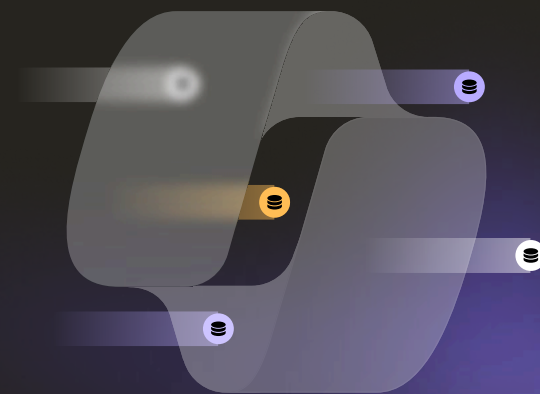




Secure Microsoft 365 Copilot Adoption

Prevent privacy and compliance violations and sensitive corporate data leakage.



The Data Blind Spots Holding Back Copilot Adoption

Microsoft 365 Copilot injects generative AI into core productivity apps like Word, Excel, Outlook, and Teams, but its ability to surface data across SharePoint, OneDrive, and Teams also creates a serious risk. Forgotten legacy files, shadow data, and over-permissioned repositories may suddenly appear in prompts and outputs. Without full visibility and governance, enterprises risk data leakage, compliance violations, and reputational damage.

Stop Shadow Data and Over-Permissioning Before They Surface in Copilot

Copilot respects Microsoft Entra ID permissions, but that also means any data a user can access, including files they shouldn't, can appear in responses. Outdated HR records, unsecured financial data, or unclassified PII may be aggregated or echoed into generated outputs. Shadow data and improper sensitivity labeling compound the risk. The [2024 EY Human Risk in Cybersecurity Survey](#) found that 80% of CISOs were concerned about AI assistants exposing sensitive data, but most lacked the real-time monitoring or remediation needed to prevent it. Copilot magnifies existing cracks in governance, turning small permission issues into systemic enterprise risks.

Sentra Secures Copilot Data Access and Output End-to-End

Sentra enables organizations to adopt Microsoft 365 Copilot securely by discovering and classifying sensitive data across SharePoint, OneDrive, Teams, and Exchange before Copilot accesses it. The platform discovers shadow data, enforces least-privilege access, and applies Microsoft Purview Information Protection (MIP) sensitivity labels automatically at scale. These labels feed directly into Purview and Copilot DLP policies, ensuring sensitive data can't be surfaced in AI-generated content. Sentra continuously monitors Copilot interactions, enforcing data encryption, data masking, and access policies in real time. With automated governance mapped to frameworks like GDPR, HIPAA, and the EU AI Act, enterprises can embrace Copilot without compromising compliance or trust.

Dashboard

Issues

Threats

Catalog

Data

Data Stores

Data Assets

Identities

AI & ML

Similar Data

Control

Policies

Reports

Integrations

Automations

Settings

+ AI & ML

☆

Sensitivity

Data Class

Data Context

Account

Service

Model Family

Save View

Q Search AI Asset

< 1 / 1 >

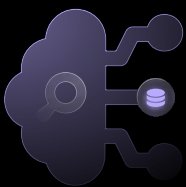
[6] 6 Columns

Export

Showing 10 AI & ML Assets

Name	Account	Model Family	Sensitivity	Data Class	Data Context
HR Agent Agent	Acme M365 Microsoft Copilot Studio	GPT	High	Employee ID 30K Home Address 29K +2	HR U.S. Employee Data
RFI Agent Agent	Acme M365 Microsoft Copilot Studio	GPT	High	Customer Name 1M Email Address 985K +1	Intellectual Property
Support Bot Agent	ACME-PROD Amazon Bedrock	Claude	High	User Email 24K Ticket ID 23K +1	E.U. Customer Data
Compliance Assistant Agent	ACME-PROD Amazon Bedrock	Claude	High	Policy ID 21K Compliance Violation Logs 20K +1	Corporate Security
Customer Insights Agent Agent	Acme M365 Microsoft Copilot Studio	GPT	High	Customer ID 25K Demographic Data 23K +1	E.U. Customer Data
Finance Bot Agent	ACME-GOOGLE Google Vertex	GPT	Moderate	Transaction History 20K Bank Account Number 18K +1	Corporate Financials
IT Helpdesk AI Agent	ACME-PROD Amazon Bedrock	Claude	Moderate	Support Tickets 20K Device ID 19K +1	Intellectual Property
Employee Onboarding Assistant Agent	Acme M365 Microsoft Copilot Studio	GPT	Moderate	New Hire Info 22K Government ID 22K +1	HR Intellectual Property
Compliance Advisor Agent	Acme M365 Microsoft Copilot Studio	GPT	Moderate	Audit Logs 21K Access Records 20K +1	Intellectual Property
Incident Reporting Assistant Agent	Acme M365 Microsoft Copilot Studio	GPT	Moderate	Incident ID 23K Witness Statement 23K +1	Legal Employee Data

Why Enterprises Trust Sentra to Secure Microsoft 365 Copilot



Discover and classify sensitive data across SharePoint, OneDrive, and Teams



Apply and enforce
MPIP sensitivity labels
automatically



Identify and remediate shadow data and over-permissioned access

How An Insurance Provider Securely Scaled M365 Copilot

An insurance provider used Sentra to securely roll out Microsoft 365 Copilot to an initial test group of ~200 employees. During deployment, Sentra discovered shadow PII buried in employee OneDrives and flagged over-permissioned access to HR data (as possible compliance violation) that could have surfaced in Copilot prompts. It automatically applied MPIP sensitivity labels and enforced access controls, preventing data leakage. The pilot gave the CISO confidence to scale Copilot adoption enterprise-wide to over 2,500 employees without introducing new data risks. Enterprise wide deployment helped the company reduce its exposed sensitive data footprint by nearly 80% and pass a GDPR compliance audit.

Ready to Secure Your Copilot Deployment Before It Exposes Sensitive Data?

Get A Demo

or learn more in our guide:

[Adopt Microsoft 365 Copilot Securely with Sentra.](#)

