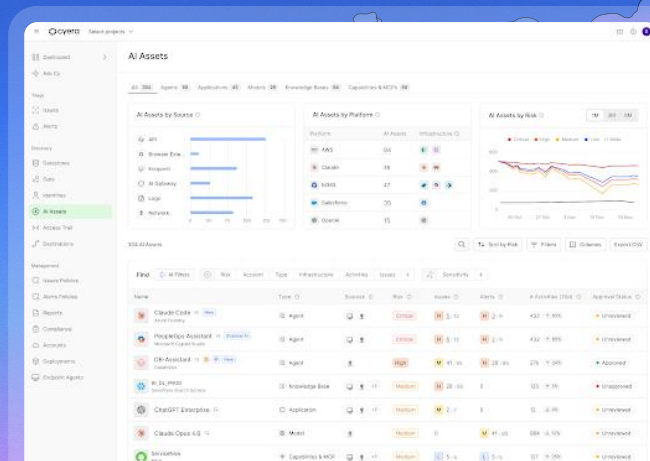


Secure the Agentic Enterprise with an AI Gateway



The Agentic Security Paradigm

Deploying an autonomous agentic workforce introduces complex security challenges across enterprise operations. Security teams must authorize agentic initiatives while managing risks tied to over-privileged machine identities and non-deterministic execution paths.

Autonomous agents inherit broad human credentials and related permissions that enable them to access a vast amount of confidential records at machine speed. Non-deterministic reasoning can cause agents to drift from business intent, executing rogue actions or unapproved system commands. Unlike traditional logging, which captures only the initial prompt and final output, the AI Gateway captures every intermediate reasoning step and tool call in between, the part of the transaction where data exposure actually happens.

Cyera Agent Guardian Security Controls

Achieving complete protection across enterprise environments requires flexible control methodologies. Cyera works with organizations to build the right mix of control points that align directly with their specific network topologies, latency constraints, operational preferences, and their stage on the agentic adoption journey.

The Cyera platform secures the agentic ecosystem across every environment where agents live and act, with comprehensive coverage spanning an AI Gateway plugin, endpoint agents, browser extensions, cloud platform APIs, log analysis, and native agent hooks. Grounded in deep data and identity understanding and context, these flexible sensors feed telemetry to Cyera's central policy engine. Within this multi-layer strategy, the inline AI Gateway plugin serves as one of the primary enforcement points for centralized agentic security and governance.

The Cyera AI Gateway Plugin Architecture

The Cyera AI Gateway operates as a lightweight, guardrail plugin that integrates directly with existing LLM gateways in your organization, such as LiteLLM, Kong, Apigee, and others. Native support for all LLM API formats ensures compatibility with any gateway you already use. Security teams can install the plugin directly into their active routing pipelines. This avoids the operational complexity of hosting new infrastructure or editing individual agent settings.

The plugin intercepts bi-directional transactions at the network perimeter. As agents transmit requests to backend models, the plugin decodes the raw payload in transit. This payload includes prompt histories, system context, and proposed tool calls. The plugin forwards these elements to the Cyera platform's central policy engine. This engine evaluates the transaction against active policies and returns an immediate determination. The experience of real-time collaborative applications remains unaffected.

Core Operational Capabilities

The plugin architecture dynamically orchestrates security policies in the data flow path. This delivers continuous governance through four main capabilities:

Real-Time Prompt Analysis

The integration inspects the textual content of user prompts to detect malicious instructions and jailbreaks before they reach the model.

Granular Tool Control

The integration evaluates proposed agentic tool calls to allow safe operations like read-only queries, while blocking unsafe behaviors like excessive data deletions.

Identity Context Mapping

The integration correlates active agent sessions with organizational directory services to enforce precise, role-based authorization.

The Data and Identity Context Advantage

The primary differentiator of the Cyera AI Gateway is its integration with the core data classification and identity mapping engines of the Cyera platform. Point solutions inspect conversational text in isolation, failing to determine whether a transaction involves benign public information or highly restricted intellectual property.

Cyera Agent Guardian provides the critical backend intelligence required for accurate gateway enforcement. Knowing the exact sensitivity of data accessed by an agent and the exact permissions of the acting identity allows the Cyera platform to apply context-aware rules. The Cyera platform can permit an agent to query public documentation while limiting that same agent if a query targets restricted source code. This deep data and identity understanding and context eliminates false positives and establishes a predictable, audit-ready agentic posture.

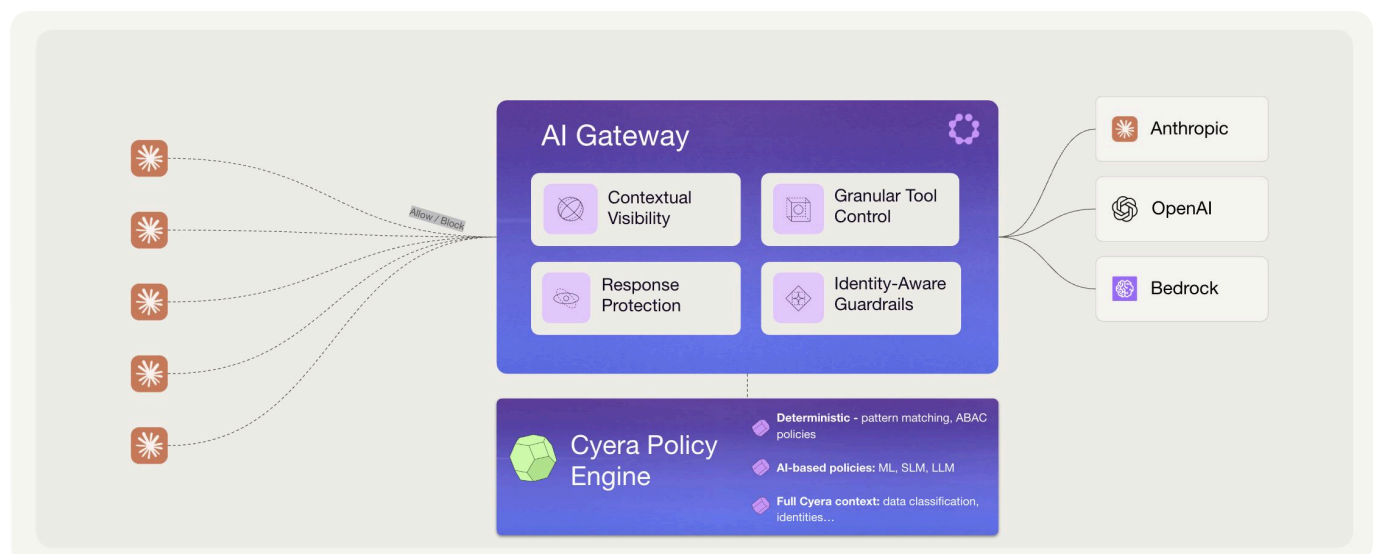


Image 1: An Illustration of Cyera AI Gateway deployment

Deployment and Lifecycle Onboarding

The rollout of the Cyera AI Gateway plugin follows a structured progression across four operational pillars to ensure stability:

Unify data and identity intelligence

Discover

Catalogs all agents routed through the AI gateway, populates the AI asset registry with agents and MCPs, maps posture, and visualizes relationships between identities and databases.

Govern

Evaluates configurations against policies to identify overprivileged machine identities, tuning governance rules without operational disruption across active enterprise routing pipelines.

Protect

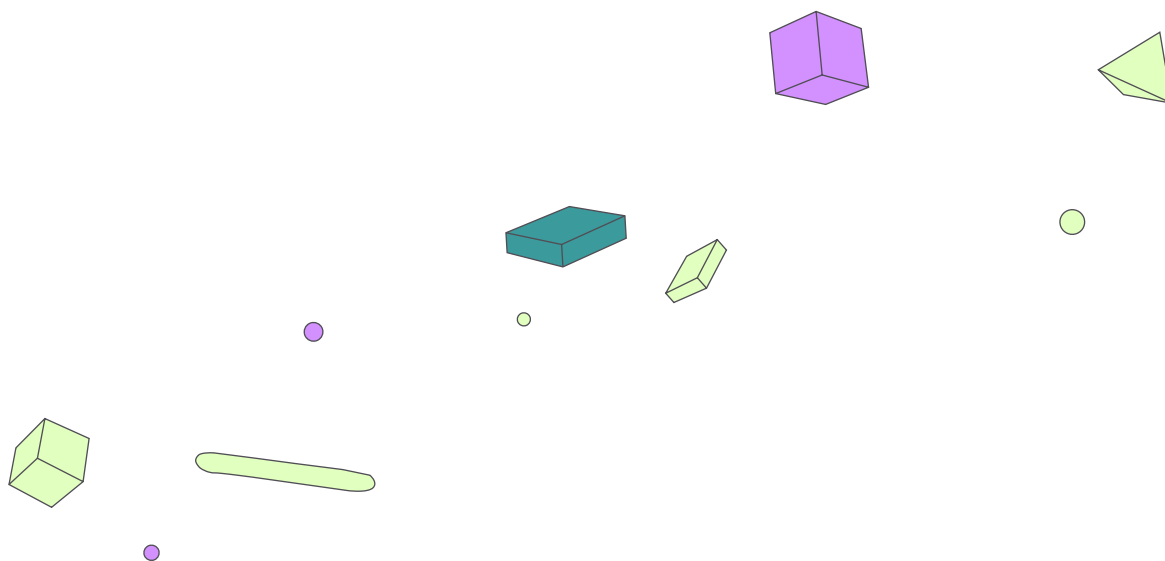
Deploys dynamic runtime controls such as data security, prompt-injection defense, and sensitive-data redaction to intercept risky agentic actions, alert on policy violations, and block unauthorized traffic.

Validate

Conducts continuous adversarial testing and automated red teaming to verify security controls remain effective against emerging prompt injections and complex jailbreak attempts.

Summary

Cyera Agent Guardian, through the AI Gateway, delivers continuous runtime governance and execution defense across the modern enterprise agentic landscape. By unifying flexible control-point deployments with the deep data and identity context of the Cyera platform, security teams can eliminate visibility blind spots, prevent destructive agentic tool calls, and maintain continuous compliance. That is the trade-off Agent Guardian removes: security teams can say yes to agentic adoption without losing sight of what those agents are actually doing underneath the hood.



Explore how the AI Gateway plugin fits into your existing routing pipeline without adding new infrastructure.

Book a demo

