Unlock Trusted Agentic AI Faster on Databricks

Accelerate AI Innovation While Strengthening Governance, Security, and Compliance

Organizations are rapidly adopting Databricks Data Intelligence Platform to build intelligent assistants, autonomous agents, AI-powered applications, and next-generation analytics experiences. As these AI systems become more capable, organizations are looking for ways to empower AI agents to access and use enterprise data while maintaining the governance, security, and compliance standards required by the business.

TrustLogix helps organizations accelerate the journey from AI pilot to production by embedding governance, authorization, and security directly into AI agents and applications. Leveraging Databricks Unity Catalog as a centralized source of governance and access policies, TrustLogix extends policy enforcement to AI agents and applications, ensuring secure and compliant access to enterprise data and services. Instead of slowing deployments with manual reviews, policy exceptions, and fragmented controls, organizations can confidently deploy AI agents knowing enterprise policies are enforced automatically and consistently.

Together, Databricks and TrustLogix help enterprises accelerate AI adoption while ensuring that data remains protected, policies remain enforced, and AI activity remains accountable.

Operationalize Unity Catalog Governance for AI Agents

Databricks Unity Catalog provides a centralized foundation for governing data, AI assets, and access policies across the enterprise. As organizations adopt AI agents, however, governance must extend beyond asset-level permissions to the real-time decisions agents make as they retrieve data, invoke tools, interact with applications, and take actions on behalf of users.

TrustLogix complements Unity Catalog by enforcing authorization, security, and governance policies at the point of agent execution. This enables organizations to apply consistent enterprise controls across AI agents, tools, APIs, and business workflows without introducing manual reviews, policy exceptions, or operational bottlenecks.

By embedding policy enforcement directly into agent interactions, TrustLogix helps organizations accelerate AI deployment while ensuring agents operate securely, compliantly, and in alignment with enterprise governance requirements from day one.

Context-Aware Authorization
Make access decisions using business context, user context, data sensitivity, and AI context. TrustLogix evaluates who is requesting access, which agent is acting, what data is involved, and how that data will be used before access is granted.This intent-driven approach enables organizations to deploy AI agents with confidence, ensuring every action is authorized according to enterprise policies while minimizing over-privileged access and operational risk.

Purpose-Based Access Controls
Enable policies that reflect how data is being used, not simply whether access exists. Organizations can safely support AI use cases such as summarization, analytics, customer support, software development, and business automation while maintaining appropriate controls around sensitive information.

Trusted AI Operations
Establish accountability for AI-driven actions through comprehensive visibility into user activity, agent activity, policy decisions, and data access patterns. This enables organizations to scale AI initiatives with confidence while maintaining trust across business, security, and compliance teams.

Turn Security and Governance into an **AI Accelerator** with TrustLogix

Faster Production Deployment
Organizations often discover governance and security concerns late in the AI development lifecycle, resulting in delays, rework, and extended approval cycles. TrustLogix enables governance-by-design by embedding enterprise policies directly into AI workflows from the start. Development teams move faster, security teams gain confidence, and organizations deploy AI agents into production more quickly.

Eliminate Governance Bottlenecks
Reduce the friction between AI innovation and enterprise security requirements.By automating policy enforcement and authorization decisions, TrustLogix minimizes manual reviews and policy exceptions that frequently slow AI initiatives.

Secure Data Access at Scale
Apply consistent governance policies across users, applications, agents, service principals, and automated workflows. As AI adoption expands, organizations can confidently scale access without increasing governance complexity.

Strengthen Compliance Posture
Support regulatory requirements and internal governance standards through centralized policy management, continuous monitoring, and comprehensive auditability.

Reduce Operational Complexity
Simplify policy management through centralized governance that adapts as business requirements, organizational structures, and AI deployments evolve.

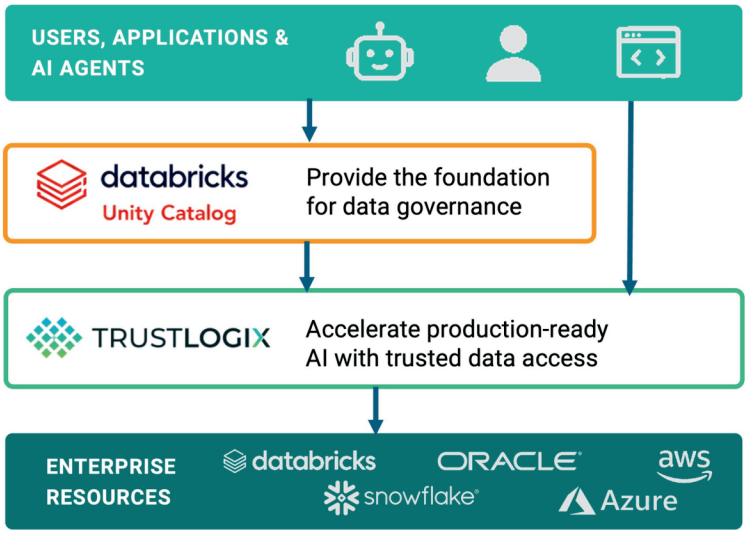
Key Capabilities

- **Intent-based Access Controls** Enforce based on purpose, not solely on roles or entitlement
- **Agent-to-Data Policy Decisions** Evaluate users, agents, data, action and business context
- **Cross-platform Policy Consistency** Extend beyond Databricks to Snowflake, SaaS, APIs, enterprise apps and MCP tools
- **Decision Logs** Capture details on why an agent action was allowed, denied, masked, or escalated using Guardian agent
- **Complement Unity Catalog with Runtime Policy Intelligence** Use Unity Catalog governance as the source of truth while enforcing business policies in real time.

From AI Pilots to **Enterprise AI**

Building AI agents is easy. The challenge lies with governing what they can access, what action they can take, and how they operate within enterprise policies.Databricks provides a powerful foundation for building and deploying AI applications and agents, with Unity Catalog delivering centralized governance for data and AI assets. As agents become more autonomous, however, organizations need real-time authorization and business-policy enforcement that extends beyond static permissions and asset-level controls.

TrustLogix complements Databricks by applying runtime, intent-aware authorization to agent interactions, ensuring every data access request, tool invocation, and business action is evaluated against enterprise policies. By combining Databricks governance context with dynamic policy decisioning, organizations can accelerate AI adoption, protect sensitive data, simplify compliance, and confidently scale agentic AI across the enterprise.



TrustLogix + Databricks
Build Faster. Deploy Sooner. Govern Everywhere.