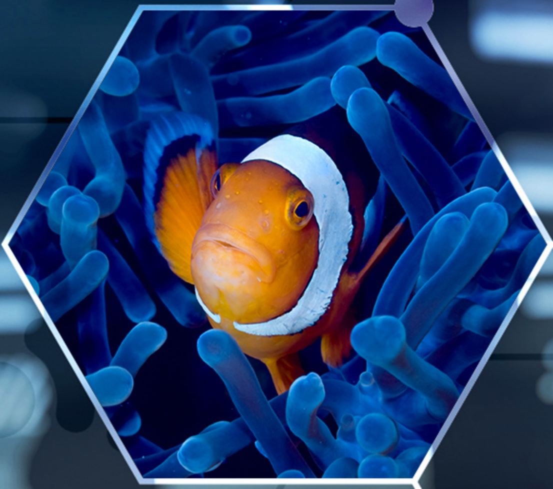
ATEMPO
preserving data ecosystems

WHITE PAPER

BACKING UP LAPTOP FLEETS:

NEW CHALLENGES



ATEMPO.COM

Do you know the old saying, **"It's too late to close the stable door after the horse has bolted"**?

The same happens with data. We wish we could back it all up once our computer has been stolen or lost in an airport. However, increasing numbers of employees work mainly on laptops likely and are likely to carry unsecured data somewhere on their laptop.

CONTENTS

How does losing a laptop affect a company?

While there are a thousand ways to lose data or lose a computer, the consequences are always the same: at best it is the frustration of having misplaced a few files, and at worst it is a tragedy, an irrevocable loss.

Some impacts:

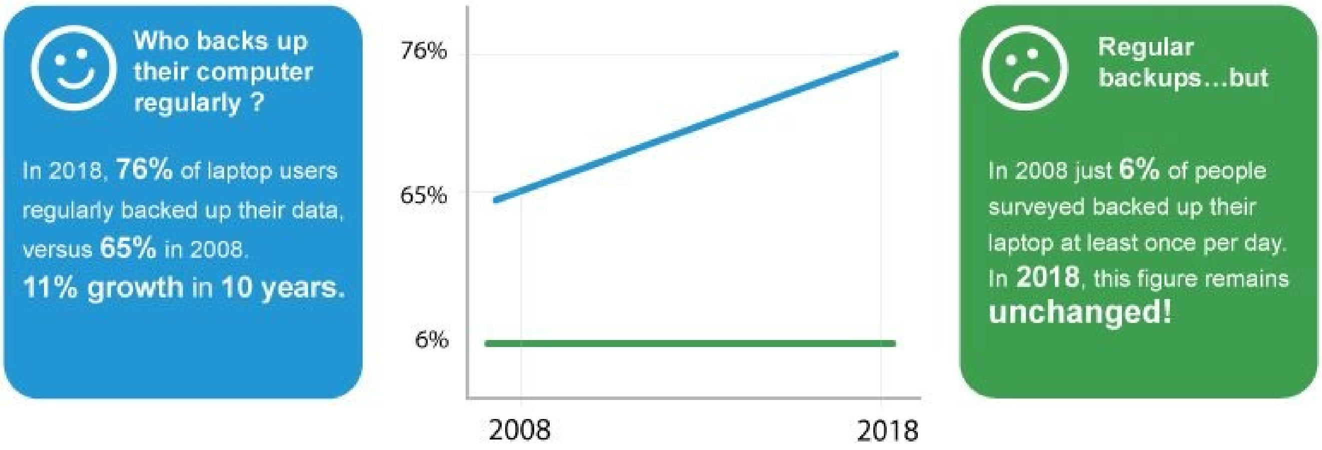
Financial Impacts
The cost of losing a laptop is far higher than the price of the replacement machine. The average cost of losing a laptop is estimated at around $50,000[1]. Leaked data and lost intellectual property make up 80% of this cost. The cost rises even further if the data has not been encrypted or if the laptop is not declared lost or stolen for several days.

Reputation Impacts
Aside from the expense, how embarrassing would it be for your business if a director lost a laptop at the airport a few hours before an important meeting with your investors? This scenario becomes a reality for more than 30,000 people in France each year. Less than 3% of these computers are recovered.

Productivity Impacts
Theft is not just an abstract concept, with around 10% of businesspeople having had a laptop stolen. This has a real impact on productivity for companies, causing losses of business and legal, technical and financial information.

Security Impacts
Cyber-attacks are increasingly a major cause of permanent data loss. Laptops, which often connect to less secure networks, are extremely vulnerable to this type of attack.

From the previous figures, it is absolutely clear that laptops must be protected, and frequently. A study[i] conducted over 10 years by the company Backblaze shows how behaviour has changed over time: in 2008 only 65% of laptop owners were performing regular backups. In 2018 this figure has risen to 76%. This is certainly better, but it implies that 24% of them still do not perform regular backups. Oops!


Who backs up their computer regularly ?

In 2018, **76%** of laptop users regularly backed up their data, versus **65%** in 2008.

11% growth in 10 years.

Regular backups...but

In 2008 just **6%** of people surveyed backed up their laptop at least once per day. In **2018**, this figure remains **unchanged!**

Figure 1- Backblaze 2008/2018 study on backup regularity

But there is a more serious problem here. Consider the notion of "regular backup".

- The same report shows that only 6% of respondents backed up at least once a day in 2008, and this figure had not increased in 2018.
- The study also indicates that more than half of respondents never back up their data or only back it up once a year or less. This is far from ideal.

94% **of users back up less than once a day**

Admittedly, these figures come from a study conducted among personal computer owners. It should be reasonably expected that professionals are more aware of the issue and have more resources.

However, this is not what we have observed in the field. Our experience shows that, all too often, laptops still escape corporate backups.

What is hindering the protection of laptop fleets in the workplace?

The good news is that the weakness of these figures leaves a huge margin for improvement in terms of protecting the company's assets and complying with legal constraints.

So, what makes it so difficult to implement an effective backup strategy for laptop fleets in the workplace?

Mobility

The fact that these computers are mobile necessarily poses a problem if the backup solution schedules the protection of a particular computer at a set time. While in the past this scheduling was justified by the allocation of scarce and costly resources (tape drives for example), the democratisation of disk storage has done away with this constraint. Many backup solutions now offer real-time protection that allows laptops to be protected much more effectively.

What slows down the deployment of backup solutions is their ability to "track" the movement of laptops outside the company's internal high-speed network. Two issues arise:

- How to secure the backup,
- How to manage data volumes with varied and often limited network speeds (home, hotel, airport or on a remote site of the company).

The complexity of securing backups

There are several possible approaches to securing the backup of these mobile computers once they are outside the company:

- Backing up to encrypted removable disks. This option poses its own significant risks of loss, breakage and theft.

- Creating a secure link from each computer to the company in order to perform the backup over an encrypted channel.

- Trusting a third party to host your data and back up your laptops for you.

The complexity of the issue of security for these laptops is often linked to the fact that having a laptop is still strongly correlated to the employee's position in the company. And often, the higher the position, the higher the "value" of the information to be protected will be.

Network weakness

Home offices and occasional sites have common problems of limited network capacity due to poor quality Wi-Fi connections and ADSL links with very limited upload capacity.

It isn't unusual to come across IT teams from companies that have deployed a real-time backup solution only to find that users have stopped their backups because they made the computer unusable. Machine and network resources were simply preventing them from working well!

Remote sites face a volume problem multiplied by the number of active laptops on the site: network occupancy peaks when the computers are connected, and their users want to access their messages or business applications.

Delegating

to the user as a last resort

Mobility, security and networks: three factors which when combined still lead far too many companies to give up on trying to back up their laptop fleets and delegate it to their users, with little or no instructions or follow-up. Yes, you read it right: to their users. This is real life. I am sure you can imagine what happens to the USB sticks and other portable hard drives that "secure" these computers...

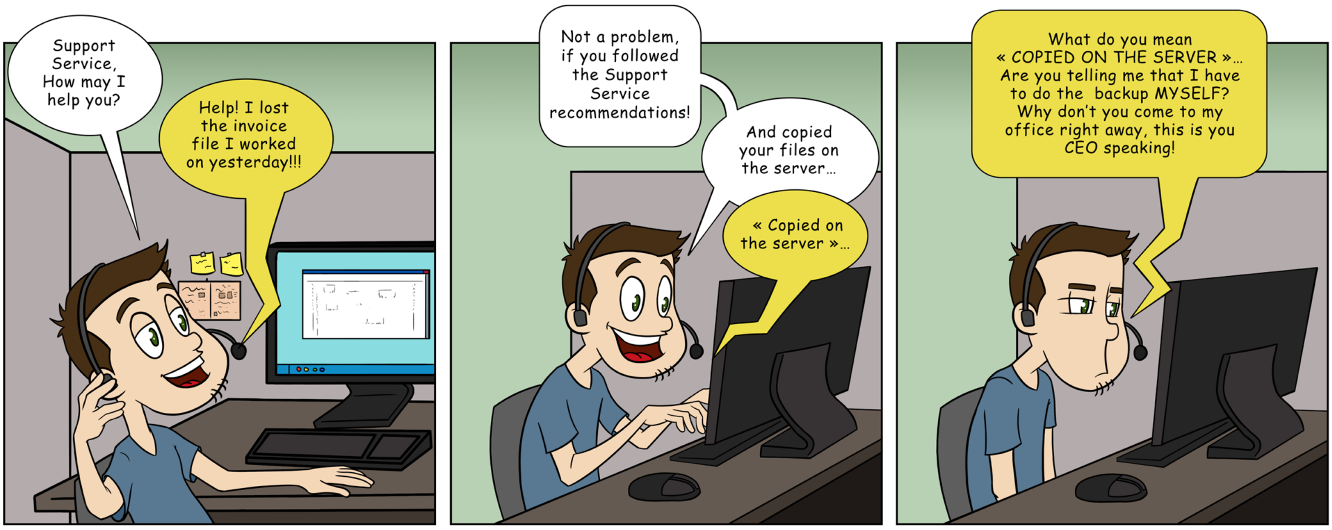
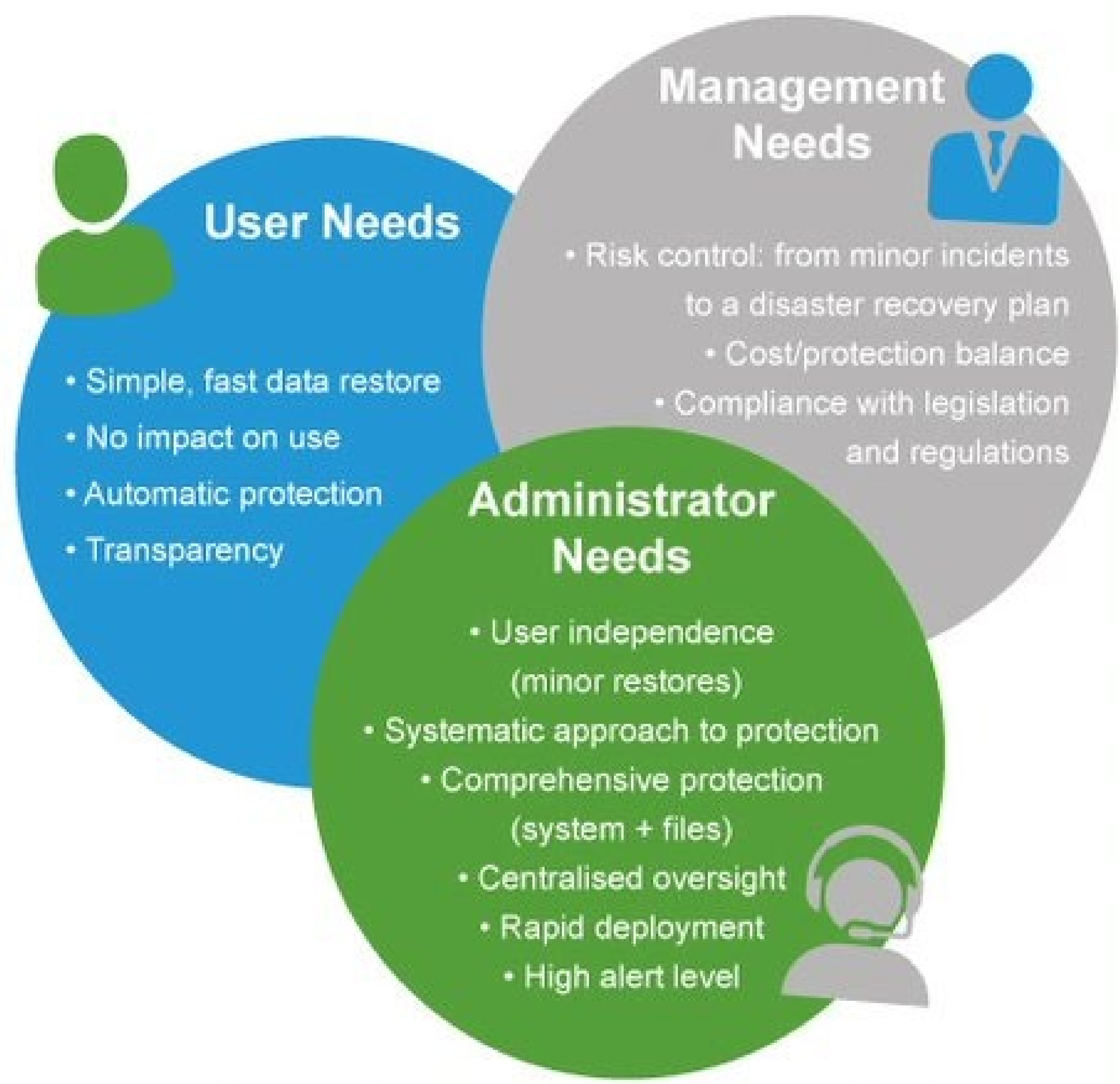

Support Service, How may I help you?
Help! I lost the invoice file I worked on yesterday!!!
Not a problem, if you followed the Support Service recommendations!
And copied your files on the server…
« Copied on the server »…
What do you mean « COPIED ON THE SERVER »… Are you telling me that I have to do the backup MYSELF? Why don't you come to my office right away, this is you CEO speaking!

Figure 2 - The limits of a backup policy "delegated" to users

Criteria for choosing a backup solution adapted to laptop fleets

Several parties are usually involved when it comes to choosing a solution to protect the company's laptops. Implementing the optimal strategy requires taking into account all their expectations without neglecting any of them.



User Needs

- Simple, fast data restore
- No impact on use
- Automatic protection
- Transparency

Management Needs

- Risk control: from minor incidents to a disaster recovery plan
- Cost/protection balance
- Compliance with legislation and regulations

Administrator Needs

- User independence (minor restores)
- Systematic approach to protection
- Comprehensive protection (system + files)
- Centralised oversight
- Rapid deployment
- High alert level

Checklist
of choices

The following checklist ensures that a backup solution is appropriate for protecting the laptop fleet of a company:

- □ Enabling to work on the move regardless of the network and without requiring user or administrator intervention.
- □ **Enabling to work continuously**, without imposed time slots, in a discreet and transparent manner for the user: it should avoid interruptions but must clearly indicate any alerts.
- □ **Quick** to deploy and configure.
- □ **Easy to monitor** / supervise: incidents and missed backups must be visible and reported.
- □ **Fast and simple restoration** to be carried out directly by the actual user. The administrator should not be solicited for this type of routine operations.
- □ **Complete protection**: files and operating system protection to enable the reconstruction of a replacement computer in a single consolidated step.
- □ **Restoring** files using a secure web interface **from anywhere** in the world.
- □ **Economical in the volume** of files to be transmitted to the server via the network.
- □ **Economical in central storage** by managing repeated files across several laptops.
- □ **Encrypting** backup communications and **authenticating** by SSL certificate.

Lina meets 100% of these needs - Testimonials

lina ATEMPO

AS USED BY FRENCH ARMED FORCES

All-in-one protection for mobile computer fleets
THE BEST DEFENSE AGAINST THEFT, CYBERCRIME AND DATA DAMAGE OR LOSS

Babolat

Ivan Audouard
Systems and Network Manager

*"Our needs are simple: **effective, user-friendly restore to protect laptops** from loss, theft and breakage**, transparent backup** for users that does not impact workstation performances, and minimum maintenance for the administrator, since the IT support team consists of just three people, based in France, serving the needs of the workforce worldwide."*

*"**Atempo support is great**, the products are great.*

If it takes us more than 5 minutes to install and make it run, we simply aren't interested!"

BARCHESTER
Celebrating life

Andy Giddy
Groupe IT Operations Manager

DUFRESNE CORRIGAN SCARLETT
ADVERTISING

Julien Brevière
IT Manager

*"If a salesperson loses or damages a laptop, we could lose contracts. With Lina, I'm not worried anymore. If I know that a file was on a laptop, I have a **backup ready to restore** from any point time and from any place.*

Lina, the admiral of your laptop fleet

- **Automated backup**:
  Backups are performed automatically and transparently for the user. Configuration is also automated through protection profiles predefined by the administrator.

- **Continuous backup**:
  Modifications of computer data are detected in real time. Depending on the criticality of the data, Lina allows you to set the cursor for sending data to the server from a continuous flow to a frequency of once a day.

- **Backup in deduplicated block mode**:
  In order to optimize disk storage and network bandwidth, every file created or modified is split into small blocks. Only new blocks are sent to the server, in small quantities.

- **Network / CPU optimisation**:
  Lina adapts to your network configuration and finds the best way to transfer data according to the bandwidth. The backup, with block deduplication, is complemented by the ability to limit the bandwidth used depending on the connection and to adapt the compression.

- **Seven restore modes**:
  Local, remote, crossed, web-based… Lina offers seven restore modes covering all the restore needs and scenarios of users and administrators.

- **Reconstruction of a complete computer**:
  Lina restores the most recent image of your computer, consolidating the system, applications and data.

- **Centralised administration**:
  A single administration console allows you to configure and supervise all the workstations in the fleet from a web browser.

- **Scalability of the software platform**:
  Setting up the backup of a new laptop takes 5 minutes to install the software and associate it directly with a predefined backup profile.

***

Seven ways to restore

Focus on key features of Lina

With Lina the focus is on restore facilities. Your users are granted full autonomy to restore their files, freeing up IT teams to focus on more essential tasks. However, if your company's policy is to let the administrator manage restores, this is also possible.

1. Restore via a wizard
2. Restore directly via Windows File Explorer or macOS Finder
3. Web restore
4. BMR (Bare Metal Restore) of an entire computer
5. Cross-restore
6. Restore by the administrator
7. Restore by Time Navigation

Saving costs

Through resource control via three-level deduplication

Lina answers the following double challenge:

- protecting **all** your users' valuable data
- while **reducing** the storage volume required for backup

Lina applies deduplication at three levels:

- at the source
- on the storage
- before sending (WAN mode)

Advantage no. 1: Saving network resources

Lina performs an initial backup of all the selected files. After this, only new or modified files are protected. All file modifications are detected by Lina and sent to the data repository. The power of the backup engine makes it possible to manage changes at the block level. This means that network and storage bottlenecks are a thing of the past.

Advantage no. 2: Saving server storage

Splitting files into blocks also helps to optimise storage space. Indeed, only new blocks are sent over the network and stored in the repository.

Protecting my laptop fleet – the final word

Your laptop could be stolen from a café terrace or a train in the blink of an eye. The same can be said of falling victim to a cyber-attack. The costs to the company (which finds itself without a recent backup of its unique and valuable data) are sometimes hidden but always high.

Lina is here to help, with an affordable and efficient solution.

[i] Source : Backblaze – 2018