ATEMPO
preserving data ecosystems

Modern Data Protection
Opportunities & Risks

Ensure business continuity for all your workloads

DATA PROTECTION

An Atempo Tech Paper

Businesses today must deal with economic crises, global pandemics, ever-changing regulations, and cybercrime.

Increasingly sophisticated ransomware attacks are specifically targeting backup data and administrator functions. AI-based spear phishing and hybrid work – the cyber threat landscape remains tense. Cybercrime-as-a-service is becoming a major business model, and criminal tactics are evolving by the minute.

And Microsoft 365 is not immune to these cyberattacks. It makes sense for attackers to target it due to the massive uptake of this SaaS platform.Gartner predicts that by 2025, at least 75% of IT organizations will face one or more attacks.

Attacks can come from two directions:

- External threats: Hackers attacking the company from the outside, usually for money, but sometimes for political or other reasons. Attacks launched from outside must gain access to the network through stolen credentials or software breaches or backdoors.
- Internal threats: Employees cannot be ignored as a threat. In some respects, internal attacks are easier to mount as the attacker already has access to the network and does not need to breach firewalls, even if privilege escalation may still be required.

One Ransomware attack every **11 seconds** in 2021
(Cybersecurity Ventures)

By 2025, **40%** of all enterprises will require ransomware defense mechanisms
(Gartner)

Cybercrime cost in 2021 = **€6,000 billion**. Covid-19 = €9,400 billion
(Cybersecurity Ventures – World Bank)

44% of entry point attacks are through phishing Email, malicious links
(Data protection trends 2022)

To prevent risks in hybrid environments, a key requirement is to build security into every stage of software development. A secure-by-design backup solution requires a couple of requirements to be met:

COMPANIES SHOULD DEVELOP A ZERO TRUST SECURITY CULTURE

Atempo has security teams involved during the whole development process and their duty is to align people, processes, and technology to minimize software risk.

The security teams are actively involved in implementing ISO 27001 standards and in the continuous improvement process.

Another aspect of their job is to follow latest cybersecurity technology trends, security reports highlighting latest attacks, subscribing to RSS feeds and organizations such as ANSSI (The National Cybersecurity Agency of France) as well as participating at industry security events (such as the FIC: International Cybersecurity Forum).

A SECURE-BY-DESIGN BACKUP SOLUTION

Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as architecture analysis, continuous testing/ penetration testing, authentication safeguards and adherence to best programming practices (such as static code analysis).

For modern web-based backup solutions, such as Atempo Data Protection, security teams respect OWASP Security design principles created to help developers build highly secure web applications. Security teams are focused on applying all Security principles.

We all remember the recent attack on the US based MSP software provider which is estimated to have infected up to 2000 global organizations with ransomware. The ransomware group targeted a vulnerability in MSP remote computer management tool to launch the attack.

We see in this example that MSPs can be efficient vehicles for ransomware because they have wide access to many of their customers' networks. This is why Secure-by-design matters for a software provider.

LINUX OS FIRST

Linux systems are rarely infected by malware such as viruses, worms etc., thereby making it as a very secure OS.

Security is a very fast and evolving topic! Given the fact that Linux is an Open Source and many experts are watching it, many of the security issues are managed by releasing frequent patches. Added to that, there are some OS design-level aspects like memory management, user/kernel memory space separation, virtual memory, log management, file access control that make it even more secure. Atempo Data Protection is designed to work with Linux which, when we follow architecture best practices, makes it a very secure solution. Keep in mind that to ensure a high level of security the Linux OS and Atempo Data Protection must apply the latest patches to avoid any risk of a security breach.

ARCHITECTURE YOUR BACKUP SOLUTION RESPECTING SECURITY BEST PRACTICES

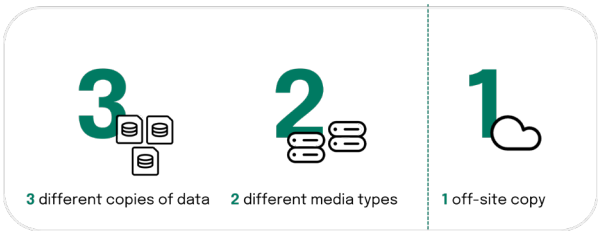
When it comes to configure your backup solution in hybrid environments a couple of best practices must be taken into account.

- A good practice is to isolate your backup service and make sure you server is hidden from your Active Directory, making it invisible avoids risks from ransomware attacks.
- Make sure only computers that need to access your backup environments can access this server with secure communications and encryption between servers and any storage nodes.
- Limit physical access to data backups. However you choose to store your data

backups on the server, NAS, tape or cloud, be sure the access is controlled in those facilities. Encrypt your backups; encryption implemented and managed in the right way serves as an excellent layer of defense.

RESPECTING INDUSTRY BEST PRACTICES AND COMPANY USER DEFINED SECURITY RULES

There are several industry backup strategy or good practices like the 3-2-1. A 3-2-1 backup strategy states that you should have 3 copies of your data on two different media (disk and tape for example) with one copy off-site for disaster recovery. We see in the backup strategy the importance of the application of Air-Gapped Protection.



Atempo Data Protection is flexible enough to comply with industry best practices and adjusting to each company specificities and building their own security strategy adding object lock or WORM Tapes as part of the backup strategy.

INCLUDE YOUR BACKUP SOLUTION IN YOUR DR STRATEGY

Data backups can be compromised or destroyed in situations such as a ransomware outbreak, employee break-in or something environmental including a flood or hurricane. Otherwise, good backups can be adversely affected. You must have a plan outlining what you are going to do if that time comes. Configure your Atempo Data Protection secondary server to prevent risks of disaster recovery enabling the continuity of your backup service.

PRIVILEGE CONTROL

Backup solution should care about being able to define precise Role Based Access Control (RBAC) for user access the solution to respect the Principle Of Least Privilege (POLP). This principle states that a user should have a minimum set of privileges required to perform a specific task. Atempo Data Protection Solution provide multi-factor authentication (MFA) to increase control on accessing the data by the user.

RESPECTING VENDOR STANDARDS

Atempo technology ensures data respects 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. Atempo Data Protection only uses Microsoft Graph APIs and not Exchange Web Services APIs (EWS). Microsoft strongly urges partners to use Microsoft Graph APIs when accessing Exchange Online data. It is

Atempo Data Protection Zero trust adoption has accelerated its response to the rapid rise of mobile and remote workers. While these trends benefited users and brought new levels of flexibility to IT, they also reduced the ability of the organization to control and secure access to data and network resources. Zero trust brings this control back, tightening up security in the face of permeable network perimeters.

The flexibility of the solution enables a continuous security improvement process and comes with constant innovation to protect and monitor your data.