End-to-End Security Platform for Large Language Model Pioneers.

Imagine a future where LLM technology isn't just productive, it's safe.

The challenge: an untamed frontier

Large Language Model (LLM) 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 operations.[1]

But for all their benefits, LLMs also bring a new set of risks and security challenges. These include exposure of sensitive data, notably source code, and the surge in advanced cyber threats, and 'smart malware'. Most vendors hosting GenAI models cannot fully protect users from these risks.

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

1 - "The state of AI in 2023: Generative AI's breakout year," August 1, 2023, McKinsey Global Institute.

Key Benefits

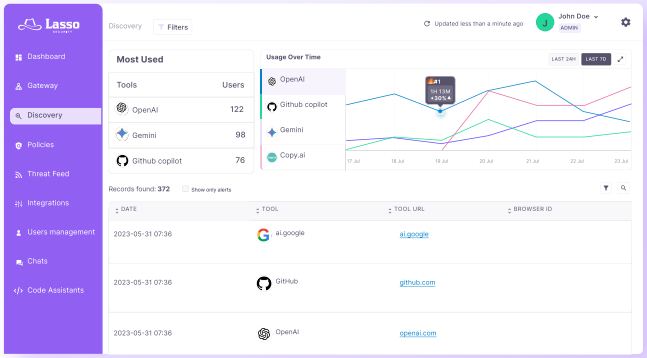
- Gain full visibility over employees' use of LLMs for business tasks, which tools and how they are using them
- Safely leverage GenAI technology for application development, with seamless integration and real-time data masking
- Prevent leakage of sensitive information into unsecured models
- Automatic anomaly detection of threats for rapid response and remediation
- Fully tailored policy enforcement with customized defense

contactus@lasso.security | +1-917-997-2350 | www.lasso.security

Lasso SECURITY

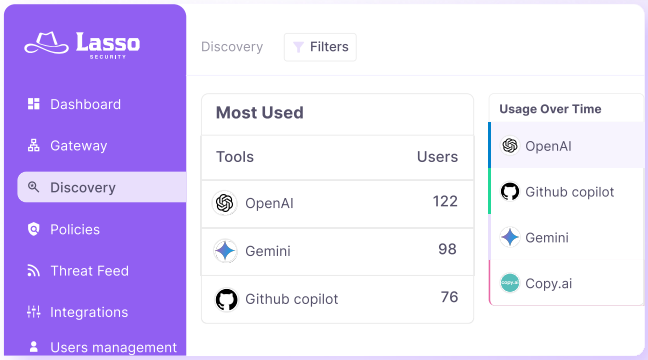
Easy Onboarding & Integration

Quick and easy installation, suitable for any deployment style. Integrate Lasso and start monitoring data flow through and from GenAI applications in minutes, using a user-friendly and intuitive dashboard.



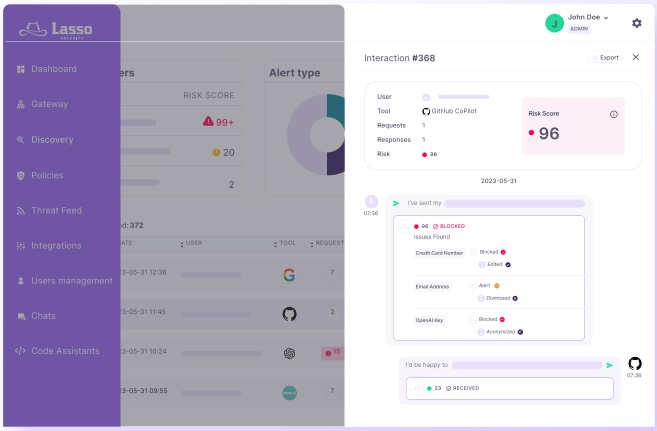
Always-on Shadow LLM™

Uncover every LLM interaction and facilitate the precise identification of active tools, models, and their users within the organization.



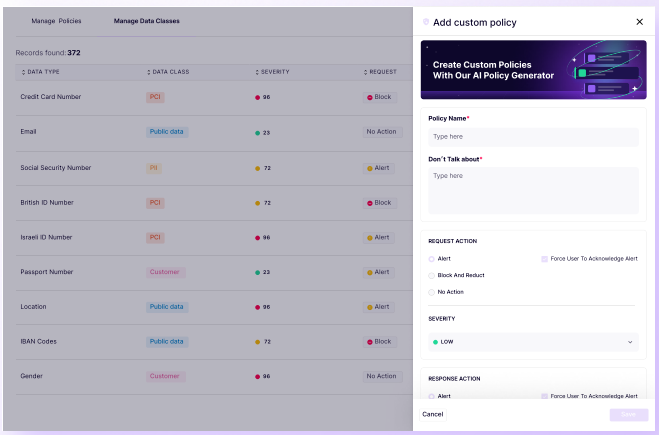
Real time Response and Automated Mitigation

Swift alert mechanisms provide timely notifications to both users and security teams for rapid response and protection against real-time threats.



Customized Policy Management Wizard

No coding, development or data science expertise is required to use the wizard. Users can apply free-form language to create policies tailored to their specific needs.



contactus@lasso.security | +1-917-997-2350 | www.lasso.security

The good news: There's a new sheriff in town

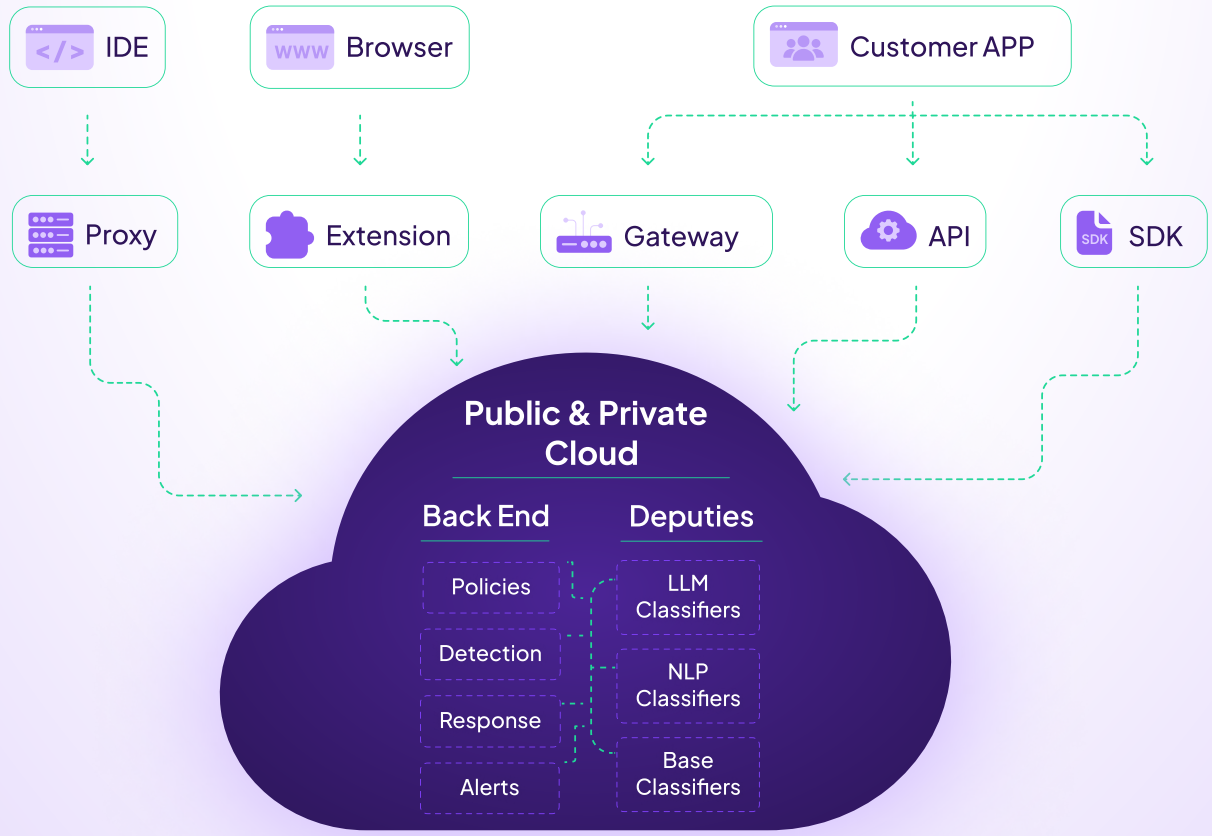
Lasso's comprehensive security suite specifically designed for the challenges associated with Large Language Model (LLM) and GenAI technology.

Rather than an add-on to a broader cyber security framework, solving LLM vulnerabilities is our sole focus. This understanding allows us to meet immediate client's security needs and proactively adapt to the evolving landscape of LLM cyber security challenges.

Lasso is security-centric and adheres to strict compliance standards. We provide custom solutions to meet security threats, ensure compliance with **MITRE ATT&CK®**, and actively contribute to the **OWASP Top 10 for LLM**.

Check all GenAI Security Boxes with Lasso Security

- Content Anomaly Detection
- Hallucination Detection
- Insecure Output Handling
- Supply-Chain Vulnerabilities
- Prompt Injection Detection
- GenAI Application Security
- Data & Knowledge Protection
- Privacy & AI Compliance

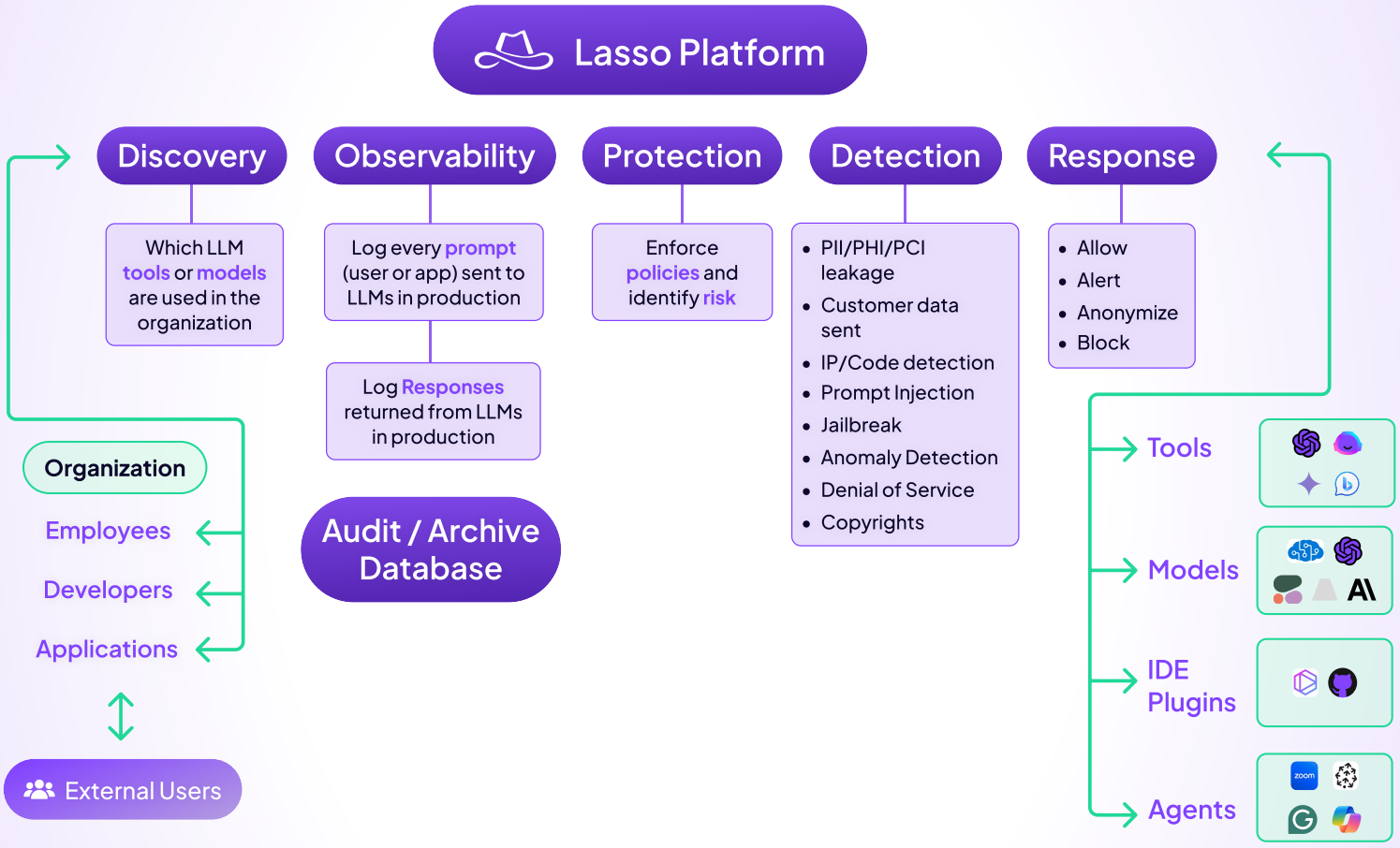


contactus@lasso.security | +1-917-997-2350 | www.lasso.security

Lasso SECURITY

How it Works

Lasso's suite sits between the LLMs and data consumers, including internal teams, employees, software, 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.



Why Lasso Security

Our founding team is made up of cyber security experts with deep knowledge and experience in the rapidly evolving field of large language model (LLMs) and GenAI technology.
Lasso is committed to safeguarding against LLM threats, and to help organizations make this crucial transition, embracing progress without compromising their cyber security posture.

Partnered with world-leading vendors

Microsoft Proud to partner with Microsoft for Startups
NVIDIA INCEPTION PROGRAM
AWS Startup Loft Accelerator Proud members
Global Infosec Awards Winner Cyber Defense Magazine 2024
AICPA SOC 2
ISO 27001 Certified

contactus@lasso.security | +1-917-997-2350 | www.lasso.security