CONCENTRIC Ai

# Five Myths About Copilot Security

Copilot is powerful. But it isn't nearly as secure as you think it is.

## Copilot inherits your existing security controls

**The truth:** The content that Copilot produces doesn't inherit sensitivity labels from the source files. If the source file contained sensitive data, it is possible that the new document will have it as well, but will be unclassified.

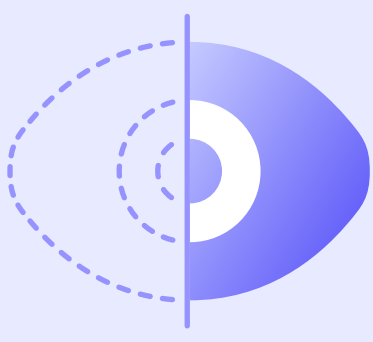
**Why it matters:** If your classification strategy relies on inheritance, you're flying blind while Copilot's serving up spoilers.

## Microsoft Purview takes care of Copilot Access

**The truth:** Yes, Purview can label and monitor M365 data. But it doesn't track what Copilot generates, what it references, or who it whispers secrets to.

**Why it matters:** Copilot creates a whole new layer of data sprawl... like you needed another layer.

## Copilot's access is limited to what users can see



**The truth:** Technically, yes. But "what users can see" often includes a lot they shouldn't, thanks to unclassified and misclassified data and misconfigured permissions.

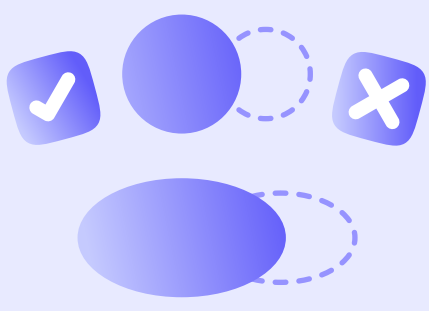
**Why it matters:** Trusting old permissions is like trusting everyone did folder hygiene. Spoiler: they didn't.

## If a file is labeled, it's good to go for security

**The truth:** Many data records are misclassified. Copilot won't know if your label is wrong. If it can read a file, it can spill it. Shared folders and loose permissions included.

**Why it matters:** Bad labels upstream = bigger mess downstream. Copilot just speeds up the crash.

## Users will know what data is safe to use

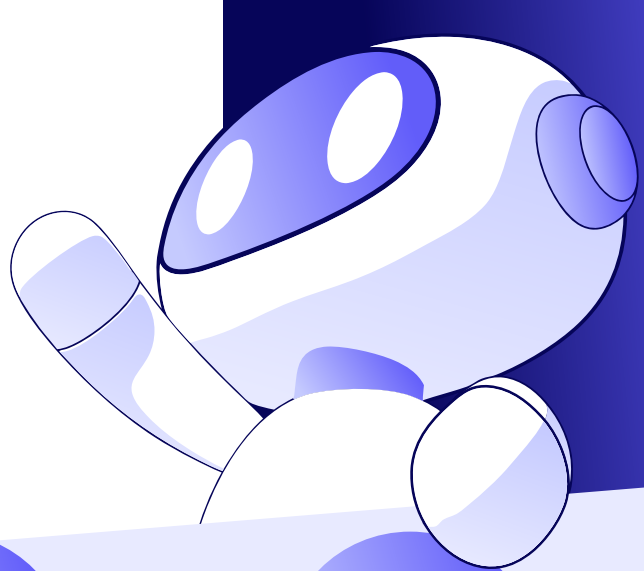


**The truth:** Most users assume if Copilot shows it, it's safe to share. Meanwhile, that "safe" doc could leak unreleased financials or a client NDA.

**Why it matters:** Relying on users to double-check AI output is like asking interns to run legal review. That's more liability than strategy.

## Know Your Data, Secure Your Copilot

With Semantic Intelligence™ you control what Copilot can access and still keep everyone productive.



Know what Copilot can retrieve and eliminate surprise data leaks.

Fix permissions before sensitive data becomes searchable and accessible.

Enjoy the productivity and innovation of Copilot without the security risks.

**Want to test your data to see how Copilot-ready it is? Request a demo today.**

Schedule a Demo