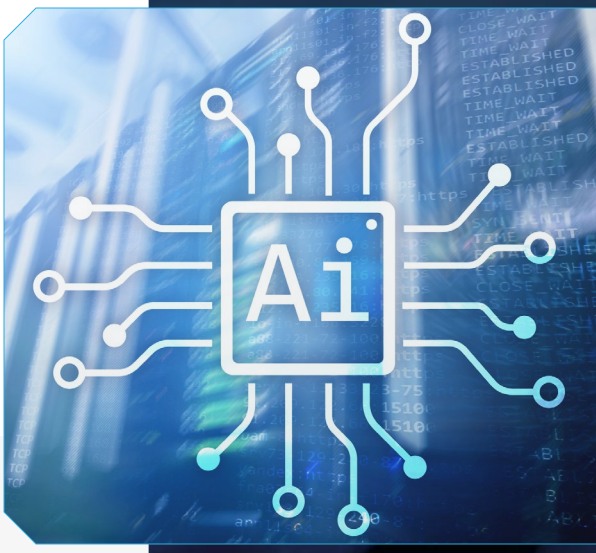
Make generative AI safer for your business.

Keep your confidential data out of ChatGPT—without blocking use.

EAP/ BETA

PlurilockAI PromptGuard



THE NEED

Keep the data you can't share out of the hands of AI platforms, automatically.

The age of generative AI is here, and your users are adopting it at a rapid pace across your organization. But as AI use climbs, so does the amount of company data pouring into platforms.

Document summaries. Formatting data into tables. Drafting documents and letters. Each of these tasks threatens to leak confidential data when carried out by an employee—putting compliance and governance at risk.

THE SOLUTION

Plurilock AI PromptGuard makes AI safety easy.

Ease of Use

PromptGuard maintains the familiar back-and-forth chat structure users know.

Mode Selection

Optionally leverage GPT system prompts to enhance AI capabilities.

Data Protection

Redact, anonymize, or encrypt AI prompts automatically, in the flow of interaction.

Invisibility

Real data isn't sent to AI platforms but appears seamlessly in returned answers.

Maturity

Relies on a mature DLP engine for data detection and classification before redaction.

Governance

Establish guardrails for AI use without having to block entire platforms or prompts.

Plurilock

www.plurilock.com
sales@plurilock.com

+1 888 282-0696 (USA West)
+1 908 231-7777 (USA East)
+1 866 657-7620 (Canada)

Cybersecurity and Zero Trust
Assessments and consulting
IT products and solutions
Professional services
Managed services

HOW IT WORKS

PromptGuard hides your data from AI—but not from you.

Plurilock AI PromptGuard is a powerful tool for AI guardrails and governance inside your organization—one that that supports, rather than undermines, the productivity gains that AI offers.

Data detection

PromptGuard identifies sensitive pieces of data and tags each of them uniquely as important-but-confidential.

Data redaction

Before a prompt is delivered to the AI platform, these pieces of data are replaced with similar anonymized or encrypted placeholders.

Data restoration

When the AI platform returns an answer containing these placeholders, the original data is restored before the answer is shown to the user.

Why PromptGuard is Different

The first solution of its kind, Plurilock AI PromptGuard doesn't block AI platforms or prevent AI prompts.

Instead of obstructing use, PromptGuard enables employee AI use safely, so that AI productivity gains remain—while data leakage is stopped.

Why PromptGuard Matters

AI enables hours-long tasks to be completed in minutes. Employees are going to find a way to use it—and employers need a way to leverage these gains without data risk.

PromptGuard restores the promise of AI for organizations that would otherwise face difficult adoption choices.

PLATFORM

- Cloud software-as-a-service
- In-browser application

BROWSER COMPATIBILITY

- Chrome
- Safari
- Firefox
- Edge

SUPPORTED LLMS DURING BETA

- GPT-3.5

SUPPORTED REDACTION MODES

- Anonymize
- Encrypt
- Randomize
- None / Pass-through

AUDIT DATA (END Q3)

- Full user prompt history
- Full AI response history
- Interaction event timestamps
- Full attribution

LOGIN SECURITY (END Q3)

- SSO integration via SAML
- SSO integration via OIDC

Plurilock™

PlurilockAI
Least privilege solutions

- **Plurilock AI Cloud**
  Single sign-on, access control, and email data safety
- **Plurilock AI Cloud DLP**
  Single sign-on, access control, email data safety, and agent-based data loss prevention (DLP)
- **Plurilock DEFEND™**
  Continuous authentication and risk scoring behavioral biometrics
- **Plurilock AI Complete**
  Single sign-on, access control, data loss prevention, and continuous authentication with integrated DEFEND™ technology for real-time least privilege and risk scoring

www.plurilock.com
sales@plurilock.com

+1 888 282-0696 (USA West)
+1 908 231-7777 (USA East)
+1 866 657-7620 (Canada)

Cybersecurity and Zero Trust
Assessments and consulting
IT products and solutions
Professional services
Managed services