Process Intelligence Reveals the Gaps. Kirin Cyber Closes Them.

How Kirin Cyber's Self-Protecting Data Technology Addresses the Security Vulnerabilities Hidden Inside Your Business Processes

3,322
U.S. Data Breaches in 2025 (All-Time High, +79% since 2020)

$4.88M
Global Average Breach Cost (2024 Peak)

800M+
Daily Cyberattacks Worldwide in 2025

16B
Credentials Exposed in a Single 2025 Mega-Leak

THE PROBLEM

Implementing transformation without understanding your business is operationally catastrophic.

Organizations are deploying AI workflows, cloud-native microservices, and Zero Trust architectures — but they're doing it without mapping how the business actually works. The gap between the **intended process** and the **actual one** is where breaches live, where regulatory findings surface, and where AI models produce outputs nobody expected.

In a cloud-native environment, sensitive data moves between dozens of services, APIs, vendors, and cloud regions — often with minimal visibility. Entitlement drift accumulates silently as roles change and access is never revoked. AI agents carry privileges their function doesn't require. The blast radius of any single compromise can propagate across the entire workflow in milliseconds.

Process intelligence — a continuous, holistic understanding of how data flows through the business — is the discipline that reveals these gaps. But even the best process model has a critical missing layer: **what happens to the data itself once it's in motion?** Knowing where data flows is not the same as controlling what happens to it.

Process models can describe the blast radius. They can map the data lineage. They can define least-privilege access. But they cannot enforce any of it once data has left its origin — traversing APIs, AI pipelines, third-party services, and cloud regions beyond the reach of any perimeter control.

THE KIRIN CYBER SOLUTION

Security infused into the data — not just the process around it.

Kirin Cyber addresses the vulnerability that process intelligence exposes but cannot fully close. By infusing protection directly into each piece of data, Kirin ensures the data **self-enforces its own access controls** — across every service, API, and cloud environment it enters, for its entire lifecycle. Even when the process model is imperfect and identity controls drift, the data holds its ground.

HOW KIRIN CYBER CLOSES THE GAPS

- **Blast Radius — Contained at the Data Layer**
  Even if a microservice, API, or AI pipeline is compromised, Kirin-protected data remains encrypted and self-protected. The blast radius cannot reach the data regardless of how far lateral movement extends.
- **Data Flow Visibility — With Enforcement**
  Kirin's forensic lifecycle logging records every access, copy, and transfer from creation to destruction — providing the data lineage control requires, plus active protection current controls cannot deliver alone.
- **Identity Drift — Neutralized by Multi-Condition Access**
  Stolen credentials or over-provisioned service accounts cannot unlock Kirin-protected data. Access requires verified identity plus geolocation, device, time, and permission checks — all simultaneously.
- **Compliance Built Into the Data**
  Access controls, audit trails, and revocation rights are embedded in the data wrapper — making compliance architectural, not bolt-on, exactly as Tenet 3 prescribes.
- **AI Pipeline Protection**
  As AI agents process sensitive data, Kirin ensures that data remains self-protecting throughout the pipeline. If the model or integration is compromised, the data does not become exposed.
- **Owner Control — For the Life of the Data**
  Data owners can revoke or modify access at any time, from any device — even after data has traversed dozens of services. The process intelligence model defines the policy; Kirin enforces it in the data.

THE MISSING LAYER IN EVERY PROCESS INTELLIGENCE MODEL

Process intelligence tells you where your data is, how it flows, and what should protect it. Kirin Cyber ensures the data protects itself — independent of whether every process is perfectly modeled, every identity perfectly managed, or every perimeter perfectly held. Any data. Anywhere. Anytime. Always secure.