AvePoint

A Step-by-Step Guide to Secure, Scalable GenAI and Agentic AI Adoption in Microsoft 365

AvePoint

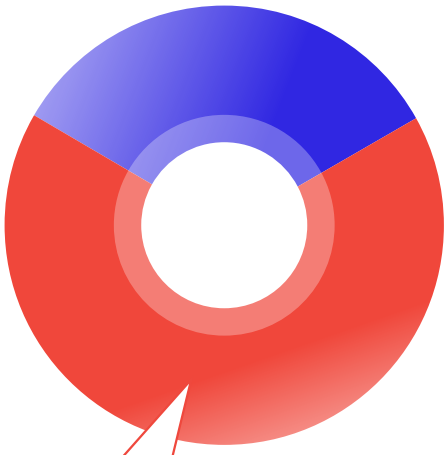
A STEP-BY-STEP GUIDE TO SECURE, SCALABLE GENAI AND AGENTIC AI ADOPTION IN MICROSOFT 365

Introduction

AI is delivering measurable impact. PwC's 28th Annual Global CEO Survey in 2025 revealed that for 56% of organizations, GenAI has resulted in time efficiencies for employees, while 32% report increased revenue. At the same time, organizations are expanding beyond foundational use cases. According to Boston Consulting Group, 35% have already begun using agentic AI, and another 44% plan to do so, signaling growing interest in more autonomous AI capabilities.

As AI adoption expands, many organizations are turning to tools such as Microsoft 365 Copilot and Copilot Studio Agents. From streamlining manual and repetitive processes to augmenting employee decision-making and accelerating innovation, AI is increasingly embedded in how work gets done. Microsoft reports that more than 90% of Fortune 500 companies trust Microsoft 365 Copilot and over 230,000 use Copilot Studio.

Because Microsoft integrates AI directly into familiar workflows and applications, it's easy to get Copilot up and running. However, it's important to recognize that simply acquiring the software and necessary licenses is not enough to ensure that your leaders and their teams can take full advantage of the new product. A McKinsey study found that nearly two-thirds of organizations remain stuck in the pilot phase, unable to scale AI across the enterprise. PwC further reports that challenges such as automating governance, clarifying roles and responsibilities, and aligning leadership around a consistent approach continue to slow progress.



2/3

OF ORGANIZATIONS HAVE YET TO SCALE AI ACROSS THE ENTERPRISE

That's where this guide comes in. This eBook is designed to help organizations address those challenges and scale generative and agentic AI within Microsoft 365 in a secure, responsible way. It outlines the key actions required to prepare and secure data, establish effective governance, and optimize operations as AI use grows.

With the right foundations in place, organizations can move beyond experimentation and realize sustainable value from AI across the enterprise.

4 Best Practices to Prepare for Sustainable AI Adoption

To support secure, sustainable AI adoption, organizations should focus on four best practices that address the most common readiness gaps.

Prepare Your Data

Centralize your data in Microsoft 365 and improve your data quality to enhance AI recommendations.

Secure Your Data

Understand where you have sensitive and overshared content in Microsoft 365, and implement robust measures to secure permissions and access controls.

Optimize Your Operations

Elevate your data management practices by implementing and enforcing governance controls to fuel sustainable AI success.

Govern Your AI Agents

Establish clear policies, roles, and oversight for AI agents to ensure they operate responsibly, securely, and in alignment with your organization's goals.

These best practices are not mutually inclusive. Even with a solid information management infrastructure in place, organizations still need to strengthen their data security. Applying the right strategies where gaps exist helps establish a strong foundation for scaling AI adoption within Microsoft 365.

PREPARE YOUR DATA

Centralize your data in Microsoft 365 and improve your data quality to enhance AI recommendations.

One of the most critical factors for successful AI implementation is **high-quality, well-organized data**.

GenAI and agentic AI algorithms rely on large amounts of data to learn and make accurate predictions; the quality of their output depends on the quality of the data they are trained on. If the data is decentralized, disorganized, outdated, non-compliant, or contains errors, algorithms may produce inaccurate results, leading to poor decision-making and business outcomes. That is why it is essential to prepare the data before feeding it into an AI system like Copilot.

With strong data management practices in place, you will be able to make data-driven decisions with confidence and improve the overall efficiency and effectiveness of your operations

How to Prepare Your Data for AI

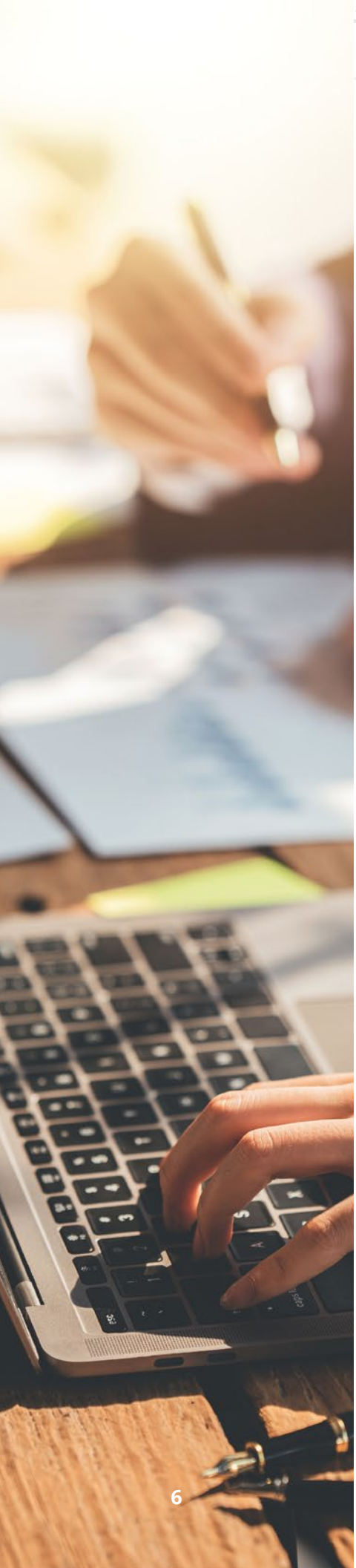
Centralize All Business-Critical Data to Microsoft 365

Copilot bases its recommendations and outputs on the data it can access in Microsoft 365. To provide the most accurate and comprehensive insights, any data you store elsewhere – such as self-hosted databases or other clouds – must be brought into your Microsoft 365 tenant so Copilot can analyze and make recommendations based on all relevant data. This will ensure that Copilot can provide accurate and complete insights. To achieve this, migrate all content to Microsoft 365 using AvePoint Fly.

Fly simplifies the migration process, providing flexibility and ease of use with real-time monitoring, granular scheduling, and robust security measures. Fly ensures a smooth, secure transition to Microsoft 365, enabling Copilot to access all relevant data.

Ask yourself:

Are there repositories outside of Microsoft 365 where some departments store business-critical data?



Complete a Data Inventory

The State of AI report 2025 revealed that 79.2% of organizations now manage 1 PB or more of data, up 25% from last year. This makes maintaining control over who can access what data across different cloud platforms increasingly challenging.

Once you have your data in the right environment, it's important to improve its quality. To start, conduct a discovery and analysis exercise to understand the data you have and how it is currently organized in your environment. A data assessment helps identify redundant, outdated, or trivial (ROT) data that clutters your environment and skews AI results.

Effective information management solutions will offer this capability. This will provide a clear picture of your data landscape, enabling you to make informed decisions to improve it. With this inventory in hand, you can clean up your data, remove duplicates and redundancies, and begin establishing information management processes and data governance policies. These measures help maintain high data quality over time and ensure that Copilot continues to provide valuable insights.

AI TRiSM Framework: Complete Guide to Trust, Risk, and Security in AI

READ NOW →

Classify Content to Improve Results

Now that you have a data inventory, it's time to organize it properly to improve the performance of your AI tools, such as Copilot.

One effective way to do this is to use metadata, labels, and tags to classify your content in Microsoft 365. Metadata provides information about your data, while labels and tags assign categories to it. AI tools like Copilot don't "read" all data equally — they rely on metadata, labels, and tags to understand what content is relevant, sensitive, authoritative, or up to date. When Copilot retrieves information, those classifications help prioritize what it can pull into an answer, while governance policies act as guardrails that determine whether it's allowed to use that data at all. By having these tags and classifications in place, AI can confidently surface the right information while respecting sensitivity, compliance, and access boundaries.

If you're struggling to manage your data effectively, AvePoint Opus can help. AvePoint Maestro, Opus' AI-powered classification capability, allows organizations to identify high-value content, tag and classify it at scale, and automatically apply the appropriate lifecycle policies. This prepares your data for AI even without significant manual input.

Prepare your Microsoft environment for AI with AvePoint.

Migrate your content to Microsoft 365.

Explore AvePoint Fly today.

AvePoint FLY

Take your information lifecycle management to the next level.

Explore AvePoint Opus today.

AvePoint Opus

SECURE YOUR DATA

Understand where you have sensitive and overshared content in Microsoft 365 and implement robust security measures to secure it.

About 63% of organizations either do not have or are unsure whether they have the right data management practices for AI, according to a Gartner survey. This is why data security and permission management go hand-in-hand when it comes to AI use. Although Copilot has native guardrails to protect privacy and ensure compliance and security, it can access information from anywhere it has permission. Thus, it's critical to monitor and strictly control its access.

To ensure your data remains secure while using Copilot, there are steps you can take.

How to Secure Your Data for AI

Run a Risk Assessment

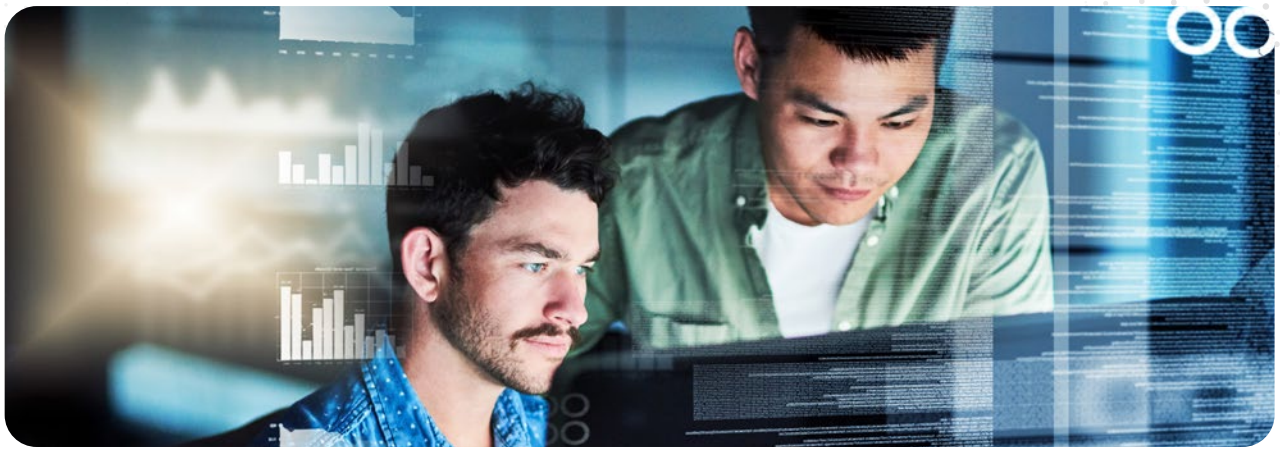
Protect your data by having visibility of the state of access controls in your organization. Running a risk assessment will help you identify your sensitive and overshared data in Microsoft 365, such as unprotected personally identifiable information (PII), financial data, and content with anonymous sharing links.

Then, assess your environment for security risks manually by reviewing each workspace's content and corresponding site permissions, or do it automatically with AvePoint Insights.

Insights allows you to scan and aggregate sensitivity and activity data across your Microsoft 365 tenant, seamlessly identifying permissions issues for action. Insights' risk priority matrix also helps admins know which issues to prioritize.

Microsoft 365 Copilot and Data Security: Ensure Your Information is Protected

READ NOW →



Clean Up Permissions and Enforce Policies

Now that you know what risks exist in your environment, it's time to act on them. Clean up any concerning permissions – consider a least privilege access model, especially for sensitive content – to ensure AI's output excludes information your entire organization shouldn't see. This is not only a critical step for AI, but also a gold standard for modern security postures to prevent unauthorized access to your data.

It's also a good idea to implement policies that mandate secure practices, such as limiting membership for Microsoft Teams or sites that contain confidential data, and train users on the proper controls they should implement to keep data secure. Alternatively, leave no room for error and use AvePoint Policies to automatically apply the necessary security rules to your Teams, Groups, Sites, and OneDrives, or your entire Microsoft 365 tenant if needed.

Policies proactively monitors configuration drift and reverts out-of-policy changes as often as every two hours to ensure proper access controls and permissions are applied without relying on end-user execution. It also provides out-of-the-box policies and custom-built policies that can easily be deployed for AI use cases.

Ask yourself:

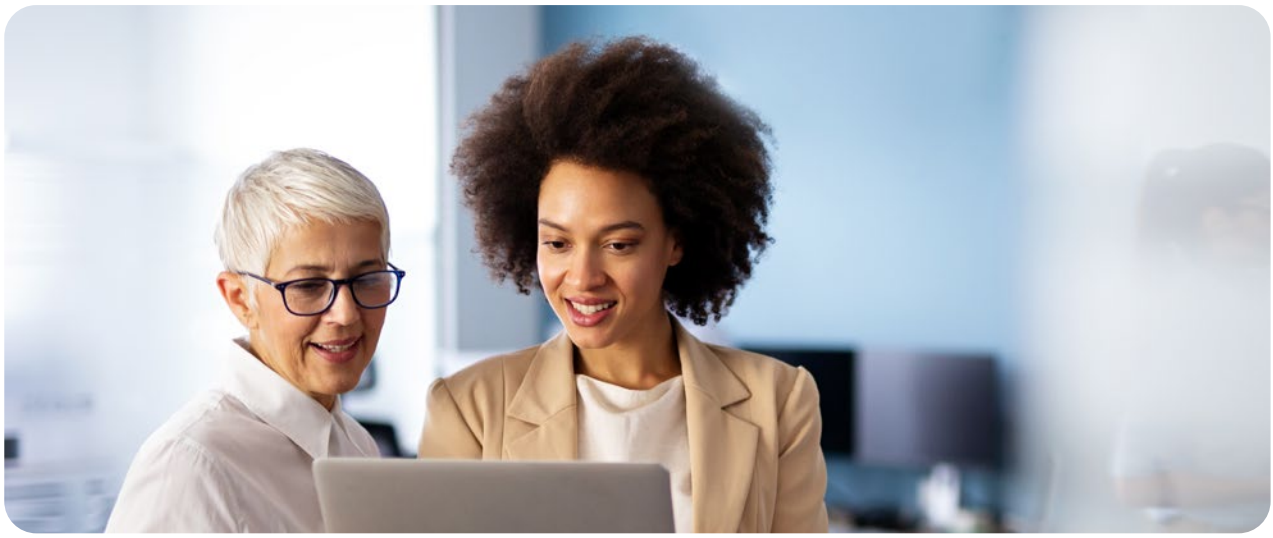
What sensitive data should Microsoft 365 Copilot not have access to?

By implementing these measures, you create guardrails that AI will respect, ensuring the continued security and compliance of your data.

Maintain Your Security Measures

Once your environment is in good shape, you'll want to keep it that way. Regularly review and update your security policies to ensure they remain up-to-date. This includes monitoring user activity, permissions, and access controls, as well as implementing new policies to address new and emerging concerns.

AvePoint Insights provides automated reporting in at-a-glance dashboards, as well as proactive alerts to flag anything amiss. If the solution flags an issue, you can adjust your security measures from within the tool in response to what it finds, making it fast and easy to act on any potential concerns.



OPTIMIZE YOUR OPERATIONS

Elevate your data management practices by implementing and enforcing governance controls to fuel sustainable AI success.

As you begin to leverage AI tools, you'll generate even more data. In fact, nearly 20% of organizations believe that in 12 months, more than half of their data will be created by GenAI. So how can you manage and govern this data safely to ensure its accuracy, security, and compliance?

Without proper maintenance, cracks can begin to surface, and AI's output could become inaccurate or inconsistent. That's why effective governance and data management are a must-have to ensure the way you leverage Copilot years down the road is the same safe and secure way you use it today.

Proactively setting up effective governance and data management processes can help your organization scale AI use without sacrificing security or compliance, driving long-term benefits and avoiding the risk of management issues and IT burden.

Ask yourself:

As AI adoption and data volume grow, can we maintain these security controls and management processes?

How to Optimize Operations for Copilot

Establish a Management Framework

As Microsoft 365 Copilot transforms the way we work, managing content, like data and workspaces, will become more complex. Users will be working faster, creating content more quickly, and producing large volumes of data. To keep up with this rapid pace, IT teams will need a consistent and structured framework that dictates what type of content Microsoft 365 Copilot can access, who is responsible for this content, and how often this content's settings are reviewed, among other concerns, to ensure nothing falls through the cracks.

AvePoint Cloud Governance provides a crucial role in establishing this framework by automating the delivery of certain IT services, such as provisioning Teams, Sites, and Groups, or applying conditional permissions and settings, ensuring content is created and maintained in accordance with your governance policies. By helping organizations implement an extensible Microsoft 365 governance strategy, Cloud Governance enables tighter control over Copilot without requiring end-user or IT intervention, delivering automated, secure management processes.

Implement Content Lifecycle Management

To ensure optimal AI performance, it's important to recognize that not all data is useful, and retaining data for the sake of retention can degrade the quality of AI output in Microsoft 365. Moreover, it introduces compliance risk when organizations hold on to data for longer than they should. AI can surface this non-compliant data. It is crucial to keep data only as long as necessary to ensure AI models are trained with high-quality, relevant data.

Automate content lifecycle management with AvePoint Opus. By automating business rules in Opus, you can manage the entire content lifecycle from creation and classification to archiving or disposal. This will not only improve the quality of your AI outputs but also help you reduce storage costs.

Automate Reviews and Renewals

Even with a strong governance strategy, it is important to double-check that the appropriate controls are applied to your content, especially when using AI. With AI's unparalleled access to content, it is essential to establish additional safeguards to ensure that content is secure and well-managed.

Content owners should regularly review permissions, memberships, and access controls to ensure content remains secure and continues to serve the organization's goals. AvePoint Cloud Governance can help establish these activities as part of a larger automated governance strategy. Organizations decide how often they'd like content owners to receive automated alerts to review and renew the content, streamlining security and management efforts.

Optimize your AI operations with AvePoint.

Automate a comprehensive governance strategy.

Explore AvePoint Cloud Governance today.

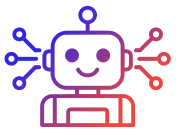
AvePoint Cloud Governance

Take your information management to the next level.

Explore AvePoint Opus today.

AvePoint Opus

GOVERN YOUR AI AGENTS



Establish policies, roles, and lifecycle controls to manage how AI agents are built, deployed, and monitored across the organization.

The promise of agentic AI is autonomy — but autonomy is powerful only when it's understood. Today, many organizations can't answer even the most basic questions about their agent ecosystem:

- What agents exist across the tenant?
- What data do they touch?
- Who owns them?
- Which agents are abandoned or redundant?
- Which ones present risk based on permissions or activity?

This isn't a documentation problem as much as a lack of oversight. When visibility is fragmented, ownership gets lost, permissions quietly drift out of alignment, and sensitive data exposure becomes easier. Shadow AI is inevitable when innovation outpaces visibility — and unchecked agents quietly take hold.

Visibility is the first pillar of responsible AI adoption. You can't govern access if you don't know which agents have it. You can't enforce ownership if you don't know who created what. You can't validate or retire unused automation if you don't even know it exists. Every other governance control depends on this foundation.

How to Govern Your AI Agents within Microsoft 365

Establish Clear Ownership and Accountability

Responsible AI governance requires someone to be accountable for every agent in the environment. Without clearly defined ownership, agents are easily abandoned as teams restructure, projects end, or employees move on. Establishing ownership ensures there is always a responsible party to review access, assess risk, approve changes, and determine whether an agent should continue operating.

AvePoint's AgentPulse Command Center maps every agent to its creator and owner, ensuring accountability doesn't disappear as teams evolve, roles change, or employees move on. With ownership clearly defined, organizations can enforce responsibility for ongoing maintenance, reviews, and risk management.

Maintain a Centralized Agent Inventory

AI agents can be created quickly — and just as easily forgotten. Manual inventories quickly become outdated as agents multiply across platforms and teams. You can't enforce ownership if you don't know who created what. You can't validate or retire unused automation if you don't even know it exists. Every other governance control depends on this foundation.

It is critical to have a centralized inventory that serves as a single source of truth for which agents exist, where they operate, and how they're being used. Without it, organizations are forced to rely on outdated spreadsheets, self-reporting, or incomplete snapshots that can't keep up with the pace of innovation. AgentPulse continuously discovers and surfaces every agent automatically, creating a trustworthy inventory — without spreadsheets, self-reporting, or department-by-department checks.

Understand Agent Access and Data Exposure

Not all agents pose the same level of risk. Governance depends on understanding which agents access sensitive data, how permissions have evolved over time, and whether access still aligns with business intent. Gaps in visibility make it difficult to detect permission creep, overexposure, or misconfigurations before they result in compliance or security issues.

AgentPulse provides clear insight into which agents access sensitive data, where permissions have expanded beyond their original intent, and which configurations require attention, helping organizations identify exposure risks before they become incidents.

Understand Agent Access and Data Exposure

Not all agents pose the same level of risk. Governance depends on understanding which agents access sensitive data, how permissions have evolved over time, and whether access still aligns with business intent. Gaps in visibility make it difficult to detect permission creep, overexposure, or misconfigurations before they result in compliance or security issues.

AgentPulse provides clear insight into which agents access sensitive data, where permissions have expanded beyond their original intent, and which configurations require attention, helping organizations identify exposure risks before they become incidents.

Track Consumption and Cost to Manage ROI

As agent usage expands, so does consumption. Tracking usage patterns and costs allows organizations to separate high-value agents from those that are underused, redundant, or no longer delivering value. Visibility into consumption supports informed decisions about optimization, cost control, and long-term return on investment.

AgentPulse makes consumption visible by showing usage patterns and pay-per-use interactions, allowing organizations to distinguish high-value agents from dormant or redundant ones and make informed decisions to manage spend and maximize ROI.

Building a Secure, Scalable AI Future

AI tools, such as Microsoft 365 Copilot, Copilot Studio, and Azure AI Foundry, offer organizations a powerful way to optimize their Microsoft 365 environments and achieve their business goals. Remember the old saying, though: with great power comes great responsibility.

That is why a successful and sustainable AI adoption requires sufficient preparation and governance controls. By taking the necessary steps to harness the power of AI and implementing effective data practices, organizations can reap all the benefits of GenAI and agentic AI, including:

- Saving time and increasing productivity
- Enhancing employee skills
- Driving rapid innovation

AvePoint offers a holistic approach to AI adoption: The AvePoint Confidence Platform can help you build a robust data foundation, security, and a sustainable approach to AI. With our expertise and support, you can establish a solid foundation for AI success.

AvePoint US Headquarters
525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310
+1.201.793.1111 | sales@avepoint.com