TrustAI Solution Brief

TRUSTLOGIX

Preemptive Data Security for the Age of AI Agents

Executive Summary

AI innovation is outpacing traditional data security. As organizations deploy autonomous agents and AI-driven workflows, data exposure risks have exploded — from sensitive PII/PHI leakage to uncontrolled model access across multiple clouds.

TrustAI by TrustLogix brings preemptive, enterprise-grade data security to the world of AI. Built on the proven TrustAccess and TrustDSPM foundation, TrustAI serves as a dynamic data security layer between enterprise data platforms and AI agent frameworks. It continuously evaluates every data request, enforces least-privilege and just-in-time access, and masks sensitive fields — all without slowing AI innovation.

With TrustAI, enterprises can move fast with AI while staying secure, compliant, and auditable.

The Challenge: AI at Machine Speed, Security at Human Speed

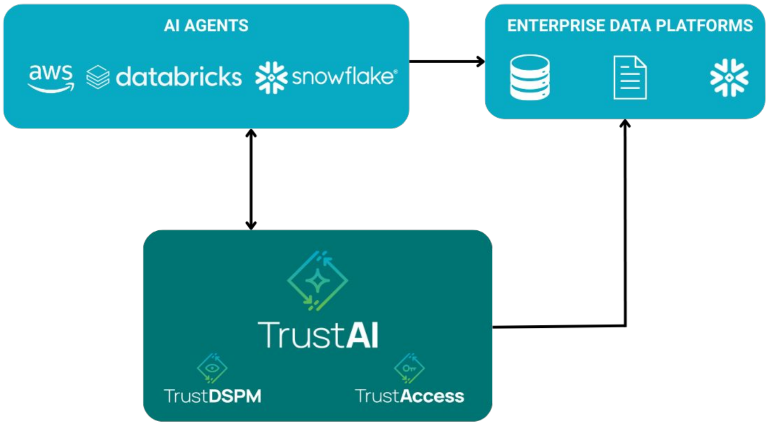
AI adoption has introduced a new class of risk. AI agents and connectors act autonomously, often with persistent privileges and little visibility into their activity. This creates dangerous blind spots:

- Over-permissioned access: AI agents often hold standing credentials to entire datasets.
- Unmonitored usage: Security teams cannot see which agents access what data, on whose behalf, or for what purpose.
- Regulatory exposure: Sensitive PII/PHI data flows into AI prompts and models, violating compliance frameworks like SOX, GDPR, and HIPAA.

As Gartner warns, the age of AI-driven attacks and automation demands preemptive, autonomous security — not reactive monitoring. Organizations need the same speed and intelligence in their data governance that AI brings to their operations.

The Solution: TrustAI — Dynamic, Preemptive Data Security for AI

TrustAI transforms the TrustLogix data security platform into an AI-aware, policy-driven defense layer that proactively governs how AI agents interact with enterprise data.
It delivers continuous control, visibility, and auditability for every data request — human or non-human — across data platforms, AI frameworks, and clouds.



Core Capabilities:

1. Dynamic, Context-Aware Access Controls

TrustAI continuously evaluates each data request in context — who (human or non-human or agent), what data, for what purpose, and under what conditions — before granting access. Policies adapt in real time based on identity, sensitivity, and project, ensuring that only authorized data is ever exposed.

> *Result: No more static permissions or over-privileged agents — access evolves dynamically with business and risk context.*

2. Just-in-Time Access and Privileged Account Management

AI pipelines often depend on privileged service accounts or API tokens that never expire. TrustAI replaces these with just-in-time access — granting temporary entitlements only when required and automatically revoking them after use.

> *Result: Eliminates standing privileges and reduces insider and automation-related data risks.*

3. Unified, Autonomous Governance Across Data and AI

By extending TrustAccess and TrustDSPM, TrustAI brings AI agents into the same unified governance model that secures enterprise data. Global policies (e.g., “No PII in model training”) can be centrally defined, while departmental local teams configure business-domain-specific rules — combining central control with local autonomy.

> *Result: Frictionless collaboration between data, AI, and security teams.*

4. Continuous Visibility and Compliance

TrustAI provides continuous monitoring and immutable audit trails for every AI data interaction. Security and compliance teams can easily trace who accessed which data, when, and why — meeting emerging AI governance and audit requirements.

> *Result: Compliance confidence for regulated industries like financial services, healthcare, and life sciences.*

Why TrustAI Now

- AI data risk is accelerating: Autonomous agents and LLMs are connecting to sensitive data faster than governance can keep up.
- Reactive controls can’t keep pace: Human approvals and static access lists fail at machine speed.
- Regulators are tightening oversight: New AI and data privacy regulations demand explainable, traceable data use.

TrustAI enables enterprises to adopt AI safely — moving from reactive control to proactive assurance.

The Cost of Inaction (Do-nothing)

Enterprises that fail to deploy an AI-aware data security layer risk:

- Uncontrolled data sprawl across agents and RAG pipelines
- Non-compliance and reputational damage from data leaks or audit failures
- AI project delays as security teams revert to manual gating and blanket denials

Without TrustAI, organizations face the same "velocity gap" Gartner warns about in preemptive cybersecurity — a world where humans can't respond as fast as AI can act.

The TrustLogix Advantage

- Proven TrustAccess and TrustDSPM platform already deployed across leading enterprises
- AI-native, proxyless architecture — no data access, no data movement, no agents
- Policy-driven data access and real-time enforcement at the data source
- Seamless integration across Snowflake, Databricks, AWS, Azure, and AI Agent frameworks

Outcome	Benefit
Accelerate AI innovation securely	Enable data and AI teams to experiment safely with governed access
Reduce risk and compliance exposure	Enforce real-time controls and auditable data lineage for every AI interaction
Streamline governance operations	Automate policy enforcement and entitlement management
Build enterprise trust in AI	Ensure transparency, accountability, and explainability for all data used in AI

Summary

AI's potential depends on trust — and trust begins with secure, governed data access. TrustAI enables enterprises to innovate with confidence by uniting AI speed with security precision. It's not about slowing down AI. It's about ensuring AI never outruns your governance.

TrustAI — Preemptive Data Security for the AI-Driven Enterprise.