

Secure Agent & Data Access Across the Microsoft Platform

One security control plane from AI agents to the data they reach across Fabric, OneLake, and beyond. Discover, observe, and secure the agent lifecycle, by the creators of Apache Ranger.

THE PROBLEM

Agents Are Outpacing Enforcement Across the Microsoft Estate

Gartner projects that by 2029, over 50% of successful attacks on AI agents will exploit access control weaknesses. As Fabric and OneLake widen access to enterprise data, authorization must travel with it.

Shadow AI

Agents spin up in Copilot Studio, Azure AI Foundry, & Microsoft 365 without being registered. So enterprises undercount them by 3 to 10X.

Overprivileged Access at Platform Boundaries

Permissions don't follow data across platforms. Users end up overprivileged when Fabric queries data governed elsewhere via OneLake shortcuts.

No Comprehensive Observability

Untraced agent actions across Fabric, Power BI, and Azure AI Foundry make it difficult to audit or assign accountability. Token spend runs unchecked.

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

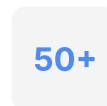
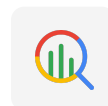


SaaS Apps

SharePoint, Salesforce, ServiceNow

Data Security

PBAC and FGAC



AI-native metadata travels with every request

Agent identity

Declared purpose

Live policy state

Numbers from Production



Governance Intelligence Agent

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



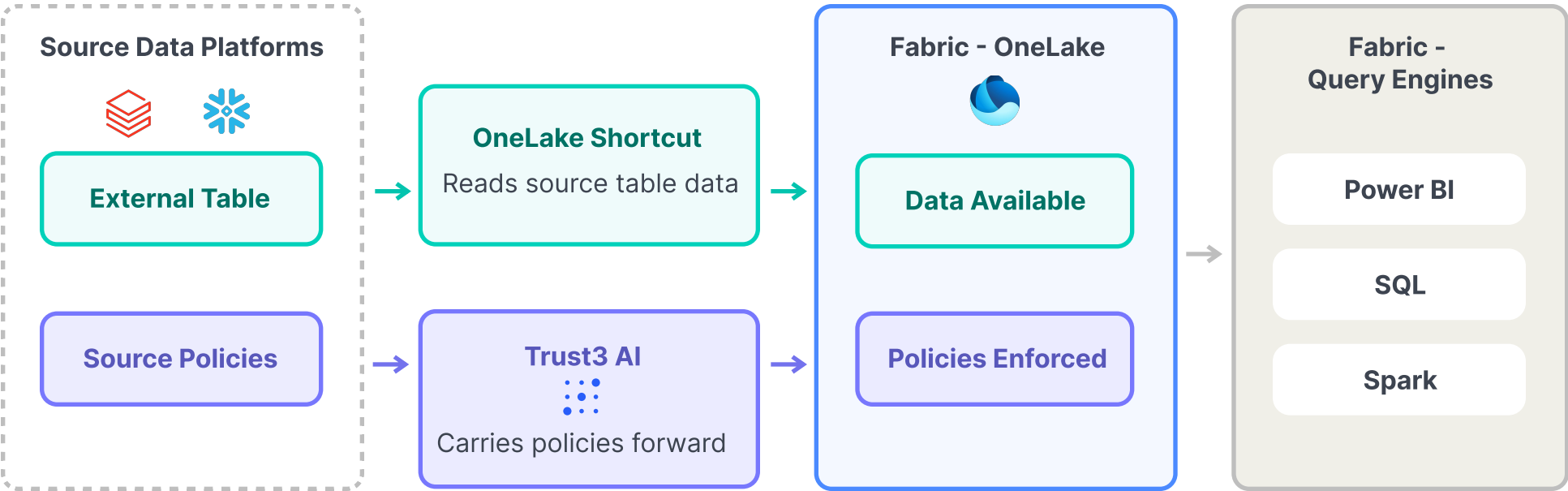
ASK GIA · GOVERNANCE INTELLIGENCE AGENT

Define & enforce access policies in plain English

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

Sync External Policies Into Fabric - OneLake

Source policies don't follow the OneLake shortcut.
Trust3 AI translates them into OneLake security roles so Fabric users get the same access decision.



Agent Security

- **Discover:** every agent, including shadow AI, across Azure AI Foundry, Copilot Studio, Microsoft 365, and 50+ platforms
- **Observe:** end-to-end traces of every agent step, input to output, with deviations scored as they happen
- **Secure:** purpose-based access, MCP and A2A tool control, runtime guardrails and a kill switch on agent actions

Data Security

- **Discover & classify:** sensitive data across ADLS, Synapse, OneLake, Power BI, and beyond
- **Control access:** row, column and tag-based policy; attribute- and purpose-based, replacing over-privileged roles
- **Protect & monitor:** encryption, tokenization, usage lineage and continuous audit evidence

FEATURED INTEGRATION

Secured Access to Any Data Source from OneLake

OneLake shortcuts let Fabric read Databricks and Snowflake data in place without a copy pipeline. Trust3 AI syncs the policies from those sources into Fabric, so access control stays consistent.



CIO - FORTUNE 50 ENTERPRISE

"We operate across multiple clouds and data platforms, and governance complexity was slowing us down. Trust3 AI gives us one trust layer across our data and AI systems."

Enterprise Customers' Stories

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.

COMPLIANCE

Pre-Built Compliance 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

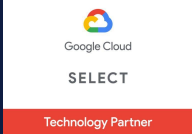
"By 2027, 60% of firms may fail to realize AI value due to poor governance."

GARTNER · 2025









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 →

© 2026 Trust3 AI All rights reserved.