sentra

Secure Microsoft 365 Copilot Adoption

Prevent privacy and compliance violations and sensitive corporate data leakage.

The Data Blind Spots Holding Back Copilot Adoption

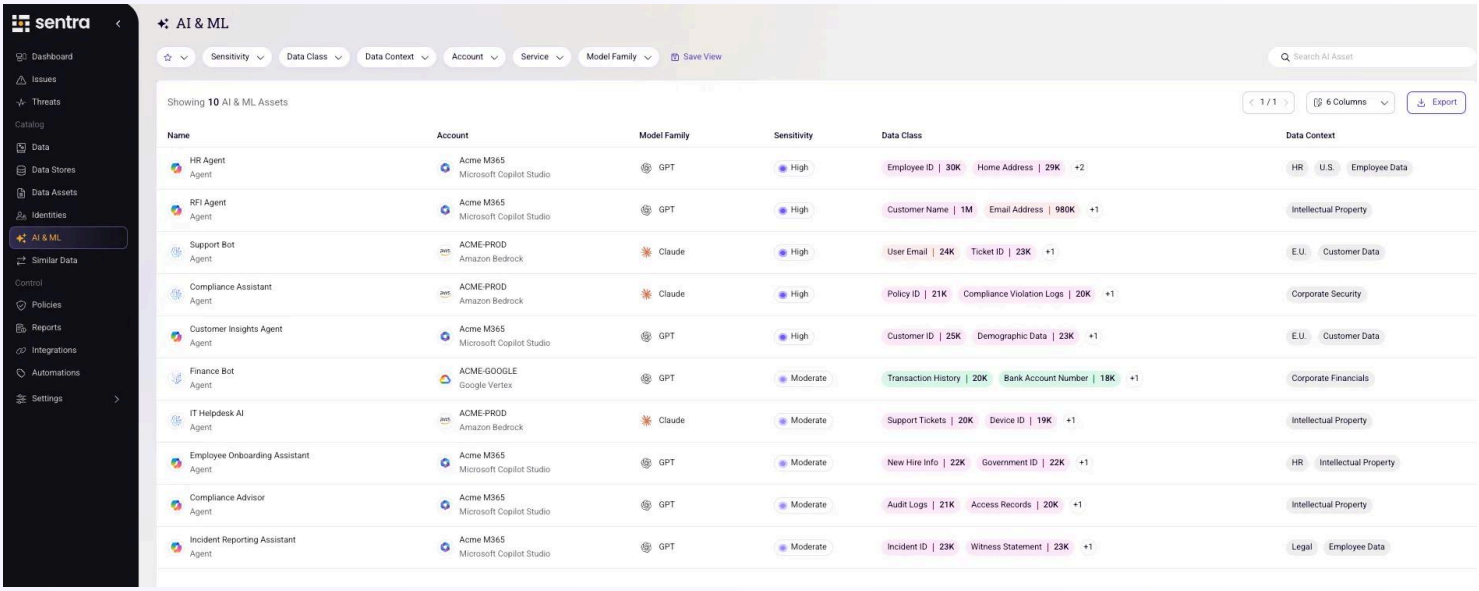
Microsoft 365 Copilot injects generative AI into core productivity apps like Word, Excel, Outlook, and Teams, but its ability to surface data across SharePoint, OneDrive, and Teams also creates a serious risk. Forgotten legacy files, shadow data, and over-permissioned repositories may suddenly appear 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

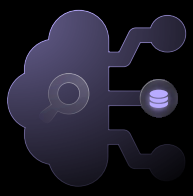
Copilot respects Microsoft Entra ID permissions, but that also means any data a user can access, including files they shouldn't, can appear in responses. Outdated HR records, unsecured financial data, or unclassified PII may be aggregated or echoed into generated outputs. Shadow data and improper sensitivity 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 (MPIP) 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.



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.

sentra