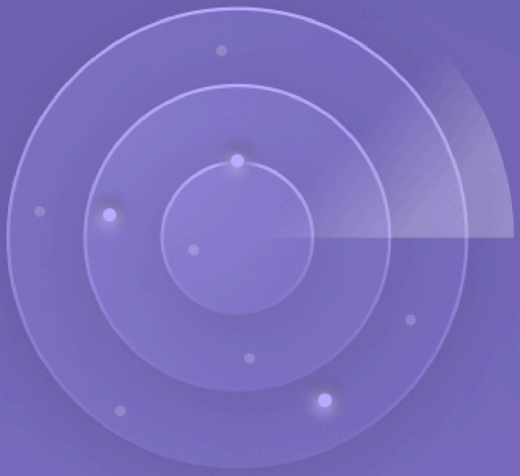
EBOOK

Secure Microsoft 365 Copilot Adoption

Sentra, Inc. 2025



Confidential

Executive Summary

Microsoft 365 Copilot introduces a new era of productivity, embedding powerful generative AI into the everyday tools organizations rely on, like Word, Excel, Outlook, and Teams. But with innovation comes new risk. Copilot's ability to surface and echo enterprise data means sensitive information, intended or not, can appear in generated content. Without proactive data governance, Copilot may inadvertently amplify exposure of outdated, over-permissioned, or unlabeled data.

That's where Sentra comes in. As a leader in cloud-native data security posture management (DSPM), Sentra helps security teams unlock the value of AI securely. This paper outlines the key risks introduced by Copilot, how Sentra mitigates each one, and what a secure deployment roadmap looks like for large, cloud-first organizations.

The Promise and Peril of Microsoft 365 Copilot

Copilot brings enterprise-grade AI into the productivity suite, helping teams move faster, communicate more effectively, and surface relevant content through natural language queries. But beneath the convenience lies a critical shift: AI systems like Copilot aggregate data from across Microsoft 365 sources (SharePoint, OneDrive, Teams, Outlook) in the user's environment, or shared with the user. If a user has access to sensitive information, regardless of whether they should, it can surface in Copilot outputs.

Core mechanisms compound this risk:

- **Data Aggregation:** Copilot queries all user-accessible data, including buried or forgotten files that were previously 'secure by obscurity'.
- **Context Stitching:** It can combine benign data points into sensitive inferences.
- **Sprawl Risk:** Content generated by Copilot can inadvertently include sensitive or regulated data, potentially violating internal policies or external compliance mandates.

Security teams must now assume that if a user can access it, Copilot can surface it. Managing this new exposure boundary requires data security posture management, access governance, and policy enforcement. Sentra delivers all three.

Addressing three key risks of M365 Copilot adoption

1. Unnecessary data exposure & shadow data

The risk:
Legacy files, test environments, or outdated snapshots often contain sensitive data. In the past, they lived in obscurity. Now, Copilot’s smart querying brings them into the spotlight, sometimes unintentionally.

Sentra solution:

- Discovers and classifies sensitive data across SharePoint, OneDrive, and Teams.
- Identifies redundant, outdated, or orphaned files known as "shadow data."
- Provides visibility and context to support deletion, archiving, or remediation.

With Sentra, teams gain complete visibility into what data exists, where it resides, and whether it should be retained. This is the foundation of a secure Copilot deployment.

2. Improper access & overpermissioning

The risk:
Employees often have access to more data than they need. This overpermissioning was already a risk, but with Copilot summarizing across everything a user can see, the blast radius grows.

Sentra solution:

- Shows a summary of all data accessible by an identity.
- Maps sensitive data to the identities that can access it.
- Surfaces over-permissioned users and enables quick remediation.
- Reinforces least-privilege access principles through granular insights.

Security teams can pinpoint where policy enforcement breaks down, like a junior employee accessing HR records, and take immediate action to prevent misuse or accidental exposure through Copilot.

3. Data leakage in AI-generated content

The risk:
Even in a sanitized environment sensitive data exists and can be accessed and included in Copilot output. DLP can protect against this, but it relies on MPIP labels. Manual or misconfigured labeling (or total lack of labeling) leads to files being left unprotected. So even with Microsoft Purview in place, its classification and auto-labeling rules often lack the context to catch every sensitive asset.

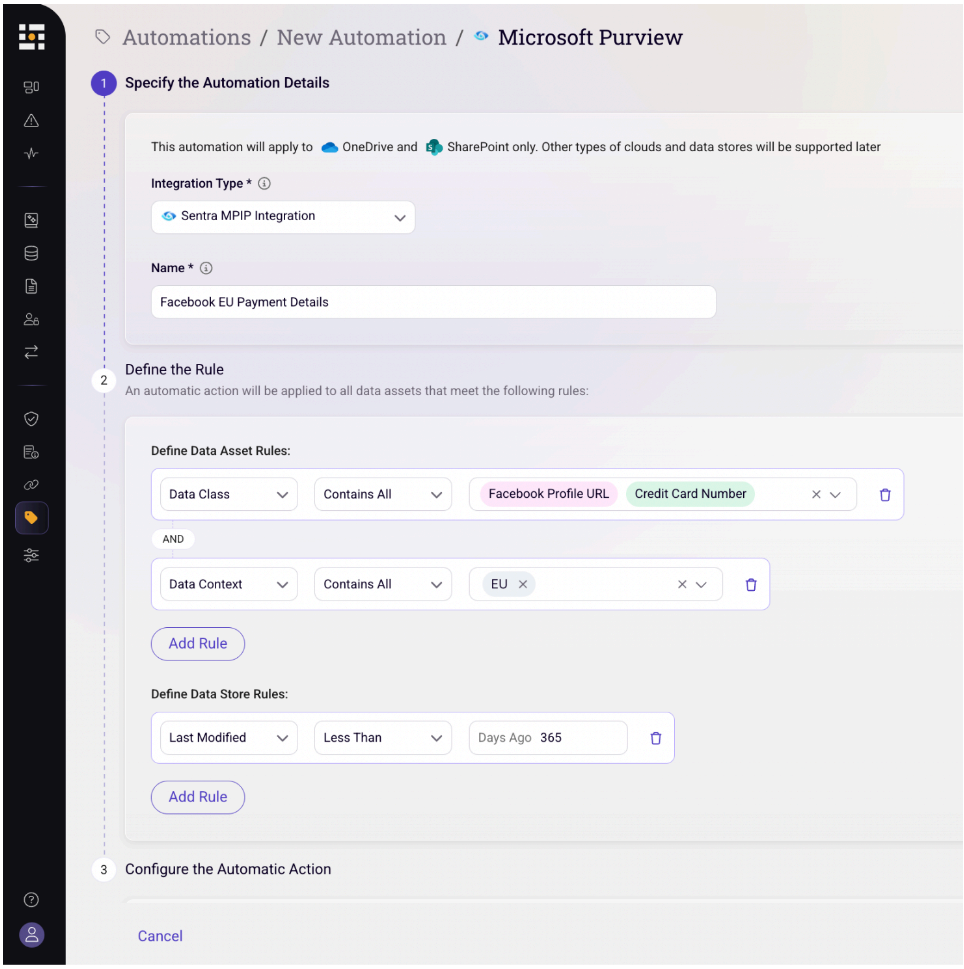
Sentra solution:

- Rich, high-accuracy classification of structured and unstructured data, using AI/ML, regular expressions, dictionaries, and metadata.
- Automatically applies Microsoft Purview Information Protection (MPIP) sensitivity labels at scale, based on in-depth custom business logic.
- Continuously monitors for incorrect or missing labels and remediates them.

Correct labeling isn't just a best practice, it's the prerequisite for Copilot's internal DLP policies. Copilot will not include information from data assets labeled with defined MPIP labels - reducing the risk of sensitive data sprawl and leakage.

Seamless Integration with Microsoft Purview

Sentra integrates directly with Microsoft Purview with rich, comprehensive custom labeling logic extending and automating its capabilities:



Automations / New Automation / Microsoft Purview

1 Specify the Automation Details

This automation will apply to OneDrive and SharePoint only. Other types of clouds and data stores will be supported later

Integration Type *: Sentra MPIP Integration

Name *: Facebook EU Payment Details

2 Define the Rule

An automatic action will be applied to all data assets that meet the following rules:

Define Data Asset Rules:

Data Class | Contains All | Facebook Profile URL, Credit Card Number

AND

Data Context | Contains All | EU

Add Rule

Define Data Store Rules:

Last Modified | Less Than | Days Ago 365

Add Rule

3 Configure the Automatic Action

Cancel

Proven Outcomes for Cloud-First Enterprises

Sentra customers in technology, finance, healthcare, and retail/ecommerce report:

- Up to 80% reduction in exposed sensitive data.
- Significant decrease in audit findings and compliance violations.
- Streamlined operations through automation and centralized governance.
- AI-readiness with confidence—turning Copilot into an asset, not a liability.

From Risk to Readiness: Getting Started with Sentra

AI is already transforming how we work. Microsoft 365 Copilot offers incredible promise, but only for organizations that match innovation with responsibility. Sentra helps security teams do just that.

Implementing a secure Copilot deployment with Sentra is straightforward and fast. The process includes:

1. **Data Discovery:** Scan all M365 repositories (SharePoint, OneDrive, Teams) to locate sensitive data.
2. **Classification:** Accurately tag data by sensitivity class and context automatically.
3. **Access Review:** Map identity-level access to sensitive assets; enforce least privilege.
4. **Policy Activation:** Define and apply custom MPIP label logic and enable Microsoft 365 Compilot DLP policies.
5. **Continuous Monitoring:** Maintain hygiene with automated alerting, and actionable insights.

Sentra customers typically see results within days to weeks, achieving both rapid time to value (TTV) and long-term security gains.

By discovering, classifying, and protecting sensitive data across the Microsoft 365 stack, Sentra empowers organizations to adopt Copilot with confidence. With you at the helm, your company can lead securely into the AI-powered future.

Ready to get started?
Book my demo
Visit Sentra Microsoft 365 Copilot