



Advania Private ChatGPT with Azure OpenAI

Reducing corporate risk from
ChatGPT on the public internet



Why do I need this?



The issue: using ChatGPT on the internet presents a significant business risk. Employees commonly share sensitive data without understanding how ChatGPT uses it

- Some controls exist, but asking all employees to individually make sure they've pressed a certain button doesn't work. There are no org-wide controls.
- OpenAI use everything sent to train their AI models further**



6. Will you use my conversations for training?

- Yes. Your conversations may be reviewed by our AI trainers to improve our systems.

7. Can you delete my data?

- Yes, please follow the [data deletion process](#).

8. Can you delete specific prompts?

- No, we are not able to delete specific prompts from your history. Please don't share any sensitive information in your conversations.

ARTIFICIAL INTELLIGENCE

Oops: Samsung Employees Leaked Confidential Data to ChatGPT

Employees submitted source code and internal meetings to ChatGPT just weeks after the company lifted a ban on using the chatbot.

ChatGPT could be a security nightmare waiting to happen

ScienceAlert on MSN · 1d

Many Companies Are Banning ChatGPT. This Is Why.

ChatGPT is proving to be a rather alluring assistant in many professions, but it's not without risks, and some companies have ...

NEWS

'Shadow' AI use becoming a driver of insider cyber risk

Off-the-books use of generative AI tools will inevitably lead to a costly, high-profile data breach for someone,

What does the solution consist of?

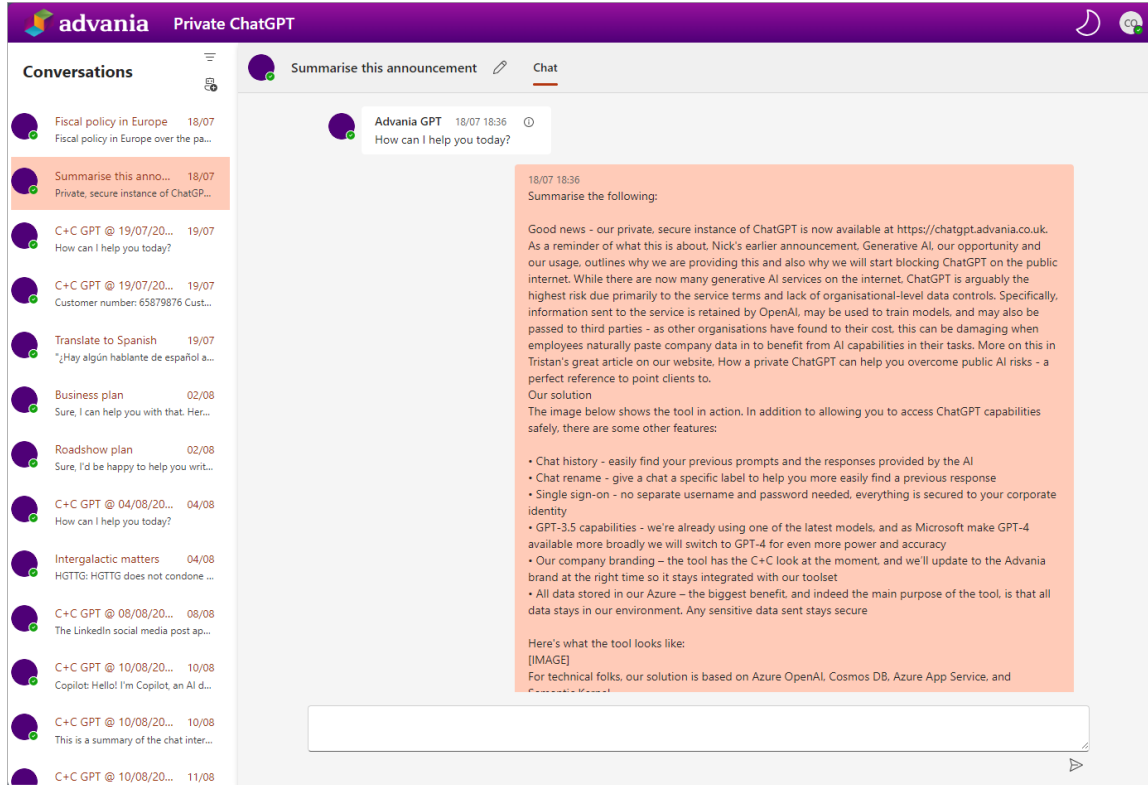


Advania implement our 'Private ChatGPT' solution entirely hosted in your Azure environment

- ◆ All data is now kept within your Azure subscription – no data is shared with the internet or the OpenAI organisation
- ◆ Data is NOT used to train models or enhance the service - any sensitive data sent stays secure
- ◆ All the benefits of 'trusted Azure' apply - security, compliance, privacy, and data sovereignty
- ◆ Users interact with a simple web application within your environment
- ◆ Solution uses **your** company branding

The screenshot shows the Advania Private ChatGPT interface. The header is purple with the Advania logo and 'Private ChatGPT' text. A sidebar on the left lists several conversations, including 'Fiscal policy in Europe', 'Summarise this anno...', 'C+C GPT @ 19/07/20...', 'Translate to Spanish', 'Business plan', 'Roadshow plan', 'C+C GPT @ 04/08/20...', 'Intergalactic matters', 'C+C GPT @ 08/08/20...', 'C+C GPT @ 10/08/20...', and 'C+C GPT @ 10/08/20...'. The main chat area shows a conversation with 'Advania GPT' where the user asks 'How can I help you today?'. The AI response, dated 18/07 18:36, provides a summary of the service and lists features such as chat history, chat rename, single sign-on, GPT-3.5 capabilities, company branding, and data security. The response also includes a placeholder for an image and technical details about the solution's infrastructure.

Can't I do this myself? What's the special sauce?



While creating an Azure OpenAI instance is relatively easy for an experienced in-house Azure team, providing a front-end to the business is the bigger challenge.

We've invested effort in refactoring code and building on a Microsoft sample app to provide:

- + Production-grade quality
- + Suitability for real world deployment
- + Removal of unnecessary Azure complexity and Semantic Kernel demo code not required for core capability
- + **Azure consumption costs reduced from ~£5-7k per year to less than £1k per year**



Technical architecture

Technical details - what gets deployed to Azure?

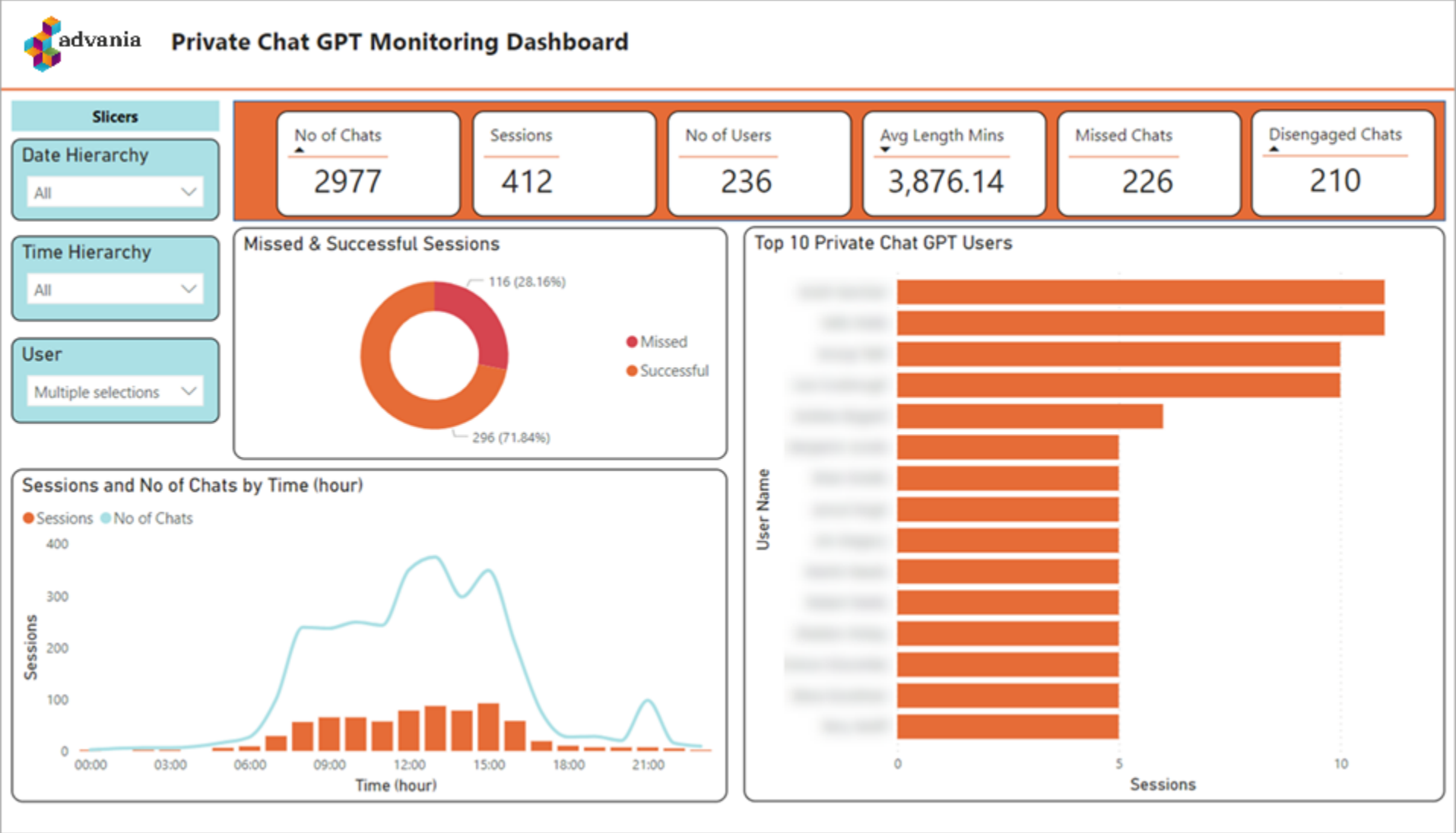


| Resource | Used for | Details | Pricing tier (recommended) | Tier flexibility? |
|--|--|--|----------------------------|---------------------------------|
| Azure OpenAI instance | Provides Azure-hosted ChatGPT | Can be provisioned to a different region to other components if required (e.g. for GPT-4) | Standard S0 | No – consumption based |
| Azure App Service/ App Service Plan | Hosts the web application and API used by the tool | Back-end API integration is via API key (as per default Microsoft sample) | Standard S1 | Yes (F1/D1 plans not supported) |
| Azure Cosmos DB | Database used to store user's chat history and provide other features (N.B. data is non-critical) | Minimal config used: + Serverless capacity mode (elastic pricing) + Default 7-day backup | N/A | N/A |
| Azure App Insights | Logging and diagnostics | | N/A | N/A |
| Entra ID (AAD) App Registration | Single sign-on | Only permission required is User.Read – solution does not access data | N/A | N/A |




Power BI reporting

Analytics – usage overview



Analytics – conversation detail




Private Chat GPT Monitoring Dashboard-All Chats Drill-through
⏪

All Chats
🔍 🗒️ ⋮

| Session Title | User Name | Timestamp | Date | Content |
|--------------------------------|------------|---------------------|----------------|---|
| C+C GPT @ 2023/08/09, 07:50:01 | [Redacted] | 09/08/2023 14:54:38 | 09 August 2023 | proof read this for me |
| C+C GPT @ 21/07/2023, 15:46:56 | bot | 09/08/2023 14:54:02 | 09 August 2023 | <p>It looks like there's an issue with the 'Get-CsOnlineApplicationInstance' cmdlet, which is returning a null-valued permission to access Microsoft Teams Online application instance information, or if there are no auto attendants.</p> <p>To troubleshoot this issue, you can try running the 'Get-CsOnlineApplicationInstance' cmdlet by itself to see if it returns any auto attendants, then that is likely the cause of the error. If it does return results, then you may need to check your permissions to access Microsoft Teams Online application instance information.</p> <p>Additionally, I noticed that there seems to be some incomplete code in the script (e.g., lines 17-23). Please review the script and ensure it is functional.</p> <p>Let me know if this helps!</p> |
| C+C GPT @ 21/07/2023, 15:46:56 | [Redacted] | 09/08/2023 14:53:55 | 09 August 2023 | <p>## Auto Attendant Selection Script</p> <pre> \$autoAttendantArray = @() \$autoAttendantList = Get-CsOnlineApplicationInstance Where (\$_.TypeDisplayName.Contains("Auto attendant")) for (\$i=0; \$i -lt \$autoAttendantList.Count; \$i++) { if(\$autoAttendantList[\$i].TypeDisplayName.Contains("Auto attendant")) { if(\$autoAttendantList[\$i].LocationProfile.StartsWith("/") { continue # Skip auto attendants located in subfolders of root directory. } else{ continue } } } </pre> |

Total



Leveraging AI beyond Private ChatGPT

The AI journey for some of our clients



For many organisations, the value comes from integrating organisational data

Now

1

Deploy core Private ChatGPT (this scope)

- + Provide safe, compliant ChatGPT access with a branded and integrated tool
- + Choose between Standard and Premium options
- + Gather feedback and use cases from the business

Release 1

Support for your use cases:

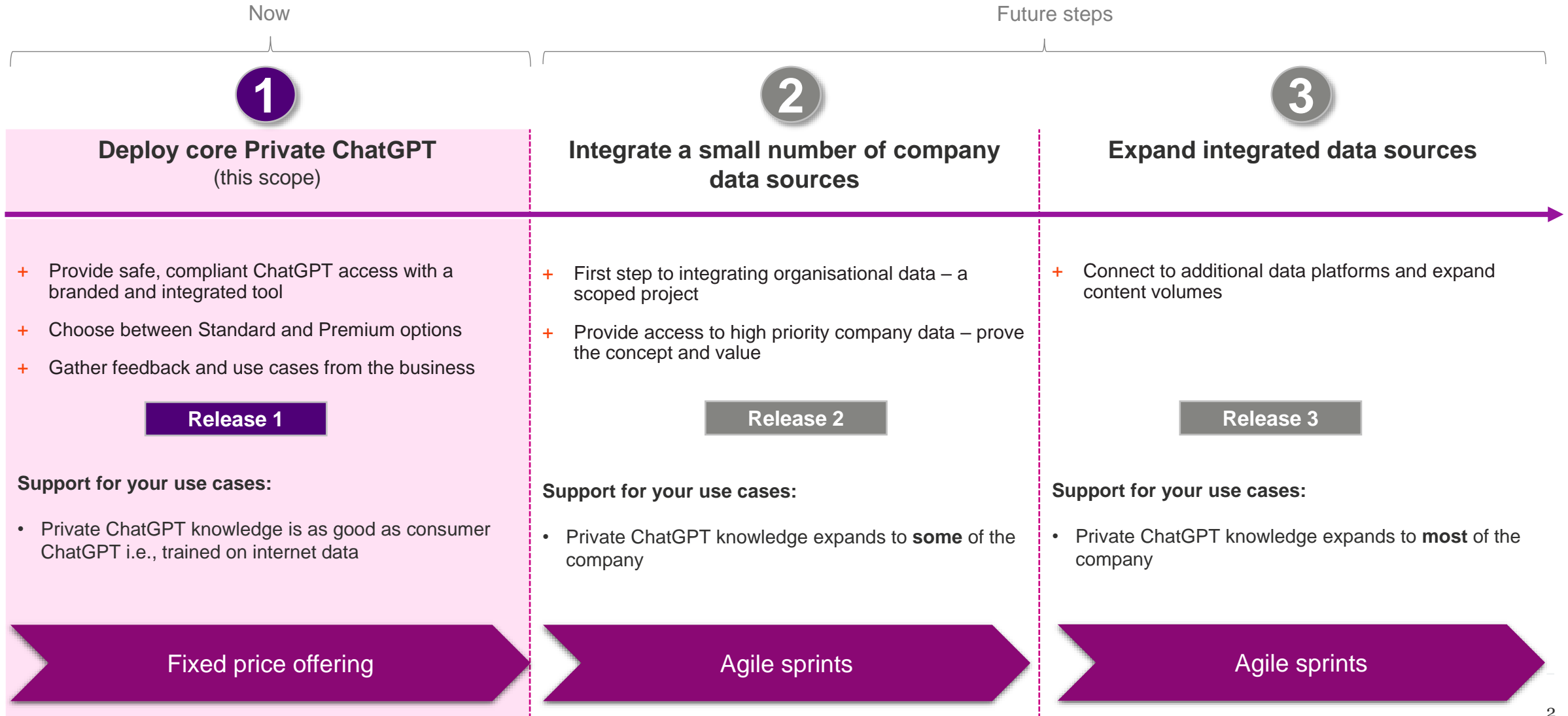
- Private ChatGPT knowledge is as good as consumer ChatGPT i.e., trained on internet data

Fixed price offering

The AI journey for some of our clients



For many organisations, the value comes from integrating organisational data



Beyond Private ChatGPT – other Advania services



Integrate your data and documents with ChatGPT



Copilot for Microsoft 365 Copilot – security & readiness, plugin development etc.



AI and automation with Microsoft Syntex



Power Platform solutions with ChatGPT



AI privacy, security, and compliance services



AI strategic framework

Why Advania?



We know this space – we’re working with many organisations on their AI journey and have worked with Microsoft AI and the underlying platforms for years



We’re in the Microsoft 365 Copilot preview programme (one of the few organisations globally)



We are a Microsoft UK prioritised partner for Copilot implementation services (1 of 2)



We have a strong heritage and extensive capability across Teams, the Power Platform, SharePoint, and Microsoft Syntex



We have “Preferred” status in Microsoft’s Content AI Partner Programme – giving us early access to new features and roadmap info



advania

e hello@advania.co.uk **w** advania.co.uk **t** 0333 241 7689

Advania, One Old Jewry, London EC2R 8DN