
Acronis Ransomware Protection

Table of contents

1 Introduction

1.1 What is Acronis Ransomware Protection?

Acronis Ransomware Protection is a software suite that ensures the security of information on your PC. It combines two features that supplement each other to provide you with enhanced protection of your personal data:

- **Acronis Active Protection**

  This service protects your computer from ransomware—malicious software that blocks access to some of your files or entire system and demands a ransom for unblocking. Based on a heuristic approach, Acronis Active Protection monitors processes running on your computer by using the real-time mode. When it detects a third-party process that tries to encrypt your files or inject malicious code into a healthy process, it informs you about it and asks if you want to allow the process to modify your files or block the process. Even if your files were encrypted by ransomware, you can recover them from temporary copies. Refer to Acronis Active Protection (p. 11) for details.

- **File-level backup to Acronis Cloud**

  You can protect files such as documents, photos, music files, and video files from corruption or loss by backing up them to the secure Acronis Cloud. Because files are stored on a remote storage, they are protected even if your computer is lost, stolen, or destroyed. Your data can be entirely recovered onto a new device, if needed. Changes to the protected files are automatically uploaded to the cloud storage to keep the backup up-to-date. With Acronis Ransomware Protection, you receive a free 5 GB of cloud storage space. If this is not enough, you can buy more space. Refer to Backing up files and folders (p. 8) for details.

Acronis Mobile

Because you have storage space on Acronis Cloud, you can use it to protect not only the data on your computer, but your mobile data as well. Acronis Mobile is a free application that allows you to back up your data to Acronis Cloud, and then recover it in case of loss or corruption to the same or a new mobile device. The application supports smartphones and tablets running iOS or Android operating systems. Refer to Acronis Mobile (p. 15) for details.

With the Acronis True Image desktop application or the Acronis True Image NAS application, you can back up your mobile data to your computer or an NAS device. Refer to Upgrading Acronis Ransomware Protection (p. 4) for details.

1.2 System requirements

Acronis Ransomware Protection requires the following hardware:

- Processor Pentium 1 GHz
- 1 GB RAM
- 1.5 GB of free space on a hard disk
- Screen resolution is 1024 x 768
- Mouse or other pointing device (recommended)

Other requirements:

- An Internet connection

- Administrator privileges to run Acronis Ransomware Protection

Operating systems:

- Windows 7 SP1 (all editions)
- Windows 8 (all editions)
- Windows 8.1 (all editions)
- Windows 10 (all editions)

1.3 Installing Acronis Ransomware Protection

Installing Acronis Ransomware Protection

To install Acronis Ransomware Protection:

1. Run the setup file. Before starting the setup process, Acronis Ransomware Protection will check for a newer build on the website. If there is one, the newer version will be offered for installation.
2. Click **Install**.

   Acronis Ransomware Protection will be installed on your system partition (usually C:).
3. In the opened window, sign in to your Acronis account.

   Refer to Acronis account (p. 6) for details.

Removing Acronis Ransomware Protection

Select **Start** -> **Settings** -> **Control panel** -> **Add or remove programs** -> **Acronis Ransomware Protection** -> **Remove**. Then follow the instructions on the screen. You may have to reboot your computer afterwards to complete the task.

If you use Windows 10, click **Start** -> **Settings** -> **System** -> **Apps & features** -> **Acronis Ransomware Protection** -> **Uninstall**.

If you use Windows 8, click the Settings icon, then select **Control Panel** -> **Uninstall a program** -> **Acronis Ransomware Protection** -> **Uninstall**.

If you use Windows 7, click **Start** -> **Control Panel** -> **Uninstall a program** -> **Acronis Ransomware Protection** -> **Uninstall**.

1.4 Upgrading Acronis Ransomware Protection

Acronis Ransomware Protection allows you to back up only files and folders and only to Acronis Cloud. If you want to back up all the data on your computer or separate partitions, you must upgrade to Acronis True Image. This product provides you with a full feature set for protecting your data, including file-level and disk-level backup to local storage, an NAS, or Acronis Cloud, data archiving, data sync, protecting your mobile data, and many more.

To upgrade, just install Acronis True Image on a computer where Acronis Ransomware Protection is installed. You can buy Acronis True Image at the Acronis website.

To buy more space on Acronis Cloud:

1. Start Acronis Ransomware Protection.
2. Click the account icon, and then click **Buy more space**. The Acronis website opens.
3. Choose a quota that better suits your needs, and then provide your payment information.

1.5 Technical Support

Support for Acronis Ransomware Protection is community-based and is provided through Acronis Knowledge Base and Acronis Ransomware Protection Forum.

2 Getting started

In this section

2.1 Acronis account

For Acronis Ransomware Protection to work, you must be signed in with your Acronis account. When you sign out, Acronis Active Protection keeps working, but the application stops updating the cloud backup.

How to create an Acronis account

After starting Acronis Ransomware Protection for the first time, you see the registration form.

If you do not have an Acronis account yet:

1. Complete the registration form.

   To keep your personal data secure, choose a strong password, guard it from getting into the wrong hands, and change it from time to time.

2. Click **Create account**.
3. An email message will be sent to the address you specified. Open this message and confirm your wish to create an account.

How to sign in

To sign in to your Acronis account:

1. To switch the registration form to the sign-in form, click **I already have an account**.
2. Enter your registration email address and password, and then click **Sign in**.

How to sign out

To sign out of your Acronis account:

1. Start Acronis Ransomware Protection.
2. Click the account icon, and then click **Sign out**.

2.2 Getting started with Acronis Cloud

Acronis Cloud might be unavailable in your region. For more information, click here: https://kb.acronis.com/content/4541

Remote storage

On the one hand, Acronis Cloud is a secure remote storage which you can use to store backups of your files and folders. With Acronis Ransomware Protection, you obtain a free 5 GB of cloud storage space. If this is not enough for protecting your files, you can buy more space. Refer to Upgrading Acronis Ransomware Protection (p. 4) for details.

Because files are stored on a remote storage, they are protected even if your computer is stolen or your house burns down. In the case of a disaster or data corruption, you can recover your files.

With one account, you can save data from several computers and all your mobile devices running iOS and Android operating systems.

Web application

On the other hand, Acronis Cloud is a web application that allows you to recover and manage the data you store on Acronis Cloud. To work with the application, you can use any computer connected to the Internet.

To access the application, go to https://www.acronis.com/my/online-backup/webrestore/, and then log in to your Acronis account.

2.2.1 How we ensure security of your data

When you use Acronis Cloud as storage for your backups, archives, or synced data, you want to be sure that your personal files won't get into the wrong hands. You may be especially concerned about your mobile device, because all of your data will be transferred through the Internet.

Let us assure you that your data will be safe. First of all, we use encrypted protocols (SSL, TLS) to transfer all data through both the Internet and LAN. To access the data, sign in to your account by providing the email address and password for that account.

Furthermore, we store your data on our servers in encrypted form. Only you have access to your encrypted data.

3 Backing up data

In this section

3.1 Backing up files and folders

Acronis Ransomware Protection allows you to back up your files such as documents, photos, music files, video files to Acronis Cloud. In case of their corruption or loss on your computer, they can be easily recovered from the cloud storage.

To back up files and folders:

1. Start Acronis Ransomware Protection.
2. Open the backup configuration step of the tutorial or the main application window.
3. To specify the files and folders that you want to back up, do one of the following:
   - In File Explorer or other file manager, select the files and folders, and then drag them to the Acronis Ransomware Protection window.
   - Click **Add them manually**, and then browse to the folders on your disks.

   The backup starts automatically.

The first backup may take a considerable amount of time to complete. Further backup processes will likely be much faster, because only changes to files will be transferred over the Internet. Acronis Ransomware Protection checks for data changes every 15 minutes and automatically uploads them to Acronis Cloud.

To change the backup settings, click the gear icon in the main application window.

Retention rules

Because Acronis Ransomware Protection permanently monitors the backed-up data and uploads the changes to Acronis Cloud, the backup could consume the storage space quite fast. To reduce the number of file versions and optimize the cloud space consumption, Acronis Ransomware Protection keeps only the following file versions:

- All versions for the last hour
- The first versions of every hour for the last 24 hours
- The first version of every day for the last week
- The first version of every week for the last month
- The first version of every month

All other versions are automatically deleted. The retention rules are pre-set and cannot be changed.

3.2 Removing data from Acronis Cloud

Because the available space on Acronis Cloud is limited, you need to manage your Cloud space by cleaning up the obsolete data or the data you do not need anymore. Cleanup can be done in a variety of ways.

Deleting an entire backup

The most drastic option is deleting the entire backup on Acronis Cloud.

To delete an entire backup:

1. Go to https://www.acronis.com/my/online-backup/webrestore/, and then log in to your Acronis account.
2. On the **Storage status** tab, point to the backup that you want to delete, click the gear icon, and then click **Delete**.

Deleting specific files and folders

You can also manage Acronis Cloud by deleting individual files and folders.

1. Go to https://www.acronis.com/my/online-backup/webrestore/, and then log in to your Acronis account.
2. Select files and folders you want to delete, and then click **Delete**.

4 Recovering data

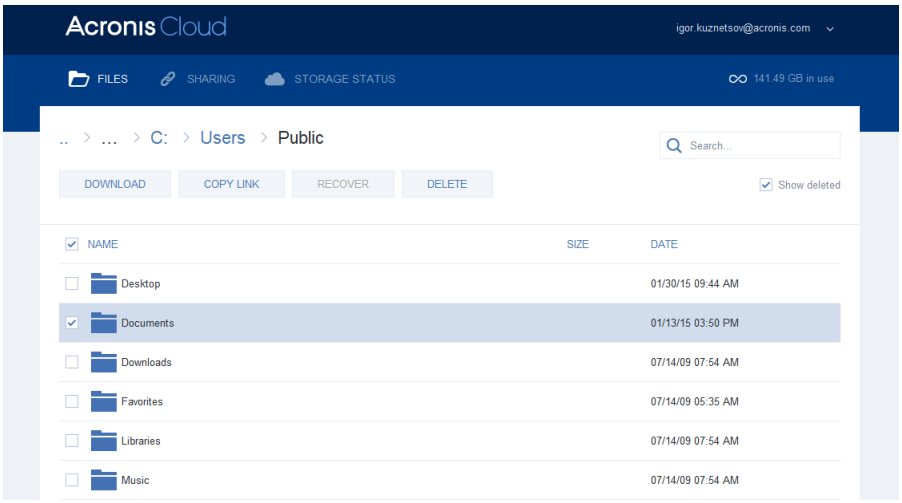
In this section

4.1 Recovering data from Acronis Cloud

Once your files are backed up to Acronis Cloud, you can use the Acronis Cloud web application to recover the files to a computer.

To recover files and folders from Acronis Cloud:

1. To open the Acronis Cloud web application, do one of the following:
   - Go to https://www.acronis.com/my/online-backup/webrestore/, and then sign in to your account.
   - In the main window of Acronis Ransomware Protection, click the account icon, then click **Browse my data**, sign in to your account, and then click **Backups**.
2. After the **Files** tab on the Acronis Cloud website opens, select the required online backup in the **Backups** area.
3. Select the files and folders you want to recover. Click the **Download** button to start recovery.



If you selected several files and folders, they will be placed into a zip archive.

By default the data will be downloaded to the **Downloads** folder. You may change the download path.

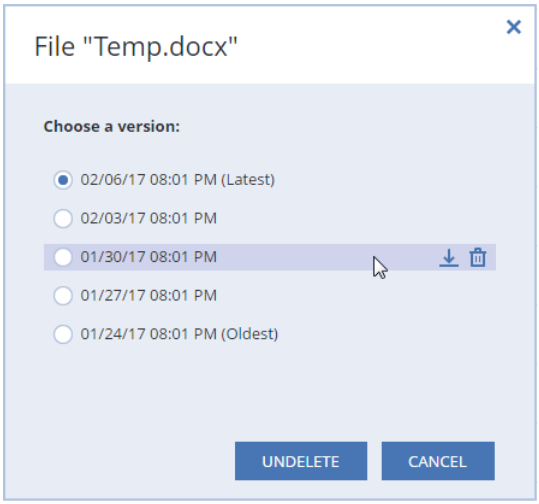
4.2 Recovering a file version

By default Acronis Ransomware Protection selects the latest versions with respect to the date you specified. However, for any file you can select a specific version of the file to recover.

Note that this option is not applicable to folders.

To recover a specific file version:

1. In the backup contents, select the file which version you want to recover, then click the gear icon at the right-hand side. Select **View versions** in the opened menu.
2. In the window that appears, point to the required version, and then click the **Download** icon.



   By default the data will be downloaded to the **Downloads** folder.

For more information about the backup retention rules, refer to Backing up files and folders (p. 8).

5 Acronis Active Protection

What is ransomware?

Ransomware is malicious software that blocks access to some of your files or entire system and demands a ransom for unblocking. The software shows you a window informing you that your files are locked and that you have to pay urgently, otherwise you will not be able to access the files anymore. The message may also be disguised as an official statement from authorities, for example, the police. The purpose of the message is to frighten a user and make them pay without asking for help from an IT specialist or the authorities. Moreover, there is no guarantee that you will regain control over your data after paying the ransom.

Your computer can be attacked by ransomware when you visit unsafe websites, open email messages from unknown people, or when you click suspicious links in social networks or instant messages.

Ransomware can block your access to:

- **Entire computer**

  You cannot use Windows or do anything on your computer. As a rule, ransomware does not encrypt your data in this case.
- **Specific files**

  Usually, this is your personal data, such as documents, photographs, and videos. Ransomware encrypts the files and demands money for the encryption key, which is the only way to decrypt your files.
- **Applications**

  Ransomware blocks some of your programs so that you cannot run them. It most often attacks your web browser.

How Acronis Ransomware Protection protects your data from ransomware

To protect your computer from ransomware, Acronis Ransomware Protection uses the Acronis Active Protection technology. Based on a heuristic approach, this technology monitors processes running on your computer by using the real-time mode. When it detects a third-party process that tries to encrypt your files or inject malicious code into a healthy process, it informs you about it and asks if you want to allow the process to modify your files or block the process. Refer to Protecting your data from ransomware (p. 12) for details.

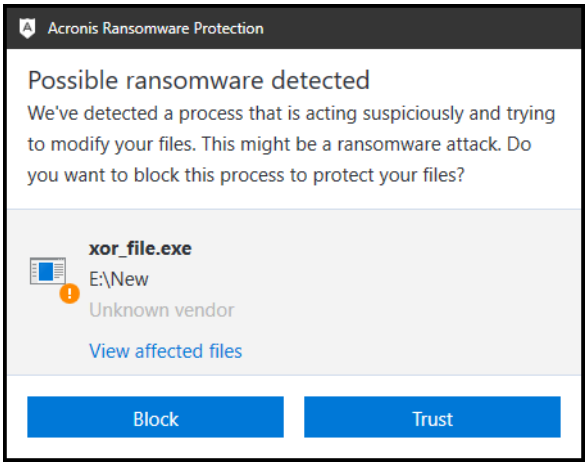
A heuristic approach is widely used in modern antivirus software as an effective way to protect data from malware. As opposed to the signature-based approach which can detect only one sample, heuristics detects malware families that include samples with similar behavior. One more advantage of this approach is an ability to detect new kinds of malware that do not have a signature yet.

Acronis Active Protection uses behavioral heuristics and analyzes chains of actions done by a program, which is then compared with the chain of events in a database of malicious behavior patterns. Since this method is not precise, it admits so-called false positives, when a trusted program is detected as malware. To eliminate such situations, Acronis Active Protection asks you if you trust the detected process. When the same process is detected for the second time, you can add it to the permission list and set the default action for this process by marking it as trusted or blocked. If you do not, you will be able to blacklist this process. In this case, this process will be blocked every time it tries to modify your files.

To collect as many as possible different patterns, Acronis Active Protection uses Machine Learning. This technology is based on mathematical processing of big data received with telemetry. It is a self-learning approach, because the more data is processed, the more precisely a process may be detected as ransomware or not.

5.1 Protecting your data from ransomware

When the Acronis Active Protection service is on, it monitors the processes running on your computer by using the real-time mode. When it detects a third-party process that tries to encrypt your files, the service informs you about it and asks if you want to allow the process to modify your files or block the process.



Before you make your decision, you can view the list of files that the process is going to modify.

To allow the process to modify the files, click **Trust**. If you are not sure if the process is safe and legal, we recommend that you click **Block**. In any case, next time the process is run Acronis Ransomware Protection will ask you again. To give the process permanent permission or to block it every time it

tries to modify your files, select the **Remember my choice for this process** check box, and then click **Block** or **Trust**. The process will be added to the permission list. You can manage the list in Settings.

After blocking the process, we recommend that you check if your files have been encrypted or corrupted in any way. If this is the case, click **Recover modified files**. Acronis Ransomware Protection will search the latest file versions and recover the files from the temporary file copies that were preliminarily created during the process verification.

To make this action the default, select the **Always recover files after blocking a process** check box.

5.2 Managing Acronis Active Protection

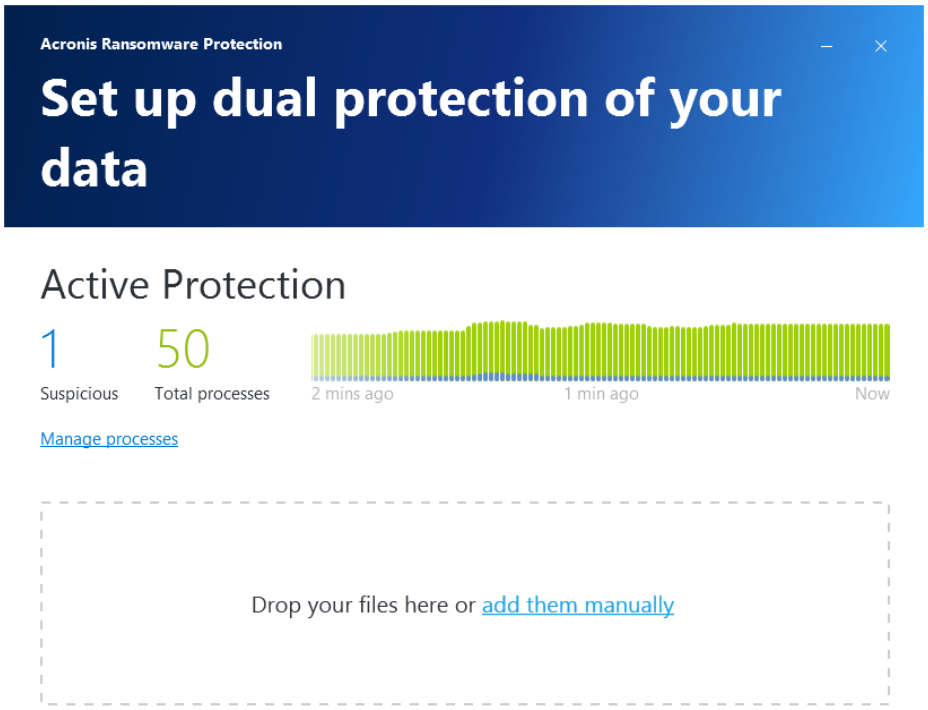
When the Acronis Active Protection service is on, it monitors the processes running on your computer by using the real-time mode. When it detects a third-party process that tries to encrypt your files, the service informs you about it and asks if you want to allow the process to modify your files or block the process. Refer to Acronis Active Protection (p. 11) for details.

You can configure Acronis Active Protection settings and control the protection process from several places:

- Acronis Active Protection section
- Windows taskbar notification area

Acronis Active Protection section

This section covers statistics for the protection process and allows you to configure the Acronis Active Protection permission list.



You can:

- See in real-time mode the number of monitored and safe processes.
- Manage the permission list to trust or block applications.

Windows taskbar notification area

Right-clicking the notification area icon opens the following menu items:

- **Turn off Active Protection** (**Turn on Active Protection**)—click to turn the ransomware protection off or on.
- **Open**—click to open the application main window.

6 Acronis Mobile

Acronis Cloud might be unavailable in your region. For more information, click here: https://kb.acronis.com/content/4541

Acronis Mobile allows you to back up your data to Acronis Cloud, and then recover it in case of loss or corruption.

Which devices does the mobile app support?

You can install Acronis Mobile on any mobile devices that runs one of the following operating systems:

- iOS 8.0 and later (iPhone, iPad, iPod)
- Android 4.1 and later (mobile phones and tablets)

Key features

Acronis Mobile allows you to:

- Back up your personal data, including:
  - Photos
  - Videos
  - Photos and videos located in iCloud (iOS only)
  - Contacts
  - Calendars
  - Messages (Android only)
  - Reminders (iOS only)
- Encrypt backups with the AES-256 cryptographic algorithm
- Automatically back up new and changed data
- Access cloud backups from all your mobile devices and recover data from these backups

Where can I find these apps?

You can view additional information and download Acronis Mobile from the Apple App Store or Google Play:

- Acronis Mobile for iOS devices:
  https://itunes.apple.com/us/app/acronis-true-image-cloud/id978342143
- Acronis Mobile for Android devices:
  https://play.google.com/store/apps/details?id=com.acronis.acronistrueimage

In this section

6.1 Installing Acronis Mobile

Depending on your mobile device, go to the Apple App Store or Google Play and search for the Acronis Mobile app.

For example, to find and install Acronis Mobile for iOS:

1. On your iPhone, open **App Store**.
2. Tap the Search icon.
3. Enter **acronis** in the search field.
4. Select **acronis mobile** in the search results to go to the app page.
5. Follow the standard installation procedure.

The procedure to find and install the Android app is similar.

6.2 Backing up your mobile device to Acronis Cloud

A mobile backup is your guarantee that your data on your mobile device is safe and can be recovered in case of corruption or loss. You can also use the backup to transfer your personal data and settings from your old smartphone to a new one. Refer to Acronis Mobile (p. 15) for details.

To back up your mobile data to Acronis Cloud:

1. Start Acronis Mobile.
2. Select Acronis Cloud as a backup destination.
3. Sign in to your Acronis account.
4. Tap the gear icon and select the data categories that you want to back up, or tap **Back up** if you want to back up all of the data.
5. [optional step] Tap **Use encryption** to encrypt the backup and protect it with a password. Otherwise, tap **Skip**.
6. Tap **Back up**.
7. Allow Acronis Mobile to access to your personal data.

When the backup is complete, your data is uploaded to the secure Acronis Cloud. If you want data changes (for example, new photographs) to be backed up automatically, make sure the **Continuous backup** setting is turned on. If this setting is turned off, the new data is backed up only when you tap **Back up**. Refer to Mobile app settings (p. 17) for details.

6.3 Recovering mobile data

Recovering with your mobile device

With your smartphone or tablet, you can access any mobile backup stored in Acronis Cloud. In general, you can open, view, recover, and perform some other operations with a file or data category. Note that because of operating system limitations, some operations can be unavailable for the specific file types.

To access mobile data by using a mobile device:

1. Install and start Acronis Mobile.
2. To access a cloud backup, sign in to your Acronis account, if prompted.

3. To open the side menu, slide from the left border of the screen to the right, and then tap **Access and Recovery**.
4. Select the backup that contains the desired file or data category. You can select the backup by name or by the device that contains the desired data. For example, to access data from your current mobile device, select this device from the list.
5. Browse to the desired file or data category.
6. Depending on the data type, the following operations can be done:
   - **Open**
   - **Recover**
   - **Recover all**

6.4 Recovering data to a new smartphone

When you have a mobile backup of your smartphone, you can easily transfer your personal data to another mobile device. For example, this is handy when you buy a new smartphone. Just recover your data from Acronis Cloud to your new device.

To recover your data to a new smartphone:

1. Install and start Acronis Mobile.
2. Tap **Back up to Cloud**, and then sign in to your Acronis account.

   Acronis Mobile detects that there are mobile backups in Acronis Cloud.
3. Tap **Recover data**.
4. Select the mobile device to recover your data from, and then tap **Select device**. For example, if you want to transfer your data from your old smartphone, select it.
5. Select the data categories that you want to recover, and then tap **Recover**.
6. Allow Acronis Mobile access to your personal data.

When the recovery is complete, your data is downloaded to your new device.

6.5 Mobile app settings

To open the **Settings** section, slide from the left border of the screen to the right, and then tap **Settings**. The following settings are available:

- **Continuous backup**

  If this setting is turned on, Acronis Mobile automatically detects new data and uploads it to Acronis Cloud.
- **Back up using Wi-Fi only** or **Back up using Wi-Fi and cellular connection**

  You can choose an Internet connection type for the data upload and download. This is useful because sometimes a Wi-Fi connection is cheaper (or free) or more reliable than other connection types.
- **Help**

  Tap this item to open a web-based product help.
- **Send feedback**

  This command allows you to send feedback about Acronis Mobile, report a problem, or contact customer support.
- **Clear remembered passwords**

If you select the setting for the app to remember the password when encrypting a backup, the app does not ask for the password when you work with the backed-up data on your mobile device. Clear remembered passwords if you want the app to ask you for the password every time you access the backup.

Copyright Statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

7 Glossary of Terms

A

Acronis Active Protection

A technology that protects data from ransomware, malicious software that blocks access to some files or an entire system and demands a ransom for unblocking. Based on a heuristic approach, this technology monitors processes on a computer in real-time mode and informs the user about attempts to encrypt data on the computer. In case files are encrypted, they can be recovered from the temporary copies or backups.

B

Backup

1. The same as Backup operation (p. 20).
2. A set of backup versions created and managed by using backup settings. A backup can contain multiple backup versions created using full and incremental (p. 20) backup methods. Backup versions belonging to the same backup are usually stored in the same location.

Backup operation

An operation that creates a copy of the data that exists on a machine's hard disk for the purpose of recovering or reverting the data to a specified date and time.

Backup version

The result of a single backup operation (p. 20). Physically, it is a file or a set of files that contains a copy of the backed up data as of a specific date and time. Backup version files created by Acronis Ransomware Protection have a TIB extension. The TIB files resulting from consolidation of backup versions are also called backup versions.

I

Incremental backup

1. A backup method used for saving data changes that occurred since the last backup version (p. 20) (of any type) within a backup.
2. A backup process that creates an incremental backup version (p. 20).

Incremental backup version

A backup version (p. 20) that stores changes to the data against the latest backup version. You need access to other backup versions from the same backup (p. 20) to restore data from an incremental backup version.

O

Online backup

Online backup - a backup that is created using Acronis Online Backup. Online backups are stored in a special storage named Acronis Cloud, accessible over the Internet. The main advantage of an online backup is that all backups are stored on the remote location. It gives a guarantee that all backed up data will be safe independently of a user local storages. To begin to use Acronis Cloud a user should subscribe to the service.

R

Recovery

Recovery is a process of returning of a corrupted data to a previous normal state from a backup (p. 20).

S

Suspicious process

Acronis Active Protection (p. 20) uses behavioral heuristics and analyzes chains of actions done by a program (a process), which is then compared with the chain of events in a database of malicious behavior patterns. If the program acts similar to ransomware behavior

and tries to modify a user's files, it is considered as suspicious.