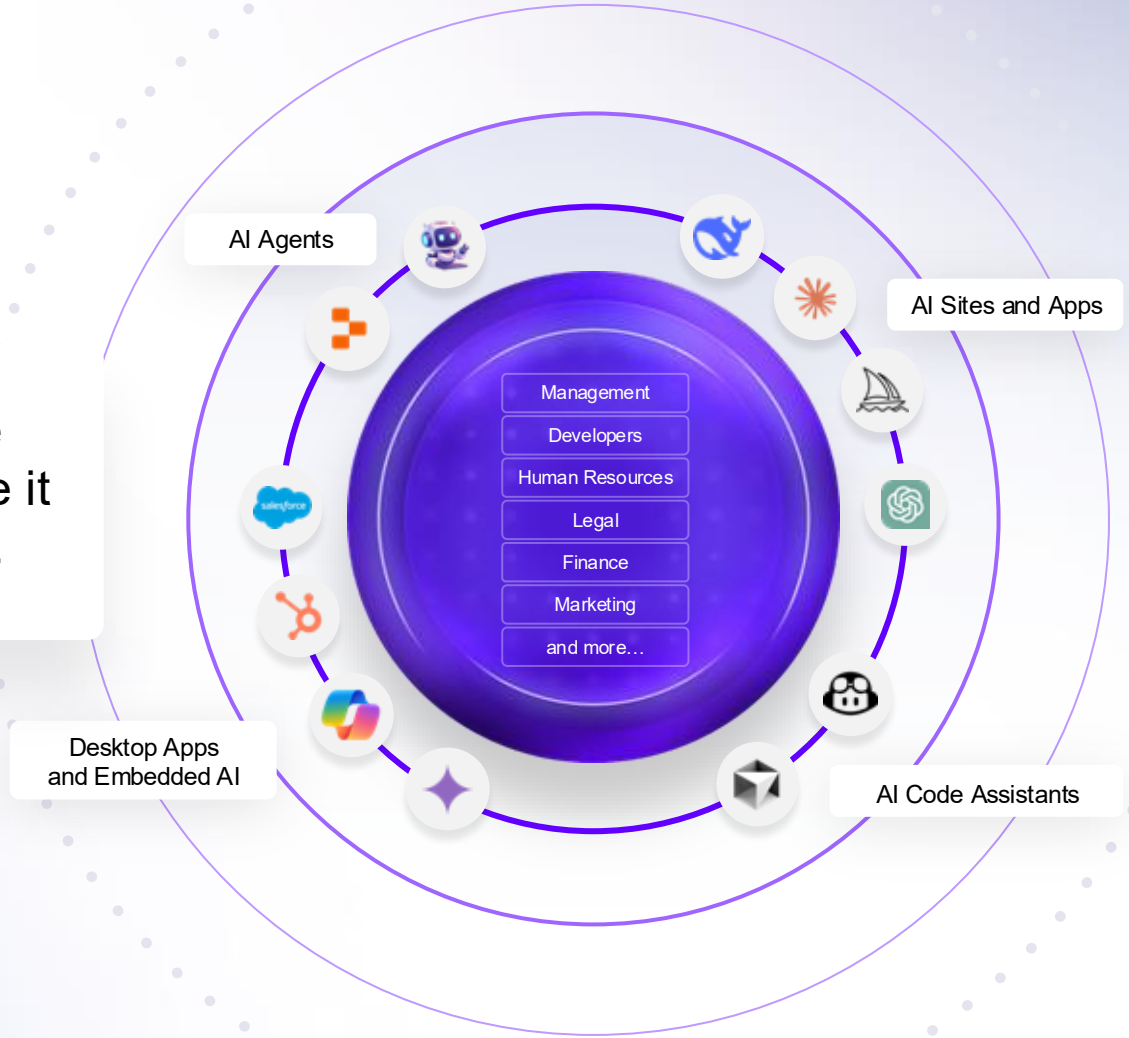
Prompt:

A SentinelOne Company

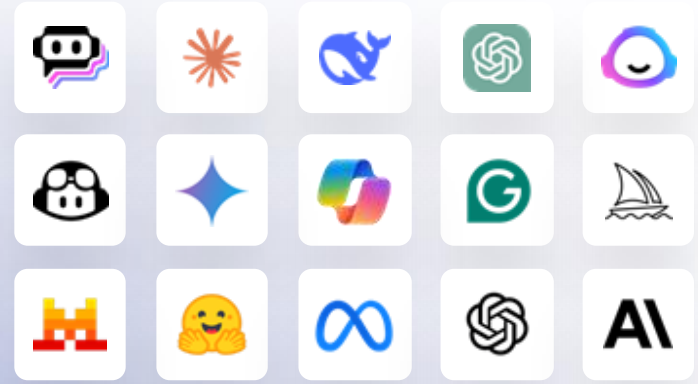
AI Security Platform

SentinelOne

By now, AI is everywhere in the organization, where it affects every department.



Employee adoption of AI tools and development with AI systems brings a spectrum of risks that can impact security, compliance, and trust.



## Risks

- Shadow AI and Shadow MCPs
- Exposing secrets or IP (e.g. API keys, cloud access tokens) through AI code assistants
- Discussing topics not allowed in the workplace
- Prompt injection, jailbreaks
- Homegrown Apps producing harmful or misaligned content that causes business and brand damage

# Prompt Security Protects Against AI Threats

## Employee Usage of AI

Enable employees to adopt AI tools without worrying about Shadow AI, data privacy and regulatory risks

## Developers Using AI Code Assistants

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

## Homegrown AI Applications

Eliminate the risks of prompt injection, data leaks and harmful LLM responses from your AI apps

EARLY ACCESS

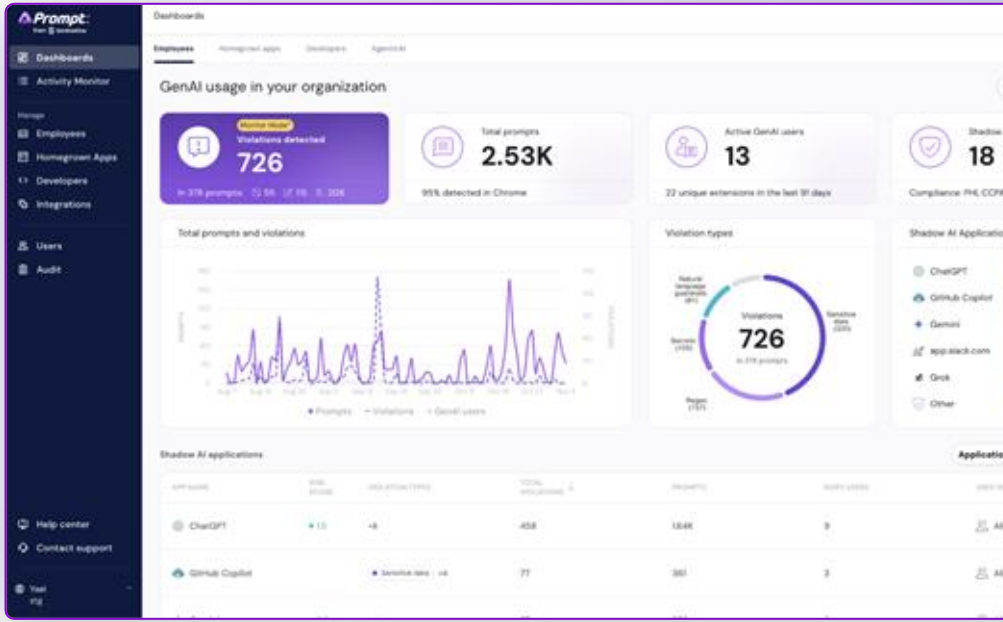
## Agentic AI Usage and Deployment

Full visibility into MCP activity with our MCP Gateway, & dynamic risk scoring to understand agent behavior patterns.

# Prompt for Employees

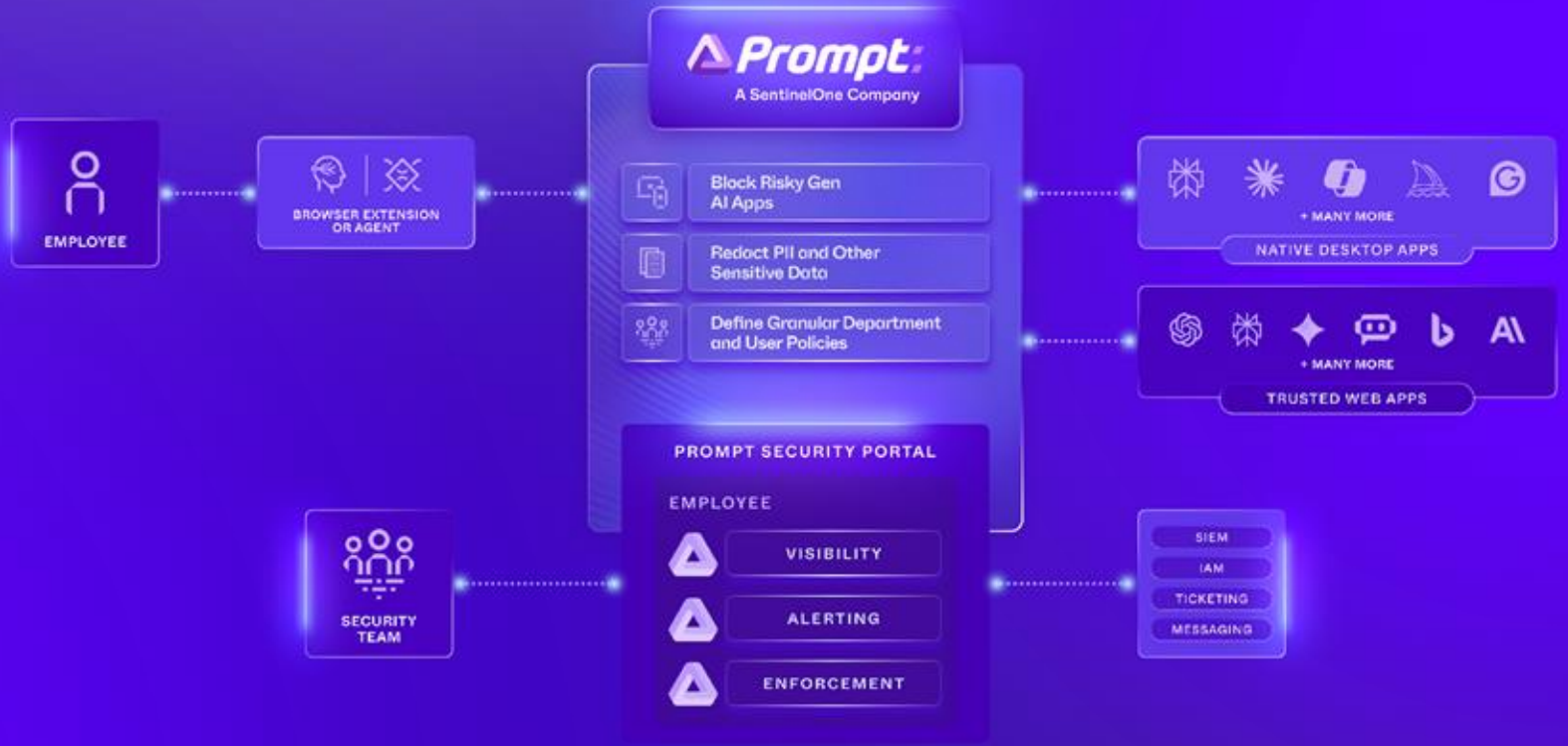
## Enable employees to adopt AI tools without worrying about Shadow AI, Data Privacy and Regulatory risks

- **Observability:** Detect and monitor all AI tools used within the organization and eliminate Shadow AI
- **Data Privacy:** Prevent data leaks through automatic anonymization
- **Risk Management and Compliance:** Enforce granular department and user rules and policies
- **Employee awareness:** Coach your employees on the safe use of AI tools



# Prompt for Employees

Prompt:
A SentinelOne Company

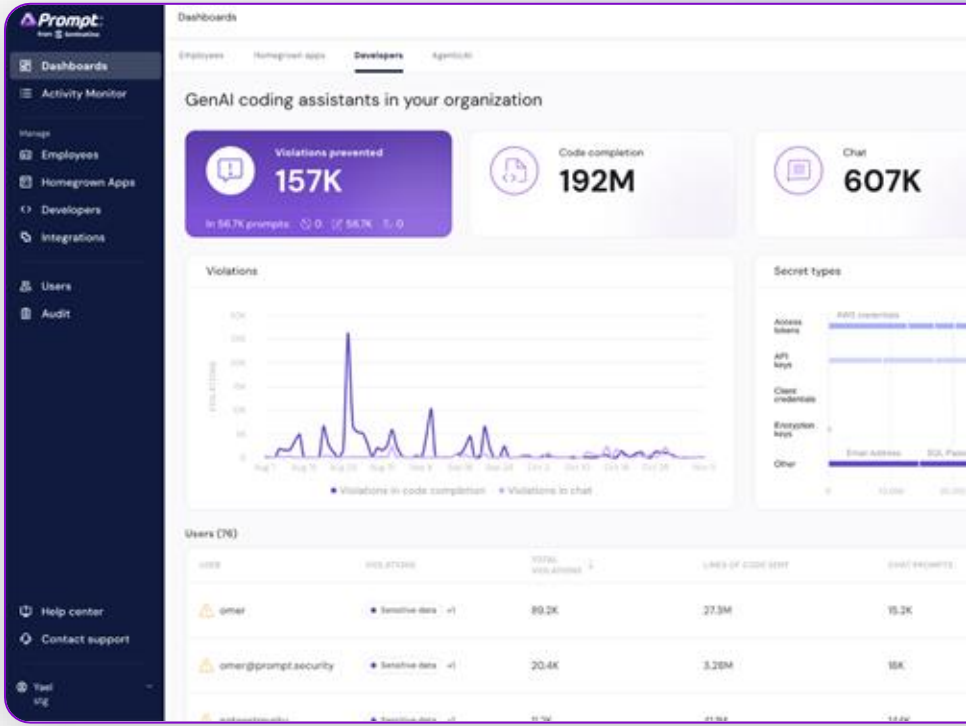



SentinelOne

# Prompt for AI Code Assistants

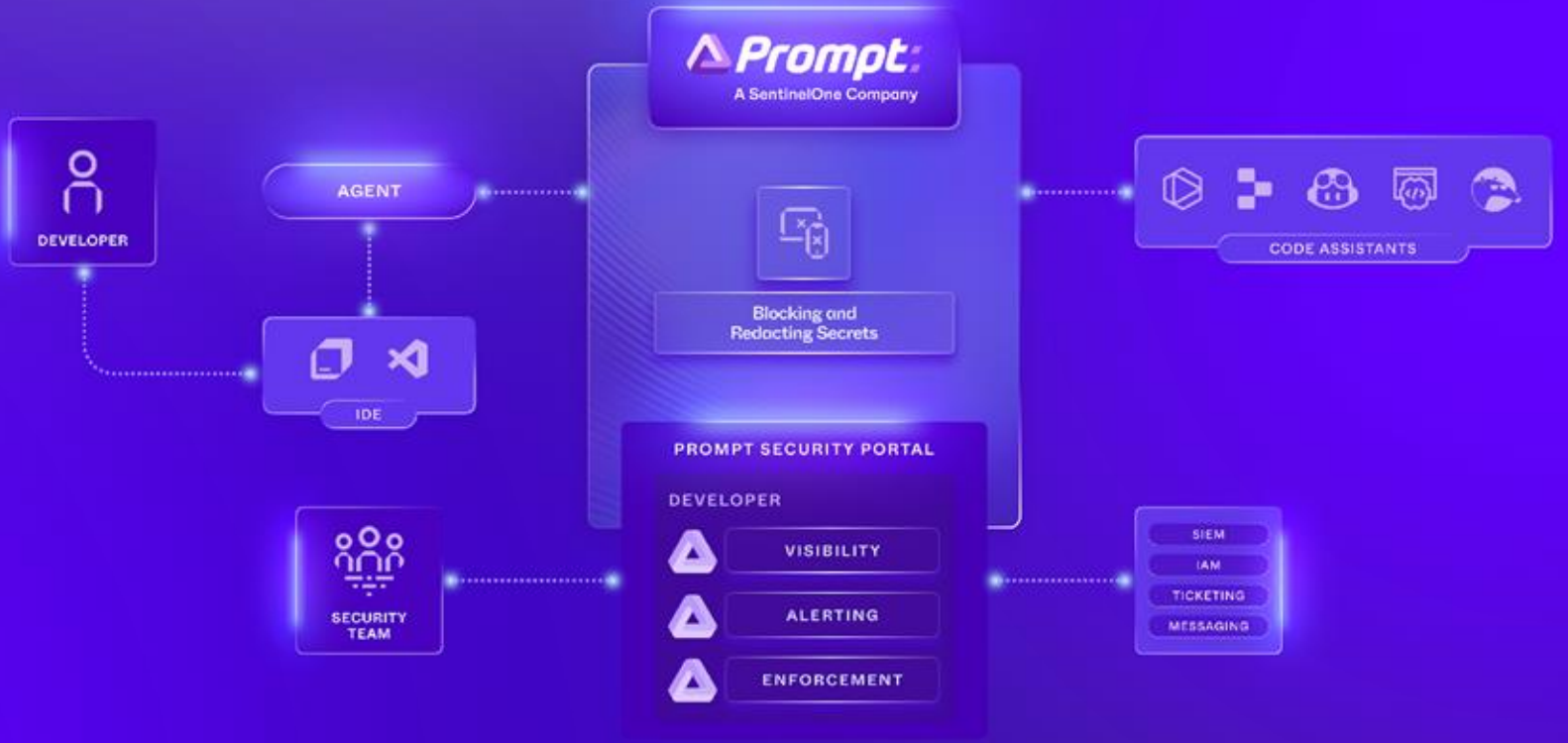
## Adopt AI code assistants like GitHub Copilot and Cursor while safeguarding secrets and PII

- **Secrets and PII Protection:** Redact and sanitize code to prevent the exfiltration of secrets, PII and IP
- **Full Visibility & Governance:** Gain visibility into AI usage across development cycles and detect potential privacy violations
- **Any tool, any programming language:** Integrate with thousands of web-based AI tools and dozens of AI code assistants, supporting nearly 30 programming language.



# Prompt for AI Code Assistants

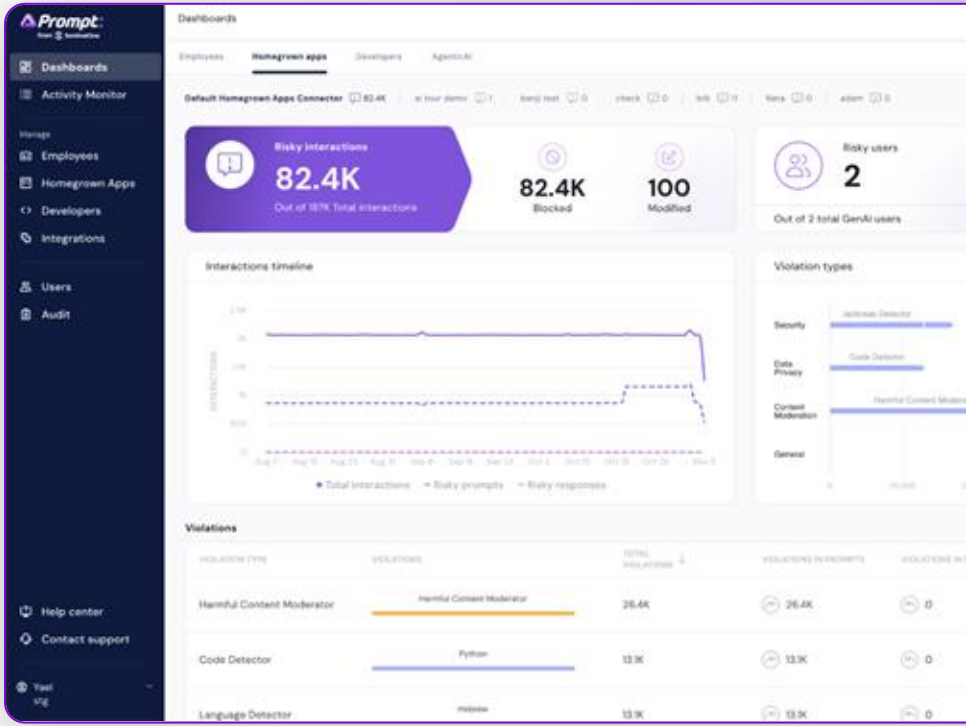
Prompt:
A SentinelOne Company



# Prompt for Homegrown AI Applications

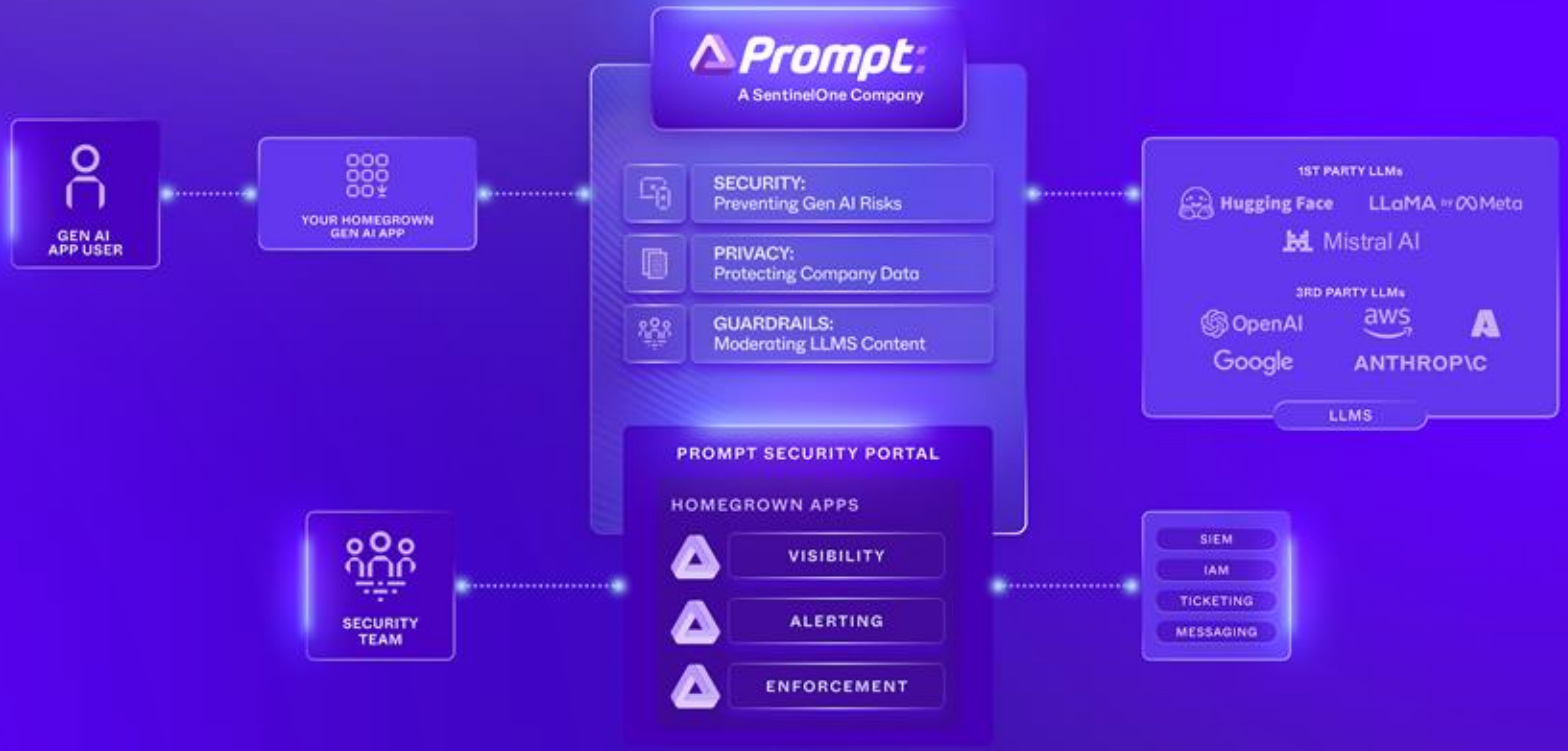
Protect your AI-powered applications from prompt injection, rogue agents, unsafe content, and data leakage without impacting UX

- **Addressing AI Risks:** Instantly secure your homegrown AI apps from Prompt Injection, Jailbreaks, Denial of Wallet, RCE and other risks.
- **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.
- **Content Moderation:** Prevent your users from being exposed to inappropriate, harmful or off-brand content generated by LLMs.



# Prompt for Homegrown AI Applications

Prompt:
A SentinelOne Company



Prompt
A SentinelOne Company

WHY PROMPT SECURITY?

# Don't Take *Our* Word For It

★★★★★

Gartner
Representative vendor AI TRiSM

Latio
AI SECURITY LEADER
2025

- Broadest AI Security Coverage
- One Platform, Modular & Scalable
- Fastest Time-to-Value in the Market
- Trusted by 75+ Enterprises (incl. Fortune 500s)
- Designed for AI's Fast-Evolving Stack

Prompt:
A SentinelOne Company

# Thank You

Sentinelone.com