ThreatLens

DATASHEET

ENTERPRISE AI GOVERNANCE & DATA LOSS PROTECTION

Govern every AI request — classify, protect, route, and record — before any model sees your data.

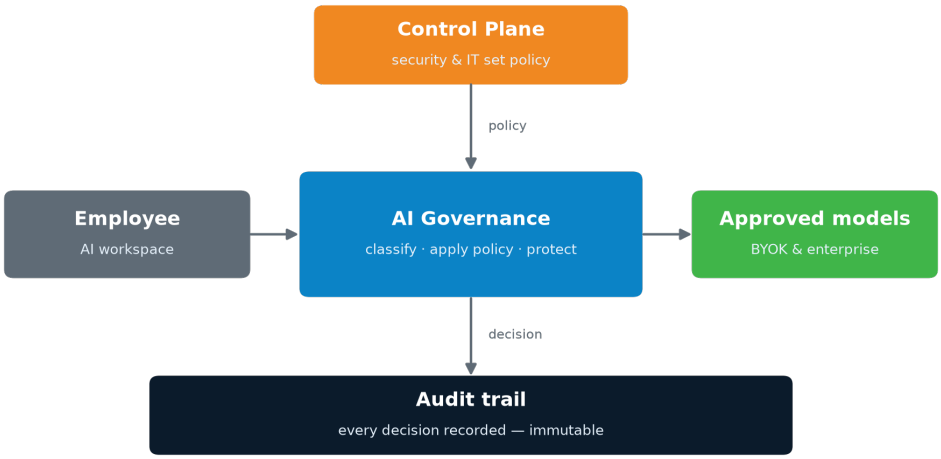
Your people are already using AI, and the productivity gains are real — but every prompt is a potential data-loss event. ThreatLens is the intelligence layer that sits in front of every AI request: it classifies the content, applies your policy, protects sensitive data, and records the decision — before any model sees it.

THREE FACES, ONE PLATFORM

AI Workspace	AI Governance	Control Plane
A familiar chat experience where employees use approved models, grounded in your own company knowledge.	The engine in the middle of every request: classify, apply policy, protect sensitive data — showing the decision before the answer appears.	Where security, compliance, and IT set the rules, connect their own models, manage identity, and review the audit trail.

ARCHITECTURE AT A GLANCE

Every request flows through the governance layer before it reaches an approved model. The Control Plane sets policy; every decision is recorded to the audit trail.



KEY CAPABILITIES

Capability	What it does
Content classification	10 data classes (PCI, PII, secrets, source code, financial, legal, HR, strategy, customer) via deterministic + semantic detection.
Policy matrix	Set, per data class, the minimum trust tier, the action, and the internet-access mode. One grid, owned by security.
Trust-tiered routing (BYOK)	Keep confidential work on your own approved models (Azure OpenAI, AWS Bedrock); never a public one.
Data loss protection	Inline redaction of sensitive spans, inbound and outbound; raw secrets and prompt-injection always blocked.
Governed retrieval	Answers grounded in your Microsoft 365 content, access-trimmed per user, fail-closed.
Immutable audit trail	Every decision recorded, hash-chained and tamper-evident; the system of record, streamable to your SIEM.
Monitor or enforce	Run observe-only first to measure exposure, then switch enforcement on with confidence.
Identity & access	RBAC (21 permissions, role-based), SSO/SAML (Entra, Okta, Google), group→role mapping.
Secrets vault	Provider and SIEM secrets, local or Azure Key Vault backed; every control-plane change audited.

ENFORCEMENT ACTIONS

Action	What happens
Allow	Send the request as-is.
Redact	Mask sensitive values, then send.
Route	Send only to a destination that meets the required trust tier — else block.
Warn	Warn the user, then proceed.
Approval	Hold for admin approval.
Block	Stop the request before any model sees it.

DEPLOYMENT & SECURITY

Deployment	SaaS (managed), private cloud, or fully self-hosted.
Your models	Bring your own models and keys — Azure OpenAI, AWS Bedrock.
Topology	Backend stays private behind a single, rate-limited front door.
Security	Fail-closed by design; tamper-evident audit; least-privilege RBAC; SSO; secrets vault.
Data handling	Content-safe logging — hashes and redacted excerpts, never raw sensitive payloads.
Built for	CISOs and security teams, platform / IT, compliance and risk.

See it live.

Request a demo at thethreatlens.com · Read the docs at docs.thethreatlens.com