



ENJOY SAFER TECHNOLOGY®

SIX WAYS FOR YOUR BUSINESS TO BACK UP DATA

Six ways to back up your data and protect your business

By Alan Martin, ESET Staff

Is your organization performing regular data backups? We hope so.

Scheduling regular backups should be part of your business continuity plan. Not only does it make sense in case of a natural disaster or employee error that causes data loss or a system failure—it gives you more options for recovery in case of a ransomware attack. This is a particularly nasty strain of malware that encrypts your files and threatens to delete them if you don't pay a ransom within a certain time period.

ESET doesn't recommend giving in to ransomware demands for many reasons both ethical and practical (not least because you mark yourself as a possible target for future attacks), but if your files are all safely backed up, you won't even feel tempted to negotiate with them in the first place.

Businesses have several options available for backing up data, all with their own pros and cons. Using more than one backup method for additional security is highly recommended.



1. USB stick

Small, cheap and convenient, USB sticks are everywhere, and their portability means that they're easy to store safely, but also pretty easy to lose. There are physical limits on the number of write cycles they can take, so they should be supplemented with other backup methods.

For extra peace of mind, choose a proven USB drive such as the [Kingston DTVP 3.0 USB Flash drive with DriveSecurity by ESET](#). It protects drive content from malware and secures the data with 256-bit encryption as well.

Pros:

- + Extremely portable
- + Very cheap
- + Can easily transfer data to other sources

Cons:

- Portability means they're small and easy to lose
- Write cycle limits means longevity may be shorter than that of a hard drive



2. External hard drive

External hard drives are just what they sound like—hard drives that live outside your computer, meaning they can be plugged in to other sources. If using them for backup, it's best not to use them as an "extra everyday hard drive"—instead, designate one particular drive solely for backup and always disconnect it when the backup has finished. This is particularly true in the case of ransomware. For example, if you back up your computer to an external hard drive, but leave that drive connected when you are not doing backup, some ransomware will try to encrypt those backup files as well.

Pros:

- + Relatively cheap
- + Plenty of storage space for larger files

Cons:

- Potentially open to problems which lost files in the first place (a power surge or malware)

3. Time machine

For the Mac® users out there, Time Machine is an option that backs up to external hard drives automatically. Apple sells its own brand of dedicated wireless Time Capsules, but you can use any hard disk for it. Using this method, you'll automatically keep backups hourly for the last 24 hours, daily for the last month and then weekly backups until the machine is full.

Pros:

- + Automated, meaning you don't have to remember to stay up to date
- + Frequency of backups means you should never be too out of date
- + Backs up whole drive, not just the key files

Cons:

- Dedicated wireless machine is expensive
- Mac only

4. Network attached storage

At one time only larger organizations tended to back up their files to network attached storage. But since prices have come down, a dedicated wireless storage solution is a convenient option for even small or home businesses. And since you can set automatic backups, it requires little thought.

Pros:

- + Automatic backups mean you don't risk forgetting
- + Wireless solutions also work with phones and tablets

Cons:

- Can be expensive
- Can be awkward to set up and maintain

5. Backup and recovery solutions

Backup and recovery solutions such as [StorageCraft® ShadowProtect®](#) reliably back up everything from systems to data, enabling a fast recovery in the event of natural disaster, hacking attack or computer failure. StorageCraft is a data-, applications- and systems-recovery solution for both physical and virtual Windows® IT environments. It creates sector-level backup images of a disk drive, including not just data but also the operating system, applications, services and configuration settings. Suitable for businesses of any size, backup and recovery systems may also be implemented by home users who want comprehensive backup of all their data and systems or want to ensure business continuity for a small or home office.

Pros:

- + Backups can be scheduled to occur automatically
- + Backup includes entire disk drive: systems, applications, services, configurations, settings, and data
- + Allows you to quickly and easily boot any backup image as a virtual machine

Cons:

- Can be expensive

6. Cloud storage

While network attached storage is essentially your own cloud server, there are plenty of third party cloud storage options around: free, paid, or free with paid extras. iCloud, Dropbox, Google Drive and OneDrive are big names, but others are available.

Pros:

- + Can be done automatically
- + A certain amount of space is usually free
- + Device agnostic

Cons:

- Requires an Internet connection to work
- You can't account for their security breaches
- Companies aren't obliged to keep these services around forever

Too often, companies take their valuable data for granted. So whatever backup methods your business implements, be sure they're completed on a regular basis—ideally, once every 24 hours. At minimum, backup should be completed once a week.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.



© 1999-2016 ESET, LLC, d/b/a ESET North America. All rights reserved.

ESET, the ESET Logo, ESET SMART SECURITY, ESET CYBER SECURITY, ESET.COM, ESET.EU, NOD32, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid and LiveGrid logo are trademarks, service marks and/or registered trademarks of ESET, LLC, d/b/a ESET North America and/or ESET, spol. s r.o., in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.