ai squared | NetFoundry
Secure by Design

[SECURE THE FUTURE OF AI INTEGRATION]

AI, Meet Zero Trust: Secure Access to Real-World Data at Scale

Accelerate your AI journey
Scan here to learn more.

Executive Summary

Enterprise AI adoption is accelerating. As organizations embed LLMs into daily workflows, the need to connect data securely, intelligently, and at scale becomes critical.

AI Squared simplifies AI adoption by embedding intelligent workflows directly into existing applications, without forcing refactoring or data duplication. All sources of data, no matter where it exists, can transform into new value.

NetFoundry adds zero-trust connectivity beneath the surface, ensuring data paths remain private, resilient, ephemeral, and policy-bound, without VPNs, firewall rules, or tedium of implementation.

Controlling, securing, and moving data from any source to any destination is now effortless without compromise. Alone, each platform solves a hard problem; together, they solve the right problem. AISquared connects data and insight at the edge; NetFoundry enforces security and control behind the scenes. Their integration isn't just additive, it's architectural and smart, giving enterprises a dual advantage: seamless AI experiences and uncompromising governance, anywhere.

Rethink AI Data Ingest

Enterprises are under pressure to harness AI without derailing their existing tech stack. Most are deeply invested in SaaS ecosystems, cloud storage, and on-premise systems. All of these are potential sources of insight, but also security liabilities. To make matters more complex, most AI applications today require exposing data through APIs, integrating with third-party services, or replicating data to intermediary platforms. These approaches carry operational risk, regulatory scrutiny, and performance tradeoffs.

AI Squared provides a unified interface to connect, process, and deliver AI insights across dozens of enterprise systems, without forcing data to move or be reshaped. Their platform abstracts the complexity of application interoperability while enabling secure LLM access, inside or outside the customer's environment.

NetFoundry complements this model by eliminating reliance on VPNs, exposed APIs, or static firewall rules. Instead, it provides just-in-time, identity-based, zero-trust overlays that create private, ephemeral connections, directly from the data source to the AI layer.

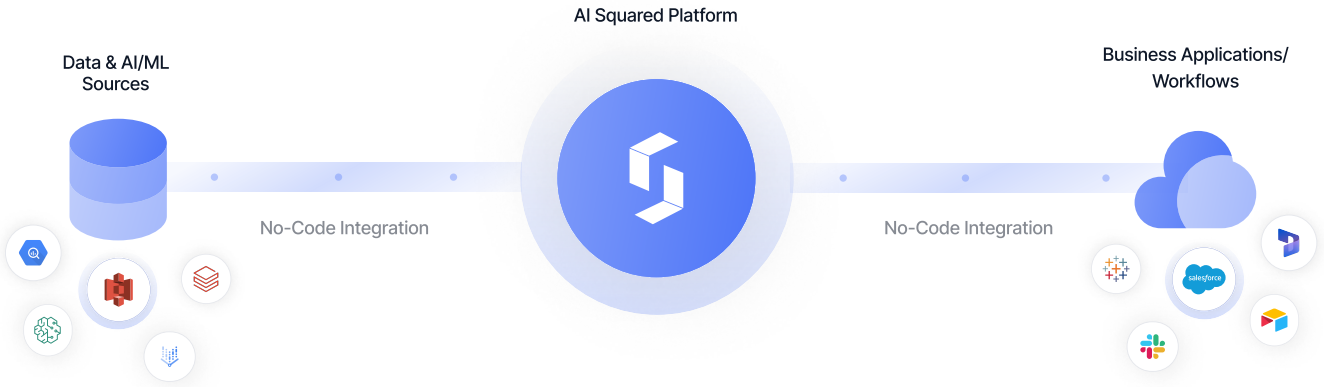
This integration blueprint demonstrates how modern AI systems can be deployed securely, flexibly, and at scale, without rewriting the enterprise architecture.

Platform Overview

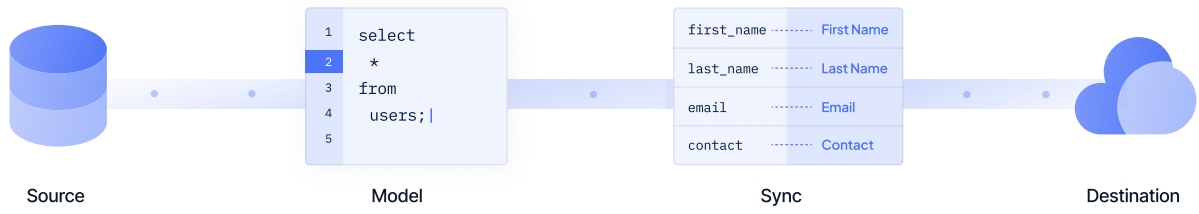
AI Squared Architecture Overview

AI Squared acts as a universal conduit between enterprise data, AI models, and end-user applications. Their platform ingests structured and unstructured data from sources such as CRMs, ERPs, cloud storage, and even on-premise systems. Once ingested, data is normalized and routed through a user-defined logic layer, allowing large language models (LLMs) to process the information according to business context and policy.

This architecture eliminates the need for invasive integration methods, such as third-party replication, custom middleware, or complex interworking. Instead, insights are delivered directly into enterprise-facing applications like Slack, Tableau, or Salesforce, and without disrupting existing workflows or forcing data movement.



AI Squared's flexibility also extends to deployment models. Whether running as a cloud-native service or deployed adjacent to sensitive data sources, the platform abstracts away technical complexity, offering a uniform interface for AI orchestration and insight delivery. Regardless of the deployment model, there are four major distinctive stages for data: source, model, sync, and destination. Connectors can be installed as standalone services near data sources or embedded directly within customer applications. They are designed to interface with APIs, databases, and application servers while remaining lightweight and infrastructure-agnostic. This flexibility allows AI Squared to support varied customer environments without imposing rigid requirements.



NetFoundry's Role in the Architecture

NetFoundry plays a critical role in securing on-premises data sources that AI Squared connects to for AI-powered insights. While AI Squared's platform can interact with data from both cloud and on-prem environments, this integration focuses specifically on private infrastructure, and how that private infrastructure connects its data sources to AI Squared. These include databases, application servers, or ERPs hosted within one or multiple customer internal networks. Instead of relying on public IPs, open firewall ports, or VPNs, NetFoundry provides a zero trust overlay network that connects on-premises data sources directly to AI Squared's services. These connections are identity-based, end to end encrypted, and governed by precise policies. No static configuration is required, and no shared credentials or persistent tunnels are exposed. Access is controlled mutually by the customer and AI Squared.

This approach ensures that every connection from a private data source to AI SquaredThis approach ensures that every connection from a private data source to AI Squared travels through a secure, isolated path. It works in complex environments, legacy systems, and modern infrastructures without changing the network or adding exposure. Together, AI Squared and NetFoundry offer a unified, composable AI architecture. On-premises data becomes accessible and secure without compromising control, visibility, or operational integrity.

Existing Approaches of AI Data Ingest

Many organizations adopting AI today rely on traditional data integration methods, especially when working with on-premises data sources. These methods often involve public API forwarding, static firewall rules, or broad VPN access. While these approaches are familiar and widely used, they also introduce challenges around operational complexity, control, and risk exposure.

Challenges of Existing Approaches

Standard trust models are typically structured around direct API integrations, third-party replication tools, or self-hosted connectors that forward data into AI pipelines. As data moves from enterprise environments into cloud-based AI systems, the network paths can become harder to secure and audit. This is especially true when multiple services, teams, or endpoints are involved.

The illustration below captures a common reference architecture. It highlights areas where security and operational control may be more difficult to enforce using conventional methods. In the two methods of access shown, each has its own distinct burdens and advantages.

Existing Approaches of AI Data Ingest

Public API Endpoints

This method allows customer connectors to reach outbound of their network (usually on the common HTTPS/443 port) to connect to AI Squared's well-known, publically available, endpoint.

Burden: This exposes the AI Squared endpoint, requiring diligent monitoring and edge protections to prevent denial of service or even discovery of weak access mechanisms by threats. Protection at this level is expensive and time consuming to maintain and monitor. Additionally, a bad-actor could obtain the keys for access by a known good-actor. This level of monitoring requires behavioral analysis to mitigate, which is an even greater cost to the organization.

Advantage: Easy to enable this access. The connector software simply needs to connect to the Internet.

Private API Endpoints via VPN

This method allows a customer to provision a VPN client for AI Squared to utilize for permitting access into the private source site.

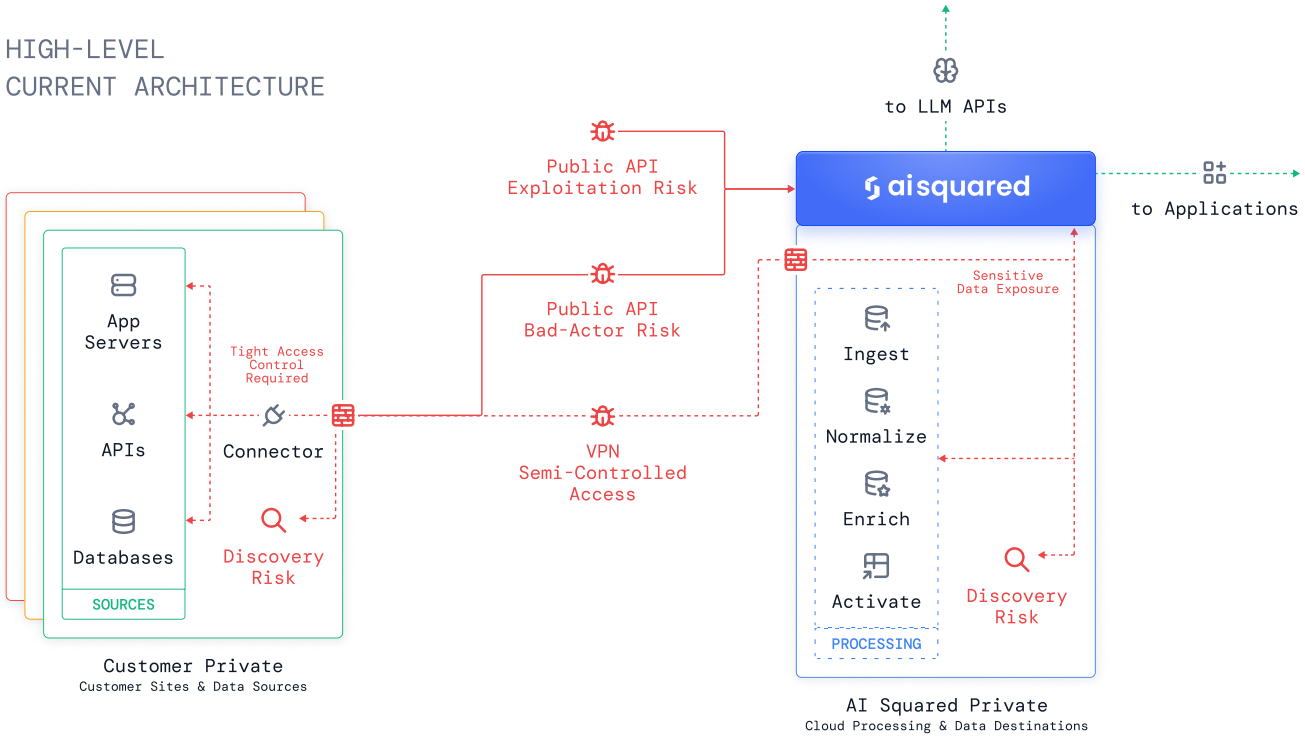
Burden: The customer, or even AI Squared, must provision and maintain a VPN with ACLs for each source site involved. Unless a complex client access mechanism is in place, centralized routing must also occur for access to other site sources. Configuration and maintenance alone are reasons why this method is highly unscalable, though this also leaves both parties in a trust limbo. At minimum, the server side of the VPN must be publically exposed to facilitate access by clients, which again creates a requirement to protect the service with potentially expensive montoring and mitigation infrastructure. VPN solutions vary widely in their responsiveness to security vulnerabilities, both in hardware and software, which is one of the biggest reasons why they are considered insecure as a whole.

Advantage: More security and more privacy between the parties. However, this is very much an illusion that deteriorates post implementation. This method is not scalable, prone to error and data leak, and invites malicious activity if not tightly controlled.

Method	Advantage	Burden/Trade-Off
Public API Endpoints	Easy to enable, Internet-accessible	Broad attack surface, requires constant monitoring
VPN-Based Access	More private, removes public-facing APIs	Operationally complex, hard to scale, introduces trust gaps

While both approaches offer a path to connectivity, they each introduce varying degrees of exposure, operational burden, or scalability limitations. A better approach is needed, one that integrates security and flexibility without these compromises.

HIGH-LEVEL
CURRENT ARCHITECTURE



Zero Trust Approach to AI Data Ingest

Rather than rely on public APIs or insecure VPNs, AI Squared and NetFoundry collaborated to build a foundation of secure connectivity that elevates beyond what is unfortunately standard accepted in the industry. The result is a streamlined data ingestion path that preserves security principles while enabling the velocity AI demands.

Key Benefits of the Zero Trust Approach

- **Zero Trust Overlay:** NetFoundry provides an identity-based, encrypted overlay network that connects edge data sources directly to AI Squared's services. These connections are invisible to the public internet and hardened against spoofing or unauthorized access. Service access that is not provisioned by policy to a consumer is not visible to the consumer.

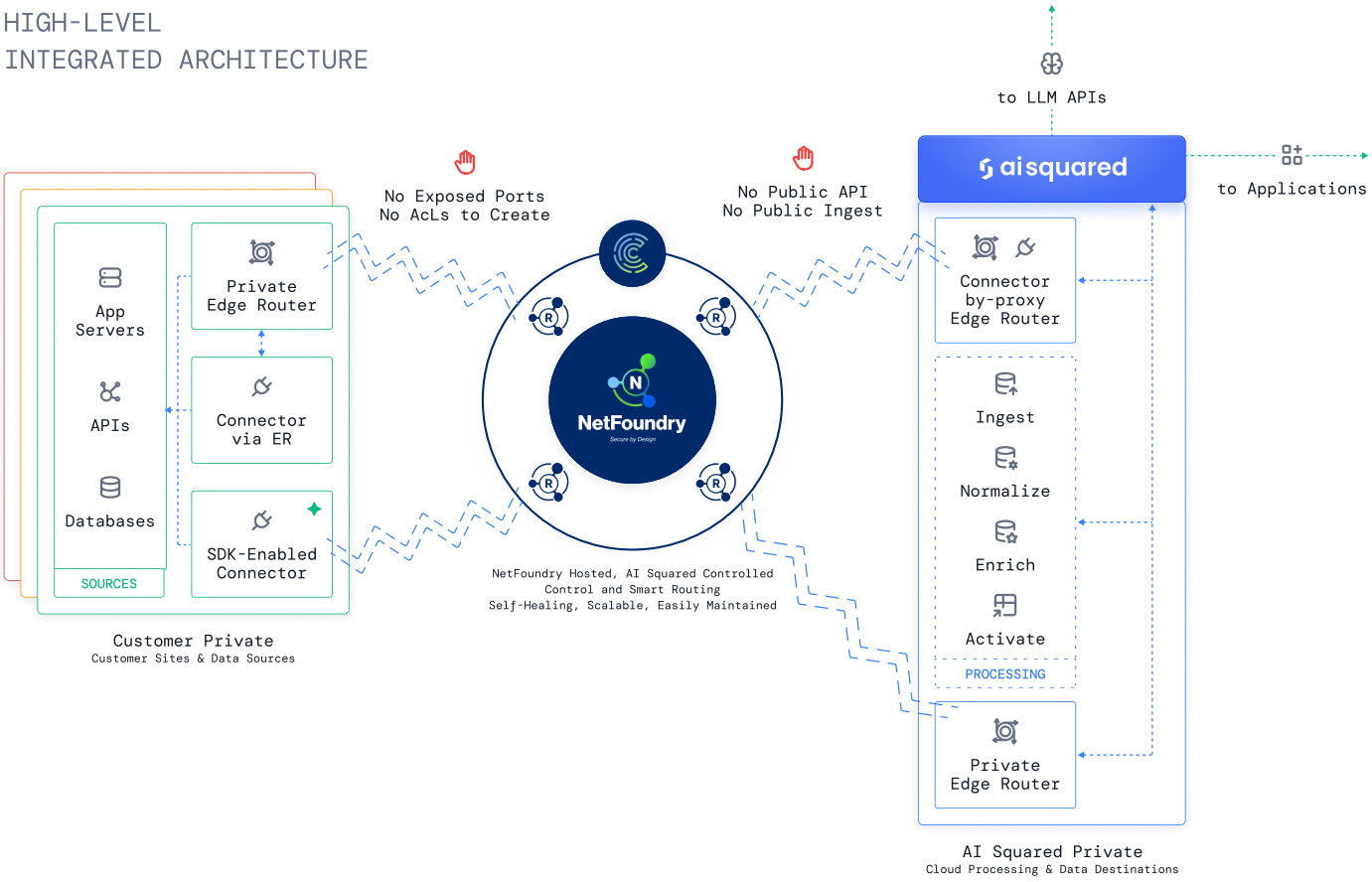
- **Edge-to-Cloud Simplicity:** AI Squared customers can deploy software connectors on-premises or at the edge without reconfiguring firewall rules or opening inbound ports at either side of communication. The system adapts to existing network conditions, removing complexity for IT teams.

Zero Trust Approach to AI Data Ingest

- **Microsegmentation by Identity:** Every connector is assigned a unique identity, allowing AI Squared to enforce precise policies on which systems can talk to which data sources. Unauthorized connections are blocked by design, not by configuration. With this segmentation is detailed analysis of all management changes to the policy as well as the usage of the policy.
- **No VPNs and No Public Exposure:** Unlike traditional connectivity models, this approach eliminates public IP dependencies and lateral movement risks at all edges of the communication. The attackable surface area is dramatically reduced, accelerating security audits and compliance reviews. Services are directional and microsegmented by policy. Undesired service discovery from any point in the network is highly reduced and tightly controlled.

  Together, this solution allows AI Squared to offer its customers a path to secure, scalable data integration without requiring them to become experts in networking or security.

HIGH-LEVEL
INTEGRATED ARCHITECTURE

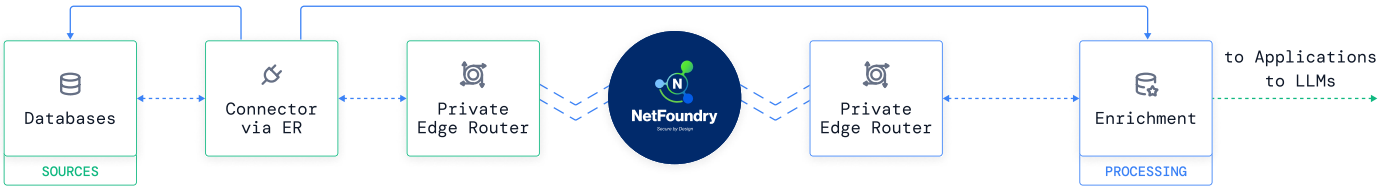


Network Integration Models

The following section outlines three supported deployment models that preserve security and simplicity while accommodating different customer environments. Each option ensures private data never traverses the public internet unprotected.

Option 1: Local Connector with Adjacent Edge Router (Simplest On-Prem Setup)

In this model, the connector communicates over the local network with a nearby NetFoundry Edge Router. The Edge Router handles all secure overlay communication, allowing the connector to reach remote AI Squared destinations without exposing the customer's internal services to the public internet. No inbound ports are opened, and no DNS or IP changes are required. Correlating customer access to AI Squared services is extremely difficult as the source and destination are never revealed in a single packet.



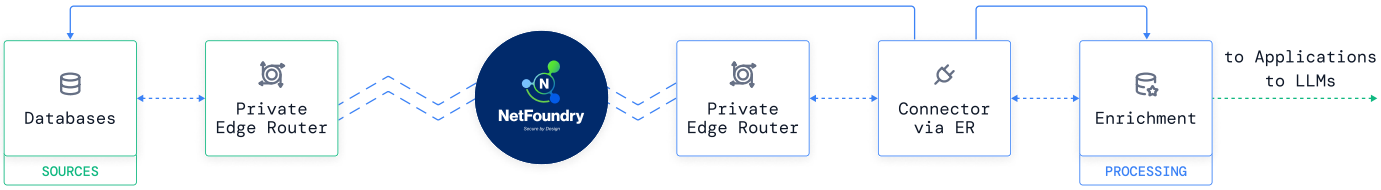
Option 2: SDK-Enabled Local Connector (No Extra Router Needed)

When embedded with NetFoundry's SDK, the connector itself becomes a secure endpoint identity. It joins the overlay fabric directly, using its identity to authenticate and route traffic through the private network. This option removes the need to deploy and manage Edge Router software, enabling streamlined deployments in environments with limited infrastructure.

Option 3: Far-End Connector via Customer Edge Router (Centralized AI Access with Remote Trigger)

In this model, the connector is deployed within AI Squared's infrastructure, not the customer's. However, NetFoundry Edge Router software is still present in the customer's network. This Edge Router establishes an outbound-only, identity-authenticated connection to the fabric, enabling the far-end connector to initiate secure, policy-bound access to private data sources through the overlay.

The customer continues to have complete control over what sources are network visable to the Edge Router as well. Unlike traditional pull models that require public IPs or inbound firewall rules, the far-end connector leverages the fabric to appear virtually "inside" the customer network for only explicit access to the defined resources. This enables centralized operations by AI Squared without compromising the security perimeter of the customer's infrastructure. data security.



Policy Enforcement and Observability

Each connector, regardless of deployment model, is assigned a unique identity within the fabric. This identity is used to define precise policies that govern which data sources the connector can communicate with. Unauthorized attempts are denied by design. All access is logged at the network layer, giving AI Squared and its customers visibility into connector behavior without additional tooling.

Operational Benefits of the NetFoundry-Enabled Integration

- **Simplified Network Management:** With no need to manage VPNs, static IPs, or complex firewall rules, operations teams are freed from the typical burdens of maintaining secure remote access. Network changes, certificate rotations, and ACL updates are abstracted into identity-based policies managed centrally.
- **Ephemeral, Policy-Driven Connections**: Connections are only created when needed, and only between explicitly defined identities. This ephemeral nature reduces lateral movement risk and ensures no exposed ports or persistent tunnels remain open.
- **Reduced Attack Surface:** By eliminating the need for inbound access, public endpoints, or shared credentials, the platform architecture drastically limits exploitable vectors. This architecture adheres to zero-trust principles by default.
- **Auditable and Observable by Design:** Traffic is encrypted and segmented, and each connection is attributed to a specific identity. Combined with centralized orchestration, this makes regulatory compliance and operational oversight more achievable.
- **Better DevSecOps Alignment:** The approach supports infrastructure-as-code deployment, integrates easily into CI/CD pipelines, and separates policy from transport, enabling teams to manage AI data flows in a programmable, testable way.

Operational Comparison

These distinctions don't just reduce risk, they also shift security and connectivity from a manual, reactive process to a programmatic, policy-driven model. For organizations scaling AI adoption, these operational gains are often what unlock broader rollout and faster time-to-value.

TRADITIONAL VS. NETFOUNDRY-ENABLED INTEGRATION

Dimension	Traditional Approach (VPNs, Static Rules, Public APIs)	NetFoundry-Enabled Integration (Identity-based, Ephemeral Overlay)
Access Control Model	IP/Port-based ACLs, manual firewall rules at every site/edge	Identity-based policies, centrally managed, with multiples per site/edge
Exposure Surface	High - requires inbound rules, public IPs, or NAT traversal	Minimal - outbound-only, no exposed IPs or ports - at every site/edge
Connection Persistence	Always-on tunnels or persistent API endpoints	Just-in-time, ephemeral connections, private-only API endpoints
Operational Burden	High — requires coordination between teams for routing, firewall, VPN config	Low — abstracted via fabric overlay, no network reconfiguration required
Credential Handling	Shared secrets or service credentials embedded in configs	Zero-trust posture - identities are mutually authenticated per session
Scalability	Brittle - scaling means replicating complex networking constructs	Elastic - connections scale based on identity, not topology
Change Management	Risky - DNS/IP changes can require redeployment	Resilient - abstracted from underlying network topology
Auditability & Observability	Siloed - depends on local log aggregation and VPN telemetry	Centralized - each connection is logged, attributed, and inspectable
Security Alignment	Perimeter-based, trust-on-first-use, trust only within application layer	Zero-trust, least privilege by design, trust established well before application access
Maintenance Overhead	Manual cert rotation, ACL upkeep, NAT traversal fixes	Minimal - policy changes via control plane, identities rotate automatically

Even Deeper: Compliance and Adherence are Built In

Beyond performance, visibility, and control, enterprise data architectures must increasingly demonstrate compliance with strict regulatory and security mandates. NetFoundry's fabric addresses this imperative by enabling deployment configurations that conform to **FIPS 140-3** cryptographic standards.

Through the use of FIPS-validated cryptographic modules within the NetFoundry edge routers, controller, and fabric transport, organizations can design data flows that **inherit FIPS-compliant security guarantees** from end to end. Whether handling sensitive healthcare records, financial transactions, or other regulated data, the overlay network can be architected to align with the cryptographic requirements imposed by federal or industry frameworks.

In contrast to traditional VPNs or SD-WANs, which often rely on a patchwork of encryption practices and vendor-specific modules, NetFoundry embeds compliance directly into the secure overlay itself - **not as a bolt-on, but as an operational default when deployed accordingly**. This not only reduces audit complexity but accelerates time to attestation for regulated workloads.

Both AI Squared and NetFoundry are SOC-Compliant companies.

Conclusion

Secure the Future of AI Integration

AI transformation shouldn't come at the cost of security, agility, or operational sanity. Yet most existing data ingest models force a compromise, trading visibility and control for brittle, over-exposed pipelines.

By combining AI Squared's composable AI architecture with NetFoundry's identity-based, zero-trust networking, organizations can easily integrate sensitive, on-premises data into modern AI workflows without sacrificing control, scalability, or speed.

This isn't just another point solution. It's a foundational shift in how enterprises can securely and efficiently unlock the full potential of their data, no matter where it resides.

What's Next?

Whether you're a data scientist, architect, or business leader, the path to AI-enabled transformation starts with an infrastructure that's secure by design and flexible by default.

- Learn how to deploy a NetFoundry + AI Squared integration
- Request a technical demo or solution architecture
- Connect with our experts to explore use cases tailored to your data landscape

Let's eliminate the barriers to AI, without creating new ones.

Bring AI To Where Work Happens

Our partners and customers