OmniIndex Dropblock

The confidential file system to secure your workflow and ensure regulatory compliance

OmniIndex

White Paper

OmniIndex Dropblock is a Web3 file system designed to address the security and compliance challenges that prevent organizations from fully leveraging cloud-based tools and analytics.

Dropblock integrates with Google Cloud, Microsoft 365 and other cloud workflows to enable users to store files on their own blockchain, process it with fully homomorphic encryption (FHE), and perform analytics while data remains encrypted.

It also works independently, allowing you to sign into your own blockchain file storage from anywhere – including mapping to the file on your desktop or signing in online.

OmniIndex's combination of patented and award-winning technologies provides ransomware inoculation for users and enables them to use their most regulated data in the cloud compliantly.

This White Paper introduces the Dropblock solution and why it is necessary in 2025.

Zero-Trust Access

Real-Time Integration

Homomorphic Encryption

Blockchain Storage

OmniIndex

The Cloud Problem

Traditional cloud solutions, while enabling collaboration and productivity, present security and compliance risks for highly sensitive data. This is because they necessitate data exposure to multiple entities, including employees and cloud providers. They also require files to be stored in their own centralized systems.

Furthermore, the need to decrypt data for search and analysis exposes it to potential vulnerabilities, as cloud providers maintain control over decryption keys and have access to stored files.

The Dropblock Solution

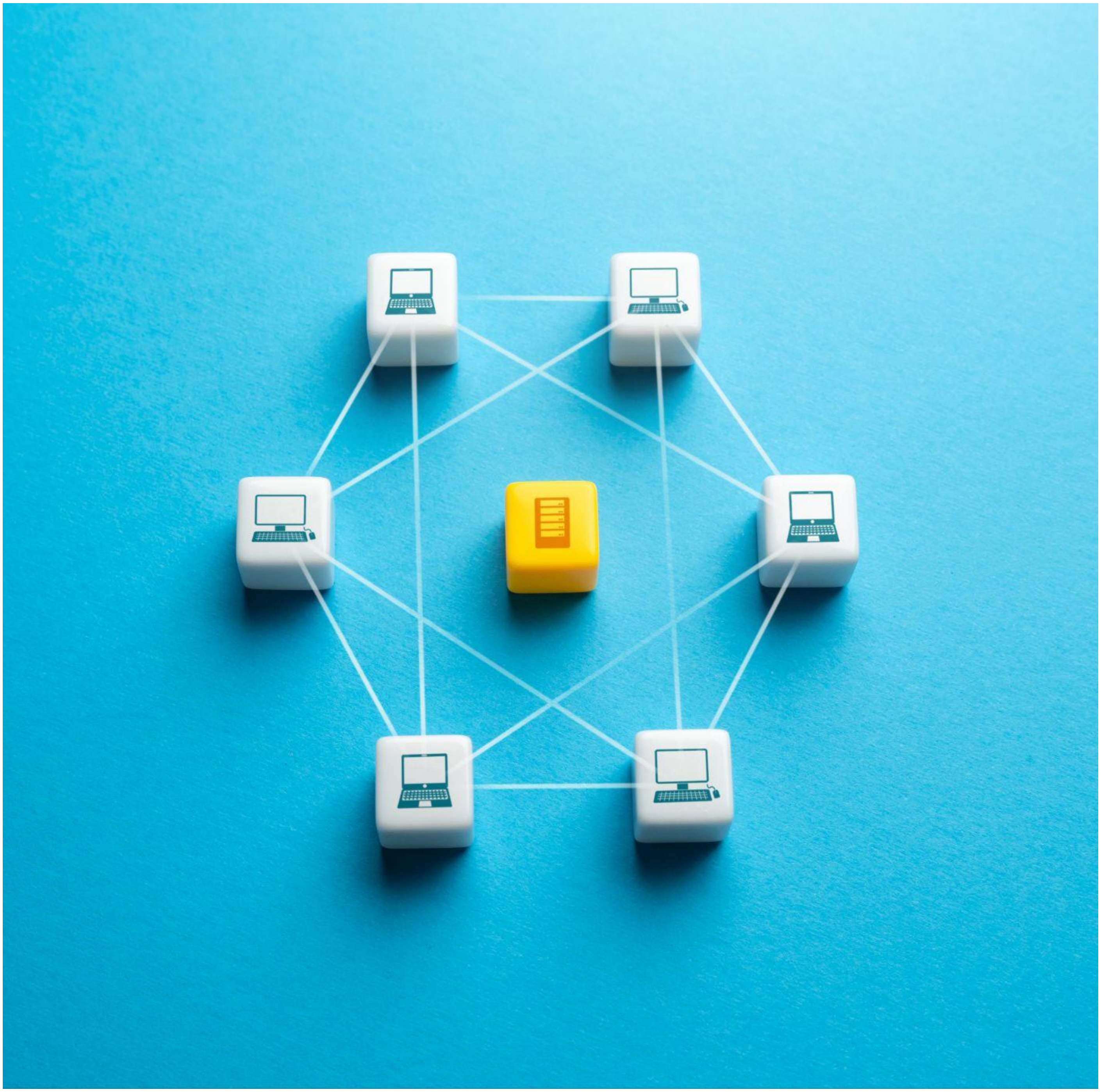
With Dropblock, files never leave the customer's control and data remains encrypted at all times with keys only the customer has access to. It is also immutable, meaning it cannot be manipulated.

This means there is no third-party access, and no risk of exposure.

OmniIndex

Dropblock File & Data Security

OmniIndex's award-winning cybersecurity technology inoculates files from ransomware attacks, and ensures data is private and compliant in the cloud.



OmniIndex

Secure Web3 File Storage

Dropblock is 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.**

Encrypted data is stored in the customer’s own blockchain which is hosted on Google Cloud or another location of the customer’s choosing. **Crucially, only the user is able to decrypt that data – not OmniIndex nor the chosen host.**

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

Each user's files and data are also ‘sandboxed’ into their own chain with any customer data then also sandboxed. 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-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 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 your 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.

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

Automated Compliance & Security

OmniIndex's award-winning AI technology provides automated PII protection and threat intelligence for files stored in Dropblock.

PII Redaction

Dropblock's automatic PII redaction enables an organization and user 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 stored or shared.

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 encryption key or authorization.

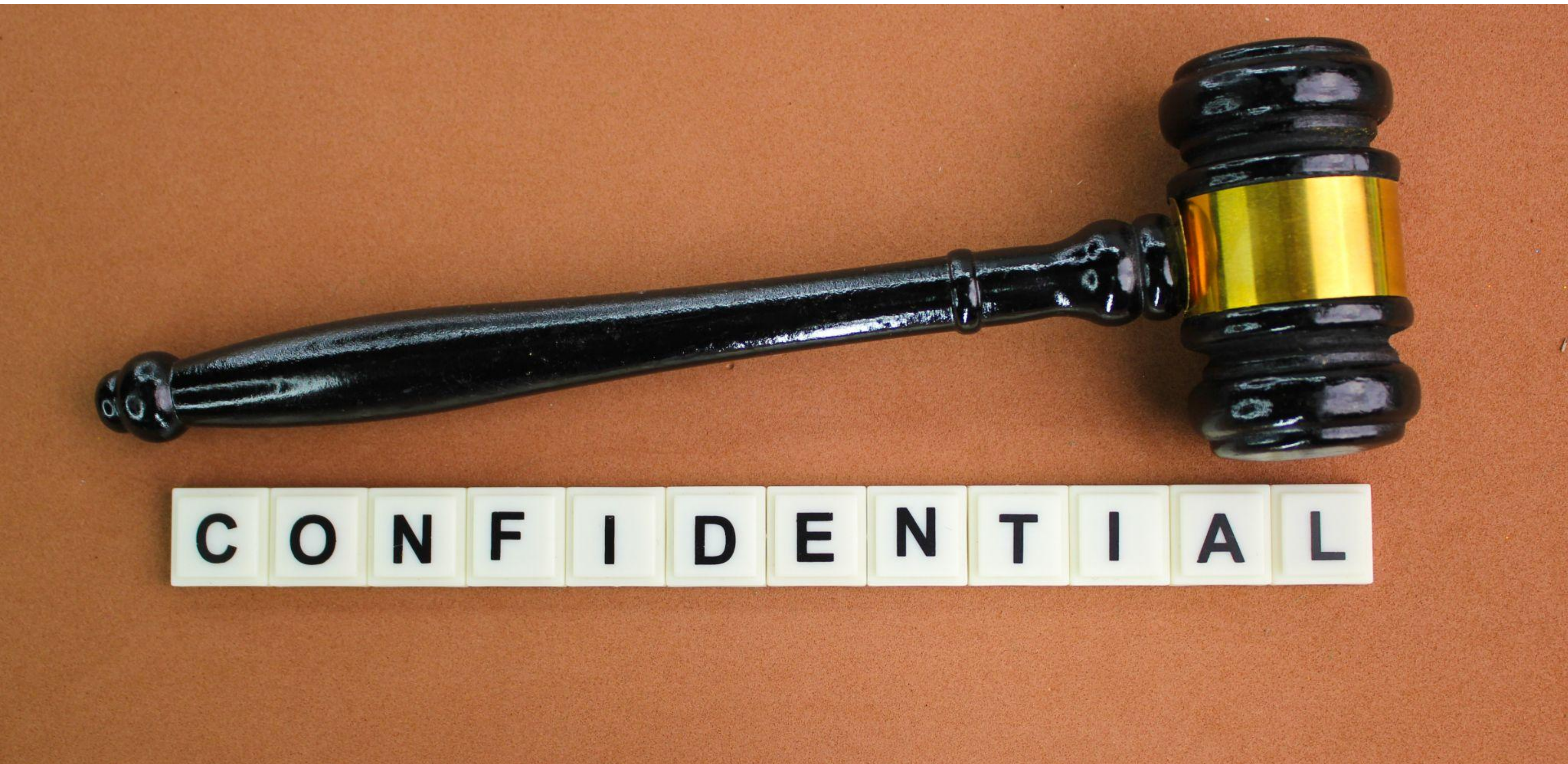
PII can be redacted automatically when a file is saved, or it can be redacted while the file is being worked on by using Dropblock's AI chatbot Boudica to find any PII data and then redact it.

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
$)\d{3}(-?)\d\d\3\d{4}$
```



Threat Intelligence

Dropblock is the only solution enabling real-time AI threat intelligence of your files and data from encrypted log files.

Unlike other log management and analysis tools, Dropblock 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 your own secure blockchain to ensure protection from ransomware attacks and exposure.

Our native and private AI, Boudica, then analyzes your encrypted log files to identify patterns, threats and vulnerabilities in your 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:

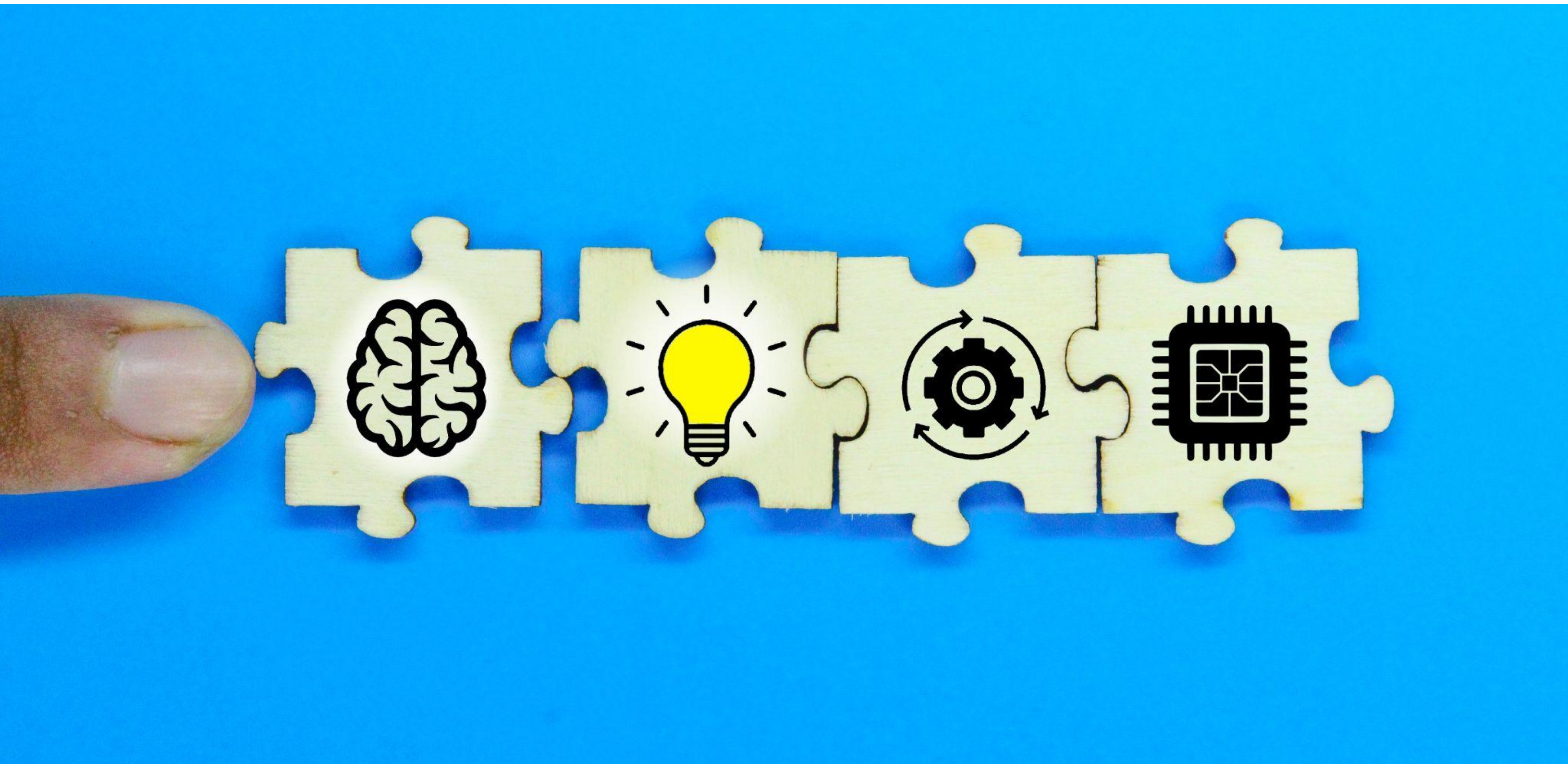
Brute Force Attacks:
Frequent failed login attempts from unusual IP addresses or locations could suggest a brute force attack is underway.

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.



Dropblock is available in a number of different plans to suit all needs. This includes a **free Developer account** for a single user, and the ability to add additional user packs.

Small Business – 250 Users – $1250 monthly subscription

Medium Business – 1,500 Users – $6,375 monthly subscription

Enterprise – Unlimited Users – $25,125 monthly subscription

Please visit our website or get in touch with us today to book a discovery meeting and learn more about the OmniIndex solutions for confidential data.

Zero-Trust Access

Real-Time Integration

Homomorphic Encryption

Blockchain Storage

OmniIndex

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