BusinessGPT

SECURITY AND GOVERNANCE FIREWALL FOR GENERATIVE AI

http://AGATSoftware.ai

THE PROBLEMS

AI models and applications aren’t innately reliable and secure.

SECURITY

- Connecting AI models to company data can lead to data privacy violations

GOVERNANCE

- Employees rely on AI for business operations. can lead to Business Financial or reputational harm

Usage control and data protection concerns limit companies from leveraging Generative AI.

Source : Gartner 2023
AI Governance webinar

1 in 3 enterprises prohibit using public Generative AI

THE PROBLEMS

SECURITY

- **Fact**

Getting insights from public AI like ChatGPT requires company data public exposure.

- **Problem**

Sensitive data becomes public.

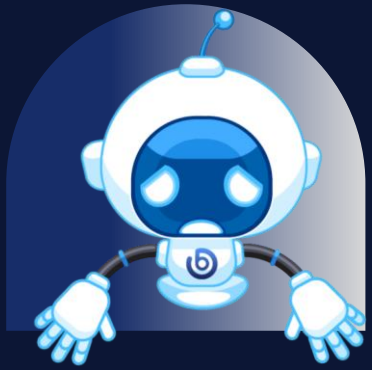
GOVERNANCE

- **Fact**

Employees rely on AI for business operations.

- **Problem**

Misuse and hallucinations of AI lead to business harm.

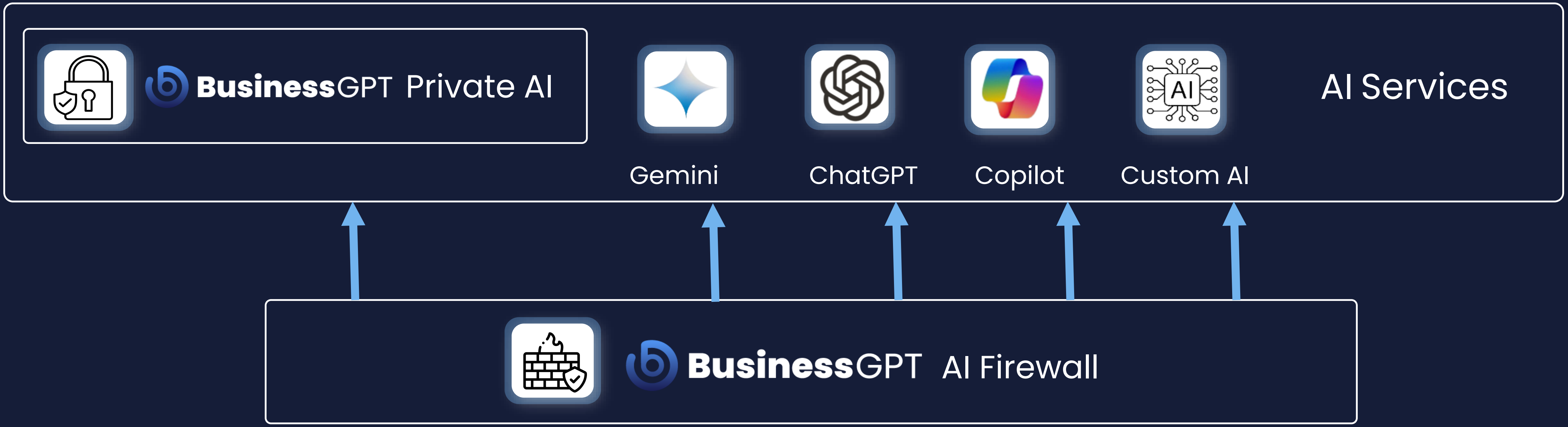


Usage control and data protection concerns limit companies from leveraging Generative AI.

Source : Gartner 2023
AI Governance webinar

1 in 3 enterprises prohibit using public Generative AI

Solution Overview



- **Governance:**
  Risk management Firewall ensuring Compliance and Responsible AI usage with real-time AI usage control.

- **Security:**
  Securely use AI with zero data exposure with a private AI solution.

Empower users with responsible and secure AI
for generating insights from your company's data.

BusinessGPT Private AI

Private AI module- Capabilites

Secure on-prem/ Private Cloud.

Data does not leave company control.

Data connectors – Grounding.

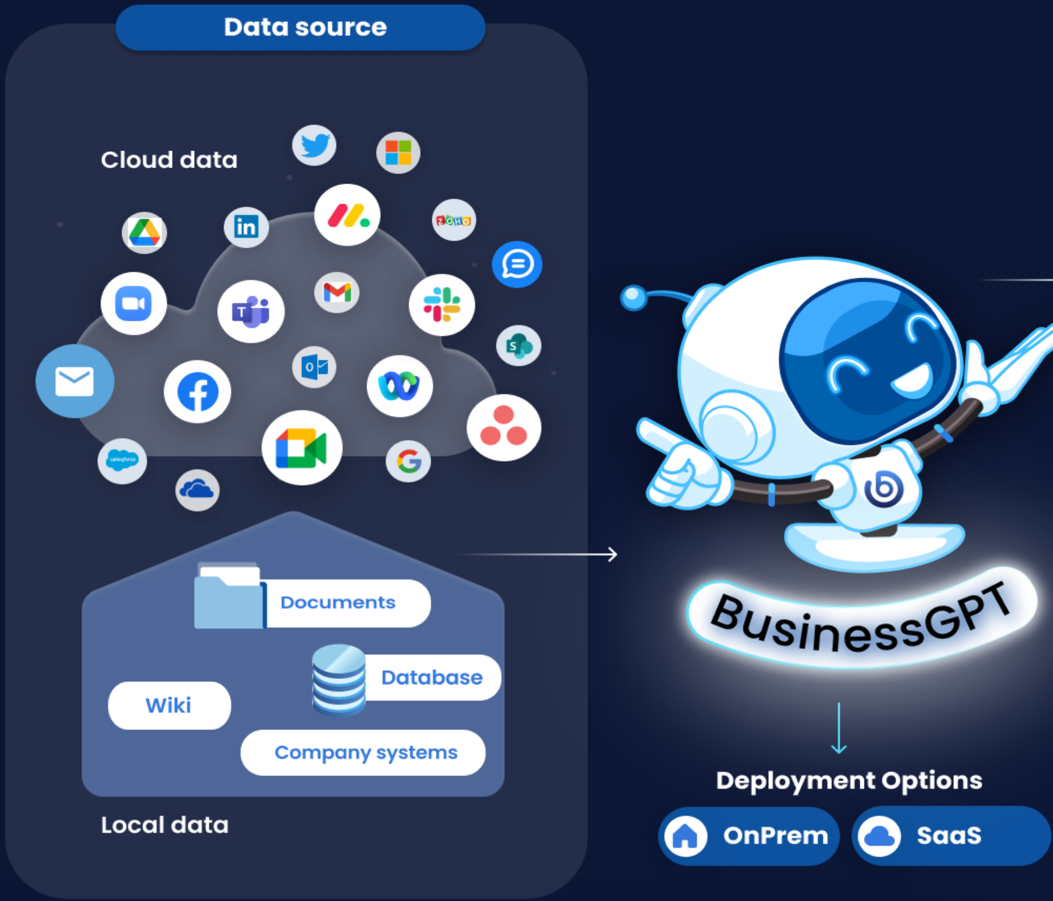
Connect to main company data sources

Sync source Access Control permissions

Generate answers based on data access.

Manage sensitivity classification.

Prevent the use of sensitive data in AI



End-to-end private AI solution

BusinessGPT Private AI Supported Data Sources

Microsoft:
Teams chats, Team channels, Teams meeting transcripts, One Drive, SharePoint, Email (Exchange /Outlook), Planner.

Google:
Meeting transcripts, Drive, Gmail.

Slack:
Channels, Chats.

Zoom:
Meeting transcripts.

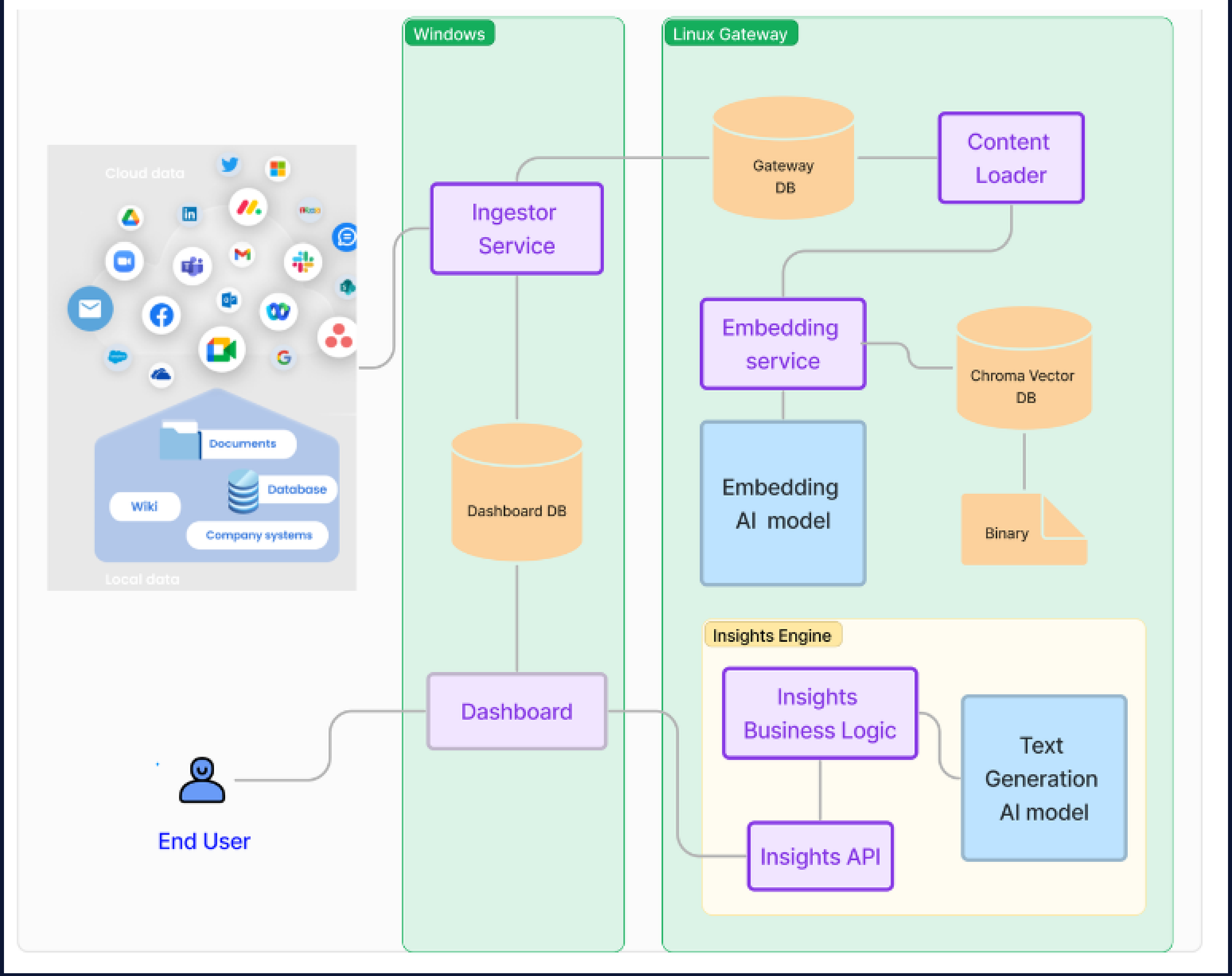
Webex:
Spaces, Direct messages, Meeting transcripts.

CRM & Tasks
Planner, Monday, Asana

Coming soon:

salesforce ZOHO Discord Google Sheets zapier

Secure AI on prem topology



AI Models supported:

- Mistral
- Llama2

BusinessGPT AI Firewall

Gemini

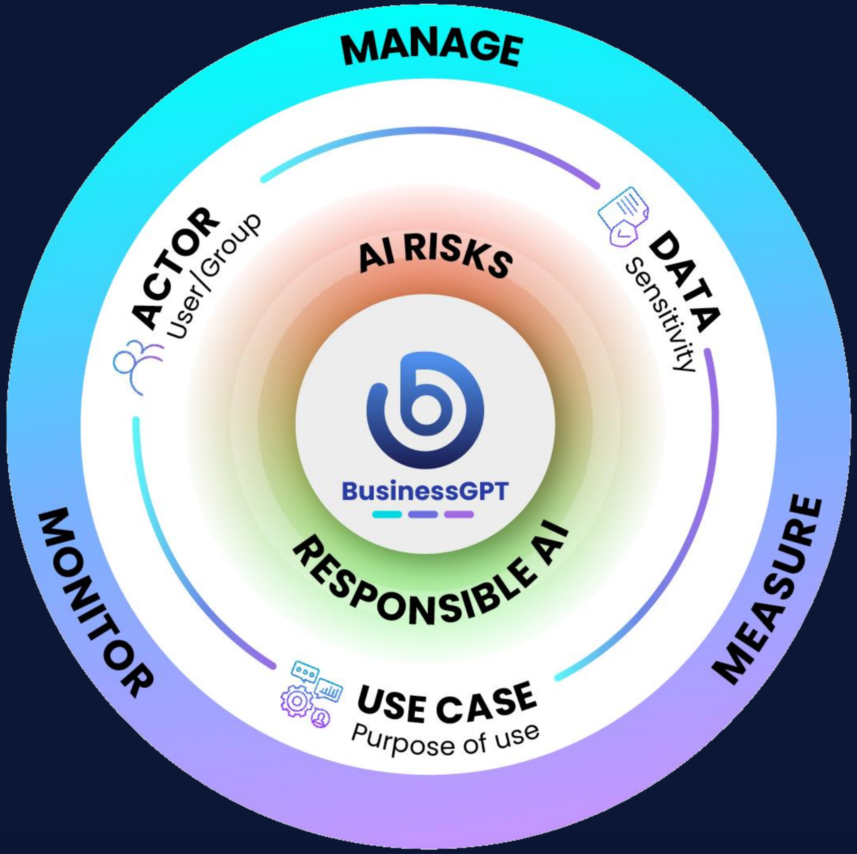
ChatGPT

Copilot

Custom AI

BusinessGPT AI Firewall- Capabilities

Governance for on-prem and public AI like ChatGPT



Mitigating AI risks with visibility and control of AI usage

- Monitoring AI usage
- Measure risk based on defined company policies.
- Manage risks by defining rules controlling AI usage.
- Compliance – Maintain compliance with regulations like EU AI ACT and AI RMF.
- Define Responsible AI for your company.

AI Firewall

Responsible AI by Safeguard and Monitoring Risks

Firewall modules

Auditing

Monitor and measure usage.

Data Classification

Data Classification

Usage classification

Policies

Define risks and actions for AI usage

AI Firewall for Risk Management and Prevention

AI GOVERNANCE FEATURES

AUDITING

- Record every question/answer
- Automatic usage classification by topics
- Identify usage risk levels per user

DATA CLASSIFICATION

- AI Usage detection and classification
- Category Classification of data and Q&A
- Company Data Sensitivity level
- Questions and answers topics
- Questions and answers categories
  - Regular expression
  - Natural language AI
  - System rules (PII, HIPPA, Finance, Self-harm, Sexual , Violence etc)
  - Content Sensitivity classification

AI POLICIES

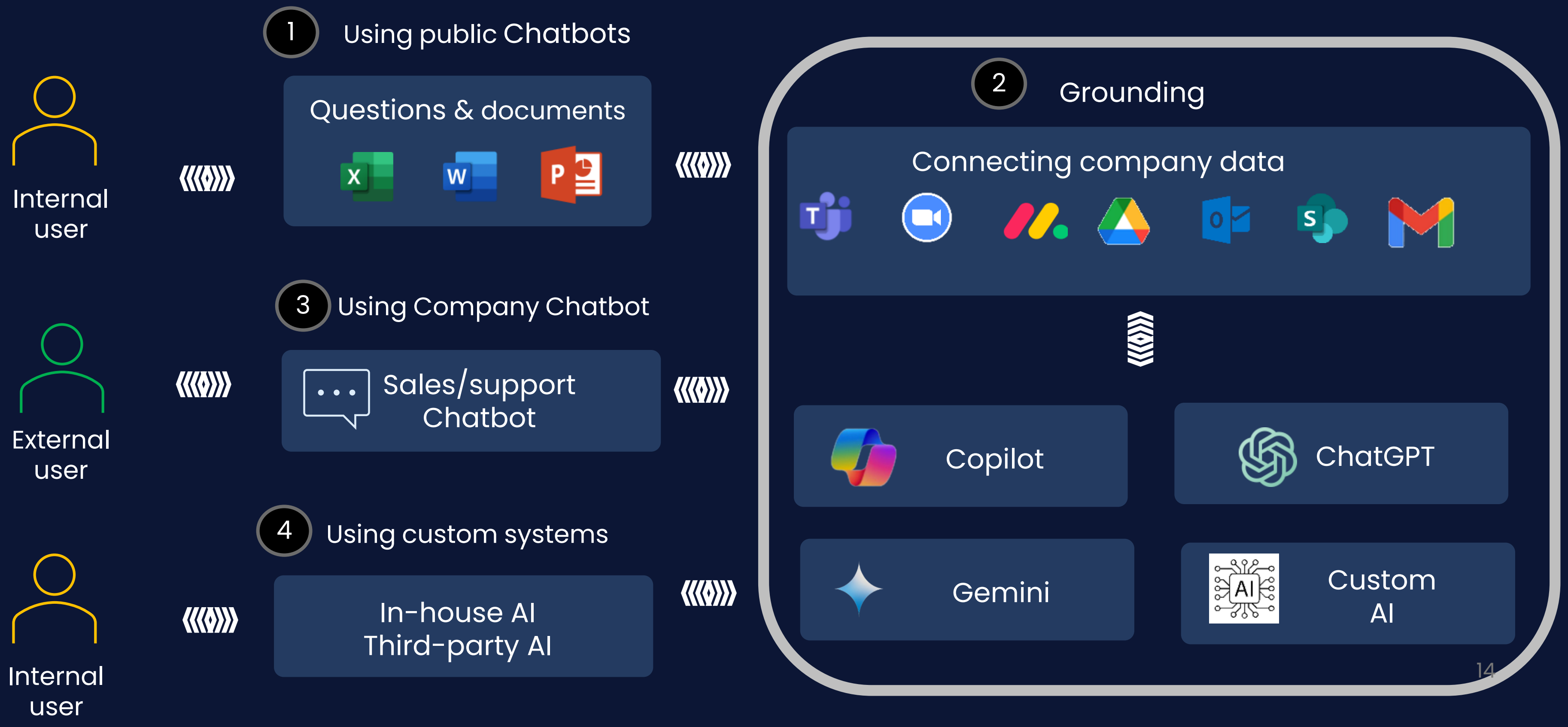
- Define risk-based company AI usage policies
- Permitted / Forbidden Access
- Inspect and apply rules based on source data and Q&A content.
- Set rules per user/ group
- Define action – Block/Allow
- Use data classification for policy risk

Benefits of BusinessGPT

- **Control AI usage across platforms:** ChatGPT, Gemini, Copilot, Internal and external AI systems
- **Secure sensitive data by regulations** PII, HIPPA, Finance
- **Mitigate OWASP risks:** Prompt injection, Prompt leak, Jailbreak, DDoS.
- **Manage AI Usage:** Users, Content, Activity

- **Handle risks:** Reputational damage, IP lost, Financial Business Loss
- **Meet industry standards:** NIST AI RMF and ISO standards.
- **Implement AI Governance** Internal Policies
- **Meet industry standards: NIST AI RMF (Risk Management** Framework) and ISO 42001 (Artificial intelligence Management system)

BusinessGPT Supported Use Cases



Internal user

1 Using public Chatbots

Questions & documents

3 Using Company Chatbot

External user

Sales/support Chatbot

4 Using custom systems

Internal user

In-house AI
Third-party AI

2 Grounding

Connecting company data

Copilot

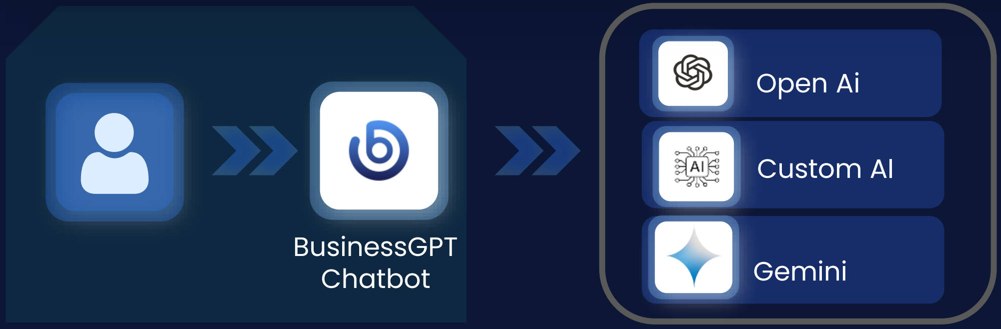
ChatGPT

Gemini

Custom AI

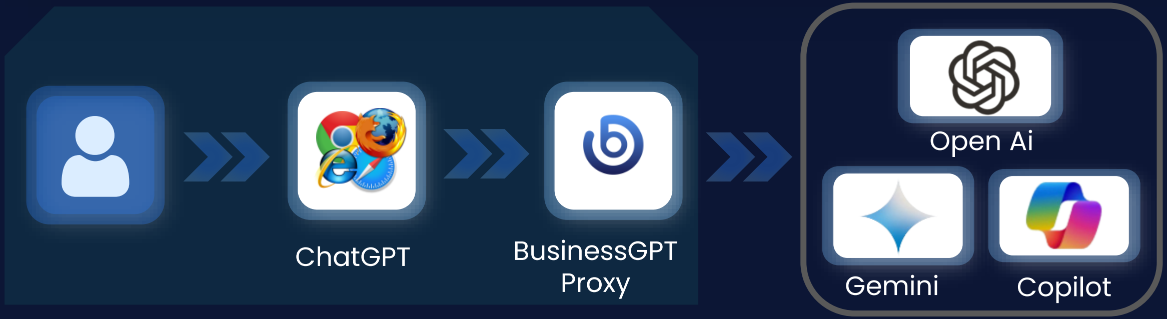
BusinessGPT TOPOLOGIES

API proxy



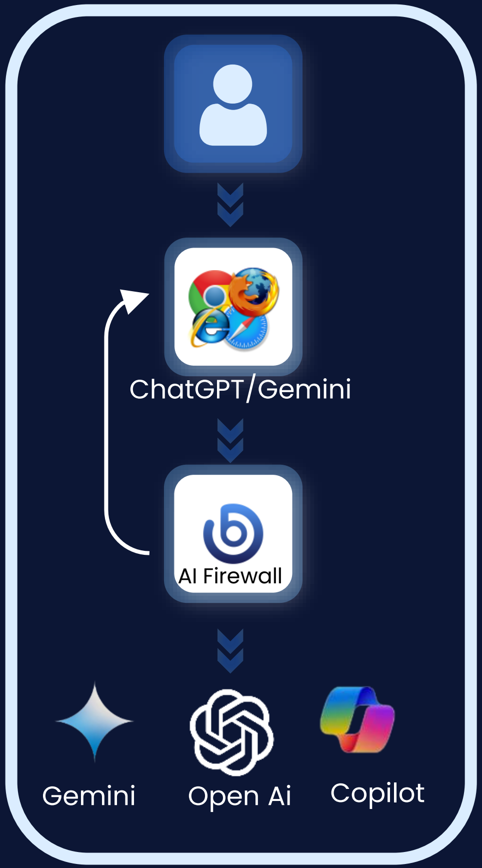
Using ChatGPT/Gemini through BusinessGPT Chatbot.

Network Proxy



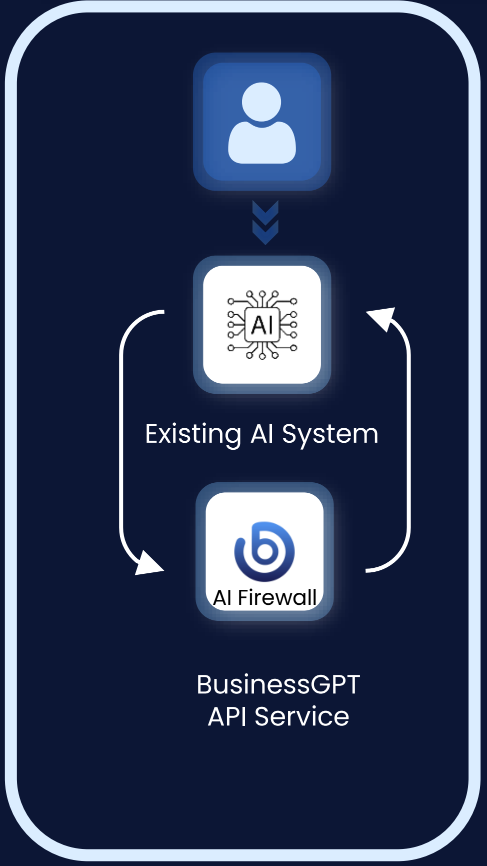
Forward traffic to BusinessGPT Proxy

Browser Extension



Browser extensions or Rest API

Service API



Connect your AI system with restAPI

Start your
AI business Journey

Contact Details:
www.agatsoftware.ai