Forcepoint

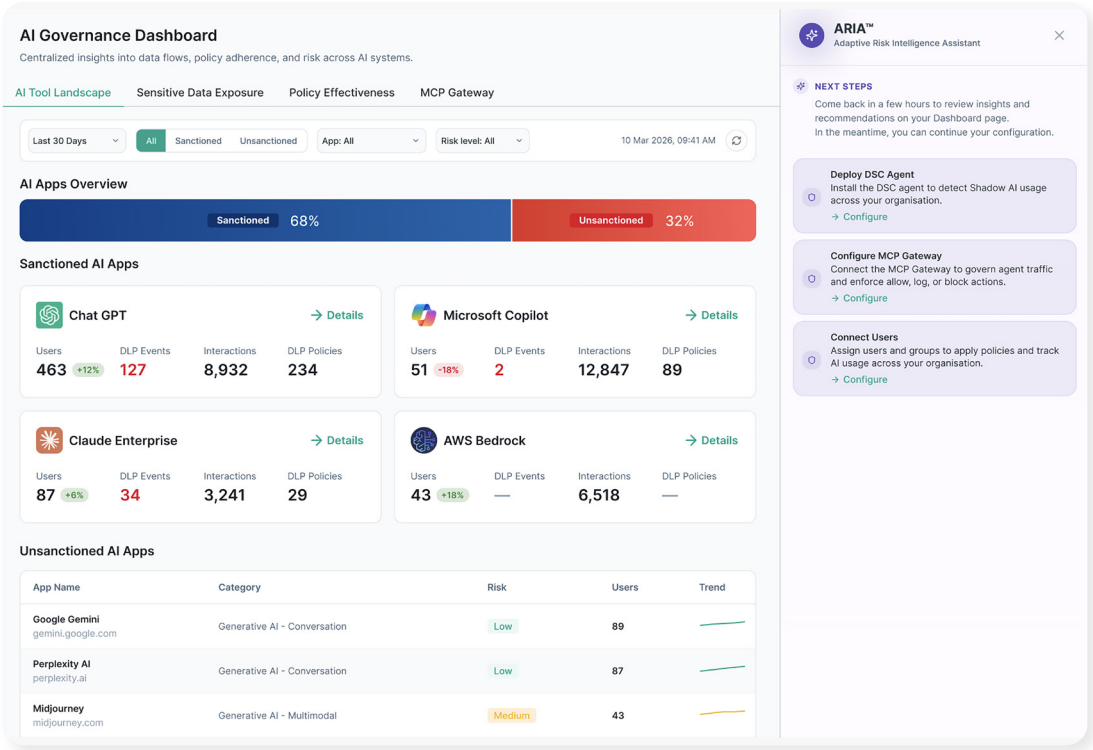
Forcepoint AI Security

AI Governance Dashboard

Unified visibility across every AI surface in your environment: sanctioned platforms, shadow applications and autonomous agents. ARIA monitors continuously, surfaces what matters and recommends the controls to act.

Three AI Risk Surfaces Active Now

- → **Users interacting with public LLMs and Copilots:** Every prompt is a potential data transfer. PII, source code and financial data move outside enterprise control instantly.
- → **Unapproved Shadow AI tools:** The average organization has 37 AI agents, most of them unknown to IT.
- → **Autonomous AI Agents and LLMs:** Agents inherit user permissions, then query, aggregate and transmit sensitive data at machine speed with no human in the loop.



The Solution

One Dashboard. Every AI Risk Surface. One Policy Framework.

The AI Governance Dashboard is the operational center of Forcepoint AI Security. Every connected AI platform backfills historical interaction data on first connection so security teams start with a populated view. ARIA, the Adaptive Risk Intelligence Assistant, monitors activity and provides observations and policy recommendations.

Capabilities

Capabilities Across Four Operational Views

AI Tool Landscape Connected enterprise AI platforms display per-tool DLP event counts, user totals and interaction volumes. Shadow AI tools appear ranked by risk level and user adoption with enforcement available immediately.

Sensitive Data Exposure Financial data, source code, credentials, PII and PHI are classified and surfaced by event volume and destination tool. A live feed attributes every recent violation to a specific user, application and data classification.

Policy Effectiveness Total hits, user impact and escalations are displayed alongside an action graduation path from audit-only observation through user coaching to hard block. ARIA flags misconfigured or zero-hit policies and recommends enforcement.

MCP Gateway Tool call volume, fields redacted, policy denies and pending approvals display alongside anomaly alerts that fire when agents query heightened data volumes, present unregistered credentials or exceed their approved scope.

Callouts

- → **Four operational views. Every AI surface in one place:** AI Tool Landscape, Sensitive Data Exposure, Policy Effectiveness, Spend Governance and AI Agent Gateway. One dashboard, no switching consoles.
- → **From login to governed in under 60 minutes:** ARIA guides administrators through platform connections and policy selection based on region, industry and data sensitivity. No professional services required.
- → **Zero reclassification. Day one coverage:** Existing Forcepoint DLP policies extend to every AI channel on connection. No new taxonomy, no policy rebuild and no disruption to sanctioned workflows.

Business Outcomes

- → **Reduce AI Data Risk:** Identify sensitive data exposure across sanctioned AI, shadow tools and autonomous agents. Every event is attributed to a specific identity, human or agent, for investigation and response.
- → **Accelerate Time to Governance:** Connect AI platforms and reach first insight in under 60 minutes with ARIA-guided setup and automatic historical backfill. Security teams operate from a populated dashboard on day one.
- → **Prove Responsible AI:** Export a closed-loop audit record of every AI interaction, policy decision and enforcement action. Regulatory report templates support EU AI Act, GDPR and NIST AI RMF requirements.

Request a Live Demo of the AI Governance Dashboard

[FP-AI Data Security AI Gov Dashboard-One Pager-EN] 31Jul2026