SECUR-SERV

Securing Tomorrow

AI and Data Protection

Why Building a Strong AI Foundation Begins with M365 Backup

Securing Tomorrow: AI and Data Protection

AI has the potential to transform business productivity, but its success hinges on one crucial element: data. In this eBook, you will discover why data is essential to Copilot and the critical importance of protecting it for a secure future. Discover the key components of an AI-ready data protection solution that is comprehensive, compliant, and complete. Finally, learn how to get started on your own journey

CHAPTER 1

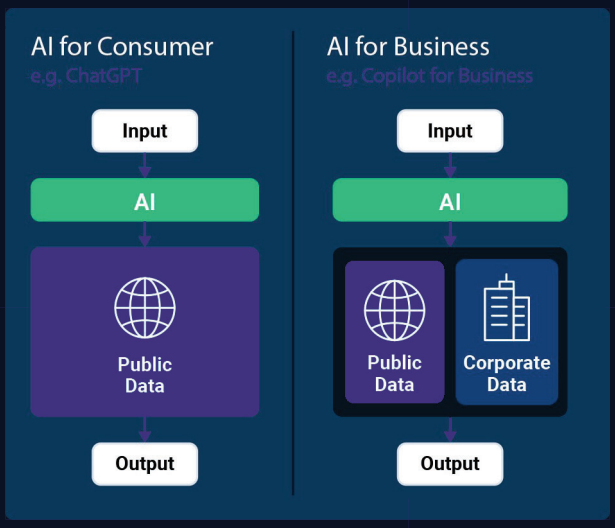
Data Foundations: Modern Backup in The Age of AI

The rapid advancement of artificial intelligence (AI) technologies has reshaped how businesses operate. AI has the potential to drive unparalleled business productivity, but its success relies on one key element - data. As AI tools like Microsoft Copilot become increasingly integrated into business processes, the need for intelligent data protection has never been more crucial.

This chapter serves as a primer on why your data is foundational to AI-driven business applications, highlighting both its value and the significant risks it faces today.

How AI Leverages Different Types of Data

It is important to clarify how AI operates differently in consumer versus business contexts. Although both scenarios involve using data and AI to generate relevant outputs, a key distinction lies in how corporate data is handled in an AI environment.



Consumer AI tools like ChatGPT operate on a straightforward model—users enter prompts (input), and the AI uses patterns learned from a broad dataset, including publicly available data, to generate a response (output). Since the training data is derived from publicly accessible or licensed sources, the output typically does not involve any confidential or proprietary information

In contrast, business AI, like Copilot for Business, requires more stringent guardrails. It handles input similarly but combines both public and private company data to generate responses. Enriched with corporate data, these responses then become more relevant and valuable, as they benefit from the added context. As a result, businesses should prioritize their data protection efforts, given the sensitivity of the data being used.

To illustrate this, imagine that your business implements Microsoft Copilot. Suppose an employee uses Copilot within PowerPoint to request a current organizational chart. Copilot retrieves the most recent data, but instead of showing the current chart, it displays one reflecting a recent reorganization—an update that had not yet been communicated to the broader team.

This example highlights some of the key challenges related to data overexposure or oversharing. To prevent such incidents, consider the following guardrails:

Data Protection
How is the latest organizational chart safeguarded against accidental or malicious deletion?

Data Classification
How are the different versions of the organizational chart labeled? Are there specific labels for higher sensitivity, or do all versions share the same classification?

Data Access
Who in the company has access to the various versions of the organizational chart? Are certain versions restricted to senior leaders only?

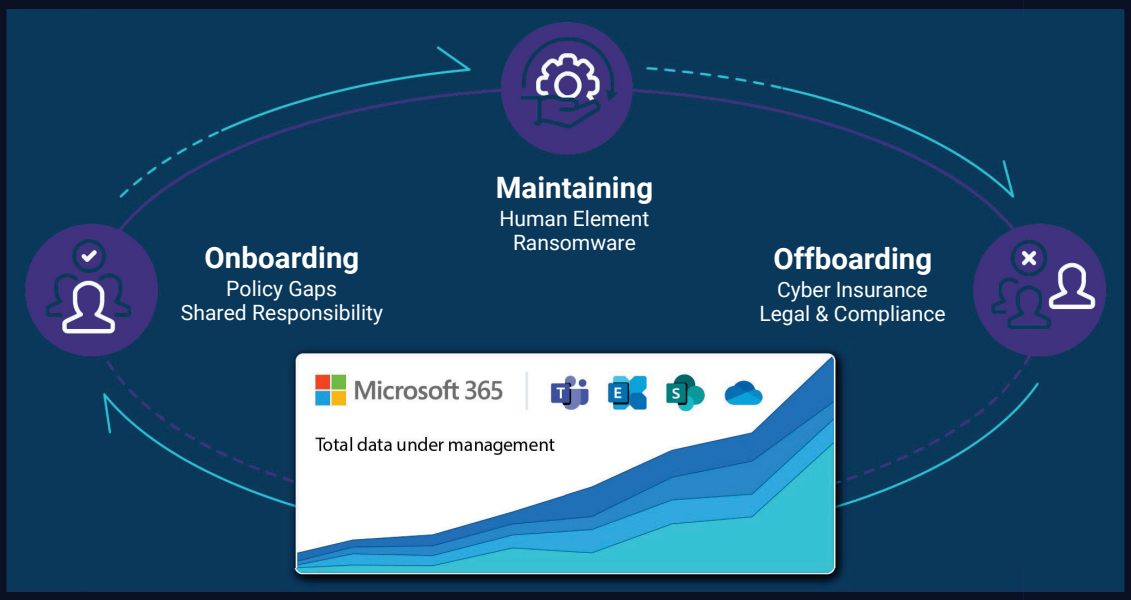
Data Governance
How are legacy charts decommissioned or removed from access and distribution?

Incidents like this underscore the vital importance of monitoring the data that AI systems access and ensuring proper safeguards are in place to prevent the accidental sharing of sensitive information. This guide will delve into the critical role of data protection, as corporate data is the cornerstone of generative AI solutions. Without adequate safeguards, data risks can prevent AI from producing the most accurate and effective responses.

The Corporate Data Lifecycle

In the previous section, we explored how Copilot utilizes corporate data to provide useful responses. It is crucial to recognize that this data carries inherent risks, even before being integrated into AI applications. To effectively evaluate these risks, it is helpful to apply the Corporate Data Lifecycle. This approach highlights the potential vulnerabilities and challenges that must be managed throughout the data's lifecycle.

Customers generate and leverage data at every stage of their cloud journey from onboarding and maintenance to offboarding. Therefore, understanding the Corporate Data Lifecycle is important for MSPs who want to help safeguard their customers' data effectively. Because data proliferation is evident throughout each stage of the lifecycle, there are many data risks, including policy gaps, ransomware, and human error. Therefore, each phase requires specific measures to ensure data integrity and security.



Stage 1: Onboarding
When new employees join, they are onboarded and introduced to the technologies you use, such as Microsoft 365. It is essential during this time for them to understand existing policies and the concept of Shared Responsibility, which clarifies what they are accountable for versus what the IT team manages. Identifying and addressing any policy gaps early on is crucial, as these gaps can create vulnerabilities that may lead to data loss. If left unmanaged, vulnerabilities can expose the business to significant risks, potentially disrupting operations.

Stage 2: Maintenance
Once your employees are comfortable with the tools, the focus shifts to their daily tasks. At this stage it is important that they use the technology effectively while staying alert to potential risks, such as human error and ransomware. Keeping employees informed and educated on best practices is essential to minimizing the risk of accidental data loss. Human error or falling victim to ransomware can disrupt operations, lead to financial losses, and damage the business's reputation.

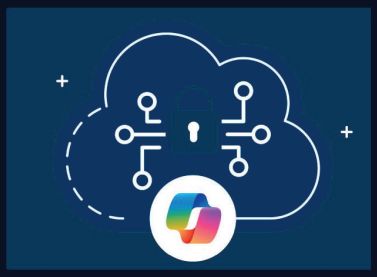
Stage 3: Offboarding
Eventually, employees may transition out of the company, entering the offboard stage. It is essential at this point to ensure their work is properly concluded, and any data they have handled is securely managed in accordance with legal and compliance requirements. Adhering to the business's offboarding procedures helps protect sensitive information and ensures a smooth transition. Failure to meet legal and compliance standards during this stage can lead to security breaches, legal consequences, and significant harm to the business's future stability and success.

Overall, the Corporate Data Lifecycle highlights the vast amount of data generated by employees and the critical need to protect it at every stage – from onboarding and daily operations to offboarding. Addressing policy gaps, preventing human error and ransomware, and adhering to legal and compliance standards are all essential. This means that, consequently, having robust data protection is foundational to managing corporate data risk before leveraging AI.

CHAPTER 2

The Right Data Protection Solution for AI Deployment

In Chapter 2, we explore the essential elements of a reliable backup solution that are crucial for maintaining data integrity and ensuring business continuity. Effective data protection must be comprehensive, compliant, and complete. These elements work together to safeguard all critical data and meet industry standards, to ensure that every byte is protected. By understanding these key components, you can employ an optimal backup solution that supports the seamless deployment of AI.



Why M365 Usage and Comprehensive Data Protection Go Hand-in-Hand

As businesses adopt Microsoft 365 (M365) to drive modern productivity, understanding the connection between M365 usage and comprehensive protection is essential. Microsoft 365 offers a wide array of services that enhance collaboration, streamline workflows, and improve overall efficiency. However, with these benefits comes the responsibility of protecting the large volumes of data generated, shared, and stored on this platform.

Copilot Delivers More Relevant Responses with Access to Increased Data

Microsoft Copilot provides a significant advantage by generating more relevant and insightful responses, particularly when it has access to a larger pool of corporate data. Copilot's effectiveness is directly tied to the volume and quality of data available from M365 applications - the more data it can access, the more nuanced and valuable its responses become. Therefore, ensuring that this data is protected and readily accessible is key to maintaining Copilot's effectiveness.

Are You Making the Most of Your M365 Subscription

Before your business can truly unlock Copilot's capabilities, assessing whether you are maximizing your use of M365 is important. Are you fully leveraging the entire suite of M365 applications, or are there gaps in your adoption? Copilot is designed to integrate seamlessly across the M365 ecosystem, and the advantages are fully realized only when there is substantial adoption of these tools.

Additionally, as businesses consolidate their SaaS applications to drive efficiency, it is important to consider the costs and potential drawbacks of using non-Microsoft platforms for collaboration and communication. Leveraging M365 not only streamlines operations but also ensures better integration with Copilot, boosting productivity and decision-making across your organization.

However, to fully drive AI transformation with Copilot, comprehensive data protection is essential. Without strong data protection measures, the risks of data breaches, compliance violations, and operational disruptions can outweigh the benefits of AI integration.

Does Your Data Protection Solution Cover All Points Where Data Is Created and Consumed?

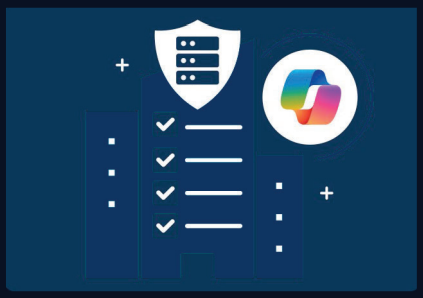
As data is generated across various M365 services, it is crucial to ask: does your data protection solution cover all the places where your data is being created? Reliable backup solutions are essential to safeguard against data loss, corruption, or breaches, ensuring that your critical information is always secure and recoverable.

Your data protection strategy must encompass all of the M365 services that your business relies on, from traditional services like Exchange and OneDrive to newer workloads like Microsoft Teams and Planner. It is important to ensure that every area where data is created and stored is covered by a robust protection plan.

Is Your Data Protection Solution Limited by Storage-Based Pricing?

One less obvious reason why not all data gets protected is the way data protection costs are structured for both Partners and customers. Legacy backup vendors often charge based on storage, which can deter comprehensive data protection due to the higher costs associated with protecting more data. This is why vendors that offer unlimited storage and base charges on other factors, like the number of users, are more favorable, as they remove this barrier to comprehensive data protection.

Key Takeaway: To fully unlock Microsoft Copilot's potential, you must embrace M365 and implement a comprehensive data protection strategy free from storage-based pricing. Using a backup solution with unlimited storage and user-based charges removes barriers to full protection, ensuring Copilot has access to a broad, secure dataset. A solid foundation of M365 adoption and cost-effective, comprehensive backup is key to your successful AI transformation journey.



Simplifying Compliance in AI and Data Protection

Now that we have covered why comprehensive data protection is a must for AI transformation, let's dive into the next key element. While excitement around AI is at an all-time high, it is important to remember that leveraging your data with AI must occur within the bounds of compliance and cybersecurity standards. Ensuring that you understand and adhere to compliance requirements will not only protect your data but also safeguard your operations from legal and financial repercussions. By staying within these guardrails, you can confidently unlock the full potential of AI while preserving the trust and security that your business depends on.

Compliance is Always Evolving

Compliance is not a static target; it constantly evolves across different markets and industries. Each has its unique requirements, and these can change rapidly in response to new regulations, technological advancements, and emerging threats. What was compliant yesterday might not be tomorrow. And as regulations change and new standards emerge, staying updated is imperative. This is particularly relevant in regulated industries like healthcare, finance, and legal, where data protection laws are stringent, and non-compliance can lead to severe penalties.

The chart below outlines key global regulatory bodies and indicates whether they classify backup as mandatory or recommended:

	Regulatory Body		Framework	Enforced
	CISA	Cybersecurity And Infrastructure Agency	CISA Cyber Essentials CPG (Cross-Sector Cybersecurity Performance Goals)	Recommended
	NCSC	National Cyber Security Centre	Cyber Essentials	Mandatory when working with UK Government Suppliers
	NIS2	European Union	10 Minimum Measures	EU Cybersecurity Regulation
	BSI	Bundesamt für Sicherheit in der Informationstechnik	IT-Grundschutz	Recommended
	ACSC	Australian Cyber Security Centre	Essential 8	Recommended
	Cert NZ	New Zealand's Computer Emergency Response Team	10 Critical Controls	Recommended

The Emergence of Regional AI Policy Acts

In Europe, efforts are already underway to drive stronger AI governance in businesses. Introducing new policies like the AI Policy Act underscores the increasing importance of compliance in AI applications like Copilot. Such regulations are designed to ensure that AI technologies are used responsibly, transparently, and ethically. As these policies become more prevalent, businesses will need to align their AI strategies accordingly. However, it is important to recognize that compliance with AI-specific regulations is built on a foundation of broader compliance and cybersecurity frameworks.

The Need for Compliant Backup

As your business looks to explore Copilot's potential, safeguarding your data becomes paramount. Ensuring that your data is protected in a compliant manner is essential for mitigating risks and maintaining the integrity of your operations. By establishing robust data protection frameworks, you can ensure that your journey to AI adoption remains secure.

Even if you have a backup solution in place today, it's critical to evaluate whether it meets current compliance standards. As regulations evolve, so must your backup strategies. This ensures that your data is not only protected but also recoverable in a way that meets regulatory requirements. A compliant backup strategy is a cornerstone of any solid data protection plan and provides the peace of mind that your business is safe and prepared for the future.

Simplifying Compliance for your Customers to Take Action

One of the key challenges your business may face is navigating the complexities of compliance. The legal language used in regulatory frameworks can often make it difficult to understand how these regulations apply and why they are important. If the connection is unclear, it is easy to overlook the urgency of compliance. It is helpful to break down these regulations into simpler terms and emphasize the broader need for action. By understanding the importance of compliance and taking proactive steps, you can protect your business from risks and ensure long-term success.

Key Takeaway: To fully harness the potential of AI while ensuring data security, businesses must prioritize comprehensive data protection and remain vigilant about evolving compliance requirements. Compliance is an ongoing process, not a onetime task, and requires regular updates to keep pace with changing regulations, especially as new AI-specific policies emerge. Simplifying complex regulations and implementing compliant backup strategies are crucial for safeguarding data, maintaining operational integrity, and confidently embracing AI-driven innovation.

Complete Data Protection for Your Copilot Strategy

Now that we have discussed the importance of having a comprehensive and compliant backup, it is time to explore the last critical piece of robust coverage, which is ensuring that your data protection strategy is complete by backing up everything. Today, Microsoft Copilot is transforming business operations by leveraging vast amounts of corporate data. With more than 2.5 billion files created in Microsoft 365 every day, any gaps in protection can significantly impact Copilot's effectiveness and leave your business vulnerable to data loss.

Gaps in Data Protection Lead to Increased Risks

Data risks are indiscriminate— it doesn't matter whether some data is protected if other critical pieces are not. Any unprotected data can lead to severe disruptions, harm your reputation, and threaten your financial stability. Therefore, it is important to have a backup solution that not only covers all of your data but also makes it easy to identify and address any potential gaps.

Understanding the Data Gaps

Understanding and identifying data gaps can be challenging, particularly if your current backup tools lack clarity. While it may seem complex, it doesn't have to be. By leveraging tools that offer clear, actionable insights, you can better understand and address vulnerabilities.

Is Your Data Protection Protecting the Right People and Resources?

The Corporate Data Lifecycle reveals that businesses are centered around employees, who create and use corporate data. If your data protection technology cannot track when employees join or leave the business, it can create security gaps. This challenge impacts companies of all sizes, from small businesses to large enterprises. Automation technology helps address this issue by ensuring seamless data protection during employee transitions.

Key Takeaway: To fully harness the potential of AI while ensuring data security, businesses must prioritize comprehensive data protection and remain vigilant about evolving compliance requirements. Compliance is an ongoing process, not a onetime task, and requires regular updates to keep pace with changing regulations, especially as new AI-specific policies emerge. Simplifying complex regulations and implementing compliant backup strategies are crucial for safeguarding data, maintaining operational integrity, and confidently embracing AI-driven innovation.

CHAPTER 3

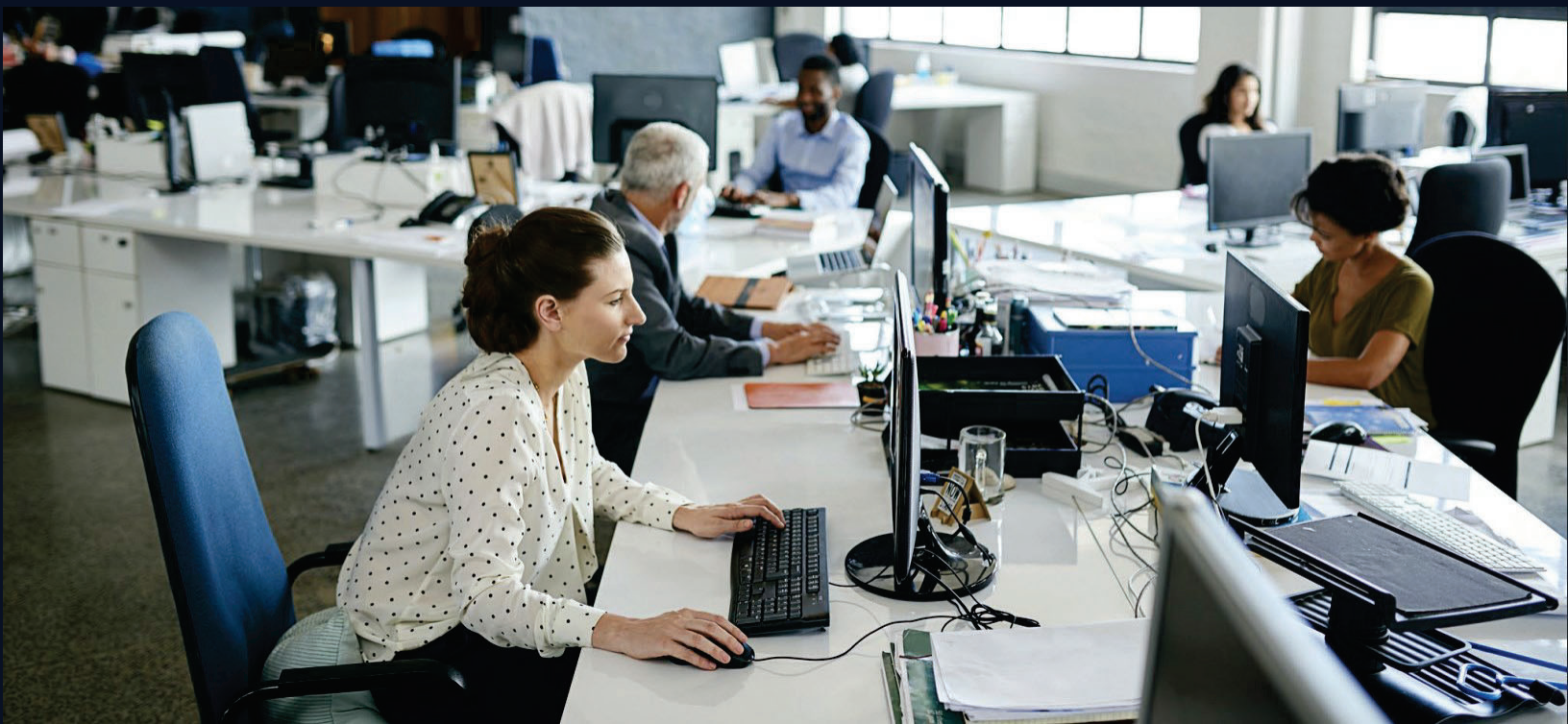
Early Lessons - Starting Small to Win Big

In this chapter, you will find valuable tips on adopting the right strategies and approaches to maximize the benefits of AI tools like Copilot. We will conclude with a comprehensive checklist to help you evaluate your readiness and ensure you are on track for successfully leveraging this innovation.

Data Protection by Function

The Employee-First Strategy to Copilot

Many businesses are unsure about how Microsoft Copilot will fit into their current workflows. The key is to focus on how Copilot can add value to specific departments and roles within your organization. For instance, think about how Copilot can bring value to each department. How would that look for a sales representative vs a customer service agent? You also want to consider how that will impact the type of data protection that should be used. Copilots' effectiveness is tied to the quality and security of the data it interacts with. By tailoring your data protection strategy to the specific needs of each department, you can ensure your business is fully prepared to leverage Copilot's capabilities.



	Key Activities	Copilot Benefits	Common M365 Data Locations	Need for Data Protection
Human Resources	Manages recruitment, onboarding, and benefits administration. Handles sensitive data like employee records, payroll, and performance reviews.	Automates routine tasks, assists in report generation, studies trends in employee feedback, and creates onboarding schedules.	**SharePoint Online** (employee documents) **OneDrive for Business** (HR personnel files) **Teams** (internal communications)	Protects sensitive employee data from breaches, maintains confidentiality, and upholds employee trust.
Finance	Manages budgeting, payroll, financial reporting, and forecasting. Deals with sensitive financial data.	Automates financial processes, analyzes data, provides insights into spending patterns, and forecasts revenue.	**Excel** (financial models and reports) **SharePoint Online** (financial documents) **Exchange Online** (communications)	Protects financial information from breaches, ensures stakeholder trust, and complies with financial regulations.
Sales	Manages customer relationships, follows leads, and closes deals. Requires accurate and accessible sales data.	Automates routine tasks, provides predictive insights, assists in data analysis, and drafts personalized sales pitches.	**Exchange Online** (communications) **SharePoint Online** (sales documents) **OneDrive for Business** (pitch decks)	Protects sensitive sales information, ensures compliance with regulations like GDPR, and maintains customer trust.
Marketing	Develops marketing strategies, analyzes trends, creates content, and manages campaigns.	Optimizes campaigns, provides automated insights, assists in data analysis, and suggests optimal posting times.	**Microsoft Planner** (project management) **Exchange Online** (communications) **OneDrive for Business** (marketing assets) **Teams** (collaboration)	Protects sensitive data like customer demographics and campaign performance. Ensures compliance with regulations.
Customer Service	Manages support tickets, addresses inquiries, and resolves issues. Needs accurate and up-to-date customer information.	Provides insights for automation, faster resolution, data analysis, suggests solutions, drafts responses, and generates reports.	**Outlook** (communications **SharePoint Online** (support documentation) **Teams** (case management)	Protects personal customer details and service history. Maintains customer trust and confidentiality in interactions.
Legal	Ensures company compliance with laws and regulations. Manages legal documents, contracts, and litigation.	Manages legal documentation, and tracks compliance.	**SharePoint Online** (legal documents) **OneDrive for Business** (personal files) **Outlook** (communications) **Teams** (case discussions)	Protects highly sensitive legal information from breaches, unauthorized access, and ensures compliance with legal standards and regulations.

Get Started Today with Cloud Backup

To ensure you are Copilot-ready, selecting the right data protection solution is critical for successful Copilot integration. As AI continues to advance, your Microsoft 365 data protection must be comprehensive, compliant, and complete to meet the evolving demands of AI.

AI-Ready Data Protection Checklist	Key Requirements	Cloud Backup
✓ Comprehensive	Does the solution protect all Microsoft 365 services where data is created and stored? Does the solution offer unlimited storage to back up all data without constraints?	Protects Exchange, SharePoint, OneDrive, Teams, and Planner. Secur-Serv offers unlimited storage and retention at a fixed price.
✓ Compliant	Is the data protection solution aligned with multiple compliance standards? Is it straightforward to demonstrate and communicate compliance to stakeholders?	Our Cloud Backup adheres to multi-level compliance standards including HIPAA, GDPR, ISO, Cloud Security Alliance, and Data Pro certifications.
✓ Complete	Are all of your organization's data assets currently protected? Does the solution offer robust monitoring and automation features to ensure continuous protection and swift response to potential threats?	Has Smart Insights which allows you to have data-driven conversations to close the data protection gap. Additionally, has automation through M365 Groups Management.

Get started with intelligent data protection for Microsoft 365

BOOK A DEMO

SECUR-SERV

www.secur-serv.com