Environ

Identity • Data • Security

FRAUD COMBAT CONTROLS

Enterprise Intelligence, Behavioural Analytics & Proof-of-Life Security

Environ delivers a custom-built enterprise fraud intelligence platform designed to protect financial institutions from both internal and external fraud in an AI-enabled threat environment.

Core Capabilities

- AI-driven behavioural analysis of branch and back-office staff
- Early-warning indicators for insider risk and privileged misuse
- Permission-based logical access control with threshold escalation
- Finger Vein biometric Proof-of-Life as a digital signature for critical actions

Why Traditional 2FA Fails

Passwords, PINs, OTPs and tokens authenticate credentials, not people. AI-enabled social engineering, credential replay and impersonation render traditional 2FA insufficient.

Why Finger Vein is the Final Control Layer

Finger Vein verifies internal vascular patterns and live blood flow. It cannot be copied, replayed, shared or synthetically generated by AI.

Fraud Combat Controls Architecture

High-level illustration of how Environ integrates behavioural intelligence, logical access control, and Finger Vein Proof-of-Life into enterprise banking systems.

Users / Staff	Environ Fraud Combat Platform	Core Banking & Apps
Behaviour monitored	AI • Access Control • Audit	Transactions executed

Nigeria Fraud Risk Context

Nigeria's rapidly digitising financial system faces elevated fraud risks driven by identity compromise, insider abuse, and AI-enabled social engineering.

Risk Area	Nigeria Context
Digital & Electronic Fraud	1 trillion+ estimated annual exposure
Insider & Privileged Abuse	High detection complexity
Authentication Weaknesses	Primary fraud enabler