Trust3 AI

PRODUCT BRIEF

Secure Agents Everywhere And Everything They Touch

Security control plane extends from agents to the data agents reach.
Discover, observe & secure across the complete agent lifecycle, by the creators of Apache Ranger.

THE PROBLEM

Agents Are Running Without Security

Agents are sprawling across data systems, applications & tools. Gartner projects that by 2029, over 50% of successful attacks on AI agents will exploit access control weaknesses to reach enterprise data.

Shadow AI
Agents spin up on approved infrastructure and never reach a registry, so enterprises undercount them by 3–10X.

No Comprehensive Observability
Untraced agent actions leave no way to audit or assign accountability. Token spend runs unchecked for the same reason.

Access Too Broad for Autonomy
Access is granted by role, not by purpose, so agents hold entitlements far beyond single tasks. Blast radius compounds when one agent invokes another.

Incomplete Lifecycle Enforcement
Agents go unreviewed at build time and unchecked at runtime. Enforcement rarely holds from creation to action.

THE SOLUTION: TRUST3 AI

Trust3 AI Security Control Plane

Agent Security
Agent DOS: discover, observe, secure

Everything Agents Touch — Attack surfaces

Tools
Web search, email, code exec, browser

MCP Servers
GitHub, Postgres, Slack, custom

APIs
REST, GraphQL, Internal APIs

SaaS Apps
Salesforce, Slack, ServiceNow, Workday

Data Security
PBAC and FGAC

50+

AI-native metadata travels with every request — Agent identity · Declared purpose · Live policy state

Agent Security

- **Discover**: every agent, including shadow AI, across Databricks, Azure AI Foundry, Copilot Studio, Microsoft 365 & more
- **Observe**: end-to-end traces of every agent step, input to output, with deviations scored as they happen
- **Secure**: purpose-based access, MCP & A2A tool control, runtime guardrails and a kill switch on agent actions

Data Security

- **Discover & classify**: sensitive data across warehouses, lakehouses, cloud storage & vector / RAG stores
- **Control access**: row, column & tag-based policy; attribute- and purpose-based, replacing over-privileged roles
- **Protect & monitor**: encryption, tokenization, usage lineage & continuous audit evidence

THE DIFFERENTIATOR

Coverage with Enforcement Depth

ENFORCEMENT ↑

Native enforcement, data only

Immuta · Snowflake-native · Databricks-native.
Deep native enforcement, but data only and blind to agents.

Trust3 AI

Native enforcement across agents & data

Fine-grained policy enforced natively across both the agent layer and the data it reaches, in one model, build-time to runtime.

POSTURE ↓

Agent or identity-only

Palo Alto Prisma AIRS · Zenity · Noma · Okta · Entra ID.
Partial coverage; guardrails or identity, not data enforcement.

Security posture only, across agents & data

Cyera · Rubrik · Securiti · Microsoft Purview.
Broad visibility and posture, but not native fine-grained enforcement.

← DATA OR AGENTS ONLY — AGENTS & DATA →

CIO - FORTUNE 50 ENTERPRISE

"Operating across multiple clouds and data platforms, governance complexity has historically slowed our ability to operationalize AI. With Trust3 AI, we now have a unified trust layer that consistently governs both our data and AI systems, significantly accelerating enterprise-wide adoption."

RESULTS

Numbers from Production

10X
Faster from POC to production

6X
Faster audit preparation

50+
Native data sources, zero proxy latency

100%
Of discovered agents scored, incl. shadow AI

AGENTIC SECURITY

Governance Intelligence Agent

A conversational interface to your security posture. Query & act on agents, policies, compliance status & data access in natural language.

ASK GIA · GOVERNANCE INTELLIGENCE AGENT

Define & enforce access policies in plain English

"Grant Finance Analysts read access to REVENUE tables for Q4 close, expiring January 15."

PROOF

Use Cases from Five Enterprise Customers

FORTUNE 500 · FINANCIAL

300+ agents discovered during an audit. Audit-ready without pausing operations, with a continuous Trust Score per agent.

FORTUNE 100 · FINTECH

Hit AWS IAM limits; replaced overprivileged roles with attribute-based access and eliminated manual provisioning.

TOP 5 US · HEALTHCARE RETAIL

Thousands of BigQuery tables across hundreds of GCP projects, governed without a ticketing queue.

FORTUNE 50 · HEALTH SERVICES

HITECH-grade, column-level Snowflake governance. Rapid model development for billing, claims & health trends.

FORTUNE 50 · MEDIA + TELECOM

Replaced failed DIY governance; Customer 360 unblocked on a single hybrid-cloud control plane.

ACROSS THE BASE

40% Fortune 500 customers. Enforcement native to each platform, with zero proxy latency.

THE SHIFT

From Fragmented to Unified

What changes when Trust3 AI is in place.

Without Trust3 AI	With Trust3 AI
Enterprises undercount agents by 3–10×	Every agent discovered automatically, including shadow AI
Agents run with standing access and no purpose scoping	Just-in-time, purpose-based access; auto-expiring, zero standing access
Quarterly compliance fire drills and manual evidence gathering	Every prompt, tool call & decision traced live and replayable
Fragmented policies across siloed tools that drift over time	One policy authored in natural language, enforced natively across 50+ platforms
AI initiatives stalled waiting on governance sign-off	10× faster path from POC to production
Wrong actions discovered in post-mortems or audits	One-click audit packs that are always current, never rebuilt from scratch

COMPLIANCE

Ship Into Any Regulated Environment

Pre-built policy packs. One-click evidence generation. Continuously updated as standards evolve. No rebuild required as your stack or requirements change.

GDPR · HIPAA · SOX · NIST AI RMF · EU AI Act · CCPA · PCI-DSS

*"By 2027, **60% of firms may fail to realize AI value** due to poor governance."*

GARTNER · 2025

Trust3 AI

Funded by:
Point72 Ventures, Sapphire Ventures
Insight Partners, Battery, Accel

See it in your environment.

30-minute live demo.
Bring your stack, and we show you how the Trust Layer governs every agent through it.

demo@trust3.ai

trust3.ai

Request a Demo →