The Zero-Trust Data Platform

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

OmniIndex

Simon Bain

OmniIndex

What Is Zero-Trust Access?

Zero-trust means no trust, no access. Every device, user, or network that attempts to access your data is forced to prove itself every time access is requested with strict verification and authentication to protect against exposure. No user has the power to access, edit, or manage all data.

Why Is It Important?

The increasing sophistication of cyber threats and rise in successful ransomware attacks is making it necessary for companies to add additional levels of security to their existing infrastructure.

By demanding strict verification and authentication for every access attempt, regardless of the source, zero-trust helps to mitigate the risks posed by advanced persistent threats, insider threats, and other emerging vulnerabilities. What's more, it can be combined with established perimeter-based defences to enhance what organizations already have in place.

OmniIndex

How Zero-trust Works: Security & Privacy

Continuous Verification

Every request is validated and authenticated before granting access.

Least Privilege Access

Users are granted only the minimum necessary permissions to perform tasks.

Micro-segmentation

The network is divided into smaller, isolated segments to limit the spread of potential attacks.

Constant Encryption

Data is encrypted at rest, in transit and in use to ensure it is never exposed: even while being AI searched or analyzed.

OmniIndex

Super Users & Zero Trust

A super user account, often referred to as the administrator or root account, possesses unrestricted privileges within a traditional database system.

This elevated access allows for any database action, from data modifications to schema changes.

As such, a compromised super user account can lead to a complete database breach, rendering security measures like network hardening ineffective.

To mitigate the risks associated with super user privileges, OmniIndex ensures super users are able to do their job without being able to do any harm; either intentionally or accidentally.

For example, they cannot read any of the data while they are searching or managing it with it remaining homomorphically encrypted throughout. They also cannot edit or delete data.

OmniIndex also includes native AI log file intelligence into all instances to automatically and constantly analyze whether a user attempts to access data they do not have rights to.

OmniIndex

Real Case Study: Educational Data

Cross River State in Nigeria is using OmniIndex PostgresBC 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 Educational Management System.

OmniIndex

The Problem

Future-X's system stores highly confidential and regulated educational data from multiple sources in one secure, aggregated, yet sandboxed platform. Different schools, groups, and individuals need to be able to access and use the platform, managing data and gaining analytics, but none of the stored data must ever be exposed to those separate users.

The Solution

The EMIS (Educational Management Information System) was migrated to OmniIndex PostgresBC where the zero-trust web3 storage and patented homomorphic encryption enables all the different teachers, schools, analysts and admins to work with the data they need without being able to decrypt it or access anything beyond the bare minimum they require.

OmniIndex

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.

OmniIndex

Technology Stack

OmniIndex Zero-Trust works on our Confidential Web3 Data Platform: PostgresBC. It combines a number of innovative and patented technologies with established security protocols to enable not just maximum security, but maximum insights.

OmniIndex

Fully Homomorphic Encryption

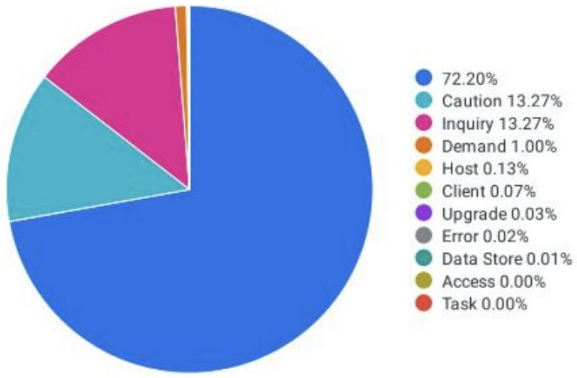
OmniIndex's patented fully homomorphic encryption provides the only commercial solution for searching and performing computations on encrypted data.

It is based on Synchronous AES 256 using the CryptoPP libraries which are deemed uncrackable through brute-force attacks.

This ensures zero trust at a granular level for maximum security & privacy with data able to remain encrypted at all times.

Data fully encrypted with OmniIndex's homomorphic encryption can be analyzed in real-time with AI.

For example, an AI risk assessment of our in-house logs holding over 1.5 million encrypted records pulling back 200,000 rows can be done in under 400 milliseconds.



> **The problem with encrypted data is that you must decrypt it in order to work with it. By doing so, it's vulnerable to the very things you were trying to protect it from by encrypting it.**
>
> **There is a powerful solution to this scenario: homomorphic encryption.**

FORBES

OmniIndex

Blockchain Storage

Our Web3 technology aligns with zero-trust principles by enforcing least privilege, promoting transparency, and leveraging cryptography.

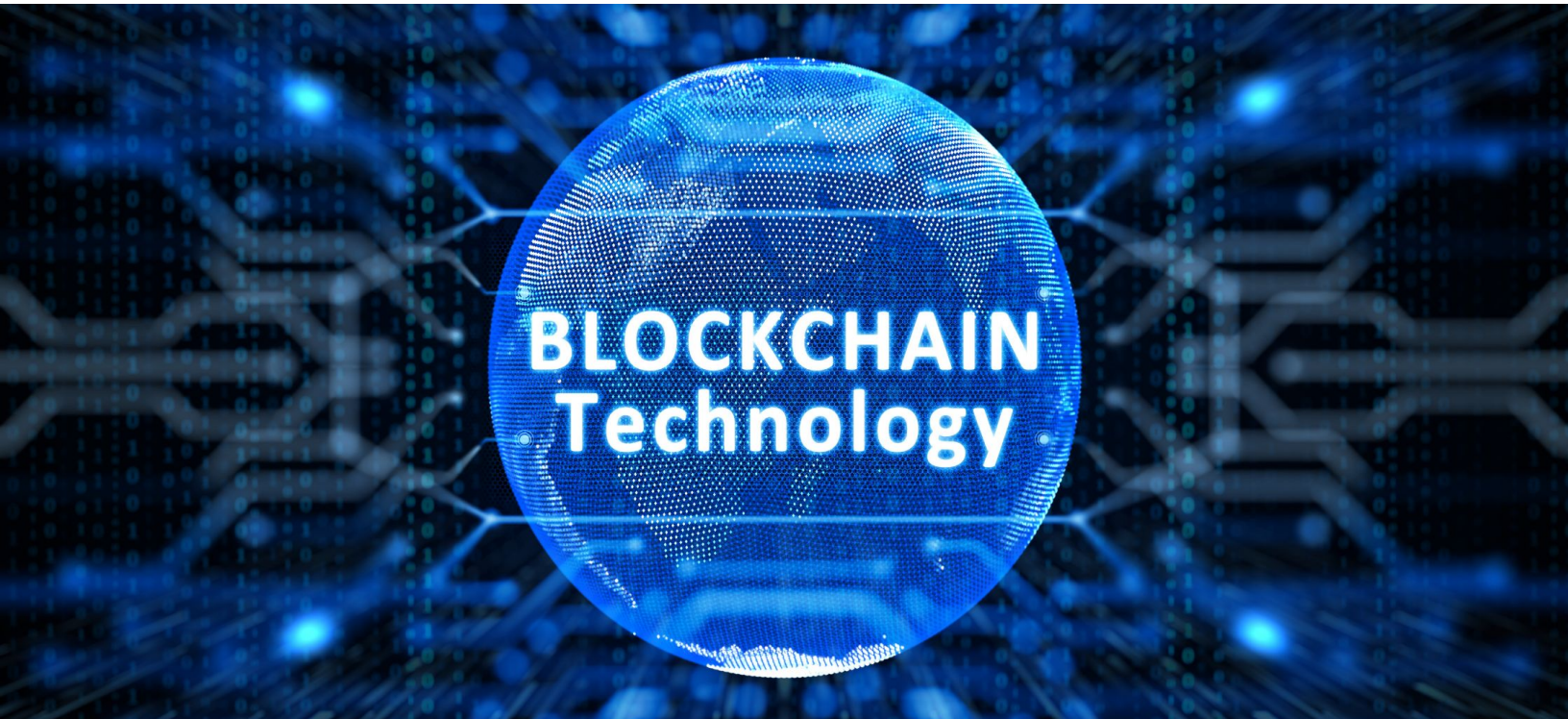
Data access is strictly controlled to ensure users only have access to necessary information. The blockchain's immutable ledger provides a transparent record of data changes, making it easier to detect and investigate unauthorized access.

What's more, when combined with our FHE and other practices, the threat of ransomware is eliminated.

Immutable data: Data cannot be modified once it is stored. This means it cannot be corrupted or held to ransom because an attacker cannot overwrite data with their own encryption.

Decentralized storage: This, along with strong cryptography, significantly hinders attack attempts as there's no single point of vulnerability.

No data loss: If a node in the decentralized network is somehow compromised, data can be recovered instantly by accessing one of the other nodes with zero data loss or disruption.



OmniIndex

Native AI

Boudica is an SLM (Small Language Model) AI engine empowering users to gain insights on their encrypted data without any data ever being exposed or shared externally. This award-winning private engine has a number of direct benefits for users.

1: Privacy
Boudica is a private and native AI solution. This means user data is not shared externally of the system to generate answers, and there is no third-party access to the user's queries or answers with data encrypted at all times.

2: Accuracy
SLMs like Boudica only work on small pools of controlled data that they are supplied with and are therefore far less likely to contain biases and inaccuracies than LLMs which learn from huge pools of varied data.

Boudica's patent-pending use of multiple separate thesaurus models and its probability matrices also ensure that only the optimum response is given to a user.

3: Efficient & Optimized
SLMs do not require extensive training on huge pools of data and can be adapted to offer specialist services in different languages and areas simply by changing their ontologies.

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

Please get in touch to learn more.

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