Your data is secured: **Acronis** encryption capabilities

When it comes to backing up your data, you want to be in control. Most of us have heard that data can be leaked, accidentally or not, or can be unlawfully obtained by criminals that want to exploit it. We at Acronis understand that you may, and most likely have, this concern, which is why we give you all the controls in hand and we can assure you that our infrastructure for your data is very secure. Even if data is intercepted, we use mechanisms to render such attempts useless. This is mainly achieved through the use of encryption.

Encrypt everything

You may have heard of encryption in relation to your other device or web-related activities. For example, https access to sensitive websites, like when you access your email or your bank website. Encryption is one of the founding pillars of data security.

However, it needs to be applied properly, with all data-protection scenarios in mind.

First, we need to be sure that local backups can be secured from unauthorized access in case someone gains access to your desktop, laptop, or mobile device. By using the industry-grade AES-256 algorithm, you can be sure that your data is safe. It is very hard to decrypt data secured by this algorithm. AES-256 is not that fast in terms of time and performance during the encryption process, so you may consider using shorter key lengths (AES-256 means that encryption key length is 256 bit) like 128 or 192 bits, in order to improve performance when protecting data that is not that sensitive.
Users can set the encryption algorithm and password that is used for encryption, and the Acronis agent

ACRONIS HELPS YOU CONTROL ACCESS TO YOUR DATA

To summarize, with Acronis products you can be sure that your data won't be accessed by someone who shouldn't have access to it. You can encrypt data on the device and send it in an encrypted form to the cloud by using a secured, encrypted channel. This data in the cloud will be additionally secured through a strict data center security policy.

handles key creation. The password you assign for backup can't be retrieved, so you need to memorize it. This is actually done on purpose, as this is a proper security approach. In case of a targeted or malware attack, your password won't be found in the agent/program files, and thus there will be no way to decrypt the backup file(s).

Technologically, the password is also converted through an algorithm into the actual encryption key, so it's really secure. You, of course, can set different passwords for each backup plan (that means that each backup will be encrypted using different encryption key).

Secondly, the same goes for cloud storage: you better store backups in an encrypted format. Some of us are cautious about our data being stored in the cloud somewhere. There is still an issue of trust, especially after some major security breaches of recent years, like with PSN or iCloud. We at Acronis understand that this is why we give our users an option to store data on Acronis Cloud in an encrypted form. To encrypt and decrypt your data, the program needs the password, that you specify when you configure the online backup. The process and approach is the same as with a local backup – you need to memorize your password. Alternatively, you can use password manager software, which will do it for you.

Thirdly, what else do we need to backup and care about? Facebook, our online social life. That is why we recently added an option of Facebook backup encryption as well. This backup can be located in the cloud, but we can encrypt data on the fly during backup creation, thus minimizing any possible data breach, again.

Ensure that your data goes to secured cloud storage, via a secure channel

We have already covered that all data needs to be encrypted, no matter where it is stored – locally or in the cloud. But it's also very important to eliminate a chance of data interception during its way to the cloud. This means that the channel to the cloud needs to be secured via SSL – which is how Acronis products talk to Acronis Cloud.

Acronis Cloud, on the other hand, consists of many data centers distributed across the globe and they are very well secured against various types of attacks. Physical security is ensured via high fences, 24/7 security personnel, and video surveillance with ninety-day archiving. Biometric scans and a proximity key card are required for access. Acronis data centers are equipped with UPS and backup diesel-generators, and are designed to ensure constant power availability for up to forty-eight hours, to sustain an undefined power outage. In addition, there are redundant HVAC, network, and UPS. The Tier-IV data centers do not interrupt availability for any planned activity, and can sustain at least one worst-case scenario unplanned event and experience no critical impact. With over ninety-nine percent availability, Tier-IV is the highest availability level for any data center on the planet.

Acronis data centers are also SSAE 16 certified. SSAE 16 is a framework for a data center organization to have an outside entity examine their internal controls. Compliance-sensitive companies, such as publicly traded enterprises, financial firms, and healthcare organizations, often require SSAE 16 certification.

Acronis

For additional information, please visit **www.acronis.com**