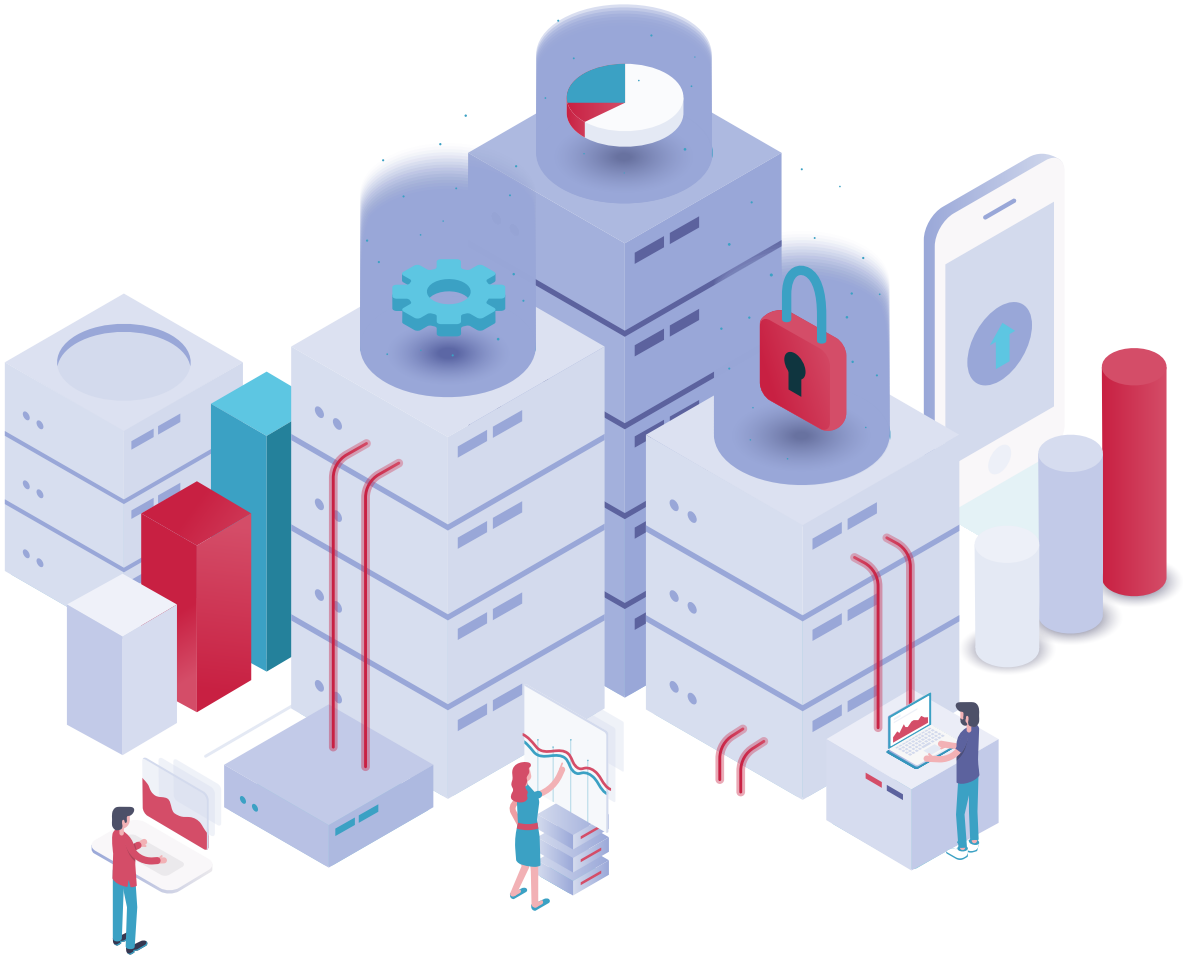
ninjaOne

Backup Solutions for a Changing Workplace

Table of Contents



Executive Summary

Modern workers rely on digital workplace tools to share, store, and collaborate on projects as they expect constant connectivity on any device from anywhere.

With the rise of ransomware and other prevailing threats like natural disasters, human error, and social engineering, you can't guarantee 100% access to data around the clock.

When organizations lack access to essential business data, they cannot operate and make money. But with the right data protection tools, you can ensure data is backed up and restorable.

In this report you'll find:

- A deep dive into the trends that are shaping the workplace in the 2020s out of the COVID-19 pandemic
- A comparison of on-premises and cloud backup solutions in distributed and hybrid workplaces
- The benefits of moving data backup to the cloud
- An outline of use cases for image and file and folder backup solutions

PART 1

The Changing Workplace

In 2022, the definition of workplace flexibility has changed. As a result, IT organizations must face the reality of three trends that have been progressing over the past decades that are now coming into the mainstream for the modern worker.

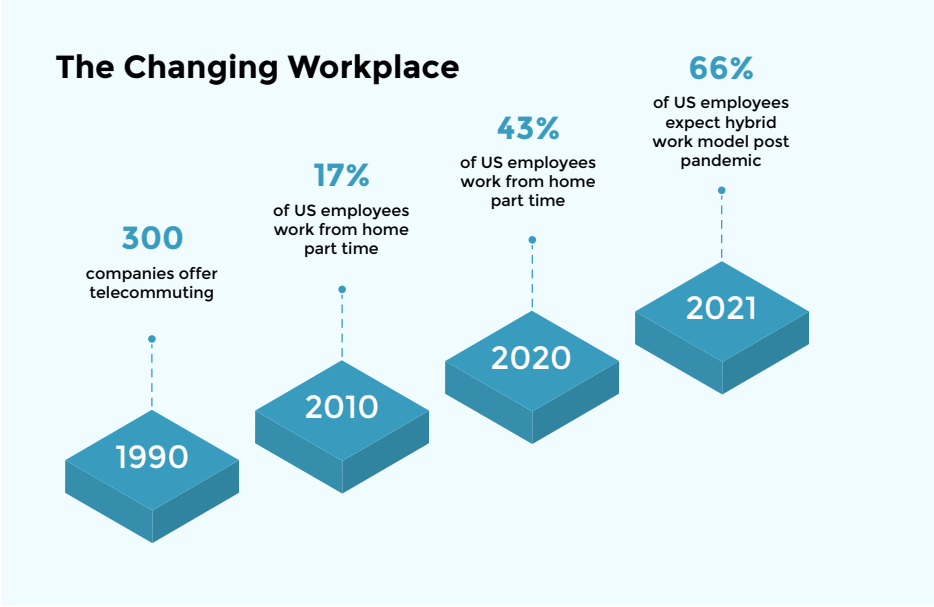


Image referencing survey data from We Work Remotely and FlexJobs

1. Post-2020, many companies are adopting a hybrid workplace approach

At the end of 2021, nearly 1 in 2 people (48%) said that if they were no longer able to work remotely, they would start looking for another job that offered more flexibility. (According to Owl Labs State of Remote Work 2021)

To combat the great resignation and give workers great flexibility, employees have turned to the hybrid workplace model that combines both traditional in-office working and remote working. In most hybrid workplaces, employees have the freedom to choose where they work and when they work, expanding operating hours beyond the classic 9-5.

PART 1

The Changing Workplace

According to respondents from our upcoming NinjaOne report on hybrid work, only 13% of those surveyed companies have implemented a formalized hybrid workplace policy that determines when an employee will work from the office and when they'll work from home.

The setup of a hybrid work environment depends on the company; some might have staggered schedules for when teams will work in-office, some have a portion of employees that work entirely in-office, and some that are fully remote, or it could be almost primarily office-based with just a handful of employees working remotely.

Whichever way a business organizes a hybrid model, the end goal is to maximize employee productivity and satisfaction while enabling employees to collaborate in and out of the office.

Depending on the organization, some might require the usage of a company device there, as others implement the "bring your own device" model (BYOD). For example, in NinjaOne's upcoming report on hybrid work, we found that 55% of hybrid workers use company devices, as 23% can use a personal and/or company device. In both scenarios, employees may be required to sign into a VPN.

2. For many, a fully remote model is here to stay

Remote and hybrid overlap by the numbers:

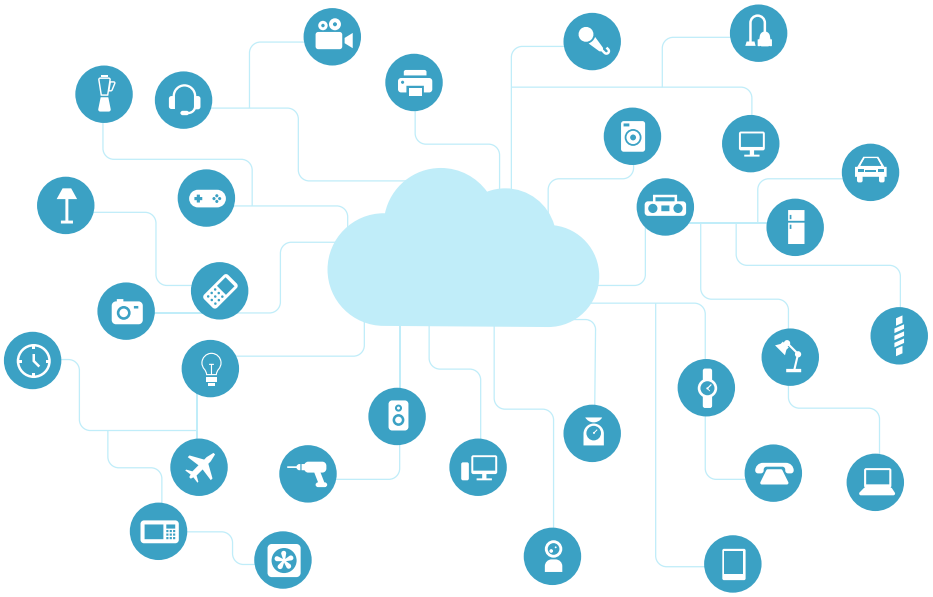
- "90% of remote employees say they are at the same productivity level - or higher - working from home compared to the office. "
  - *According to Owl Labs State of Remote Work 2021*

- "As of November 2021, the percentage of people working in hybrid and remote arrangements has increased to 58% (from 46% in May 2021) in the United States.
  - *According to Slack's Future-Forum Pulse Report*

Remote work allows employees to do their job from a different location than a centralized office operated by an employer. For example, some remote work locations include an employee's home, a co-working space, a private office space, or any other place that isn't the traditional corporate office space.

Telecommuting isn't a new phenomenon. It was introduced in the early 1990s for some executives and has continued to expand in the following decades. According to We Work Remotely, by 2010, 17% of office workers in the United States were working remotely. By the midpoint of 2020, this number had accelerated to 43% due to the COVID-19 pandemic.

3. A distributed workforce model creates new security concerns



A distributed workforce exists when an organization operates with employees working in multiple locations, including their homes, co-working spaces, a central office, and satellite offices. Pre-Pandemic, many larger corporations already operated a distributed model. Today's realities have also caused small and medium-sized businesses to adopt this model and have sped up their acquisition of collaborative remote software solutions.

Since the start of the pandemic, distributed workers have been using personal computers and other personal devices for work at a higher rate than ever before. According to findings from HP's Wolf Security study, "70% of office workers surveyed admit to using their work devices for personal tasks, while 69% are using personal laptops or printers for work activities." In addition, they also found that "one-third (30%) of remote workers surveyed have let someone else use their work device."

As the lines between home and office continue to blur, this has created entirely new cybersecurity risks ranging from gaming-themed malware to massive increases in phishing attacks.

Collaborative software solutions create the need for more flexible data backup.

Whether remote, hybrid, or distributed, a host of collaborative software solutions connect workers and enable them to work on projects together, hold virtual meetings, share files, and replicate the in-office experience no matter where they are. These tools withhold and share essential business data that must be backed up in the case of a natural disaster, cyber-attack, or accidental deletion.

Shortcomings of legacy on-prem solutions

For fully on-site businesses, backing up employee business data is easy — almost any solution will work so long as you can get a copy of the data off-site. Not only that, but the actual risk of data loss is also much lower. When devices aren't leaving the premises, the likelihood of data loss due to device theft, loss, or destruction is far lower.

But for hybrid and remote employees, the risk of data loss is far higher. Traditional network also or domain-based backup solutions pose significant challenges.

Other things to keep in mind include:

- No office = no company network and no on-prem storage options
- VPN usage can cause additional costs in terms of employee productivity and security
- For field employees, a VPN paired with on-prem backup simply doesn't work.

	On-Premises Solutions	Cloud Backup Solutions
Distributed Offices	■ Costly and complex architecture with centralized network gateways and storage points at each location ■ Hardware, maintenance and labor costs ■ Scalability, limited by hardware investment ■ Slow, time-intensive implementation	■ Infrastructure free ■ Built-in scalability ■ Fast efficient implementation ■ No hardware, maintenance or labor costs associated with infrastructure ■ Local-only storage options
Hybrid Workplace	■ Added monetary and productivity costs of VPN per user ■ Increased security risk if VPN is not implemented correctly	■ Seamless backups as endpoint transitions from on-site, to at-home, and office networks ■ Hybrid local and cloud storage options
Fully-remote workforce	■ Backup must be managed from on-prem ■ No direct access to endpoints	■ Automated backup on or off a VPN ■ Integrated with remote management tools for easy remediation ■ Cloud-only storage options

PART 2

5 Benefits of Moving to Cloud Backup

Clients and users don't care how or where their data was backed up; they just want it fixed and restored as fast as possible. In our changing workplace reality, cloud backup gives IT professionals the ability to remotely recover from any event, whether it's a cyberattack, accidental deletion, or natural disaster that makes on-prem recovery impossible.

1 **Protect essential data even in the case of a natural disaster**
On-premises backup solutions rely on hardware for local backups. In the case of a catastrophic natural disaster like a flood, fire, tornado, or hurricane, these local devices can be destroyed, and essential data lost as a result. With data backed up in the cloud, a business's physical infrastructure may be destroyed in the case of a natural disaster. Still, business data is secure in the cloud and can be quickly recovered to avoid costly downtime.

2 **Data is accessible and restorable from anywhere in the world**
With cloud backup, data is accessible and restorable from anywhere in the world with an internet connection. Restoring full programs or operating systems from the cloud might take time, but in the case that you need a few essential files, you'll be able to restore them in a timely fashion.

3 Connecting with a cloud backup provider may result in better security

From employees not using or failing to set up VPNs to staff sharing login credentials properly, there are many threats to on-prem backup. Businesses that partner with a secure cloud provider can avoid costly VPNs while enjoying better data security.

4 Ability to scale presenting upsell and cross-sell opportunities

Scaling on-premise backup can become a challenge as you'll need to install and maintain hardware at each location. Scaling cloud backup services can be done remotely and on-demand. Be careful with scaling quickly as your subscription price may significantly increase with some backup providers due to increased storage needs.

5 Less hardware maintenance = money saved

On-premise backup requires hardware that must be maintained and eventually upgraded to ensure the fastest recovery time objectives. With cloud backup, an organization doesn't need to worry about the cost of hardware maintenance, the cost associated with the software necessary to monitor backup hardware, and negotiations around businesses purchasing new hardware to stay in compliance and up to date.

Bonus = Pairing backup with RMM provides automation and tools that can prevent human error

Ninja deploys backup automatically, so you don't have to undertake or delegate deployment, saving techs time and limiting potential room for error. On top of this, RMM allows you to easily remote control into a device while identifying issues with one click from the same interface when something goes wrong.

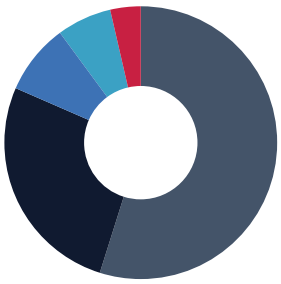
PART 3

Image v. File and Folder

Many MSPs and end-users believe that their data is safe and ready to recover with a file and folder backup solution. File and folder backup is excellent for retaining data over long periods of time, but it will not fully restore the operating system, including applications. Image backup offers a more complete disaster recovery solution if critical systems are compromised and need to be restored quickly.

File and folder backup will restore files, but not the applications that run them. This can impact the recovery time objective (RTO) for servers and complex computer systems and potentially be a business-ending event if application data is needed to maintain daily business operations.

When looking for a quicker restore of business data like text documents on a single laptop or workstation, file and folder backup might be the best way to avoid operating system mismatches and dissimilar drivers resulting from restoring to a new device.



	File & Folder	Image
System & Reserved	51 GB	51 GB
Applications	28 GB	28 GB
Business Data	3 GB	3 GB
Other	15 GB	15 GB
Backed Up	3 GB	97 GB
Cloud Storage Used	2.1 GB	68 GB

*Sample data from Employee Machine**

In this case, only 3% of the data on this device was backed up and restored using file and folder backup. This 3 GB of "business data'' makes up the documents that are essential to work and collaboration like text documents, presentations, and meeting recordings. The other 97% of this data was not backed up as it is not essential to full recovery in this single workstation use case.

PART 4

Protect the Changing Workplace with Backup

Backup flexibility is critical in the hybrid work world. Employees expect their data to be backed up and restorable as they seamlessly transition from working on-site to their home office or even to the office on the company network. Backup has always been an essential pillar for business reliance, but the continued spike in ransomware and other threats to data backup continues to be that last line of defense when it comes to cyber security.

In 2022, pairing your backup solution with your remote monitoring and management system can provide visibility and help prevent some of the risks of human error when it comes to backup.

PART 4

Protect the Changing Workplace with Backup

Can Ninja Data Protection be your solution?

Ninja Data Protection is built to help you protect critical business data for today's distributed workforce. Backup endpoints wherever they are with flexible solutions that meet your data protection, cost, and RTO objectives every time.

Ninja Data Protection has provided our technicians with an intuitive backup solution that allows them to focus more on supporting our clients and less on unreliable and disjointed backup systems"

Jesse Vella, Network Engineer

Key Features:

- Full image or file-only backup options
- Flexible data protection and retention policies
- Bare metal, file, and self-service recovery
- Ransomware resistant backup and storage
- Incremental block-level backup technology
- Proactive backup status and activity alerting

TRY NINJA DATA PROTECTION FOR FREE

ninjaOne