AI Threat Intelligence

Actionable AI Threat Intelligence for your files and data from Fully Encrypted Log Files

OmniIndex

White Paper

OmniIndex

The Log File Challenge

A key way to gain threat intelligence is through analyzing log files. This is because they provide a detailed record of system activity, enabling you to identify and predict security incidents. However, log files also offer a dangerous repository of information for potential attackers, meaning they need to be constantly protected.

The Log File Solution

Only OmniIndex enables logs to remain encrypted at all times even while being analyzed with AI/ML. This ensures they're protected while still enabling real-time actionable AI intelligence.

OmniIndex

How It Works: Security & Intelligence

1: Data Collection

Open Telemetry libraries collect log data.

2: Data Encryption

Data is encrypted with our homomorphic encryption.

3: Real-Time Integration

Encrypted data is exported in real-time to your storage.

4: Security & Privacy

Data is stored in an immutable and decentralized blockchain.

OmniIndex

5: Real-Time Threat Intelligence & Insights

Encrypted log files can be queried using familiar SQL commands.

Our AI Chatbot, Boudica, also enables you to ask natural language questions and receive meaningful answers directly from your encrypted data. As it is a private SLM model, no data is shared externally with none of your private data ever exposed.

You can also add your encrypted log files to all leading tools to conduct further analysis and data visualizations. This includes using the Dropblock extensions for Google and Microsoft to use BigQuery or PowerBI.

OmniIndex

Log File Intelligence Case Study

Cross River State in Nigeria is using OmniIndex's log file intelligence 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 as the data platform for their Educational Management System.

OmniIndex

The Problem

Educational data is highly sensitive and regulated. As such, it is crucial to have a transparent record of data access and to identify any potential threats/vulnerabilities in the database while keeping that information confidential and secure.

The Solution

The EMIS (Educational Management Information System) was migrated to OmniIndex PostgresBC and our log file threat intelligence was therefore able to run automatically on the fully encrypted data to provide real-time threat intelligence and ensure confidentiality.

They also use the Dropblock file system and extensions as well as our compliance intelligence.

OmniIndex

Potential Threat Intelligence

Given the sensitive nature of educational data, it's crucial to monitor log files for any activities that could indicate potential threats. Here are a few examples of potential actionable security insights possible with LoggerBC from the data and file systems.

1. Unauthorized Access Attempts:

- **Brute Force Attacks:** Frequent failed login attempts from unusual IP addresses or locations could suggest a brute force attack is underway.
- **Unauthorized User Access:** Detection of logins by users who should not have access to the system or attempts to access restricted resources.

2. Data Exfiltration:

- **Large Data Transfers:** Unusual spikes in data transfers, especially outside of normal business hours, could indicate data exfiltration attempts.
- **Suspicious File Downloads:** Monitoring for downloads of sensitive data files by unauthorized users or to unusual destinations.

3. SQL Injection Attacks:

- **Error Messages or Unexpected Behavior:** Unusual error messages or unexpected behavior in the application could be indicative of SQL injection attempts.
- **Suspicious Query Strings:** Analyzing query strings for potentially malicious input.

4. Malware Activity:

- **Unknown Processes or Files:** Detection of unknown processes or files running on the system, which could be signs of malware infection.
- **Network Traffic Anomalies:** Unusual network traffic patterns, such as excessive outbound connections or suspicious DNS requests.

5. Insider Threats:

- **Privilege Abuse:** Monitoring for instances where users with elevated privileges are accessing data or performing actions they shouldn't have permission to do.
- **Unusual Access Patterns:** Detecting unusual access patterns from trusted users, such as accessing sensitive data outside of normal working hours or from unusual locations.

6. Data Breaches:

- **Data Loss or Corruption:** Identifying instances of data loss or corruption, which could be indicative of a data breach.
- **Unauthorized External Access:** Detecting unauthorized access to the system from external IP addresses.

OmniIndex

Technology Stack

OmniIndex's threat intelligence utilizes our award-winning and patented technology. This includes our homomorphic encryption, blockchain data storage, and native SLM AI engine Boudica.

OmniIndex

Fully Homomorphic Encryption

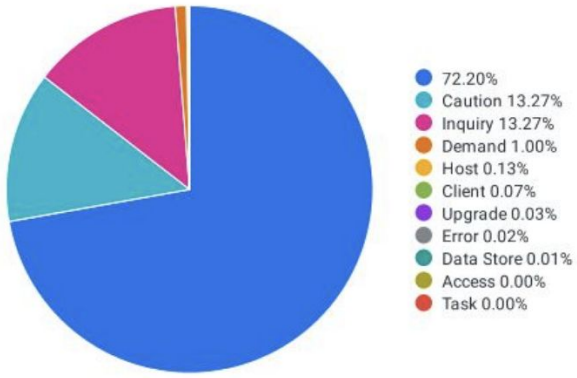
OmniIndex's patented fully homomorphic encryption provides the only commercial solution for searching and performing computations on fully encrypted log files.

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

This means data does not have to be decrypted and left vulnerable to exposure through accidental or deliberate actions.

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

OmniIndex stores the encrypted log files in PostgresBC: The OmniIndex zero-trust blockchain data platform.

The security and privacy benefits of blockchain revolve around the enhanced integrity and security of the data with it being tamperproof, and the decentralization of the network making it more difficult to attack.

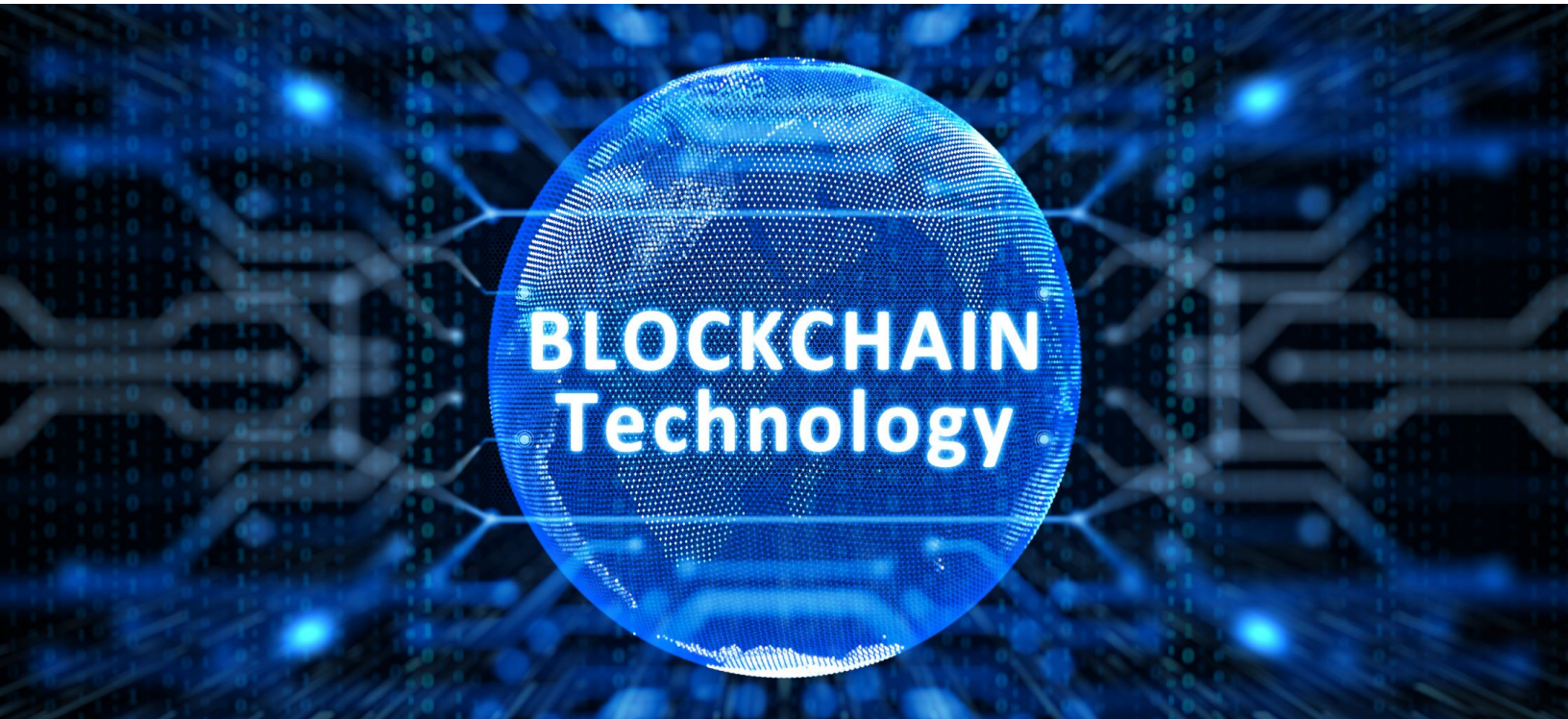
When combined with homomorphic encryption and our zero-trust access, the threat of ransomware attacks is eliminated.

*This is the same whether you are using PostgresBC, or Dropblock.

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.

What's more, 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 private AI engine has a number of direct benefits for users.

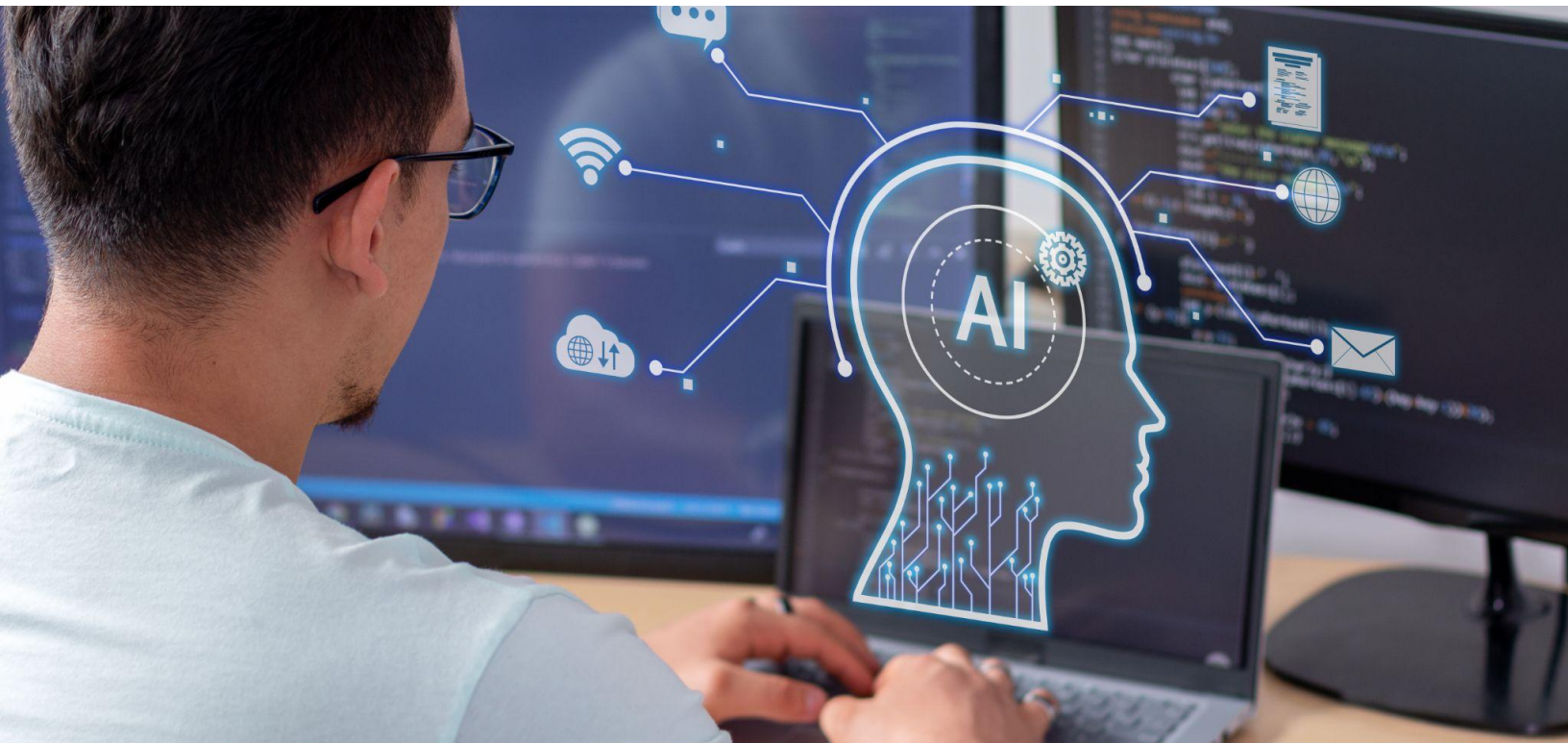
1: Privacy
Boudica is a private and native AI solution. This means user data is not shared externally of the system to generate answers, and there is no third-party access to the user's queries or answers.

Finally, all data is encrypted while it is being subjected to AI analytics.

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 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 in order to be used and can be adapted to offer specialist services in different languages and areas simply by changing their ontologies. They also require less powerful hardware to run.



For more information, including a demo request or personalized pricing, please get in touch.

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