Security Tools Expire. Your Data Doesn't Have To.

How Kirin Cyber's Self-Protecting Data Technology Solves the "Imminent Obsolescence" Problem

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

Every security tool carries a built-in expiration date.

The principle of **Imminent Obsolescence** holds that security mitigations are engineered for the threat landscape at the moment of conception — not deployment. By the time a solution ships, the environment it was designed to protect has already evolved.

Businesses grow, adopt new technology, merge with other companies, and shift to cloud-first architectures. The perimeter tools protecting them cannot keep pace. The result: mitigations go obsolete not because they fail, but because the world moves around them.

Worse, organizations often discover this obsolescence **the hard way — by compromise** — rather than through proactive planning. Record breach figures prove the point: current approaches are structurally losing the battle.

THE ROOT CAUSE

Traditional cybersecurity protects the environment surrounding data — perimeters, endpoints, networks, clouds. But environments are dynamic. They are designed to change. Any security model anchored to the environment inherits that instability.

What has been missing is a security model anchored to the **data itself** — one that travels with the data everywhere it goes, regardless of what platform, device, or cloud service surrounds it.

THE KIRIN CYBER SOLUTION

Self-protecting data that never becomes obsolete.

Kirin Cyber solves the root cause — not the symptoms. Rather than building another layer around an ever-changing environment, Kirin infuses the protection directly into each piece of data. The data itself becomes intelligent, self-aware, and self-protecting: on any platform, any device, in any cloud, for the full lifecycle of the data.

CORE CAPABILITIES

- **Protection Infused Into the Data**
  Patented multi-key encryption wraps each file in independent security layers. No single layer can be compromised without triggering protection in surrounding layers.
- **Platform-Agnostic & Always Current**
  Works on any device, OS, cloud, or data center. Uses the CryptoAPI of whatever platform the data lands on — so it automatically upgrades as encryption standards evolve.
- **Owner Control After Possession**
  Data owners can revoke or modify access at any time, from anywhere — even after the file has left their hands. No chasing down copies across systems.
- **Geo-Sensing & Conditional Access**
  Data can geo-sense and geo-fence itself. Outside an approved location? It self-encrypts and alerts the owner. Offline? A "default safe and closed" policy applies.
- **Forensic Lifecycle Logging**
  Every access, copy, and storage event is recorded from creation to destruction — providing proof of custody and control that travels with the data.
- **Post-Quantum Futureproofed**
  Designed to be interchangeable with next-generation encryption standards including blockchain and quantum methods — eliminating the primary driver of Imminent Obsolescence.

WHY KIRIN CYBER IS THE PARADIGM SHIFT

Cybersecurity has always operated on one insurmountable premise — that data cannot protect itself. Kirin Cyber changes that premise entirely. By making data self-protecting, organizations are no longer racing to keep perimeter tools current against an evolving threat landscape. The protection travels with the data — any data, anywhere, anytime, always secure. With an enterprise API enabling OEM integration into existing applications, products, and services, Kirin Cyber is positioned as a foundational layer for a new technology ecosystem.