The case for secure AI enablement

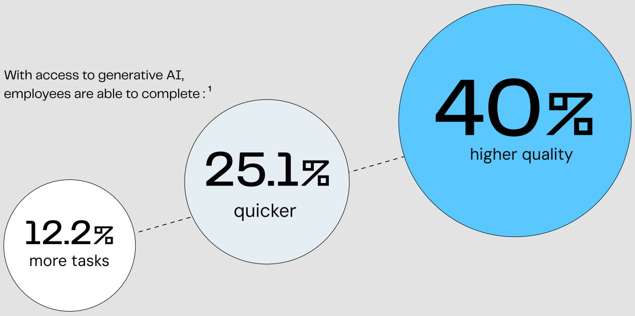
Liminal

Remarkable capabilities and unprecedented accessibility have made generative AI one of the fastest growing technologies ever. As the adoption of generative AI continues to grow, data from research firms and industry experts on usage trends and security implications demonstrates the need for an approach that prioritizes both security and enablement.

Gen AI is powerful and accessible

The explosion of generative AI is driven by both it's incredible productivity benefits and its accessibility.

With access to generative AI, employees are able to complete :[1]



12.2% more tasks

25.1% quicker

40% higher quality

The landscape of generative AI models and tools is rapidly expanding :[2]

350k Number of available LLMs in market today

25k Number of AI-enabled applications released in last year

Different models and applications excel at different tasks and are increasingly becoming more specialized, leading organizations to adopt a multi-model approach.

97% of enterprises that are using generative AI are leveraging multiple models[3]

But it comes with real security challenges

Data is the lifeblood of LLMs. When employees share sensitive company and customer data with these models, it introduces a host of challenges related to:

Regulatory Compliance Risk

Inadvertently sharing PII/PHI with LLMs and non-compliant entities may violate local, national, and international data privacy laws

Sensitive Data + IP Leaks

Intellectual property and enterprise data deemed sensitive can be exposed if provided to an LLM

Inappropriate Exchanges

LLMs can provide results that are deemed inappropriate, offensive, and/ or contain data that shouldn't be included

And the scope of these concerns is not small

55% of gen AI users report using unapproved tools at work[4]

63% of employees report being comfortable sharing at least some personal or proprietary information with LLMs[5]

Employees at companies with well defined policies are nearly **4x** more likely to share sensitive information than those at companies with no policy[5]

As a result, organizations have taken a restrictive approach

Over **68%** of organizations have policies in place partially restricting or fully blocking access, with data privacy + security being the top reason **(47%)**.[5]

And it makes sense that the top controls organizations want are focused on security, governance, and observability.

Top 5 AI controls needed[6]

43%	**Prevent sensitive data from being uploaded to AI**
42%	**Log all activities & content in AI tools for potential investigations or incident response**
42%	**Block user access to unauthorized AI tools**
42%	**Train employees on secure AI tool use**
41%	**Identify risky users based on queries into AI**

Sources:
1. Navigating the Jagged Technological Frontier, Harvard Business School, 2023; **2**. There's an AI for That, TAAFT, 2024; **3**. Generative AI - LLM developers, CB Insights, 2024; **4**. More than Half of Generative AI Adopters Use Unapproved Tools at Work, Salesforce, 2023; **5**. Gen AI Adoption in Regulated Industries, Liminal, 2024; **6**. Data Security Index Report, Microsoft, 2024

The challenge is that employees aren’t waiting

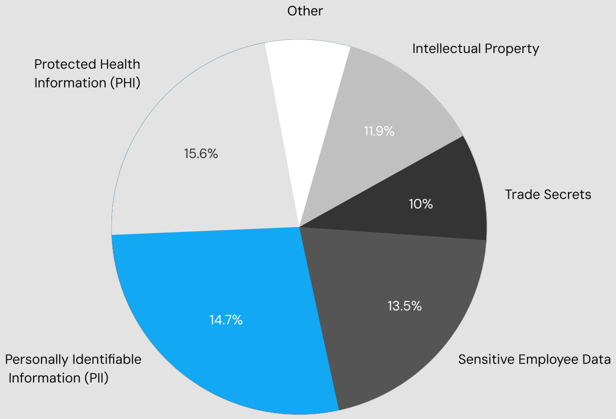
Motivated by generative AI’s productivity benefits and at their own personal risk, workers are willfully circumventing organizational policy to access the tools they want – where and how they want them.

75%	78%	3.8
of global knowledge workers report using gen AI for work today[7]	of gen AI users report bringing their own tools into the workplace[7]	Average number of AI applications users leverage[8]

Actual generative AI usage via Liminal in a large enterprise shows that

37%

of generative AI prompts contained sensitive data[9]



This rise in **Shadow AI** introduces several challenges for enterprises absent an enablement-focused solution

No control

Organizations lack ability to manage what data is shared, by whom, and with which models – introducing a host of risks related to regulatory compliance, sensitive data + IP leakage, and reputational harm.

No observability

Without visibility and monitoring capabilities, security teams are missing critical data needed to understand and enforce policy compliance, analyze user behavior, assess threat exposure, and respond to incidents

No insights

Unsanctioned AI usage not only hinders organizational ability to protect unsafe engagements, but also to uncover and proliferate high-value use cases

Better security through enablement

The data shows that traditional restrictive approaches to AI security aren’t working. Blocking access or providing limited availability is only serving to drive AI usage off-network, thereby increasing organizational risk.

Employees want to use generative AI, want to engage multiple models, and want it available everywhere they work – and they’re willing to circumvent policy to get it. Instead, organizations are achieving better security outcomes through strategic, sanctioned enablement via solutions that address the needs of end users and security teams alike.

- Prevent Shadow AI
- Proactively manage risk
- Enjoy enhanced control and visibility
- Increase productivity and innovation
- Gain competitive advantage

Security and User Experience in Perfect Harmony with Liminal

Liminal is designed to help organizations confidently address generative AI. With Liminal, enterprises can safely equip employees to experience the productivity benefits of unlimited, multi-model generative AI across any website, application, and platform, while providing unparalleled data protection, observability, and governance capabilities.

- Unlimited Access to Any Models
- Available Anywhere Work Gets Done
- Best-in-Class Security
- Total Observability
- Most Cost Effective

Liminal is the **most secure, most flexible, most productive, and most cost-effective way** for organizations to securely enable generative AI.

Get started today by visiting liminal.ai/start or by contacting the team directly at sales@liminal.ai.

Liminal
www.liminal.ai

Sources:
[7] Work Trend Index Annual Report, Microsoft, 2024; [8] Artificial Intelligence Statistics: Essential Insights for Business Success, Master of Code, 2024; [9] Customer Usage Data, Liminal, July 2024