

Pervasive Protection for LLM Pioneers

Your Organization Is Already Using GenAI.

Lasso Protects Every LLM Interaction — Simple, Seamless, Secure.

Generative AI technology is now a non-negotiable asset for businesses striving to maintain a competitive advantage. Recognizing its productivity and efficiency boosting potential, an estimated 60% of organizations deploying AI tools incorporate LLM and Generative AI (GenAI) technology in their operations¹

As businesses develop proprietary LLMs and build GenAI-powered applications, and employees use GenAI tools to boost productivity, security and legal leaders face critical challenges.

LLM security is markedly different from conventional security challenges; they are non-deterministic and can't be protected by traditional means. LLMs are pervasive, touching the business at multiple points in different ways and they demand a nuanced approach to risk management. Mitigating LLM risk is deeply contextual, and malicious threats take on new and even more dynamic characteristics when LLMs are the vector.

To proceed safely, businesses of all types need to take a proactive approach to securing the way they implement and interact with LLMs.

Key Benefits

- Full visibility into GenAI apps and models across your organization, with an Always-on monitoring.
- Mitigate GenAI-specific threats like prompt injection and sensitive data leakage in real-time with built-in protection that prioritizes security from deployment.
- Use flexible, natural language to craft security policies tailored to your business's unique needs
- Fast and easy installation for any deployment style. Monitor data flow to and from GenAI in minutes with an intuitive, user-friendly dashboard.

IN-HOUSE APP SECURITY

Lasso for Applications

Get continuous protection and control over all GenAI apps, agents and models used or developed by your organization.

SECURE GENAI CHATBOTS

Lasso for Employees

Monitor and protect employee GenAI chatbot usage across all teams to ensure security and maintain compliance.

CODE PROTECTION

Lasso for Developers

Prevent infiltrations in development environments for R&D teams using AI assistants and tools.

AUTONOMOUS MODEL SCANNING

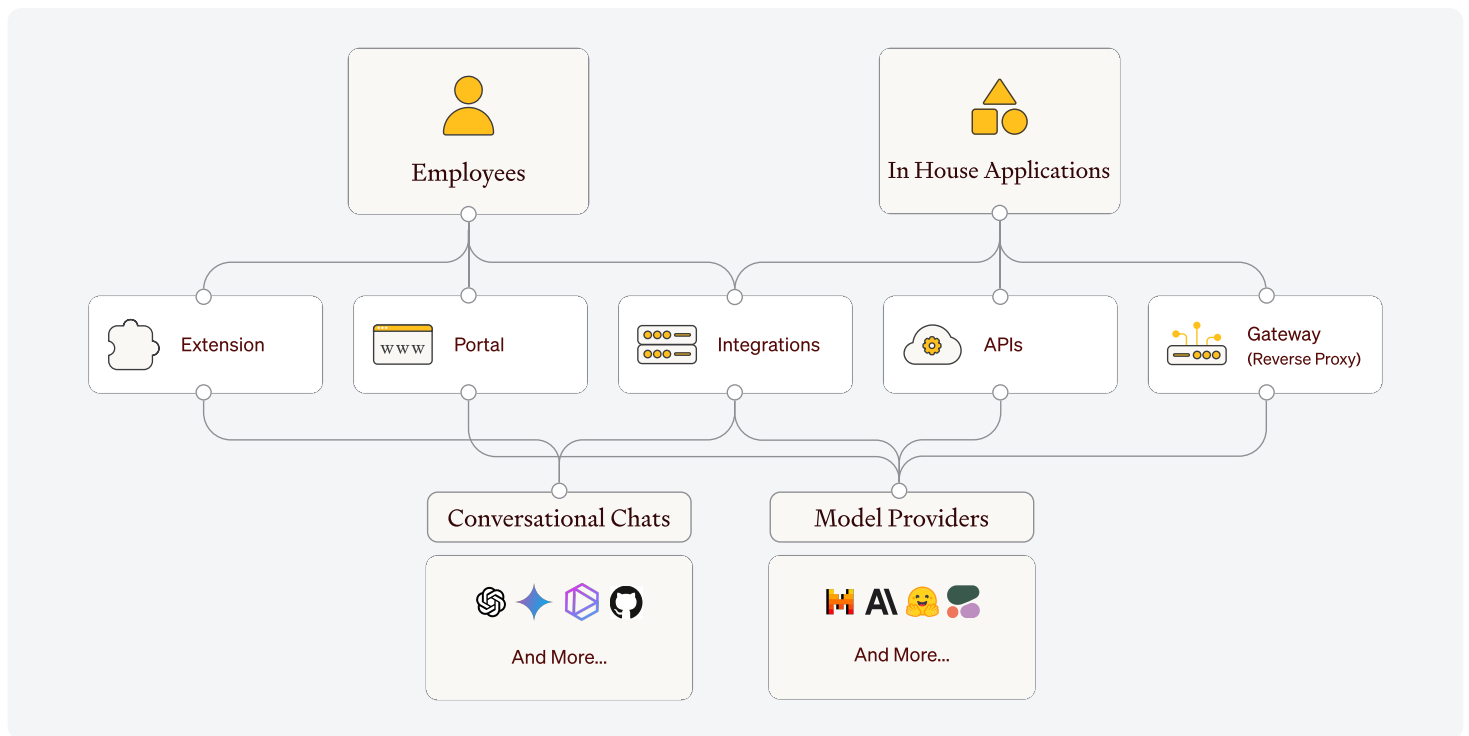
Lasso Red Teaming

Simulates real-world attacks autonomously, identifying vulnerabilities and strengthening LLM security pre-deployment and beyond.

The Lasso Suite: Take Control of LLM Risks

Lasso's GenAI security platform is designed to enhance organizational security by autonomously monitoring all GenAI interactions, detecting risks in real-time, and safeguarding activities across applications, employees, and models. With a product suite tailored to meet the diverse needs of modern organizations, Lasso empowers businesses to adopt LLMs confidently without compromising security or performance.

Lasso's suite sits between the LLMs and data consumers, including GenAI apps, internal teams, employees, models, as well as external user-facing applications. No matter the deployment style, Lasso monitors every touchpoint where data moves to or from the LLM, detecting anomalies or violations of organizational policy.



Governance & Compliance

Lasso is security-centric, adhering to strict compliance standards and aligning with key regulations such as the EU AI Act, the U.S. Executive Order on AI, ISO 27001, SOC 2, and other global governance frameworks.

- Empower your team with the knowledge and skills needed to use LLM-based technologies securely and effectively.

- You don't need to be a security expert—easily set security policies to stay a step ahead of risks and protect sensitive data.

- Lasso ensures alignment with MITRE ATT&CK® methodologies, and actively contributes to the OWASP Top 10 for LLM security project.

All-In-One GenAI Security Platform

Lasso understands the scale and complexity of LLMs and GenAI security and the urgency of adopting in order to maintain security hygiene.

Unlike traditional cybersecurity approaches where LLM security is just an add-on, Lasso focuses exclusively on identifying and mitigating vulnerabilities in Large Language Models. This specialization enables us to address immediate security concerns, anticipate emerging risks, and adapt proactively to the ever-evolving LLM threat landscape.

> Seamlessly Secure Your Entire GenAI Application Portfolio

Empowers you to control data flow and access across your internally developed GenAI applications.

> Set Dynamic, Adaptive Policies

Establish application-specific adaptive guardrails that evolve based on context, for ongoing compliance and privacy standards.

> Respond and Remediate in Real-Time

Lasso provides instant feedback, guiding users to resolve issues in their prompts by removing or masking sensitive information. Simultaneously, security teams receive alerts to investigate and address any deeper risks, enabling a proactive and balanced approach to security.

> Always-on Shadow LLM™

Monitors employee use of GenAI chatbots and tools and gain full visibility into interactions comply with company policies on data sharing.

> Instant Remediation

Shrink the risk window by proactively addressing threats and vulnerabilities as they happen. Safeguard your environment without interruptions, minimizing downtime and protecting your critical assets.

> Protection at The Speed of GenAI

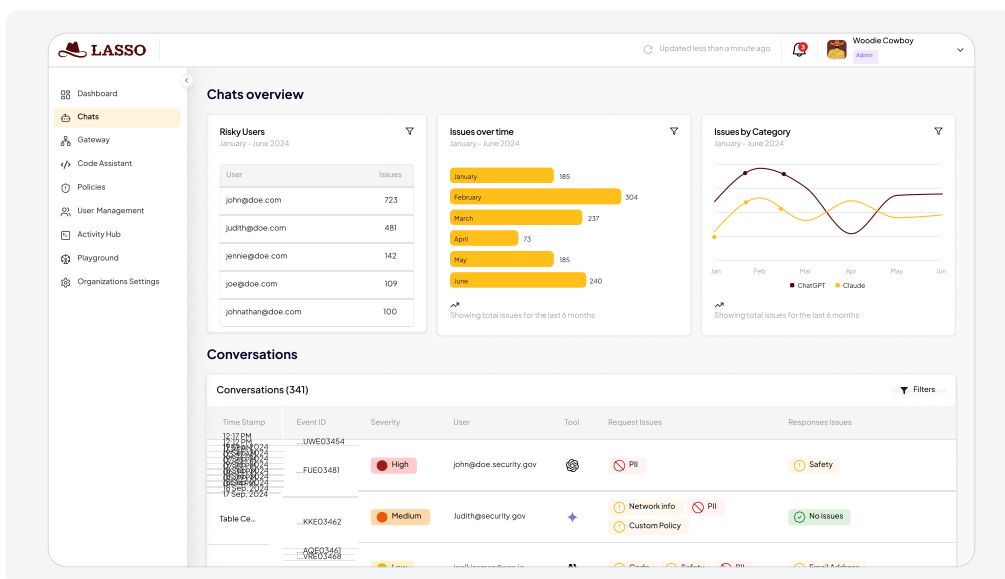
Lasso's RapidClassifier runs custom security policies in less than 50 milliseconds, providing pervasive protection at high speed. It runs unobtrusively in the background with no impact on system performance.

> Activate Seamlessly Across Platforms

Achieve full-coverage security for your applications across various platforms, without disrupting existing workflows.

> Simple, Quick Set-Up

Regardless of deployment style or cloud environment—gain powerful security solutions effortlessly with a single line of code.



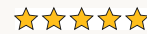
Next-Level Security for The GenAI Era

Lasso offers a flexible and comprehensive suite of GenAI security solutions designed for organizations across industries and the public sector to address a wide range of GenAI-driven cybersecurity challenges.

Whether securing Generative AI applications, protecting sensitive data, or implementing robust AI governance, Lasso provides a unified platform to help organizations maintain a strong security posture in the GenAI era.

Use Cases

- **Enterprises adopting GenAI at scale** often struggle to secure diverse applications across multiple departments, or business units. Lasso ensures consistent security policies and centralized visibility.
- **Security teams lacking visibility into GenAI activities** require comprehensive monitoring and auditing. Lasso provides always-on Shadow LLM detection, audit trails, and threat intelligence to detect and respond to GenAI-related risks.
- **Organizations with rapidly evolving LLM usage** face challenges in predicting security risks and managing compliance. Lasso offers dynamic policy enforcement to adapt to changing environments.
- **Public sector agencies confront growing national security and cyber threats.** Lasso provides dedicated security controls to protect critical infrastructure, safeguard sensitive data, and ensure compliance with strict regulatory and national security standards.



"Lasso Security's comprehensive security suite has been a critical part in securing our GenAI infrastructure. The level of control and visibility it provides ensures that both our internal data and client information are shielded from emerging threats, and gives us the confidence to embrace GenAI safely."

> CISO & VP of Global IT,
> Large Global Telecom Company



Lasso is a GenAI security platform that enhances security posture by autonomously monitoring all GenAI interactions, detecting risks in real-time, and enabling organizations to effortlessly safeguard their GenAI activities.

Lasso is on a mission to empower organizations to confidently adopt GenAI without compromising on security or performance.

For more information visit lasso.security



Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer's digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, VeteranOwned and HUBZone certified Small Business.

Learn more at swishdata.com

