swish Technology Solutions LASSO

Solution Brief

Generative AI and LLM Security

GenAI and Large Languate Models are powerful but it's critical to continuously secure against vulnerabilities and adversarial attacks.

Generative AI technology is now a non-negotiable asset for agencies striving to meet mission outcomes. Recognizing its productivity and efficiency boosting potential, most organizations are deploying AI tools that incorporate Large Language Models and Generative AI (GenAI) technology in their operations.[1]

As agencies 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 an organization at multiple points in various 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 and meet government compliance mandates agencies of all types need to take a proactive approach to securing the way they implement and interact with LLMs.

Top Public Sector CAIO Priorities in 2025 (MeriTalk):

- *#1 Establishing AI governance and compliance*
- *#2 Implementing security, privacy, and risk management*

Key Benefits

- Full visibility into GenAI apps and models across your organization, with 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 agency's unique needs.
- Automated Red Teaming and Guardrails to simulate real-world attacks, uncover vulnerabilities, and proactively adapt protections.
- Comply with NIST AI RMF, AI 600-1, SP 800-218A and address OWASP LLM identified vulnerabilities.
- SaaS and private cloud deployment models with cleared U.S. Citizen Support and Services.

IN-HOUSE APP SECURITY

Lasso for Application

Continuous protection and control over all GenAI apps, agents and models.

SECURE GENAI CHATBOTS

Lasso for Employees

Monitor and protect employee GenAI chatbot usage to ensure security and compliance.

CODE PROTECTION

Lasso for Developers

Prevent infiltrations in development environments for R&D teams.

AUTONOMOUS MODEL SCANNING

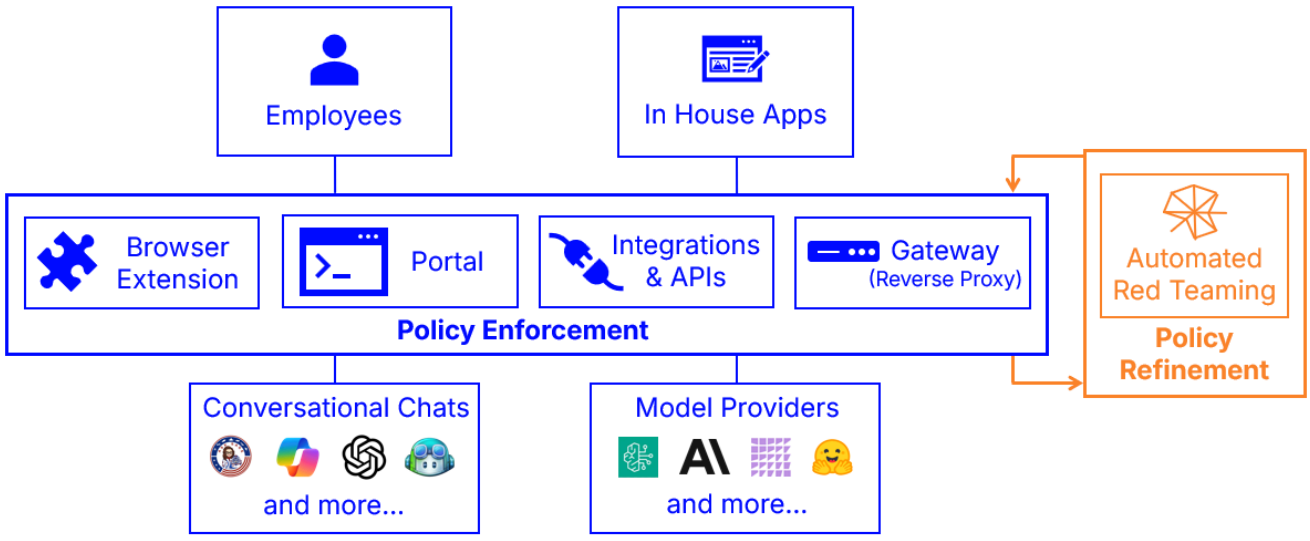
Lasso Red Teaming

Simulates real-world attacks, identifying vulnerabilities and strengthening LLM security.

The Lasso Platform: Take Control of LLM Security

Lasso's GenAI security platform is designed to enhance agency-wide security by autonomously monitoring all GenAI interactions, detecting risks in real-time, and safeguarding activities across applications, employees, models, and agents. With a product suite tailored to meet the diverse needs of government, Lasso empowers agencies 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 and Compliance

NIST Artificial Intelligence Risk Management Framework suggests agencies Map, Measure and Manage risks unique to or exacerbated by AI. The OWASP Top 10 for LLM Applications is a roadmap for navigating the unique challenges posed by GenAI systems. Key regulations such as the U.S. Executive Order on AI, ISO 27001, SOC 2, and others reflect the collaboration insights of a global community dedicated to advancing AI security.

- Empower your team with the knowledge and skills needed to use LLM-based technologies securely and effectively.
- Set intelligent security policies to stay a step ahead of risks and protect sensitive data.
- Swish and Lasso help agencies address MITRE ATLAS® TTPs and actively contribute to the OWASP Top 10 for LLM security projects

swish Technology Solutions

Solution Brief

All-in-one GenAI security solution

We 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, our solution combines technology, support, and specialized services to help agencies implement thoughtful continuous security and governance for GenAI platforms. 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

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

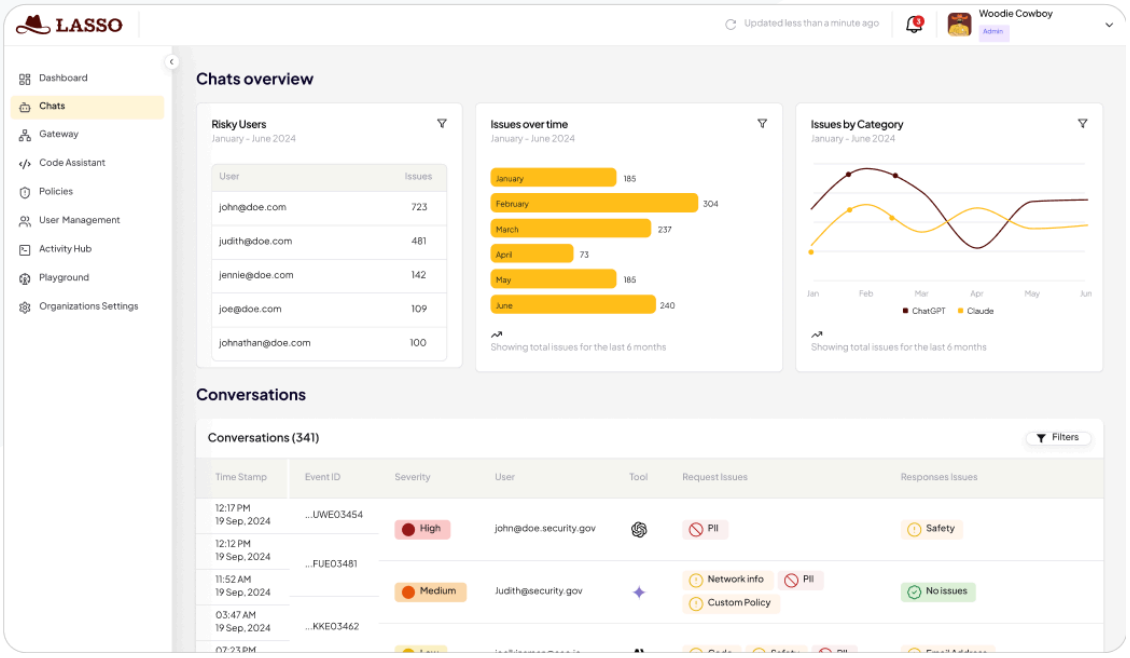
RapidClassifier runs custom security policies in less than 50 milliseconds, providing pervasive protection at high speed. It runs unobtrusively in the background with no impact on system performance.

Activate Seamlessly Across Platforms

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

Trusted Support and Services

Trusted support and services from cleared U.S. Citizens helps clients successfully navigate this rapidly changing space.



Next-Level Security for the GenAI Era

Our solution offers a flexible and comprehensive suite of GenAI security capabilities designed for organizations across 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, We provides a unified platform with cleared U.S support and specialized services 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.
- **Agencies 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.

The Swish Advantage

Securing GenAI requires not only the enabling technologies, but specialized support and services from cleared U.S. Engineers. Swish is the exclusive Public Sector Support and Services Provider for Lasso Security. With years of experience and a proven framework for delivering mission value for government clients, Swish works with your agency to ensure your GenAI security outcomes are realized. Swish provides a vast array of services including cleared U.S. Citizen support, AI Security workshops, planning services, implementation services, staff augmentation, and fully managed service offerings. We work with every client to design a solution plan to deliver agency-wide adoption and outcomes. Swish has a deep understanding of the public sector acquisition management process and solutions are available from a variety of contract vehicles and marketplaces.

LASSO

Lasso Security 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.

www.lasso.security

swish Technology Solutions

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, Veteran-Owned and HUBZone certified Small Business.

www.swishdata.com

1420 Spring Hill Road Suite 320 McLean, VA 22102

P 703.635.3324 / E info@swishdata.com