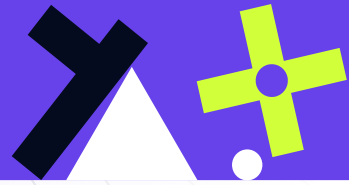


# SECURE LLM OFFERING



## Issues with standard LLMS (ChatGPT, Grok, Gemini).

### Data Privacy and Confidentiality.

01 ↗

- **Risk of Data Leakage:** Employees might unintentionally input sensitive company data (e.g., proprietary code, customer PII, trade secrets) which could be stored or used for model improvement.
- **Lack of Control Over Data:** In many AI-as-a-service models, data is processed in third party cloud environments outside your control and visibility, making it difficult for companies to ensure data residency or retention policies are met.

### Compliance and Regulatory Issues.

02 ↗

- **Industry-Specific Regulations:** Highly regulated sectors (e.g., finance, healthcare) must comply with frameworks like GDPR, HIPAA, SOC 2, etc., which might conflict with how AI models handle data.
- **Auditability:** Most AI applications are “black boxes”, making it hard to audit decision-making processes or reproduce outputs for compliance reviews.

### Intellectual Property Risks.

03 ↗

- **IP Exposure:** Submitting proprietary information into a third-party AI Applications may inadvertently transfer IP outside the organization's control.
- **Model Contamination:** There's concern that AI models trained on enterprise data may “learn” from it in ways that could benefit other users (especially in shared models).

## Security of the Tool Itself.

04 ↗

- **Third-Party Vulnerabilities:** ChatGPT and similar tools rely on APIs or external hosting environments that could be targeted by cyberattacks.
- **Phishing and Social Engineering:** Malicious actors could exploit AI-generated content to craft more convincing phishing emails or misinformation.

## Content Generation Risks.

05 ↗

- **Misinformation and Hallucinations:** ChatGPT can confidently generate plausible but incorrect or misleading information, which can be risky in enterprise decision-making.
- **Offensive or Biased Outputs:** Enterprises are wary of tools generating harmful, discriminatory, or reputationally damaging content.

## Employee Over-Reliance or Misuse.

06 ↗

- **Over-trust in AI:** Employees might treat AI-generated content as fact without validation.
- **Inappropriate Use Cases:** ChatGPT could be misused for tasks it's not suited for (e.g., legal advice, financial analysis) without appropriate safeguards.

## SpurTree's Secure LLM

SpurTree's Secure LLM solves these issues and provides your team the control you need.

