ATEMPO
preserving data ecosystems

Restoring in all situations

Desktop and laptop protection

Adapt data restore methods to different situations

Executive Summary

Whether caused by human error, a cyber attack, or a physical disaster, data loss costs organizations millions of euros every year (3.5 million euros on average according to the Ponemon Institute). Backup remains the method of choice to protect access to company data and ensure their availability.

But a good backup strategy must necessarily be accompanied by a good disaster recovery strategy. The purpose of this white paper is to present the best restore practices depending on the situation you are in, in order to save valuable time!

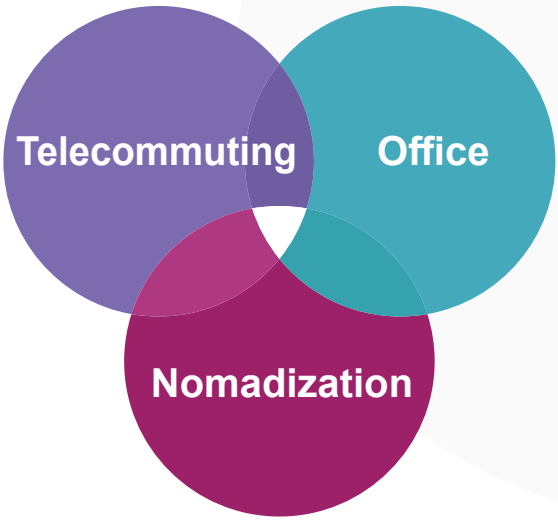


Table of Contents

EXECUTIVE SUMMARY 2

CONTEXT 4

WHAT ARE THE STAKES BEHIND THE RESTORING ENDPOINT USER DATA? 5

SOLUTION: RESTORING ENDPOINT DATA USING LINA 6-7

1. RESTORE FOR THE MOST NOVICE USERS 8-10

2. RESTORE FOR OFF SITE USERS 11-13

3. RESTORE FOLLOWING LOSS, BREAKAGE OR THEFT OF TERMINALS 14-16

4. RESTORE FOLLOWING A CRYPTOLOCKER VIRUS ATTACK 17-19

ATEMPO SOLUTIONS 20

ABOUT ATEMPO 21

Context

According to a study published in 2020 by a major US cloud provider, in 2019, nearly half of the world's businesses experienced data loss resulting in a reduction in their business activity. How can this number be explained when, according to the same study, about 90% of companies back up their data? A first answer comes from the number that do it daily (less than one in two), but also from a lack of preparation for fast data recovery.

Whatever protections are applied to the company, all IT departments know that zero risk is a myth. Whether the origin is intentional or not, all organizations will face at least one IT disaster during their existence: a crash, loss, laptop theft, ransomware attacks, the risk is always present. As eliminating the risk is impossible, we should try to mitigate it and reduce its impact. Backups are therefore a very good idea. At this stage, most organizations have implemented solutions to maintain the availability of their data, but the aftermath still has to be prepared, i.e. what to do after the disaster with business teams that are often IT novices.

In addition, the digital transformation of companies has created a continuously growing phenomenon: workstation nomadization. This nomadization, leads to an overexposure to the risk of data loss for companies. We consider that without active measures, almost one third of company data is stored nowhere else than on users' mobile devices.

What are the issues behind restoring your computer data?

- Guaranteeing the availability of your data in the event of an attack: this challenge seems to be the most obvious. If data is lost, the primary data is no longer in your possession. In terms of security, the main advantage of backups is to minimize the impact of a ransomware type attack. The main purpose of backups is therefore to guarantee the availability of the data and as such it is one of the last solutions in cases of a successful attack.

- Protecting your business activity: this more global issue applies equally well to cases of negligence to malicious action on your data. In this case the impact will be felt at the company activity level, which will no longer be able to operate without certain essential data. This can apply at the organisational level if the network is infected, but also at the individual level if a computer is lost or stolen, depriving the person of their data.

It is therefore essential to know how to react to these situations in order to restore data as quickly as possible and limit financier impacts.

In short, choosing the right backup solution to protect and secure a set of laptops is more than just a list of technical capabilities. Continuous Data Protection (CDP) should be available, as well as the ability to restore a file or an entire machine (Bare Metal Restore or BMR) and deduplicated block mode to save both space and the network. However, if you need to choose your company's laptop protection solution, do not limit yourself to this list of features and do not lose sight of the basics:

In the event of a disaster, **you** are in an emergency;

YOU must first and foremost restore your files fast!

Solution: Restoring your computer data using Lina

Let's go back to the basics: lose as little data as possible **AND restore as quickly as possible**, as close as possible to the lost files, for each user profile and each data loss situation. Being in charge of your company's laptop assets means being confronted with different user profiles.

- Non-technical profiles who do not apply your backup instructions, and do not see the warning signs of equipment fatigue,
- A few careless people who give your equipment a hard time by exposing it to more shocks and temperatures spikes than the manufacturer intended,
- The inevitable “geek” employees who back up their own laptops and forbid you from laying a finger on their machine until the day ...,
- Accommodating salespeople, but who are always between two planes or trains,
- Victims of cryptoviruses and other cryptolocker type mishaps removing access to data at the most critical times,
- The CFO to whom you have already tried to explain that the difference in price between a server class SSD and an entry-level hard drive is justified, but who continues to focus on cost cutting

All these profiles have one thing in common: they are always in an emergency situation when it comes to restoring their precious documents, wherever they are on the planet.

So it is better to anticipate and **choose a backup solution that can deal with any data loss situation and offers several restore methods**: the security of your company's data is at stake, but also the productivity of your users.

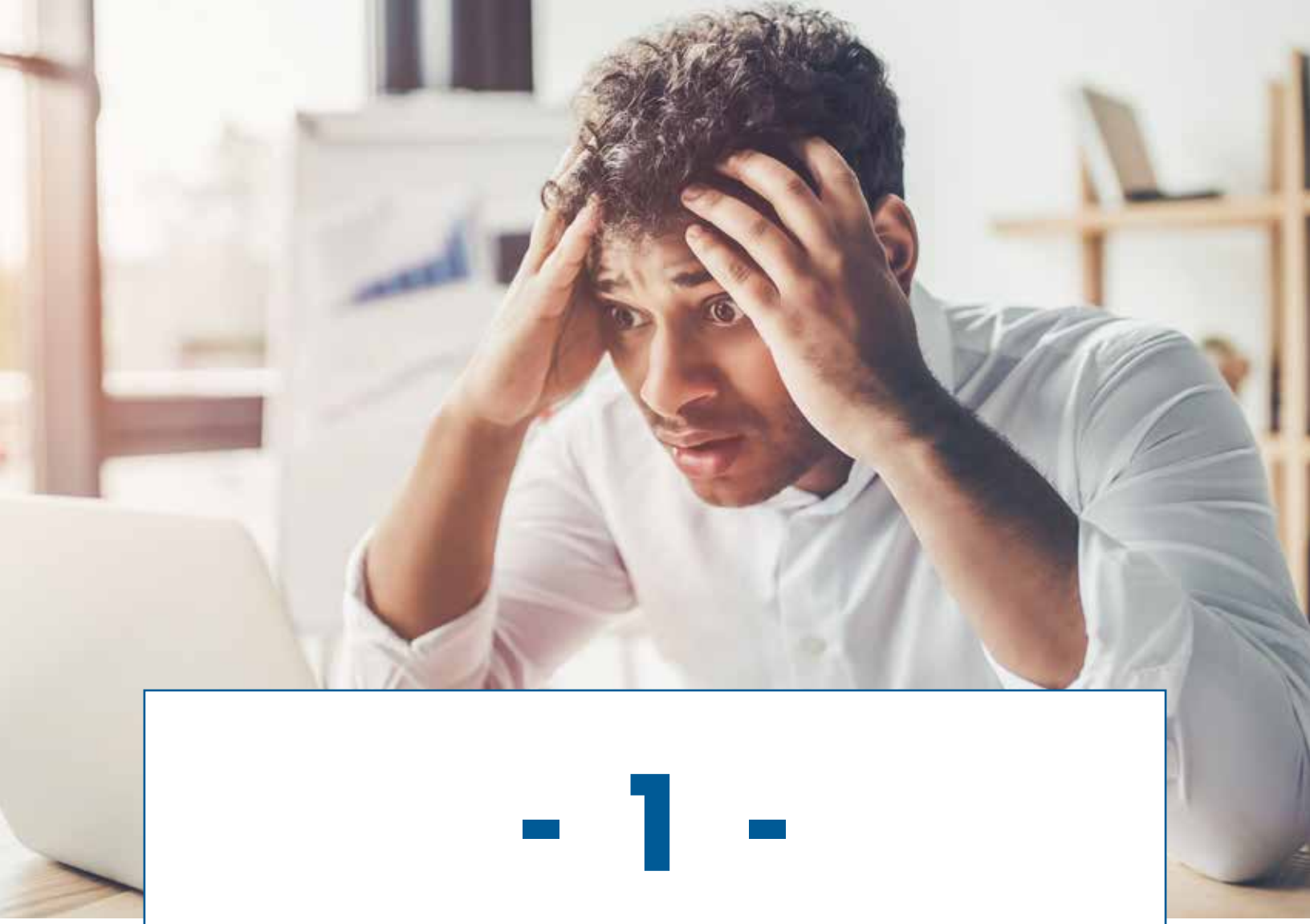
These are the 4 restore angles and associated scenarios proposed in this document

-1- Restore for the most novice users

-2- Restore for offsite users

-3- Restore in the event of loss, breakage or theft of terminals

-4- Restore in case of attacks by a cryptolocker virus



- 1 -

Restore for the most novice users

RESTORING USING A WIZARD

SCENARIO:

- The user cannot remember the lost file name or type
- Single file & emergency restore

PROTECTED TARGETS:

- Laptops, desktops and other user terminals

CHARACTERISTICS OF THIS RESTORE:

- Fully autonomous restore by users
- Guided restore using a wizard

This is a fairly typical situation in which employees or customers no longer remember the lost file name or type. They can only remember approximately when they last used it.

If their workstation (desktop or laptop) is protected by Lina, your employees have access to a **restore wizard** that can be launched by a simple click on the Windows, Linux, or MacOS workstation taskbar.

If you prefer, you can assist your users on the phone the first time they do this. However **the wizard is designed to guide users gradually until the lost file is recovered**. The operation takes less than 3 minutes!

Lina's **restore wizard** guides your users with a few simple questions and enable them to find the missing file, to choose the version to restore and where to restore it. Lina restore wizard will become a valuable tool, allowing your users to quickly restore lost files and folders by themselves.

RESTORING USING WINDOWS EXPLORER OR THE MAC OS FINDER

This is to meet the needs of slightly more advanced users who know how to browse their file storage space (for example: My Documents) **using explorer on Windows and the MacOS Finder**.

Two typical use cases:

- users need to revert to a previous version of a file,
- or they find that files are missing from a folder.

On a workstation (desktop or laptop) protected by Lina, your users can take action directly **from Windows Explorer or the MacOS Finder** at the missing file storage folder level.

The explorer is used to directly view the protection status of a folder or file : the presence of a green dot indicates that the item is protected by Lina. This is a great time saver - no need to access the backup configuration as you have all the information you need at a glance.

This self-service mode, enabling to restore directly from the file explorer or Finder will be especially suitable for users that are autonomous in the organization of their files. **They will be able to solve most "crises" on their own and will only call on your services** for the most serious cases and after attempting to restore on their own.

PROTECTED TARGETS:

- Laptops, desktops and other user terminals

CHARACTERISTICS OF THIS RESTORE:

- Fully autonomous restore by users (self-service)
- Very fast restore in 3 easy steps

- 2 -

Restore for offsite users

RESTORE USING A WEB INTERFACE

SCENARIO:

- Users who do not have their machine and are located outside of the company perimeter, without direct access to the data center
- Occasional restore of an urgent document from a browser

PROTECTED TARGETS:

- Laptops, desktops and other user terminals

CHARACTERISTICS OF THIS RESTORE:

- Fully autonomous restore by users (self-service)
- Remotely operated secure restore

This restore mode very effectively addresses cases of users located outside of the company perimeter, needing to restore data without direct access to the data center. Your goal is then to help them restore their data.

Even if the situation seems complex, **Lina will give you the means to get your users out of trouble**. They can either use their mobile phone or a colleague's laptop to **connect to the backup platform using a web browser**. Once security has been cleared (two-factor authentication), the file can easily be located in their machine's file system and downloaded in a few clicks.

Lina allows your users to complete the planned task without any problems by letting them restore their files on their own quickly and properly using Lina's web interface. The critical emergency is dealt with! Furthermore, your users are not limited to the latest version of their files: **Lina's web interface can go back in time to find previous versions.**

It should be noted that if it is not a mishap and your machine needs replacing, you will again have the opportunity to use Lina to restore all the documents from a stolen machine, or to reinstall the operating system and files from the backup.

REMOTE RESTORE BY THE ADMINISTRATOR

Despite the simplicity of the wizards available to your users, there will inevitably be times when you will need to give a helping hand and support them, or even do things for them in their absence. You need to find a backup solution that will allow you to easily restore data to a workstation remotely, whether or not the end user is present.

In some complex cases, users may require assistance or even be completely unavailable to complete the restore operation. Never mind! Lina also allows backup administrators **to remotely control the restore from A to Z without leaving their desks** to their original location or to a different location.

If you have the user on the phone, they can confirm how the operation is progressing in real time. If they are not available, it is not a problem: the Lina agent installed locally on the workstation will have restored the files anyway.

No need to travel, no time wasted guiding users to start a remote takeover: this **restore is carried out in a few clicks directly by a Lina administrator connected to the backup server**.

SCENARIO:

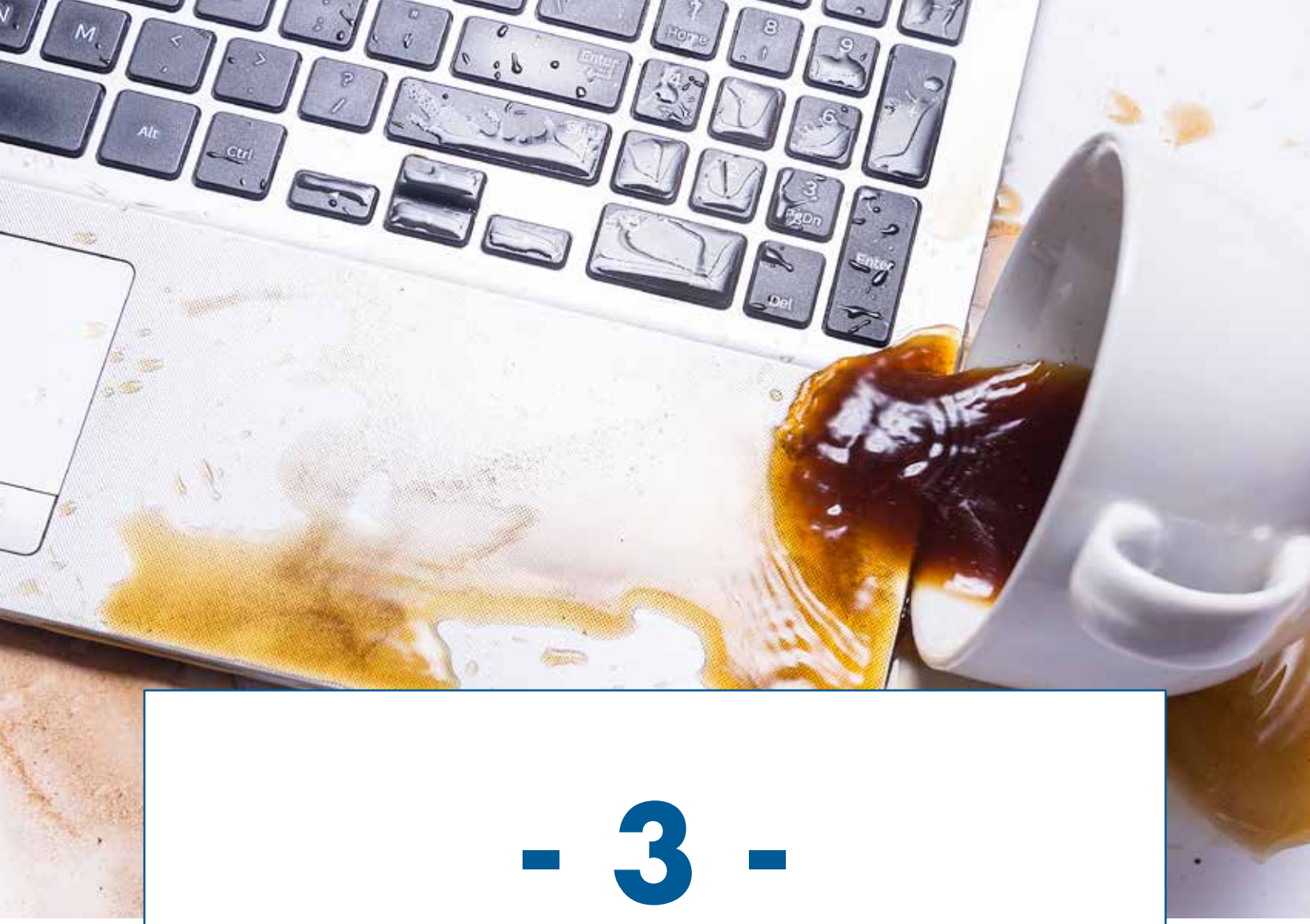
- The user is unable to restore their files without help
- The administrator will remotely restore to the remote station

PROTECTED TARGETS:

- Laptops, desktops and other user terminals
- File Servers

CHARACTERISTICS OF THIS RESTORE:

- Remote restore, without taking control of the screen
- Possibility of helping users by phone or operating in the users absence



- 3 -

Restore in the event of loss, breakage or theft of computers

BARE METAL RESTORE (BMR)

SCENARIO:

- Computer replaced by a new machine with no system installed
- Full system + data recovery from the backup

PROTECTED TARGETS:

- Laptops, desktops and other user terminals

CHARACTERISTICS OF THIS RESTORE:

- Backup administrator-operated restore

The Bare Metal Restore combined with continuous backup (CDP) makes it possible to rebuild a complete machine (system and data) directly from the backup server. Whether rebuilding a workstation following hardware replacement, or a hard drive crash, you are covered, your users will find their data as they were at backup time.

Our customers backup managers have had the opportunity to try several BMR (Bare Metal Restore) solutions. Very often, they criticize these solutions for being very cumbersome: the result is certainly often achieved, but at the cost of a long obstacle course involving several successive operations on one side for the OS, on the other for the applications, and finally for the data.

On the basis of this feedback, with Lina we decided to pursue a twofold objective:

- of course, to give users back the full working environment they are familiar with,
- but also, to rebuild their machine in a single operation covering the system, the applications and the data globally.

CROSS-MACHINE RESTORE

This scenario addresses the needs of administrators in charge of desktop or laptop assets since it involves **"replacing" users workstations with new machines** equipped with a pre-installed system. The whole point of the operation is to use the backup to restore the data to each workstation so that the **exchange of machinescan be carried out quickly and a complete workstation provided to the users**.

This procedure is highly secure (normal users do not have access to this advanced restore). It is completed in a few clicks and **allows identical restore** (last version restored in place) or file selection in the tree structure or by browsing through time.

Backup administrators do not need to access users' original workstation, no travel, no remote control. A workstation or even a file server can be replaced in a timely fashion, thereby **quickly dealing with hard drive crashes or hardware theft**.

SCENARIO:

- Workstation replacement by machines with a pre-installed operating system
- Laptop assets replacement at the end of a leasing period
- Replacing a machine following a theft or breakage

PROTECTED TARGETS:

- Laptops, desktops and other user terminals
- File Servers

CHARACTERISTICS OF THIS RESTORE:

- Advanced restore for administrators only
- Restoring from backups

- 4 -

Restore in case of attacks by a cryptolocker virus

RESTORE BY TIME NAVIGATION

SCENARIO:

- A user knows he/she has lost files but does not know where or which files
- All the files on a workstation are locked by a crypto-locker

PROTECTED TARGETS:

- Laptops, desktops and other user terminals
- File Servers

CHARACTERISTICS OF THIS RESTORE:

- Restore accessible to users or administrators
- The restore can be performed on the workstation or remotely

This restore option is a favorite with many backup managers as it enables to find lost files with very little or no information (if users cannot remember the file name, type or date they last used it), or files that have been **attacked by a crypto-locker virus.** Missing files are identified within minutes by time navigation.

Earlier, we looked at a restore method guiding users with a wizard to let them to restore a file in a few clicks using a few snippets of information. In some cases, users will need more freedom to search:

- because they have no precise information to launch the wizard search, and will have to try to "guess" which files were lost or added between two dates,
- and/or because they are victims of a cryptolocker virus and need to move back through time to restore the files to a time preceding the attack.

Restore is done by means of an extremely simple interface. In the most complex cases, for example **in the case of the crypto-locking of all the files on the workstation, the administrator can even act in the user's place**: they also have the time navigation feature and the comparison of backups between two backup dates.

As a result, even annoying cases of crypto-lockers are solved quickly. Your users will waste minimal time before being able to resume their normal everyday activities.

So, you should now be better armed to choose **an effective "restore" solution** for your laptops and desktops because it can help you in both routine and complex restore situations, save you time and increase your efficiency.

Do you have a project?
Do you want to talk about it?

Contact the Atempo experts!

Contact us

Atempo solutions

- **Miria**: Backup, archiving, synchronisation, migration and copy solution specific to unstructured data and very large volumes - peta files and storage
- **Tina (Time Navigator)**: Backup and protection of servers and applications for data centres, remote sites and distributed environments
- **Lina (Live Navigator)**: Continuous data protection (CDP) solution for desktops, laptops and file servers

About Atempo

Atempo is an independent software company based in Europe with an established global presence, providing solutions to protect, store, move and retrieve all critical data for thousands of businesses worldwide. With over 25 years of experience in data protection, Atempo offers a complete range of proven solutions for backing up physical and virtual servers, workstations and migrating very large volumes of data between different storage systems. Atempo's three flagship solutions, Lina, Miria and Tina, are labelled "Used by the French Armed Forces" and "France Cybersecurity".

Selected as part of the French Tech 120 government program to create 25 unicorns by 2025, the company, headquartered in Paris, has a powerful network of value-added wholesalers, resellers, manufacturers, integrators and managed service providers.

Find out more

ATEMPO
preserving data ecosystems

For more information: www.atempo.com