# Safely navigate AI adoption with Symantec DLP

With AI in the fast lane, the data governance challenges are accelerating.
Symantec Data Loss Prevention (DLP) can help you pilot compliance
and turbocharge your data protection controls.

## Public AI

eg ChatGPT – can contain data from anyone

## Enterprise AI

eg Copilot for Office 365 – a publicly available
AI model that only works on your internal data

**How do I use AI safely?**

**What AI apps are out there?**

**What internal data needs to be excluded from AI analysis?**

**Should AI have all my data?**

**Are they risky?**

Symantec DLP analyses the risks associated with Gen AI apps using 300+ researched attributes.

**How do I find, and mark, sensitive data (even archived data) so Enterprise AI doesn't access it?**

Symantec DLP identifies files that contain sensitive data and specifies how to classify them so that Enterprise AI understands what it can and cannot access.

**Who is using what?**

Symantec DLP monitors Gen AI apps use in real-time showing attributes such as user, location, device information and data shared.

**How do I make the process repeatable and simple to operate so I can protect future data in the same way?**

Using accurate, unified policies, Symantec DLP ensures that you apply the same protection to tomorrow's data as you do to today's.

**What data is being uploaded (via prompts) to AI systems?**

**What data is being uploaded (via prompts) to public AI for my systems?**

## AI Generated Content

**How do I protect what AI creates?**

**How do I scan and protect new AI content? I need to find sensitive data at rest or in use.**

AI generated content can't always be classified by a user. Symantec DLP reliably automates data classification decisions.