When Identity Is Compromised, Your Data Shouldn't Be.

How Kirin Cyber's Self-Protecting Data Technology Resolves the "Appropriate Trust" Problem

81%
Of Breaches Involve Stolen or Weak Credentials

$4.88M
Global Average Breach Cost (2024 Peak)

3,322
U.S. Data Breaches in 2025 All-Time High

800M+
Daily Cyberattacks Worldwide in 2025

THE TRUST PROBLEM

Identity alone is no longer a trustable source of truth.

The Principle of **Appropriate Trust** holds that classic identity — usernames, passwords, even multi-factor authentication — can no longer carry the full weight of securing access to digital assets. Credentials are routinely stolen, spoofed, and phished. Identity has become the attacker's most reliable entry point.

The compounding problem: "complex" identity solutions (MFA, PKI, zero-trust zoning) are expensive, difficult to deploy at scale, and invite user revolt. Organizations default to simpler — and more vulnerable — authentication for the general workforce. Even advanced methods like token-backed identity carry unresolved trust dependencies on third-party database sources.

The strategic question is no longer **"who are you?"** It is **"even if I know who you are, should your identity alone unlock my data?"**

WHY EXISTING SOLUTIONS FALL SHORT

Zero-trust zoned architectures, least-privilege controls, and MFA all reduce attack surface — but they share one fatal dependency: they protect the environment surrounding the data, not the data itself. Once a bad actor moves past the identity checkpoint, the data is exposed.

What security architects have long needed is a self-reliant trust model — one that is **independent of third-party attestation**, deployable at scale, and capable of enforcing access conditions even after data has left its owner's environment.

THE KIRIN CYBER SOLUTION

Trust built into the data — not the identity layer.

Kirin Cyber answers the Appropriate Trust problem at its root. Rather than stacking more authentication layers, Kirin infuses a **multi-condition trust model directly into each piece of data**. The data itself evaluates whether access should be granted. A stolen credential, compromised endpoint, or bypassed perimeter does not translate into exposed data.

HOW KIRIN ESTABLISHES APPROPRIATE TRUST

- **Multi-Condition Access — Beyond Identity**
  Access requires a selection of conditions to pass: verified identity, approved geolocation, authorized device or platform, valid time window, and current permissions. A stolen credential alone cannot unlock Kirin-protected data.
- **Owner-Controlled, Revocable Trust**
  Data owners modify or revoke access at any time — even after the file has left their possession. Trust is never permanently delegated; it remains under the owner's active control for the life of the data.
- **Self-Reliant Trust Model**
  Kirin's multi-layered protection is self-contained within the data. It does not rely on any third-party trust source— eliminating trust-chain vulnerabilities.
- **Reciprocal Proof — Forensic Lifecycle Logging**
  Every access attempt, copy, and custody transfer is logged and reported back to the data owner. The data can prove its own integrity and provide a verifiable chain of custody.
- **Platform- & Identity-Provider-Agnostic**
  Works with any existing IAM, MFA, or zero-trust architecture. Kirin adds a data-layer trust enforcement tier that complements — and survives — whatever identity infrastructure surrounds it.
- **Post-Quantum & Future-Standard Ready**
  Uses the CryptoAPI of the device or OS the data arrives on. As encryption standards evolve — AES, elliptical curve, or quantum level — Kirin's trust model automatically upgrades without re-engineering the data.

THE PARADIGM SHIFT: TRUST THE DATA, NOT JUST THE IDENTITY

Security has long asked users to prove who they are, then trusted that proof to protect everything. Kirin Cyber inverts this model: the data itself enforces a multi-condition, self-reliant trust framework that is independent of identity systems, immune to credential theft, and persistent across every environment the data enters. With a lightweight enterprise API enabling integration into existing applications and workflows, Kirin delivers the scalable, third-party-independent trust model the industry has been waiting for.