

COPILOT WITH SYMANTEC DLP

SECURE YOUR DATA BEFORE ENABLING COPILOT WITH SYMANTEC DLP

Like many Generative AI tools, Microsoft Copilot opens the door to productivity but also lets in risks. Integrated across the entire Microsoft 365 platform, it can potentially access any document, presentation, email, spreadsheet – and more. This includes your most valued and sensitive data. To use Copilot safely and productively, you need to set the boundaries (with the right data governance) from the outset.

CHALLENGES & RISKS

The key areas to resolve before you deploy Copilot!

HOW ARE YOU GOING TO BUILD YOUR DLP SYSTEM?

If you are already using Symantec DLP – good news, it’s easy to extend it provide data governance for Copilot. If you need to build a system from scratch, pick a market leading solution that covers all the bases.

Symantec DLP is renowned for accurate detection, full integration with MSFT, deployment at scale and can help you find, classify and label sensitive data fast.


1. IDENTIFYING SENSITIVE DATA

To protect your confidential data, you first have to find it, inspect it for sensitive content and label it correctly. The challenge is you need a consistent, accurate approach. An approach that will work on data that hasn’t been touched in a while, reflects your latest data security policies and is repeatable (how else will you protect new data that is generated).

Symantec DLP does all this, and integrates with Microsoft Purview to ensure Copilot knows what it can interact with, and what to leave alone.

RISK

A confused Copilot fails to recognise your confidential documents, risking data leakage.



2. LABELLING NEW CONTENT

Content generated by Copilot doesn’t automatically **inherit the security labels of its source files**. This leaves employees left to determine whether new content should be classed as confidential.

RISK

Employees may see and share sensitive information from mislabelled documents.



3. EXCESSIVE PERMISSIONS

Copilot adopts the same access rights as its users, but employees often have more permissions than they’re supposed to. This allows Copilot to access sensitive content and share it with unauthorised users.

RISK

“Over-permissioning” increases the risk of unauthorised data access and exposure.



4. INTEGRATION WITH MICROSOFT 365

All of the above is made harder due to Copilot’s deep integration with the Microsoft 365 family. **This adds complexity to data governance**, making it harder to maintain visibility and enforce least privilege access.

RISK

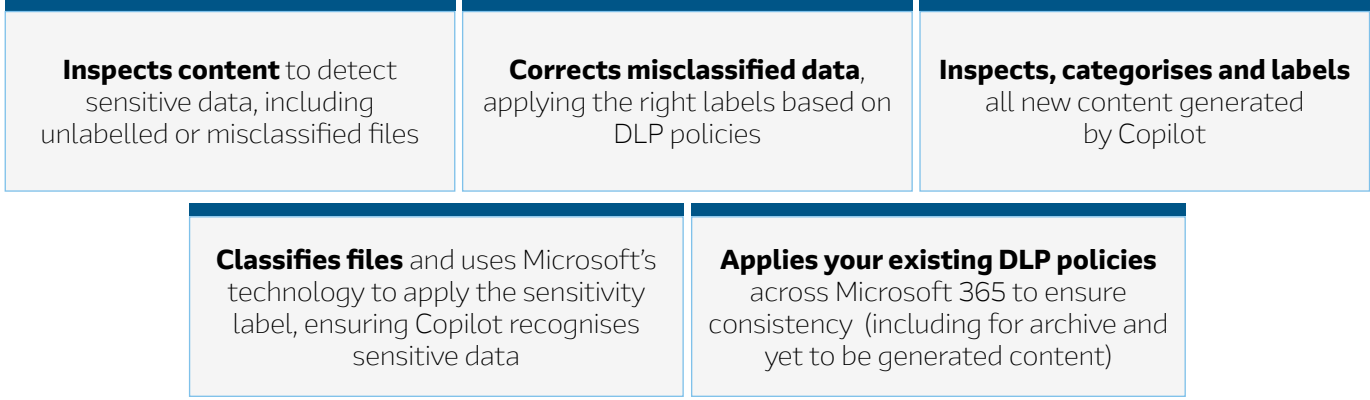
The greater the scope and complexity, the greater the risk of data exposure.



SYMANTEC DLP – THE BETTER WAY TO ENABLE COPILOT

Symantec DLP offers unique advantages to organisations deploying Copilot. Seamless integration with Microsoft 365 makes it easier to enforce consistent data governance across the entire ecosystem, protecting your data everywhere it goes.

THE AUTOMATED SOLUTION



SIMPLE, UNIFIED DATA PROTECTION

Using Copilot safely requires robust data governance. With Symantec DLP, it doesn’t have to be complex.

To see how it works in practice, get in touch today.