ATLAS TECHNICA

Solution Brief: Simple AI Necessities (SAIN)

Identity-connected access and baseline hardening for approved AI platforms

Before enabling an AI platform, establish a practical baseline: which platform is in scope, who can sign in, which settings will be configured, what activity can be logged, and who owns the handoff.

Define Scope

- *Define the exact libraries, mailboxes, and systems in scope.*
- *Confirm available platform logging.*

Approved Connectors & Sources

Configure and validate only existing, supported sources approved for this use case.

Rule of Thumb

- *Start with approved, lower-risk use cases approved data sources.*
- *Exclude trading and sensitive data.*

Foundational AI access and baseline hardening. Typical implementation effort: 3–6 hours for the initial scope.*.

**Assumes licenses, administrative access, and test users are available.*

IMPLEMENTATION MODULES

Module	What We Do	Business Impact
AI Use / Risk Waiver	Confirm the AI Use / Risk Waiver is signed and document the approved platform, use case, and in-scope users before production access.	**Documented Approval:** Records the approved platform, use case, and in-scope users before production enablement.
Baseline Platform Hardening	Apply platform-supported baseline security, logging/audit, data-handling, retention, and tenant-restriction settings, limited to the agreed scope.	**Reduced Unmanaged AI Exposure:** Steers users from personal accounts to approved enterprise tenants.
SSO & Approved Access	Configure and validate SSO, security groups, and approved-user access for each in-scope AI platform.	**Secure, Simplified Access:** Centralizes sign-in and approved-user access for each in-scope platform.
Logging & Audit	Enable and validate available platform logging and audit settings; document visibility limits.	**Platform-Supported Audit Visibility:** Enables available platform logging and audit settings. Event fields and retention vary by platform; document visibility limits.
Ownership & Escalation	Document the client owner, administrative contacts, and escalation path for the configured environment.	**Clear Accountability:** Establishes an owner for integrations, exceptions, and escalations.

Start with the essentials. Scale with control.

SAIN establishes SSO, approved-user access, and baseline hardening for approved AI platforms. It is a light-touch implementation service—not an ongoing AI security or governance program.

SAIN Access → **SAIF** Hardening → **SAIG** Governance

SAIN configures approved platforms and existing supported connectors only.

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.