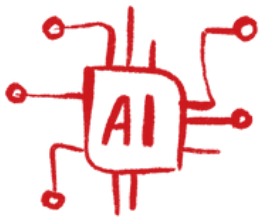
AI in a protected space: Secure OpenAI implementation for a multinational office technology company

Artificial intelligence (AI) is no longer a hype topic, but is part of the basic equipment of future-proof companies. Our customer, a leading manufacturer in the office technology sector, recognises this and wants to rely on the potential of ChatGPT in the future. There were clear priorities during implementation: security and compliance were the focus right from the start.



The company brought Cloutomate on board for this project. Our task was to provide an internal demo application based on the Azure OpenAI service that not only meets the highest security standards, but is also flexible enough to integrate company data and applications in the future.

Challenges on the way to secure OpenAI integration

Every project brings its own challenges - for our customer, in addition to security and compliance, everything revolved around seamless technical integration. Our goal: a solution that allows no compromises in these areas.

1. Security

OpenAI was to be provided in the cloud – in a protected environment that meets the highest security requirements. Unlike the standard Azure configuration, it was therefore ensured that the service is not publicly accessible, but is only operated in an isolated environment.

2. Technical complexity of the integration

The implementation of the Azure OpenAI service in combination with a web application in a private cloud required technical finesse and precise planning. The network architecture was specially adapted to specifically control the access points and comply with all internal security guidelines.

3. Internal authentication and access control

Another concern was the implementation of a centralised authentication system. Only selected user groups were to be granted access to the OpenAI service. Special measures and configurations as well as manual adjustments were required to reliably prevent unauthorised access.

In order to tailor the project specifically to the requirements of the technology company and ensure that all specifications were taken into account from the outset, we started with intensive workshops. We took into account both technical and operational requirements as well as the legal framework.

Cloutomate GmbH | info@cloutomate.de | +49894132977-00 | Zielstattstr. 9, 81379 München

Customised security architecture: Isolated provision and protective measures

Based on the requirements, we developed a customised architecture that enables the **secure operation of the Azure OpenAI service in an isolated environment**. We secured the Azure OpenAI service via private endpoints so that the service is only accessible via the internal network and public access is completely excluded.

An Azure Virtual Network (VNet) isolated the data flow within the cloud infrastructure and consistently prevented any connection via the public internet. A reverse proxy, which is set up on a Kubernetes cluster, also controls access to the OpenAI services. It encrypts all requests and checks them for potentially unauthorised access, **ensuring secure and efficient forwarding of data between external requests and the OpenAI service.**

Secure provision – but simple for users, please

Despite the technical complexity, our goal was clear: the solution should be **simple and straightforward for users**. The OpenAI service was therefore provided as a user-friendly web app in the Azure App Service, fully secured via private networks and protected by a customised domain. This allows the internal teams to securely access the ChatGPT demo and gain initial experience.

Access to the service is managed centrally with **Microsoft Entra ID (Azure AD). Role-Based Access Control (RBAC)** makes it possible to define user rights granularly so that only authorised user groups and selected employees can access the application. We have seamlessly integrated the **Microsoft 365** authentication policies to standardise the login process and further increase security. Special firewall rules also restrict access to authorised internal IP addresses, and network security groups have been set up to specifically control the flow of data between resources within the VNet.

Encrypted communication & automatic certificate management

E**ncrypted communication is ensured by automatic certificate management** using the Cert Manager and Let's Encrypt. The certificate is automatically provided and managed by the Kubernetes cluster so that all connections to the web app run securely via HTTPS. This means that data transmission is continuously encrypted without any manual effort on the part of the user.

Intelligent content filtering for secure content

Intelligent content filters also ensure that the content generated always meets the customer's quality and security standards. They automatically recognise and remove inappropriate content such as offensive language, violence or misinformation.

Flexible, secure and ready for the future

The office technology manufacturer can now use the **Azure OpenAI service** securely and efficiently to **gain internal experience with AI** – all in a compliant environment. The solution is not only optimised for current use, but also offers flexible scope for future expansions, such as the connection of SAP data, and is designed to keep pace with the company's growing requirements.