Forcepoint

Solution Brief

# Forcepoint AI Data Security

## Secure AI. Start with the Data.

### Challenge:

- Autonomous AI agents act without oversight, inheriting user permissions to query, aggregate and transmit sensitive data at machine speed with no human in the loop
- The average organization has 37 AI agents in use, most unknown to IT and spreading as fast as a browser extension
- Every prompt into a public LLM or Copilot is a potential data transfer, moving PII, source code and financial data outside enterprise control instantly

### Solutions:

- Govern autonomous agents at the point of action by enforcing least-privilege access and identity-aware controls so every action is attributed and controlled
- Discover and control shadow AI by continuously identifying unsanctioned tools and applying access policy before they become an unmanaged exposure
- Extend data protection to every prompt by applying existing classification and DLP policy to prompts, responses and file uploads across sanctioned AI platforms

### Outcomes:

- Adopt AI with confidence while maintaining consistent data protection
- Extend existing data security investments to AI without rebuilding policies
- Demonstrate responsible AI governance with clear, auditable evidence

AI has transformed the landscape of data security, opening new risk pathways that traditional security tools are unable to block. Employees share sensitive information through prompts instead of files. Shadow AI tools spread faster than IT can track. Autonomous agents query and transmit enterprise data with no human review. What this moment calls for is security that governs what AI can access before it reaches it.

### Govern Every AI Interaction from a Single Platform

Forcepoint AI Data Security extends the same protection already trusted for other channels to every AI interaction.
Apply your existing data protection policy automatically to AI prompts, agent responses and agent-to-application traffic with zero reclassification.

### See Sanctioned AI, Shadow AI and Agents on One Console

A unified console governs every AI surface: sanctioned platforms employees use every day, shadow AI tools that never went through review and autonomous agents acting on enterprise data outside human supervision. Nothing requires a separate tool or policy.

### Enforce Across Every AI Surface

Forcepoint AI Data Security acts on risk instead of only reporting it: remediating sensitive prompts and responses, revoking overshared access and holding high-risk agent actions for approval. One policy framework drives every response, so protection stays consistent no matter where the risk surfaces.

### Achieve Governed AI in Minutes, Not Months

Forcepoint ARIA, the embedded AI assistant, gets administrators from first login to a governed AI environment, with no professional services required. It recommends a starting policy configuration based on region, industry and data sensitivity, giving guidance in plain English.

### Get Proof of Governance for Regulators and Your Board

Every AI interaction and agent action is logged in a single, immutable audit trail, supporting EU AI Act, NIST AI RMF, GDPR, DORA, NIS2 and SEC requirements. Now you can demonstrate governance on demand instead of after the fact.

## How It Works: Know, Adapt, Protect

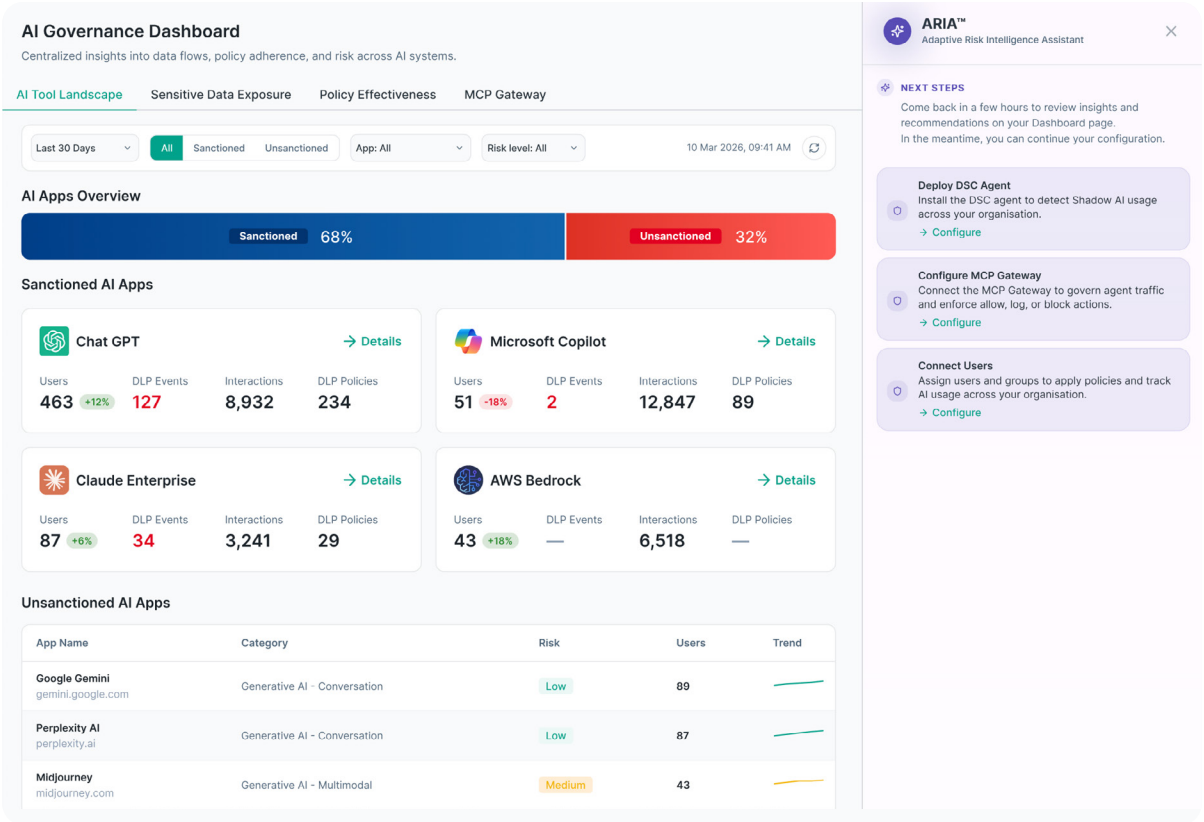
### Know

### Understand AI risk as it forms

Forcepoint AI Data Security provides a continuously updated view of the enterprise AI environment:

- → A centralized inventory of sanctioned AI platforms, shadow AI tools and AI agents
- → API-based visibility into enterprise AI services, including historical activity upon connection
- → Endpoint visibility to detect unapproved AI applications and locally executing agents
- → Upstream classification of sensitive data across structured and unstructured sources, making AI interactions data-aware from the outset
- → Full attribution of every AI interaction to the human user, AI agent or agent-user pair involved

Security teams gain a single operational view of where AI risk exists and who is responsible for it.



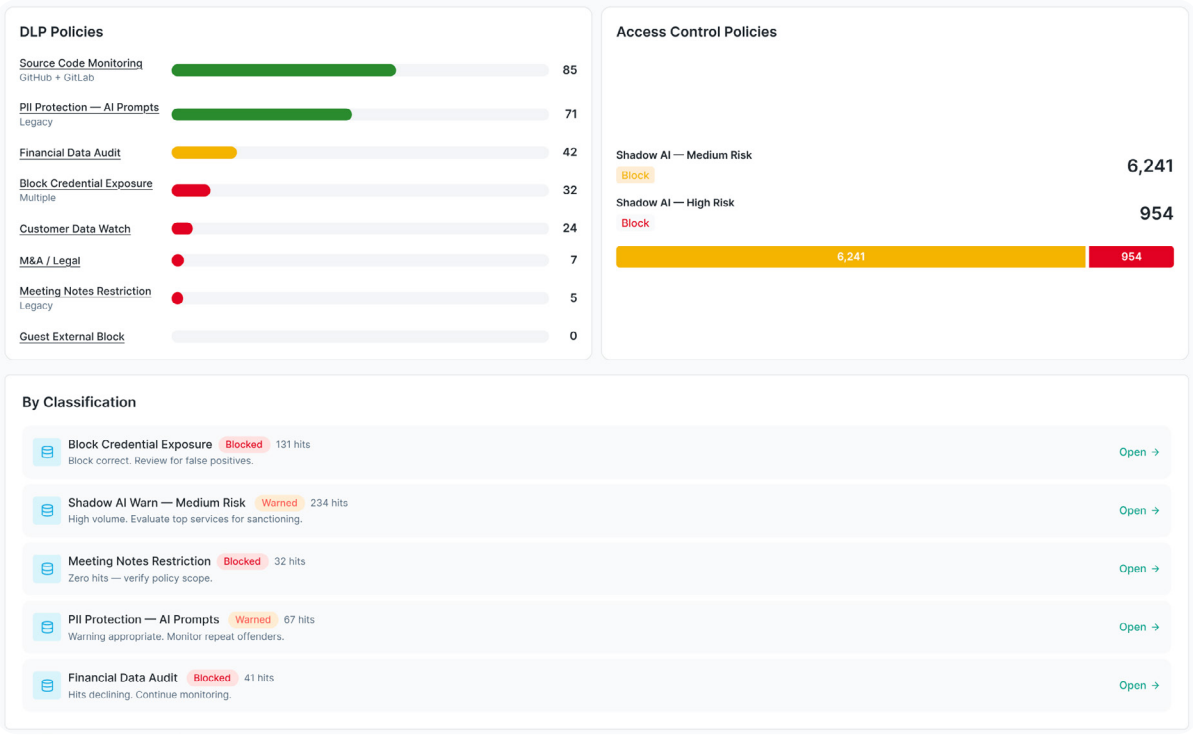
## Adapt

### Translate insight into action at the speed of AI

Visibility alone is not enough if enforcement cannot keep up. Forcepoint AI Data Security adapts protection automatically as AI usage evolves:

- → Existing data security policies extend to AI prompts, responses, file uploads and agent actions without policy rebuilds or reclassification
- → A single policy framework governs email, web, endpoint, SaaS and AI for consistent protection everywhere data flows
- → Forcepoint ARIA guides administrators from first login to a governed AI environment, with no professional services required
- → Remediation controls allow teams to coach users, restrict actions, require approval for agent execution or block high-risk activity
- → Autonomous agents are restricted to least privilege, stopping inherited-permission and prompt-injection overreach before it starts

This approach allows organizations to govern AI adoption without slowing productivity.



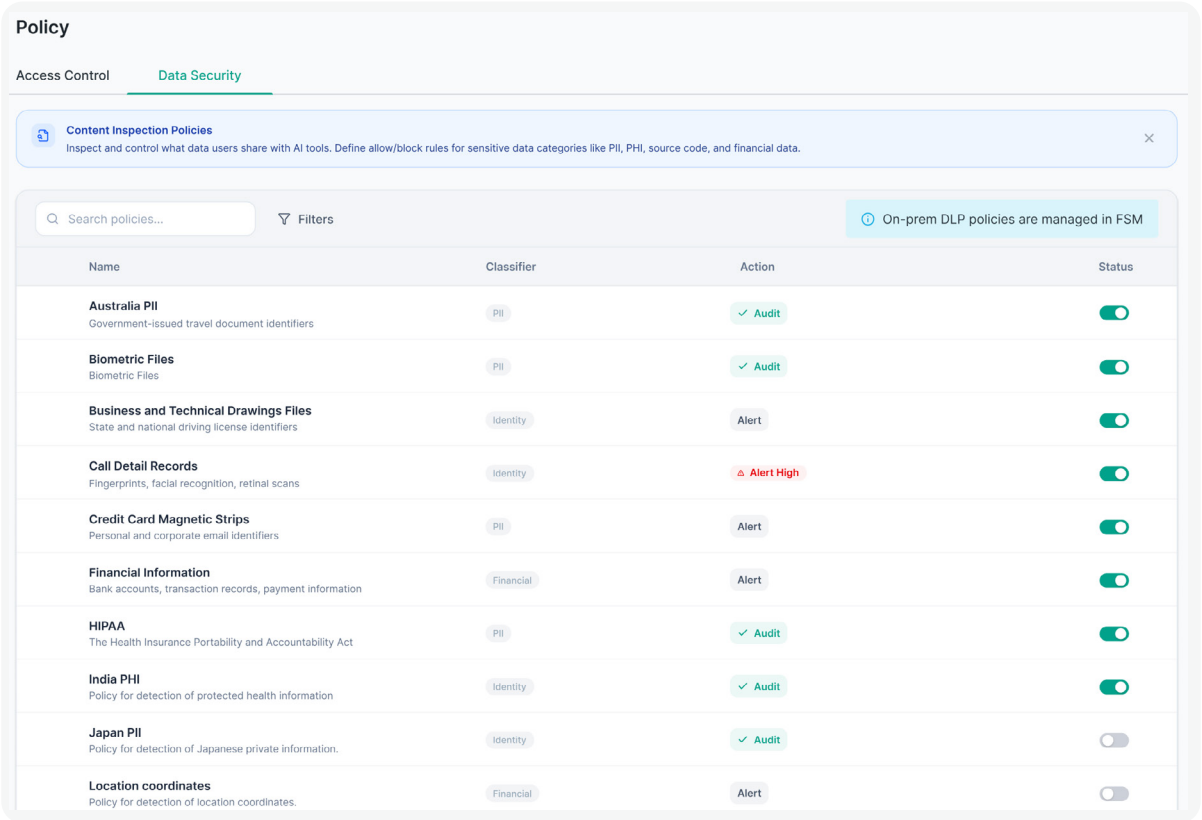
## Protect

### Enforce consistent protection wherever AI interacts with data

Forcepoint AI Data Security enforces protection at the point of interaction, not after exposure occurs:

- → API-based enforcement connects directly to sanctioned AI platforms to inspect prompts, responses and agent actions without requiring proxies, browser extensions or network changes
- → Endpoint enforcement extends protection to AI activity occurring locally on devices, including locally executing agents and browser-based AI tools
- → The AI Agent Gateway brokers credentials for autonomous agents calling business applications like Salesforce and Microsoft 365, inspecting every response at field level and holding high-risk actions for approval
- → Data access guardrails prevent AI assistants from exposing overshared or misclassified data by remediating access before exposure
- → Nearly 2,000 templates, policies and classifiers cover 80 or more regulatory regions out of the box, blocking risky pastes, uploads and shares without shutting employees down
- → Every enforcement action is logged with full identity attribution to create an auditable record

This delivers immediate, consistent protection across human-driven and autonomous AI activity.



## Key Capabilities

### Data Protection Across AI Interactions

Inspect AI prompts, responses and uploads using the same data classifications that already protect email, web and endpoint.

### Shadow AI Discovery and Control

Discover and manage unsanctioned AI tools from a single dashboard, with risk scoring and access control policies applied per application.

### Data Access Controls for Sanctioned AI

Identify and remediate overshared or misclassified data before AI assistants like Copilot can surface sensitive content.

### Custom AI Agent Monitoring and Governance

Capture detailed activity logs for AI agents, including who triggered them, what data they accessed and what actions they performed.

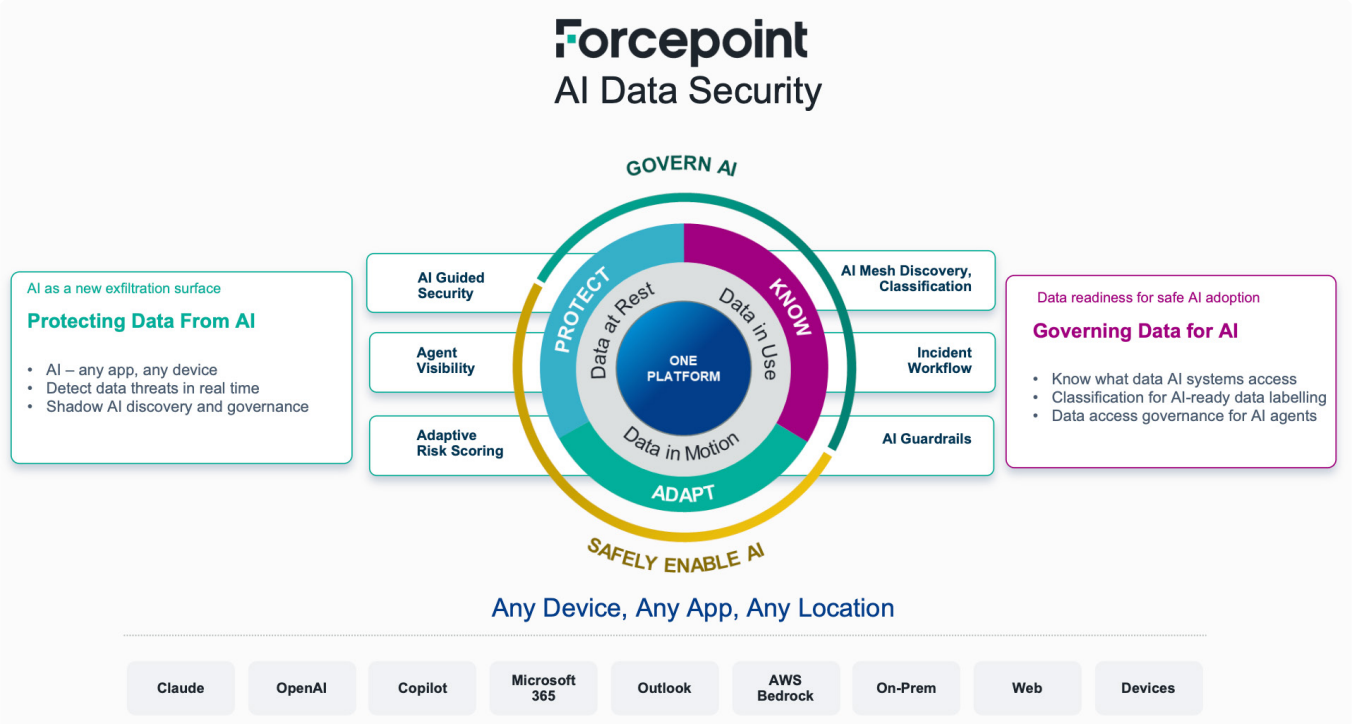
### AI Agent Gateway: Runtime Control and Enforcement

Broker agent credentials and enforce field-level data protection on every agent-to-application transaction, with human approval for high-risk actions.

## One Platform, Every AI Interaction

Forcepoint AI Data Security platform secures data on both sides of AI: governing data so it becomes safe to feed into AI, and protecting data from the risks AI introduces. The same protection follows data everywhere: managed laptop or personal browser, sanctioned app or shadow tool, the office or a phone at home.

Forcepoint is the only company that secures any data, structured or unstructured, on-premises and in the cloud, across every channel it moves through, including AI. Other vendors bolt AI security on as a separate tool. Forcepoint extends the data security organizations already trust to the AI front door.






forcepoint.com/contact

©2026 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.
[FP-Solution Brief-AI Data Security-EN] 06Aug2026