

Solution Brief: Secure AI Foundation (SAIF)

Institutionalizing Intelligence: From Shadow AI to a Governed AI Operating Boundary



As the industry's first Managed Intelligence Provider (MIP), Atlas Technica uses SAIF to establish a secure, enterprise-grade AI operating boundary that moves firms from unmanaged, shadow AI to a governed model built on approved access, data controls, and ongoing oversight.



Governed Access

Control who can use AI and under what conditions.



Data Boundaries

Keep sensitive information inside managed control.



Auditability

Maintain usable visibility for compliance and regulatory review.

Governed AI control layer typically deployed & tested in 3-4 weeks*.

* subject to client access, readiness & approvals

IMPLEMENTATION MODULES

MODULE	WHAT WE DO	BUSINESS IMPACT
 Shadow AI Containment	Identify unsanctioned AI usage patterns and steer users toward approved tools through supported browsers, and endpoint controls.	Reduces shadow AI risk. Creates visibility into real usage and helps limit data exposure through unsanctioned AI tools.
 Identity & Device Controls	Configure SSO, MFA, conditional access, approved-user groups, and managed-device requirements for sanctioned AI platforms.	Strengthens access posture. Ensures approved users access AI through the organization's identity and device posture.
 High-Level Permission Audit	Review SharePoint for oversharing and inherited access risk.	Reduces exposure risk. Helps reduce accidental exposure of sensitive content through AI.
 Sensitivity Labeling	Publish and apply a practical label, including restricted content where appropriate.	Clearer data boundaries. Creates practical boundaries for AI usage and governance.

ONGOING SERVICE & GOVERNANCE

Atlas provides a structured operating layer after go-live to keep AI access governed, auditable, and supportable as usage expands.

			
Governance Review Regular review of approved AI access, block lists, shadow AI categories, and monitor/block settings as usage evolves.	Reporting & Oversight Governance reporting on usage trends, notable activity, key exceptions, and recommended control adjustments.	Operational Support Ongoing handling of AI-related tickets, access issues, control exceptions, and remediation as adoption expands.	Guardrail Tuning Access workflow updates, and periodic guardrail tuning to reflect regulatory expectations and changing platform behavior.



Atlas Technica is the premier technology partner for the alternative investment industry and the industry's first Managed Intelligence Provider (MIP), purpose-built for capital markets. Founded in 2016, Atlas Technica delivers enterprise-grade IT, cybersecurity, cloud, and AI so firms can place IT on our shoulders.