SyberKey

SYBERKEY — Cryptographic Path Enforcement (CPE)

Patent Pending ---AI-Driven - Post-Quantum - Biometric Digital Identity - Zero Data Breach Architecture — the first system that does not rely on server trust or admin permissions.

1. The Vision

SyberKey aims to become the **global standard for quantum-secure identity and data access**, ensuring that no attacker — internal or external — can ever access enterprise data without AI-approved, biometric-anchored cryptographic authorisation.

We secure the entire path to data, not just the login.

SyberKey is creating a new cybersecurity category:
Cryptographic Path Enforcement (CPE).

With AI-governed key release, post-quantum protection, and biometric anchoring, SyberKey becomes the first platform capable of (near) guaranteeing:

“No data breach — even if the attacker controls your entire backend.”

This is the future of enterprise security.

2. The Problem

Despite massive investment in IAM, MFA, PAM, Zero Trust, and endpoint tools:

- Data breaches continue at **historic highs**
- MFA is bypassed, credentials get stolen
- Admin accounts & backend servers are compromised
- Zero-days enable lateral movement

- Cloud misconfigurations expose data
- Ransomware steals data before encrypting it
- **Quantum computing threatens RSA/ECC encryption**

Identity is not enough.
Infrastructure cannot be trusted.
Existing systems cannot stop backend-level compromise.

3. The SyberKey Breakthrough

SyberKey introduces *AI-Governed, Post-Quantum Cryptographic Path Enforcement*

Three core innovations: Patent Pending

1. Biometric Digital Identity

A single encrypted Bio-ID replaces passwords, tokens, device secrets, and certificates.

2. AI Control Plane

Evaluates every access attempt using:
• identity • device posture • software legitimacy
• behavioural baseline • context • anomaly signals

3. Just-In-Time Post-Quantum Key Release

Data is always encrypted.
AI releases a **short-lived PQ decryption key** only if the entire path is trusted.

No AI approval = no key = no access
—even for admins, malware, insider threats, or compromised servers.

4. Why It Matters

✓ Stops breaches even during total system compromise

No stored keys. No backend trust. No decrypt capability anywhere.

✓ Quantum-safe architecture

Built on NIST-approved PQ algorithms.

✓ True Zero Trust

Identity, device, software, behaviour & data are validated continuously.

✓ Cross-industry applicability

Banking • Healthcare • Government • Defence • SaaS • Education • Critical Infrastructure

✓ Regulator-friendly

Quantum-ready + continuous verification + PQ-signed audit logs.

5. Market Opportunity

SyberKey operates at the intersection of **$180B+ global markets**:

- Identity & Access Management
- Zero Trust Architecture
- PQ Cryptography
- Data Security
- AI Security & Governance

Demand driven by ransomware, insider threats, cloud complexity, and quantum-readiness mandates.

6. Business Model

SaaS Subscription
Per-user, per-device, per-database/data pool.

Enterprise Add-Ons
PQ Vault • PQ Audit • Compliance Packs • AI Risk Engine.

OEM Licensing
Core banking, healthcare EMR/EHR, cloud IAM, defence systems.

7. IP & Defensibility

- Parent patent: biometric digital identity
- New patent-of-addition: AI control plane + PQ cryptographic enforcement
- Claims cover:

- AI-driven key release
- PQ-signed telemetry
- Path-level cryptographic blocking
- Backend compromise immunity
- Multi-entity verification chain

This IP portfolio creates a deep, defensible moat.

8. Funding required to accelerate

- Finalisation of AI + PQ products
- Enterprise integrations (Okta, Entra, AWS IAM, CyberArk)
- Regulatory compliance (ISO/SOC2/APRA)
- GTM execution
- SOC, support, engineering expansion