OmniIndex Dropblock

The inoculated & intelligent file system to secure your workflow and ensure regulatory compliance

OmniIndex

White Paper

OmniIndex Dropblock is a secure 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, inoculate them from attack, and perform analytics while data remains fully encrypted.

It also works independently, allowing you to sign into your own Dropblock 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 enables analytics of fully encrypted files inside the file store with AI. 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 files are stored in the customer’s own blockchain hosted on the cloud or on-premises. **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**.

Within a company, each user's files and data are ‘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.

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

OmniIndex

Threat Intelligence

Dropblock enables real-time AI threat intelligence of your files and data 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 our 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.

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.

OmniIndex

Compliance Intelligence

Dropblock also enables real-time AI-driven compliance intelligence of your fully encrypted files inside the file store.

Dropblock's award-winning AI (Boudica) scans files in real-time to identify any breaches based on the parameters you set. This means Boudica can be customized to your own specific industry, region or indeed company to ensure accurate compliance screening.

Furthermore, because files are stored in OmniIndex's web3 storage, there is an immutable log of all access attempts, edits and file shares that are also included as part of the intelligence. These audit logs are analyzed in an encrypted state to ensure no exposure of the sensitive content they contain.

Potential Compliance Insights:

Data Residency Breaches
Identification of files stored or processed in unapproved geographic locations, violating data residency regulations.

PII Data Exposure
Detection of PII data that has not been encrypted in a file before it is stored or shared. (See also Dropbox's automated PII redaction.)

Privacy Regulation Infringements
Identification of potential violations of privacy regulations, such as GDPR or CCPA, including improper collection, storage, or use of personal data.

Audit Trail Irregularities
Detection of gaps or inconsistencies in audit logs, suggesting potential tampering or non-compliance with audit requirements.

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

AI Semantic Search

Semantic search offers a significant advantage over traditional keyword-based search, particularly in enhancing user productivity and data governance due to its enhanced results and efficiency.

This is because semantic search understands the intent and meaning behind a query, rather than simply matching keywords, enabling users to find relevant information even if they don't know the exact terms used in the file or content.

When compared to traditional keyword search, semantic search results are far more optimized with fewer inaccurate results.

OmniIndex's patented encrypted semantic search for secure compliance

OmniIndex adds the further benefit of being able to uniquely search encrypted content.

This is possible due to the combination of our patented homomorphic encryption technology with our Boudica AI engine which enables NLU search capabilities.

In other words, you can ask Boudica questions of your encrypted content in normal language and it will search for you.

For example: "*what PII data is within this document?*"

It will then find that content for you based on its ability to understand context and meaning.

This elevates the previously simple search feature into being an intelligent & secure solution for compliance insight generation.

Dropblock is available in a number of different plans to suit all needs. This includes our enterprise plans for large companies to store all user file and manage it securely and intelligently, as well as our individual droplock.online accounts for 2GB free file storage.

Please visit our website or get in touch with us today to book a discovery meeting and learn more about OmniIndex's inoculated and intelligent data and file solutions.

Zero-Trust Access

Real-Time Integration

Homomorphic Encryption

Blockchain Storage

OmniIndex

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