arcserve®

eBook

DON'T GET CAUGHT ASSUMING

How to protect Microsoft Office 365 data

arcserve®

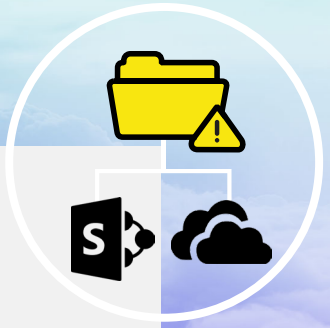
eBook

YOUR ORGANIZATION IS ONE OF THE 56% OF BUSINESSES THAT USE MICROSOFT OFFICE 365

Office 365 allows your employees to work anywhere, anytime – and your organization is dependent on it for email communication, team collaboration and document retention.

But while Microsoft does an excellent job at taking care of the infrastructure for these services, it's a misconception that they also take care of your data in the way you might expect. Read on to see if your business is at risk with security gaps you may not be aware of and learn how to gain control over your Office 365 data.

SCENARIO 01



Your engineering team hosts critical development files on both OneDrive for Business and SharePoint Online, and you need to access files from a project that took place several years ago. Unfortunately, one of your colleagues accidentally deleted your team's folder, along with all the documents you need for an upcoming product release. In desperation, you quickly check the recycle bin to recover the deleted files, only to find the documents aren't there, either.

Assumption:

Office 365 items are backed up by Microsoft for long-term retention.

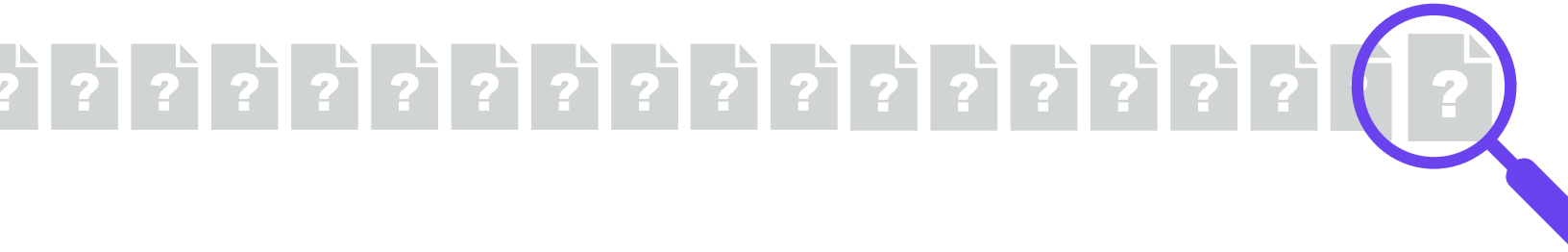
Reality:

Items in Office 365 are retained for only 90 days in the recycle bin but can be emptied at any time, making the data completely unrecoverable.

And, even when data is retrievable, point-in-time recovery is out of scope for Microsoft, leaving you with no other choice but to recover the latest version available in the recycle bin with all modifications you may not want. Further, retention policies vary for each application in the cloud platform, making the process of recovering deleted items even more cumbersome.

Result:

Hundreds of hours (and money!) lost searching for unrecoverable documents and reworking lost files.



SCENARIO 02

In the rush to stand up a remote workforce to meet new virtual office requirements, your organization provisioned laptops to employees and didn't prioritize backup for Office 365. A month into the new work situation, you determine that cybercriminals took advantage of your organization's disruption and encrypted your Office 365 data, deleting critical emails and files of telecommuters. Despite a massive ransom payment sent to the cyberattackers via Bitcoin, the data cannot be restored.

Assumption:

Office 365 applications are safeguarded from external cyber threats and data loss.

Reality:

Controlling Office 365 data is your responsibility, including protecting your Exchange Online email from ransomware, malware, and hackers.

Without a third-party data protection solution in place, you won't have the ability to access a separate copy of your data should a ransomware attack occur.

Result:

External security attacks and data breaches can wreak havoc on an organization, causing crushing financial impacts to your bottom line and irreparable damage to your brand reputation. Further, you may be held accountable for expensive fines relative to regulatory compliance and data privacy if internal and customer data is affected.

SCENARIO 03

One of your employees resigned a year ago and the account was deleted to save on licensing costs for inactive users. Unfortunately, this employee has unexpectedly taken legal action against your organization and you're required to produce information respective to the dispute.

Assumption:

Office 365 has built-in Litigation Hold, so all is well.

Reality:

Many organizations are motivated to delete old users to avoid the financial burden of paying licensing fees for terminated employees or those that have left the organization. This can present challenges when legal disputes arise because deleting a user means their personal SharePoint site and OneDrive account is gone for good, too. And while Litigation Hold is a safeguard put in place by Microsoft to reduce the risk of losing data, it can't take the place of third-party data protection to address compliance requirements and regulations.

Result:

Legal action can be crippling when you account for legal fees and the consequences or fines you may face if you're unable to provide necessary information. You never know when you'll need to produce emails or other documentation, so staying prepared is the only way to keep your organization out of jeopardy.

arcserve®

eBook

PROTECT OFFICE 365 DATA WITH ARCSERVE

Microsoft offers backup as part of a shared-responsibility model, meaning they're responsible for the physical security of their data centers and software failures on their part, but it's your responsibility to protect your data from cyberattacks and data loss caused by human error, intentional deletion, and programmatic issues.

Make Office 365 protection a reality with Arcserve Cloud Backup for Office 365 Secured by Sophos. Achieve total protection against data loss and ransomware with fully integrated backup and cybersecurity for Exchange Online, OneDrive for Business, and SharePoint Online, including:

- Granular recovery and rapid restore back to Office 365
- AI-powered cyber protection
- A unified management console and role-based access control
- Policy-based management
- Role-based administration
- SLA reporting
- Straightforward, subscription-based licensing with egress included

Take control of your Office 365 data with Arcserve.