VisionX Governance

Govern every AI model, agent and employee prompt from one control plane.

VisionX Governance brings AI governance, compliance readiness and vendor risk together with an AI control plane, governed employee Workspace chat and Shadow AI Guard. Inventory models and agents, review risks, inspect prompts and responses, route approved models and assemble evidence packs. It prepares evidence and readiness; it does not certify your company.

Key modules

AI Governance & GRC

Inventory AI systems, manage the risk register and impact assessments, map frameworks and policies, collect evidence and export audit packs.

Third-party risk

Tier vendors, review security, privacy and AI questionnaires, and track findings, documents, renewals and reassessments.

AI Shield / Control Plane

Inspect prompts and responses for DLP, secrets, PII, person names and business-confidential content classification.

Intent & insider risk

Review pseudonymized metadata-only risk indicators. Identity reveal requires a second administrator and human review.

Smart model routing

Route by cost, quality and latency with fallbacks, budgets and a simulator before policy rollout.

MCP & agent gateway

Control tool permissions, schema locking, approvals and session replay. Self-hosted gateway v0.5.0 is available only in Private / Regulated.

VisionX Workspace

Give employees governed multi-model chat with company policies and approved AI models.

Shadow AI Guard

Browser extension 1.2.1 checks typed prompts and pastes, applies redaction, department/group rules and site risk tiers, and supports IT force-install.

Audit & integrations

Hash-chained audit log, SIEM export, SSO, API and webhooks with second-admin approved destinations.

Cloud AI discovery and Data stores & AI access

Read-only discovery and access with customer-owned credentials for S3, Azure Blob, Google Drive, SharePoint/OneDrive, Google Cloud Storage and PostgreSQL.

Top benefits

Govern AI adoption, protect sensitive employee AI use, review autonomous agents, prepare readiness evidence, assess vendors and control model cost.

AI inside

AI is bring-your-own-key. Your approved model runs the classifier, your provider bills AI usage directly, and raw prompts and responses are never stored. Sensitive decisions remain under human approval.

Security & compliance

Raw prompts and responses are never stored. Insider risk is pseudonymized and metadata-only; identity reveal needs a second administrator. SSO, hash-chained audit, SIEM export and second-admin approved destinations support human oversight. Regional requirements are reviewed during deployment. SOC 2 audit in progress. Readiness and evidence preparation only; no certification.

Browser and gateway support

Shadow AI Guard 1.2.1: Chrome, Edge, Brave, Opera and Vivaldi; Firefox edition coming. Typed-prompt and paste checks, redaction, department/group rules, site risk tiers and IT force-install. Self-hosted gateway v0.5.0 is Private / Regulated only.

MCP scope

Hosted MCP proxy: Business includes tool permissions, approvals and audit replay; Enterprise and Private / Regulated add schema locking. Stateless Streamable HTTP; initialize, ping, tools/list and tools/call. No stdio, persistent MCP sessions, older SSE, resources or prompts. Approval-held calls require resubmission with single-use approval.

Integrations

OpenAI / Azure OpenAI, Anthropic, Google Gemini, Amazon Bedrock, MCP servers, Okta / Microsoft Entra ID, Splunk, Sentinel and generic SIEM webhook. S3, Azure Blob, Google Drive, SharePoint / OneDrive, Google Cloud Storage and PostgreSQL use read-only access and customer-owned credentials.

Plans at a glance

Developer	Free	3 users; 2 agents; 25 AI systems; 10,000 policy-check calls / month; No GRC frameworks or vendors; 30-day retention. Community support
Business	from $12,000 / year	25 users; 10 agents; 200 AI systems; 2 GRC frameworks enabled at once; 50 vendors; 30-day retention; 10 gateway clients. Business-hours support
Enterprise	from $48,000 / year	250 users; 100 agents; Unlimited AI systems, frameworks and vendors; 365-day retention; 100 gateway clients. 24x5 support with a named contact
Private / Regulated	from $120,000 / year	Unlimited users, agents, systems, frameworks and vendors; 7-year (2,555-day) retention; Unlimited gateway clients and upstreams. 24x7 support with SLA and deployment assistance

Workspace add-on (governed AI chat), per user per month: Free level $0, Business level $15, Enterprise level $29. Included in the Enterprise and Private / Regulated editions.

Annual from-prices in USD. Prices exclude taxes; final pricing depends on deployment size. AI provider usage is billed separately.

Your first week

Connect identity and AI keys / register AI systems and import vendors / observe AI Shield / deploy Shadow AI Guard / enable routing and policies / export the first audit pack.

Who it is for

Healthcare, financial services, insurance, technology / SaaS, public sector and professional services.

Pilot with our team

Request an approval-based trial or a guided discussion: visionx.software/contact. Explore the read-only fictional US Northwind visitor demo without an account at visionx-governance.visionx.software.

Documentation

User Guide · Admin Guide · Gateway install guide · API reference

Sign in | User Guide | Admin Guide | Take the tour