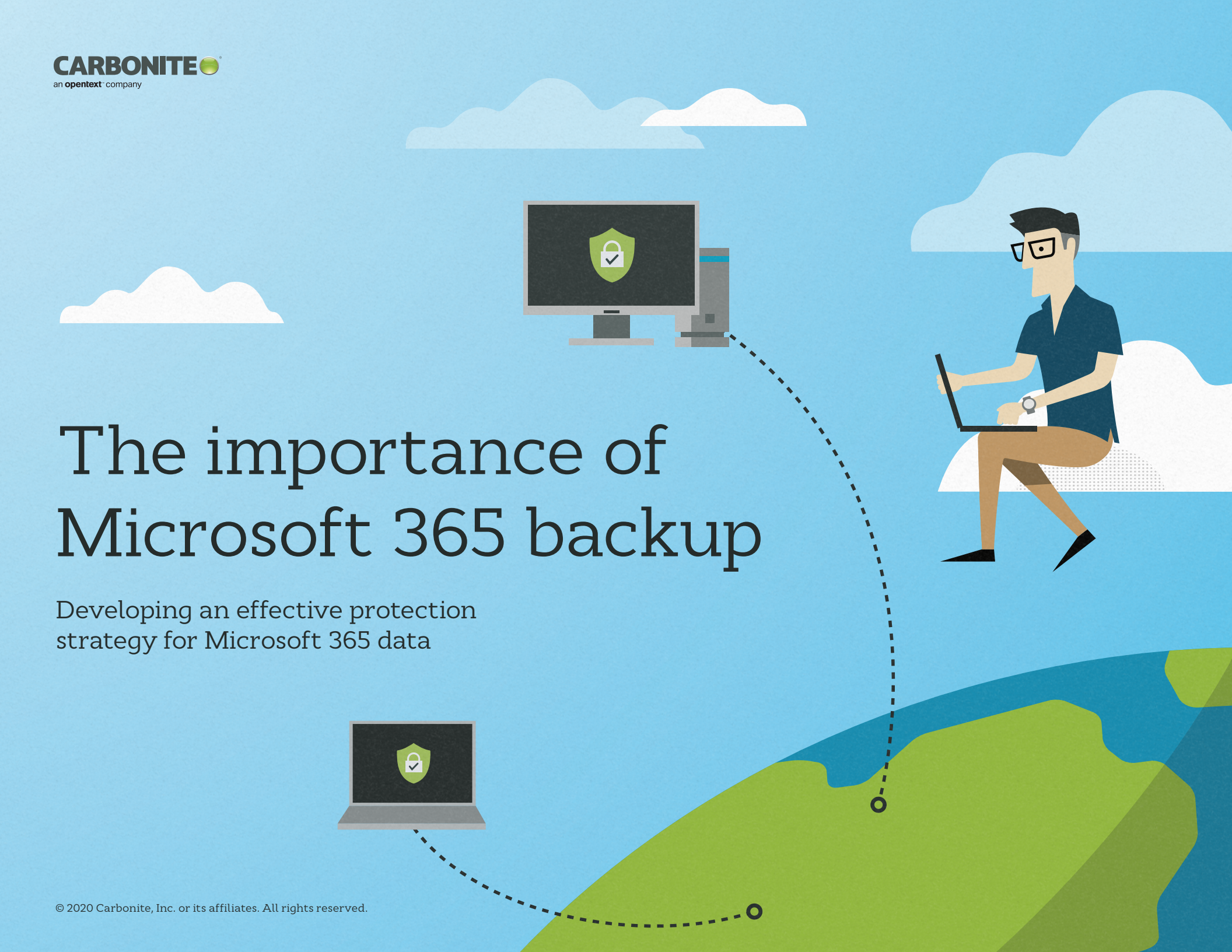
CARBONITE
an opentext company



The importance of Microsoft 365 backup

Developing an effective protection strategy for Microsoft 365 data

Developing an effective protection strategy for Microsoft 365 data

SaaS productivity apps like Microsoft 365 just make sense in today's mobile world—the benefits of easy access to documents from any device and improved collaboration are obvious. However, many organizations believe that moving to Microsoft 365 means backup is no longer necessary. According to a recent Enterprise Strategy Group report, one in four businesses don't believe they need to back up Microsoft 365.

Some of the confusion might be due to the fact that Microsoft 365 offers some safeguards to prevent data loss. Others simply believe that because data is in the cloud, it is automatically backed up. Still others believe that Microsoft OneDrive file sync is a replacement for backup. These are all misconceptions. Backup is equally important for Microsoft 365 as it is for onsite deployments of Microsoft applications.

In this e-book, you'll learn the most common causes of data loss in Microsoft 365, why relying on the Recycle Bin or OneDrive isn't enough, and what you can do to protect your organization's essential Microsoft 365 data.

Microsoft 365 vulnerabilities

Microsoft's data protection policies do not guarantee complete and fast restores of deleted or corrupted Microsoft 365 data. In short, Microsoft ensures that it won't lose your data. However, Microsoft doesn't make any guarantees about recovering it.

Obviously, this is a problem. Being unable to recover critical business information can result in lost revenue, lost customers and reputation damage. And, if your business is subject to data retention requirements, data loss can even have legal implications.

As noted above, Microsoft 365 data is subject to many of the same vulnerabilities as data hosted onsite. Let's take a look at the most common ones:

Accidental deletion:
First, and most obvious, is accidental deletion—an employee mistakenly deletes a file or folder. Users can easily delete data and conversations in SharePoint, Groups or Teams—or overwrite versions of existing data. Data deletion isn't the end of the world if is noticed right away. You can restore from the Recycle Bin. However, deleted files are only held in the Recycle Bin temporarily.

Malicious deletion:
In some cases, data deletion isn't accidental. Disgruntled employees may intentionally delete their own files or files in shared folders before leaving the company. Or an outsider might gain access to Microsoft 365 files and folders via a stolen laptop with a weak password. Worst case scenario: a Microsoft 365 global administrator wipes user accounts on his way out the door and locks other admins out.

When important files are lost due to accidental or malicious deletion, productivity is obviously impacted. This isn't merely an inconvenience. When employees can't perform their normal tasks, revenue loss is inevitable. And, if your organization is subject to data retention requirements, there may be legal implications, as well.

Ransomware (and other malware):
Another common misconception about Microsoft 365 data is that it is safe from ransomware and other types of malware. This definitely is not the case. Ransomware can lock Microsoft 365 files in the cloud to impact many users. Here's how: A user accidentally downloads ransomware to their laptop and local files are infected. If users have OneDrive sync turned on, infected files are immediately copied to the cloud. And it doesn't stop there. Ransomware is designed to spread across networks via shared files and folders. Since OneDrive is designed for collaboration, it can be particularly vulnerable to this type of attack.

Customization issues:
Microsoft 365 customization offers a lot of benefits, however custom designs, solutions, workflows, branding and other modifications to user-facing sites introduce the potential for technical faults and glitches. This means customization may need to be rolled back once errors have been found. Depending on the system affected, data loss can result in hours, or even days, of downtime.

OneDrive is not backup

Since OneDrive stores a copy of a user's files in the Microsoft cloud, many people believe that it is a replacement for backup. However, using OneDrive as a form of backup can result in data loss. Here's why: If a file is deleted or infected on a local device, that change is automatically synced in OneDrive. In other words, the file is automatically deleted or infected on all synchronized devices.

Microsoft 365 retention gives organizations control over what files are kept and for how long. Retention policies can be based on the creation or last modified date, file type or keywords, among other criteria. This can help organizations meet regulatory requirements around data retention and reduce risk in the event of litigation or a security breach. However, Microsoft 365 retention settings vary among Microsoft 365 applications, and some apps, like Microsoft Teams, do not have native retention capabilities.

OneDrive does offer some restore capabilities via the Recycle Bin. However, the Recycle Bin lacks many of the characteristics of a true backup:

- File versions are not immutable, isolated recovery points. So, if an active file is deleted, all the older versions of the file are deleted as well. If files are deleted permanently from the Recycle Bin, there is no way to restore.
- It doesn't enable centralized management of user data. In other words, it doesn't give IT control of backup and recovery.
- It doesn't maintain consistent recovery points across files, folders and users, so a large restore is a time-consuming, manual process. For example, to restore following a ransomware attack, a user would need to manually search for the proper restore points and restore each file one by one.

Again, this isn't just an inconvenience. All of this takes manual intervention, which takes IT and/or employees away from their normal tasks. As noted above, business downtime results in revenue loss.

Developing a Microsoft 365 data protection strategy

A Microsoft 365 protection strategy starts with employee education. Most cyberattacks originate with phishing or malicious web sites, so it is important that employees understand how to identify phishing emails, and whom to alert if they encounter suspicious email. Additionally, it is essential to create and enforce guidelines around safe Internet use. Finally, teach employees about the importance of strong passwords and how to create and manage them.

Antivirus protection is also crucial. Since viruses and malware can easily spread from a local machine to data hosted in the cloud, IT security measures are an essential piece of Microsoft 365 protection. Ransomware is constantly being modified to avert detection, so be certain that you keep antivirus software up to date, as well. Some antivirus solutions are cloud-based, which means that updates occur automatically. This can be beneficial from a management standpoint.

Backup is the best way to protect against accidental or malicious file deletion, other user errors, ransomware and data corruption. Microsoft's native tools offer some protection, but third-party backup solutions ensure that you can restore quickly and meet data retention and sovereignty requirements for all Microsoft 365 data.

Not all Microsoft 365 backup tools are created equally. In fact, most don't offer protection for the entire suite of products—for example, many lack support for Microsoft Teams. Others don't offer granular and permissions restores. So, when you are choosing a backup product for Microsoft 365, be certain that it protects everything you need it to. Carbonite® Backup for Microsoft 365 protects the entire Microsoft 365 suite, including Teams, OneDrive, Exchange, SharePoint, Planner and Skype for Business.

Some Microsoft 365 backup tools have features that can help meet governance and compliance needs, such as GDPR requirements. For example, Carbonite® Backup for Microsoft 365 offers a dedicated Privacy dashboard, giving users "right to be forgotten," DSAR processing, auditing and data purge controls.

Finally, establishing a Microsoft 365 backup strategy can also help reduce retention costs. If your organization must retain user data for a specific amount of time, maintaining former employees' Microsoft 365 licenses can get expensive. Carbonite® Backup for Microsoft 365 allows them to retain their files and email at a fraction of Microsoft licensing costs.

Contact us to learn more about Carbonite® Backup for Microsoft 365:

Phone: 877-542-8637
Email: partners@carbonite.com

About Carbonite and Webroot
Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.