SOLIDWALL AI SECURITY GATEWAY

INTELLIGENT FIREWALL FOR AI APPLICATIONS AND APIs

Built on Yandex Cloud technologies and SolidLab expertise.
Available for deployment in the customer environment or as a cloud service.

USE CASES

- Protection against major attacks on AI applications covered by OWASP LLM Top 10 Risks and OWASP Top 10 for Agentic Applications, including prompt injection, jailbreaks and sensitive information leakage.
- Protection against major web application attacks covered by the OWASP Top 10 and against business logic attacks on AI applications.
- Full API protection with API gateway capabilities and tools to create and refine security models.
- Defense against brute-force attacks and bots through a positive security model, rate limiting and analysis of user behavior when accessing AI-specific application features.
- Protection against targeted resource-exhaustion attacks (“smart DoS”), taking the operating characteristics of large language models into account.
- Monitoring user actions through analysis and retention of legitimate transactions, together with business logic controls.

ADVANTAGES

- Interpretable machine learning, with tools to analyze and manually refine learned models, reducing the resources needed for configuration.
- Adaptive block pages that make it harder to use AI/LLMs to attack AI applications.
- Attack detection based on a negative security model.
- Defense against brute-force attacks and repeated requests.
- Protection based on positive application security models.
- Quick false-positive suppression by the SolidWall AI Security Gateway operator, with fine-tuning of individual parameters.
- Decision rules based on the source and destination of an HTTP transaction, as well as anomalies or relevant data detected within it.
- Security event monitoring and auditing through statistics and alerts, with data export to reports.
- Integration into corporate application delivery infrastructure.
- Detection of anomalies and significant events.

OPERATING MODES

Analysis nodes can protect AI applications inline between application users and the application itself, with blocking mode quickly enabled or disabled.

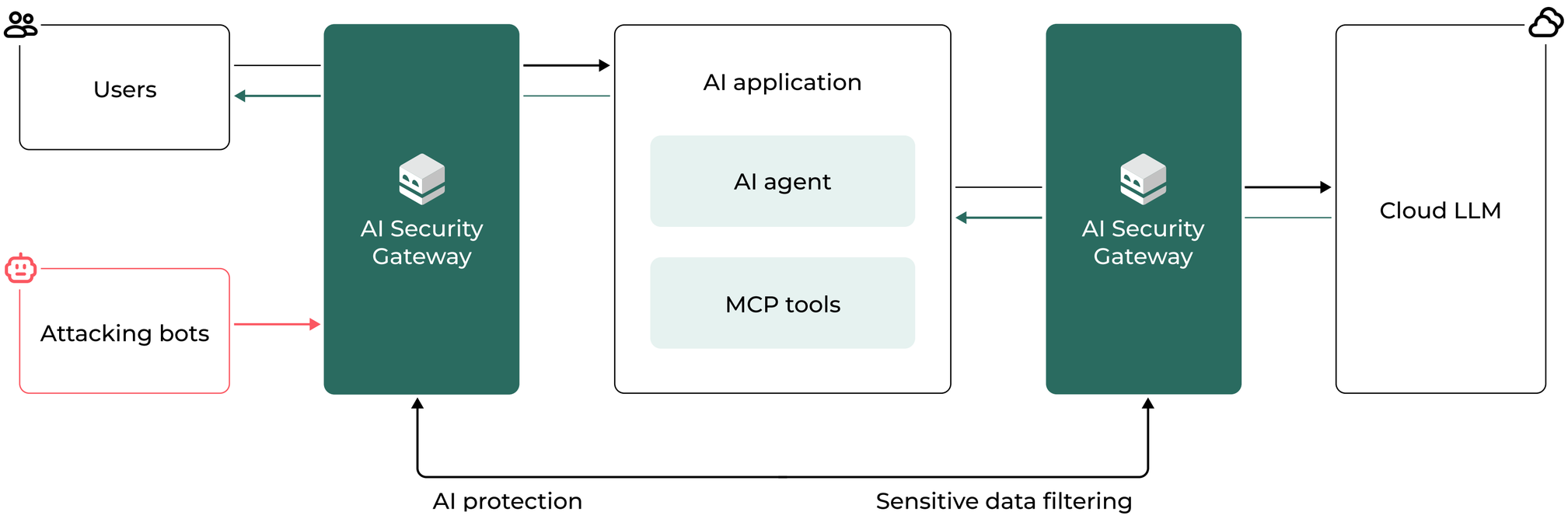
Analysis nodes can protect sensitive information inline between an AI application and an external LLM provider, filtering outbound requests that contain sensitive information.

HIGH AVAILABILITY

- Active/active or active/passive clustering for analysis nodes, and active/passive operation with replication for the management system.
- Software bypass mode and execution of the default action without inspection during local failures or sudden traffic spikes.

INTEGRATION WITH EXTERNAL SYSTEMS

- Integration with SIEM systems
- Integration with other systems through Syslog, SQL and REST APIs
- Import OpenAPI specifications as actions in the business logic model, including integration into CI/CD workflows.
- Integration with the SolidPoint application security scanner for early identification of AI application security weaknesses and vulnerabilities covered by OWASP LLM Top 10 Risks.
- APIs for sending data to external systems
- Software and hardware health monitoring with Zabbix and Prometheus



47A Vavilova St., Moscow 117312
solidlab.ru/en
info@solidlab.ru

SolidLab Group has worked in information security for over 15 years, protecting organizations against cyber threats, preventing attacks and minimizing the risk of financial and reputational damage. SolidLab offers a full range of services, from penetration testing to application security, incident response and establishing SDLC processes.