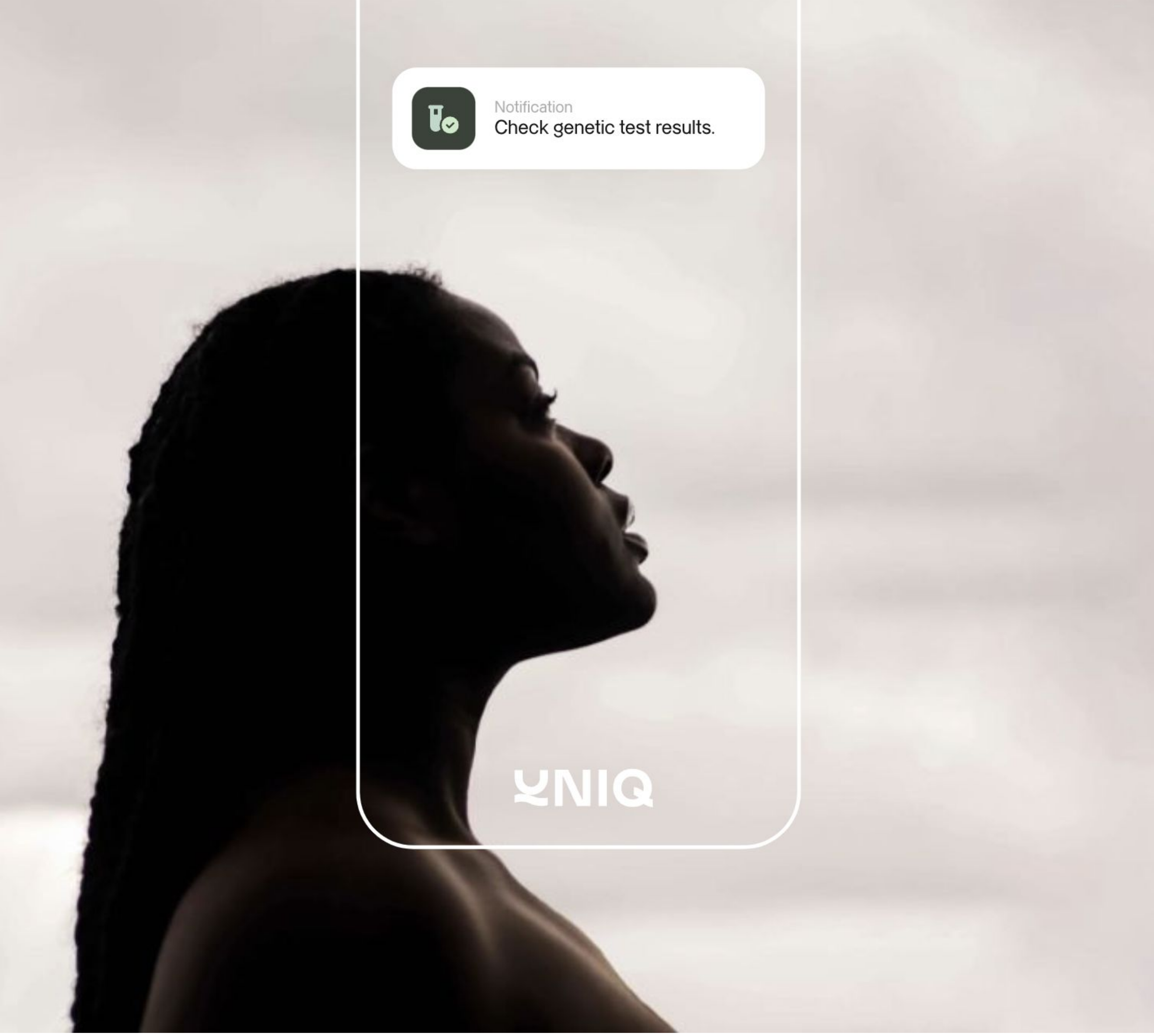


Health data analytics and security

An OmniIndex Customer Use Case: Uniq Health App

OmniIndex

White Paper

Use Case:
How OmniIndex secures Uniq’s regulated and confidential health data.

“Uniq is a deep-dive into the inner you, with easy at-home Gut, Blood and DNA tests, AI generated analysis with personalised recommendations, disease risk insights, and behavioural adaptations.”

They are using OmniIndex’s patented and award-winning technology to ensure they can provide these vital personalised insights to their customers without compromising the security, privacy, or integrity of the sensitive and regulated health information.

This paper explores this use case, outlining the OmniIndex technology that makes this possible.

OmniIndex

Secure, Encrypted, Data Storage

OmniIndex's patented technology enables all data to be encrypted and stored with ransomware inoculation. This includes structured and unstructured data.

Constant Encryption

OmniIndex provides the only solution enabling analytics of fully encrypted data. This FHE technology is protected by multiple international patents including 'secure database searching' and ensures **data is never exposed as it remains encrypted at rest, in transit, and in use.**

The encrypted data is stored in the company's own blockchain hosted on Google Cloud, and only Uniq's authorized users are able to access and decrypt this data: not OmniIndex, nor Google.

Two key security and privacy benefits of this storage and encryption are that it ensures **no unauthorized access** to the files or data, and that **all stored data is immutable**.

Each of Uniq's customers and groups are then 'sandboxed' into their own chain. This means it is impossible for one user within an organization to accidentally or deliberately access another's data with each attempt automatically validated and checked with OmniIndex's robust zero-trust access controls and SLM AI key management.

As files and data are stored across multiple nodes instead of being in one location, data is not lost if there is a corruption or technical issue because the remaining nodes will automatically reshare the data to secure the network once more.

These innovative technologies provide Uniq with critical **ransomware inoculation**. This is because an attacker cannot access files or data unless they have been given permission, and the immutable data cannot be encrypted with an attacker's own encryption to overwrite it and hold it to ransom.

OmniIndex

Zero-Trust File Access

Zero-trust means no trust, no access. Every device, user, or network that attempts to access Uniq's files and 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.**

This is important because 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. Especially in healthcare.

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.

How it works:

Continuous Verification:
Every request is validated and authenticated before granting access.

Micro-segmentation:
The network is divided into smaller, isolated segments to limit the spread of potential attacks and ensure nobody inside a system has complete access.

Least Privilege Access:
Users are granted only the minimum necessary permissions to perform tasks.

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.

What's more, OmniIndex mitigates the risks associated with super user or admin privileges by using our patented FHE to enable administrators to do their job without actually being able to read the data.

OmniIndex

Threat Intelligence

OmniIndex is the only solution enabling real-time AI threat intelligence from encrypted log files.

Unlike other log management and analysis tools, OmniIndex uniquely ensures log files are never left vulnerable to attack through decryption. This is because OmniIndex's patented and powerful homomorphic encryption enables data to remain encrypted at rest, in transit, and in use. What's more, log files are stored in their own secure blockchain to ensure protection from ransomware attacks and exposure.

Our native and private AI, Boudica, then analyzes the encrypted log files to identify patterns, threats and vulnerabilities in the system. These can then be added to tools such as Google Looker or Microsoft PowerBI for live alerting, detailed analysis and visualizations.

Potential Security Insights:

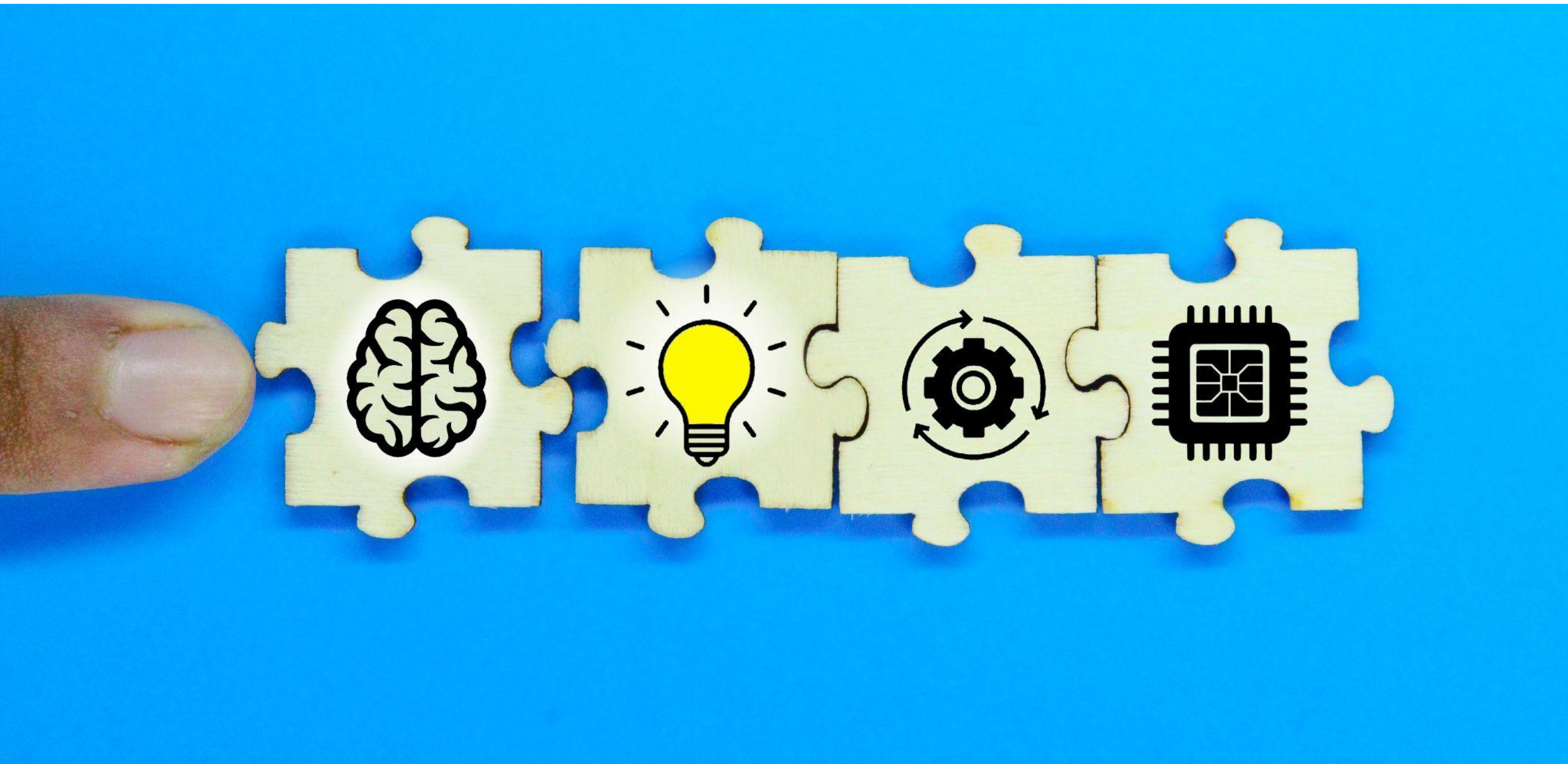
Brute Force Attacks:
Frequent failed login attempts from unusual IP addresses or locations could suggest a brute force attack is underway.

Unauthorized User Access:
Detection of logins by users who should not have access to the system or attempts to access restricted resources.

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.

Unusual Access Patterns:
Detecting unusual access patterns from trusted users, such as accessing sensitive data outside of normal working hours or from unusual locations.



OmniIndex

Secure, Encrypted, Data Analysis

OmniIndex's patented technology enables all data to be searched and analyzed in real-time even while encrypted: including DICOM and other medical images.

OmniIndex

Medical Image Analytics

OmniIndex uniquely enables organizations like Uniq to analyze fully encrypted health records and images. This includes the ability to fully encrypt and analyze DICOM.

DICOM stands for Digital Imaging and Communications in Medicine. These images contain many different types of data including device usage and patient administration information. This type of information is commonly used in Healthcare and Life Science, however not usually from the DICOM records themselves. This is because of the confidentiality and privacy requirements of these heavily regulated health images

OmniIndex ensures compliance by protecting the privacy and security of this data by keeping it encrypted at all times, and storing it in an immutable blockchain to eliminate third-party access and ensure the data's integrity.

One example use is that DICOM images can offer valuable insights into device utilization. This information is potentially valuable for managing expensive medical imaging equipment. However, it is very rarely used due to the compliance complications of accessing it.

OmniIndex enables companies to analyze this encrypted data with Boudica: OmniIndex's award-winning native SLM AI engine. Doing so can reveal usage patterns, identify potential bottlenecks, and optimize workflows within healthcare practices. It has also been shown to aid the efficiency of patient care by being able to rapidly discover who had what scan when, and automate alerting of what follow-up procedures are required.

Furthermore, the data can be added to any workflow in a secure and compliant way with OmniIndex Dropblock.

In the case of Uniq, they are using Dropblock to add encrypted gut microbiome data to their Google Workspace workflow to gain real-time insights and manage their client data securely and compliantly with fully redacted PII.

PII Redaction

Dropblock's automatic PII redaction enables Uniq to redact PII data (telephone numbers, social security numbers, zip codes, email addresses) to ensure none of this regulated and confidential information is exposed when a file is shared or analyzed. This is crucial when it comes to adding health records to cloud workflows for collaboration and analytics.

The redacted data is encrypted with FHE and stored in the user's own blockchain storage. Only authorized users are then able to unredact that data, meaning they can share the file with others with complete confidence the redacted information cannot be exposed.

As the redaction is done using military grade encryption, any confidential information can be protected with it impossible to read without the key.

PII can be redacted automatically when a file is saved, or it can be redacted while the file is being worked on by using Dropblock's AI chatbot Boudica to find any PII data and then redact it.

The Dropblock AI can be set at a system level to automatically redact set information within all files in an organization's workflow, or within set access levels and groups. This can be configured by the admin in a file called patterns.conf.

The admin can type any patterns that they are looking for and the system will look for these patterns and then ascertain whether it needs to redacted or not.

For example:

```
#US SSN
^(?!(.)(\\1|-)+$)(?!000|666|9..)(?!...-?00)(?!.*0000
$)\d{3}(-?)\d\d\3\d{4}$
```