

FOCUS YOUR RESOURCES ON INNOVATING WITH GENERATIVE AI, NOT ON SECURING IT

The Complete Platform for GenAI Security

As GenAI proliferates throughout organizations, security leaders and those responsible for promoting AI-driven innovation are confronted with a fresh set of security challenges. These risks range from employees sharing enterprise data with GenAI tools, which may inadvertently lead to data leaks due to the tools being trained on it, to malicious actors manipulating models through prompt injection in the organization's customer-facing applications. Yet despite all the risks, GenAI unlocks immense value, and adopting it isn't a matter of choice, it's key to business survival.

Key Risks associated with GenAI

Shadow AI

Prompt Leak

Prompt Injection

Insecure Output Handling

Denial of Wallet/Service

Brand Reputation Damage

Insecure Agent

Privilege Escalation

Jailbreak

Sensitive Data Disclosure

Prompt Security: Organizations' one-stop for GenAI Security

Prompt Security enables enterprises to benefit from the adoption of Generative AI while protecting from the full range of risks to their applications, employees and customers. At every touchpoint of Generative AI in an organization — from GenAI tools used by employees to GenAI integrations in homegrown applications — Prompt inspects each prompt and model response to prevent the exposure of sensitive data, block harmful content, and secure against GenAI-specific attacks. The solution also provides leadership of enterprises with complete visibility and governance over the GenAI tools used within their organization. Prompt empowers organizations to fully embrace Generative AI with confidence.

Embrace Generative AI with confidence

- ✓ Fully protect your organization from all the GenAI-associated risks
- ✓ Stay ahead of AI regulatory frameworks
- ✓ Deploy instantly and with no impact on productivity
- ✓ Attain full visibility and ensure data privacy and compliance

Prompt for Employees

Enable your employees to adopt GenAI tools without worrying about Shadow AI, Data Privacy and Regulatory risks

Observability

Instantly detect and monitor all GenAI tools used within the organization to eliminate Shadow AI risks, and see which are the riskiest apps and users.

Risk Management and Compliance

Establish and enforce granular department and user rules and policies.

Data Privacy

Prevent data leaks through automatic anonymization and data privacy enforcement.

Employee Awareness

Educate your employees on the safe use of GenAI tools with non-intrusive explanations on the associated risk of their actions.

Prompt for Homegrown Applications

Unleash the power of GenAI in your homegrown applications without worrying about AI security risks

Addressing GenAI Risks

Instantly secure your GenAI apps from Prompt Injection, Jailbreaks, Denial of Wallet, RCE and other risks.

Content Moderation

Prevent your users from being exposed to inappropriate, harmful or off-brand content generated by LLMs.

Data Leak Prevention

Filter and obfuscate any sensitive data on the fly to keep it private and stay compliant when connected to 3rd party LLMs or vector databases.

Visibility and Compliance

Monitor inbound and outbound traffic from the GenAI apps with full logging of each interaction.

Prompt for Developers

Adopt AI-based code assistants like GitHub Copilot without worrying about secrets exfiltration

Secrets and PII Protection

Instantly redact and sanitize code to prevent the exfiltration of secrets, PII and IP when using AI code assistants.

Observability

Detect and monitor the use of AI in development cycles and potential privacy violations.

See for yourself

Book a Demo

with Prompt Security