

Secure enterprise agentic AI at scale

Thales AI Security Fabric for Google Cloud

Executive summary

Thales and Google Cloud are expanding their collaboration to help enterprises securely adopt agentic AI at scale. By integrating Thales AI Security Fabric with the Gemini Enterprise Agent Platform, the joint solution provides a unified runtime security control plane that enables organizations to securely govern AI-driven workflows across Google Cloud environments.

As enterprises move from AI assistants to autonomous AI agents that can reason, access enterprise data, invoke tools, collaborate with other agents, and execute multi-step workflows, they face new security, governance, and compliance challenges that traditional security controls were not designed to address. The joint solution provides runtime visibility, policy enforcement, risk assessment, and centralized governance across the agentic AI lifecycle.

The solution helps organizations mitigate AI-specific threats such as prompt injection, sensitive data leakage, unsafe outputs, unauthorized actions, excessive agent privileges, and unintended autonomous actions. It also provides semantic guardrails, dynamic intent-based access control, data classification and redaction, agent identity and trust assessment, AI asset discovery, immutable audit trails, and centralized policy management to support regulatory compliance and enterprise governance.

Together, Thales and Google Cloud provide enterprises with a trusted foundation to accelerate agentic AI innovation while maintaining security, compliance, and control, helping customers confidently deploy AI agents across sensitive business systems and critical workflows.

Company overview

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale, with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.



Product highlights

Functionality provided by the joint solution

- Integrates Thales AI Security Fabric with the Gemini Enterprise Agent Platform to secure AI agents and agentic workflows running on Google Cloud.
- Provides runtime security policy enforcement across prompts, model interactions, and MCP communications, with an architecture designed to extend to agent-to-API and agent-to-agent interactions as those capabilities are introduced.
- Delivers a unified security control plane for AI applications, enabling centralized policy management, governance, and runtime enforcement.
- Protects against AI-specific threats such as prompt injection, sensitive data leakage, unsafe outputs, unauthorized tool usage, and excessive agent privileges.
- Enables semantic guardrails, dynamic intent-based access control, data classification, redaction, agent identity, trust assessment, and attestation.
- Provides runtime audit trails, AI asset discovery, and visibility into agent activity across cloud environments.

Customer benefits

- Enables organizations to adopt agentic AI on Google Cloud with stronger security, governance, and operational trust.
- Reduces business risk by enforcing policies as AI agents access sensitive data, invoke tools, and execute autonomous workflows.
- Strengthens compliance by aligning agent behavior with business policies and regulatory requirements through centralized governance and auditability.
- Provides end-to-end visibility into AI interactions, agent behavior, and runtime decisions for improved monitoring and risk management.
- Accelerates secure AI innovation by giving customers integrated controls to deploy autonomous agents at scale.

Product architecture

The Thales AI Security Fabric integrates with the Gemini Enterprise Agent Platform to provide a centralized runtime security and governance layer for enterprise AI. User requests are authenticated through enterprise identity services before being processed by AI agents. AISF provides agent and asset discovery, policy management, runtime enforcement, and auditability while governing interactions between AI agents, large language models (LLMs), and Model Context Protocol (MCP)-connected services. Security policies are evaluated in real time to enforce semantic guardrails, data protection, and intent-based access controls. The platform also provides centralized visibility and compliance reporting, enabling organizations to securely deploy and govern agentic AI workloads at enterprise scale.

Use cases

Secure enterprise AI adoption at scale

Enable organizations to securely deploy autonomous AI agents on Google Cloud as they transition from AI experimentation to production. The joint solution provides runtime visibility into agent behavior, continuous risk assessment, centralized governance, policy enforcement, and compliance monitoring across AI-driven workflows. This allows enterprises to confidently scale AI in high-value business functions such as finance, human resources, operations, and customer service while maintaining security, auditability, and regulatory compliance.

Govern AI-driven enterprise workflows

Apply centralized governance and runtime policy enforcement across AI workflows that connect users, AI agents, models, enterprise applications, MCP servers, and business systems, with the ability to evolve alongside future multi-agent architectures. The solution protects sensitive data, enforces business policies, and generates comprehensive audit trails while AI agents access enterprise resources and perform autonomous actions. This helps organizations reduce operational and compliance risk, maintain visibility across complex workflows, and securely integrate AI into critical business processes.

Learn more about [Google Cloud and Thales Group](#).