CARBONITE an opentext company | WEBROOT an opentext company

How Secure is Your Cloud Data?

With employees working remotely at higher rates, business data is increasingly at risk.

The global COVID-19 pandemic has caused a massive shift to remote work. According to one estimate, the number of days spent telecommuting has risen 49% since the pandemic.[1] While the pandemic may have triggered the shift, there's no sign things will return to normal once the crisis fades. In a recent survey, 83% of respondents said flexible work policies will remain in the foreseeable future.[2] It's obvious why – productivity has been the same or higher according to 94% of employers.

49%
Rise in number of days spent telecommuting since COVID-19

83%
Survey respondents who say flexible work will remain in place

94%
Employers who say productivity has been the same or higher

While remote work and productivity rates are high, the same can't be said about the security of cloud data that remote workers generate. In most cases, the home networks, personal devices and cloud apps that remote workers are using are less secure than their on-premises counterparts. Cloud productivity applications, like Microsoft 365, have made the transition to remote work a seamless affair. However, IT administrators are now responsible for maintaining the same high level of security for data that's more dispersed than ever, and on networks that lack the same robust protection as office networks.

When IT organizations deploy Microsoft 365, they absolve themselves of the responsibility for maintaining a complex network of hardware and infrastructure interdependencies. But what they lose in the process is granular control over the containers that hold their business data. As long as everything is running smoothly, there's no cause for concern. Challenges arise, however, when everyday data loss strikes: a disgruntled employee wipes his OneDrive clean, and empties out the Recycle Bin for good measure; someone resets permissions across an entire SharePoint collection site; or routine employee turnover leads you to pay for Exchange seat licenses you don't really need.

70%
Businesses that have lost data in SaaS environments

35%
Organizations that are only partially familiar with SaaS SLAs

33%
Businesses that think SaaS apps don't need to be backed up

37%
Organizations that rely on their SaaS vendor for data protection

There's a wide misconception that deploying in the cloud removes risk mitigation responsibilities from IT. Studies show that at least 70% of businesses have experienced some degree of data loss in Software as a Service (SaaS) environments like Microsoft 365.[3] Confusion in the cloud puts businesses at a higher risk for data loss as they rapidly shift operations to SaaS environments. According to research, 35% of businesses say they're only partially familiar with their SaaS providers' service level agreements (SLAs). Even more concerning, 33% of businesses think SaaS applications don't need to be backed up at all, while 37% rely solely on their SaaS provider to protect their application data.

SaaS providers, like Microsoft, are only responsible for the availability of their infrastructure and services, not the data their customers keep in the cloud. For everyday data loss scenarios, like accidental or malicious deletion or overwriting permissions, it's the business that will have to perform recovery when data loss occurs. And, without a complete toolset for performing different types of recovery, the process will be much more manual and error-prone than the same operation performed with purpose-built tools.

In many scenarios, IT could save time and resources by supporting SaaS applications with data protection solutions that include robust disaster recovery functionality rather than just getting by with the limited functionality that exists in certain SaaS platforms.

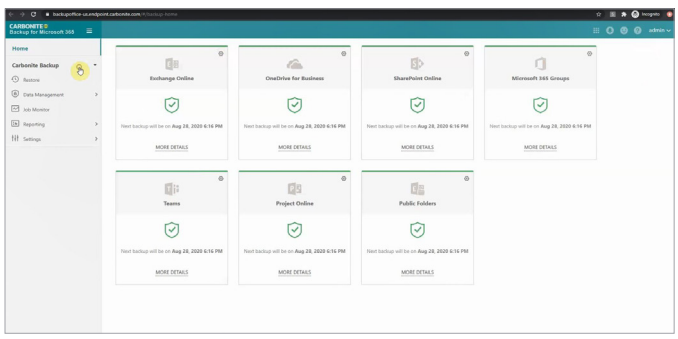
Data Loss in OneDrive

OneDrive is what's known as a file sync-and-share tool. It's very useful for its stated purpose, which is to mirror folders in the cloud and enable employees to share those files. These features are also why OneDrive is categorized as a collaboration and productivity tool. What OneDrive is not designed for is backup and recovery because it lacks a complete feature set for performing flexible disaster recovery. A true backup solution gives IT administrators multiple options for recovering files, folders as well as system state information. Depending on the nature of the data loss scenario, these features can simplify the recovery process and reduce the time it takes to recover data, also known as the Recovery Time Objective (RTO).

93
days
Recycle Bin default retention policy

With OneDrive, if a file is deleted – whether maliciously or accidentally – the likely course of action is to look in the OneDrive Recycle Bin for the deleted file. Depending on how much time has elapsed since the file was deleted, the file may or may not be there. OneDrive has a default retention policy; once the retention period has passed (or if the person who deleted the file also deleted it from the Recycle Bin) the file will not be recoverable without a third-party backup solution.

Performing large-scale file or folder recovery can be very time-consuming using any process that involves multiple manual steps. A purpose-built backup and recovery tool automates many of the steps associated with complex disaster recovery scenarios. Purpose-built backup enables both file and folder recovery through an administrative dashboard.



The dashboard also includes point-in-time recovery options that are enabled through a backup scheduling feature. By scheduling more frequent backups, administrators are able to shrink the window where data loss can occur, also known as Recovery Point Objective (RPO). Most file sync-and-share tools, because they're not designed for backup, lack these features that are standard in a purpose-built backup solution.

The same features that make file sync-and-share so convenient inadvertently make it easy for malware to propagate. If a user clicks on a malicious link in an email, not only will local files become infected with malware, but those corrupt files will also sync to the cloud, leaving the administrator without a clean recovery point. The result is the files will be lost permanently or, in the case of ransomware, the company will have to negotiate a ransom to obtain a decryption key.

90%

Newly created coronavirus domains that are scammy[4]

Backup sets with Carbonite® Backup for Microsoft 365 are immutable, which means they cannot be altered by ransomware thieves or anyone else. This helps ensure IT administrators have access to safe recovery points in the cloud if local files ever become infected. Ransomware incidents are on the rise, with deceptive new coronavirus-themed variants emerging. Users, especially remote workers on unprotected personal home WiFi networks, are especially vulnerable to these types of attacks.

SharePoint Permissions and Site Collections

IT administrators also need to be mindful of the same file deletion, corruption and sync issues when managing SharePoint environments. Site collections are equally subject to the Recycle Bin retention policy, which means deleted sites are unrecoverable beyond the retention period.

SharePoint permissions can also be deleted or broken, leaving the entire site inaccessible to certain groups, or even the administrator themselves. In most cases, there is no native functionality that will restore access to these sites. However, Carbonite® Backup for Microsoft 365 uniquely enables administrators to restore the security settings if permissions become corrupted or otherwise make the site inaccessible.

The solution also gives administrators the ability to restore an entire site collection, document or library, whichever is necessary to reverse the damage. There's also the ability to export the contents of a site, collection, document or document library to another location for archival purposes if necessary.

Recovering Teams Conversations

Today's remote workforces are relying more than ever on telecommunications platforms like Microsoft Teams for chat and videoconferencing. The more employees interact and conduct business on Teams, the more critical it is for IT administrators to protect the data that resides in Teams. Equally important is the ability to easily restore conversations without having to resort to multiple manual steps. However, restoring conversations in Teams is, in fact, a manual and labor-intensive process. In many cases, the original post cannot be recovered, or it can only be pasted as a comment
in another post.

With Carbonite® Backup for Microsoft 365, the IT administrator is able to restore Teams backup data to its original location. If a Group in Teams has been deleted from the original location, the admin is able to recover the Group in Teams and the permissions of the owner and all its members.

Carbonite® Backup for Microsoft 365 also allows you to restore a soft-deleted Group in Teams from the Microsoft 365 Recycle Bin to its last known healthy state. Carbonite will perform a check for the status of the Group in Teams to ensure Microsoft has this data, and provide options for recovering it, including using the Microsoft native restore function within the retention period, or using Carbonite backup data to roll back the entire Team, or even granular contents if desired.

Handling Exchange Mailboxes

When employees leave, the company has to decide how to handle the departed employee's Exchange Mailbox. Although it costs a lot to keep paying for licenses just to hold onto mailboxes, a lot of companies do just that. Some companies place the emails into a shared mailbox, which is not ideal for a number of reasons. There are size limits that, if exceeded, will still necessitate an assigned license. It also leaves the mailbox open to deletion, which defeats the point of archiving. If the IT admin assigns the former employee's license to a new employee, all data for the old employee will be lost.

Archiving workarounds fall short for a number of reasons. That's why the best way to archive is by using tools designed for this purpose. With Carbonite® Backup for Microsoft 365, IT administrators can simply export mailbox content in a Personal Storage Table (PST) as part of a standard end user offboarding process. Mailboxes can be exported to another location, such as another user's mailbox. This is helpful in the event a mailbox is inadvertently deleted and needs to be recreated from scratch. Mailboxes can also be imported into an e-discovery tool for litigation purposes.

Complete Portfolio Protection

Even prior to the COVID-19 pandemic, businesses were rapidly shifting their workforces to Microsoft 365 cloud apps. Now, with more employees working remotely than ever, cloud platforms and cloud collaboration tools have become essential to business operations.

While businesses have long enjoyed a comprehensive toolset for protecting and recovering data on-premises, they have not had access to the same flexible recovery options when it comes to cloud apps like Microsoft 365. With businesses lacking a clear understanding of Microsoft SLAs, it leaves much of the data that remote workers rely on to stay productive vulnerable to a range of risks. Collaboration and productivity apps, while highly effective for their stated purpose, are not designed for disaster recovery.

Carbonite® Backup for Microsoft 365 protects the entire suite of Microsoft 365 apps. It gives IT organizations the tools they need for the kinds of data loss scenarios they face on a routine basis. This saves time and resources anytime someone accidentally deletes a file in OneDrive, alters permissions in SharePoint, or when employees leave and their important business communications need to be preserved.

While the public health crisis will eventually fade, flexible remote work arrangements are likely here to stay. Remote workers may continue to be as productive as before, or better, but only if their cloud data and applications are safe from the common causes of data loss.

Contact us to learn more – Webroot EMEA
Email: carb-salesemea@opentext.com
Phone: 1 800 303 388

Contact us to learn more – Webroot APAC
Email: carb-apac_sales_team@opentext.com
Phone: 1 800 013 992

1. Gallup, U.S. Remote Workdays Have Doubled During Pandemic
https://news.gallup.com/poll/318173/remote-workdays-doubled-during-pandemic.aspx

2. Society for Human Resource Management, Study Finds Productivity Not Deterred by Shift to Remote Work, https://www.shrm.org/hr-today/news/hr-news/pages/study-productivity-shift-remote-work-covid-coronavirus.aspx#:~:text=Ninety%2Dfour%20percent%20of%20800,with%20their%20employees%20working%20remotely

3. Enterprise Strategy Group, Data Protection Cloud Strategies (June 2019)

4. ZDNet, COVID cybercrime: 10 disturbing statistics to keep you awake tonight (September 2020), https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/

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.