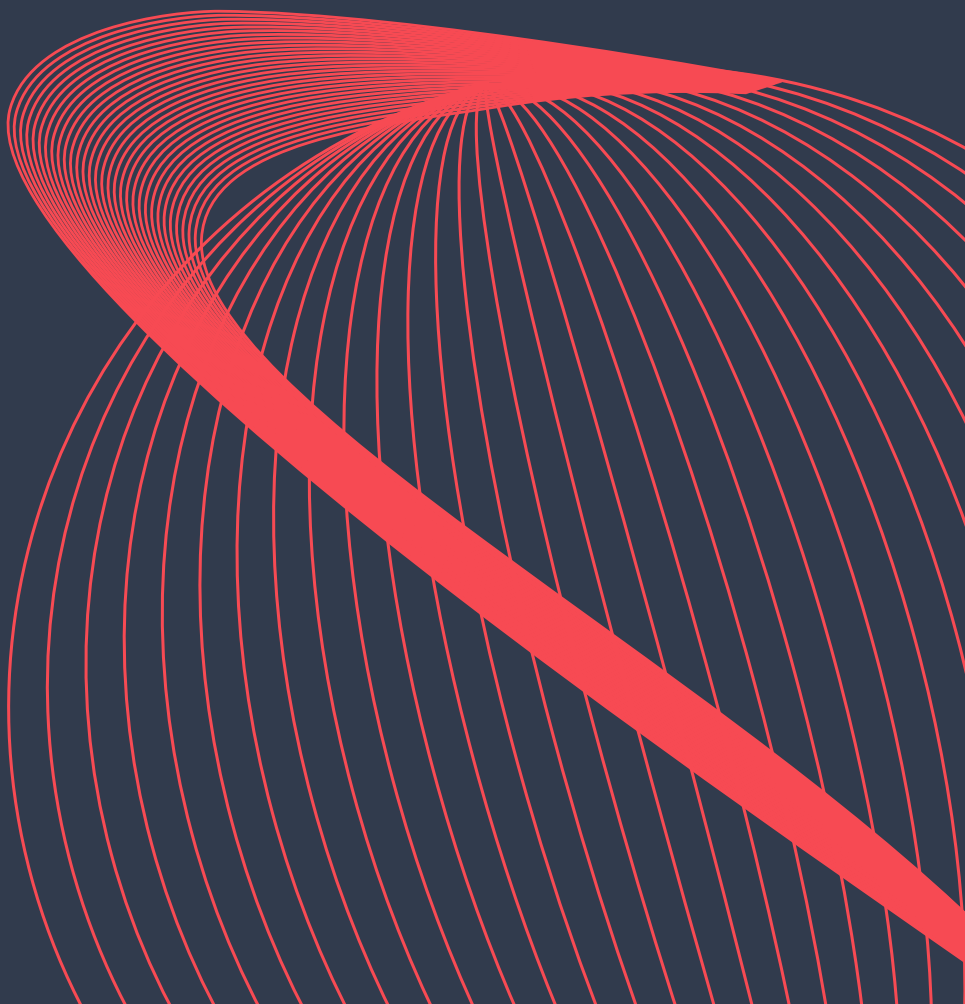
pillar

ONE PAGER

Build, run, and use AI with confidence

Pillar enables teams to rapidly adopt AI with minimal risk by providing a unified AI security layer across the organization



pillar

The Pillar Platform

An all-in-one platform that empowers organizations to monitor, assess risks, and secure their AI activities.

About Pillar

We are building the unified AI security layer to help enterprises accelerate AI transformation. Led by an experienced and visionary team, Pillar brings together experts with extensive backgrounds in adversarial cybersecurity, threat intelligence, and AI. Pillar's mission is to secure the new AI paradigm by providing complete visibility and control across the entire AI lifecycle.

A Single platform to secure the entire AI lifecycle

Pillar for AI Development

Continuously identify AI projects and assess their risks to enhance resilience against threats and ensure compliance.

- **Discover** — Continuous mapping of AI inventory
- **Evaluate** — AI red teaming and exposure management

Pillar for AI Applications

Monitor and safeguard your AI applications in with model-agnostic guardrails to prevent attacks and ensure data integrity.

- **Observe** — Real-time application monitoring
- **Protect** — Runtime application security

Pillar for AI Usage

Audit 3rd-party AI tool usage and enforce detailed security policies, authorize applications, and protect company-sensitive data.

- **Audit** — Identify and audit usage of AI tools
- **Enforce** — Enforce safety and security policies

Pillar Unified AI Security Platform

Proprietary risk detection & evaluation models, powered by real-world app interactions and threat intelligence.

- RAG VECTOR DATABASE
- GATEWAYS
- CLOUD PROVIDER
- MODEL
- NETWORK SECURITY
- BROWSER
- IDENTITY PROVIDER
- ORCHESTRATION LEVEL

Key Elements of a AI Security Platform

Use Case

Pillar platform Capabilities

Visibility and Monitoring

Challenge

AI systems lack transparency in their operations, making it difficult to understand system behavior, trace issues, and ensure compliance. This lack of visibility can lead to undetected vulnerabilities and operational inefficiencies.

Pillar's platform capabilities

- **Provide** horizontal visibility by mapping all AI application components, meta-prompts, models, and tools
- **Offer** vertical visibility through in-depth logging of every application interaction
- **Track** and trace the entire flow of events, inputs (prompts), instructions (meta-prompts), tools and generated outputs
- **Enable** thorough understanding of application logic and use cases for better management and optimization

Data Protection Mechanisms

Challenge

AI systems handle vast amounts of confidential and sensitive data, risking leaks, compromises, and poisoning attacks both internally and with external providers.

Pillar's platform capabilities

- **Prevents** data leakage and safeguards confidential information while using AI applications
- **Provides** on-demand data masking for sensitive details
- **Identifies** over 40 different data types and categories

Content Anomaly Detection and Filtering

Challenge

Unchecked AI outputs can lead to faulty decisions or harmful actions based on inaccurate or inappropriate information, risking enterprise decision-making and confidentiality.

Pillar's platform capabilities

- **Detect and block** unacceptable inputs that could compromise enterprise decision-making and confidentiality
- **Support** dynamic, prompt-aware, and contextual policy enforcement per AI application
- **Integrate AI-based** detection with traditional techniques like keyword matching and rule engines

Key Elements of a AI Security Platform

Use Case

Pillar platform Capabilities

Enhanced Application Security

Challenge

The rapid evolution of AI applications introduces new vulnerabilities, especially prompt injection and jailbreaking attacks that bypass existing filters. Traditional security systems often fail to address these AI-specific threats effectively.

Pillar's platform capabilities

- **Defend** against adversarial prompts that could put your app, data and users at risk.
- **Mitigate** risks within your AI applications, vector databases, and tool usage
- **Prevent** unauthorized or abusive usage of your AI applications
- **Provide** runtime monitoring for detecting anomalous model behavior and drift

Adversarial Resistance and App Robustness

Challenge

AI systems are susceptible to novel adversarial attacks that can undermine their integrity and performance, making regular testing and validation crucial to ensure robustness, identify deviations, and safeguard against new threats.

Pillar's platform capabilities

- **Harden** your applications against adversarial and AI-focused attacks
- **Test** your applications robustness using tailored AI red teaming activities
- **Evaluate** the resilience of your AI applications and associated models, meta-prompts and tools
- **Continuously** assess your applications to stay ahead of emerging attack vectors

Enterprise ready Scale & Security

Challenge

Integrating AI systems into enterprise operations demands scalable, secure deployment while adhering to strict data protection standards and compliance requirements.

Pillar's platform capabilities

- **Flexible Deployment:** on-premises, hybrid, and cloud options to match diverse enterprise needs
- **Seamless Integration** with existing security workflows to enhance operational efficiency
- **SOC 2** Type II report audit and adherence to strict security standards ensure data protection and system reliability.
- **Robust Role-Based** Access Controls (RBAC) to manage user permissions effectively
- **Provide actionable** alerts, analytics, and reporting for proactive threat management.

ALIGNED WITH LEADING AI SECURITY FRAMEWORKS OWASP MITRE ATLAS NIST