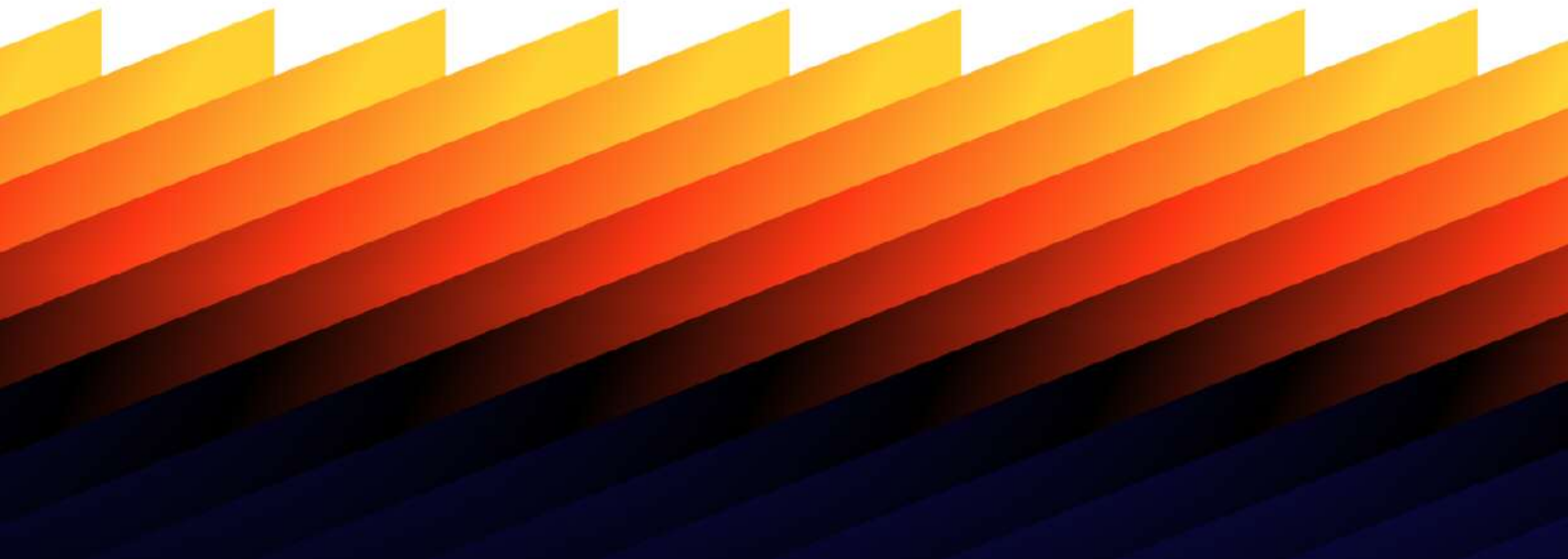
LAKERA

LLM Security Solution Evaluation Checklist

FOR ENTERPRISE SECURITY TEAMS



This is a checklist that Security Teams can use to evaluate LLM security solutions currently available on the market.

Use this short assessment to pick the tool that best fits your needs or get in touch with our team to discuss your options.

💡 **Pro tip:** Check out this list of 12 Top LLM Security Tools: Paid & Free (Overview)

LLM Security Solution Evaluation Checklist

Solution Scope

- [ ] **Supported Language Models**
  Identify if the solution supports the LLMs or providers you use (e.g., OpenAI, BERT, etc.) and is flexible enough to switch to newer models in the future.
- [ ] **Security Features**
  Evaluate the range of security features provided (e.g., data encryption, access controls, audit logs).

Security Protections

- [ ] **Prompt Injection Protection**
  Check if the solution guards against prompt injection attacks.
- [ ] **Data Leakage Prevention**
  Determine if the solution prevents sensitive data from leaking into or out of LLMs.
- [ ] **Model Validation**
  Ensure the solution validates LLM models for bias, harmful content, or hallucinations.
- [ ] **Red Teaming**
  Examine if the solution includes red teaming to test for vulnerabilities.

Customization and Control

- [ ] **User-defined Security Parameters**
  Look for the ability to customise your security priorities.
- [ ] **Data Handling Controls**
  Assess both automated and manual controls for data management.

Threat Intelligence

- [ ] **Threat Database**
  Confirm that the vendor maintains a comprehensive and updated threat database.

Monitoring and Performance

- [ ] **Continuous Monitoring**
  Ensure continuous security threat monitoring.
- [ ] **Performance Impact:**
  Evaluate any impacts on user experience or performance (e.g. latency).

Support and Responsiveness

- [ ] **Training and Support**
  Look for vendor-provided training, support, and documentation.
- [ ] **Zero Day Readiness**
  Assess the vendor's responsiveness to emerging threats.

System Usability and Management

- [ ] **Observability**
  Ensure the solution offers intuitive UX and customizable dashboards.
- [ ] **Alert Customization**
  Check for options to customize alerts to avoid overload.
- [ ] **Context-Aware Security**
  Verify if the solution distinguishes between malicious and benign prompts based on context.
  Note : Look for defenses tailored to your specific use cases.

Integration and Compliance

- [ ] **Integration with Existing Infrastructure**
  Assess compatibility with existing security setups (on-premises, cloud).
  Note: For cloud-based solutions, double-check how your data is handled and where it is stored.
- [ ] **Compliance with Industry Standards**
  Check for adherence to your relevant industry standards like ISO 27001, HIPAA, or SOC 2.
- [ ] **Data Training**
  Determine if the solution uses your proprietary data for training.