Securing your Microsoft Office 365 Environment

Wanstor's Data Protection,
Backup and Replication Solution

wanstor

Contents

wanstor

Introduction

Backup for Office 365 - Do we need to worry about it?

In the last 12 months, Wanstor's data protection experts have seen a significant increase in the number of business and not-for-profit organisations moving from on-premises Exchange environments to Office 365.

At Wanstor, we understand why many organisations are making this move and have recently done so or plan to do so in the near future. When it comes to messaging, for example, there isn't much difference (in terms of business value and competitiveness) whether you run it yourself or consume it a service.

But one area in particular does make a difference - backup and restoration. Within this document, it is probably best to start with the definition of a backup:

"an independent copy of data that can be restored if the source system or service is unavailable"

This definition is pretty conclusive in what it means for the IT team.

Now let's analyse a typical on-premises enterprise IT estate. Most have Exchange, and some have tape- or disk-based backup appliances, keeping data anywhere from 1 to 7 years.

Many IT and Finance Managers may be thinking: why did we spend all of that time and money on backup in the first place? The answer to this question is that it was not about the capability to backup data, but rather about the ability to restore data.

IT Managers are responsible for restoring entire systems or individual e-mails on demand, for a period covering the length of time that the business requires. Directors must maintain confidence in the IT Manager's ability to do this.

> IT Managers are responsible for restoring entire systems or individual e-mails on demand, for a period covering the length of time that the business requires.

With this in mind, let's evaluate standard Office 365 capabilities. Based on an E3 subscription, what does the business receive for £17.60 per user per month?

The first function to consider is restoration of deleted data, particularly useful for accidental deletion. Users can restore data with a simple click-and-drag from individual workstations. IT teams can even configure this option for unlimited retention, with 14 days being the default.

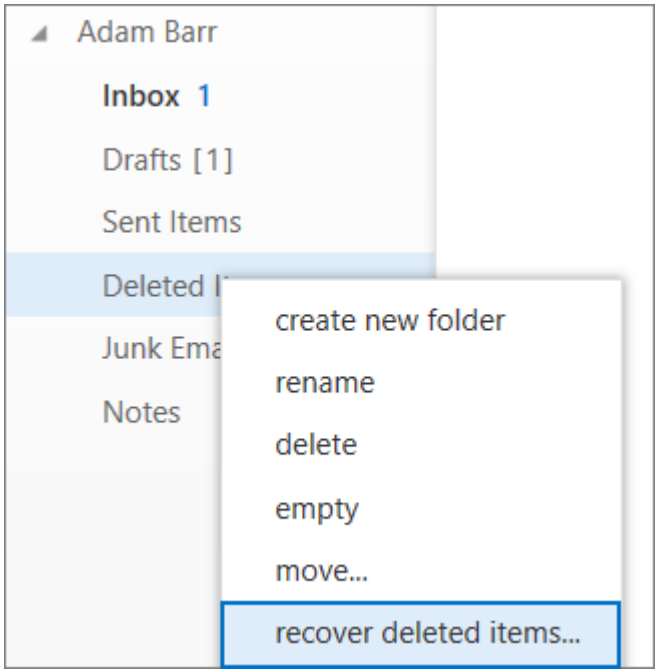

figure 1 : Office 365 functionality allowing data recovery

But what if the end user wants to make sure something is no longer in the system?

The answer is to simply delete it from the *Deleted Items* folder. This should be viewed as an end-user benefit (not to be confused with data protection). Additionally, this operation relies on Office 365 being online - if the service is offline, there is no access to emails or any deleted items.

Once the end user has deleted items from both their inbox and the deleted Items folder, what happens next?

In Office 365, there is a *Recoverable Items* folder that can retain items for up to 30 days - with 14 days being the default. Any item that stays in this folder longer than 30 days is lost. Now, most IT Managers will be asking the question - surely Microsoft has considered this?

The answer is both yes and no. Microsoft's solution to this scenario is *Litigation Hold*, which copies all of your e-mails to an immutable area (hidden from users within the *Recoverable Items* folder).

There is also an *In-Place Hold* option; Microsoft is phasing this functionality out, however; we would not suggest deploying it at this point in time or in future.

In qualifying this functionality, Microsoft states:

> *"We have postponed the July 1st 2017 deadline for creating new In-Place Holds in Exchange Online (in Office 365 and Exchange Online standalone plans). But later this year or early next year, you won't be able to create new In-Place Holds in Exchange Online."*

Phasing out the *In-Place Hold* option alongside the fact that *Litigation Hold* doesn't support public folders, means IT Managers will need a third party solution if they make a decision to back up public folders.

Many business and not-for-profit organisations require a separation of roles as security standard. In this scenario, Office 365 administrators could (rightly or wrongly) assign themselves eDiscovery Manager rights with full access to search and export from Exchange mailboxes, SharePoint folders, and OneDrive locations. They could even modify *Litigation Hold* policies.

This is a key reason why many business and not-for-profit organisations opt to use third-party backup integration with Office 365.

Such solutions usually include role-based access control and auditing, which help organisations to comply with current and up-coming data protection laws, while also allowing a different department or administrator to hold the right for restores.

Additionally, many clients insist on a recoverable offline copy of their Office 365 data. This is, in fact, the only way to protect from data corruption. (Microsoft explicitly states that point-in-time restore of data is not within the scope of Office 365.)

In summary, if you are an IT Manager looking for an independent offline backup, public folders or additional separation of security, you will need to invest in a third-party backup tool by a provider other than Microsoft.

Within this document, Wanstor's data protection experts will outline the importance of investing in such a third party data backup tool and restoration solution, supplied by a trusted IT service provider.

Things you may not know about O365 data protection

Microsoft Office 365 provides the foundation for many business and not-for-profit organisations' business-critical operations on a daily basis. However, as identified earlier, O365 backup data is limited to 30 days before it disappears forever - creating a raft of problems for IT Managers who may not be aware of this 30-day Backup and Recovery rule.

Imagine reporting to senior management that you have accidentally deleted analytics critical to quarterly shareholder reports, or that you have no way of recovering data lost due to ransomware. These examples highlight how crucial it to invest in the right tools, people and processes when protecting your Microsoft Office 365 data. With access to the right backup and recovery tools, IT Managers can mitigate risk around achieving business continuity and minimize costs associated with employee and business downtime. With adoption of SaaS offerings continuing unabated and production data moving to the cloud, many business and not-for-profit organisations remain unaware of their own responsibility for data, regardless of its location.

In short: Office 365 ensures that your application data is available, but it does not fully protect you from data loss.

Five Things often overlooked by IT Managers when considering Office 365 Data Protection

1. There Are No Data Protection Guarantees: *Microsoft Office 365 guarantees availability but not protection of your data. Microsoft takes responsibility for hardware failure, application failure and data centre outages - other issues impacting data remain the responsibility of IT teams.*

2. It does not produce true Backups: *Office 365's native Recycle Bin and version histories are not true backups allowing internal IT teams to control backup and recovery, presenting potential security risks & slower recovery times.*

3. No Customer-Controlled Backups: *Microsoft Office 365 native DR tools cannot recover all types of lost data, and require a backup solution to execute recoveries in case of file corruption, accidental deletion and malicious attacks.*

4. Point-in-Time Email Restoration is unavailable without a third-party service: *Restoration for your Exchange server is not in scope, with ransomware attacks or accidental deletion leaving you unable to roll your Inbox back to a previous state.*

5. Limited Control of Archive Period: *Mailboxes deleted without a hold are neither preserved or discoverable after 30 days, meaning that without a third-party solution, IT teams remain unable to establish long-term backups.*

wanstor

Modern Day Challenges & Threats to Your Valuable Data

As we've discussed earlier, SaaS providers do not guarantee that your data is fully protected.

While some provide comprehensive disaster recovery for disruption to data centre operations, they do not guarantee the integrity of your data against accidental deletion, virus or malware, hackers, or ransomware attacks.

Threats to this data are constantly evolving, and IT teams cannot afford to lose business-critical information. To truly protect data and meet regulatory requirements, IT Managers need to have insight and control in order to effectively execute data recovery, control where and for how long data lives, and establish end-to-end security. Common Causes of Data Loss include Ransomware, end users purging data, synchronization issues, rogue administrators and insider threats.

Shared Responsibility

Microsoft Office 365 maintains a shared responsibility model for its services, offering robust disaster recovery, but no protection against accidental deletion, viruses or malware, hackers or ransomware attacks. Users retain responsibility for protecting their data against the risk of user error and malicious intent.

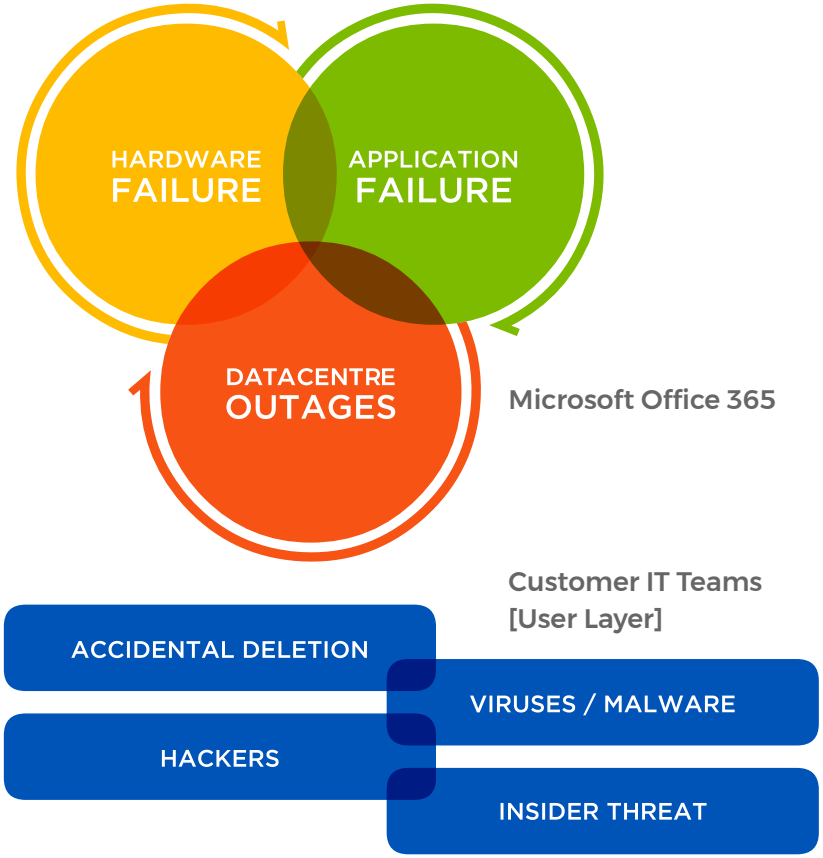

figure 2 : Microsoft Office 365 Shared Responsibility

wanstor

Data Loss is becoming more common than you may think

In today's IT environment, through proliferation of devices and users requiring varied access to information, data loss is more common than ever before. Even minor incidents can impact on day-to-day business and profitability. Establishing backup for SaaS offerings is essential to maintaining business continuity.

By implementing data recovery solutions and emergency response procedures, IT teams can proactively minimize downtime and soften the impact of application disruption and data disasters.

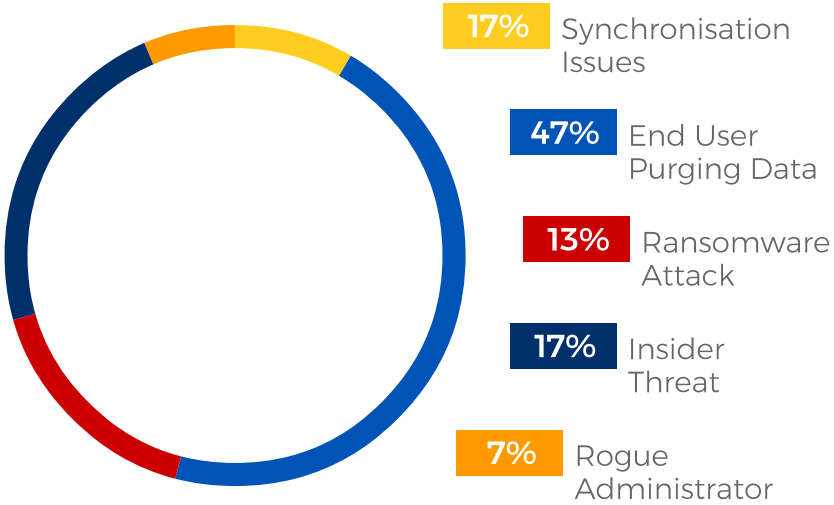

figure 3 : Common forms of data loss

Privacy and Security Controls

The integrity of data is perhaps the most important objective held by IT teams. Ensuring data privacy and security is paramount to deflecting an attack on your business or not-for-profit organisation.

Wanstor's Cloud Control product makes it easy for IT Managers and Administrators to monitor, protect and analyse data across the hybrid cloud environment. Compliance Integration with Wanstor storage targets give IT teams flexibility around where backup data resides, enabling them to easily meet offsite compliance requirements for critical data.

Every action in your Office 365 environment is captured and made available by Cloud Control via "Activity Logging", simplifying generation of and access to audit reports for legal inquires.

Data Protection

Data is encrypted in transit and at rest, for end-to-end data protection. Authorization keys are securely stored and managed using a Key Management Service (KMS), to ensure best practices are followed in cloud management.

Risk assessment tools equip IT Managers and Administrators with the means to actively monitor the SaaS environment. Cloud Control notifies users of potential security breaches immediately, allowing swift action to be taken.

wanstor

Why you should choose Wanstor as your data protection partner for O365

At Wanstor, we understand the consequences of compromised data in Microsoft Office 365 range from inconvenient to disastrous.

Solutions protecting this environment need to be agile and comprehensive, but easy to implement and straightforward to use.

Wanstor has developed a Cloud Control product for IT Managers - an easy-to-use, SaaS offering for all backup and recovery needs.

This solution requires that IT Managers or Administrators simply sign in, select services designated for backup, and identify the required storage capacity.

The single user interface allows Administrators to automate backup schedules, easily search backups and rapidly recover data at any time.

Wanstor Cloud Control for Office 365 : Product Detail

+ Cloud Control for Office 365 is agentless, making it simple to configure, manage, and administer. Backup scheduling and tiering options are available so IT Managers can automate the protection of Office 365 workloads
+ Agile DevOps teams can write code to NetApp Cloud Control APIs, seamlessly extending protection to Office 365 environments and leveraging multiple backup targets. The agility of this approach enables IT teams to scale data protection as their business grows.
+ Secure Privacy and Security controls ensure that data is compliant and safeguarded against accidental deletion, corruption or malicious intent and is encrypted and secured both in-flight using Secure Socket Layer (SSL) encryption and at-rest with advanced AES-256 bit object-level encryption.
+ Compliant Encryption keys are securely stored and managed using our Key Management Service (KMS), with unique keys for each customer. Every action is captured in Cloud Control's audit reports making meeting compliance requirements easy.

wanstor

Next Steps

Learn More

For more about the business advantages of Cloud Control for Microsoft Office 365's backup and compliance offering, simply visit **www.wanstor.com**, email us at **info@wanstor.com** or call us on **0207 592 7860** to speak with one of our Data Protection experts.

Getting Started

To install a complete backup service for your Office 365 data, simply call **0207 592 7860**, ask a Wanstor Data Protection expert to select a 12-month, 24-month or 36-month license for you, and launch the service. There is no software or hardware to purchase or install.

We also offer all new customers of our Cloud Control service a 30-day free trial.

Part of something bigger

Cloud Control is a component of a larger solution suite, specific to the cloud.

Wanstor's cloud data services seamlessly extend on-premises data management capabilities to the cloud, simplifying data management, enhancing security, accelerating data movement, streamlining DevOps and fuelling innovation across your hybrid cloud environment.

These benefits are the foundation for building a data-centric business or not-for-profit organisation.