TOP 10 REASONS TO BACKUP MICROSOFT 365 DATA

CONFUSION IN THE CLOUD HAS LED TO DATA LOSS

IRON MOUNTAIN®

IRON CLOUD™

INTRODUCTION

Applications like Teams, OneDrive and SharePoint not only help employees collaborate more efficiently and effectively, they enable a global workforce to work from anywhere.

Being hosted in the cloud, Microsoft 365 absolves organizations of the responsibility for maintaining a complex infrastructure of hardware and interdependencies; however, business organizations are still responsible for ensuring end user compliance with data security and preservation of data in accordance with their compliance regimes. As such, organizations should back up their data in the Microsoft cloud just as they would with on-premises data. **Here are 10 reasons why.**

> MORE THAN A MILLION BUSINESSES WORLDWIDE USE MICROSOFT'S SUITE OF PRODUCTIVITY APPLICATIONS, MICROSOFT 365.

1 IT'S YOUR RESPONSIBILITY

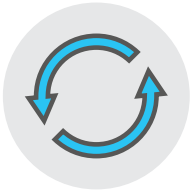
Having your data saved in the cloud is not the solution to your backup problems. Forrester states that backing up software as a service (SaaS) application data is the responsibility of the organizations that use it, not the software vendor. SaaS providers, like Microsoft, are only responsible for the availability of their infrastructure and services, not the data their customers keep in the cloud.

70%

Of companies using SaaS products have lost business data.

35%

Of businesses say they're only partially familiar with their SaaS providers' SLAs.



33%

Of businesses think SaaS applications don't need to be backed up at all.

Enterprise Strategy Group, Data Protection Cloud Strategies

2 WE'RE ONLY HUMAN

DATA LOSS HAPPENS FOR A LOT OF REASONS. FOR THE MAJORITY OF THEM, THERE'S A HUMAN BEING INVOLVED. WHETHER IT'S A MALICIOUS HACKING ATTEMPT OR ACCIDENTAL DELETION OF A FILE, MOST DATA LOSS INCIDENTS ARE CAUSED BY HUMANS, NOT COMPUTERS.

34%

Increase in phishing emails due to COVID-19

Webroot, COVID-19 Clicks: How Phishing Capitalized on a Global CrisisProtection Cloud Strategies

23%

Share of cybercrime committed by employees

CERT Insider Threat Center

64%

Data loss incidents caused by human error

Aberdeen Research

Should an end user fall for a phishing email, the ultimate result may be a disruption to critical systems, lost revenue, reputational damage and, in many cases, the payment of a large ransom. Internal threats are also potential causes of data loss and breach.

The biggest threat of all is human error. This includes accidental file deletions and overwriting of permissions and security configurations. SaaS providers like Microsoft can't and won't confirm if a request to delete is hasty or malicious.

Administrative error is also common. With great power comes great responsibility. Anyone with access to powerful tools for streamlining business processes can also be responsible for a sync error that overwrites critical business data in a single keystroke. Without the right tools, there is no easy way to reverse the damage caused by these data loss scenarios.

3 GRANULAR RESTORES

Microsoft 365 enables you to restore an entire site collection, mailbox or user, but it does not include the ability to perform granular restore. Having the flexibility to restore exactly what you need exactly at the point in time you need it can save significant time and resources when performing disaster recovery. It can also reduce the time it takes to recover data, also known as the recovery time objective or "RTO."

4 PREVENT DESTRUCTIVE RESTORES

Microsoft gives OneDrive users the ability to roll back files to a previous point in time within the last 30 days (for data that has not already been deleted). For the data that does still exist in OneDrive, this feature is an "all or nothing" destructive restore, which means a user may have to roll back all changes made in OneDrive to the selected time (even the intended changes) – instead of being able to limit the changes to certain files or folders. Being able to granularly determine what is restored – and prevent destructive restore – grants administrators the freedom to service a broad number of use cases.

5 RAPID RESTORE

A disaster recovery strategy would be incomplete without the determination of recovery objectives, specifically, recovery time and recovery point. These are referred to as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), where RTO indicates the time it takes to recover and RPO indicates how much data loss is acceptable.

As previously mentioned, recovery time is highly dependent upon having flexible recovery options for recovering exactly what needs to be recovered; no more, no less. Recovery point, on the other hand, is dependent upon backup frequency.

For both RTO and RPO, it's necessary to have a purpose-built backup tool to achieve your organization's objectives, since control over RTO requires flexible recovery options, and control over RPO requires flexible backup scheduling.

CASE STUDY:

ENHANCED (BUSINESS TECHNOLOGY CONSULTANTS)

60%
TIME SAVED PER RECOVERY REQUEST

IRON CLOUD BACKUP FOR MICROSOFT 365 WILL HAVE AN IMPACT ON OUR LONGER-TERM ROI, AND THE PROCESS OF RECOVERING DATA WILL BE MUCH FASTER.

– Technical Director Enhanced, James Cripps

6 CUSTOMIZABLE POLICIES

Microsoft 365 data can be removed from the system through either active or passive deletion. Active deletion occurs when an administrator or user takes it upon themselves to delete data. In some cases, that data may still be recoverable from the recycle bin. But if the recycle bin retention period has expired, or if the user also actively deletes the data from the recycle bin, it is not recoverable. Passive deletion occurs when the tenant subscription ends and, after 180 days, the data is automatically purged from Microsoft's infrastructure.

It's important to note that, while there are default retention periods (93 days) for OneDrive and SharePoint, retention policies can vary from service to service. And, as services are introduced, they do not always have similar safeguards available. Without complete control over retention policies, critical data can fall through the cracks.

Customizable policies also enable granular policy creation for different groups and users within the organization. C-level executives can have different backup policies than managers or individual contributors. Only a purpose-built backup tool can provide this level of control and customization.

7 SYNC ISSUES

Many people and organizations make the mistake of thinking they don't need backup because they have OneDrive. But OneDrive is actually a sync and share tool that's designed more for collaboration than it is for backup. With OneDrive, whatever happens to a document on a local machine is synced to the cloud. So, if a file is deleted or infected on that local drive, the change is automatically synced in OneDrive.

8 CENTRAL MANAGEMENT

No matter how big or small the business, there's a good chance that IT resources are stretched thin. Help desk requests can pull IT staff away from other strategic priorities. That's why, when it's time to help a user recover a lost file, folder or SharePoint site, it's essential for IT to be able to perform the recovery remotely, preferably from a central console. Central management can speed recovery times, getting users back on task and freeing up valuable IT resources for other strategic initiatives.

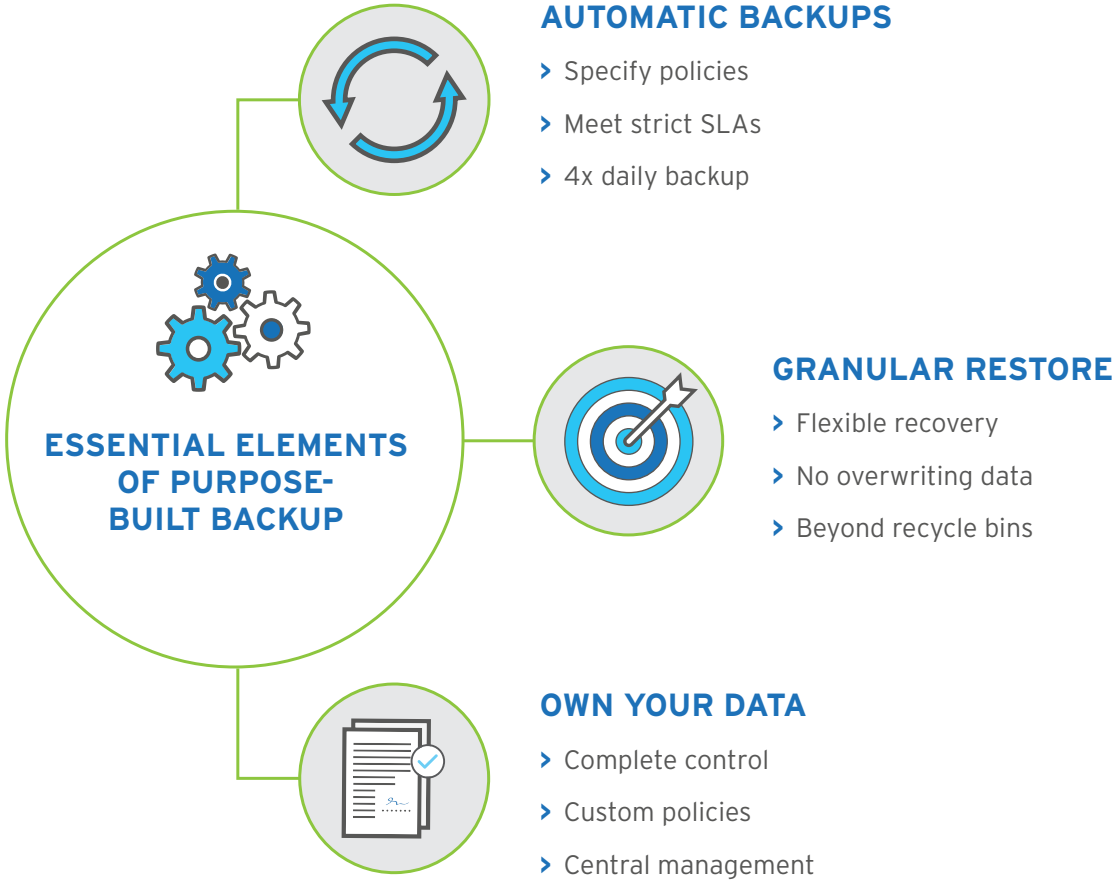
9 IT'S NOT BACKUP

It's been stated previously but deserves to be repeated: Microsoft 365 is designed for collaboration and productivity, not backup. Specifically, it's not designed for the everyday data loss scenarios that IT administrators deal with on a regular basis. Accidental file and folder deletion, ransomware, permissions overwriting – these are the types of data loss businesses are most likely to face. Microsoft is not responsible for any of them; they're the responsibility of the organization whose data lives in Microsoft 365.

With Microsoft 365, file versions are not immutable or isolated recovery points. For example, if an active file is deleted, all older versions of the file are deleted as well. If they are deleted permanently from the recycle bin, then no viable recovery points are available.

10 CONFIDENCE

Confidence comes from having the right tools for the job. That means having control over backup and retention, and not being subject to uncertain default policies. It also means flexible recovery options, so there's no need to recover more than what's necessary. And it means being able to implement recovery objectives that have been established based on business requirements.



THE IRON CLOUD DATA PROTECTION SOLUTION

Iron Cloud Backup for Microsoft 365 is purpose-built for backing up data in Microsoft's suite of productivity applications. It includes all the features and functionality necessary to perform flexible recovery and achieve stringent recovery objectives. Iron Cloud Backup for Microsoft 365 is designed for the types of everyday data loss events businesses are most likely to face. It enables businesses to recover from ransomware infections, accidental or malicious deletions, permissions overwriting, deleted mailboxes and more.

Ready to find out for yourself?

CALL TODAY: 800.899.IRON

IRON MOUNTAIN®

CARBONITE®
an opentext™ company

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

USDM-EBOOK-022621A