



MRG Effitas Comparative assessment of Data protection/backup products on protection, performance and usability

1 Table of Contents

1	Introduction	3
2	Executive Summary	3
2.1	Final results	4
3	Backup products tested.....	4
4	Test conditions.....	5
5	Test environment	5
6	Ransomware families used.....	6
7	Test scenarios.....	13
7.1	Typical scenarios.....	13
8	Detailed results	14
8.1	Backup protection	14
8.1.1	Local backup file protection against ransomware.....	14
8.1.2	Cloud backup file protection against ransomware	15
8.2	Feature comparison chart.....	18
8.3	Performance.....	19
9	Product feature comparison	23
9.1	Acronis True Image 2017 New Generation.....	23
9.2	CrashPlan.....	25
9.3	EaseUS Todo Backup Home	27
9.4	Genie Timeline Home 2016.....	29
9.5	IDrive.....	31
9.6	Macrium Reflect Home	33
9.7	NovaBACKUP.....	35
9.8	Paragon Backup and Recovery 16.....	37
10	Conclusion.....	39
11	Appendix.....	40
11.1	Methodology used in the assessment.....	40
11.1.1	Local HDD operations	41
11.1.2	Cloud operations	45
11.1.3	Local SSD operations.....	49

1 Introduction

With this report MRG Effitas' purpose was to provide an independent report of a comparative assessment of a group of data protection (a.k.a backup) products.

There's no best backup tool for every user, but an independent comparison of the options would provide a cleaner view of the demands and offerings when it comes to choosing the most suitable software for an individual.

Endpoint backup has gone beyond simple backup/restore process to a broader end-user data protection solution reducing and precluding various risks such as ransomware infection, which is a most imminent threat to an average user– with the possibilities of the smallest impact on one's productivity and convenience.

2 Executive Summary

This Comparative test report is designed to serve as a reflection of product protection, usability and performance level based on the unique and common features of each backup solution.

Being the world's largest supplier of early-life malicious binaries and malicious URLs, and from our own simulator development, we know that all endpoints can be infected, regardless of the security solution employed. That is why in these tests we first focused on the backup protection level against ransomware infection. Followed by performance and usability because besides of the data protection, the backup solution products should be fast and usable.

When conducting these tests, we tried to simulate average user behavior. We are aware that a “Real World” test cannot be conducted by a team of professionals inside a lab because we understand how certain types of software work, how Ransomware attacks and how such attacks could be prevented. Simulating normal user behavior means that we paid special attention to all alerts given by backup applications. It is very important to note that the best choice for an average user is to keep things very simple and for the product not to present many confusing settings or questions. According to this prospect we used every backup application with its default settings.

As endpoints get compromised by Ransomware on an ever-greater scale, the ability to protect the machine from being encrypted entirely and the prospect of restoring the PC and user files after the infection was the most important testing metric in this comparative assessment we paid attention to.

2.1 Final results

Among all the products we tested, only Acronis True Image 2017 New Generation was able to protect the backups from every Ransomware family tested. The other solutions have basically zero backup protection when it comes to Ransomware.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Cerber	✓	✓	✓	✓	✓	✓	✓	✓
Troldesh	✓	✓	✓	✗	✗	✓	✓	✓
Dharma	✓	✗	✗	✗	✗	✗	✗	✗
Locky	✓	✓	✓	✗	✗	✓	✓	✓
Havoc	✓	✗	✗	✗	✓	✗	✗	✗
Globe	✓	✓	✓	✗	✗	✓	✓	✓
CryptoMix	✓	✗	✓	✗	✓	✓	✓	✗
Sage	✓	✗	✓	✓	✓	✓	✓	✓
CryptoShield	✓	✓	✓	✓	✓	✓	✓	✓
GoldenEye	✓	✗	✗	✗	✗	✗	✗	✗

Based on the tests, only Acronis' backup file is protected against the tested ransomware, the other products archives are only left untouched if the ransomware is not configured to encrypt that kind of file type.

Acronis won most performance tests, and when it did not win, it finished second.

When it comes to self-protection, and protection of the cloud accounts, we could not find issues with the following solutions: Acronis, Paragon and Macrium.

3 Backup products tested

- Acronis True Image 2017 NG Build 6116
- CrashPlan Home 4.8.0
- EaseUS TODO Backup Home 10.0
- Genie Timeline Home 2016
- IDrive 6.5.1.23
- Macrium Reflect Home 6.3.1655
- NovaBACKUP 18.5 Build 926
- Paragon Backup and Recovery 16

4 Test conditions

MRG Effitas provided the resources to test the selected products' performance and to validate the data protection of the backup solutions once the test system was infected with Ransomware. The backup products tested were fully functional versions for personal use products whether they be free/trial or paid versions. All participants were installed and used in the exact same and fully patched environment, in terms of both software and hardware. Software were tested for functionality, reliability, and user experience and given the same test environment. Speed and resource usage were also tested and compared.

5 Test environment

Upon testing we tried to reproduce an average, most commonly used home user PC and network environment:

- OS: Windows 7 x64
- CPU: Intel Core i5 2540M
- Memory: 8GB DDR3
- HDD: SATA 3 Toshiba MK7559GSXP
- SSD: SATA 3 OCZ Agility 3
- Network: 802.11g


6 Ransomware families used

The following paragraph contains basic description about the ransomware families used in the test.

Dharma:



webmafia@asia.com



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail webmafia@asia.com. You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send to us up to 3 files for free decryption. Please note that files must NOT contain valuable information and their total size must be less than 10Mb.

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins

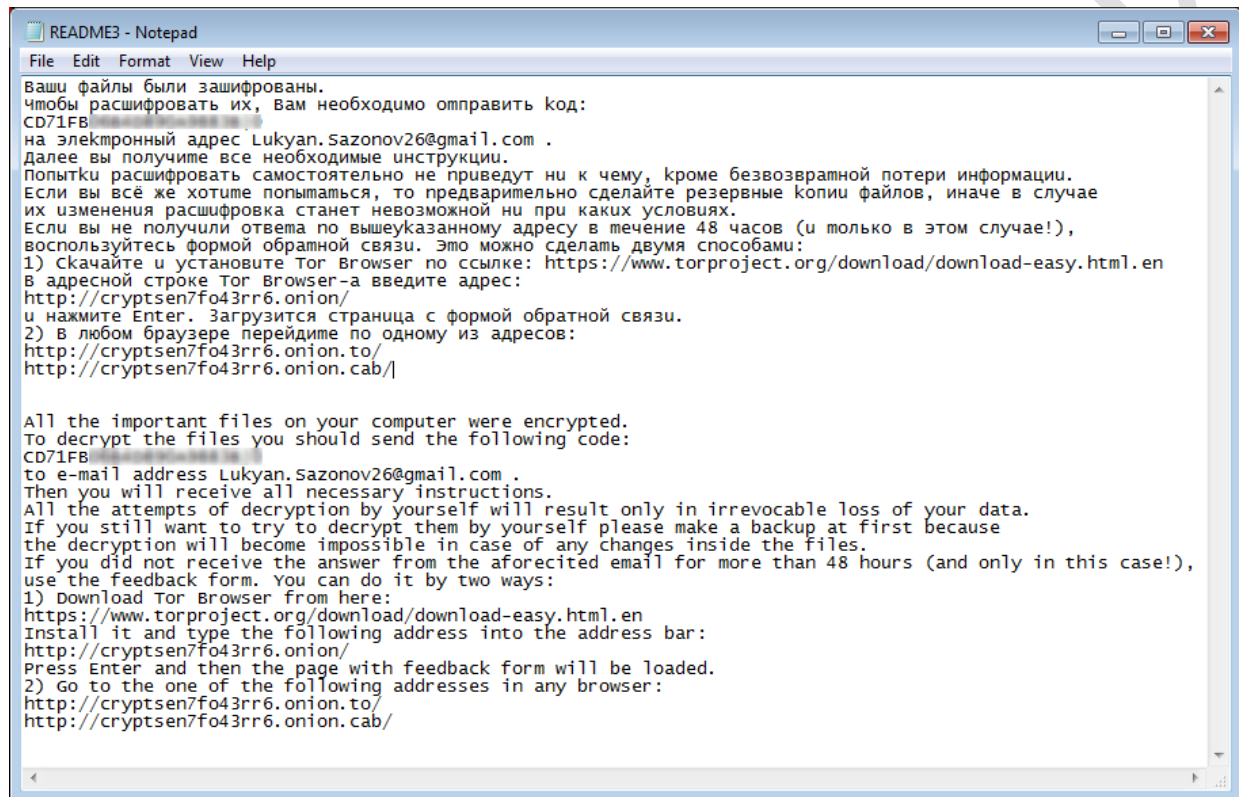
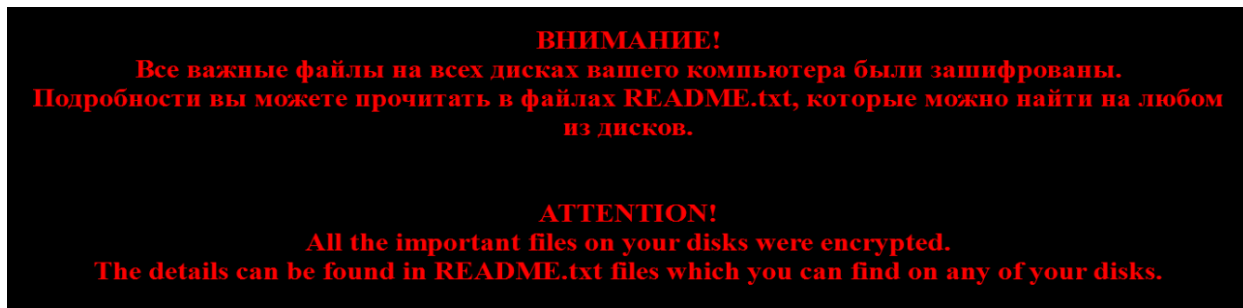
Also you can find other places to buy Bitcoins and beginners guide here:
<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

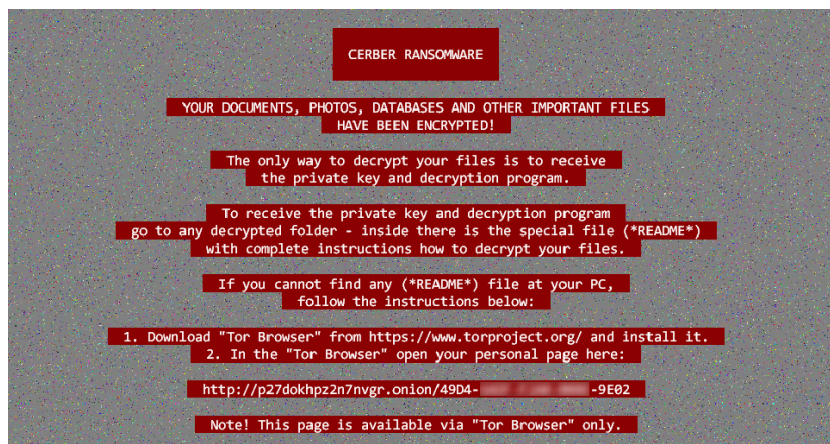
Dharma is a new variant of Crysis - a high-risk ransomware-type virus. Following successful infiltration, Dharma encrypts stored files using AES. In addition, this file-encoder usually appends the “[webmafia@asia.com]. wallet” “[webmafia@asia.com]. dharma” or “[webmafia@asia.com].zzzzz” extension and encrypts the filename too. If the ransomware is not eradicated from the system, it loads itself with every reboot and it will result in new encrypted files. The encryption cost varies for each individual. Dharma is usually dropped after an RDP brute-force attack is successful.

Troldesh:



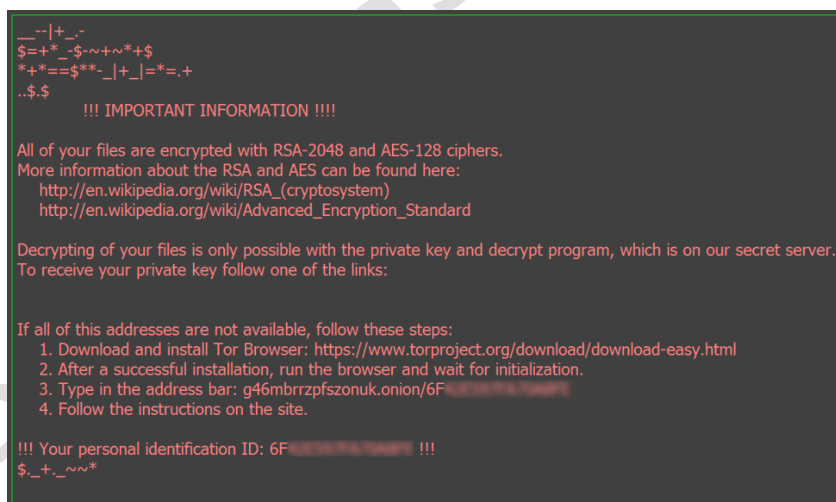
The Troldesh ransomware is also known as Encoder.858. It carries out a similar attack like most ransomware. But it will replace the files' names with random characters – making it harder to identify the files - and uses AES encryption and appends the “.xtbl” extension. Although most ransomware attacks use an online page, often through TOR and automated payment methods, the Troldesh ransomware provides an email address through which attackers communicate with the victim directly and establish the ransom and payment in rubles.

Cerber:



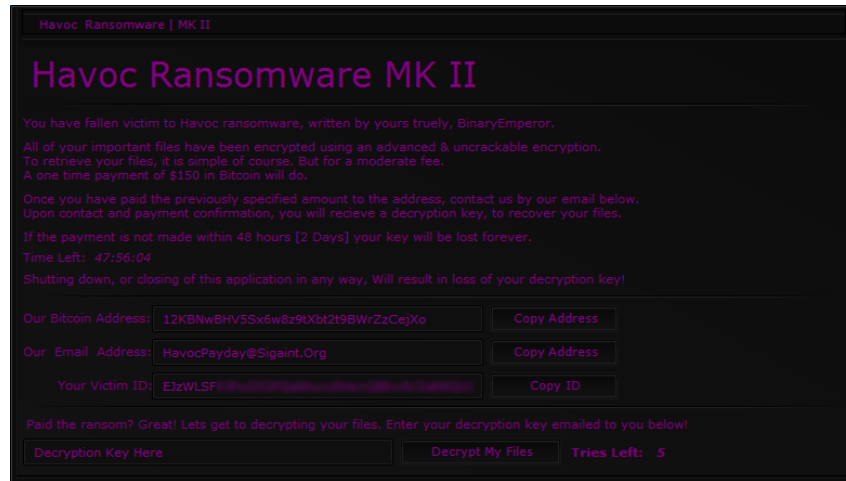
Cerber ransomware, much like many other encryption type ransomware, is known to encrypt files with AES-256 encryption on the infected computer. It creates random filenames and appends the extension “.CERBER” or “.B126” and hold those files for a substantial ransom fee. As it encrypts the victim's files, it creates TXT, HTML, and VBS files named 'DECRYPT MY FILES' with instructions on how to pay and it has audible voice saying, "Attention! Attention! Attention!, Your documents, photos, databases, and other files have been encrypted!" The victim has to pay the 1-1.25 Bitcoin (\$1000-\$1250) ransom via TOR browser within one week or the amount is doubled.

Locky:



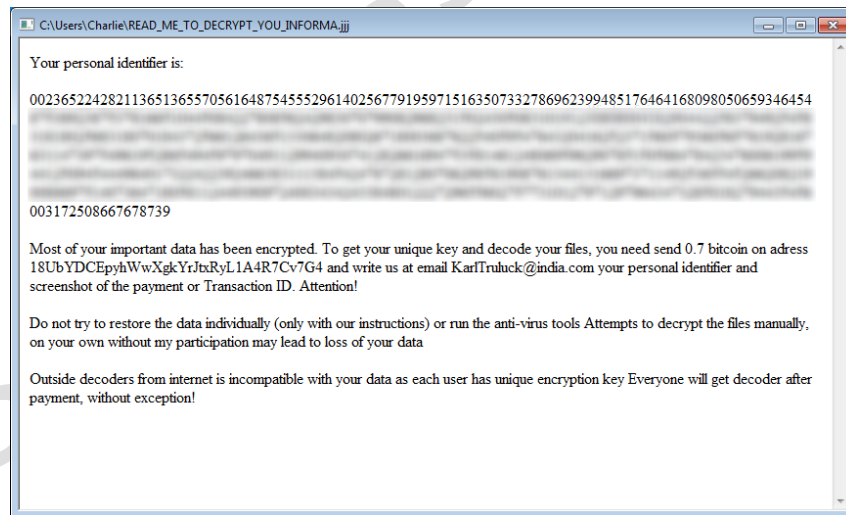
Locky ransomware is one of the most dangerous ransomware families based on the number of infections. Once it is installed on the victim's computer it will perform a scan and encrypt user files using its RSA-2048 & AES-128 encryption algorithm. It converts the filenames to a unique character letter and number combination and appends “.locky” or “.osiris” extension and deletes Shadow Volume copies of encrypted files as well as System Restore points. After encryption, a message (displayed on the user's desktop) instructs them to download the Tor browser and visit a specific website for further information where Locky demands a payment between 0.5-1 Bitcoin (\$500-\$1000).

Havoc MK II:



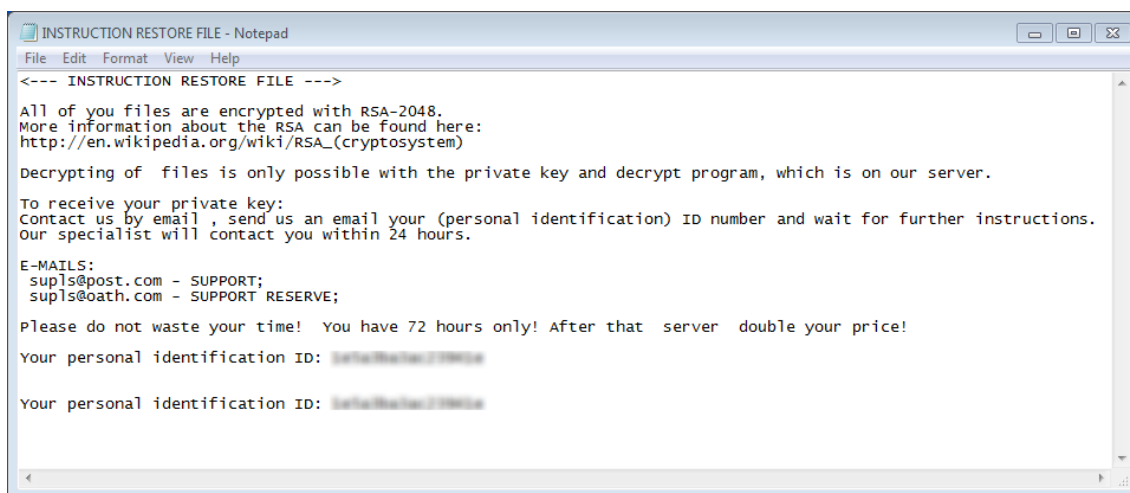
The Havoc MK II Ransomware's bright violet ransom note first appeared in public in January 2017. It uses RSA256 encryption and ".havoccrypt" extension to lock the victim's files, targeting a wide variety of files that can include video and audio files, text files, databases, images, and numerous other commonly used file types. However, Havoc Ransomware will not encrypt files that are larger than a certain limit, to make sure that the attack is as fast as possible. The user has 2 days to pay 0.15 Bitcoin (\$150) ransom fee to restore the data or the restore key is deleted.

Globe3:



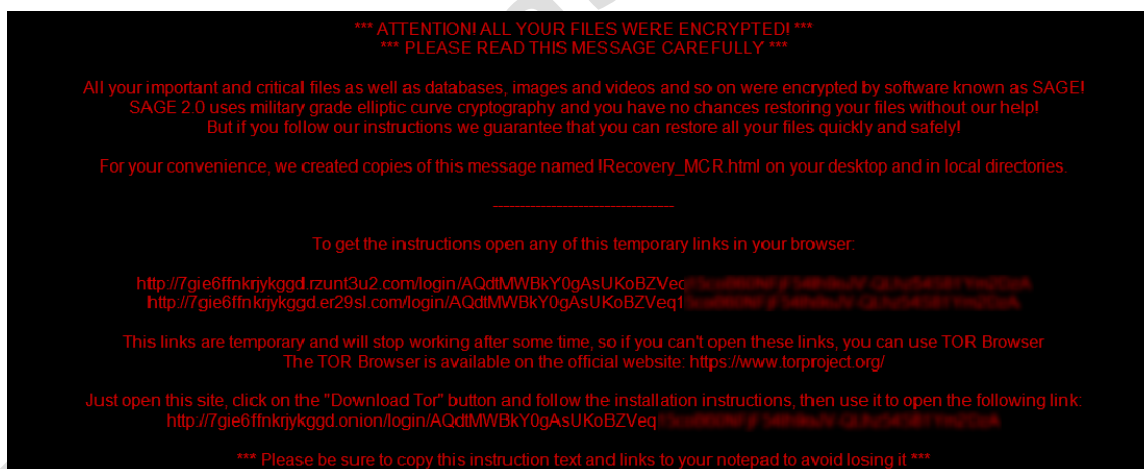
The main targets of the Globe Ransomware are small business but it causes damage to any computer it infects. This crypto Trojan encrypts user data using AES-256 + RSA and adds ".wuciwug" extension to the files. The main difference from the previous two versions of the Globe3 is on the level of encryption operations. The first version of the Globe used the Blowfish algorithm to encrypt files, Globe2 used RC4 and RC4 + XOR. After encrypting a victim's files, the Globe3 shows "How to restore your files.hta" ransom note which advises the user about the 0.7 Bitcoin (\$700) ransom fee and contains instructions on how to pay to recover the encrypted files.

CryptoMix:



CryptoMix Ransomware is made similarly to CryptoWall 3.0, CryptoWall 4.0 and CryptXXX. Just like many other encrypting trojans it uses AES + RSA-2048 ciphers to encrypt predetermined files but adds “.rdmk” extension. Victims have to email the cyber criminals on the given email address and wait around 12 hours for a response which is encrypted and password protected. The ransom fee is usually around 5 Bitcoins (\$500). CryptoMix claims that the collected profit is used for charity as the developers are calling themselves the Charity Team, who also offer a "Free tech support" for those who decided to pay up.

Sage 2.0:



Sage Ransomware is related to the TeslaCrypt family. This crypto ransomware encrypts user data using AES-256 and RSA-1024 cipher and adds “.sage” file extension to them. After encrypting, Sage delivers its ransom note as a text file on the victim's Desktop and opens an HTML file in the default browser. It will also change the victim's Desktop image into its ransom note. It then instructs the victim to use a Tor-site to pay the 2 Bitcoin (\$2000) ransom – which is doubled after 7 days – and get instructions on how to restore files.

CryptoShield 1.0:

NOT YOUR LANGUAGE? USE <http://translate.google.com>

What happened to you files?

All of your files were encrypted by a strong encryption with RSA-2048 using CryptoShield 1.0.

More information about the encryption keys using RSA-2048 can be found here: [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

How did this happen ?

Specially for your PC was generated personal RSA-2048 KEY, both public and private.

ALL your FILES were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our secret server.

What do I do ?

So, there are two ways you can choose: wait for a miracle and get your price doubled, or start send email now for more specific instructions, and restore your data easy way.

If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

To receive your private software:

Contact us by email , send us an email your **(personal identification) ID number** and wait for further instructions.

Our specialist will contact you within 24 hours.

For you to be sure, that we can decrypt your files - you can send us a single encrypted file and we will send you back it in a decrypted form. This will be your guarantee.

Please do not waste your time! You have 48 hours only! After that The Main Server will double your price!

So right now You have a chance to buy your individual private SoftWare with a low price!

Dear antivirus companies. We do not have any relation with CryptoMix or CrypMix. Please do not deceive the people.

CONTACTS E-MAILS:

restoring_sup@india.com - SUPPORT;

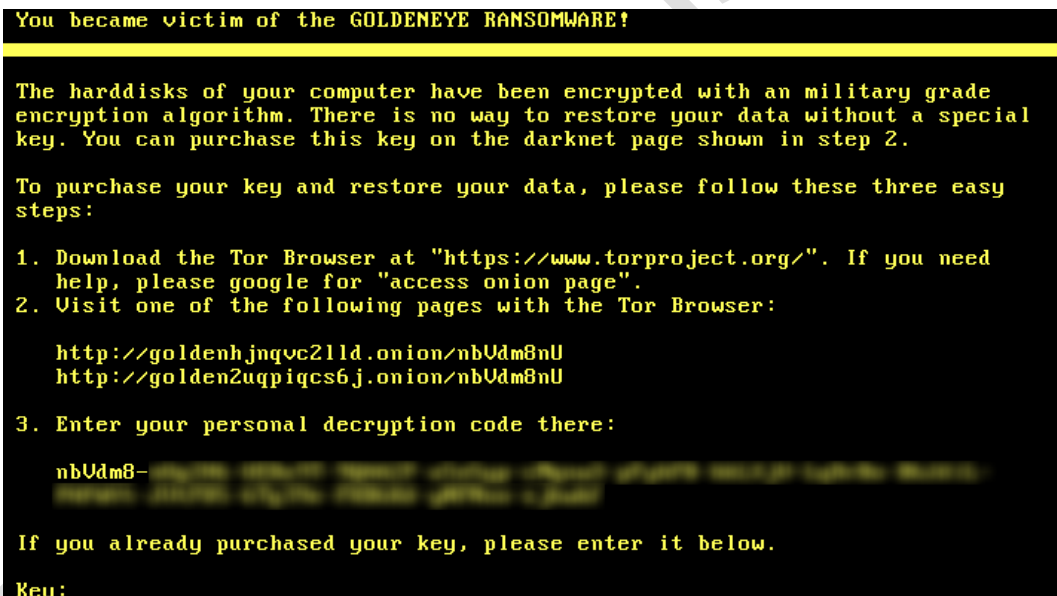
restoring_sup@computer4u.com - SUPPORT RESERVE FIRST;

restoring_reserve@india.com - SUPPORT RESERVE SECOND;

ID (PERSONAL IDENTIFICATION): ████████████████████

CryptoShield 1.0 is the newest mutation of CryptoMix. It appeared on security reports in February, 2017. CryptoShield Trojan is programmed to hide its process in the system background and use as little hardware resources as possible. It uses RSA-2048 cipher to encrypt files and ROT-13 to encrypt filenames and adds a “.CRYPTOSHIELD” extension to them. The ransom notification is loaded in the default Internet browser and a copy is saved on the desktop as “# RESTORING FILES #.TXT” which instructs the victims to contact the criminals via email. The decryption software is priced around 5 Bitcoin (\$5000).

GoldenEye:



The GoldenEye Ransomware is an improved version of the Petya Ransomware, which surfaced in March 2016. It surfaced openly in December 2016. It encrypts local drives using an AES-256 cipher and adds a random 8-characters extension to the file names. However, it avoids directories that contain system data (Windows, Program Data, Program Files, Program Files (x86), Volume Information). If GoldenEye manages to elevate its system privileges, it installs a rootkit which locks the access to the computer entirely by encrypting the drive's MFT disguising its progress as a fake check disk scan. Then the custom boot screen is loaded on the screen. The ransom fee to undo the encryption is about 1.4 Bitcoins (\$1000).

7 Test scenarios

7.1 Typical scenarios

To represent a detailed, relevant assessment about the competing products we focused our attention on the following runtime ransomware attack scenarios. The analyzed scenarios represent typical use cases, where end users need protection for their data in case of a ransomware infection and to determine whether only the backup archive is protected or the whole system before the malware encryption locks the files.

1. Local backup file protection against ransomware

This test is the main focus of our report. There are many different cases what can happen when a ransomware attacks a computer.

- i) The best case scenario for the user is if the backup solution stops the attack, and there is no need to recover the files.
- ii) The next scenario is when the files on the computer are encrypted by the ransomware, but the backup files are intact, and all the files can be recovered to the latest version. This can happen when the backup solution has continuous backup feature, and the backup files are protected by the backup solution, or the backup files are stored offline. Although this extra work from the client side, but still, the files can be recovered.
- iii) The next scenario is when files are encrypted on the computer, but the backup files are still intact. No continuous backup feature is provided by vendor. In this case, the files can be recovered to the last version, which is sometimes daily, sometimes weekly, sometimes monthly backup. This scenario can be still acceptable for users, but this might cause a lot of extra work to reproduce all the recent files which were not in the backup. This scenario can happen when the product protects the backup files, or the user uses offline backups.
- iv) Worst case scenario is when both the files and backup files are encrypted by the ransomware. There is a chance that some files can be still found in a cloud backup, but in practice only a small percentage of files are backed up to cloud, and restoring data from cloud is slow. Restoring 1 Tbyte of data can take days or even weeks to download from a cloud. This scenario can also happen in the case of ransomware like Petya, which makes the whole system unusable – and not just the files, but the whole system has to be recovered.

Having offline backups is easy to say, but when it comes to practice in a home environment users have to manually attach and remove external drives whenever they want to make new backups. This solution is tedious, and not preferred by most home users. Thus, home users tend to have online backups, which can be encrypted by the ransomware easily in case the product lacks ransomware protection.

When it comes to protecting the backup files, users might be lucky that either the ransomware is not targeting the backup files (by extension). Or if the backup is on a writeable network share, some ransomware does not check for shared drives, so the backup files will be intact. But both if these means luck, and not deliberate protection.

2. Cloud backup file and scheduled backup protection against ransomware

In order to extend the scope of the analysis, we also considered the following scenario.

A highly sophisticated, specialized piece of ransomware, besides encrypting all user data, attempts to obtain the credentials of the user's cloud backup account, and using the acquired information, to delete all backup from the cloud account. In order to access this information, it attempts to exploit any potential weakness within the backup solution. Focal points of analysis were as follows.

- SSL handling of network connections
- Local storage of cloud credentials
- Manual suspend of backup service processes

In order to simulate a realistic attack, testing efforts have been limited to 4 hours of analyst work on the backup solutions. We applied network traffic analysis, reversing and runtime monitoring to find a weakness, which can be exploited by the hypothetical piece of malware.

3. Performance testing with various circumstances.

The focus was on backup/restore large files, small files, HDD or SSD, cloud backups. We measured the time needed for backup/recovery, and resources consumed.

8 Detailed results

8.1 Backup protection

8.1.1 Local backup file protection against ransomware

In the first scenario we tried to emulate a situation in which the user computer has become infected with various types of ransomware families and we collected data whether or not the backup solution gives protection in such cases. The following table shows which backup solution file was unaffected by which ransomware family.

The reason why some backup files were not encrypted in all but the Acronis backup solution is not because the backup software protected the files, but because the ransomware was not targeting the backup files.

The number one best practice to protect against ransomware is to have backups. What most home users forget that ransomware can encrypt the backup files if these files are not offline, read-only or in the cloud. With the current home backup solutions, it is not easy to have either an offline or a read-only backup. Our view about the cloud backups can be found in chapter 8.1.2.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Cerber	✓	✓	✓	✓	✓	✓	✓	✓
Troldesh	✓	✓	✓	✗	✗	✓	✓	✓
Dharma	✓	✗	✗	✗	✗	✗	✗	✗
Locky	✓	✓	✓	✗	✗	✓	✓	✓
Havoc	✓	✗	✗	✗	✓	✗	✗	✗
Globe	✓	✓	✓	✗	✗	✓	✓	✓
CryptoMix	✓	✗	✓	✗	✓	✓	✓	✗
Sage	✓	✗	✓	✓	✓	✓	✓	✓
CryptoShield	✓	✓	✓	✓	✓	✓	✓	✓
GoldenEye	✓	✗	✗	✗	✗	✗	✗	✗

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Protecting files against ransomware	✓	✗	✗	✗	✗	✗	✗	✗
Protecting backup files against ransomware	✓	✗	✗	✗	✗	✗	✗	✗
Continuous backup feature	✓	✓	✓	✓	✓	✗	✓	✗
Cloud backup and local backup service protected	✓	✗	✗	✗	✗	✗	✗	✗

8.1.2 Cloud backup file and scheduled backup protection against ransomware

In these tests, we tested whether malware can extract cloud credentials from the backup solution, or malware can disable the backup process. In these tests, due to time limits, we only simulated attackers with 4 hours of resources. It is possible that the products where we did not find any issues are vulnerable, but we did not find it due to the time limits on the test.

Some of the issues listed here are security related, thus we notified the responsible vendors about the detailed issue. Due to responsible disclosure, we can't detail these here.

In general, our opinion is that cloud backups cannot be used to protect full systems, only some highly important files and folders, because uploading and downloading hundreds of Gigabytes to and from the cloud takes way too much time.

8.1.2.1 Acronis True Image

No vulnerability found.

8.1.2.2 IDrive v6.5.1.23

8.1.2.2.1 Insufficient protection of backup services

Testing revealed that the id_service.exe background service is not protected sufficiently against termination and suspend attempts. As a result, a piece of malware can carry out the following actions, resulting in backup disruption.

1. Manual kill of the service and repeatedly kill it whenever restarted.
2. Suspend of the service, which results in service disruption.

The attack can be carried out with administrative user privileges.

8.1.2.2.2 [Insecure handling of user cloud credentials](#)

Testing revealed that a piece of malware can access cloud account credentials using monitoring tools.

The attack can be carried out with administrative user privileges.

8.1.2.2.3 [No certificate pinning implemented](#)

Testing revealed that the IDrive application ecosystem adheres to the central Windows proxy settings. Furthermore, the windows CA store is trusted while making SSL connections. Thus, it is possible for a piece of malware to perform a Man-in-the-Middle attack against the network data flow and to obtain the cloud credentials.

The attack can be carried out with normal user privileges.

8.1.2.3 [Genie TimeLine Home / Zoolz Archive v.2.2.4.300](#)

8.1.2.3.1 [Hard coded encryption keys](#)

The application stores user account data and credential information in an encrypted format, therefore credential information cannot be directly read from the file system. However, a binary analysis revealed that the encryption key is static and wired in at compilation time. As a result, a piece of malware can decrypt the affected data. The attack can be carried out with normal user privileges.

8.1.2.4 [Paragon v.x64_10.1.28.224_000](#)

Paragon relies on 3rd party applications, which map the cloud drive to a standard Windows drive. As a result, the application itself does not implement cloud connectivity.

8.1.2.5 [CrashPlan v.4.8.0](#)

8.1.2.5.1 [Insufficient protection of backup service](#)

Testing revealed that the CrashPlanService.exe background service is not protected sufficiently against termination and suspend attempts. As a result, a piece of malware can carry out the following actions, resulting in backup disruption.

1. Manual kill of the CrashPlanService.exe and repeated kill whenever it is respawned.
2. Suspend of the service, which results in service disruption.

The attack can be carried out with administrative user privileges.

8.1.2.6 [EaseUS Todo Backup v10.0](#)

8.1.2.6.1 [Insufficient protection of backup service](#)

Testing revealed that the background services (Agent.exe, TodoBackupService.exe) are not protected sufficiently against termination and suspend attempts. As a result, a piece of malware can carry out a suspend attack, resulting in backup disruption.

The attack can be carried out with administrative user privileges.

8.1.2.6.2 Insecure token delivery channel

Testing revealed that the OAuth2 authentication flow with the live drive servers results in a couple of tokens, which are later used for API usage. It was observed that the final redirection takes place over plain text HTTP, which allows a piece of malware, acting as an invisible proxy to sniff the credentials, -even without installing a rouge certificate authority on the Windows instance.

The attack can be carried out with normal user privileges.

8.1.2.7 Macrium Reflect Home v6.3.1655

The Macrium does not support cloud backup storage.

8.1.2.8 Nova Backup 18.5build926

8.1.2.8.1 Insufficient protection of backup service

Testing revealed that the nsctrl.exe and nsService.exe background services are not protected sufficiently against termination and suspend attempts. As a result, a piece of malware can suspend the service, which results in service disruption.

The attack can be carried out with administrative user privileges.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Secure storage of cloud credentials	✓	✓	✓	✗	✗	N/A	✓	N/A
Sufficient protection of background services	✓	✗	✗	✓	✗	N/A	✗	N/A
Secure certificate check	✓	✓	✗	✓	✗	N/A	✓	N/A

8.2 Feature comparison chart

The following chart shows a feature comparison between the different data protection solutions. For a detailed feature comparison, refer to paragraph 9.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
File and Folder backup	✓	✓	✓	✓	✓	✓	✓	✓
Full Disk backup	✓	✗	✓	✓	✓	✓	✓	✓
System backup	✓	✗	✓	✓	✓	✓	✓	✓
Incremental backup	✓	✓	✓	✓	✓	✓	✓	✓
Differential backup	✓	✓	✓	✗	✗	✓	✓	✓
Scheduled backup	✓	✓	✓	✓	✓	✓	✓	✓
Continuous backup	✓	✓	✓	✓	✓	✗	✓	✗
Rescue Media builder	✓	✗	✓	✓	⚠	✓	✓	✓
MBR/GPT repair	✓	✗	✓	✓	⚠	✓	✓	✓
Cloud integration	✓	✓	⚠	⚠	✓	✗	✓	⚠
Network drive integration	✓	✗	✓	✓	✓	✓	✓	✓
Backup compression	✓	✓	✓	✓	✓	✓	✓	✓
Backup encryption	✓	✓	✓	✗	✓	✓	✓	✓
Email notification	✓	✓	✓	✓	✓	✓	✓	✗
Easily accessible logs	✗	✓	✓	✓*	✓	✓	✓	✓

✓ feature is available

✗ feature is not available

⚠ 3rd party application is required

* only restore logs are available

8.3 Performance

To summarize all the 24 separate tests, we conducted to find out how each solution perform in different realistic scenarios, we differentiated 4 categories. These categories are: the **Best**, **Good**, **Average** and the **Worst** application.

Acronis True Image earned the **Best** title as it finished first in 18 cases of 24 test and when it didn't win it finished second. Acronis did the fastest backup on HDD and on SSD as well and the connection speed to its own cloud was way faster than any other competitor's. Acronis only came in the second place in 6 out of 12 restore operations which didn't involve cloud operations.

EaseUS TODO Backup Home, **Genie Timeline Home** and **NovaBACKUP** received **Good** title because they all have good performance when the backup/restore speed is questioned both in local and cloud operations. However, EaseUS & Genie requires a third party tool to complete cloud backup. As the median of the competition time through difference performance scenarios we tested placed all three of them in the upper medium part of the standing table, we consider them as good backup solution options.

IDrive, **Macrium Reflect Home** and **Paragon Backup and Recovery** got **Average** title because in most test scenarios they produced a good to average performance but they lack of some functionality which are essential to be considered as a good backup product.

From the view of performance, the **Worst** acting attendant was **CrashPlan** since the performance factors it could produce during local HDD operations were barely average and Crashplan misses the option to perform complete disk actions so it had to be left out during all the disk backup situations.

The standing tables are below and the detailed results can be found in the appendix for further analysis.

The following table represents the end result of the large files performance test executed on HDD.

The sequence is shown from the fastest to the slowest. Detailed results can be found in the Appendix.

HDD operations with large files

Position	HDD to HDD Backup (50 x 1GB)
1	Acronis
2	EaseUS
3	Nova
4	Paragon
5	Genie
6	Macrium
7	IDrive
8	CrashPlan

Position	HDD to Cloud Backup (5 x 1GB)
1	Acronis
2	Genie
3	IDrive
4	EaseUS
5	Nova
6	CrashPlan
n/a	Macrium
n/a	Paragon

Position	HDD to HDD Restore (50 x 1GB)
1	Nova
2	Acronis
3	EaseUS
4	Paragon
5	CrashPlan
6	IDrive
7	Macrium
8	Genie

Position	Cloud to HDD Restore (5 x 1GB)
1	Acronis
2	Genie
3	IDrive
4	EaseUS
5	CrashPlan
6	Nova
n/a	Paragon
n/a	Macrium

Position	HDD to HDD Incremental Backup (5 x 1GB)
1	Acronis
2	Nova
3	EaseUS
4	Macrium
5	Paragon
6	IDrive
7	CrashPlan
8	Genie

Position	HDD to Cloud Incremental Backup (1 x 512MB)
1	Acronis
2	Genie
3	EaseUS
4	Nova
5	IDrive
6	CrashPlan
n/a	Macrium
n/a	Paragon

Position	HDD to HDD Incremental Restore (5 x 1GB)
1	Nova
2	Acronis
3	Genie
4	EaseUS
5	IDrive
6	Macrium
7	Paragon
8	CrashPlan

Position	Cloud to HDD Incremental Restore (1 x 512MB)
1	Acronis
2	Genie
3	EaseUS
4	CrashPlan
5	IDrive
6	Nova
n/a	Macrium
n/a	Paragon

The following table represents the end result of the small files performance test executed on HDD.

The sequence is shown from the fastest to the slowest. Detailed results can be found in the Appendix.

HDD operations with small files			
Position	HDD to HDD Backup (102.4K x 512KB)	Position	HDD to Cloud Backup (10.24K x 512KB)
1	Acronis	1	Acronis
2	Paragon	2	Genie
3	EaseUS	3	IDrive
4	Macrium	4	EaseUS
5	CrashPlan	5	Nova
6	Nova	6	CrashPlan
7	IDrive	n/a	Macrium
8	Genie	n/a	Paragon
Position	HDD to HDD Restore (102.4K x 512KB)	Position	Cloud to HDD Restore (10.24K x 512KB)
1	EaseUS	1	Acronis
2	Acronis	2	Genie
3	CrashPlan	3	IDrive
4	Nova	4	EaseUS
5	Paragon	5	CrashPlan
6	IDrive	6	Nova
7	Macrium	n/a	Macrium
8	Genie	n/a	Paragon
Position	HDD to HDD Incremental Backup (10.24K x 512KB)	Position	HDD to Cloud Incremental Backup (1024 x 512KB)
1	Acronis	1	Acronis
2	Nova	2	Genie
3	CrashPlan	3	IDrive
4	Paragon	4	EaseUS
5	EaseUS	5	CrashPlan
6	IDrive	6	Nova
7	Macrium	n/a	Macrium
8	Genie	n/a	Paragon
Position	HDD to HDD Incremental Restore (10.24K x 512KB)	Position	Cloud to HDD Incremental Restore (1024 x 512KB)
1	EaseUS	1	Acronis
2	Acronis	2	Genie
3	Genie	3	IDrive
4	Macrium	4	CrashPlan
5	CrashPlan	5	EaseUS
6	Nova	6	Nova
7	Paragon	n/a	Macrium
8	IDrive	n/a	Paragon

The following table represents the end result of the performance test executed on SSD.

The sequence is shown from the fastest to the slowest. Detailed results can be found in the Appendix.

SSD operations			
Position	SSD to SSD Backup (50 x 1GB)	Position	SSD to SSD Backup (102.4K x 512KB)
1	Acronis	1	Acronis
2	Macrium	2	EaseUS
3	Genie	3	Macrium
4	Paragon	4	Paragon
5	Nova	5	Nova
6	EaseUS	6	IDrive
7	IDrive	7	Genie
n/a	CrashPlan	n/a	CrashPlan
Position	SSD to SSD Restore (50 x 1GB)	Position	SSD to SSD Restore (102.4K x 512KB)
1	Paragon	1	EaseUS
2	Acronis	2	Acronis
3	Nova	3	Nova
4	EaseUS	4	Paragon
5	Macrium	5	IDrive
6	IDrive	6	Macrium
7	Genie	7	Genie
n/a	CrashPlan	n/a	CrashPlan
Position	SSD to SSD Incremental Backup (5 x 1GB)	Position	SSD to SSD Incremental Backup (10.24K x 512KB)
1	Acronis	1	Acronis
2	Macrium	2	Macrium
3	Genie	3	EaseUS
4	EaseUS	4	Genie
5	Nova	5	Nova
n/a	CrashPlan	n/a	CrashPlan
n/a	IDrive	n/a	IDrive
n/a	Paragon	n/a	Paragon
Position	SSD to SSD Incremental Restore (5 x 1GB)	Position	SSD to SSD Incremental Restore (10.24K x 512KB)
1	Acronis	1	Acronis
2	EaseUS	2	Genie
3	Macrium	3	Macrium
4	Genie	4	Paragon
5	Paragon	5	EaseUS
n/a	CrashPlan	n/a	CrashPlan
n/a	IDrive	n/a	IDrive
n/a	Nova	n/a	Nova

All performance test was executed three times, and an average is represented in the results.

9 Product feature comparison

We checked the implemented features in the data protection solutions, and compared these features against each other.

9.1 Acronis True Image 2017 New Generation

Acronis True Image 2017 NG provides simple ways to back up the entire PC, specific disk, partitions, or individual files and folders, which can be protected with 256-bit AES encryption. Backups can be saved locally or to the Acronis cloud. With enhanced NAS support Acronis can detect your storage device automatically and continues without errors even when Windows assigns a different drive letter to the backup device. The integrated Sync feature ensures key files are always available on any device.

Acronis True Image 2017 NG adds tools to wirelessly back up iOS and Android devices to your desktop (with the Acronis app on the remote device). It even has the capability to backup Facebook account content, including photos, videos, contacts, comments, and likes.

One of the most important features in the current version is the Acronis Active Protection. It is an advanced, active protection against data loss to ransomware. It protects the backup files upon a ransomware infection and is able to prevent any data loss. This feature makes True Image unique among all backup software.

The built-in search tool helps you find particular files within a backup while the Explorer integration makes the backup files openable in Windows Explorer directly.

Acronis True Image has been an established backup tool for years and now with the added new features—especially the Acronis Active Protection – Acronis surely takes the lead in this contest.

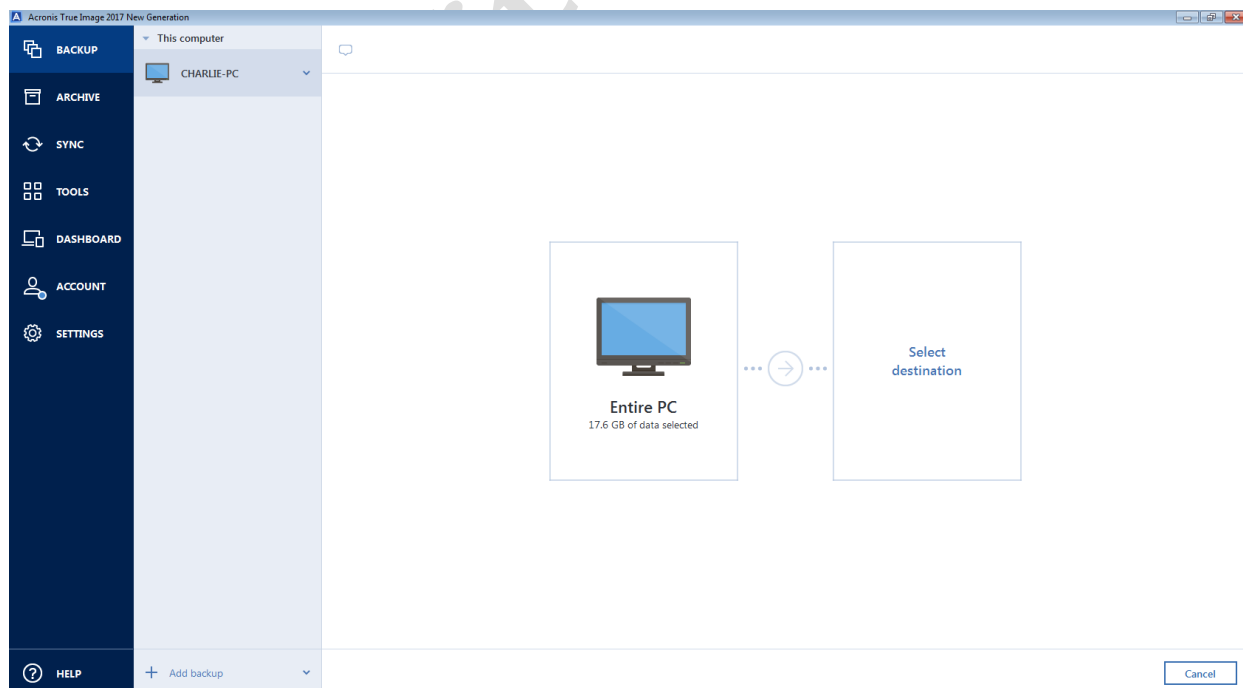


Figure 1 – Home screen

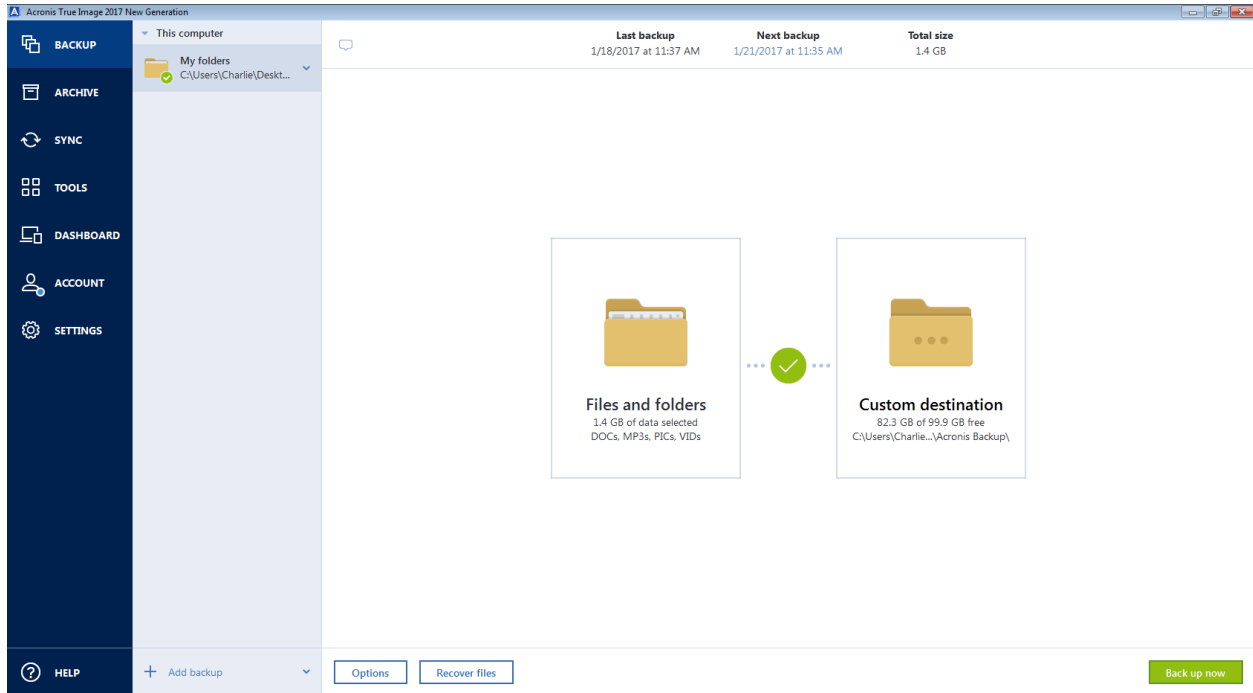


Figure 2 - Backup screen

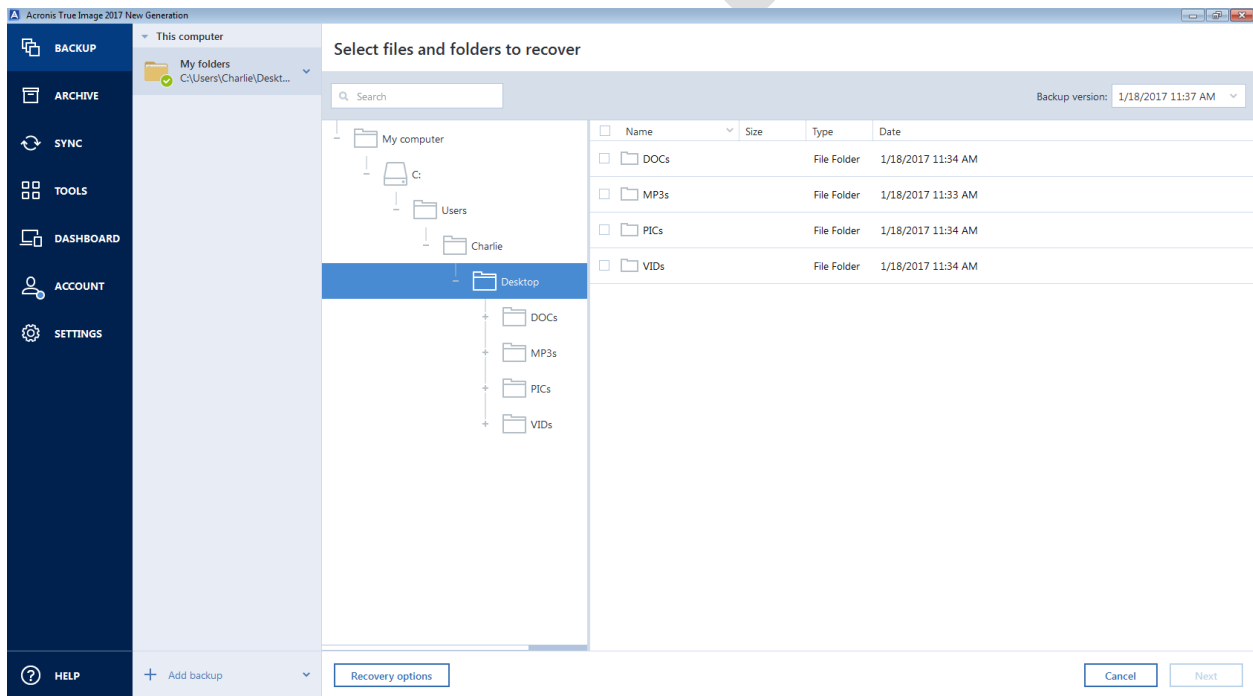


Figure 3 - Restore screen

9.2 CrashPlan

CrashPlan is a free backup tool that requires minimal user configuring once the user specifies a backup destination. It is always running in the background, backing up new or changed files from the User folder if one doesn't want to specify different files and folders.

The program can back up 448-bit Blowfish encryption protected backups to external drives, another computer or CrashPlan Cloud. Unfortunately, network drive support is still missing, but with the Triple Destination Data Storage and Protection feature it is capable of using a friend's PC over the internet as destination, if they also have CrashPlan installed.

With the mobile app the backed up files are always reachable from your mobile devices. The CrashPlan Central cloud keeps the deleted files forever (unless the user deletes them deliberately), so no matter how much time passes after the file is deleted it is still recoverable.

CrashPlan is a free backup tool that has some great features but the lack of full disk & system backup combined with the missing NAS support makes it fall short of winning this competition.

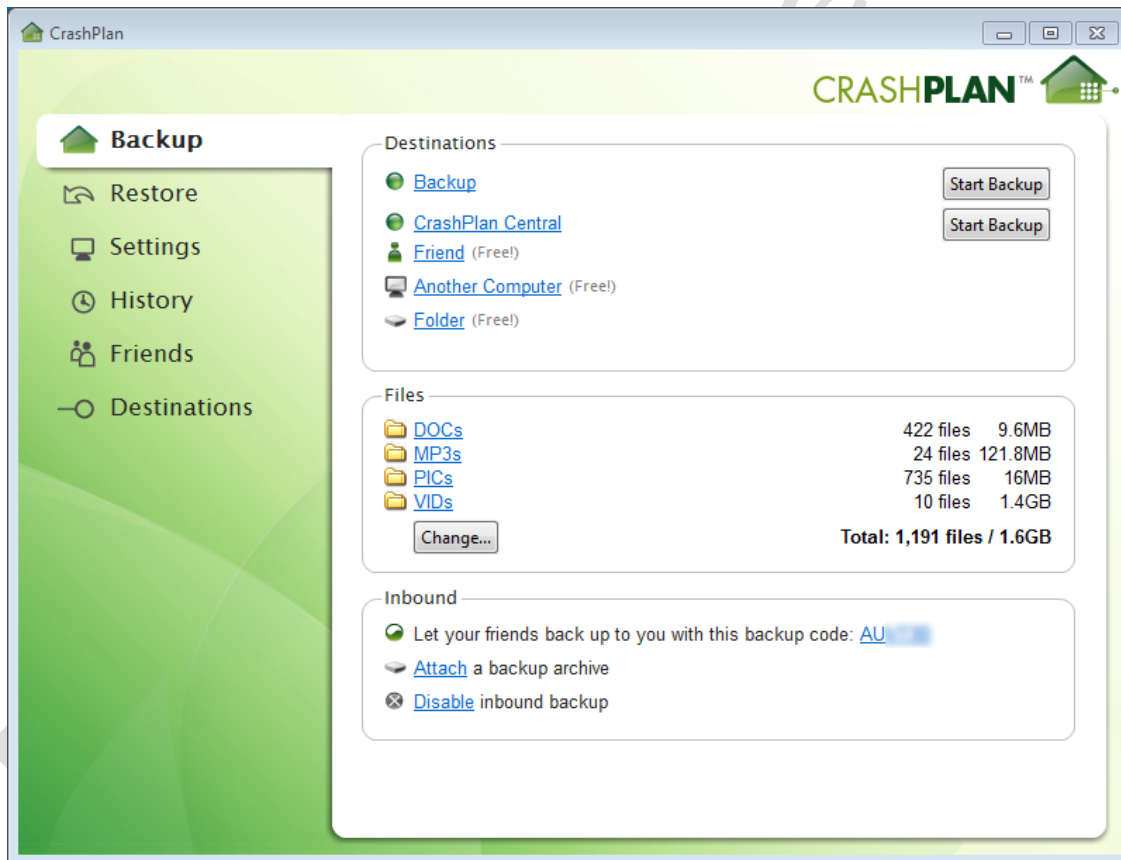


Figure 4 - home screen

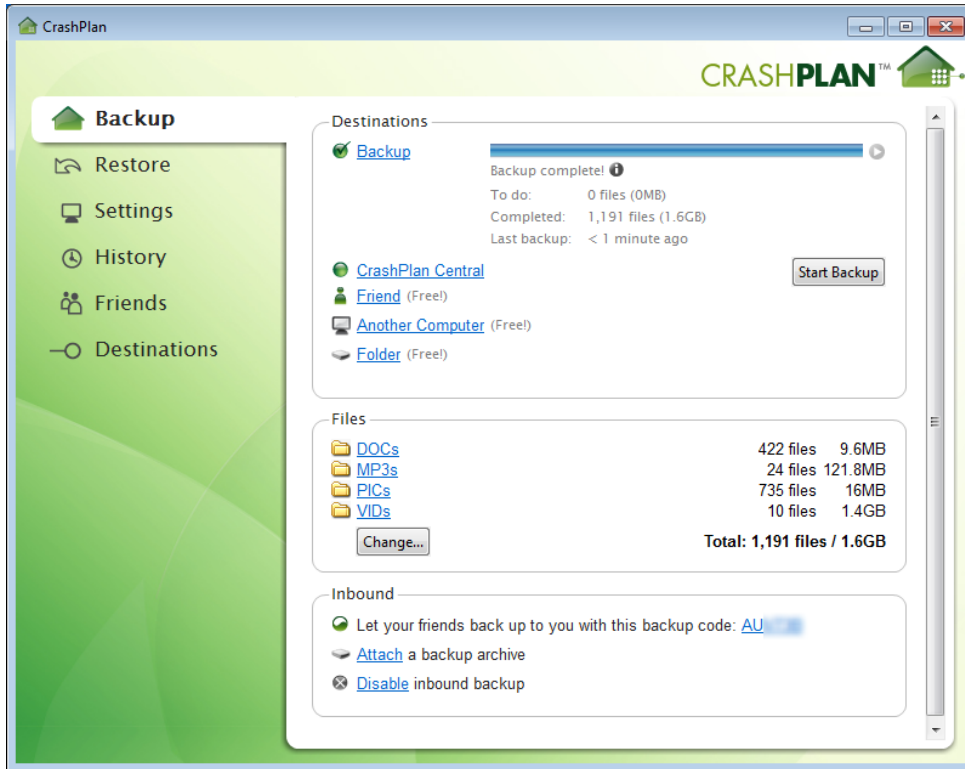


Figure 5 - Backup screen

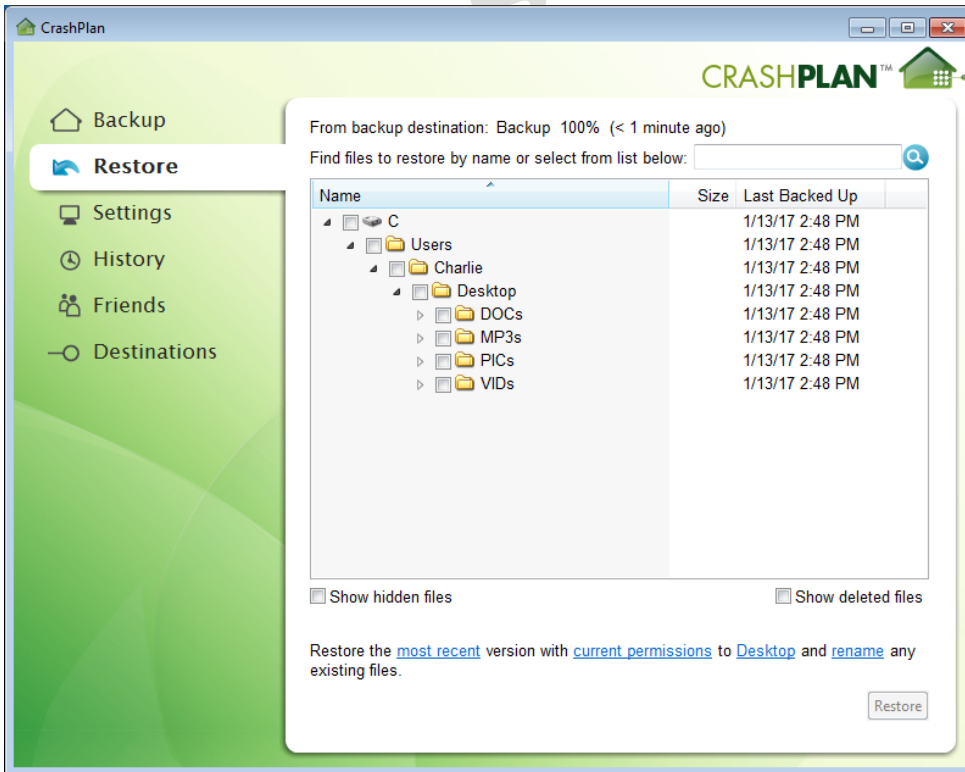


Figure 6 - Restore screen

9.3 EaseUS Todo Backup Home

EaseUS Todo Backup Home is a backup software that supports continuous user file backup or automatically backing up complete disk, the system drive or particular files and folders and even Android devices. It also has the functionality to clone the complete system to another PC.

The restore function in EaseUS Todo Backup offers an easy way to retrieve backed up files by mounting the backup image as a virtual hard drive. But the software offers the possibility to create an Emergency disk that can be beneficial when the system fails to start.

Pre-OS can be an especially useful tool when the operating system fails to boot and there is no bootable disk created, as it is considered as a simple OS environment from which EaseUS Todo Backup can be used and the backup/restore process is accessible. Among tools it also has a convenient “Logs” view which can be advantageous when dealing with multiple backup operations.

This newest release of EaseUS Todo Backup with its features and operational speed is clearly a powerful and capable backup solution which could definitely be at the top of a “Best Backup solution” comparison, not including ransomware protection.

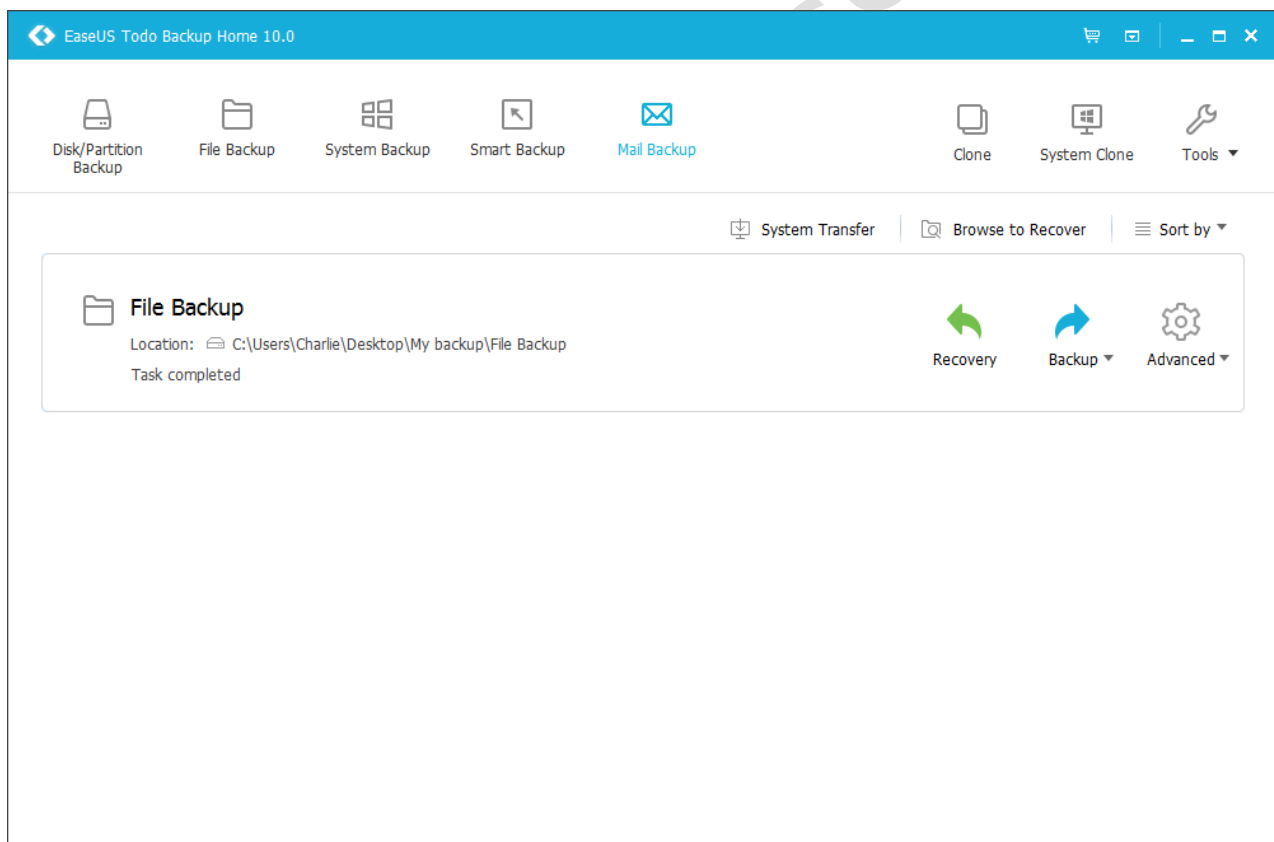


Figure 7 - Home screen

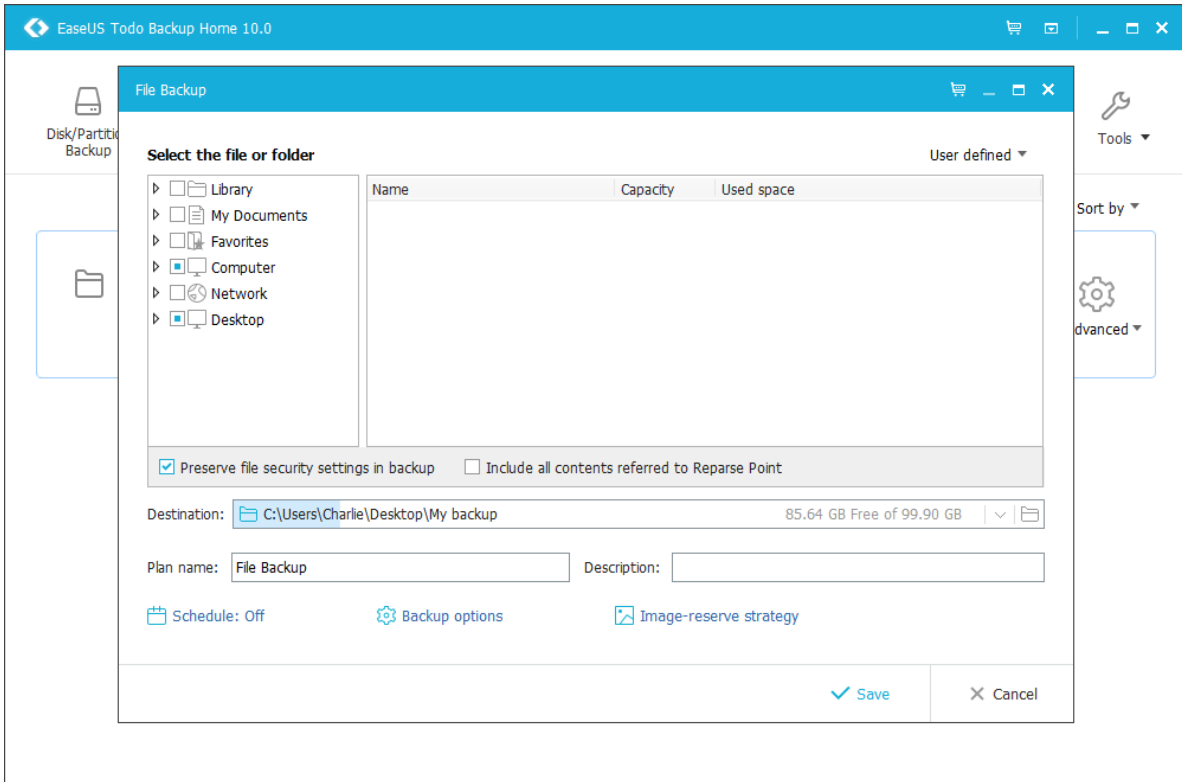


Figure 8 - Backup screen

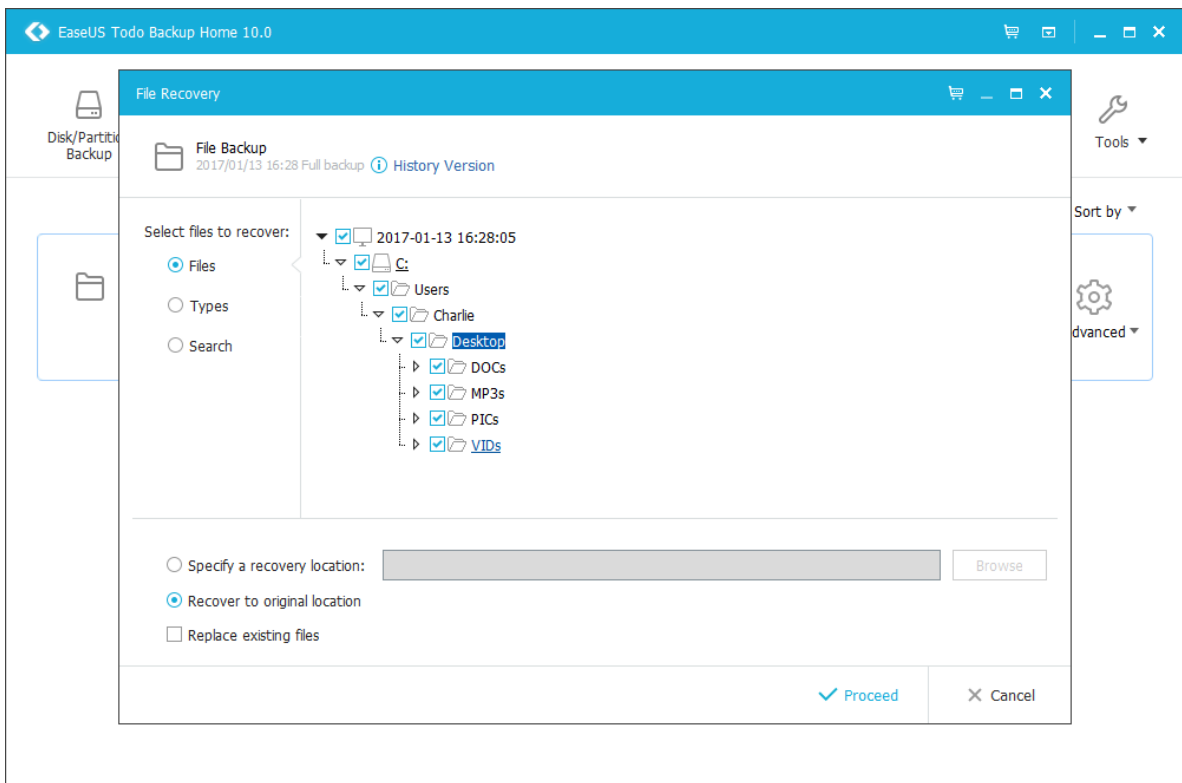


Figure 1 - Restore screen

9.4 Genie Timeline Home 2016

Genie Timeline Home 2016 is an easy-to-use tool. Backup configuration can be done in three steps. It is as easy as choosing a destination drive, and the type of files you'd like to back up (documents, pictures, emails, music, etc.). Optionally particular files and folders are also selectable.

After installation, the software creates a virtual disk entry named 'Timeline Explorer' in File Explorer. It also adds right-click options to Windows File Explorer that let the user add the selected file to the backup and open a timeline viewer showing versions for the selected file. This makes getting to an individual file's previous version easier than Windows' File History feature does.

Genie Timeline Home 2016 also has the option to create a Disaster Recovery backup to use when system failure occurs. Unfortunately, the backups are not encryptable and they cannot be incremental or differential either. The cloud backup option is also missing from the software itself, meaning one needs to install another product from the same company to backup data to the cloud. These missing features, along with the relatively slow backup speed makes Genie Timeline Home 2016 a mid-range backup solution.

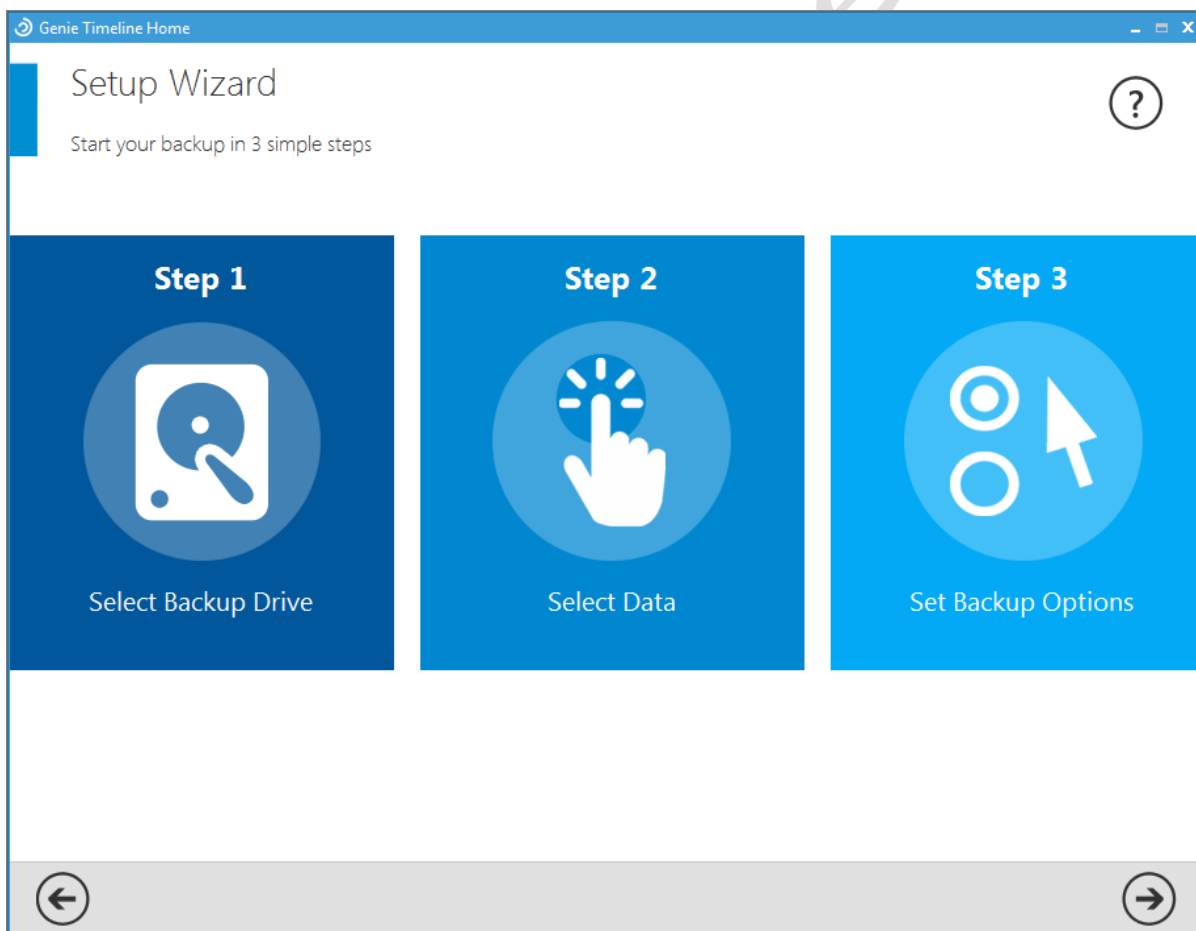


Figure 10 - Home screen

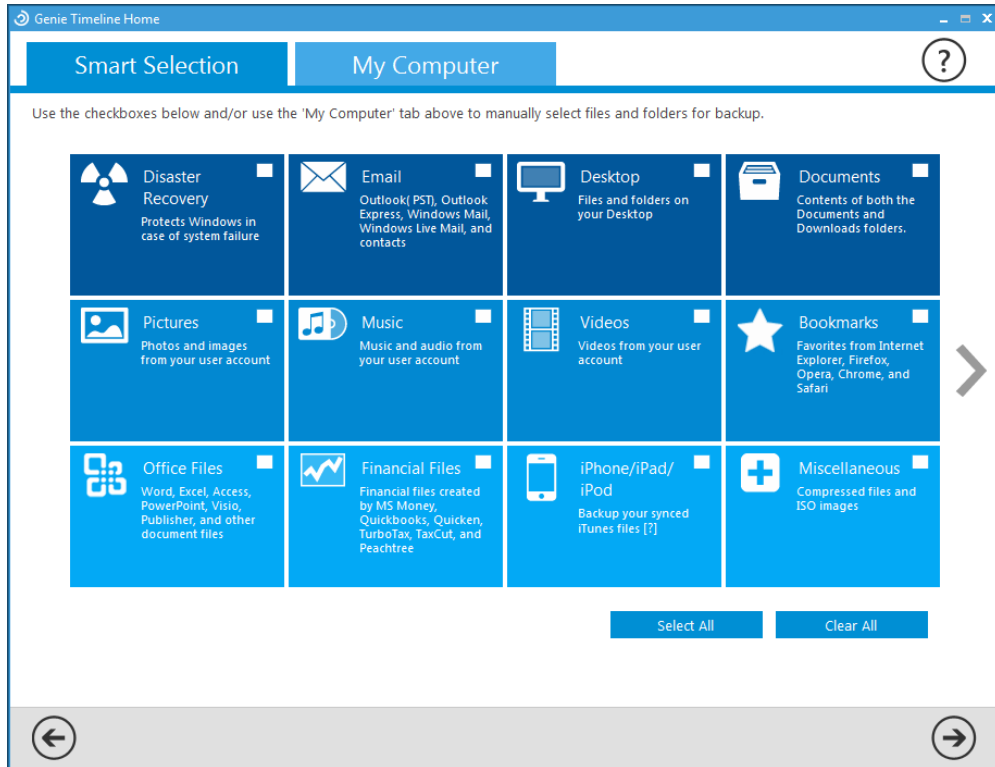


Figure 11 - Backup screen

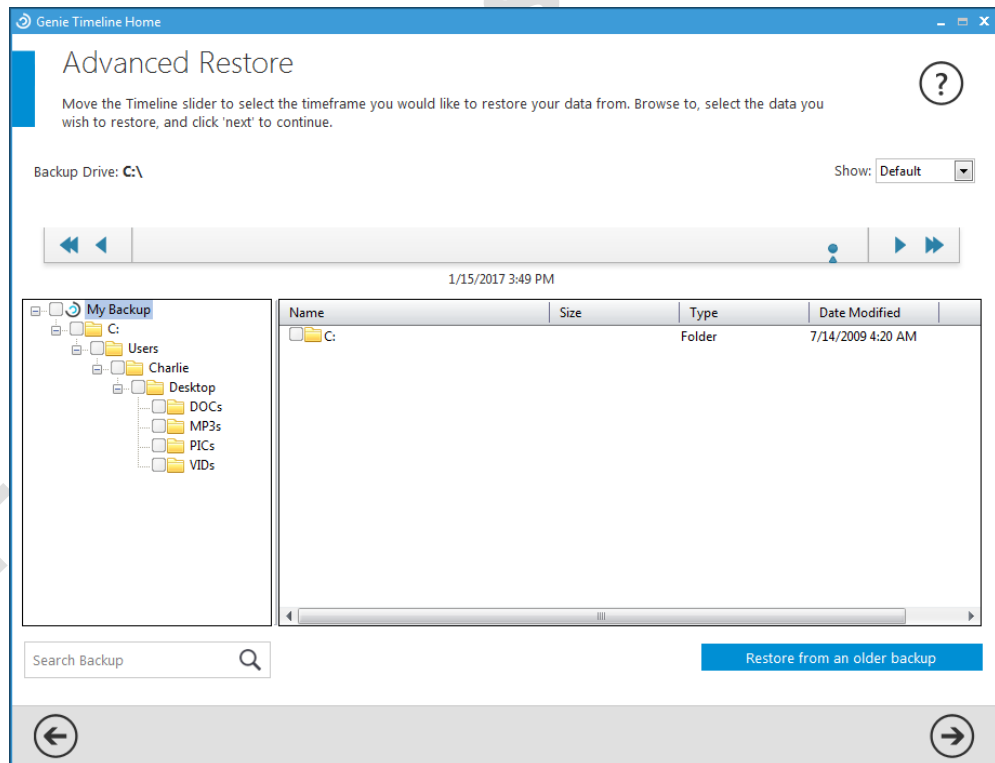


Figure 12 - Restore screen

9.5 IDrive

IDrive is a hybrid cloud data backup service – it's also an online storage service, a file-syncing service, and a file-sharing service. In addition to backing up your devices, IDrive boasts a social media backup too. Connect IDrive with Facebook and Instagram, and it will back up all of your photos and videos on those platforms.

Any file stored in your backup can be shared via a public link or privately over Facebook, Twitter, and email. The user can set passwords and permissions for collaboration, similar to the “Edit” and “View” permissions on Google Docs.

Data transfers are encrypted using SSL between your computer and the destination server. Once that data is on the cloud, it is encrypted using a 256-bit AES standard. The web app includes a similar file explorer for navigating and restoring files. It can be used to restore files on your desktop remotely from another device. The mobile app like the web app, allows you to share files and perform remote restores.

In spite of the missing differential backup option and the requirement for a third-party tool to create an emergency rescue disk, IDrive backup is still a practical choice for many home users.

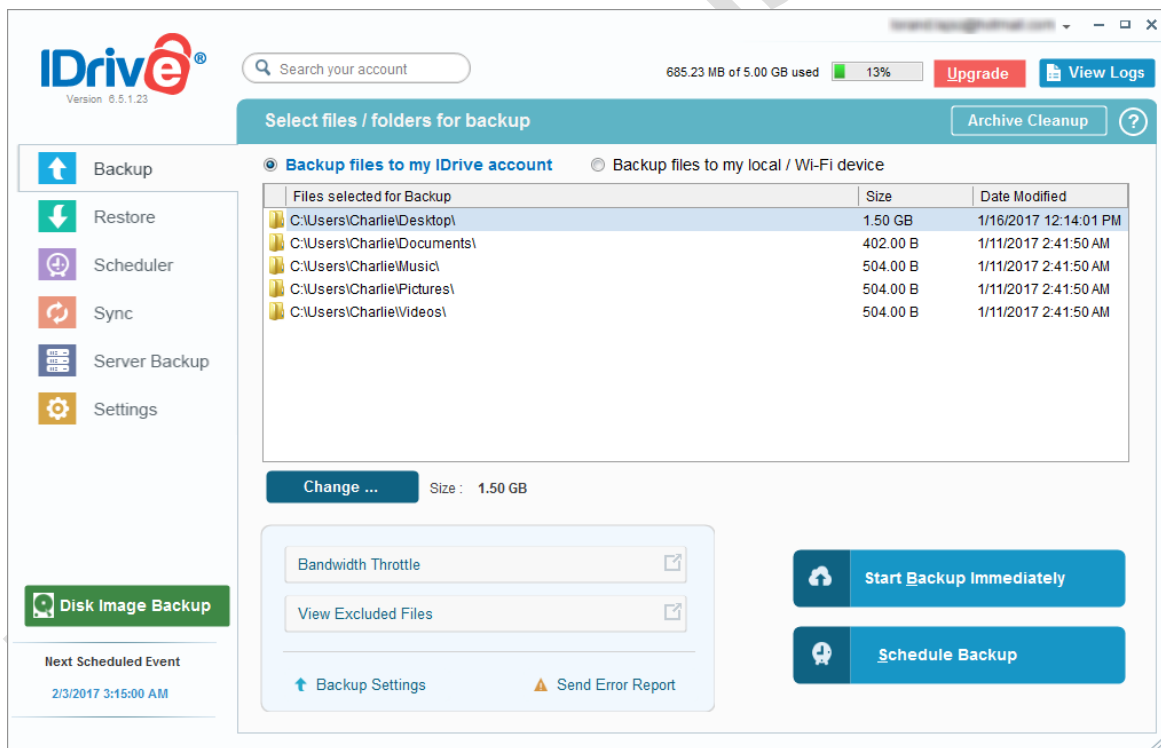


Figure 13 - Home screen

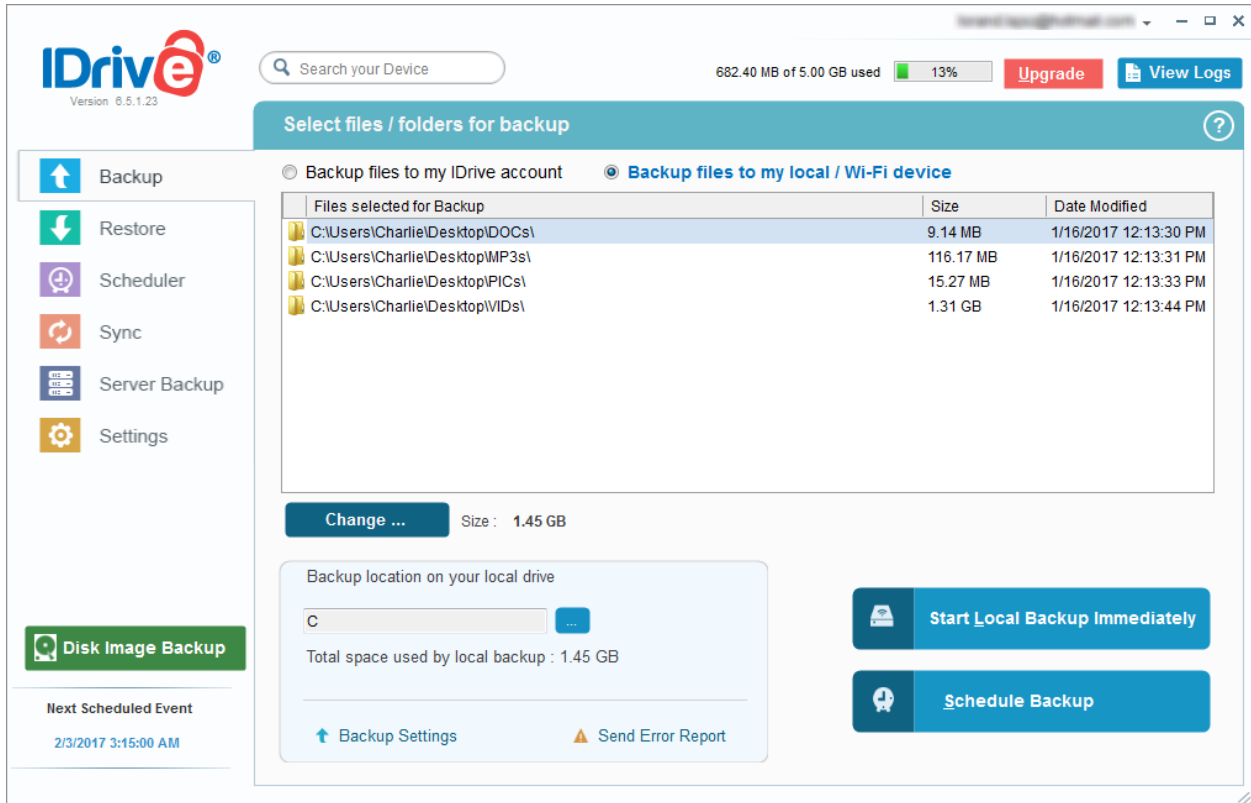


Figure 14 - Backup screen

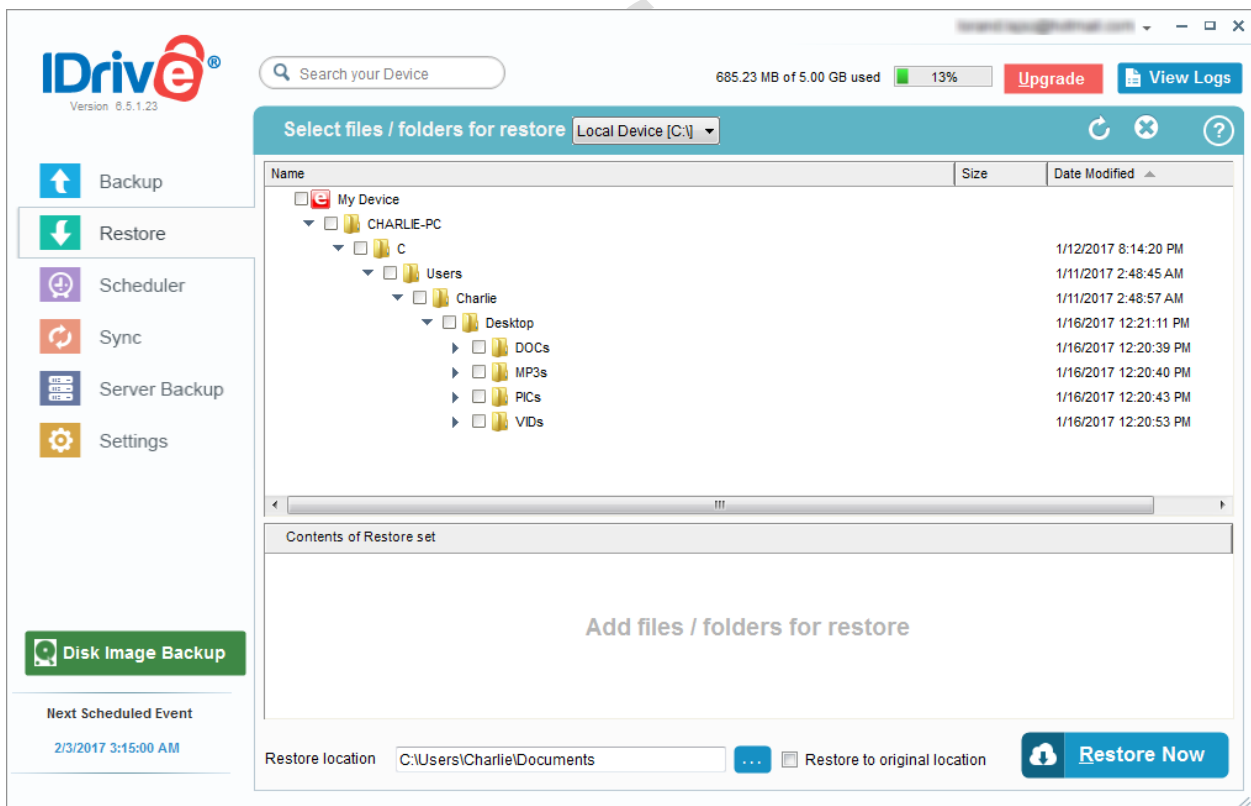


Figure 15- Restore screen

9.6 Macrium Reflect Home

Macrium Reflect Home is a well-designed Disaster recovery software which has the option to perform full, differential and incremental backups, both ad hoc and scheduled - handling any scenarios a home user may face.

It can create bootable media to use if the computer crashes or the system is to be moved to another computer. Backups can be saved as a CD, DVD or Blu-ray disc or an image file on an external hard drive or cloud server. The files can be compressed and protected with AES 256. With so many options, the software makes it easy to have an image copy on hand in case of an emergency, or to deploy multiple machines that have the same setup.

One of the most obviously missing features with this solution is the continuous backup. Users have to create and/or schedule tasks and there is no possibility to have an always-up-to-date version of a file. The other important feature that is missing is a cloud backup option. Macrium Reflect Home does not support cloud backups; neither does it provide any option to use a third-party app as a complementary tool.

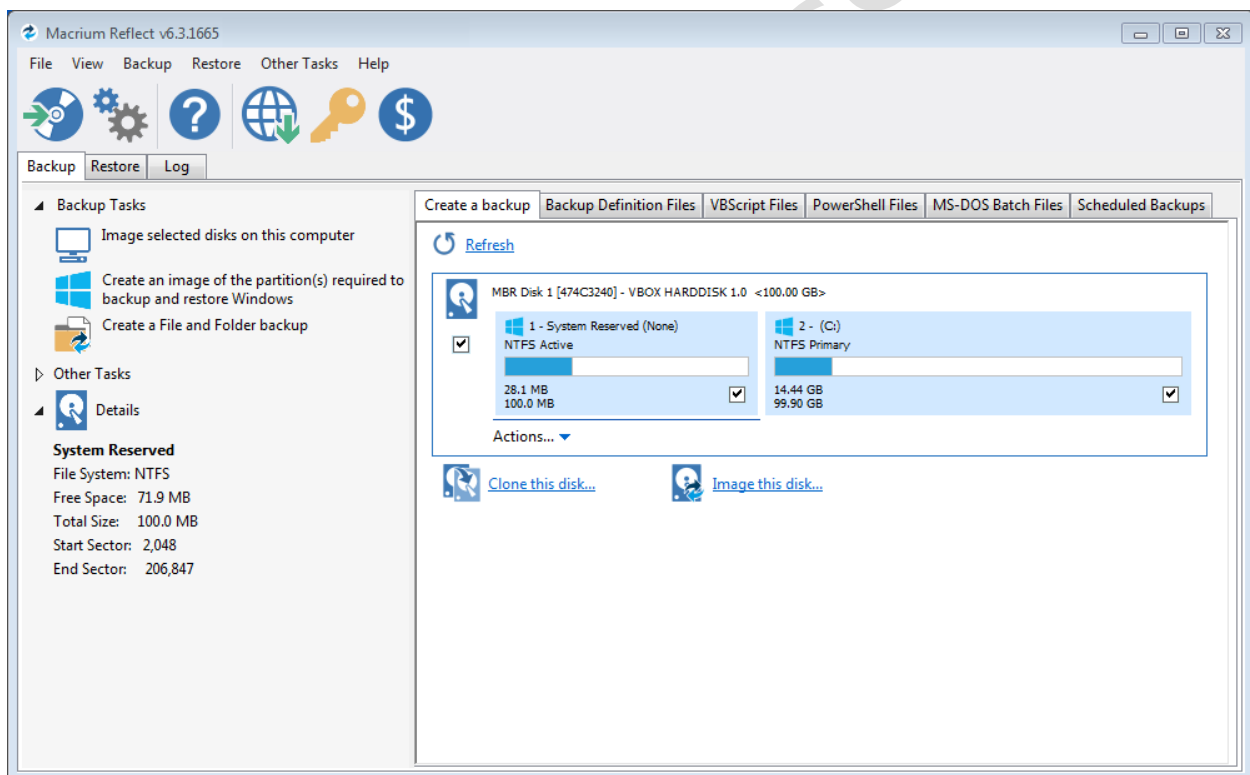


Figure 16 - Home screen

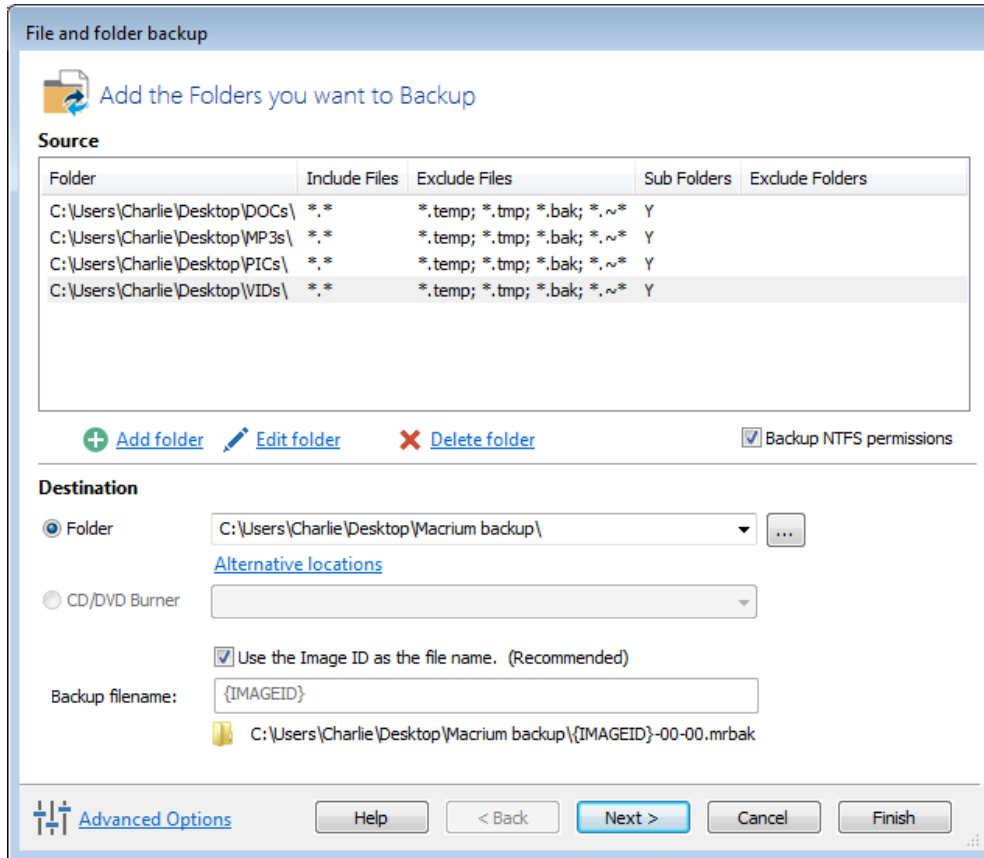


Figure 17 - Backup screen

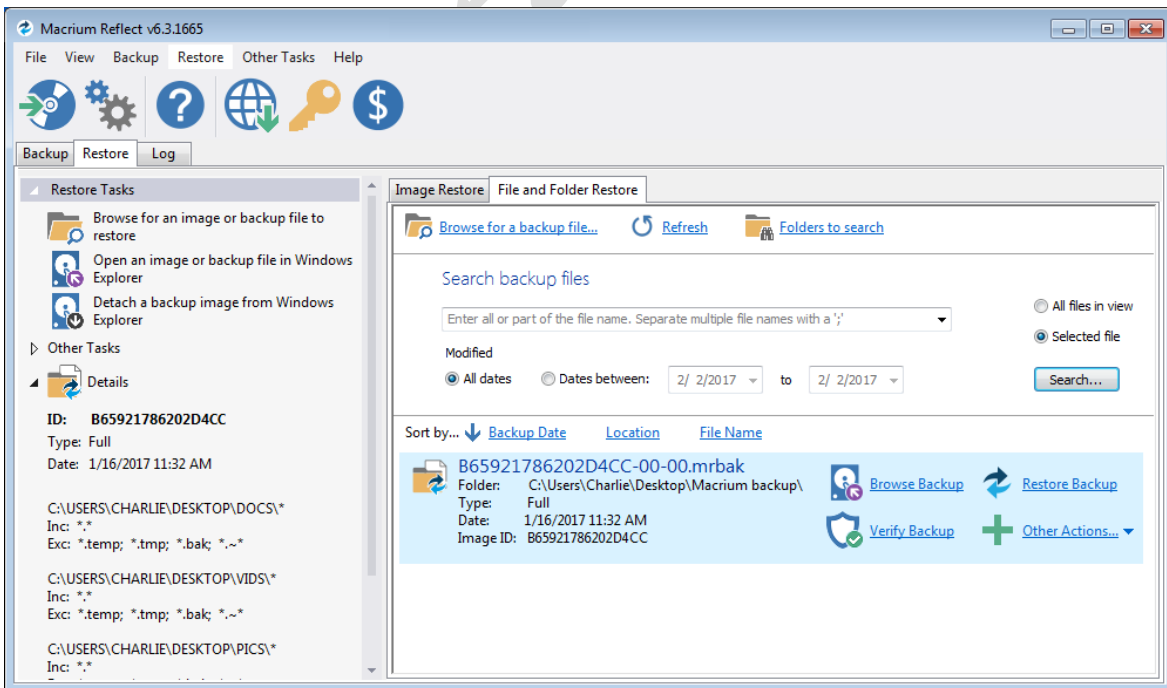


Figure 18 - Restore screen

9.7 NovaBACKUP

NovaBACKUP can do full disk image backups of PCs and laptops, in addition to backing up files and folders. It includes a tool to create boot media to recover data outside of Windows. With NovaBackup users can set various destinations, it can be a local folder, network drive or a cloud provider.

The software offers the means to create a disaster recovery disk as well, to be used with the system backup once the OS fails to start. There are two boot media types: Simple and Advanced. The software states Simple boot media is easier to create, but might require the operating system disc to complete. The Advanced media option creates a Window PE boot disc, which requires downloading additional files.

The combination of the ease of use and speed with the long list of advanced features makes NovaBackup one of the most versatile PC backup solutions available.

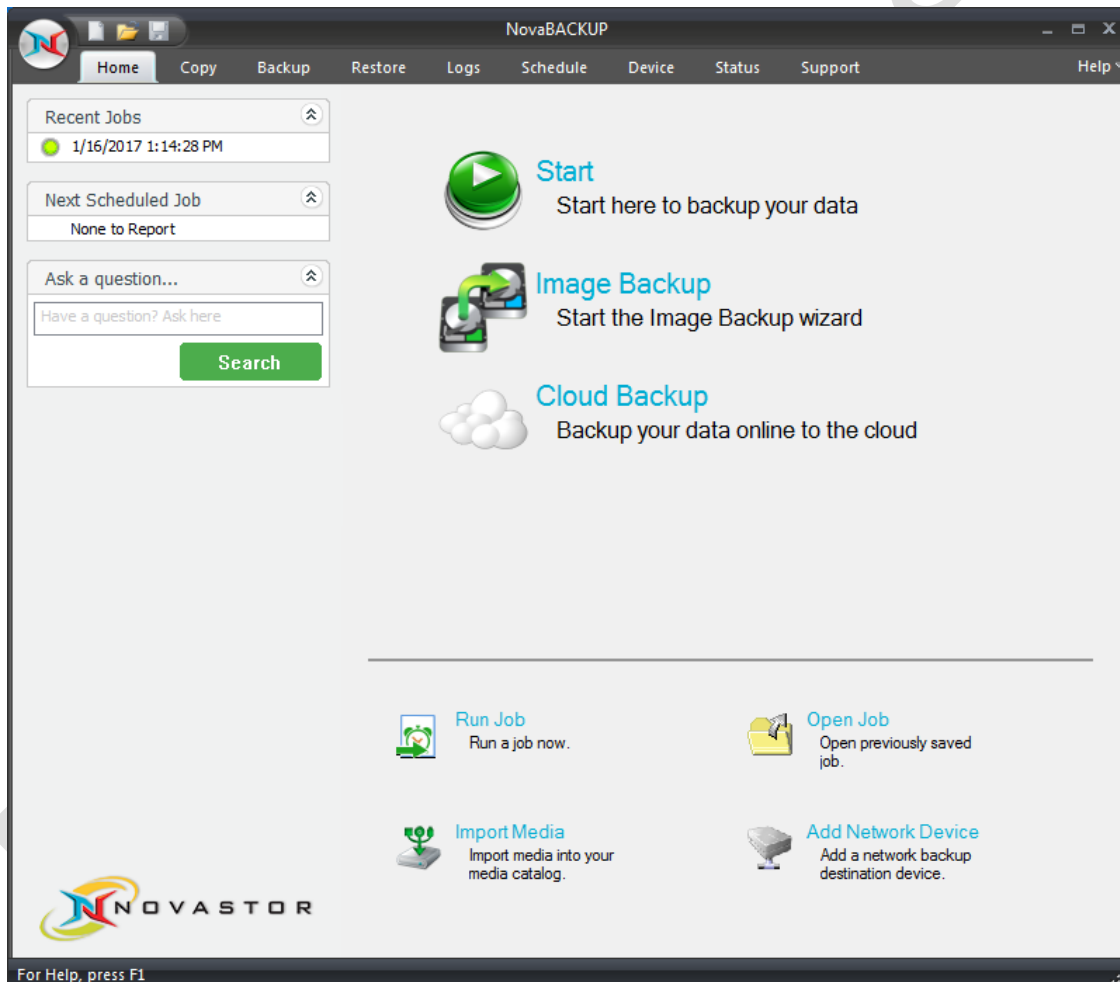


Figure 19 - Home screen

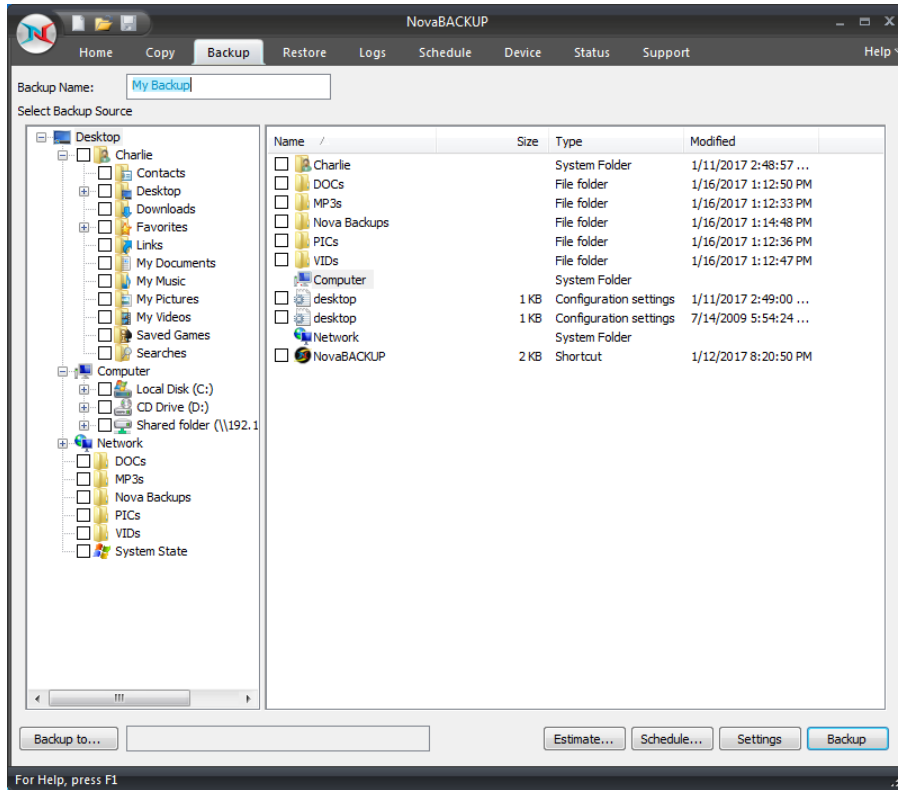


Figure 20 - Backup screen

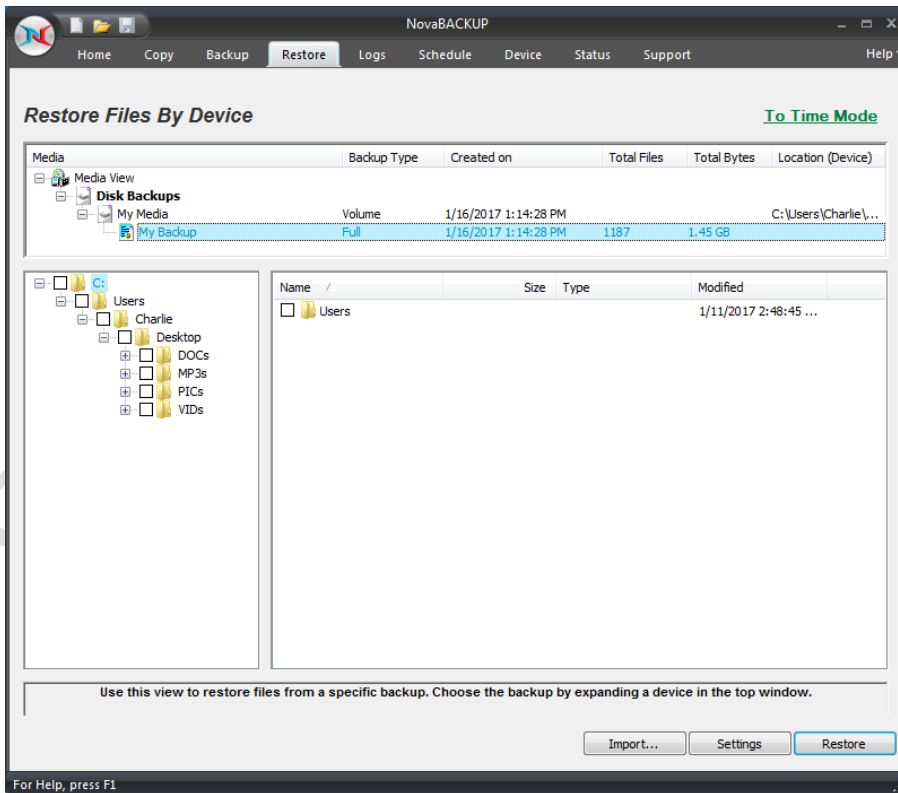


Figure 21 - Restore screen

9.8 Paragon Backup and Recovery 16

Paragon Backup & Recovery 16 is a comprehensive backup tool with a vast array of professional backup and disk management features. For instance, the program can back up a hard drive's master boot record, its first track, individual partitions or complete drives. It can also run file-based backups on the files and any folders you specify.

Encrypted full, differential or incremental backups are available, the latter including only new or modified files for improved performance. A scheduler allows backup jobs to be run when you're not around. And your backup files can be saved to local, external or remote drives, FTP servers, or burned to disc. Virtualisation support allows you to copy your entire system to a virtual drive. However, encryption and password protection are only available with pVHD (paragon virtual hard drive) backup sets.

Unfortunately Paragon Backup and Recovery users will not get an email notification once the backup/restore task has finished and will not be able to access log files as these features are not offered by Paragon.

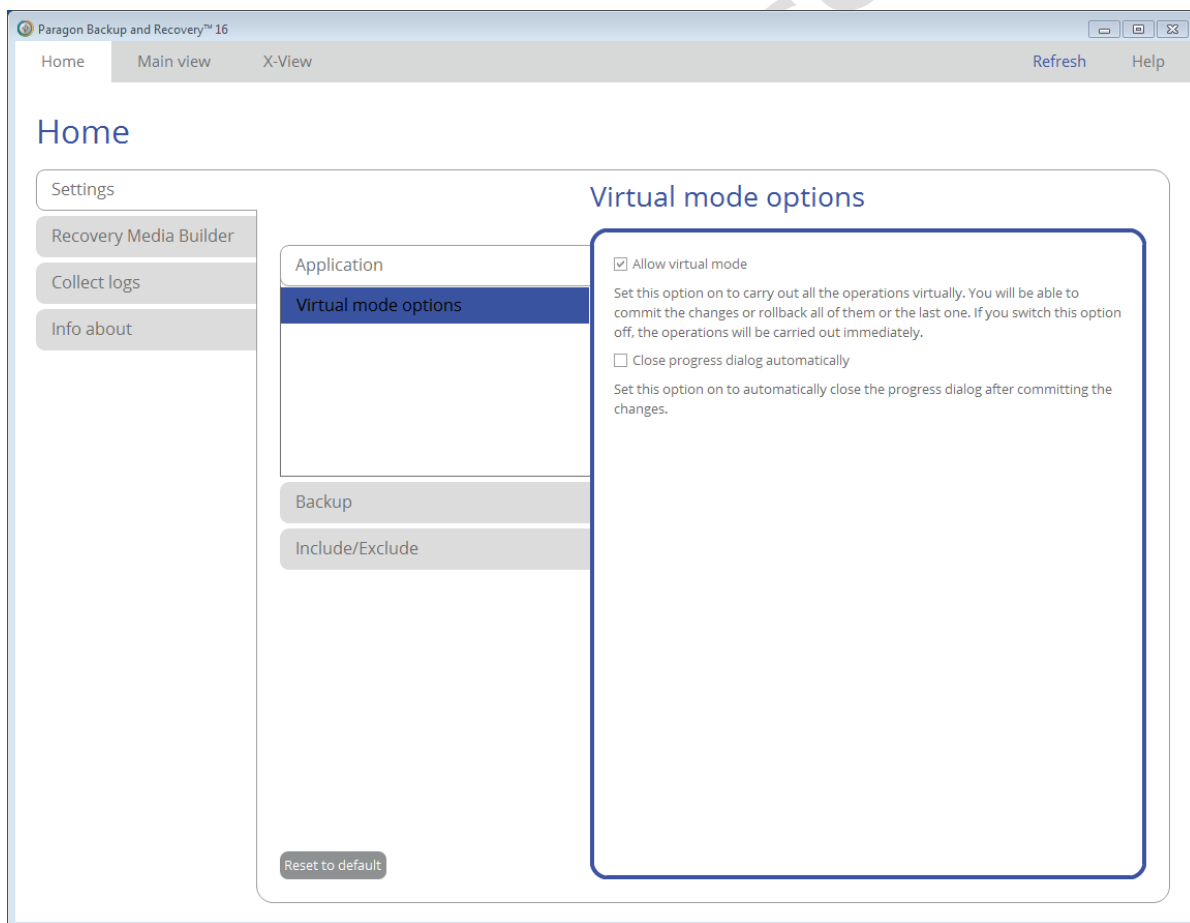


Figure 22 - Backup screen

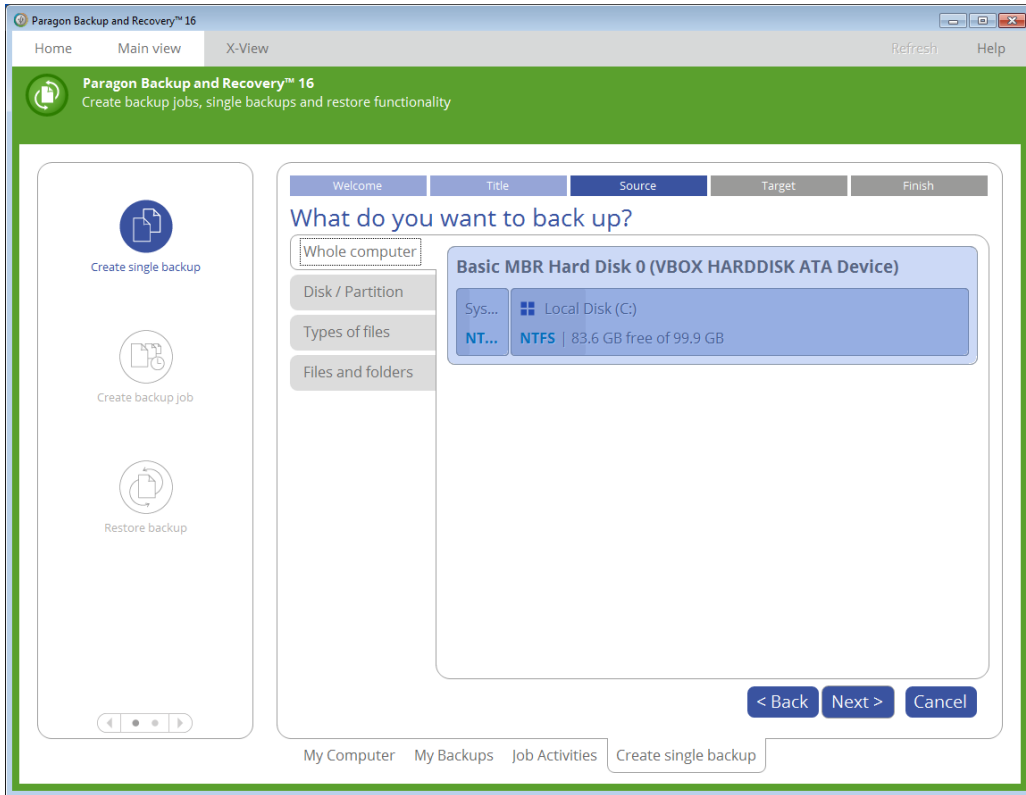


Figure 23 - Backup screen

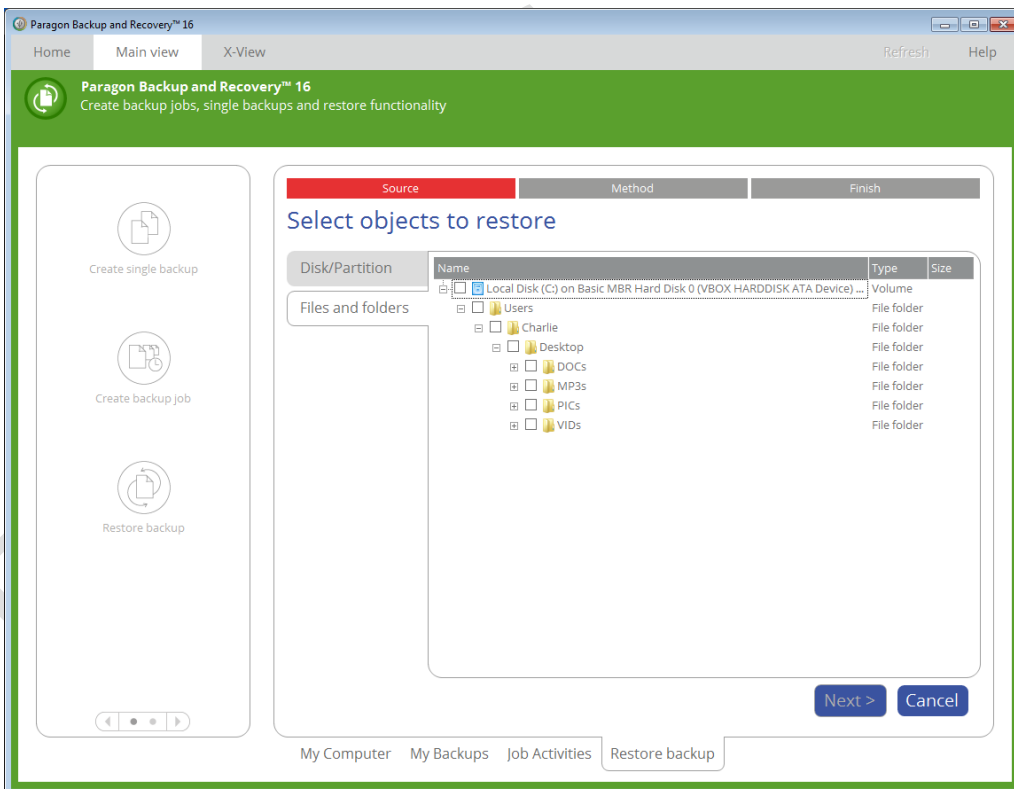


Figure 24 - Restore screen

10 Conclusion

Among all the products we tested, exclusively Acronis True Image 2017 New Generation was able to protect the backups from every Ransomware family tested. The other solutions have basically zero backup protection when it comes to Ransomware.

When it comes to self-protection, and protection of the cloud accounts, we could not find issues with the following solutions: Acronis, Paragon and Macrium.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Protecting files against ransomware	✓	✗	✗	✗	✗	✗	✗	✗
Protecting backup files against ransomware	✓	✗	✗	✗	✗	✗	✗	✗
Continuous backup feature	✓	✓	✓	✓	✓	✗	✓	✗
Cloud backup and local backup service protected	✓	✗	✗	✗	✗	✗	✗	✗

When it comes to the performance tests, Acronis won most performance tests, and in the cases when it did not win a test, it scored second.

Looking at the product feature list, Nova Backup solution won.

	Acronis	CrashPlan	EaseUS	Genie	IDrive	Macrium	Nova	Paragon
Protecting files against ransomware	Best	None	None	None	None	None	None	None
Cloud backup and local backup service protected	Best	None	None	None	None	N/A	None	N/A
Performance	Best	Worst	Good	Good	Average	Average	Good	Average
Feature list	Good	Worst	Good	Average	Good	Average	Best	Average

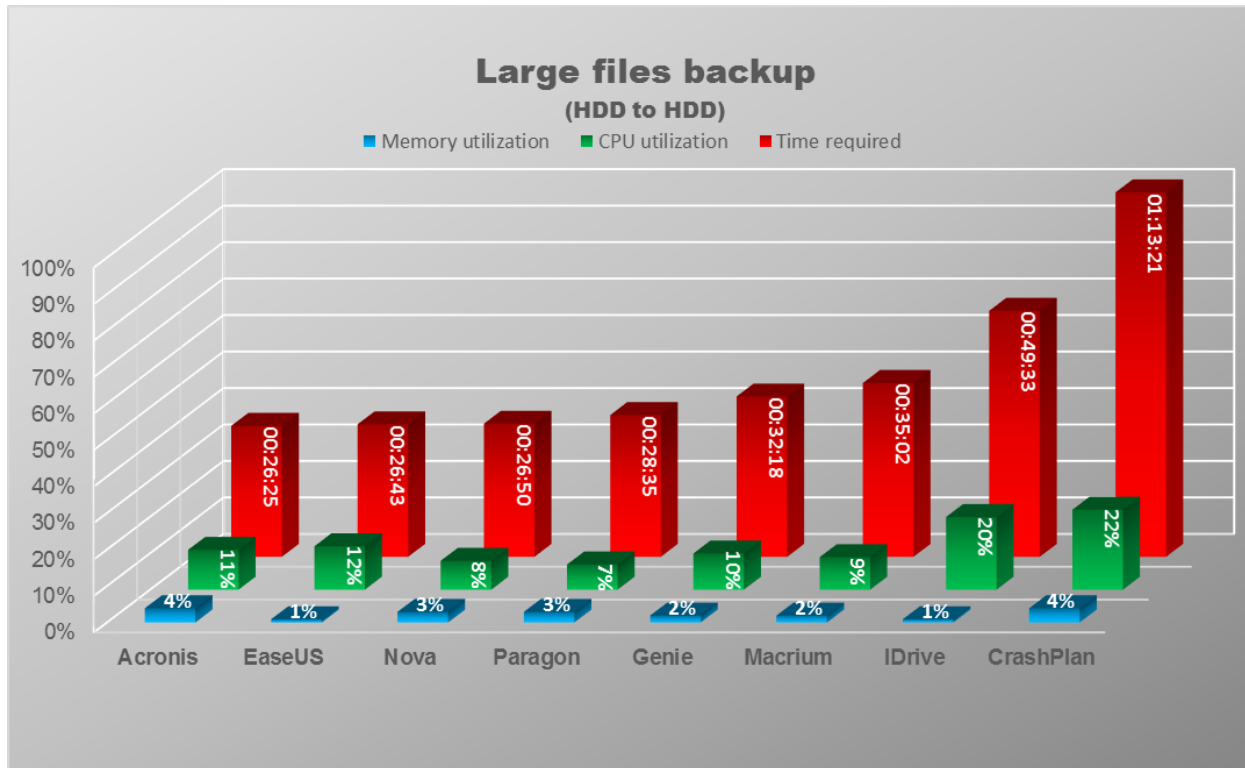
11 Appendix

11.1 Methodology used in the assessment

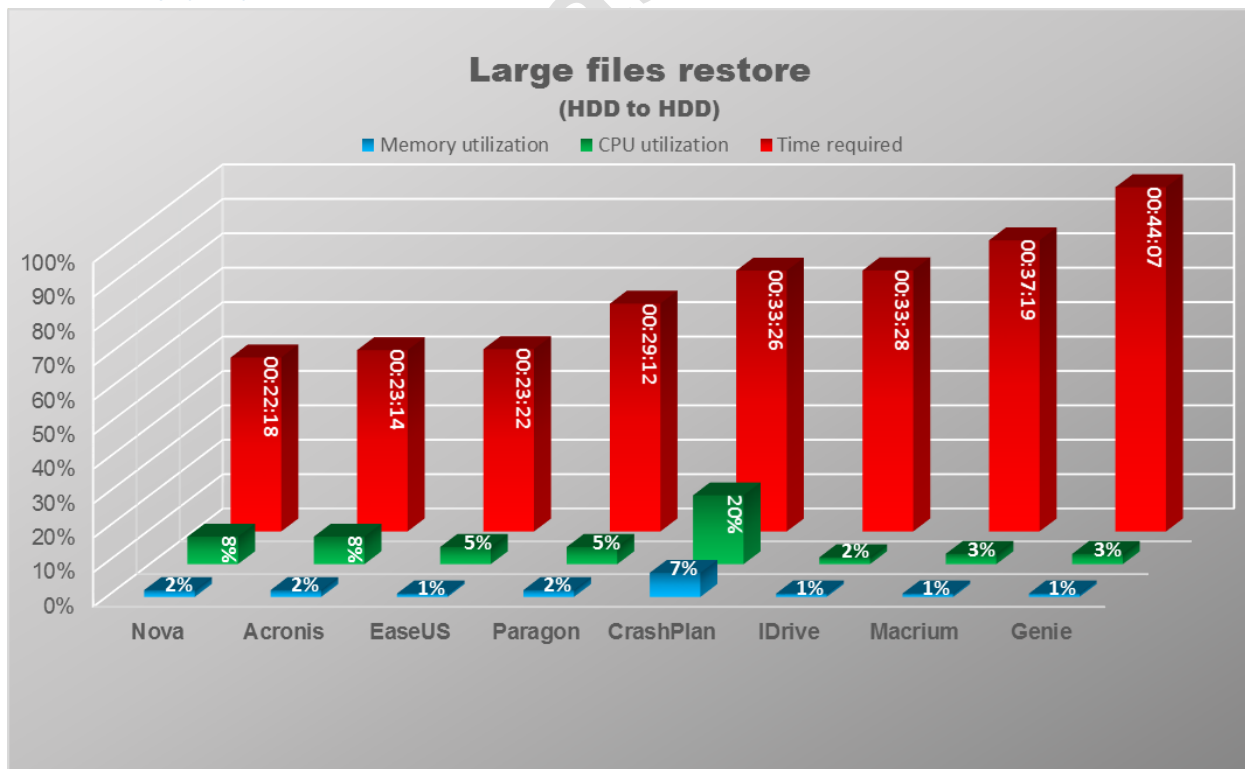
1. Windows 7 64 bit operating system was installed on a physical machine, all updates were applied and third party applications installed and updated according to our “Average Endpoint Specification”
2. An image of the operating system was created.
3. A clone of the imaged systems was made for each of the backup applications used in the test.
4. An individual backup application was installed using default settings on each of the systems created in 3. and then, where applicable, updated.
5. A clone of the system as at the end of 4. was created.
6. Each live ransomware test was conducted by:
 - Downloading a backup software from the vendor’s home page.
 - Creating user file & folder backup to another local folder
 - Downloading a single malicious binary from its native URL using Microsoft Edge to the desktop, closing Microsoft Edge and then executing the binary.
7. The backup under test was deemed to have been infected if:
 - The backup software failed to protect the local backup archives therefore making the restore impossible.
 - The backup software failed to protect the access to cloud backup accounts therefore making the cloud backups vulnerable.
8. Performance tests were conducted by using the same HW & NW configuration.
9. Testing was conducted with all systems having internet access.
10. Complete system wipe and reimage was performed before installing backup software.
11. Each individual test for each backup application was conducted from a unique IP address.
12. All backup applications were fully-functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
13. All testing was conducted during Q1 2017.

11.1.1 Local HDD operations

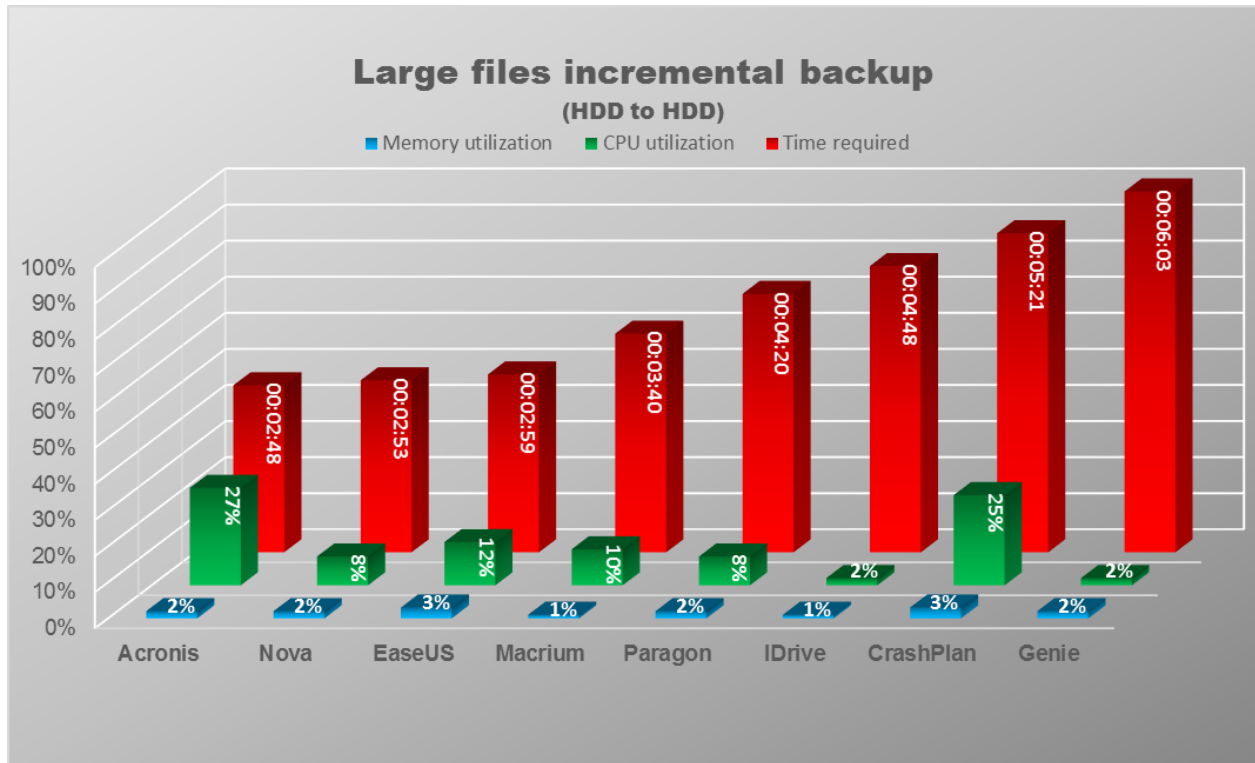
11.1.1.1 Large files full backup (50x1GB)



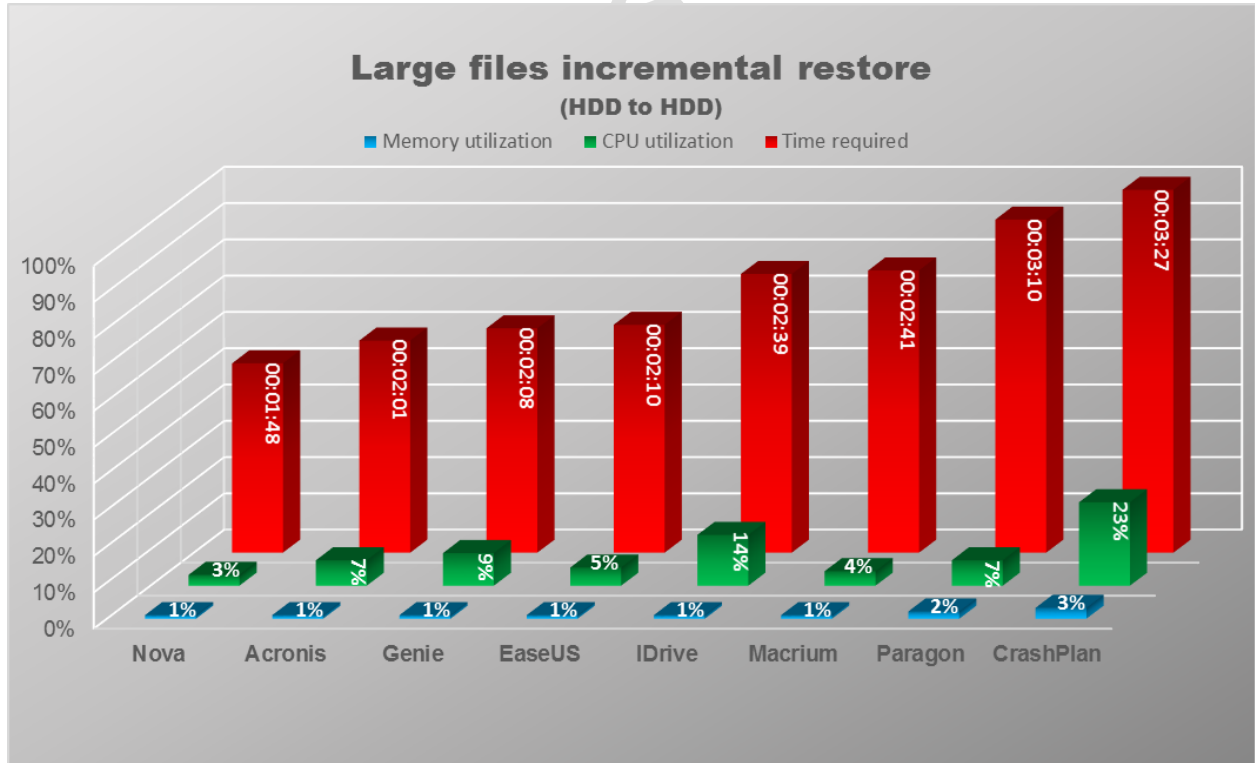
11.1.1.2 Large files full restore (50x1GB)



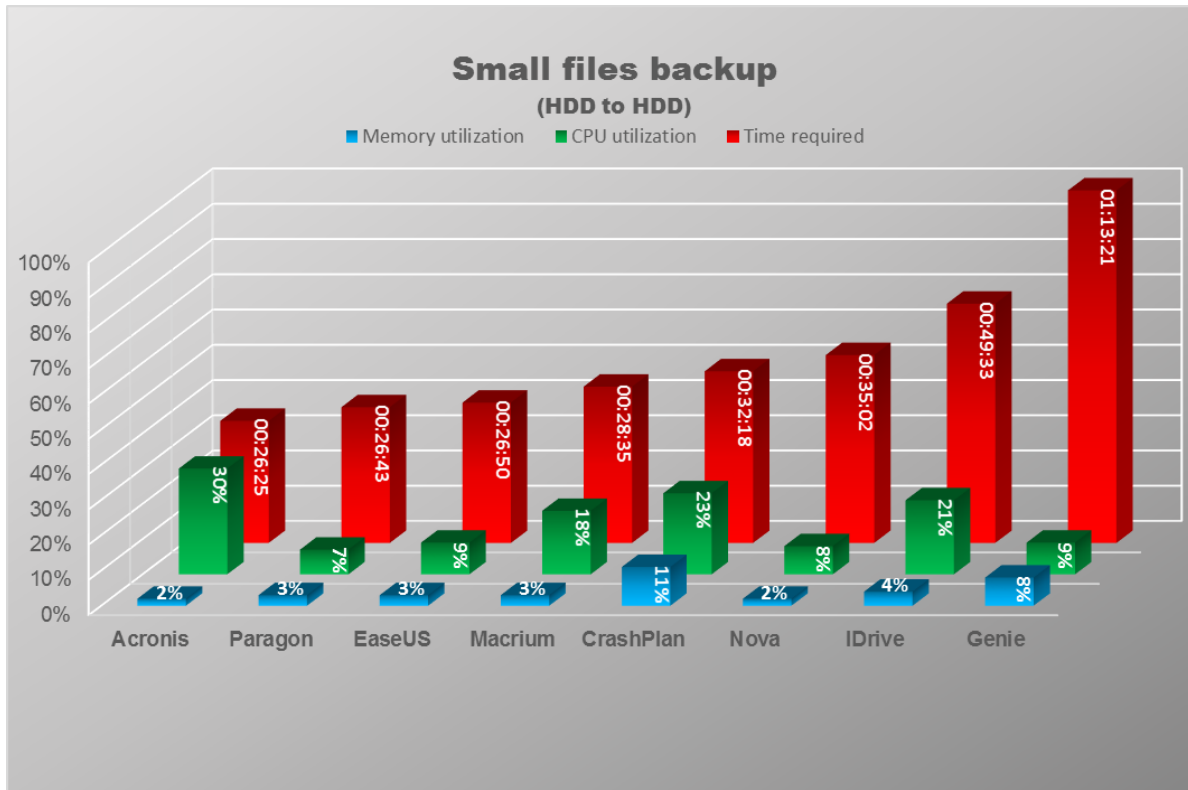
11.1.1.3 Large files incremental backup (5x1GB)



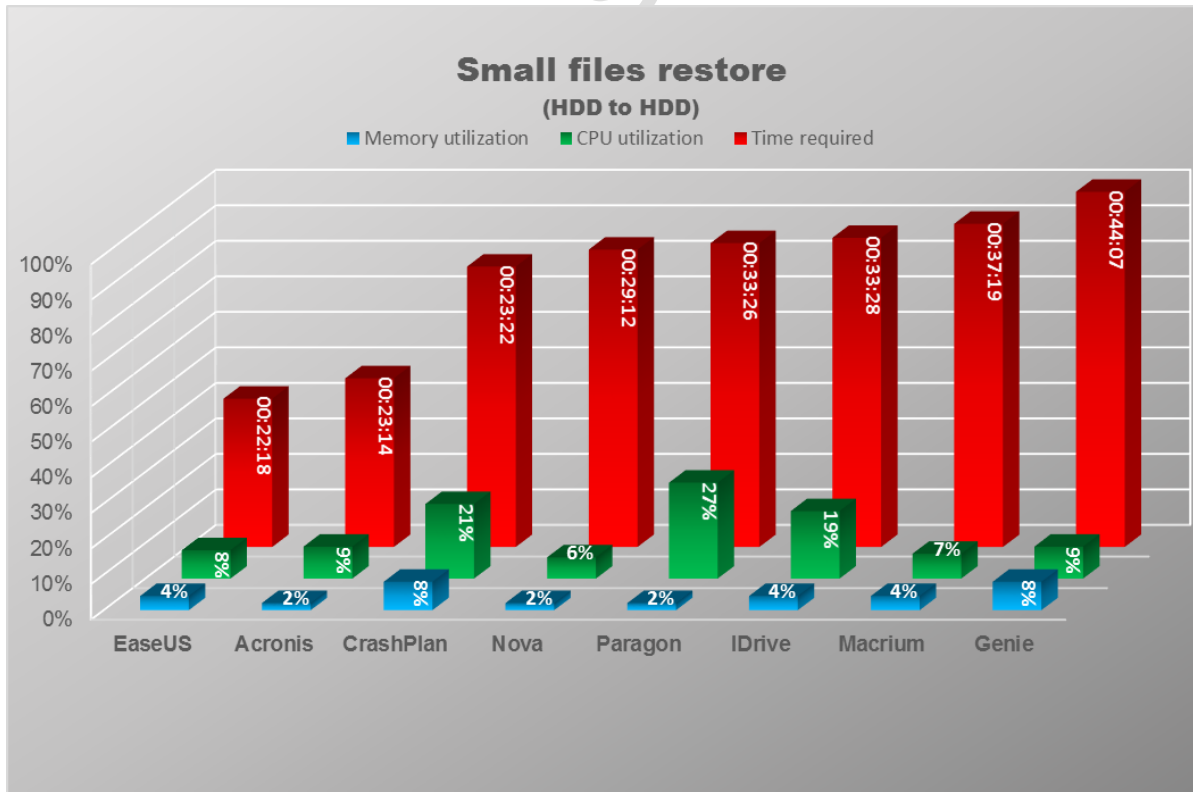
11.1.1.4 Large files incremental restore (5x1GB)



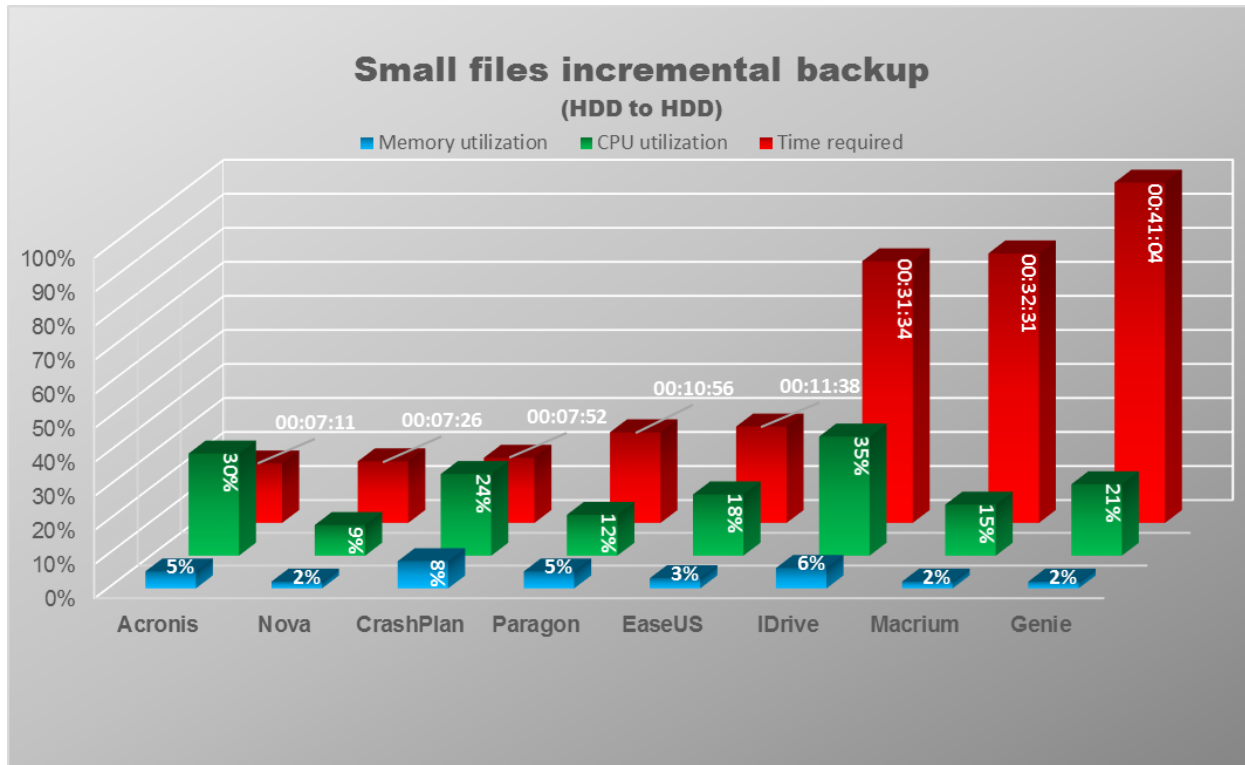
11.1.1.5 Small files full backup (102.4Kx512KB)



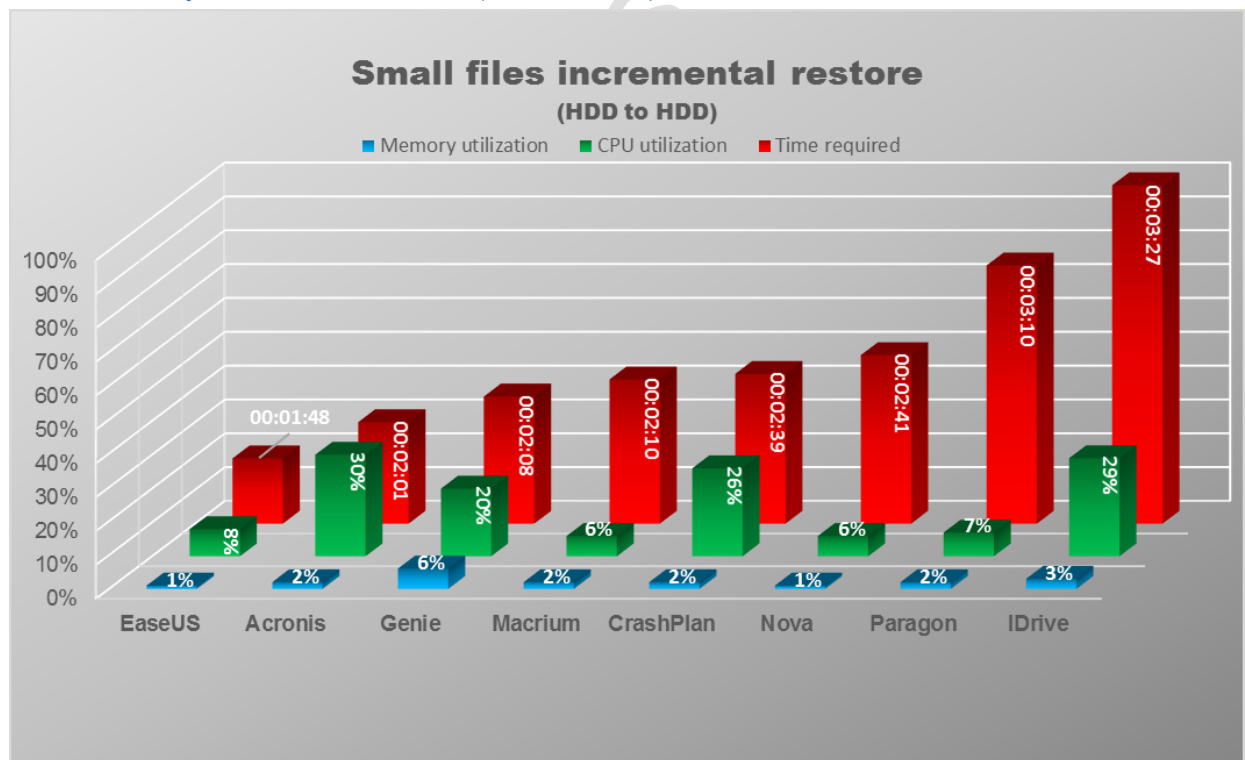
11.1.1.6 Small files full restore (102.4Kx512KB)



11.1.1.7 Small files incremental backup (10240x512KB)

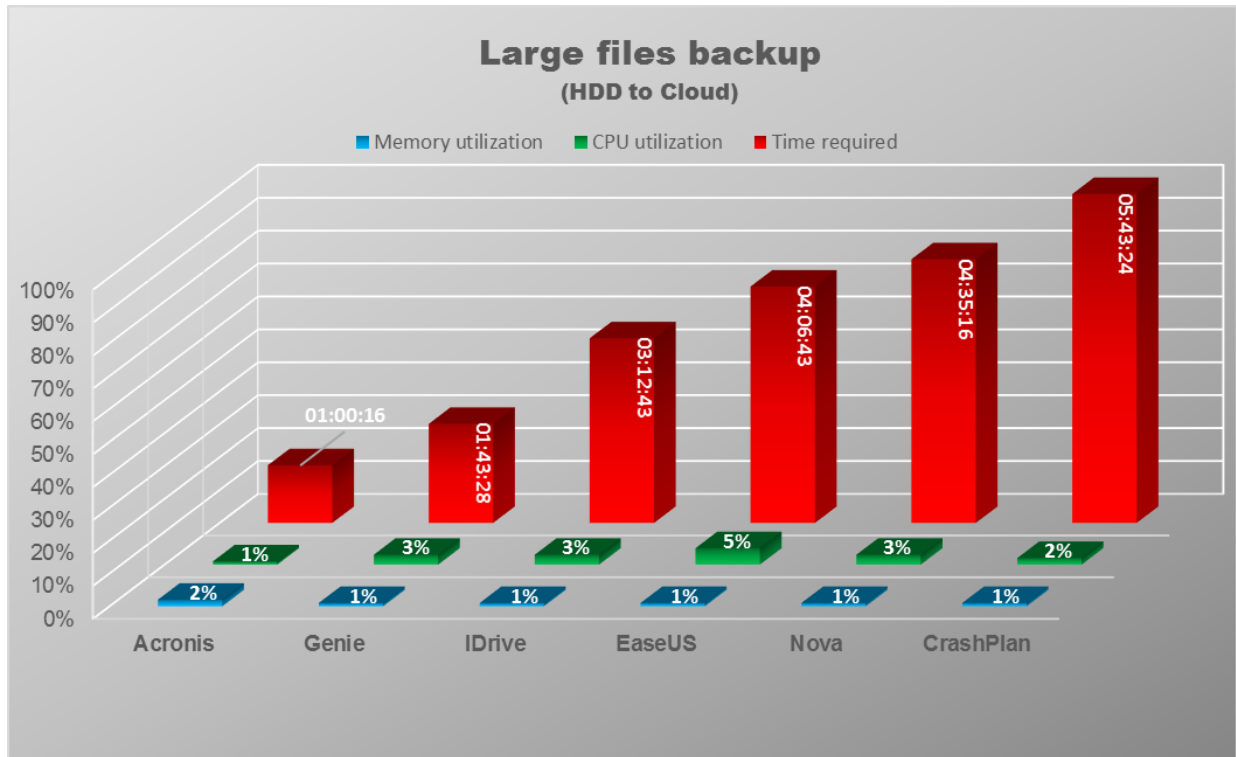


11.1.1.8 Small files incremental restore (10240x512KB)

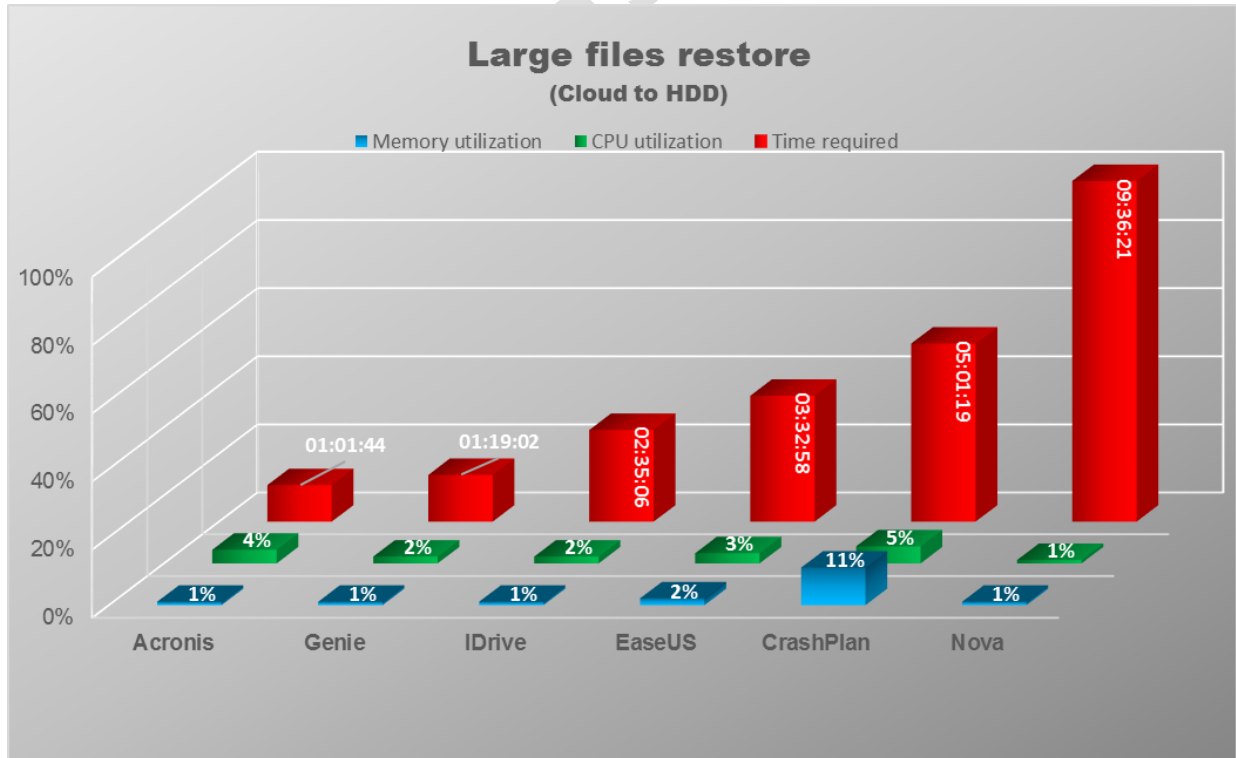


11.1.2 Cloud operations

11.1.2.1 Large files full backup (5x1GB)

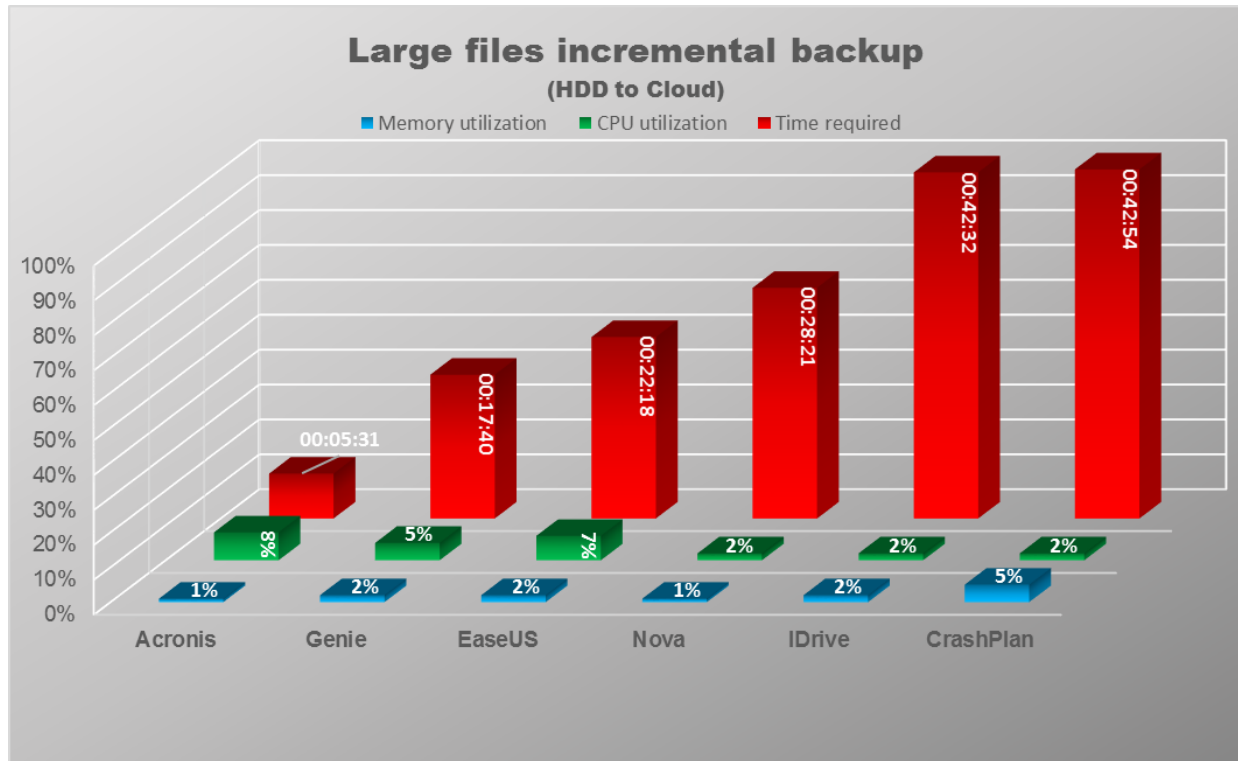


11.1.2.2 Large files full restore (5x1GB)

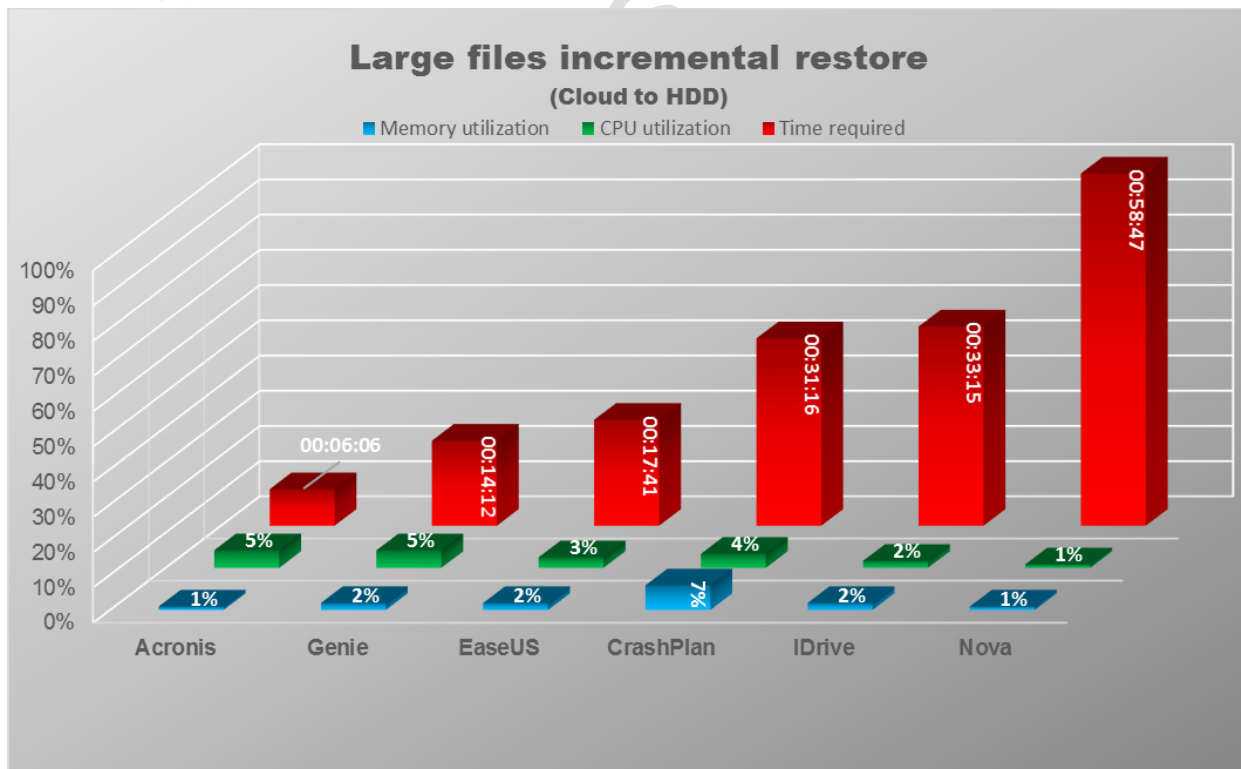


*Macrium & Paragon cannot provide cloud results

11.1.2.3 Large files incremental backup (5x1GB)

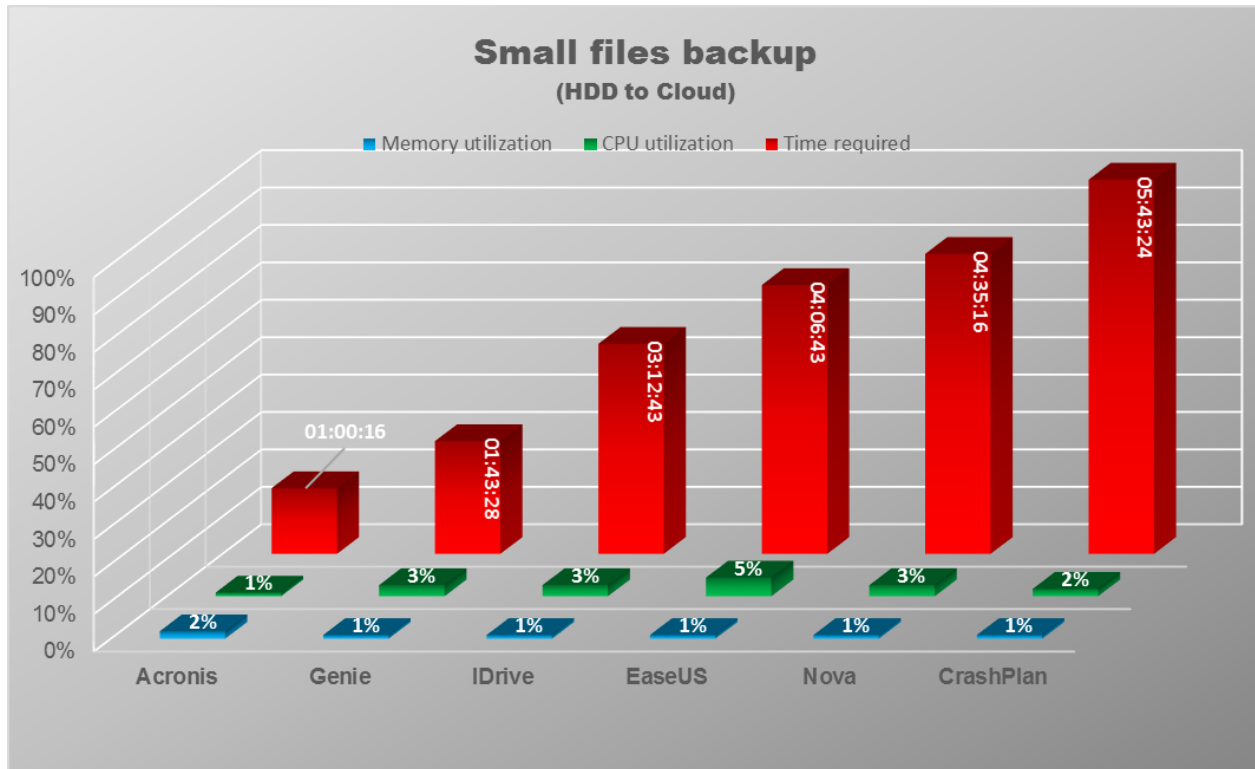


11.1.2.4 Large files Incremental restore (1x512MB)

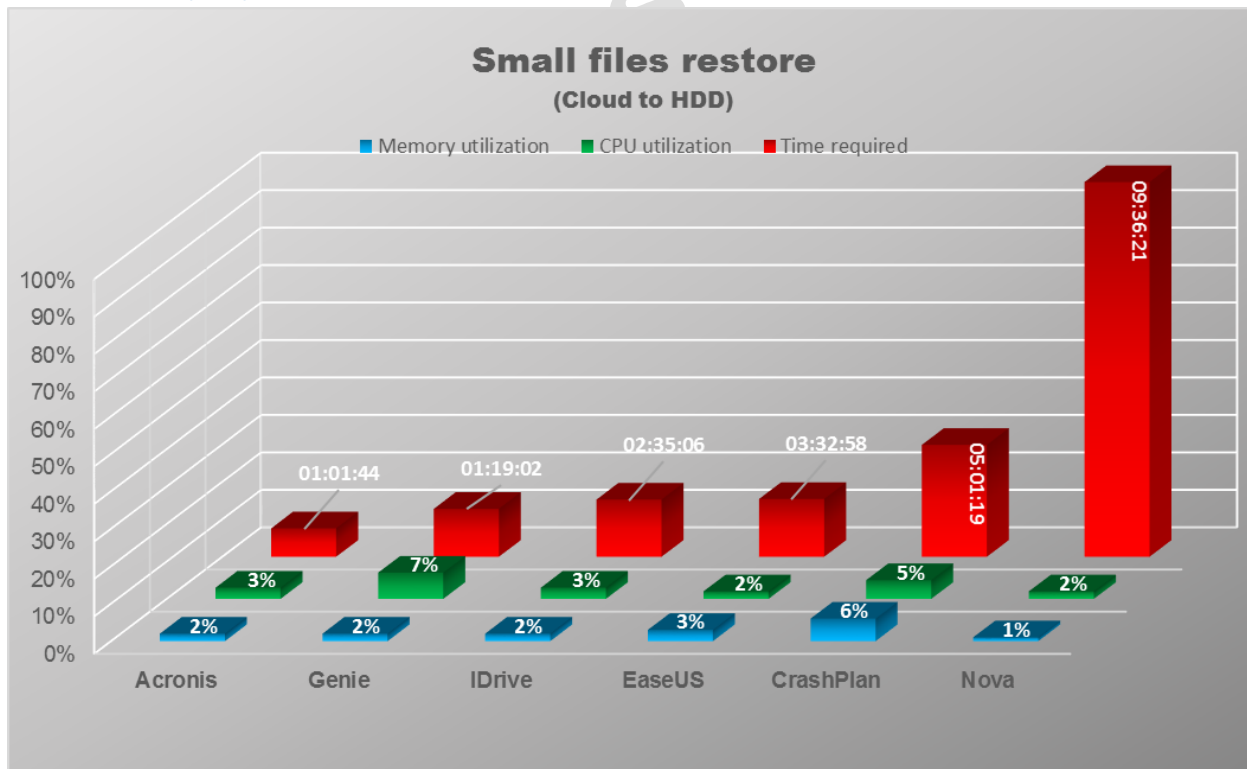


*Macrium & Paragon cannot provide cloud results

11.1.2.5 Small files full backup (10240x512KB)

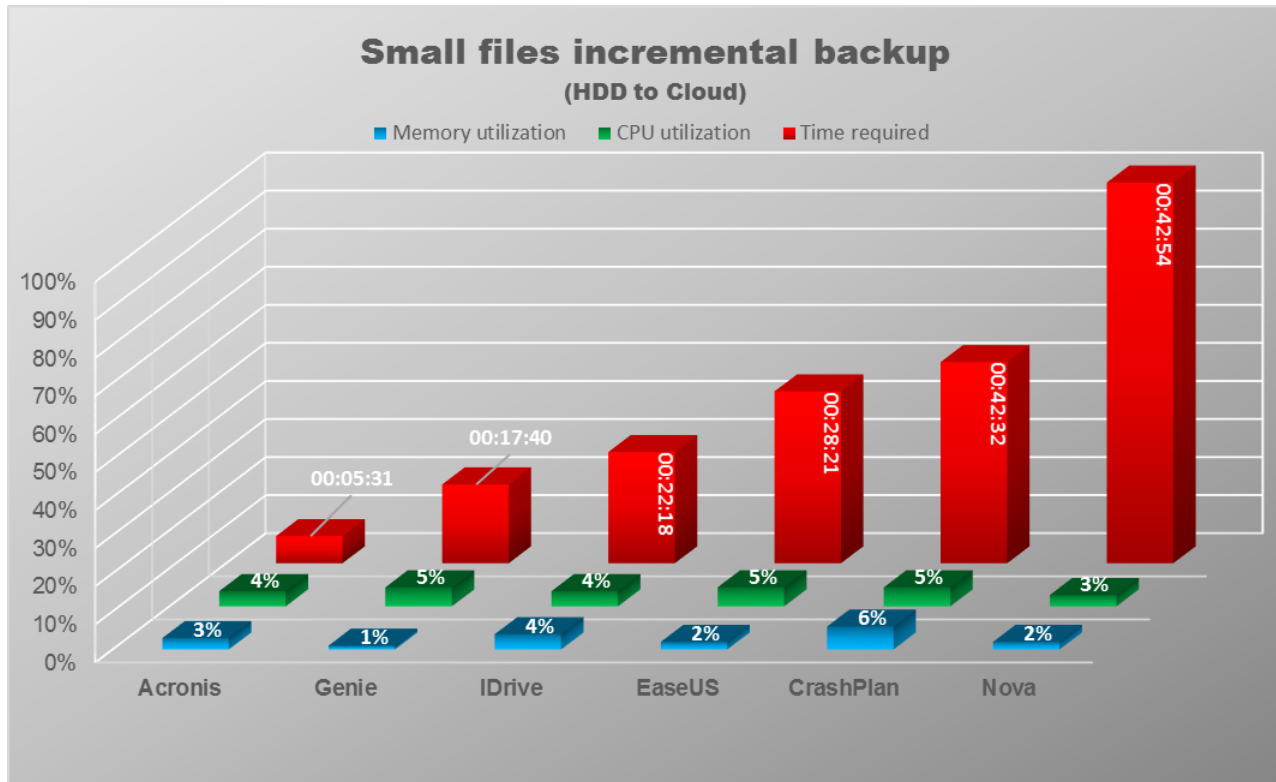


11.1.2.6 Small files full restore (10240x512KB)

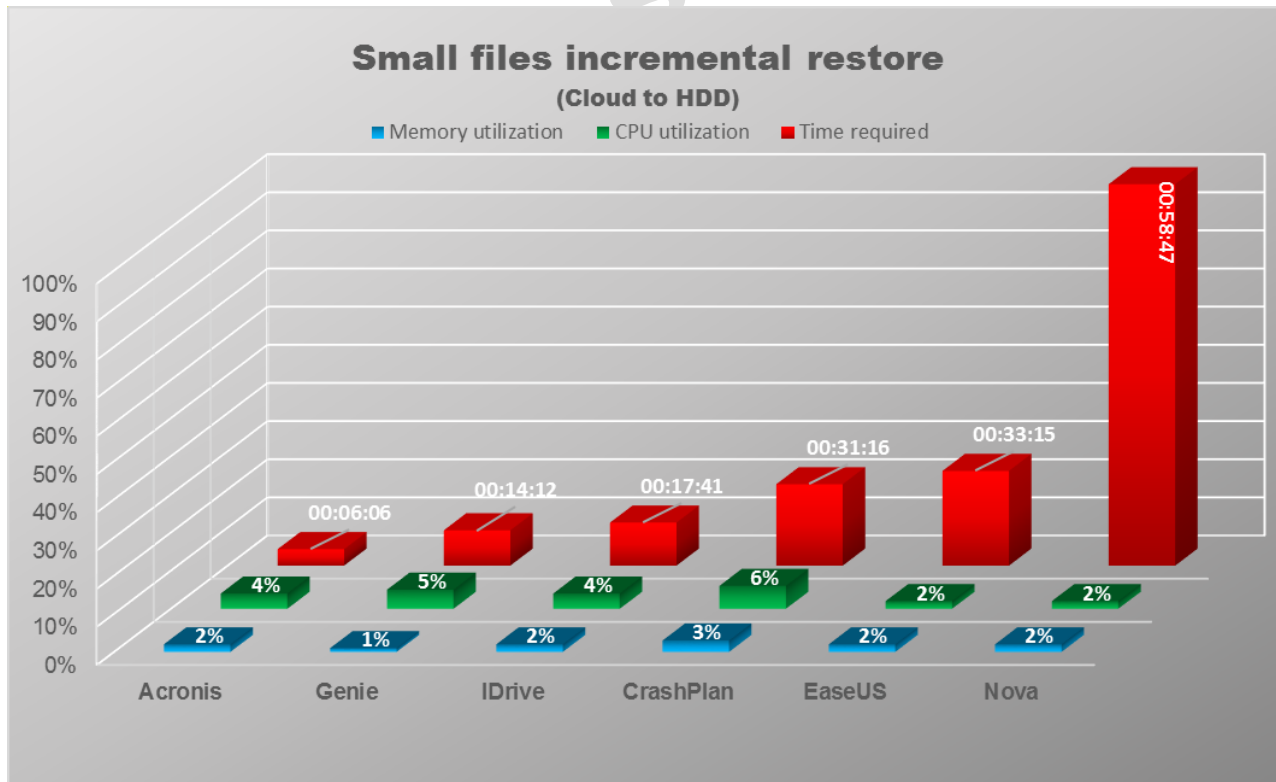


*Macrium & Paragon cannot provide cloud results

11.1.2.7 Small files incremental backup (1024x512KB)



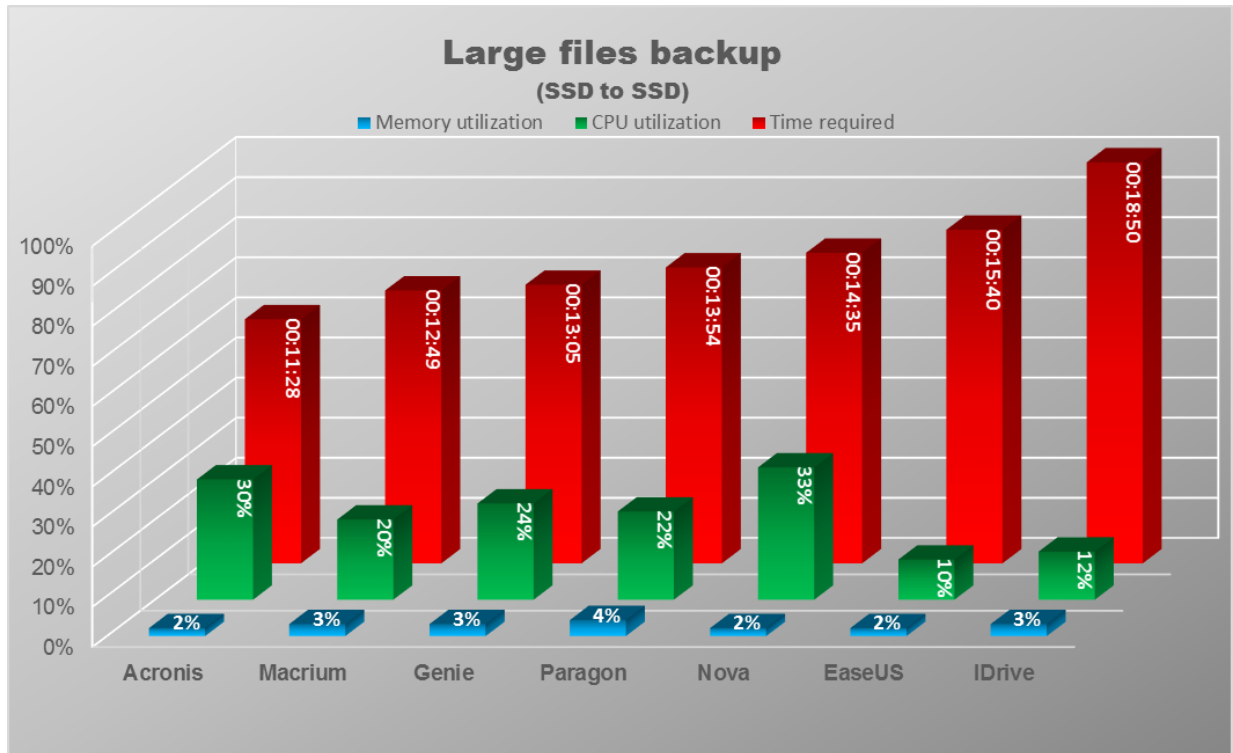
11.1.2.8 Small files incremental restore (1024x512KB)



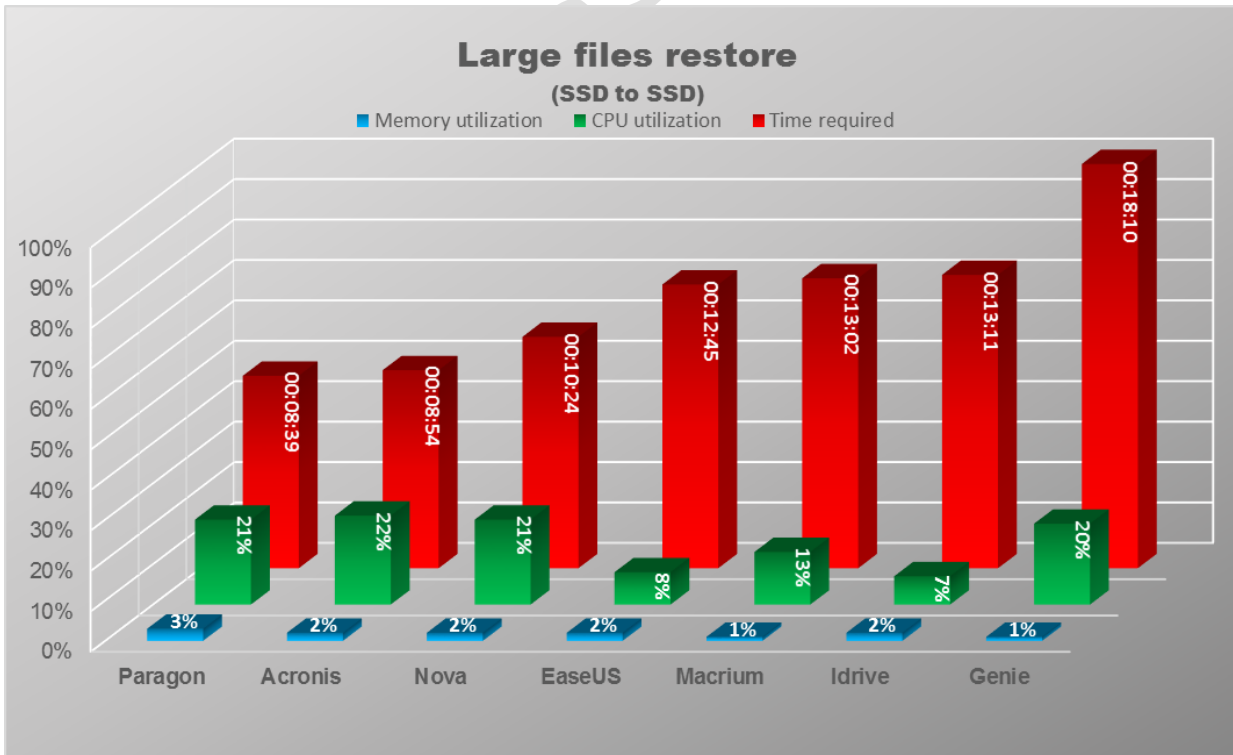
*Macrium & Paragon cannot provide cloud results

11.1.3 Local SSD operations

11.1.3.1 Large files full backup (50x1GB)

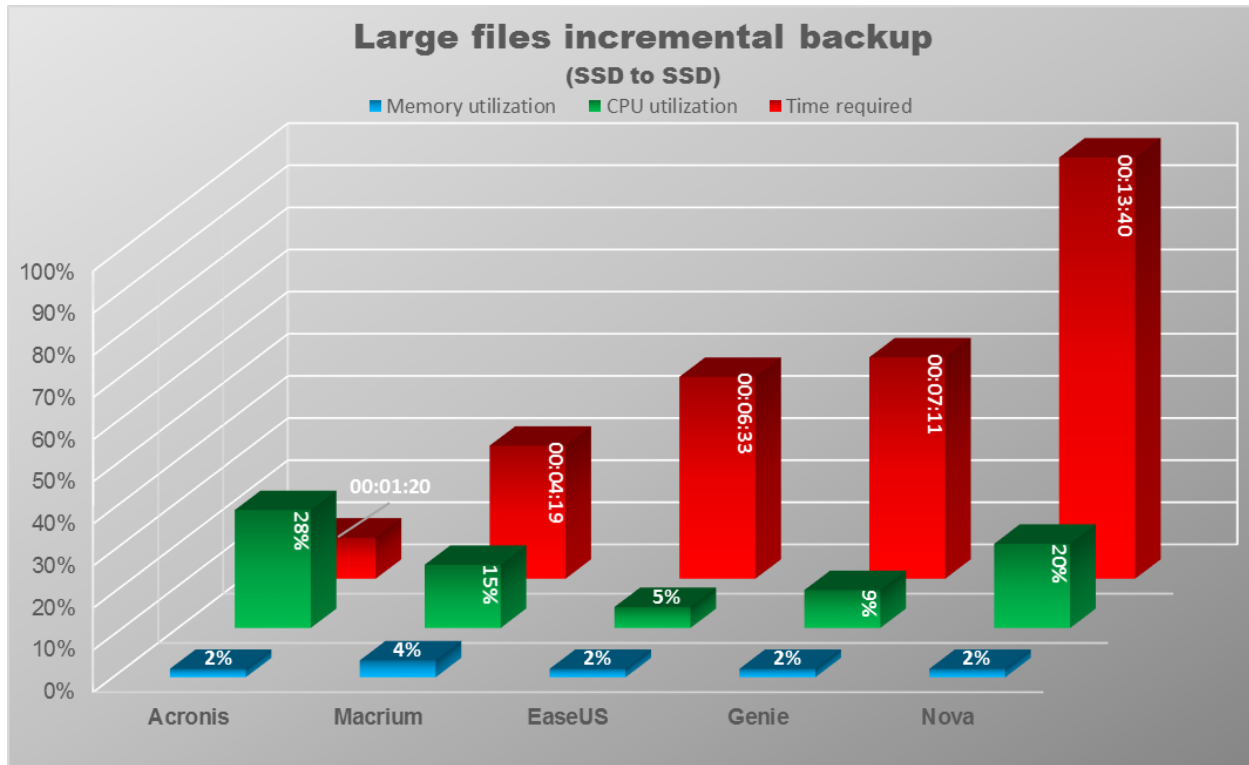


11.1.3.2 Large files full restore (50x1GB)

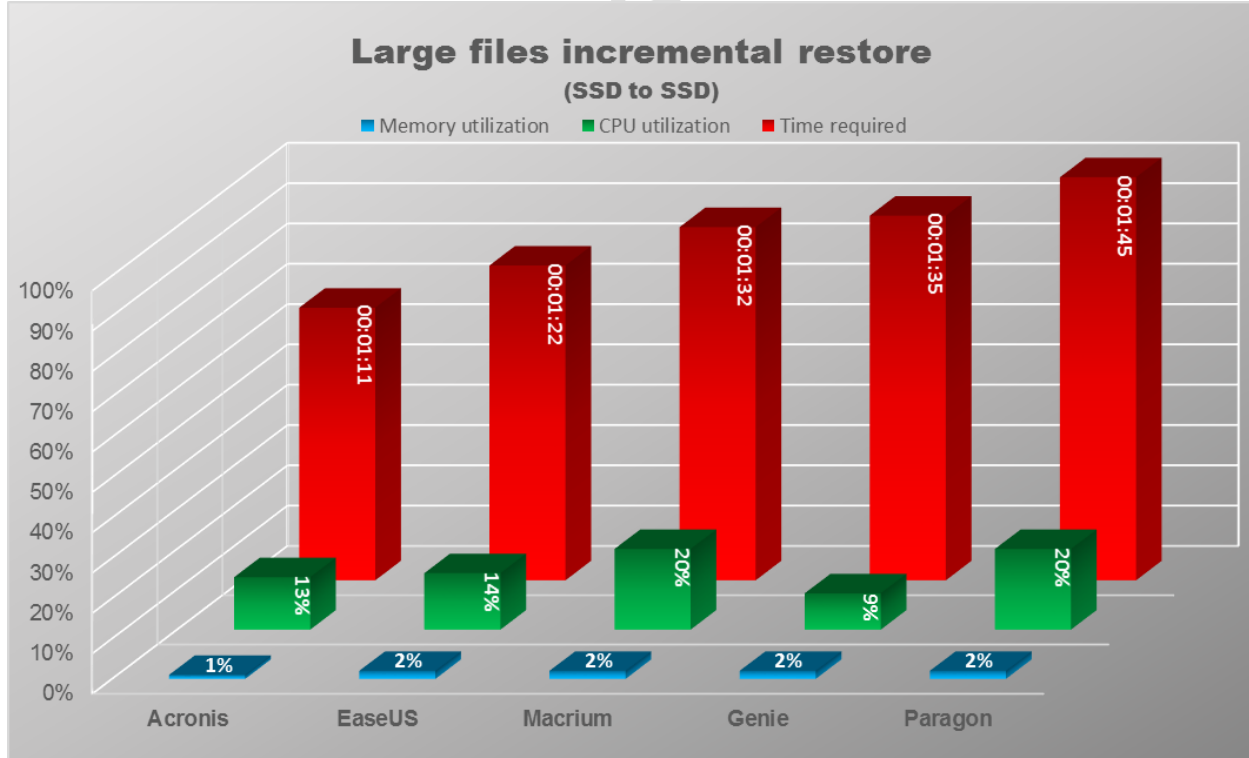


* CrashPlan does not have disk backup/restore

11.1.3.3 Large files incremental backup (5x1GB)



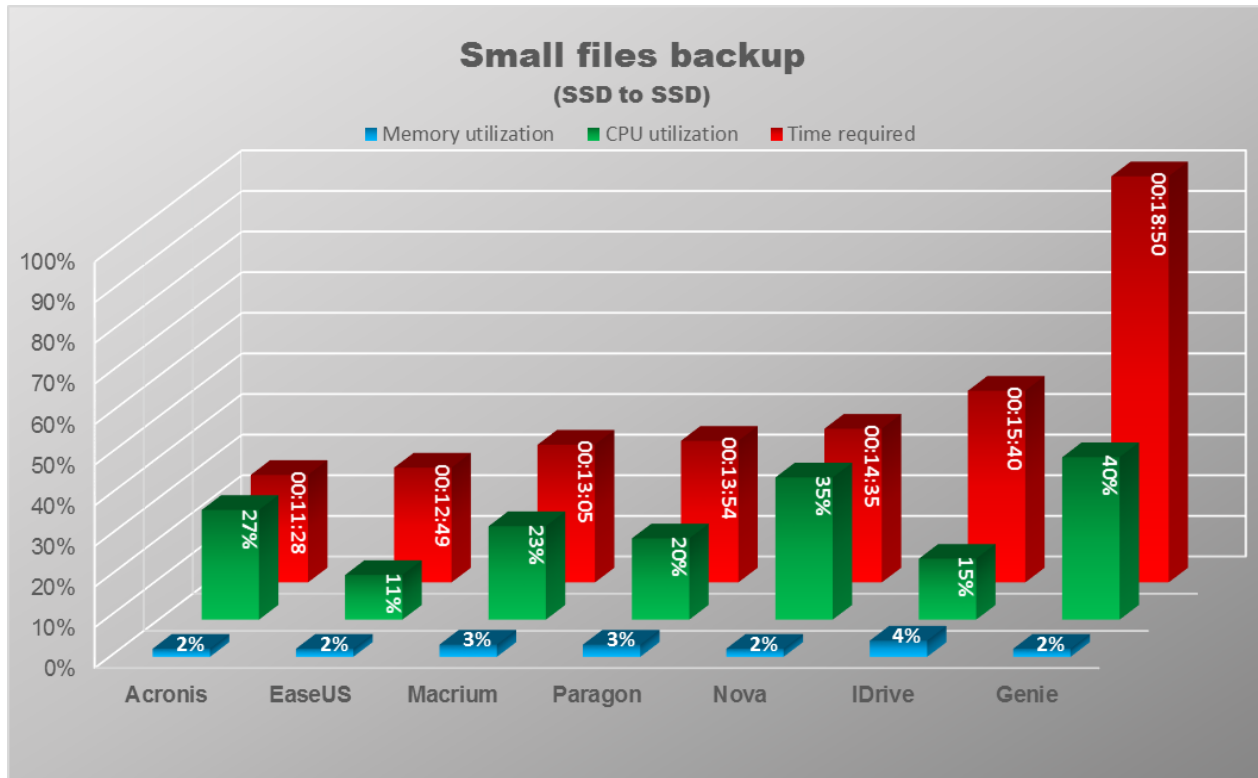
11.1.3.4 Large files incremental restore (5x1GB)



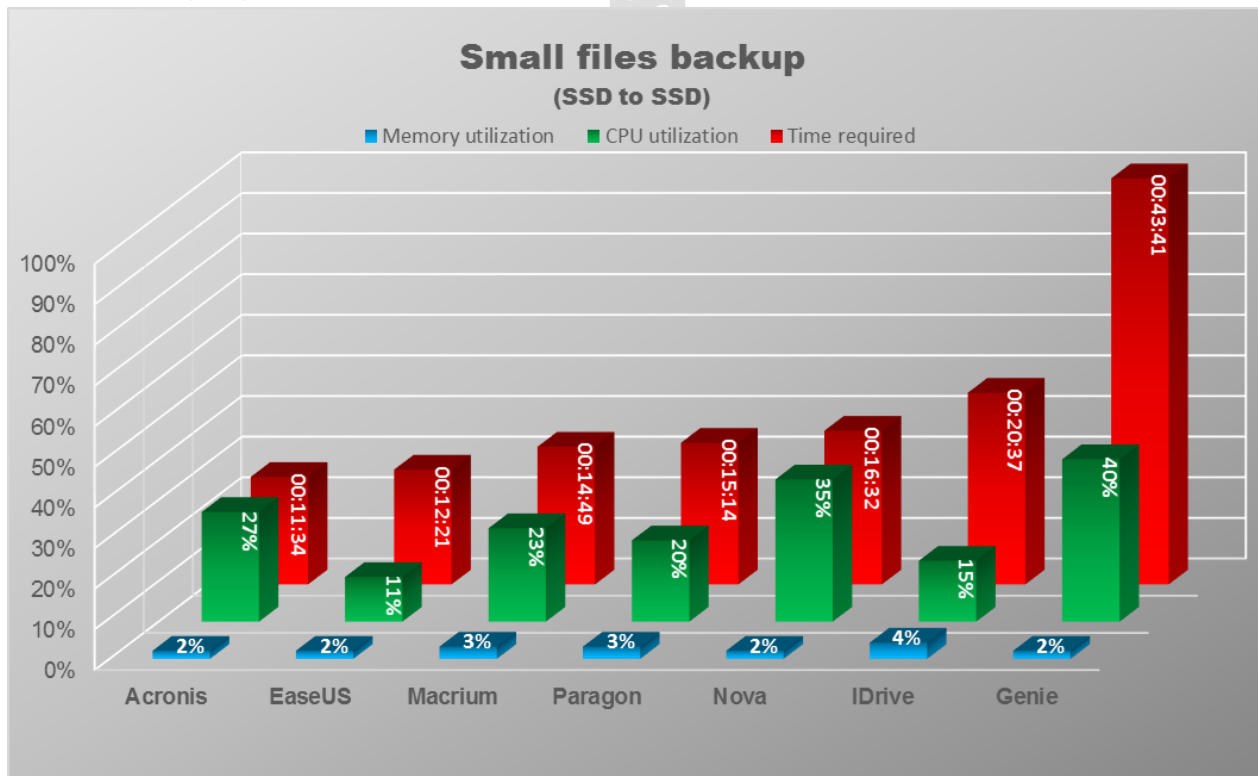
*Incremental Backup is not available with disk backup in IDrive & Nova

* CrashPlan does not have disk backup/restore

11.1.3.5 Small files full backup (102.4Kx512KB)

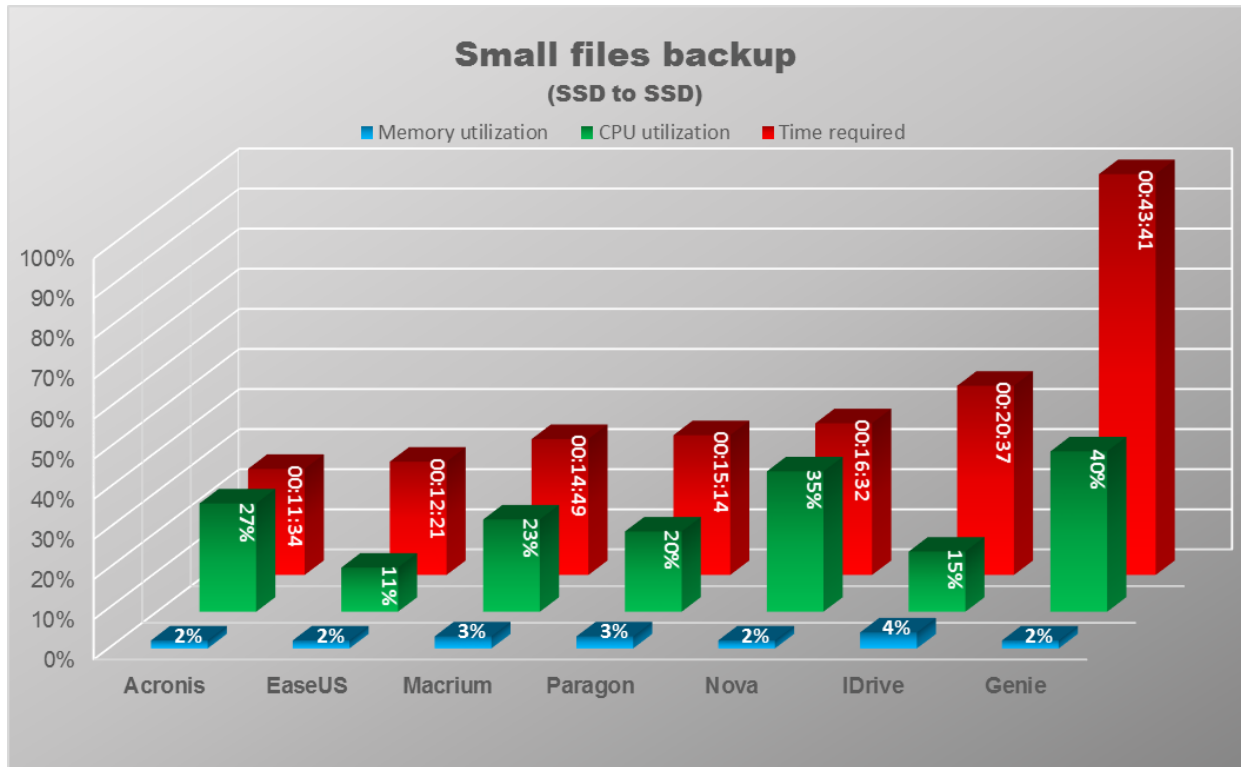


11.1.3.6 Small files full restore (102.4Kx512KB)

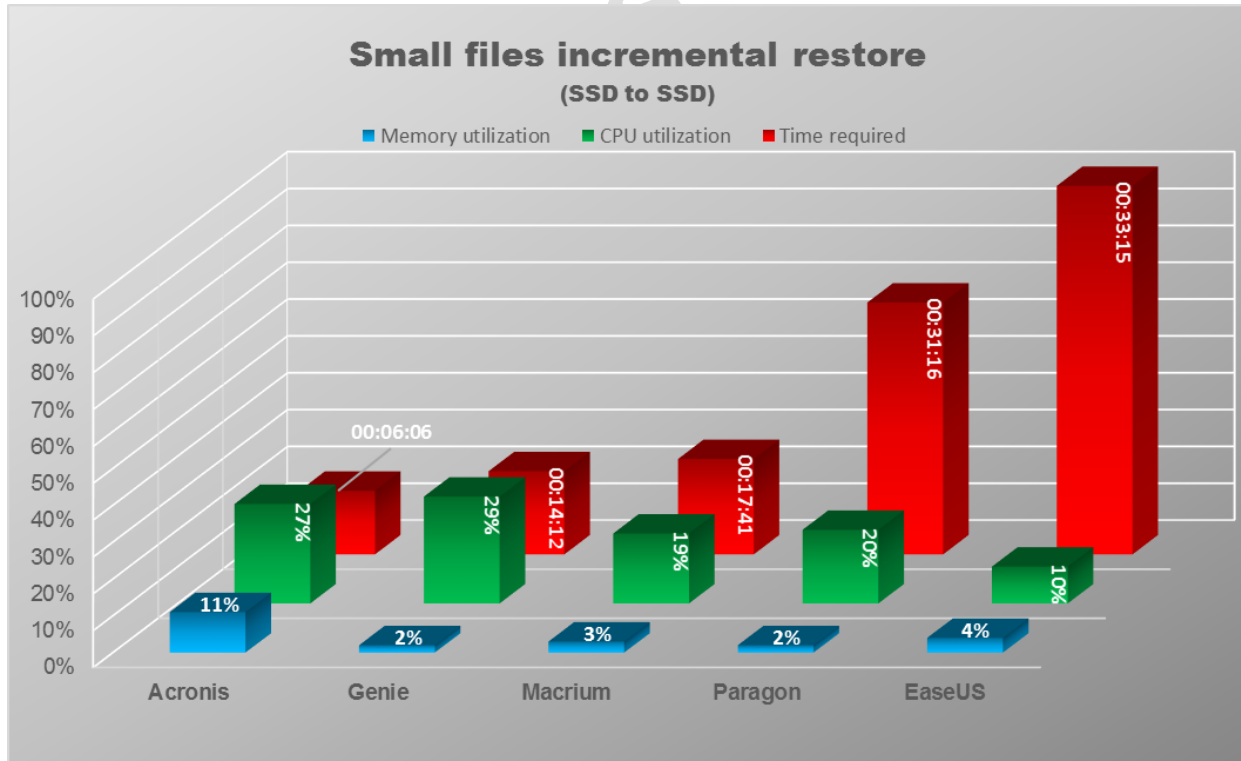


* CrashPlan does not have disk backup/restore

11.1.3.7 Small files incremental backup (10240x512KB)



11.1.3.8 Small files incremental restore (10240x512KB)



*Incremental Backup is not available with disk backup in IDrive & Nova
 * CrashPlan does not have disk backup/restore