Microsoft 365 Backups

Securing SLED Data in the Cloud

The guide for public sector IT professionals to achieve secure cloud-to-cloud backup and recovery for Microsoft 365.

A publication of

blue mantis

Table Of Contents

blue mantis

INTRODUCTION

Never lower your guard

The truth about Microsoft 365 cloud storage.

Research firm Omdia reported that approximately 85% of public sector organizations are using Microsoft 365 today. It's a prime example of how cloud-based IT infrastructure is now mainstream for SLED institutions.

But as more SLED employees rely on Microsoft 365, some administrators at these crucial public organizations are lowering their guard due to the mistaken belief that data is always backed up just because "it's in the cloud."

By default, Microsoft keeps a 14-day backup of all Microsoft 365 user data with backups created every 12 hours. Although this cloud-based backup regime from Microsoft provides users with an option for file recovery, IBM research shows the average time before IT detects a data breach is over 275 days (or about nine months).

Top analysts at Forrester, IDC, and Gartner all agree that organizations using cloud-powered software as a service (SaaS) solutions such as Microsoft 365 are often susceptible to this belief. Over the past five years, all the major analyst firms have authored various reports with similar conclusions: Microsoft 365 is a reliable cloud service, but all organizations should invest in a third-party backup solution for Microsoft 365 deployments.

It's clear that backup and recovery of your Microsoft 365 data using a dedicated third-party solution is crucial for operational continuity – and SLED IT leaders should choose one best suited to their risk profiles and budgets.

14 Days

Amount of time Microsoft keeps a backup of your Office 365 user data in the cloud

9 Months

Amount of time it takes for an IT department to detect and contain a data breach (on average)

Source: IBM 2022 *Cost of a Data Breach* report

Microsoft

> *"We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."*

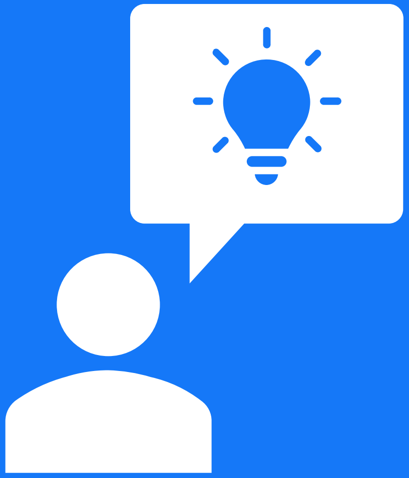
Source: Microsoft 365 Service Level Agreement (SLA)

Build Or Buy?

Do it yourself vs. managed backup

Public sector organizations use managed services from companies like Blue Mantis for the backup and recovery of their Microsoft 365 data. However, there are some IT departments very invested in the Microsoft ecosystem exploring the option of using the Microsoft Azure cloud to build and maintain their own automated backup solution for their Microsoft 365 user data.

After all, Microsoft designed their products to integrate with each other. IT departments with complex cloud automation experience can use the Microsoft cloud for a do it yourself (DIY) Microsoft 365 backup solution.



At a high level, these are the pros and cons of a managed cloud backup versus a DIY option:

	Managed Cloud Backup	DIY Cloud Backup
Pros	✓ Turnkey setup ✓ 24/7 support ✓ Built-in cybersecurity	✓ Full control over backup/restore ✓ Endless setup options ✓ Unlimited storage at scale
Cons	▪ Secure and scalable storage can be costly	▪ Setup of data backup and restoration requires technical knowledge ▪ Security must be manually configured ▪ Storage can be costly

Unless your organization has a very specific reason, a managed cloud backup solution is the obvious choice.

A COMPREHENSIVE SOLUTION

> “[Public sector organizations] incurred data breach costs that were $1.26 million higher than the average cost.
>
> **– IBM Cost of a Data Breach Report 2023**

With a comprehensive cloud-to-cloud managed backup solution for Microsoft 365, such as Blue Mantis’ managed backup solution, you can maintain the public’s trust by securing employee, citizen, and student data.

Delivered as a turnkey managed service, Blue Mantis backup and recovery solutions powered by industry-leading Veeam technology protect Microsoft Teams, Exchange Online, OneDrive for Business, and SharePoint Online data by automating the backup process to secure cloud storage. Once your data is backed up to the cloud, your IT administrators have flexible and extremely granular recovery options.

Our cloud-to-cloud approach to Microsoft 365 backup and recovery simplifies both the configuration process and maintenance because there is no need to install an agent or any server software.

- ✓ Secure storage powered by Veeam
- ✓ Fast recovery even after permanent deletion in Microsoft 365
- ✓ Convenient cloud-to-cloud solution with nothing to install
- ✓ Quick access to backup data via comprehensive search
- ✓ Reliable point-in-time recovery of single files and entire sites

Key Features

The must-haves for a managed Microsoft 365 backup solution:

Granular Recovery

Isolate files via specific points in time to restore a previous version regardless of what happened to the most recent one.

Secure Storage

Backups are encrypted in Veeam cloud storage certified for public sector data with advanced anti-ransomware technologies.

Automated Protection

Save time when new Microsoft 365 user accounts, Teams groups, and sites are added because they are automatically protected.

Complete Coverage

Secure and protect every aspect of your Microsoft 365 deployment, including Teams, Exchange, SharePoint, and OneDrive.

24/7 Monitoring

Live support for the daily maintenance and analysis required to deliver endpoint protection, patching, and drive health for your deployment.

NEXT STEPS

Connect with us.

Blue Mantis delivers true resilience for public sector organizations with our transformative combination of best-in-class technologies, talented experts, and established processes.

Email:
publicsector@bluemantis.com

Phone:
800-989-2989

blue mantis