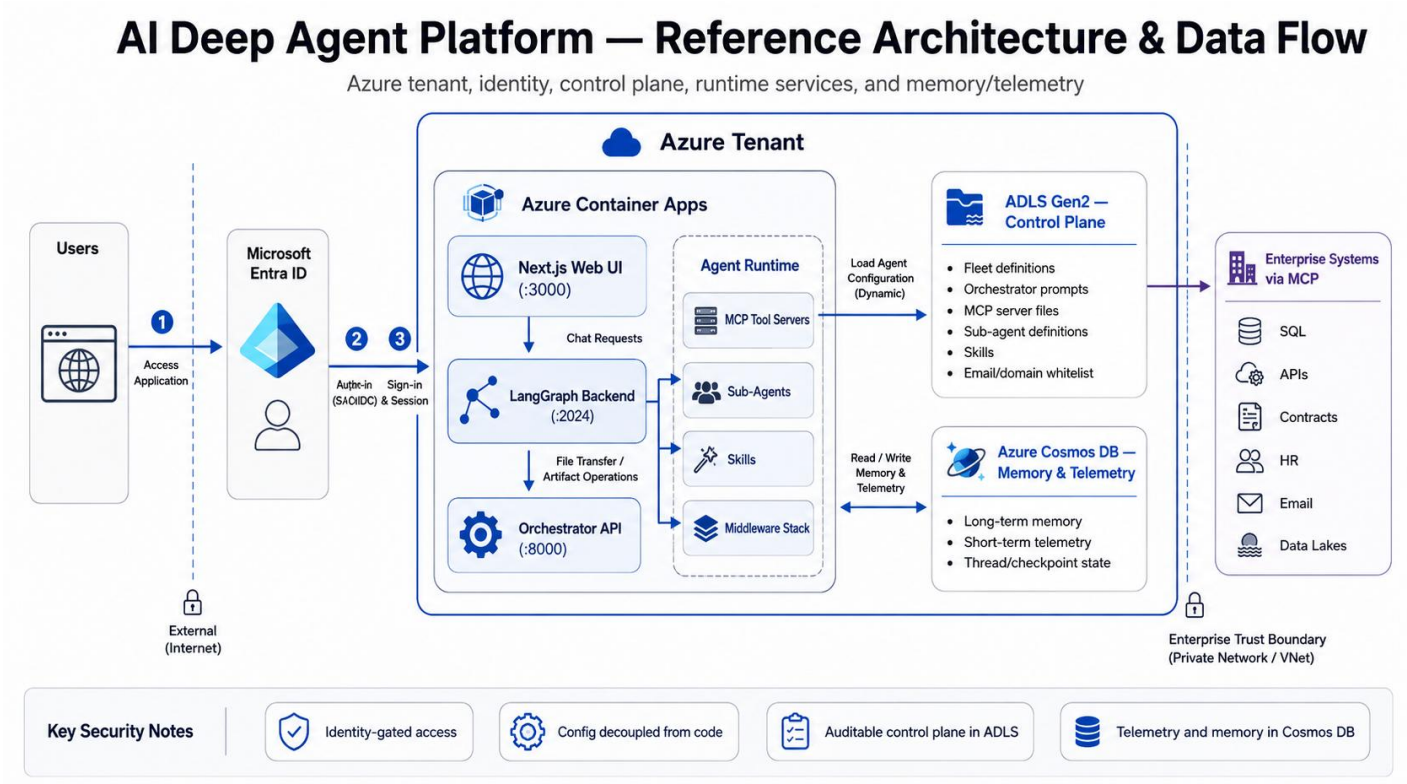
FOR THE CISO & SECURITY TEAM

Enterprise AI, *Secured by Design.*

The Security *Reality*

AI adoption is outpacing security review. Teams are racing to deploy agents and copilots — often on consumer accounts, with company data flowing to places you can't see, govern, or audit. The exposure lands on your desk: shadow AI, unmanaged data egress, and autonomous systems acting without guardrails.

ClearData AI is built to *pass* security review, not bypass it. It runs entirely on Microsoft Azure, deploys into your own tenant, and is engineered around the controls you already operate — identity, encryption, isolation, and audit. Your data stays inside your boundary; the intelligence comes to it.



Your Data, *Encrypted* and in Your Control

ClearData AI stores data in standard Microsoft Azure services — Azure Data Lake Storage (ADLS Gen2) and Azure Cosmos DB — and inherits their encryption, key-management, and compliance foundations. Nothing custom, nothing to take on faith: the same mechanisms your organization already trusts in Azure.

Encrypted at Rest & in Transit

- ✓ **AES-256 at rest, by default.** All stored data is encrypted with Azure Storage Service Encryption (ADLS Gen2) and Cosmos DB encryption — enabled by default, no configuration required.
- ✓ **Your keys, if you want them.** Use Microsoft-managed keys, or bring customer-managed keys (CMK) held in Azure Key Vault for full control and rotation.
- ✓ **TLS 1.2+ in transit.** Every client and service-to-service connection is encrypted end to end.
- ✓ **Secrets, envelope-encrypted.** Tenant credentials and OAuth tokens are sealed with AES-256-GCM envelope encryption — the master key in Azure Key Vault, never embedded in code, the data lake, or the browser.

In Your Control

- ✓ **Deployed in your Azure tenant.** Runs in your subscription and your region — data residency stays under your governance.
- ✓ **Never used to train models.** Your data serves your agents and nothing else. It is not used to train foundation models.
- ✓ **Private / on-prem inference.** Run open models in your own environment for the most sensitive workloads — data never leaves your perimeter.
- ✓ **Minimized retention.** Operational telemetry carries a 30-day TTL; you decide what is kept and for how long.

Security Controls at a *Glance*

The controls a security review asks for — mapped to exactly how ClearData AI implements them on Azure.

CONTROL	HOW CLEARDATA AI IMPLEMENTS IT
Encryption at rest	✓ AES-256 via Azure Storage Service Encryption (ADLS Gen2) and Cosmos DB — on by default; Microsoft-managed or customer-managed keys (Azure Key Vault).
Encryption in transit	✓ TLS 1.2+ across all client and service-to-service connections.
Identity & SSO	✓ Microsoft Entra ID (single- or multi-tenant) via OAuth, with Auth0 OIDC and Google Workspace as additional SSO options; signed JWT sessions validated on every request.
Access control	✓ Email / domain allow-list with least privilege. Every Azure data-plane call (ADLS Gen2 and Cosmos DB) uses an Entra managed identity — shared storage-account keys are disabled (allowSharedKeyAccess = false), and download links use short-lived, user-delegated SAS. No standing keys.
Secrets management	✓ Azure Key Vault, loaded at runtime via managed identity — no secrets in code. Per-tenant API keys and third-party OAuth tokens are envelope-encrypted (AES-256-GCM) in Cosmos DB with the key-encryption key held in Key Vault, resolved server-side per request and never sent to the browser (masked previews only).
Code-execution isolation	✓ Agent-generated code runs in ephemeral, sandboxed Azure Container Apps sessions, isolated from the core platform.
Configuration safety	✓ Configuration is parsed by a safe evaluator — no arbitrary code execution.
Human oversight	✓ Human-in-the-loop approval gates on consequential actions.
Autonomy limits	✓ Hard wall-clock and token budget caps bound every autonomous run.
Tool access	✓ Permissioned, per-agent system connections (MCP), scoped to only what each agent may touch.

CONTROL	HOW CLEARDATA AI IMPLEMENTS IT
Audit trail	✓ Every configuration change and agent action is versioned and logged to your data lake.
Observability	✓ Per-interaction telemetry: tokens, latency, tool calls, and outcomes.
Data residency & retention	✓ Deploys in your Azure tenant and region; 30-day TTL on operational telemetry, configurable.
Model data usage	✓ Your data is never used to train foundation models.

PaaS Deployed in Your Environment, *Reviewed on Your Terms*

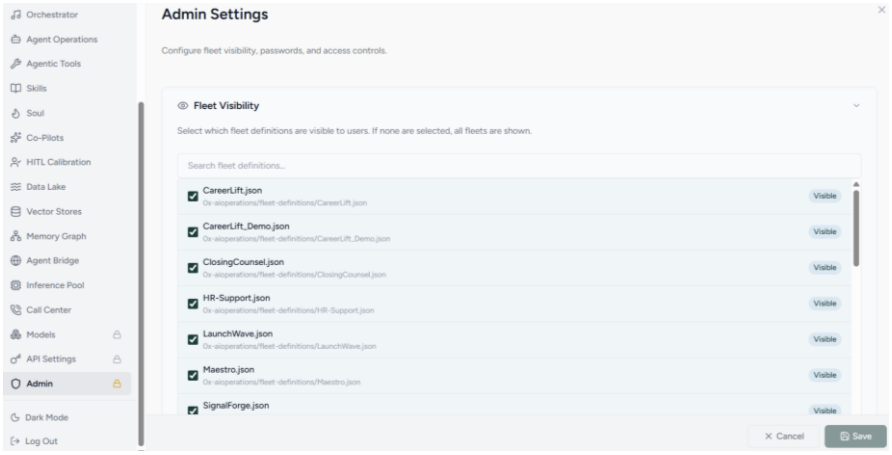
Azure-native, identity-bound, and built for the way your security team works.

Runs Where You Run

- ✓ **Your Azure subscription.** Deployed into your tenant and region — inside the perimeter you already secure and monitor.
- ✓ **Identity-bound.** Microsoft Entra ID and managed identity tie every action to a known principal under your IdP.
- ✓ **Standard Azure building blocks.** ADLS Gen2, Cosmos DB, Container Apps and Key Vault — services your team already governs.
- ✓ **Scales with your controls.** Inherits your network, logging, and policy posture instead of fighting it.

Built for Security Review

- ✓ **Architecture & data-flow docs.** Full diagrams and data-flow documentation for your review, on request.
- ✓ **Questionnaire-ready.** We complete your security questionnaire and support due-diligence and pen-test engagements.
- ✓ **Least privilege by default.** Access is scoped, time-boxed, and revocable — not all-or-nothing.
- ✓ **We review with you.** Our team works alongside yours through assessment, approval, and production hardening.



SECURE BY ARCHITECTURE. *AUDITABLE BY DEFAULT.*

ClearData AI runs in your Azure tenant, on the controls you already trust — encrypted, identity-bound, governed, and fully accountable.

Send us your security questionnaire. We'll walk your team through the architecture, control by control.

ClearData AI The AI Operating Layer for Enterprise **info@cleardataai.ai**