CLEVIR

We are Clevir!

CLEVIR

We are Clevir

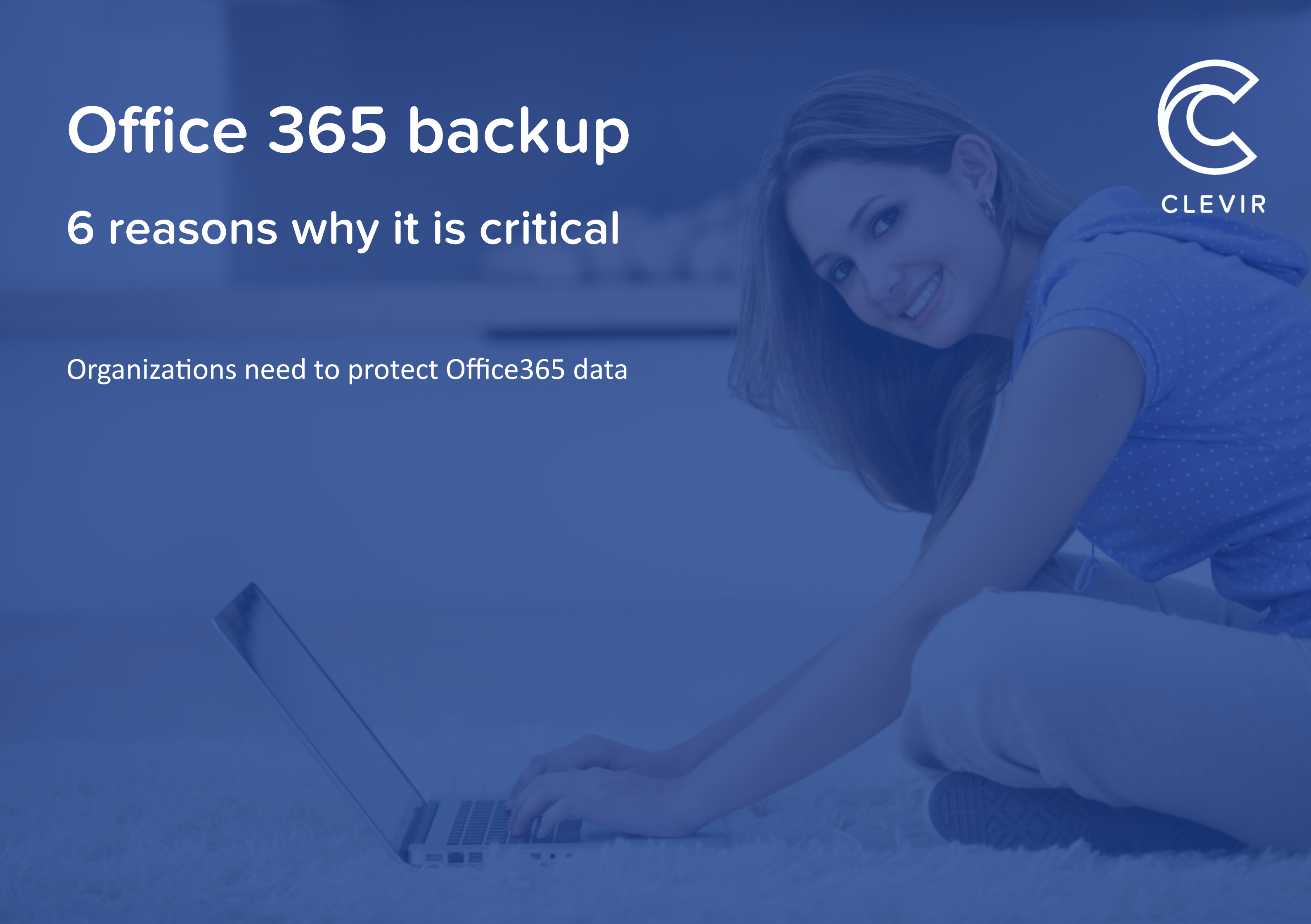
We believe in Virtual Workspaces for the Real World.

Workspaces that let users and platforms collaborate and communicate.

This way we can truly improve security, productivity, manageability and user hapiness.

More information

Get in contact



CLEVIR

Office 365 backup

6 reasons why it is critical

Organizations need to protect Office365 data

CLEVIR

Do you have control of your Office 365 data?

Do you have access to all the items you need?

Really?

Microsoft takes care of quite a bit, and provides a great service for their customers. However, Microsoft's primary focus is on managing the Office 365 infrastructure and maintaining uptime to your users. They are empowering YOU with the responsibility of your data.
The misconception that Microsoft fully backs up your data on your behalf is quite common, and without a shift in mindset, could have damaging repercussions when this responsibility is left unattended.

Ultimately, you are responsible to have access to, and control over your Exchange data (mail, calendar & contacts) and your OneDrive data.

CLEVIR

Microsoft takes care of the infrastructure,

but the data remains the customer's responsibility!

As a robust and highly capable Software as a Service (SaaS) platform, Microsoft Office 365 fits the needs of many organizations perfectly. Office 365 provides application Availability and uptime to ensure your users never skip a beat, but an Office 365 backup can protect you against many other security threats.

You Might be thinking "The recycle bin is probably good enough." This is where many people get it wrong.

Six vulnerabilities in data protection rise to the top:

- Accedential Deletion
- Retention policy gaps
- Internal Security threats
- External Security threats
- Legal & Compliancy requirements
- Managing Hybrid email

#1
Accedential Deletion

If you delete a user, whether you meant to or not, that deletion is replicated across the network, along with the deletion of their Exchange data site and their OneDrive data.

Native recycle bins and version histories included in Office 365 can only protect you from data loss in a limited way, which can turn a simple recovery from a proper backup into a big problem.

There are two types of deletions in the Office 365 platform, soft delete and hard delete. An example of soft delete is emptying the Deleted Items folder. It is also referred to as “Permanently Deleted.” In this case, permanent is not completely permanent, as the item can still be found in the Recoverable Items mailbox.

A hard delete is when an item is tagged to be purged from the mailbox database completely. Once this happens, it is unrecoverable, period.

#2
Retention policy gaps

The fast pace of business in the digital age lends itself to continuously evolving policies, including retention policies that are difficult to keep up with, let alone manage. Just like hard and soft delete, Office 365 has limited backup and retention policies that can only fend off situational data loss, and is not intended to be an all-encompassing backup solution.

Another type of recovery, a point-in-time restoration of mailbox items, is not in scope with Microsoft. In the case of a catastrophic issue, a backup solution can provide the ability to roll back to a previous point-in-time prior to this issue and saving the day.

With an Office 365 backup solution, there are no retention policy gaps or restore inflexibility. Short term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips making data recovery fast, easy and reliable.

#3

Internal security threats

The idea of a security threat brings to mind hackers and viruses. However, businesses experience threats from the inside, and they are happening more often than you think. Organizations fall victim to threats posed by their very own employees, both intentionally and unintentionally.

Access to files and contacts changes so quickly, it can be hard to keep an eye on those in which you've installed the most trust. Microsoft has no way of knowing the difference between a regular user and a terminated employee attempting to delete critical company data before they depart. In addition, some users unknowingly create serious threats by downloading infected files or accidentally leaking usernames and passwords to sites they thought they could trust.

Another example is evidence tampering. Imagine an employee strategically deleting incriminating emails or files — keeping these objects out of the reach of the

#4

External security threats

Malware and viruses, like ransomware, have done serious damage to organizations across the globe. Not only is company reputation at risk, but the privacy and security of internal and customer data as well.

External threats can sneak in through emails and attachments, and it isn't always enough to educate users on what to look out for — especially when the infected messages seem so compelling.

Exchange Online's limited backup/recovery functions are inadequate to handle serious attacks. Regular backups will help ensure a separate copy of your data is uninfected and that you can recover quickly.

#5

Legal & Compliancy requirements

Sometimes you need to unexpectedly retrieve emails, files or other types of data amid legal action. Something you never think it is going to happen to you until it does. Microsoft has built in a couple safety nets, (Litigation Hold) but again,
these are not a robust backup solution capable of keeping your company out of legal trouble. For example, if you accidentally delete a user, their
on-hold mailbox, personal SharePoint site and OneDrive account is also deleted.

Legal requirements, compliance requirements and access regulations vary between industries and countries, but fines, penalties and legal disputes are three things you don't have room for on your to-do list.

#6

Managing Hybrid email

Organizations that adopt Office 365 typically need a window of time to serve as a transition window between on-premises Exchange and Office 365 Exchange Online. Some even leave a small portion of their legacy system in place to have added flexibility and additional control. These hybrid email deployments are common, yet pose additional management challenges.

The right Office 365 backup solution should be able to handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

Conclusion

CLEVIR

Go ahead and take a closer look. There are security gaps you may not have been aware of before.

You already made a smart business decision by deploying Microsoft Office 365, now find a backup solution that offers you both complete access and complete control of your Office 365 data and avoid the unnecessary risks of data loss.

Clevir365 Office365 backup tool available from € 1 per month as an add-on to the Clevir Workspace.

Protect your intellectual assets

When it comes to data security, businesses should take full responsibility to control their precious data and protect against human errors or malicious at-

Hold data for compliance and legal purposes

With industry regulations in place, organization often face the challenge of data retention. On the long run, however, the space storage needed could incur significant costs.

Optimize the process for data restoration

As data on Office 365 might take considerable time and effort to restore, it is crucial to enhance restoration efficiency and minimize work disruption.

CLEVIR

We are Clevir

More information

Get in contact

De Gruyterfabriek
Veemarktkade 8 / Unit 7238
5222 AE ‘s-Hertogenbosch
+31 (0)88 23 56 633

www.clevirsolutions.com
info@clevirsolutions.com