Data Protection and Backup Software Test

A test performed by AV-Test GmbH
Date of the report: April 3rd, 2017

Executive Summary

In January 2017, AV-Test performed a test of Data Protection and Backup software (DPB). Data Protection software extends on classical backup features to protect against malicious security threats such as ransomware and actively guarding personal data against encryption.

The presented evaluation assesses Acronis True Image 2017 New Generation Premium, Carbonite Personal PLUS, CrashPlan for Home and iDrive.

We evaluated DPB on the following four criteria.

Usability: evaluating the ease of use, taking into account novice users. We evaluate how much effort it takes not just to install the application but also to change settings and to setup the actual backup tasks and how much of that effort is omitted by scheduled default settings. The range of clicks required until a product is setup varies, it takes 12 clicks for Acronis but only four clicks as with Carbonite. It takes more user interaction to finish the Acronis setup, but the setup process also includes a wizard which creates and setups the default backup job. Changing or creating backup tasks in Acronis is very straightforward. During installation Carbonite setups everything for the user. On the other hand, changing specifications in Carbonite is more complicated than with any of the other products. CrashPlan and iDrive are both pretty quickly when setting up and creating schedule backup tasks. CrashPlan could do with a more up-to-date interface.

Performance: measuring the amount of time taken for backup to complete depending on backup type, data composition and hard drive types. We don't just measure how well the applications perform with sample sets consisting of large or small files but also with incrementally changed files. It also demonstrates how backup software can utilize full potential of SSD and HDD drive.
Acronis True Image is the clear winner when it comes to performance. No other product reaches similar speed when backing up or restoring Data for small, large, system or changed files or data stored on HDD or SSD. Every performance test was led by Acronis, which is on average twice as fast, in some cases being 10 times as fast as the competition. CrashPlan and iDrive both coming in second, achieving similar scoring. Carbonite as a pure cloud solution was not considered.

Functionality: reviewing the amount and quality of features available to choose and customize options. Different users have different requirements. These requirements vary with different proficiency levels and the significance and composition of the data to be backed up.
This category is led by iDrive and Acronis both with 33 out of possible 39 features. Both applications allow basic backup jobs but also provide more advanced features for further configuration. CrashPlan

takes third place with 27 features provided. Carbonite is a very basic application and aims at configuring everything for the user, making it hassle free but also limiting the options for the customers.

Threat protection: testing how well the DPB copes when exposed to the threat of ransomware. Not just hardware failures and system errors pose a risk to user data but also malicious applications. Such threats can come in form of malware encrypting documents and personal data.
So far Acronis is the only product capable of detecting and stopping ransomware delivering close-to-perfect results. It detects in a timely fashion, no detection taking more than 40 seconds. Files encrypted before the stoppage of the ransomware were in most cases recovered, even without having created a specific backup of these files before.
The other products each have similar results. They did not stop the ransomware but usually allowed recovery of files previously backed up. CrashPlan was the only product in our test with a slipup. After the infection the product was also affected and therefore was not able to restore any files from backup.

Overview

Backup of important data and files and a complete backup of the entire system has been vital to preserve data integrity and security. Back in the day it was used to ensure failure of hardware devices would not lead to loss of important data. By physically separating the backups from the original copy enhanced disaster management was taken into consideration. Over the last couple of years this has been managed through cloud solutions, making the option available for private users as well as enterprises. Backup software has always been mentioned additionally to anti-virus products in improving a systems security. As of lately this has become even more essential with a spike of ransomware encrypting vital personal files on a machine and even attacking system backups.

Ransomware has been an increasingly popular method for malware developer to monetize on their bad deeds. The work by sneaking on the user's machine and then starting to encrypt the users file with some weak or in worth case strong password. Access will only be possible with the encryption key which can be purchased from the attacker. After spending their money users can only hope that a key will be provided and that it works to restore the lost files.
The damage affects private or customer files and data, which may also result in reputation damage. Mid 2016 according to the FBI there were 4000 ransomware infections per day. The trend heading towards monetary damage being increased about 40 times to 2015.
There are weaker ransomware examples which can be decrypted with designated tools provided by security vendors. The "No More Ransom Project" already has more than 100 ransomware families which can be decrypted and improving on that number constantly. Not all ransomware is that easy to clean. The developer of such application get more and more sophisticated making it less likely to decrypt those personal files without having to pay.

Typically for malware families is - they come in waves and peak before ebbing off.

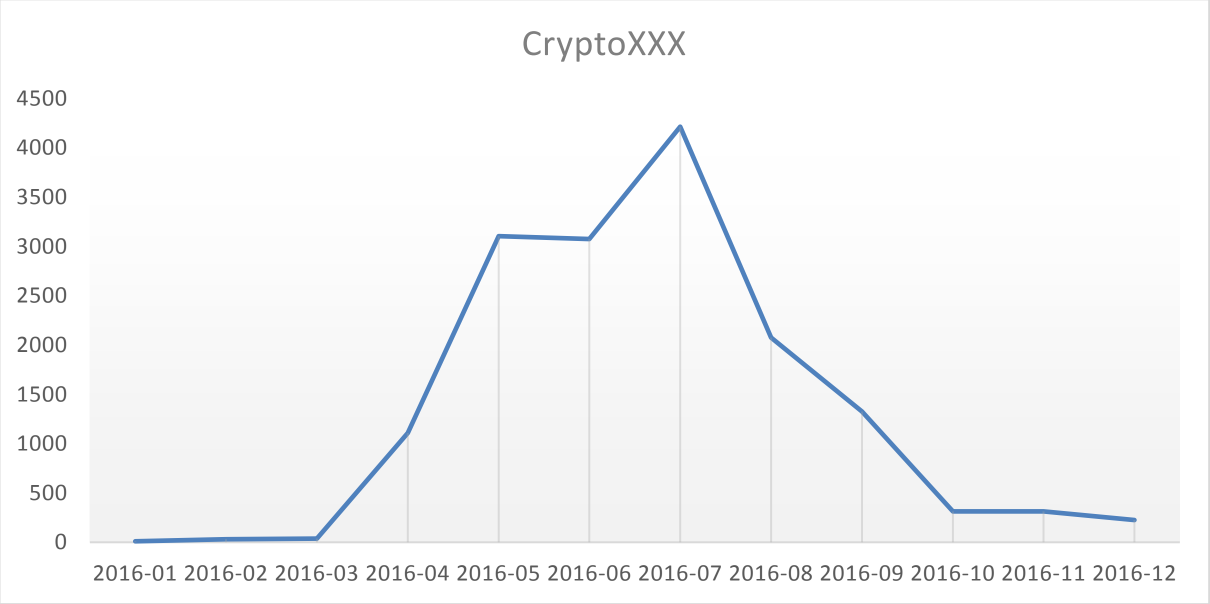


Figure 1: Displays the activity period of the ransomware family CryptoXXX as seen by AV-TEST

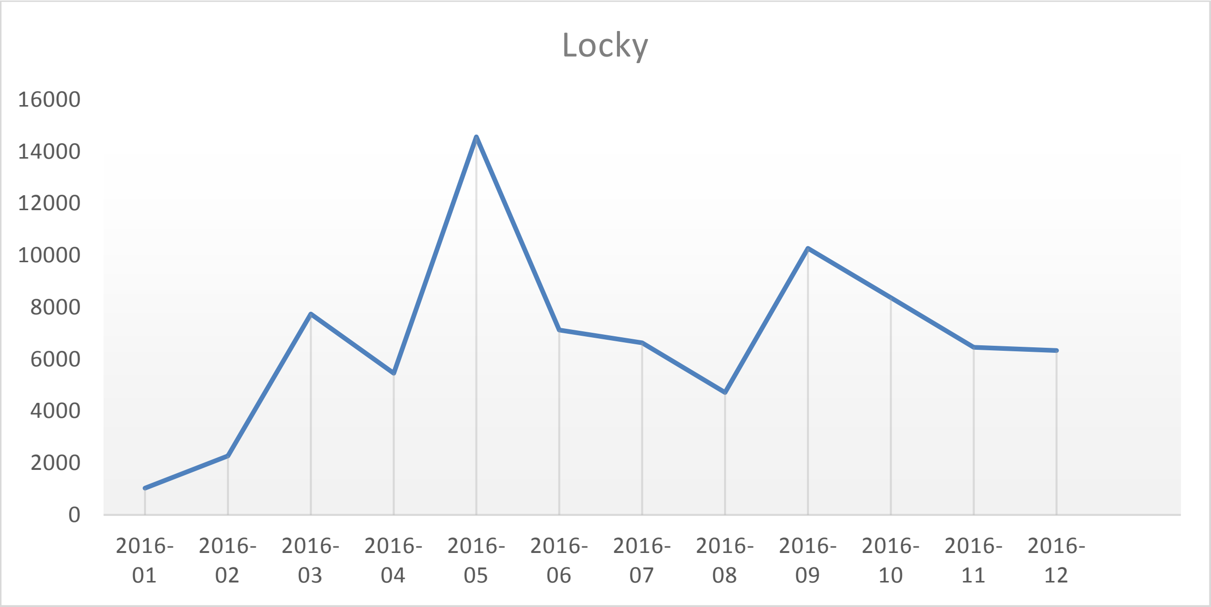


Figure 2: Displays the activity period of the ransomware family Locky as seen by AV-TEST, it looked like the distribution of Locky had already peeked and slowly fading, yet it is still going strong.

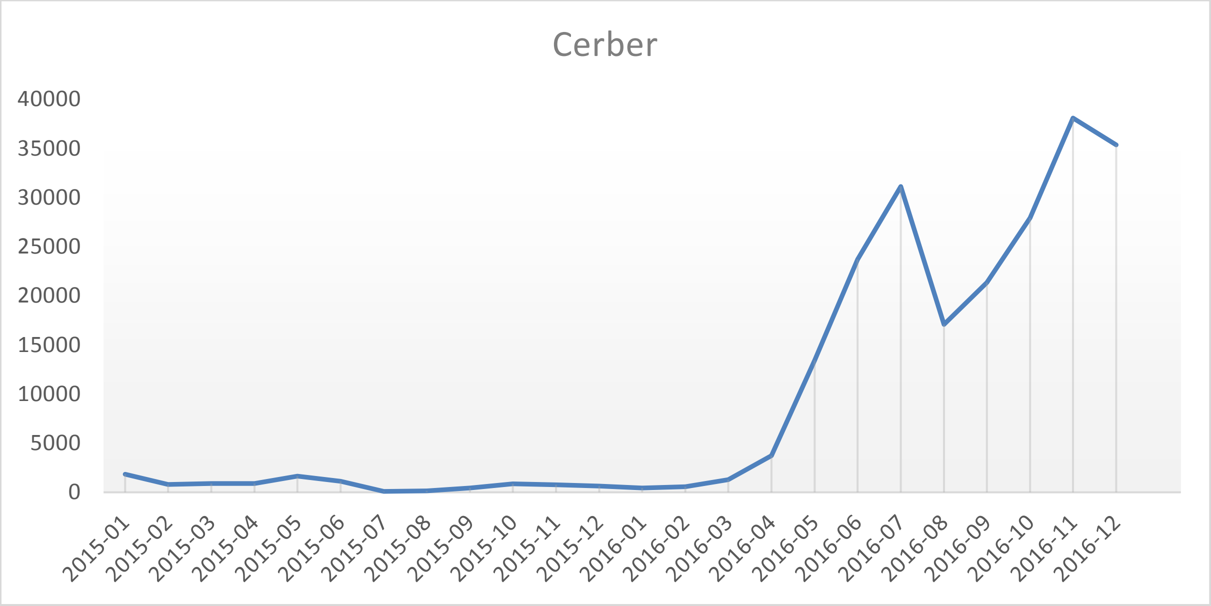


Figure 3: Displays the rise of the ransomware family Cerber which is still very active at the time of this writing, as seen by AV-TEST.

Methodology and Scoring

Tested products

The presented tests were performed in January 2017. They all featured the latest available product releases at the time of the test:

(1) Acronis True Image 2017 New Generation 21.0.0.6106
(2) Carbonite Personal PLUS 6.2.1 (build 6804)
(3) CrashPlan for Home 4.8.0 (1435813200480)
(4) IDrive 6.5.1.23

Platforms

All tests were performed on actual physical machines. No Virtual Machines were used. All tests for a defined operating system were carried out on devices with identical hardware configurations as described below.

Windows

All tests for the Windows operating system were performed on identical PCs equipped with the hardware specified in the appendix. The detection tests were performed on the Windows 7 platform. The performance test used the same Windows 7 system. All patches available on January 3rd 2017 were previously installed.

Testing Approach

There are a few generic principles that were followed:

(1) **Physical devices**. The test devices used were physical devices. No Virtual Machines were used.
(2) **Product cloud/Internet connection**. The Internet was available to all tested products.
(3) **Product configuration**. All products were run with their default, out-of-the-box configuration.
(4) **Clean device for the start of the test**. The test devices were restored to a clean state before testing the malware samples.
(5) **Sample cloud/Internet accessibility.** If the malware used the internet connection to reach other sites in order to download other files and infect the system, care was taken to make sure that the cloud access was available to the malware sample in a **safe** way such that the testing network was not under the threat of getting infected.

Usability Test

The usability scoring attempts to measure the ease and comfort level when installing and setting up the application. These applications are for private users and therefore should address different levels of computer proficiencies. Allowing the user to setup a default security plan with few clicks out of the box but also providing more advanced users to tweak and adapt according to their requirements. The number of steps to achieve the desired goal is counted and compared. The language used is evaluated, to determine if it is appropriate for all kind of users from novice to full proficient user.

Performance Test

For the performance test we measure the time taken for the user to create complete and incremental backups of the entire system and different data sets. We also measure how long it takes

to recover such data. It should also demonstrate how backup software can utilize full potential of the differences in SSD and HDD drives.
A common feature of modern Backup systems is the continuous backup of files or designated folders. The time is measured on how frequently such data is saved. In case of a sudden loss of data, for example caused by malware infection, how little of the current work done has been lost due to the data which can be swiftly recovered. Several benchmarks are determined and compared for the products:

Full system backup

a. Full System Backup from an SSD to second internal HDD drive. About 40GB of data.

Backup and restore large and small file sets

b. Backup of 50GB spread over 56 ISO and video files (large file set)
    a. From SSD to internal HDD
    b. From HDD to other partition of HDD
c. Restore 50GB of the large file set from HDD to SSD
d. Backup of 50GB spread over approximately 60 000 different files (small file set)
    a. From SSD to internal HDD
    b. From HDD to other partition of HDD
e. Restore 50GB of the small file set from HDD to SSD

Backup and restore Incremental backup large and small file set

f. Incremental backup of big file set after changing 10% of data in each file
    a. From SSD to internal HDD
g. Restore entire big file set from incremental backup
h. Incremental backup of small file set after changing entire content of every tenth file
    a. From SSD to internal HDD
i. Restore entire small file set from the incremental backup

Continuous backup

j. Time delay provided by the products for backup intervals
k. Measured time delay between backed up files in version history

Functionality Test

In order to be considered as a full data protection application, the features provided should be comprehensive. We determine the features considered vital for a data protection application and those additional features which complete this kind of application. We validate the existence of such features in the application and through information provided online by the vendors. This also provides potential customers an insight into what they buy and a guideline to use along with their own expectations from the application.

Threat Protection Test

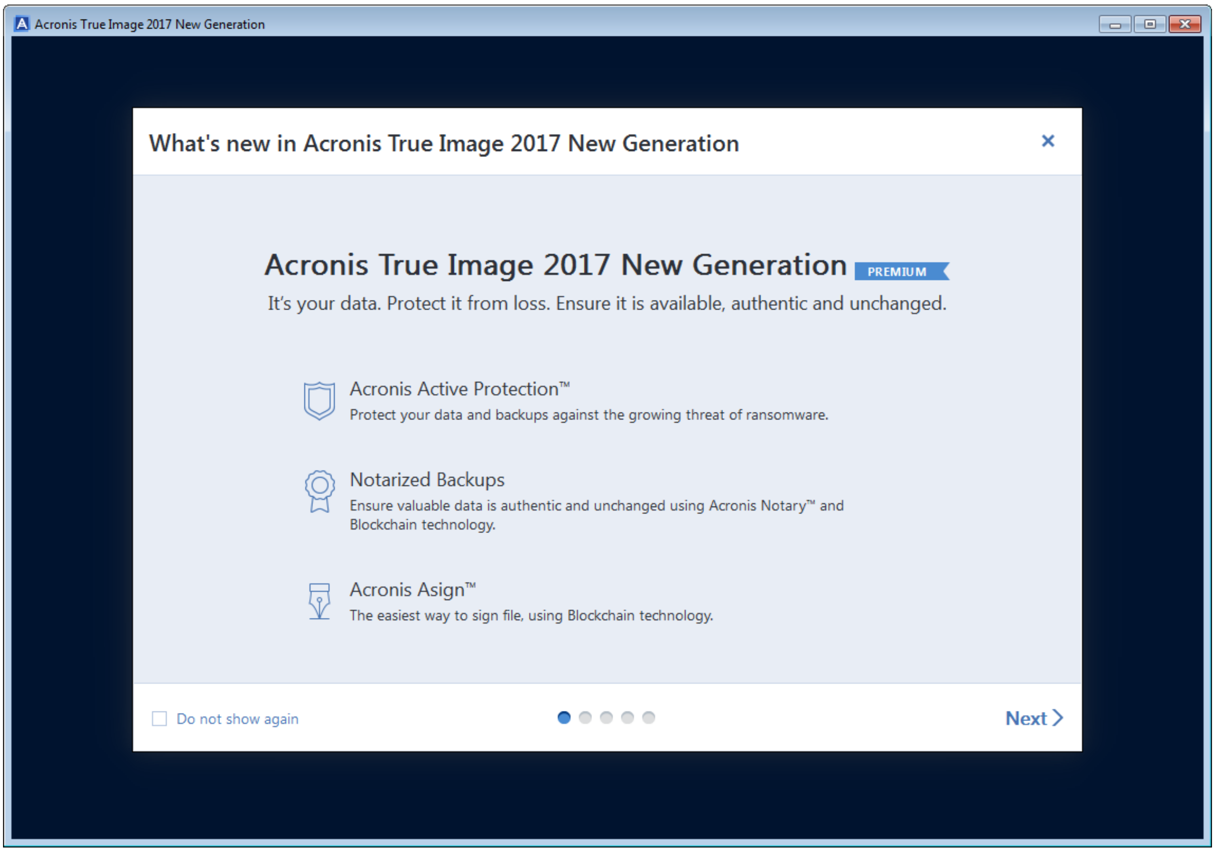
The Threat Protection Test tests the protection against malicious threats such as ransomware. The test aims to determine if the data on the system can be recovered after an infection. The data protection suite must be able to keep its recovery capabilities even after an attack has occurred. The data protection suite was installed and a backup has been scheduled and executed. The sample set to be tested consists of five widely distributed ransomware files. The test systems are set up so data is continuously backed up, either to a local storage or to the cloud. Any changes to the system like malware infections should be able to be reversed with minimal time delay and no data loss. The ransomware samples will be executed (online). The system is than monitored. If the infestation is stopped, the time of the process is measured and the files on the system validated that no data is lost. If the ransomware is not actively stopped, we determine if the backup can be restored and when the time delay between last backup and encryption of the files is worst.

Test Results

Usability

Evaluating the ease of use, taking into account novice users.

Acronis



Acronis True Image 2017 New Generation

What's new in Acronis True Image 2017 New Generation

Acronis True Image 2017 New Generation PREMIUM

It's your data. Protect it from loss. Ensure it is available, authentic and unchanged.

Acronis Active Protection™
Protect your data and backups against the growing threat of ransomware.

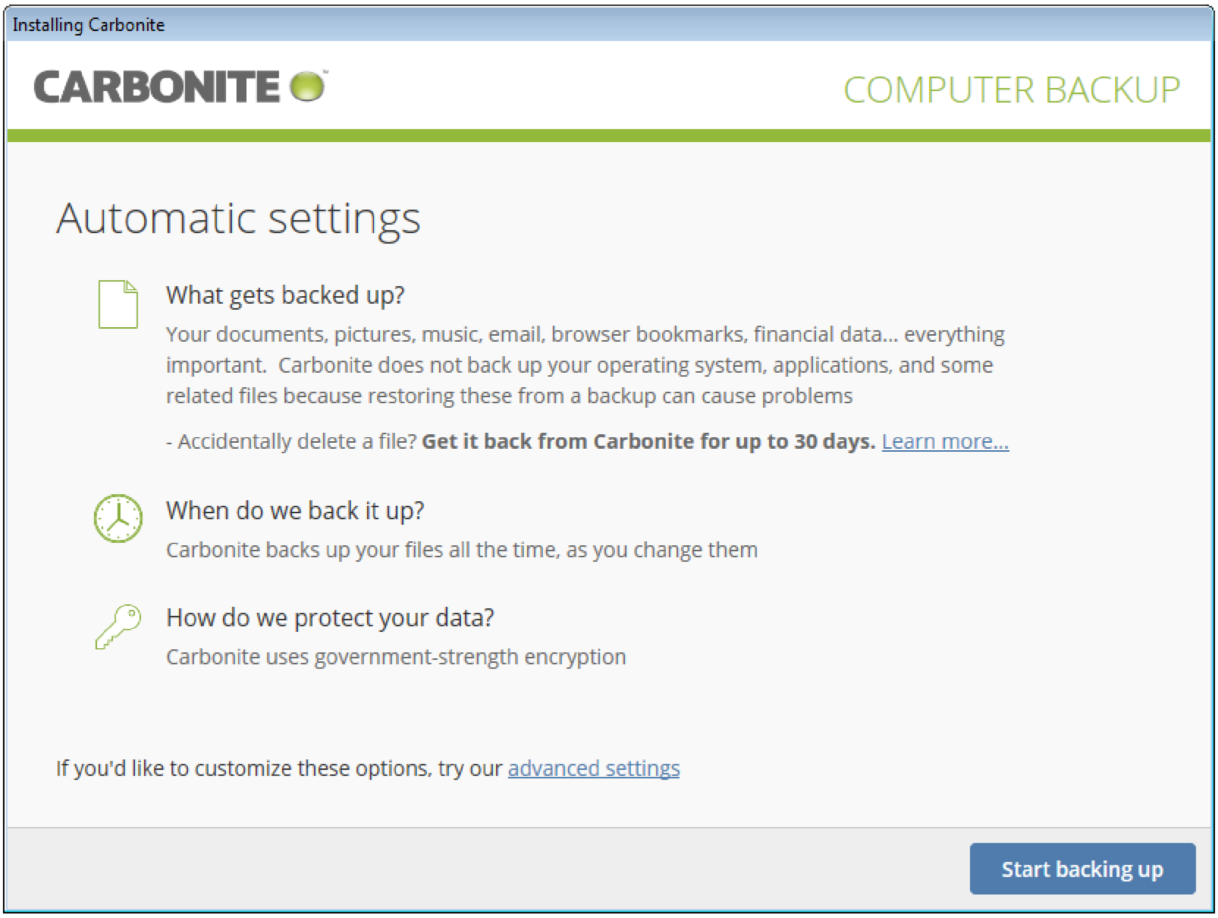
Notarized Backups
Ensure valuable data is authentic and unchanged using Acronis Notary™ and Blockchain technology.

Acronis Asign™
The easiest way to sign file, using Blockchain technology.

Figure 4: Acronis wizard started directly after setup.

Although, it takes most clicks during installation Acronis achieved the highest score in this category. The reason for the numerous clicks during setup is the backup wizard following straight after the installation. The display is nice and modern. Changing settings and interaction in general is easy and self-explanatory.

Carbonite



Installing Carbonite

Automatic settings

What gets backed up?

Your documents, pictures, music, email, browser bookmarks, financial data... everything important. Carbonite does not back up your operating system, applications, and some related files because restoring these from a backup can cause problems

- Accidentally delete a file? **Get it back from Carbonite for up to 30 days.** Learn more...

When do we back it up?

Carbonite backs up your files all the time, as you change them

How do we protect your data?

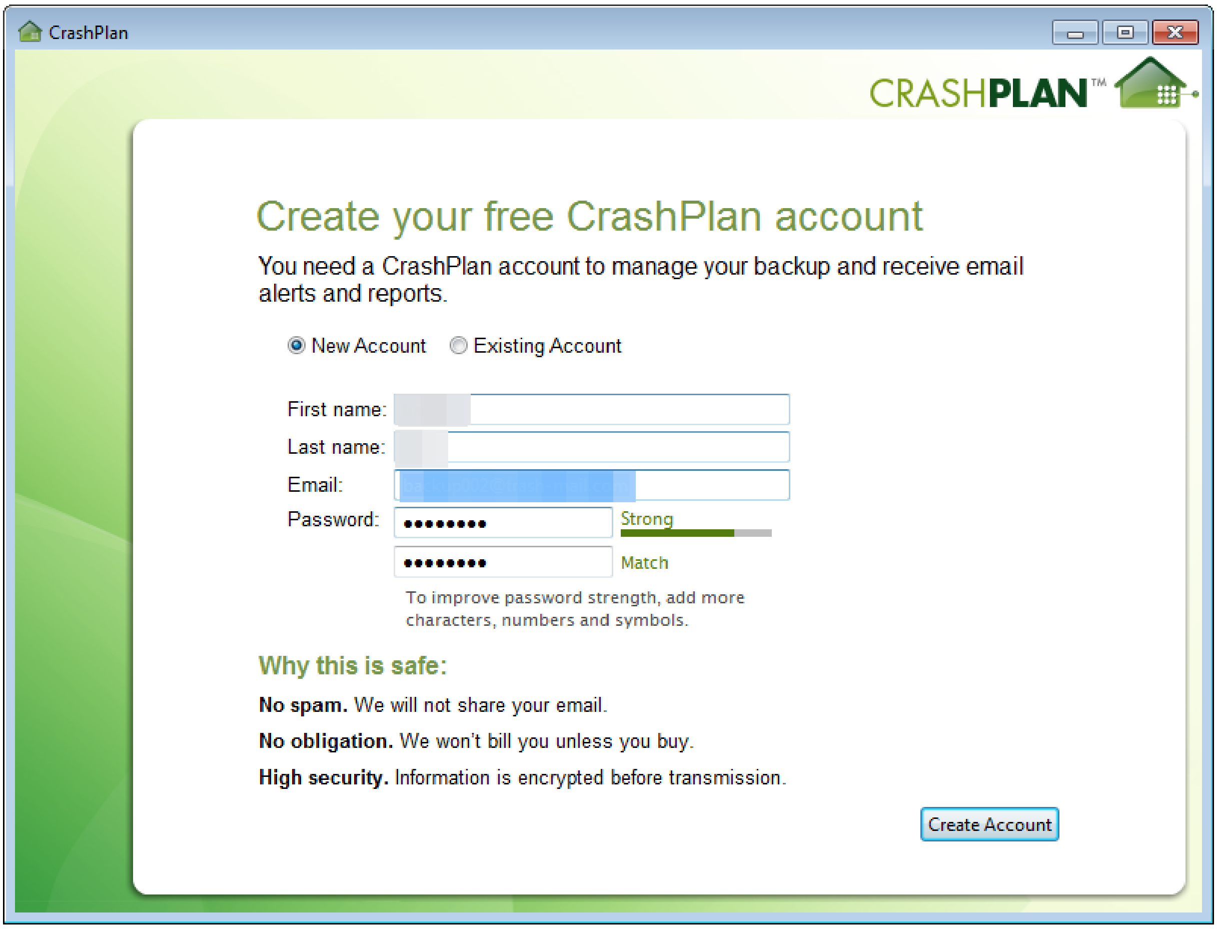
Carbonite uses government-strength encryption

If you'd like to customize these options, try our advanced settings

Figure 5: Carbonite creates the backup job automatically with setup, but allows changing advanced settings.

Carbonite does not require the user to do much during setup. The user quickly clicks through the installation and forgets that the program is running. When the user wants to add something to the backup it is done by right-clicking in the file explorer and adding the files or folders to the default backup job. The main issue with the usability of Carbonite is that some file extensions such as mp4 videos or executables are not added by default to the backup job but need to be selected individually, which a user will not notice when adding a directory to backup.

CrashPlan



CrashPlan

CRASHPLAN™

Create your free CrashPlan account

You need a CrashPlan account to manage your backup and receive email alerts and reports.

● New Account ○ Existing Account

First name: [redacted]

Last name: [redacted]

Email: [redacted]

Password: •••••••• Strong

•••••••• Match

To improve password strength, add more characters, numbers and symbols.

Why this is safe:

No spam. We will not share your email.

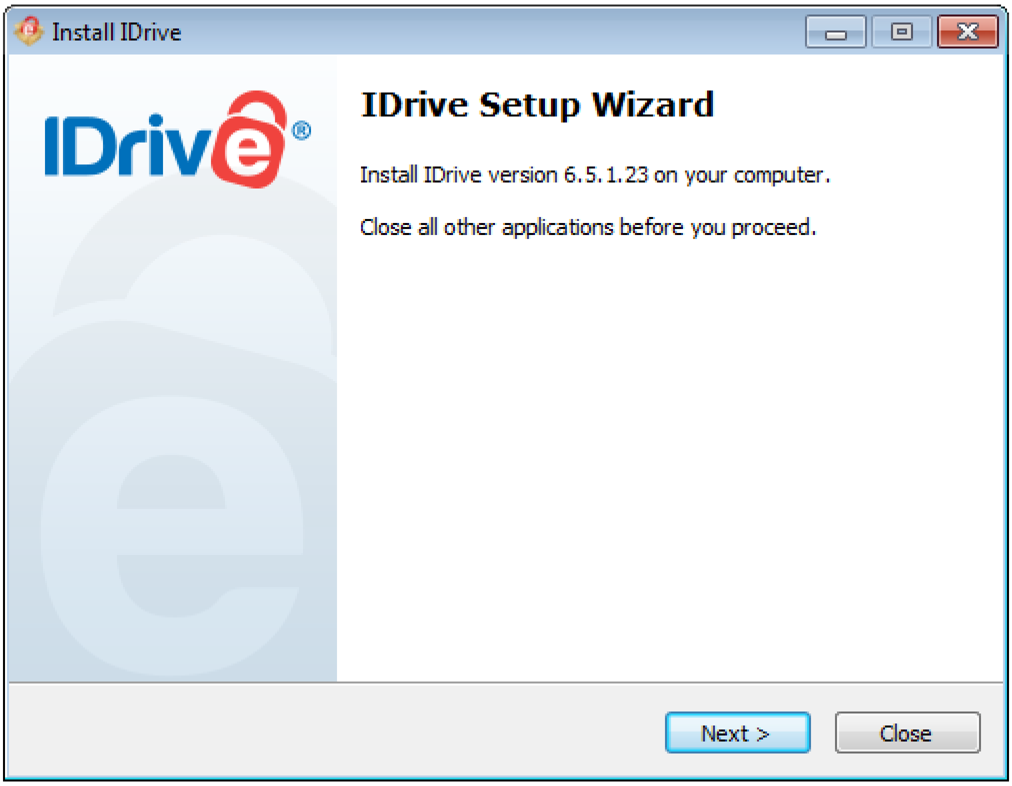
No obligation. We won't bill you unless you buy.

High security. Information is encrypted before transmission.

Figure 6: CrashPlan allows creating an account during setup.

CrashPlan has a feel of an antiquated user interface, yet installing and setting up the application is easy and straightforward. The default scheduled backup can be setup from the main window. The individual steps during creation of a backup job need a bit getting accustomed to.

iDrive



Install IDrive

IDrive Setup Wizard

Install IDrive version 6.5.1.23 on your computer.

Close all other applications before you proceed.

Figure 7: iDrive setup is straightforward and doesn't require much but to click through.

iDrive takes few clicks to finish installation. Once installed all the user needs to do is "activate" the default backup which will run straight away and schedule future runs. The GUI is well-arranged and allows easy and quick access to all options.

Performance

Measuring the amount of time taken for backup to be completed depending on backup type, data composition and hard drive types.

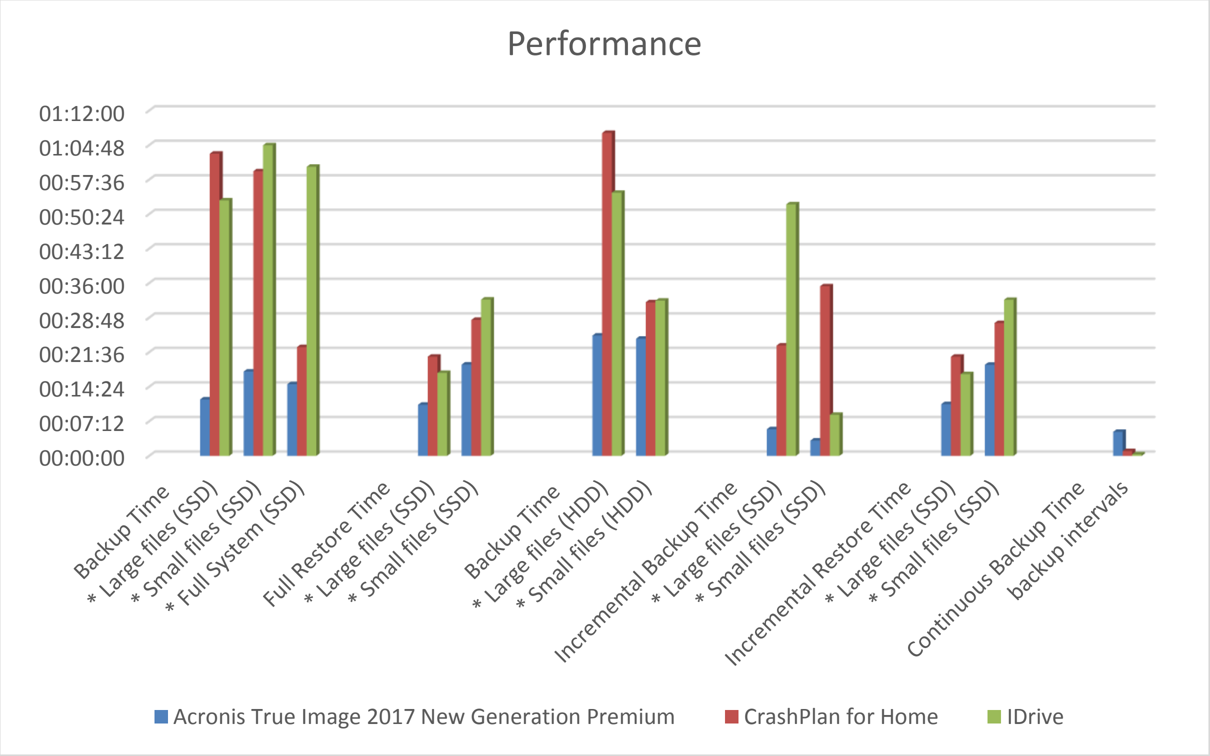
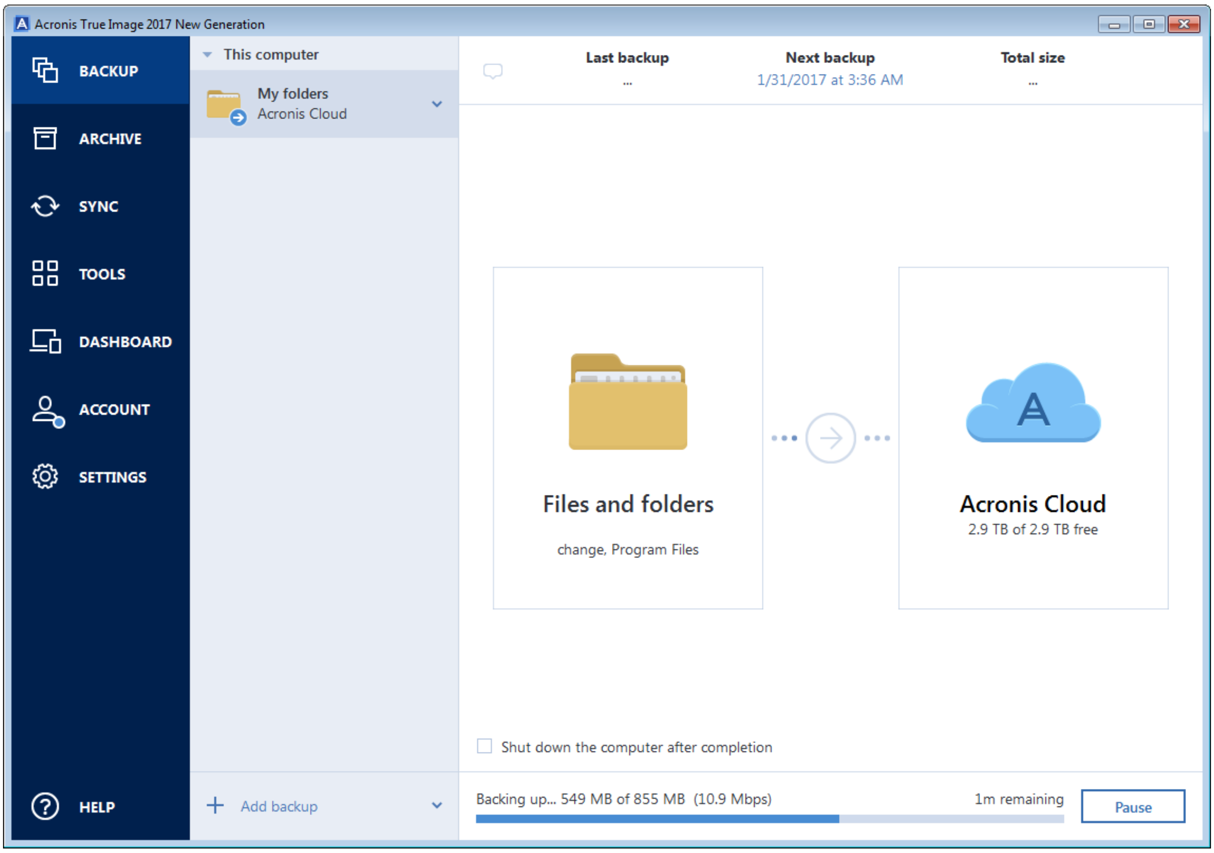


Figure 8: Performance compared between tested products (data table in Appendix).

Acronis



My folders
Acronis Cloud

Last backup	Next backup	Total size
...	1/31/2017 at 3:36 AM	...

Files and folders

change, Program Files

Acronis Cloud

2.9 TB of 2.9 TB free

□ Shut down the computer after completion

Backing up... 549 MB of 855 MB (10.9 Mbps) 1m remaining

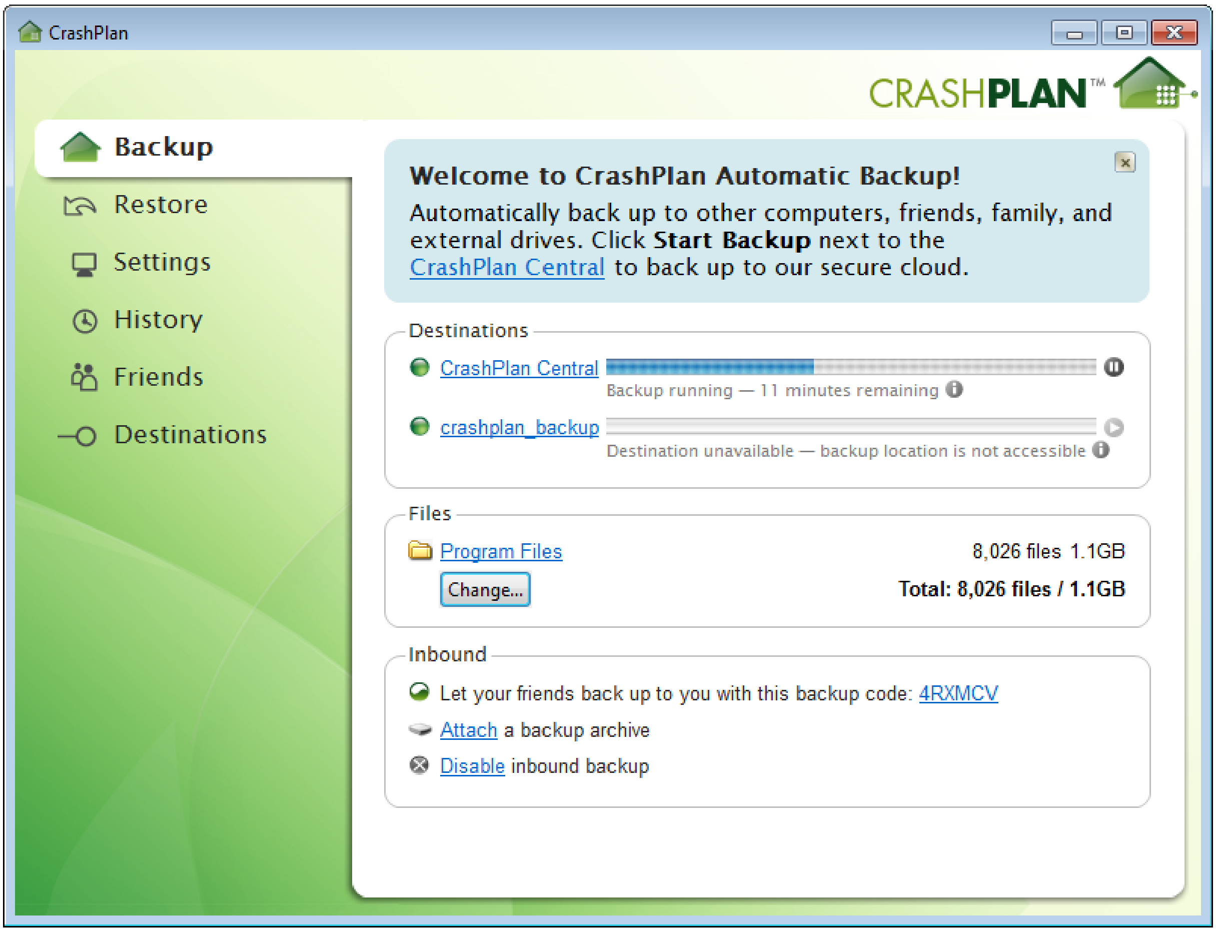
Figure 9: Acronis performance is flawless in all tested categories.

Acronis outperformed the competition in all tested performance scenarios. It uses SSD drives to its fullest potential. Incremental backups are purely that: only saving changes made to a file not the entire file, which safes space, time, performance and bandwidth.

Carbonite

Carbonite is a purely cloud based backup solution. No comparative test was performed.

CrashPlan



Welcome to CrashPlan Automatic Backup!
Automatically back up to other computers, friends, family, and external drives. Click **Start Backup** next to the CrashPlan Central to back up to our secure cloud.

Destinations
CrashPlan Central — Backup running — 11 minutes remaining
crashplan_backup — Destination unavailable — backup location is not accessible

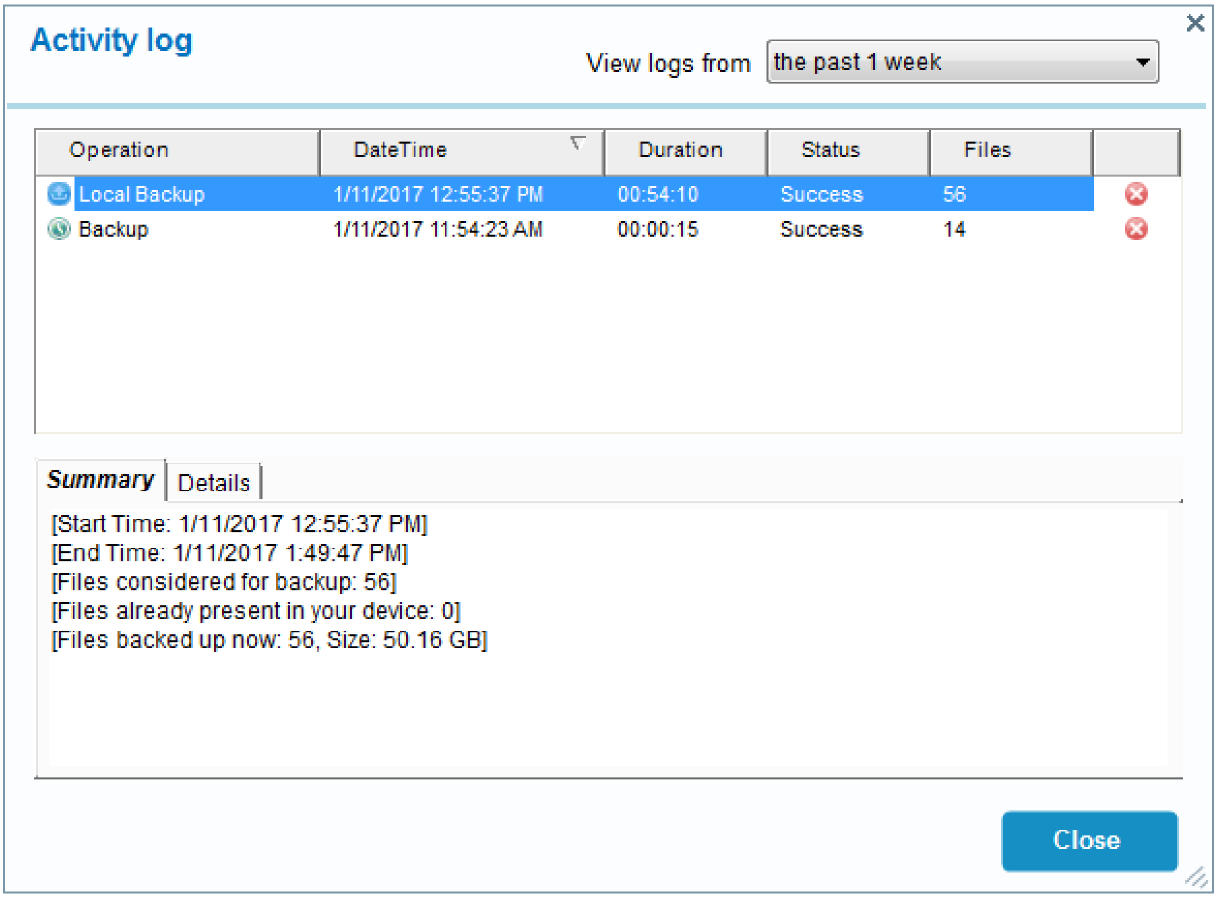
Files
Program Files — 8,026 files 1.1GB
Total: 8,026 files / 1.1GB

Inbound
Let your friends back up to you with this backup code: 4RXMCV
Attach a backup archive
Disable inbound backup

Figure 10: CrashPlan like iDrive setup is straightforward and doesn't require much but to click through.

CrashPlan does well for full system backups and incremental backup of large files on a SSD being 2 and 3 times faster than iDrive respectably, only being a few minutes slower than Acronis. On the other hand, it doesn't perform well with the incremental backups for small files. CrashPlan outperforms Acronis with a continuous backup interval of 60 seconds compared to 5 minutes for Acronis.

iDrive



Operation	DateTime	Duration	Status	Files
Local Backup	1/11/2017 12:55:37 PM	00:54:10	Success	56
Backup	1/11/2017 11:54:23 AM	00:00:15	Success	14

```
[Start Time: 1/11/2017 12:55:37 PM]
[End Time: 1/11/2017 1:49:47 PM]
[Files considered for backup: 56]
[Files already present in your device: 0]
[Files backed up now: 56, Size: 50.16 GB]
```

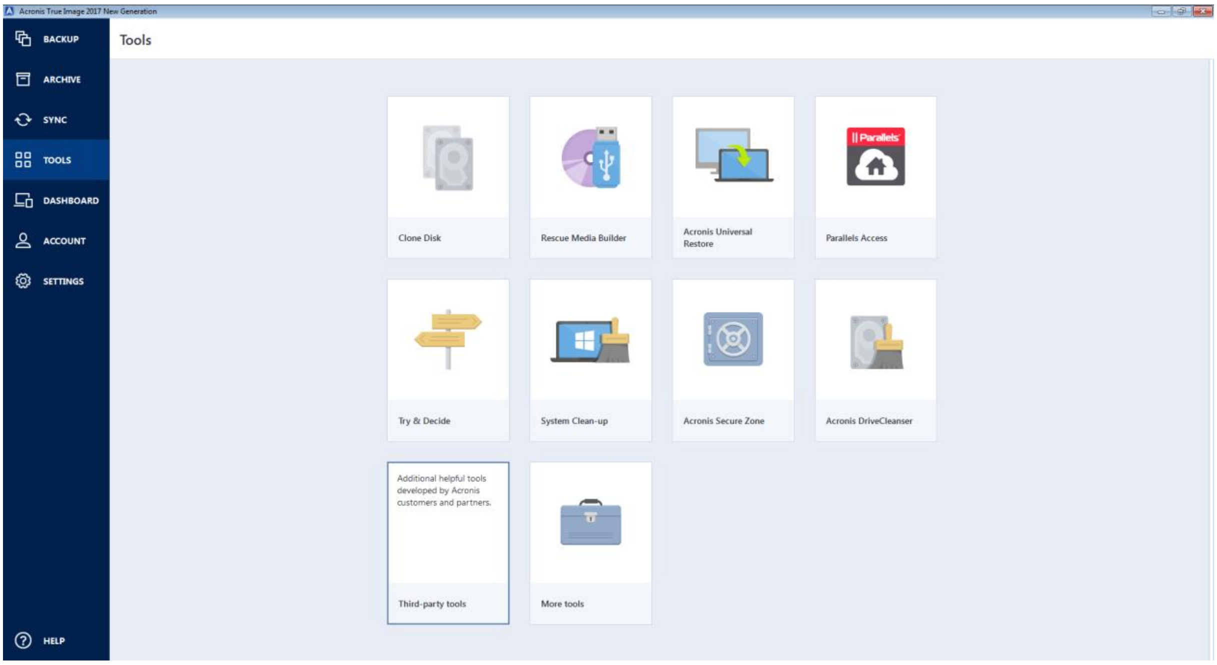
Figure 11: iDrive setup is very easy and doesn’t require much but to click through.

iDrive’s has the shortest interval for continuous backups, saving the files every 20 seconds. iDrive includes a version history which allows recovering previous states of a file with changes one might have overwritten. It also performs well when backing up large files, either from HDD or SSD, and does well when incremental backing-up many small files.

Functionality

Reviewing the amount and quality of features available to choose and customize options.

Acronis

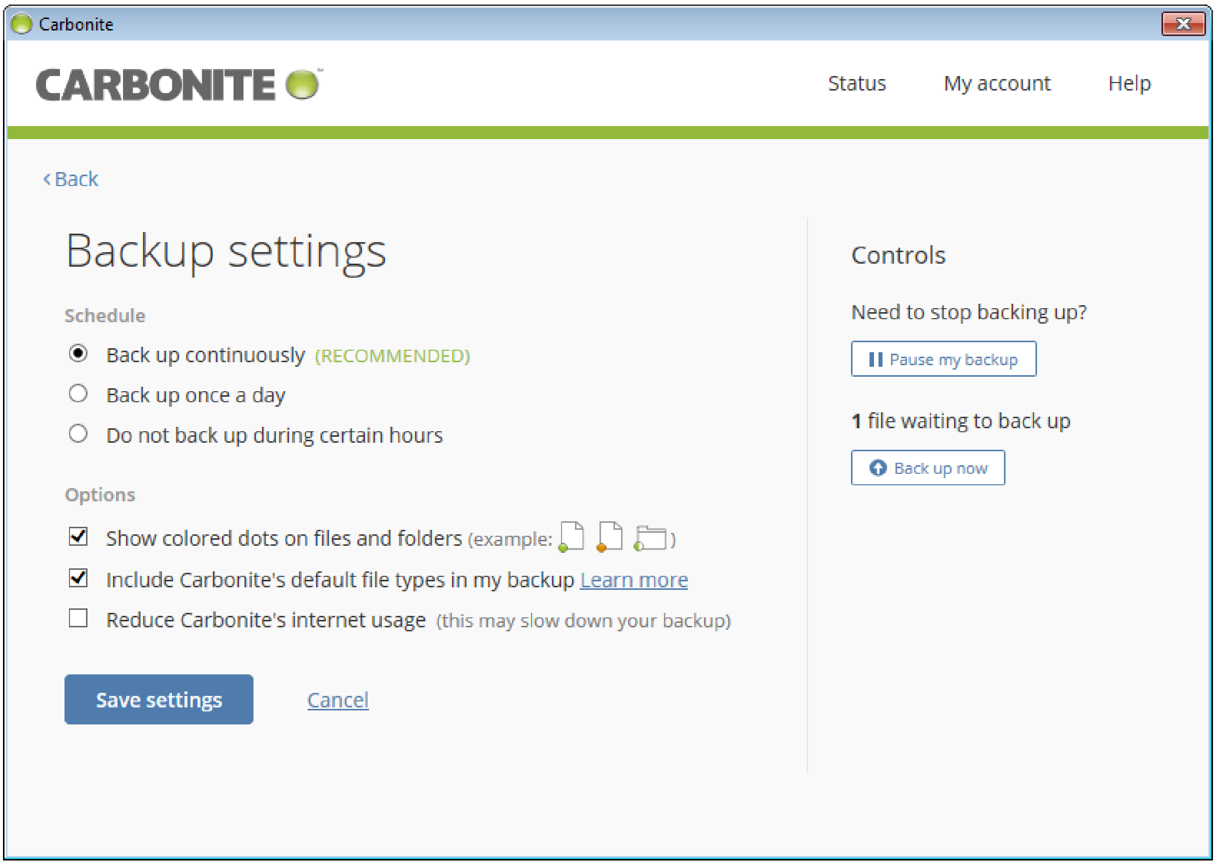


Additional helpful tools developed by Acronis customers and partners.

Figure 12: Acronis provides numerous additional tools.

Acronis shares the first place with iDrive, both having 33 out of possible 39 features required in this category. Additionally, it offers useful features such as *Try&Decide* which makes it possible to roll back the system after changes have been made which turned out to be unwanted. *System Cleanup* security wipes free disk space. *Mobile device backup* of data to local storage. Very positive is the option to choose between 9 countries of storage for the cloud data, for transfer speed and privacy concerns.

Carbonite



Backup settings

Schedule

● Back up continuously (RECOMMENDED)

○ Back up once a day

○ Do not back up during certain hours

Options

☑ Show colored dots on files and folders (example:)

☑ Include Carbonite's default file types in my backup Learn more

□ Reduce Carbonite's internet usage (this may slow down your backup)

Save settings Cancel

Controls

Need to stop backing up?

Pause my backup

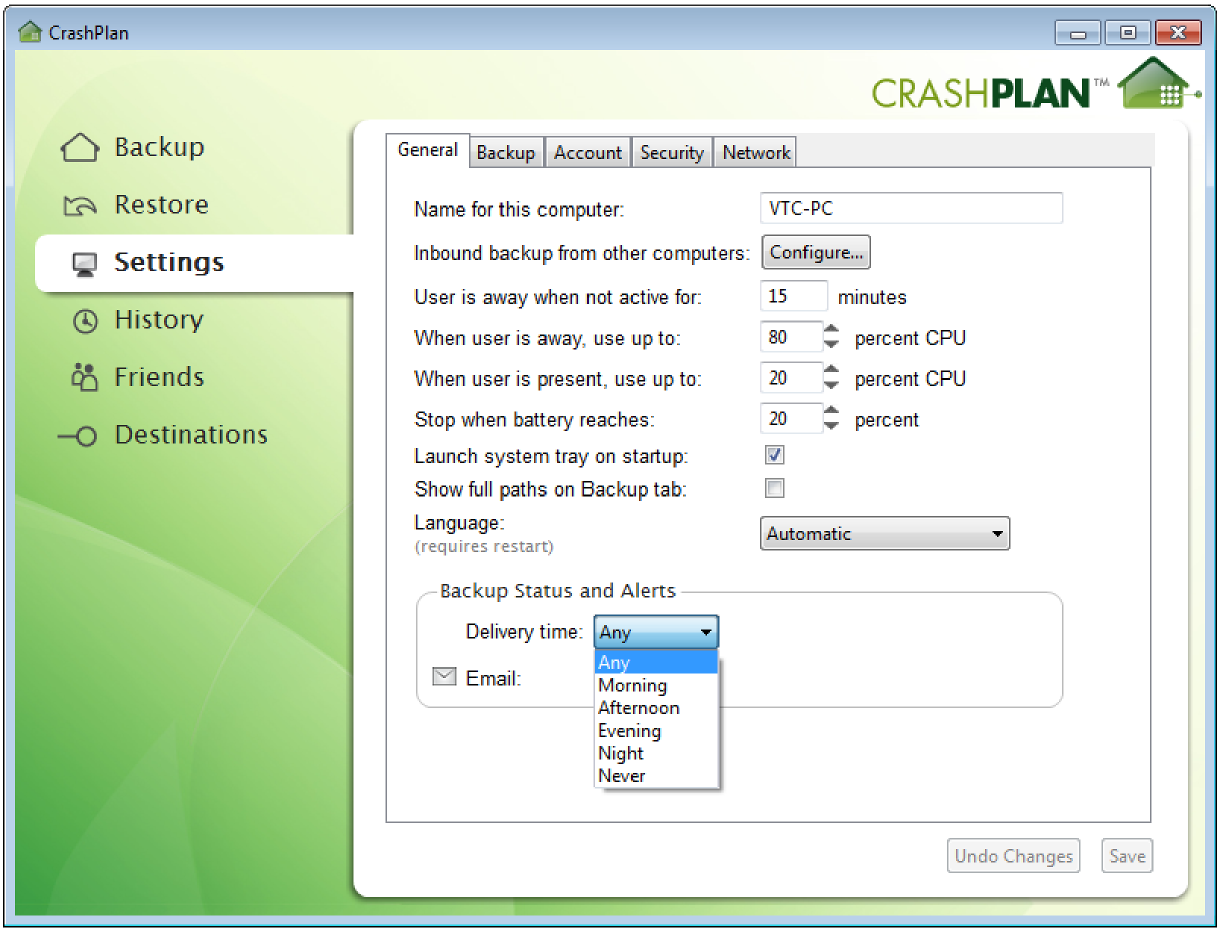
1 file waiting to back up

Back up now

Figure 13: Carbonite only offers few settings to change.

Carbonite has few options to change settings. It is an out of the box solution which looks like it aims to take all responsibility for configurations from the user. The integration into the windows file explorer can be very handy. It allows to determine whether a folder has been backed up yet or is still being processed. Backup is only available in the cloud, in the PLUS version an image of the hard drive can be created and stored locally.

CrashPlan



Name for this computer: VTC-PC

Inbound backup from other computers: Configure...

User is away when not active for: 15 minutes

When user is away, use up to: 80 percent CPU

When user is present, use up to: 20 percent CPU

Stop when battery reaches: 20 percent

Launch system tray on startup: ☑

Show full paths on Backup tab: □

Language: Automatic
(requires restart)

Backup Status and Alerts

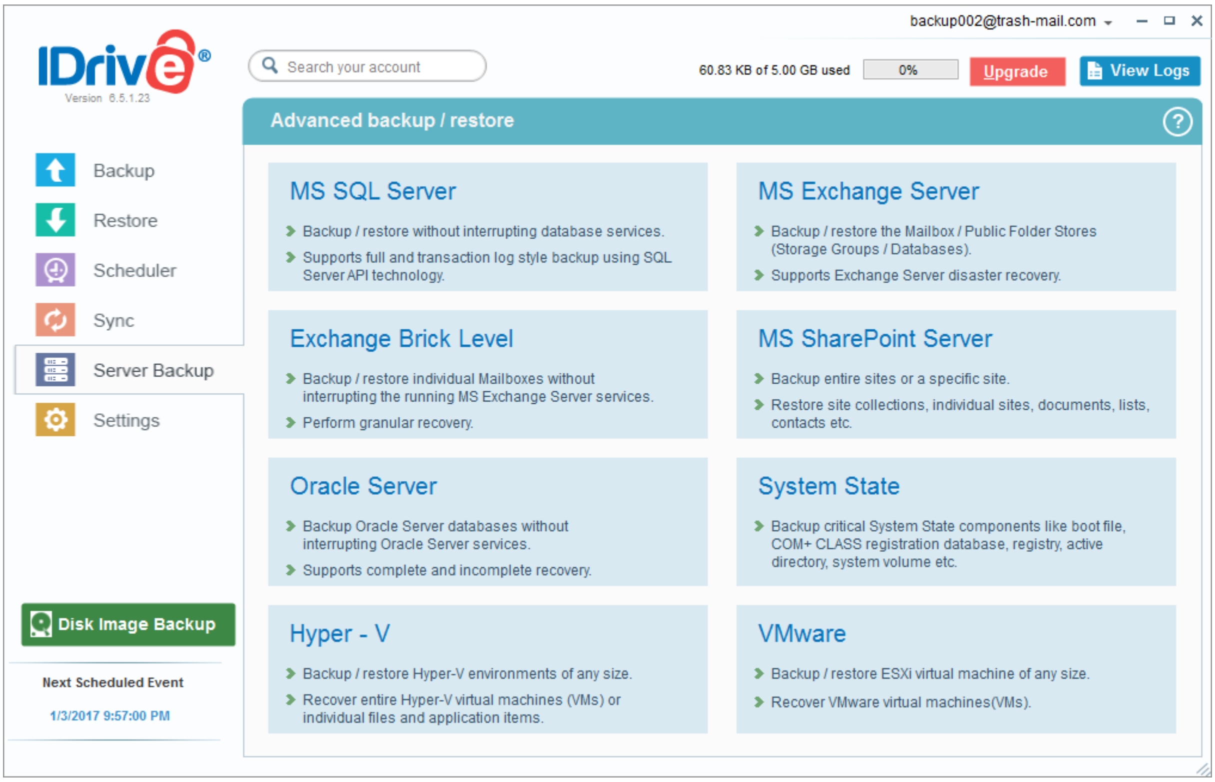
Delivery time: Any

Email:

Figure 14: CrashPlan has many individual settings to customize the user backup options.

Crashplan doesn’t have as many conventionally backup features as iDrive or Acronis but offers some helpful features often found only in professional solutions such as self healing archives, de-duplication and restoring a backup job to different computers. It also allows access to a backup job through a mobile app. It is the only product tested allowing local and cloud backup at the same time.

iDrive



Advanced backup / restore

MS SQL Server
- Backup / restore without interrupting database services.
- Supports full and transaction log style backup using SQL Server API technology.

MS Exchange Server
- Backup / restore the Mailbox / Public Folder Stores (Storage Groups / Databases).
- Supports Exchange Server disaster recovery.

Exchange Brick Level
- Backup / restore individual Mailboxes without interrupting the running MS Exchange Server services.
- Perform granular recovery.

MS SharePoint Server
- Backup entire sites or a specific site.
- Restore site collections, individual sites, documents, lists, contacts etc.

Oracle Server
- Backup Oracle Server databases without interrupting Oracle Server services.
- Supports complete and incomplete recovery.

System State
- Backup critical System State components like boot file, COM+ CLASS registration database, registry, active directory, system volume etc.

Hyper - V
- Backup / restore Hyper-V environments of any size.
- Recover entire Hyper-V virtual machines (VMs) or individual files and application items.

VMware
- Backup / restore ESXi virtual machine of any size.
- Recover VMware virtual machines(VMs).

Figure 15: iDrive offers many features useful for business purposes, not so much for private use.

iDrive shares first place for available features with Acronis. Just like Acronis it offers the option to share files from backup via email or sync files between different devices. In its free version it provides 5GB of free cloud storage. In our test iDrive supported more operation systems than any other application.

Threat Protection

Testing how well the DPBs cope when exposed to the threat of ransomware.

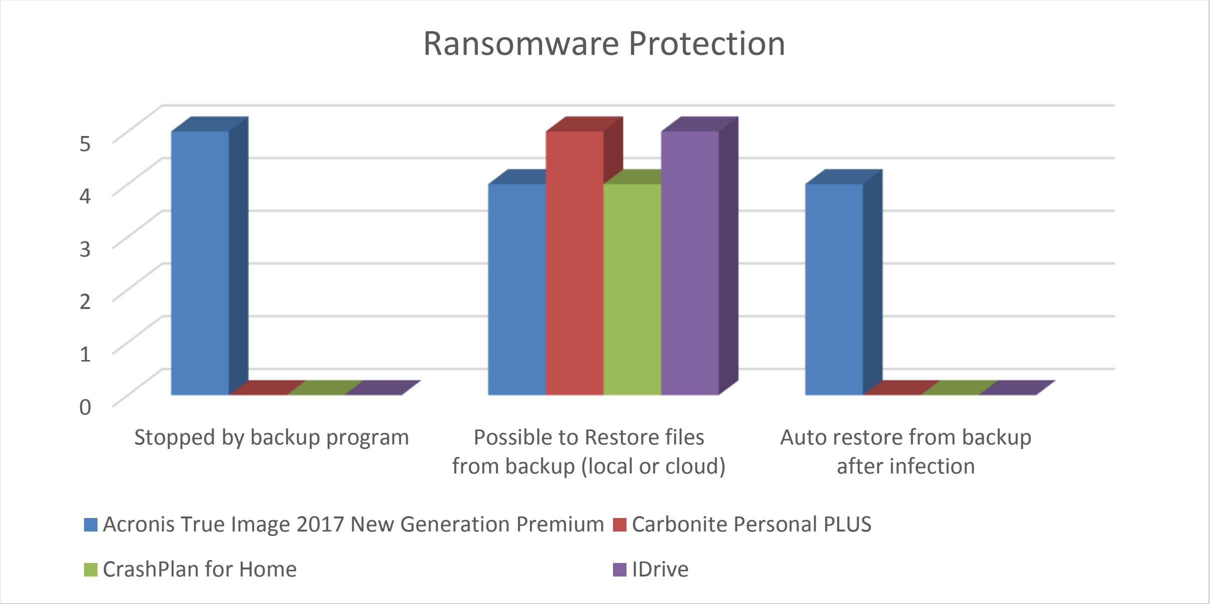


Figure 16: Individual protection displayed by products.

Carbonite, CrashPlan and iDrive

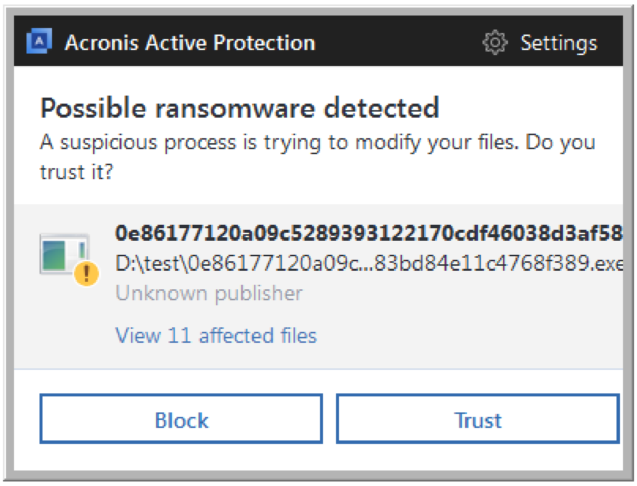
Neither Carbonite, CrashPlan nor iDrive currently provide an active protection against encryptor and ransomware. Protection provided comes in form of restoring encrypted data from backups. In our test this was possible with all three products, except in one case when CrashPlan program files were encrypted and the application stopped working. In some cases some of the backup files themselves have been encrypted on the local storage, but no vital files have been affected and recovering data from those files was still possible.

All products provide the option to use continuous backup. When this feature is used the chance to lose data after an infection during active work can be significantly reduced depending on the interval time of these backups.

iDrive creates a backup every 20 seconds which is the shortest interval in all four tested products. CrashPlan also performs well with a backup every minute. Acronis is the third quickest with a backup interval of every 5 minutes, but this is less significant as mentioned below an active protection is provided. Carbonite disappoints with a backup after at longest 10 minutes but then only backing up again 24 hours later.

Acronis

Acronis is the only tested DPB offering an active ransomware protection. It has stopped all five encryptors tested. Most of the encrypted files have been recovered. In one case the files could not be recovered by Acronis and the local backup was also affected. Only a cloud backup could have helped recover the files, but that option is not available for continuous backups.



Acronis Active Protection

Possible ransomware detected

A suspicious process is trying to modify your files. Do you trust it?

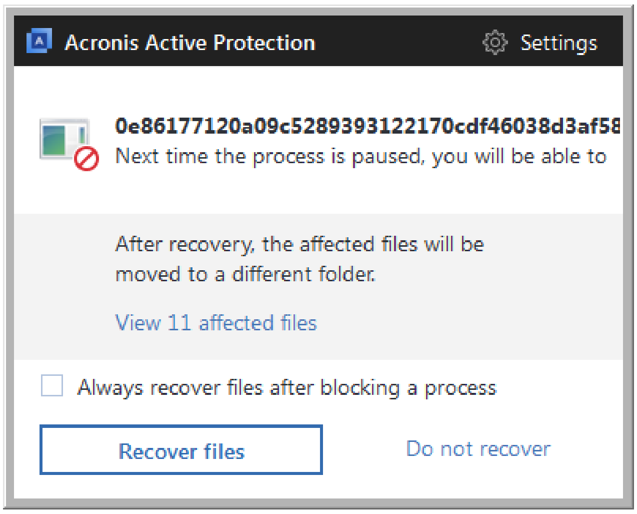
0e86177120a09c5289393122170cdf46038d3af58

D:\test\0e86177120a09c...83bd84e11c4768f389.exe

Unknown publisher

Figure 17: Acronis can detect possible encryptors and pauses them until the user has made a decision.

A few seconds after the ransomware has been initiated the Acronis Active Protection becomes active. The ransomware execution is interrupted and the user asked to validate the application and if deemed to be malicious by the user it is blocked and stopped.



Acronis Active Protection

0e86177120a09c5289393122170cdf46038d3af58

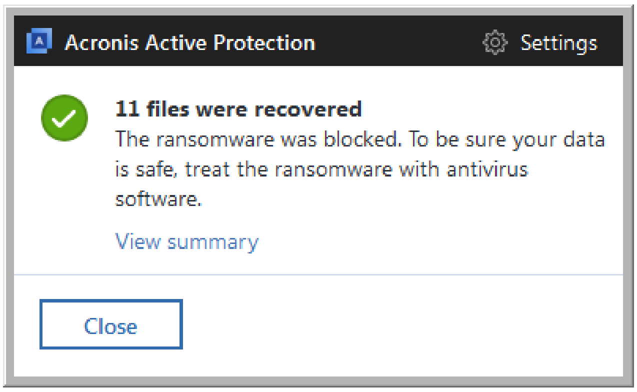
Next time the process is paused, you will be able to

After recovery, the affected files will be moved to a different folder.

□ Always recover files after blocking a process

Figure 18: Acronis offers to recover the previously maliciously encrypted files.

Acronis detects the ransomware by behavior, so some files are inevitable affected already. Acronis offers the option to recover these files from cache. The files don’t have to be included in a previously created backup. There are some cases when not all files could be recovered by this method so having a backup of all files can be recommended for the worst case scenarios.



11 files were recovered

The ransomware was blocked. To be sure your data is safe, treat the ransomware with antivirus software.

Figure 19: Acronis provides information on the data recovered.

The user is informed about the success of recovering the files. There might be some files left from the ransomware with details on how to pay ransom to recover the files. The threat is remedied and the user safe again.

Certificate: Approved Backup & Data Security Software

Criteria

The products were reviewed in the categories Usability, Performance and Functionality. In order to receive the AV-TEST APPROVED BACKUP & DATA SECURITY SOFTWARE certificate it was necessary to achieve strong results in all three categories.

Usability

Products have to be easy to configure and to use: Clear arranged menu with no unnecessary interaction, ease of use and the option to use a configuration wizard.

Performance

Products have to be fast in backing up and restoring files with minimal system impact: Use technologies intelligently to significantly reduce incremental and full backup time and make full usage off faster hardware like SSD drives.

Functionality

Products have to provide all features expected in a modern backup solution: Continuous backup, online and offline backup options, data file and transmission encryption, data compression and scheduled backups. Dedicated protection against malware attacks is a welcome addition.

Awarded

Even though, Acronis, iDrive and Crashplan were all able to fulfil the requirements set for Usability and Functionality, Acronis was the only product to fully satisfy the requirements set for Performance. Therefore Acronis is the first product to achieve the AV-TEST APPROVED BACKUP & DATA SECURITY SOFTWARE certificate.

Figure 20: APPROVED BACKUP & DATA SECURITY SOFTWARE

Conclusion

With its ability to protect against malicious encryptors, Acronis provides a comprehensive data protection solution. The comprehensive set of easy to use features combined with outstanding performance results and an integrated threat protection offer a great data protection for private users on windows.

The objective of the here-presented tests was to assess the products' completeness as a data protection tool. Indeed, Acronis's product delivered convincing results across the tested categories either coming first or shared first in all categories – scoring 78% on usability rating, 92% on performance, 90% on active threat protection and 85% on available features.

iDrive came in second place. It does not provide an active protection. On the one hand, it has an extensive list of features and is easy to use and offers 5GB cloud storage in the free version. On the other hand, the performance is nowhere near the top but reasonable compared to the competition.

CrashPlan has similar results in terms of performance as iDrive. Like most other tested products there is no active protection. The user interface is also not very convincing but all options and features can be found after a getting-used-to-it period. The range of features are not as comprehensive as with the competition but they are complemented by some semi-professional options which are a nice-to-have.

Carbonite is an install-four-clicks-and-forget-about-it solution. Not many options are made available to the user. Nevertheless, the integration into the windows file explorer is a nice addition, allowing the user to determine what is backed up yet and what data is still processed. It also allows quickly adding new files or folders to the backup job. The exclusion of executables and certain videos files is a nuisance.

Appendix

Hardware specifications

Windows

Operating system	Windows 7 Ultimate with all patches available on January 3rd 2017.
Hardware	• Intel Xeon Quad-Core X3360 CPU • 4 GB RAM • 500 GB HDD (Western Digital), 512 GB SSD (Samsung) • Intel Pro/1000PL (Gigabit Ethernet) NIC

Test Results

Usability Test Results

Ease of installation	Acronis True Image 2017 New Generation Premium	Carbonite Personal PLUS	CrashPlan for Home	IDrive
Ease of setup complete backup	++	-	+	+
Ease of setup specific file backup	++	-	+	+
Default setup backup after installation				
Default backup setup	+	+	+	+
Default backup starts automatically	-	+	-	-
Default backup is scheduled automatically or after first start	+	+	+	+
Usability score	77,78%	55,56%	55,56%	55,56%

Performance Test Results

	Acronis True Image 2017 New Generation Premium		Carbonite Personal PLUS	CrashPlan for Home		IDrive	
Backup time							
* Large files (SSD)	00:11:46	100,00%	-	01:03:00	18,68%	00:53:16	22,09%
* Small files (SSD)	00:17:34	100,00%	-	00:59:20	29,62%	01:04:45	27,14%
* Full System (SSD)	00:14:56	100,00%	-	00:22:40	65,86%	01:00:16	24,77%
Full restore time (after deleting all files)							
* Large files (SSD)	00:10:39	100,00%	-	00:20:40	51,53%	00:17:17	61,60%
* Small files (SSD)	00:19:02	100,00%	-	00:28:20	67,18%	00:32:34	58,45%
Backup							
* Large files (HDD)	00:25:04	100,00%	-	01:07:20	37,23%	00:54:51	45,70%
* Small files (HDD)	00:24:25	100,00%	-	00:32:00	76,30%	00:32:21	75,49%
Incremental backup time (after changing 10% of data)							
* Large files (SSD)	00:05:33	100,00%	-	00:23:00	24,15%	00:52:26	10,59%
* Small files (SSD)	00:03:12	100,00%	-	00:35:20	9,04%	00:08:33	37,36%
Incremental restore time (after changing 10% of data)							
* Large files (SSD)	00:10:46	100,00%	-	00:20:40	52,12%	00:17:02	63,26%
* Small files (SSD)	00:18:59	100,00%	-	00:27:40	68,59%	00:32:30	58,38%
Continuous backup time							
Backup intervals	00:05:00	6,67%	00:10:00	00:01:00	33,33%	00:00:20	100,00%
Performance score		92,22%	-		44,47%		48,74%

Functionality Test Results

	Acronis True Image 2017 New Generation Premium		Carbonite Personal PLUS		CrashPlan for Home		IDrive	
Functionality score	33/39	84,62%	19/39	48,72%	27/39	69,23%	33/39	84,62%

Threat Protection Test Results

	Acronis True Image 2017 New Generation Premium		Carbonite Personal PLUS		CrashPlan for Home		IDrive	
Stopped by backup program?	5/5	50,00%	0/5	0,00%	0/5	0,00%	0/5	0,00%
* Time it took to stop ransomware (seconds)	23,6	16,00%	-			-	-	
* Ransomware removed from machine?	0/5	0,00%	0/5	0,00%	0/5	0,00%	0/5	0,00%
Possible to restore files from backup or cloud?	4/5	24,00%	5/5 (cloud)	30,00%	4/5	24,00%	5/5 (cloud)	30,00%
* Auto restore from backup after infection?	4/5	0,00%	0/5	0,00%	0/5	0,00%	0/5	0,00%
Threat protection score		90,00%		30,00%		24,00%		30,00%