How Atempo addresses Microsoft 365 Data Protection Challenges

WORKLOAD : **MICROSOFT 365**
CATEGORY: **SAAS DATA PROTECTION**

Tech Paper - 2022

IDC states that ***"Backup for fast-growing SaaS such as M365 is no longer an option — it is imperative for security and data control."***

When the pandemic first instigated a global shift to remote work, videoconferencing emerged as an immediate solution to work-from-home restrictions. The initial era of "remote everything" has given way to durable, hybrid work models and forcing companies to rethink how they work. The shift to cloud-based solutions has become more attractive to SMBs who are looking to maximize both efficiency and productivity.

To improve internal organization, businesses have massively adopted collaborative tools. **Microsoft Teams now has 270 million monthly users up from 75 million in 2020 - an increase of 260%** (Source Microsoft).

Millions of businesses rely daily on Microsoft 365. Users would be forgiven for thinking their data is safely stored in the cloud and that Microsoft offers comprehensive backup and recovery features. This is a dangerous misconception. Microsoft's **"Shared Responsibility Model"** states that Microsoft is responsible for infrastructure maintenance while **users are responsible for protecting actual Microsoft 365 data.**

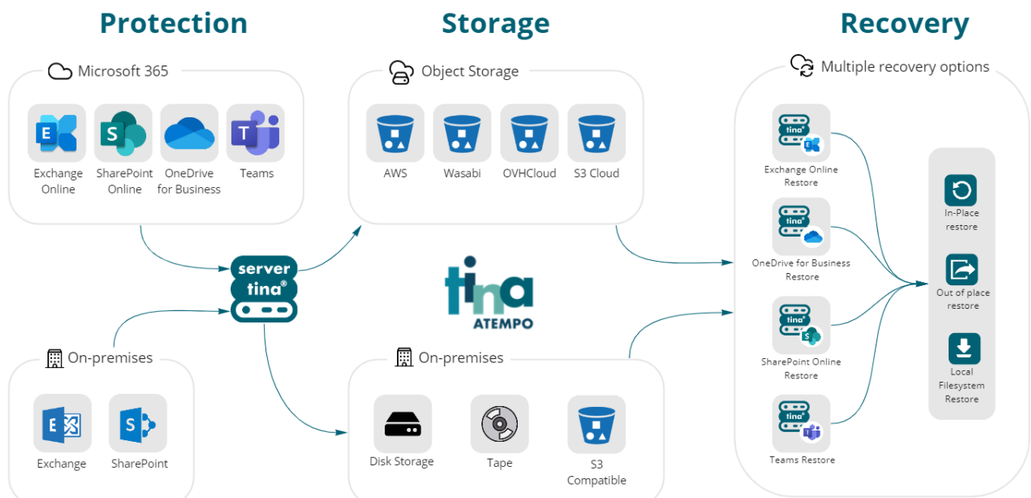
"Customers are responsible for their data and it is their responsibility to deploy long-term data storage, backup and recovery and define whether their data protection strategy is on-premises and/or in the cloud. These considerations need to be managed separately from Microsoft 365 infrastructure to ensure the highest level of protection and to meet requirements of maintaining data in a sovereign storage if they so wish." **Renaud Bonnevie, Technical Product Manager at Atempo.**

Gartner research* from 2019 highlights that "*Microsoft Office 365 offers a robust service, but* **its data protection capabilities vary across applications** *(…) I&O leaders should augment their backup and recovery strategies with* ***third-party solutions.***"

What are the main threats from not applying a consistent backup policy?

- **Accidental deletion:** unintentional deletion by an authorized user.
- **Internal Vulnerabilities:** An internal threat refers to the risk of somebody from the inside of a company who could exploit a system in a way to cause damage or steal data in other words it is mainly sabotage by former employees
- **External Vulnerabilities:** Mainly related to hackers exploiting vulnerabilities in software or "password-spraying" attacks to gain access to gain access to applications and deploy malicious software.
- **Legal and compliance penalties:** customers must maintain data archives to meet financial regulations, produce evidence for legal cases and document consumer data use.
- **Retention gaps:** several data management use cases such as inadequate backup rules or not backing up former employee data for cost reasons for example.
- **Data sovereignty:** Deloitte Tech Trends have emphasized that companies will modernize their data management approach with data sovereignty becoming a major trend.

Atempo M365 Data protection functionalities



Tina provides a **comprehensive, robust,** and **flexible** solution to current threats.

Its granular data protection across **Exchange Online, SharePoint Online, OneDrive, Teams, OneNote** and **Groups** address all accidental deletion use cases. Granular search with flexible point-in-time, in-place, out-of-place and local restore options enable accurate recovery for all deleted items from authorized users.

Tina is built on a Linux kernel and is **secure by design**. It combines the best of data protection and storage security enabling backup rules such as "3-2-1" Immutable and air-gapped backups safeguard against ransomware, accidental deletion, data corruption, and cybercriminal attacks. **The 3-2-1 rule** is the most basic rule of data protection. The rule states that at least three copies of each file should exist. They should be stored on two different types of media (LTO tape, HDD, SSD, Cloud). One of the copies must be stored off-site for maximum security. Tina provides the flexibility to apply this rule whatever the infrastructure specificities.

The highly flexible architecture of Tina not only **answers security threats, legal** and **compliance matters and retentions times.** The solution also optimizes data storage with built-in deduplication and compression. It effectively manages retentions periods with a wide range of backup and archive destinations including sovereign storage targets.

Key Features

Respecting Vendor Standards:
Atempo technology ensures data is managed in line with vendor standards guaranteeing protection and recovery. We respect Microsoft recommendations by using the latest recommended APIs to back up and restore data from the Microsoft 365 Tenant. Tina only uses Microsoft Graph APIs and not EWS APIs according to Microsoft's recommendations.

Data Conservation on Tape for Long Term Air-Gapped Protection:
Even deduplicated data can be saved to tape. To ensure every restore job is successful, the data is rehydrated from tape to the destination. And once data is on tape, you are sure your data sets are physically out of reach of cybercriminals!

Optimal Deduplication:
Tina provides industry-leading backup speeds and reduced storage for backup volumes.

Various backup location:
Relying on the wide possibilities offered by TINA backup, users can store their M365 files to a variety of media. It is possible to use the advantages of backing it up on-premises but also to the cloud. Tina for M365 is able to back up to disks, tape or S3-type on-site storage. To benefit from the price advantages of backing it up in the cloud, Tina for M365 also allows you to store your backups in the various generic S3 buckets. Thus, you can use AWS, Wasabi or OVH as object storage in the cloud.

Advantageous License Models:
Tina's flexible licensing schemes plug right into your business. With data volumes increasing all the time, additional licenses can be required to protect a growing and changing IT infrastructure. With Atempo's vertical licensing, you get all the backup for your local and Microsoft 365 infrastructure with no extra cost unlike to the competition who have an expensive licensing per user per month for Microsoft 365.

*Source: "Prevent Data Loss by Assessing Your Office 365 Backup and Recovery Needs"

*Source: IDC 2019 – "Why a Backup Strategy for Microsoft Office 365 is Essential for Security, Compliance, and Business Continuity"

maj 2022-03-29

Atempo Paris Headquarters | 23 Avenue Carnot, 91300 MASSY | Tel: +33 164 868 300 | info@atempo.com