The Confidential Data Platform

How PostgresBC provides uncompromising data security, compliance, and threat detection for confidential data

OmniIndex

OmniIndex

The Challenge

Data is the lifeblood of modern business, but it's under siege. Cyberattacks and data breaches are rampant, forcing companies to juggle increasing regulations with the critical need to harness data insights.

From protecting sensitive health records to safeguarding trade secrets, compliance has become a complex maze.

This paper highlights the challenges businesses face in keeping their data confidential and compliant, and introduces PostgresBC as a solution for your most guarded data through its unique ability to keep data encrypted **at all times.**
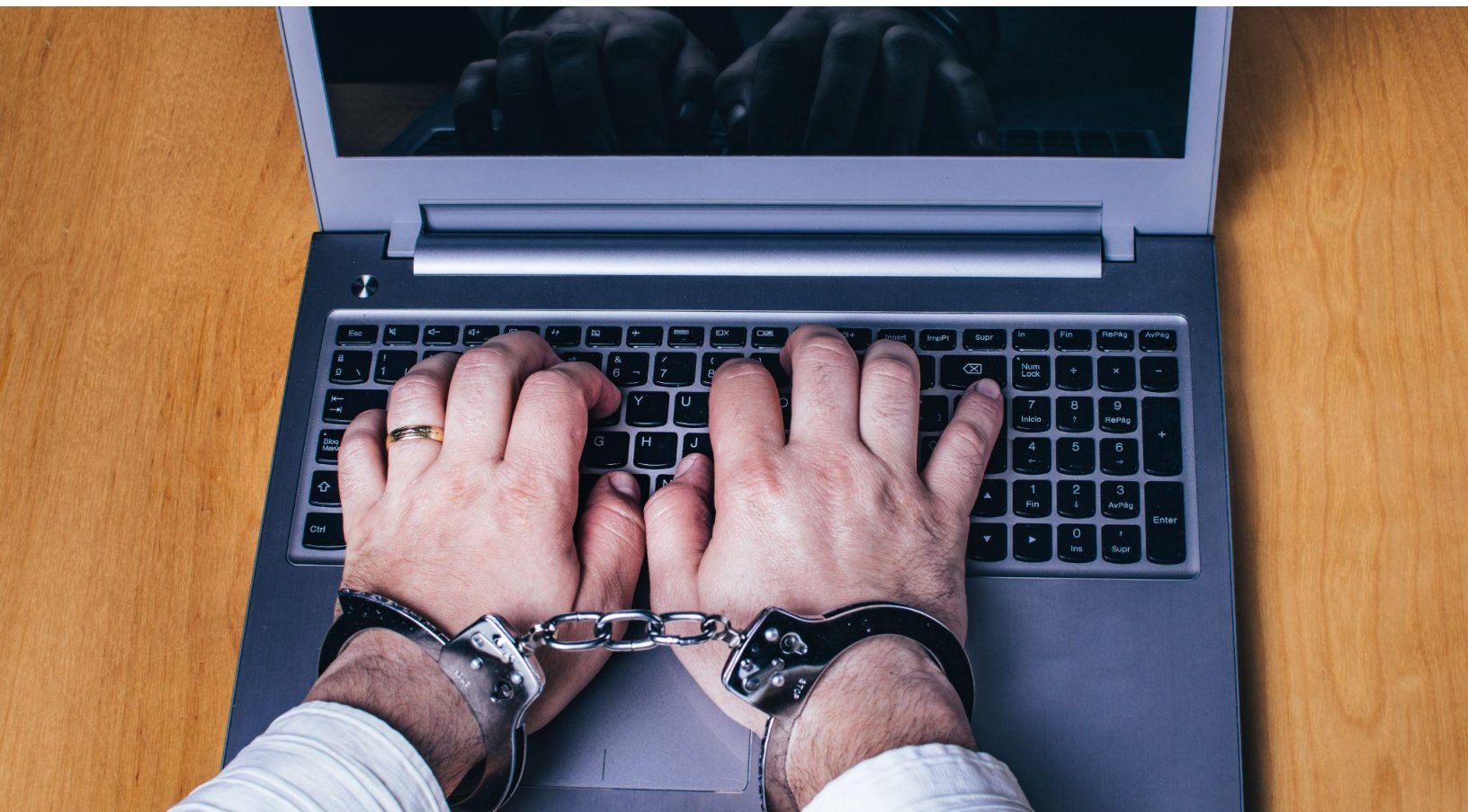
OmniIndex

With over 120 countries having regulations and countless industry-specific rules, the data landscape is a complex maze. While data protection is essential, these new regulations are causing headaches at both a board, and innovation level.

Big data is the lifeblood of modern business. Analytics and distribution are the heart of decision-making and profit. But new restrictions are forcing companies to rethink how – or even if – they can handle sensitive data.

This challenge is intensified yet further because of the need for these regulations, with cyberattacks on the rise and the global average cost of a data breach reaching record levels.

A study highlighted this dilemma. While acknowledging the need for regulation, it warns that the uncertainty around future rules is creating a technological divide with not everyone feeling able to invest or keep up with requirements:

"Some businesses have started to take the view that the cost of satisfying such strict privacy compliance obligations is too high to justify, until the product is well established. As a result, users located in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in their jurisdictions."

https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws

A Global Data Protection Framework

Data protection hinges on two critical pillars: governance and security. By mastering these, organizations can effectively manage data risks and keep confidential data private.

Data Governance:
The Challenges

Data governance ensures data is used ethically, legally, and strategically. Key principles include lawful processing, clear data purposes, and data minimization. Data Protection Officers support compliance with regular audits and threat detection.

However, traditional IT infrastructures often struggle with data mapping and classification, hindering efficient data access and analysis, impacting productivity. Also, to properly assess and manage data, staff have to be given undesirable levels of access.

Data Security:
The Challenges

Data security safeguards sensitive information. Robust infrastructure, including encryption and secure data centers, is crucial. Essential features include: access controls, regular audits, incident response plans, and employee training.

Legacy infrastructure often lacks advanced security features like homomorphic encryption and real-time threat detection, increasing vulnerability and hindering productivity through downtime and data recovery efforts with data exposed while searched or analyzed.

OmniIndex

PostgresBC:
The Confidential Data Solution

OmniIndex

Data Governance:
The PostgresBC Solution

Immutable and decentralized blockchain storage provides a tamper-proof audit trail, simplifying data mapping and classification, while eliminating the risk of accidental or malicious data corruption or loss.

What's more, PostgresBC's AI-driven classification of fully encrypted data enhances mapping and classification accuracy, while advanced AI search of encrypted data accelerates data discovery and analysis without compromising security.

Uniquely, super admins/super users manage the system without accessing underlying data, upholding the principle of least privilege with them unable to read the encrypted data.

Data Security:
The PostgresBC Solution

PostgresBC's blockchain and patented encryption technology ensure maximum data security with data never having to be left decrypted and exposed, preventing breaches and ransomware while guaranteeing uptime. This includes for AI analytics and use in third-party tools including Google Looker and Microsoft PowerBI.

Threat Detection Built in

PostgresBC also has infosecurity and advanced real-time threat detection built into the data platform thanks to OmniIndex's award-winning AI engine and Web3 architecture.

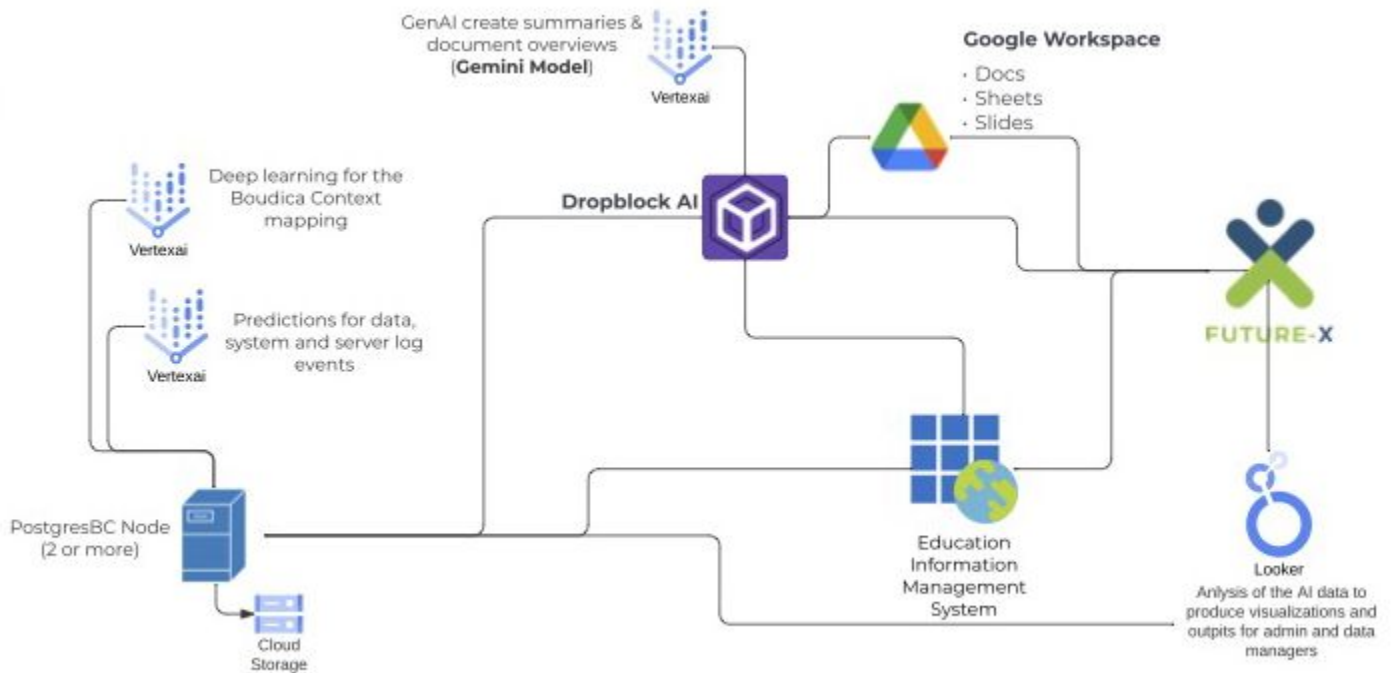# OmniIndex

Encrypted Log File Intelligence

Traditional log management solutions often compromise data security by handling log files in plaintext, increasing the risk of breaches. Additionally, reliance on external tools introduces potential vulnerabilities by adding an additional point of access into the decrypted data.

PostgresBC offers a secure, integrated approach to log management and analysis. By employing advanced homomorphic encryption, log files remain encrypted throughout their lifecycle, mitigating data exposure risks.

Meanwhile, the platform's AI engine, Boudica, is capable of extracting meaningful insights directly from encrypted data, enabling threat detection and analysis without compromising confidentiality.

Furthermore, PostgresBC's architecture allows seamless integration with popular analytics tools, providing flexibility in data exploration while maintaining data privacy and security with encrypted log files visualized for actionable insights in tools including Google Looker and Microsoft PowerBI.

OmniIndex

Customer Architecture Diagram

Future-X Education are one of OmniIndex's largest customers. They use the PostgresBC data platform to securely and compliantly store the educational data of students and teachers in Nigeria and analyze that fully encrypted data with Google Looker and Gemini AI as well as OmniIndex's AI and ML.

They are subject to strict data regulations and compliance requirements and require complete encryption and Web3 security to maintain confidentiality.

This diagram shows data stored within PostgresBC with integrations to:

- Google Workspace (Via Dropblock - the OmniIndex Add-on for Workspace)
- Vertex AI Gemini Model
- Vertex AI Deep Learning
- Vertex AI Training
- Looker Analytics

PostgresBC
The Web3 Data Platform

Please get in touch to learn more about the OmniIndex Platform and our confidential data solutions.

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