The Zero-Trust Data Platform

How to Protect Your Data with OmniIndex Zero-Trust While Enhancing Productivity through Private AI & Encrypted Analytics.

OmniIndex

White Paper

What Is Zero-Trust Access?

Zero-Trust is a security framework built on a single, powerful principle: **never trust, always verify**.

It dismisses the outdated "castle-and-moat" model where everything inside the network is considered safe. Instead, it assumes that threats can exist anywhere, forcing every user, device, and application to prove its identity and authorisation every single time access to data is requested. No single user, not even an administrator, is automatically trusted with all the keys.

Why Is It Important?

The rising sophistication of cyber threats, especially ransomware, demands a more rigorous security model. By enforcing strict verification for every access attempt regardless of its origin, Zero-Trust fundamentally reduces the attack surface. It effectively mitigates the risks of advanced cyberattacks, malicious insiders, and other vulnerabilities that exploit misplaced trust.

Crucially, Zero-Trust is not a replacement but a powerful enhancement. It can be layered on top of existing perimeter defences to create a modern, resilient security posture fit for today's threats.

How Zero-trust Works: Security & Privacy

PGBC's architecture is built on four core Zero-Trust principles that work in concert to protect your data from every angle:

Continuous, AI-Driven, Verification

Our native AI, Boudica, continuously verifies every access request in real-time by analysing user behaviour and context to ensure only legitimate interactions occur.

Data Micro-segmentation

Data is committed to an immutable blockchain where each block acts as a cryptographically isolated micro-segment, automatically containing any potential breach and preventing a spread.

Enforced Least Privilege

Users are granted the absolute minimum permissions necessary. Our Homomorphic Encryption (FHE) provides the ultimate enforcement of this, allowing administrators to run analytics on encrypted data.

Constant Encryption

Data remains constantly encrypted at rest, in transit, and during use. All AI analytics are performed directly on this encrypted data, eliminating the core vulnerability of exposure that other security models ignore.

OmniIndex

Super Users & Zero Trust

The Problem:

The All-Powerful Administrator
In traditional database systems, a "super user" or administrator account holds unrestricted privileges. This single account can view, modify, and delete any data at will. As a result, it represents the single greatest point of failure in a security architecture; if the account is compromised, the entire database is lost.

The solution:
Zero-Trust with AI & FHE.

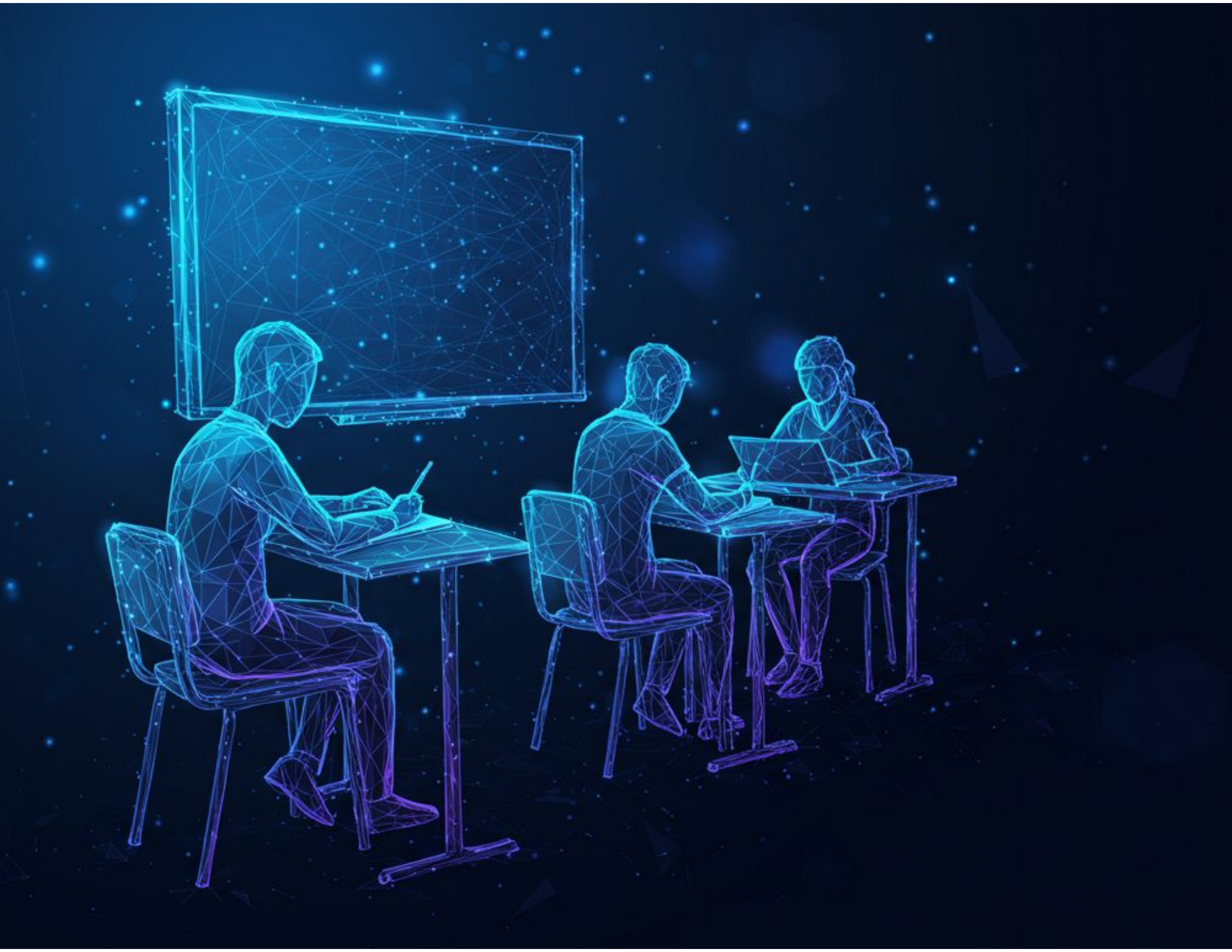
Our platform redefines the role of the administrator according to the Zero-Trust principle of least privilege.

No Ability to View Data:
Administrators can manage the system, run analytics, and monitor performance, but our Homomorphic Encryption (FHE) ensures they can never decrypt or view the raw data itself.

No Ability to Modify or Delete Data:
The immutable blockchain ledger prevents anyone, including a super user, from altering or deleting existing records, making the data immune to both malicious attacks and accidental human error.

Constant AI Oversight:
Our native AI, Boudica, continuously analyses all system logs in real-time. It instantly detects and can automatically block any user—super user or otherwise—attempting to access data or perform actions outside of their designated permissions.

OmniIndex



Customer Case Study: Educational Data & Future-X

Cross River State in Nigeria is using OmniIndex PGBC to ensure the highly confidential and regulated educational data of the state's students and staff is kept secure. This is done in partnership with Future-X Education who are using OmniIndex's zero-trust access data platform for their EMIS.

Zero-Trust Data In Action

Scenario: A school district wants to create personalized learning plans for each student based on their individual needs inspired by insights from the entire school district. However, no personally identifiable information (PII) can be exposed as it is highly confidential and regulated.

1: Blockchain Data Aggregation

The platform can securely aggregate data from various sandboxed sources, including standardized tests, teacher assessments, and student performance data.

2: Fully Homomorphic Encryption

Patented FHE (Fully Homomorphic Encryption) ensures that the data remains encrypted throughout the entire process, protecting its confidentiality so nobody can actually read the information.

3: Data Analysis

Private SLM AI models can uniquely analyze the encrypted data, allowing for insights to be derived without decryption and without letting anyone see information they do not need to see.

4: Personalized Plan Creation

Based on the generated insights from the encrypted data, users can generate personalized learning plans, tailored to each student's unique needs. Without ever seeing the PII for the student or school.

5: Secure Delivery

Teachers can securely access their students' personalized plans and action them without ever seeing the aggregated data, PII, or anything other than what they need to see.

Only OmniIndex can deliver Zero Trust at the data level without compromising your analytics or workflow.

Please get in touch to learn more about PGBC and our 'Never Decrypt' workflow.

www.omniindex.io
info@omniindex.io
+1 (650) 297-4682