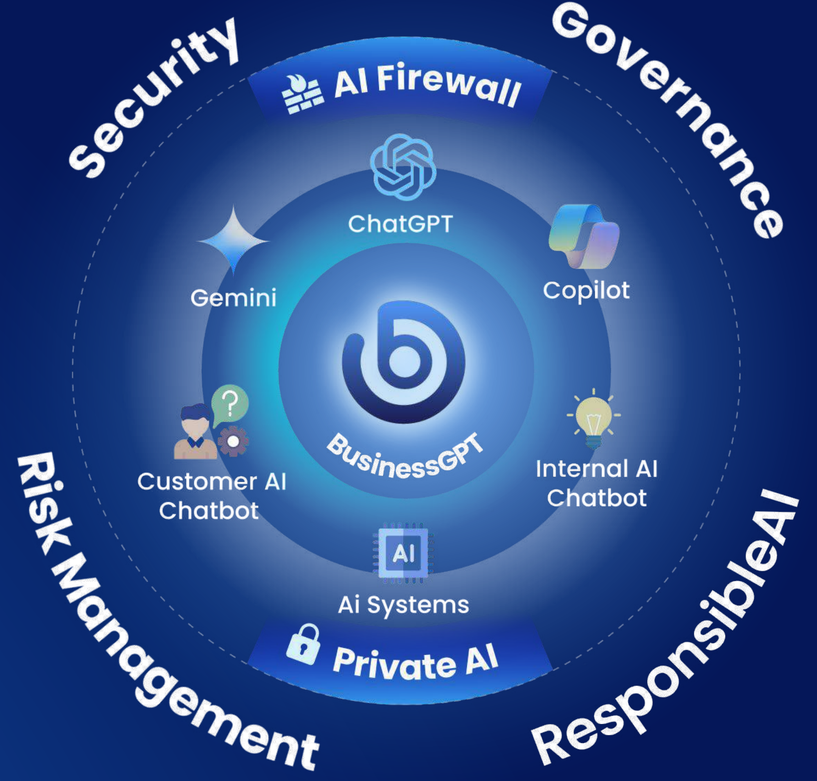
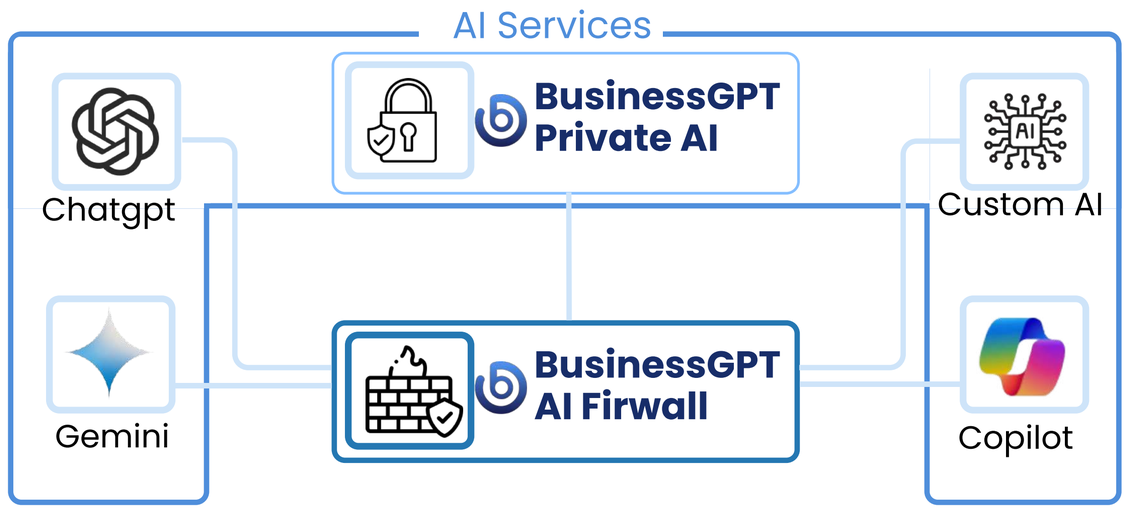
Security and Governance for Generative AI

Risk Management for AI and data privacy protection.



Product Overview

BusinessGPT provides security and governance for Generative AI usage, featuring a real-time Firewall to control AI risks, including ChatGPT/Copilot and local AI services. It offers a Private/On-prem AI solution for regulated companies, ensuring data confidentiality.



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

Solution

AI Firewall

Mitigating AI risks with visibility and control of AI usage

Identify Objectives: Identify activity objectives (e.g., asking for legal advice or improving code, price inquiry).

Public AI Support: Support for online AI like ChatGPT/ Copilot or local AI.

Risk Management: Complete activity auditing for risk management.

Sensitivity Classification: Classifying activity content to determine the sensitivity level.

AI policies: Enforce usage policies per groups/users

On-prem/ Private AI

Generate insights from your company data with zero data exposure for maximum data privacy

Privacy: Complete Chatbot AI solution with no internet exposure.

Access control: Generate answers based on source data access.

Grounding: Data connectors to most important sources, such as files, sites, emails, and meetings.

Data classification: local data classification system to determine the sensitivity.

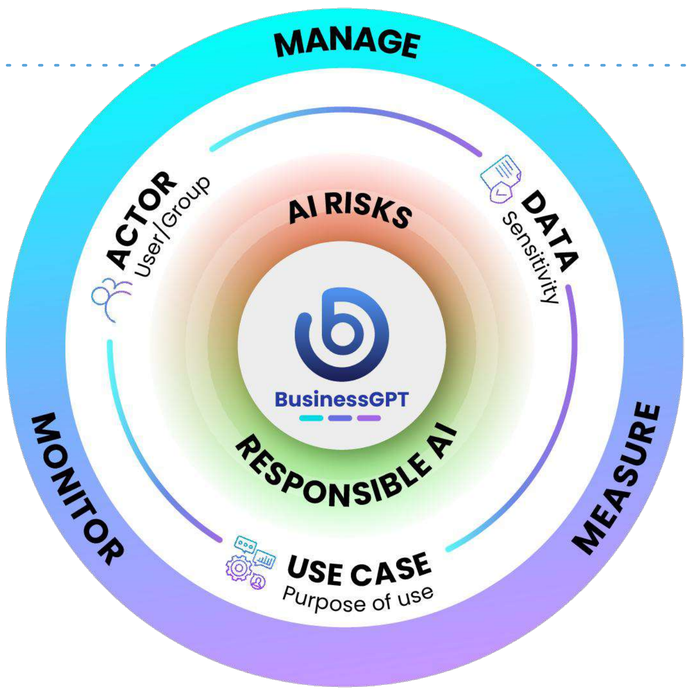
Topology: Local/ on-prem or a private cloud solution.

Capabilities

AI Governance and Security

Manage, monitor and measure all your AI usage.

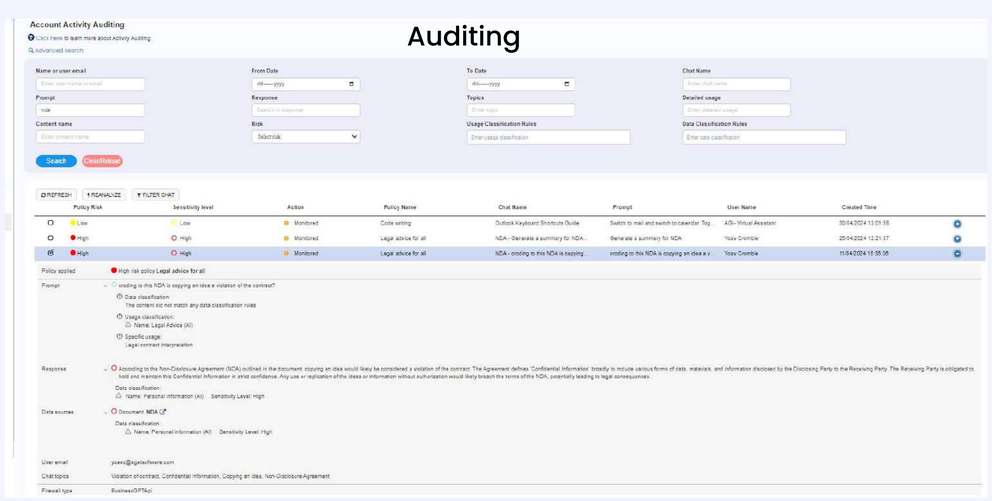
- Monitoring AI usage
- Measure risk based on defined company policies.
- Manage risks by defining rules controlling AI usage.
- Maintain compliance with regulations like EU AI ACT and AI RMF.

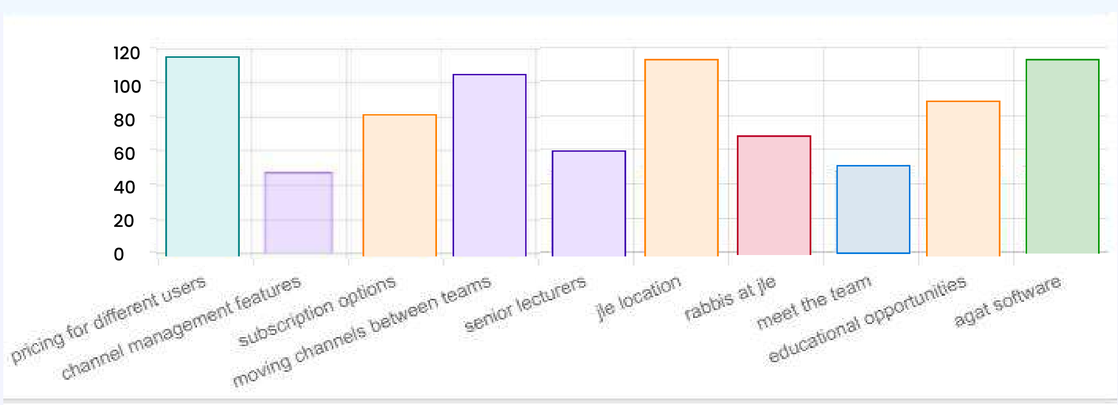


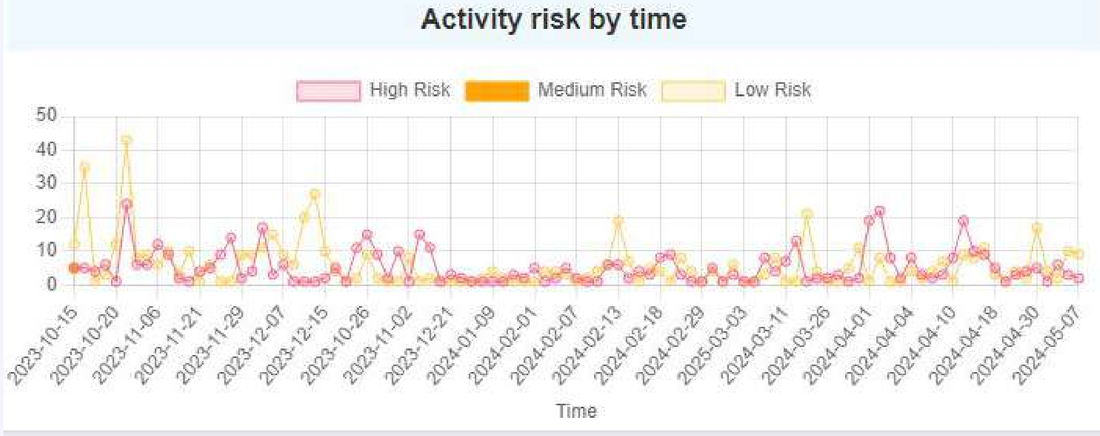
Benefits Of BusinessGPT

- **Control AI usage across platforms**
  ChatGPT, Gemini, Copilot, Internal and external AI systems.
- **Meet industry standards**
  IST AI RMF (Risk Management Framework) and ISO 42001 (Artificial intelligence Management system)
- **Secure sensitive data by regulations**
  PII, HIPPA, Finance.
- **Manage AI Usage**
  Users, Content, Activity.
- **Handle risks**
  Reputational damage, IP lost, Financial Business Loss.
- **Implement AI Governance**
  Internal Policies
- **Mitigate OWASP risks**
  Prompt injection, Prompt leak, Jailbreak, DDoS.

Management Dashboard







Get a **free trial** today to experience the power of the **BusinessGPT Assistant** and take your operations to new heights. Click Here

AGAT
info@agatsoftware.ai
+972-2-579-9123
https://agatsoftware.ai
Linkedin