times avoids the overburdening of your network with excess traffic.
- **Regularly test your backups.** If an incident wipes out your data, the last thing you want to discover is that your backup files are corrupt. Your IT specialists should perform a full restoration test from backups at least once a year.
- **Think outside the office.** Consider whether your backup processes should include your email system and data stored on your employees' mobile devices, their laptops and home computers, or your website.

A faithfully executed backup plan is an essential part of your overall security strategy. Even if all else fails, you know you will have secure data to help get your organization back online quickly and operating at full strength. While backups have always been critical, the significant recent growth in cyber threats has underscored the urgency of a business recovery process. Ideally, you will never have to find out the true value of the time and resources your organization invests in a robust backup operation.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com