AccessMatrix.AI

Agent Identified . Action Authorized . Prompt Secured . Model Protected

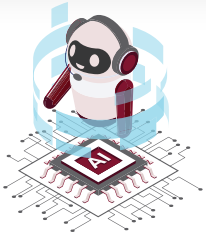
The Identity-Centric Security Platform for Enterprise AI

AI agents already act on behalf of your people. AccessMatrix.AI makes sure every one of them is identified, authorized, and accountable.

AccessMatrix.AI is an identity-centric security platform for enterprise AI. It brings AI Agent Security, AI Safety, AI Integrity, and AI Empowerment together on one platform, so every agent, prompt, model, and AI feature runs under identity-based control.

Policy is enforced at runtime on every prompt, tool call, and data flow, rather than written in a document and checked after the fact. Built on AccessMatrix, i-Sprint's identity and access management platform for financial institutions across APAC, it lets you move AI from pilot to production at speed, with the evidence your auditors and regulators expect.

Features of AccessMatrix.AI



AI Agent Security

ACCESSMATRIX.AI AGENT SECURITY PLATFORM

- Verifiable identity for every agent, user, and workload, tied to an accountable owner
- Delegated authority: agents act for a named user, never beyond that user's entitlements
- Least-privilege, short-lived tokens per task, with no standing secrets
- Provision, review, and revoke agents the same way as staff accounts



AI Safety

AGENT SECURITY PLATFORM · ENTERPRISE BROWSER

- Deterministic authorization on every tool, file, and network call before it runs
- Prompt and output inspection, with PII and secret redaction at the agent boundary
- Egress control over which endpoints agents reach and where data can go
- AI Protect in the Enterprise Browser governs how staff use AI sites



AI Integrity

APPPROTECT+ FOR AI

- Model weights, inference runtimes, and AI apps as cryptographically protected assets
- Signing, encryption, and anti-tamper for model artifacts
- Provenance verified before a model is loaded or served
- License control over where and how protected models may run

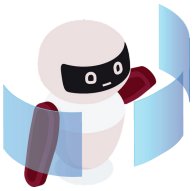


AI Empowerment

ACCESSMATRIX.AI BIZCONNECT

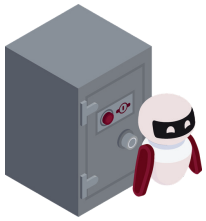
- AI capabilities embedded into existing business applications, without a rebuild
- Governed access to enterprise data and inference endpoints
- Entitlement, metering, and monetization of AI features

Why AccessMatrix.AI



Banking-Grade Identity for Users & AI Agents

Extend proven OIDC/OAuth identity and access management, with MFA, to every user, workload, and autonomous agent. Each agent has an accountable owner and acts only within the entitlements of its user.



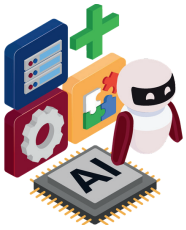
Unified AI Gateway & Forensic Auditing

Route all AI traffic to LLMs, MCP servers, and remote agents through one policy enforcement point backed by the AccessMatrix IdP. Block prompt injection, malicious agent skills, and PII leakage in-line, with every action in a tamper-evident audit trail.



HSM-Backed LLM API Key Vault

Remove hardcoded API keys from code and configuration. Keys stay encrypted in an HSM-backed vault, are injected just in time per request, and rotate automatically, so agents never hold standing secrets.



Zero-Trust Proprietary Model Protection

Ring-fence the models you build against unauthorized invocation, copying, and tampering. AppProtect+ signs, encrypts, and hardens model weights and AI apps, and licenses them to run only where you allow.



Drop-In Enterprise AI Enablement

Embed governed AI features into your applications without building security infrastructure. BizConnect grants features by role or segment, meters usage, and turns AI into billable services.

- **Quantum-safe Path**: AccessMatrix.AI pairs with QubitSafe for crypto-agility and post-quantum migration.

i-Sprint
Trust without Boundaries

For a complete list of our offices in Hong Kong, Malaysia, Thailand, Indonesia, Japan, Vietnam, Philippines & United States, please visit www.i-sprint.com/contact-us/

Global Headquarters
Blk 750D Chai Chee Road
#08-01 ESR BizPark@ Chai Chee (Lobby 1)
Singapore 469004

+65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

Copyright © 2000 - 2026 i-Sprint Innovations Pte Ltd. All rights reserved.