Service Overview

AI Security & Governance

Confidently embrace AI and Agentic AI with security and governance that protect data, enforce policy, and stop emerging threats.

TENEO
OPENING MINDS

Making the case

AI is no longer emerging; it is already reshaping how organizations work, from developers Vibe Coding to employees relying on AI-driven assistants for research, analysis, and decision-making. But while AI unlocks new opportunities for productivity and innovation, it also introduces risks that traditional security tools were never built to handle. Sensitive data can leak into, or worse out of, generative AI tools, Shadow AI use grows outside IT's control, and attackers exploit vulnerabilities unique to AI, such as prompt injection or model manipulation.

Without the right governance in place, organizations face exposure, compliance challenges, and reputational damage. What's needed is a way to balance innovation with protection, enabling safe adoption of AI without slowing progress and achieving its value.

AI Security & Governance gives IT teams the visibility and control they need to confidently embrace AI. It oversees both sanctioned and unsanctioned use, highlights shadow AI, and assigns risk scores to AI tools so IT can decide what to permit or block. It enforces Zero Trust principles across users, devices, and workloads, and extends protection into runtime environments to defend models, plugins, protocols, and agents from threats traditional security misses.

AI Security & Governance is a core part of StreamlineX, our framework for building networks that are secure, optimized, observable, and AI-ready.

Our approach

We take a consultancy-first approach to AI Security & Governance, ensuring every solution is tailored, outcome-driven, and aligned to your organization's goals.

1. Initial Assessment and Requirements Gathering

We start by working with you to understand how AI is being used across your environment.This includes mapping sanctioned and shadow AI usage, assessing data risks, and capturing compliance and governance requirements in a clear Solutions Requirements Document (SRD).

2. Design and Architecture Planning

Together, we design an architecture that applies Zero Trust principles to AI access and workloads. The design covers visibility, policy enforcement, and runtime protection, supporting both human and non-human identities such as AI models, plugins, and agents.

3. Pilot Deployment or Proof of Concept (PoC)

We validate the design in a controlled environment, testing data protection, access policies, and runtime defenses against real-world AI threats such as prompt injection and model misuse.

4. Policy Development and Fine-Tuning

Using insights from the pilot, we develop and refine policies that govern AI access, data sharing, and workload behavior. Rules are fine-tuned with stakeholder feedback, compliance needs, and evolving threat intelligence.

5. Implementation and Rollout

Once proven, we manage the deployment across your environment. Our engineers ensure a smooth rollout, supported by training and knowledge transfer so your IT teams can confidently govern and secure AI.

6. Continuous Monitoring and Optimization

We provide ongoing monitoring and analytics to track AI usage, risks, and runtime activity. Regular reviews ensure defenses adapt to evolving threats, shadow AI behaviors, and new compliance requirements, keeping your AI environment resilient by design.

Key benefits

- Visibility into sanctioned and shadow AI use
- Risk scoring for AI activity to prioritize response
- Zero Trust applied to AI access and workloads
- Protection against data leakage, prompt injection, and model misuse
- Runtime security for AI models, plugins, protocols, and agents
- Continuous monitoring of AI activity and risk
- Simplified governance and compliance reporting
- Support for both human and non-human identities
- Resilient AI adoption without slowing innovation

StreamlineX

AI Security & Governance is a cornerstone of StreamlineX, our framework for building networks that are secure, optimized, observable, and AI-ready. By extending visibility and control into AI use and workloads, it ensures consistent Zero Trust protection, safeguards against new AI threats, and supports responsible innovation. StreamlineX makes it easier for IT teams to see clearly, secure confidently, and design boldly, delivering resilient networks that are ready for whatever comes next.

Find out more about StreamlineX **here**.

Next steps

To get started with Teneo's AI Security & Governance solution, contact us to schedule a discussion today at **info@teneo.net.**

Purpose Beyond Profit

In working with Teneo, you are helping to improve the lives of a million children around the world. **Learn more**

About Teneo

Most Network and Security teams are overworked so making progress is a challenge. We securely connect users to their applications by combining leading technology with expert guidance. You stay in control, simplify your operations and keep ahead of the game.

Find out more at www.teneo.net.

UK
Teneo Ltd
20/21 Theale Lakes
Business Park
Moulden Way, Sulhamstead
RG7 4GB

T: +44 118 983 8600
F: +44 118 983 8633

France
Teneo France S.A.S.
43 47, Avenue de la Grande
Armée 75116
Paris
France

T: +33 1 55 51 30 38

USA
Teneo Inc.
44679 Endicott Drive,
Suite #355,
Ashburn,
VA 20147

T: +1 703 212 3220
F: +1 703 996 1118

Australia
Teneo Australia Pty Ltd
Level 11, 64 York Street
Sydney
NSW 2000

T: +61 2 8038 5021
F: +61 2 9012 0683