AI Security & Governance

Confidently adopt AI and Agentic AI with the visibility, governance, and security controls needed to protect data, enforce policy, and reduce risk

TENEO
OPENING MINDS

What Is AI Security & Governance?

AI Security & Governance helps organizations adopt Artificial Intelligence safely by providing the visibility, governance, and security controls needed to manage AI use across the business.

It enables organizations to understand where AI is being used, what data is being shared, and whether activity aligns with security policies and compliance requirements.

Why Does It Matter?

As employees, developers, and business teams increasingly use AI and Agentic AI tools, traditional security approaches are struggling to keep pace.

Traditional security tools weren't designed to provide visibility into AI use or enforce governance across AI-powered applications and services. Without the right visibility and control, Shadow AI can emerge, sensitive information can be exposed, and new risks can go undetected.

Common digital employee experience challenges include:

Limited Visibility into AI Usage

Most organizations don't know which AI tools are being used, who is using them, or what data is being shared. This challenge is often compounded when sanctioned apps add AI copilots and other AI capabilities.

Shadow AI

Employees can adopt AI tools without IT approval, creating unmanaged risk and increasing the potential for sensitive data exposure.

Sensitive Data at Risk

Confidential business information, intellectual property, and customer data can be unintentionally shared with AI applications.

Policy Without Enforcement

Many organizations have AI policies but lack the controls needed to consistently monitor, govern, and enforce them.

Emerging AI Threats

AI-powered applications, models, agents, and plugins introduce new attack surfaces. AI is built on open standards, which is great for rapid innovation but can make it easier for attackers to identify and exploit vulnerabilities.

Unclear AI Risk

Without visibility and governance, IT teams cannot assess AI risk or support adoption confidently. Rapidly emerging AI applications compound the challenge, leaving security teams struggling to keep pace.

How Teneo Helps

AI Security & Governance helps organizations gain visibility into AI usage, manage risk, and turn AI policies into enforceable controls so they can confidently adopt AI.

With Teneo's AI Security & Governance solution, organizations can:

Gain visibility into sanctioned and unsanctioned AI usage across the organization

Discover shadow AI, understand how AI tools are being used, and enable the safe use of approved AI applications.

Reduce the risk of sensitive data exposure through AI applications

Turn AI policies into enforceable governance controls

Assess and manage AI-related risks with greater confidence

Extend Zero Trust principles across users, devices, applications, AI Agents, AI workloads and Agentic AI

Secure AI-powered applications, models, agents, APIs, and supporting services from emerging threats

This is how organizations move from reactive AI governance to confident, secure AI adoption.

A Layered Approach to AI Security & Governance

Effective AI Security & Governance requires visibility into AI usage, governance over how AI is adopted, and protection against emerging risks. From employee use of AI tools to AI-powered applications and agentic workflows, organizations need controls that enable innovation while maintaining security and compliance.

Teneo's AI Security & Governance solution provides protection across four key areas:

AI Visibility & Discovery

Gain visibility into sanctioned and unsanctioned AI tools and usage across your organization. Discover shadow AI, understand usage patterns, assess risk, and make informed decisions about which AI applications should be permitted, restricted, or blocked.

From AI Policy to Enforceable Controls

Many organizations have AI policies but lack the ability to enforce them consistently. Transform governance frameworks and acceptable use policies into practical controls that can be monitored, measured, and enforced across the organization.

AI Data Protection

Protect confidential, regulated, and customer data from inappropriate exposure and data leakage through AI tools and applications. Apply controls that help ensure sensitive information remains protected wherever AI is used.

AI Application & Runtime Protection

Protect AI-powered applications, models, agents, APIs, plugins, protocols, and supporting services from emerging threats, misuse, and vulnerabilities. Extend security into runtime environments to identify and stop risks across AI and Agentic AI workloads that traditional security controls may miss.

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.

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).

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.

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.

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.

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.

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.

Ready to Secure and Govern AI with Confidence?

Secure AI adoption starts with effective AI Security and AI Governance. Whether you're looking to gain visibility into AI usage, reduce shadow AI risk, protect sensitive data, or translate AI policies into enforceable security controls, Teneo can help you adopt AI with confidence.

Book a Free AI Policy Enforcement Review, where we will assess your current AI policy, security tooling, and governance approach to identify potential risks and assess how effectively your existing controls support real-world AI governance and policy enforcement. You'll receive clear, actionable recommendations to strengthen your ability to enable AI innovation securely.

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

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.
1 Rue Lamartine
75009 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