# NOTRACK

We protect your documents and respect your privacy

In the digital era, sensitive documents face constant risks, even when measures such as VPNs, secure servers, and robust passwords are implemented. These practices, while helpful, are often insufficient to ensure complete protection.

The challenges range from the loss of local devices to unauthorized access during data transfer. This highlights the need for advanced solutions that ensure privacy and absolute control over information.

**Several scenarios exemplify this problem:**
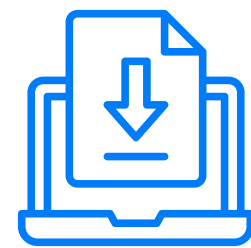
Downloading information on personal computers

Even when information is stored on secure servers, downloading it to a local PC for convenience exposes the data if the computer is lost or hacked.

Backups on local devices or USB drives

Storing backups on local devices or using USB drives to transport information creates a risk if these devices are lost or stolen.
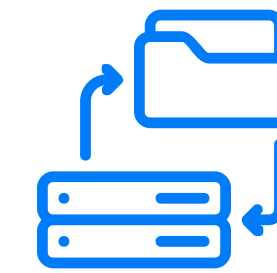
Data transfer between devices

Even the slightest data transfer can leave 'digital footprints' vulnerable to exploitation.

Our Solution

NoTrack is a comprehensive solution designed for individuals, businesses, and organizations seeking maximum privacy and control over their information.

It provides a robust and reliable environment for managing sensitive data, protecting communications, and ensuring security in every digital interaction.

How do we do it?

We combine advanced technologies such as blockchain, end-to-end encryption, and multi-factor authentication (2FA), providing the administrator with full control over information and access.

Take control

Unlock a world of possibilities while keeping your privacy fully protected.
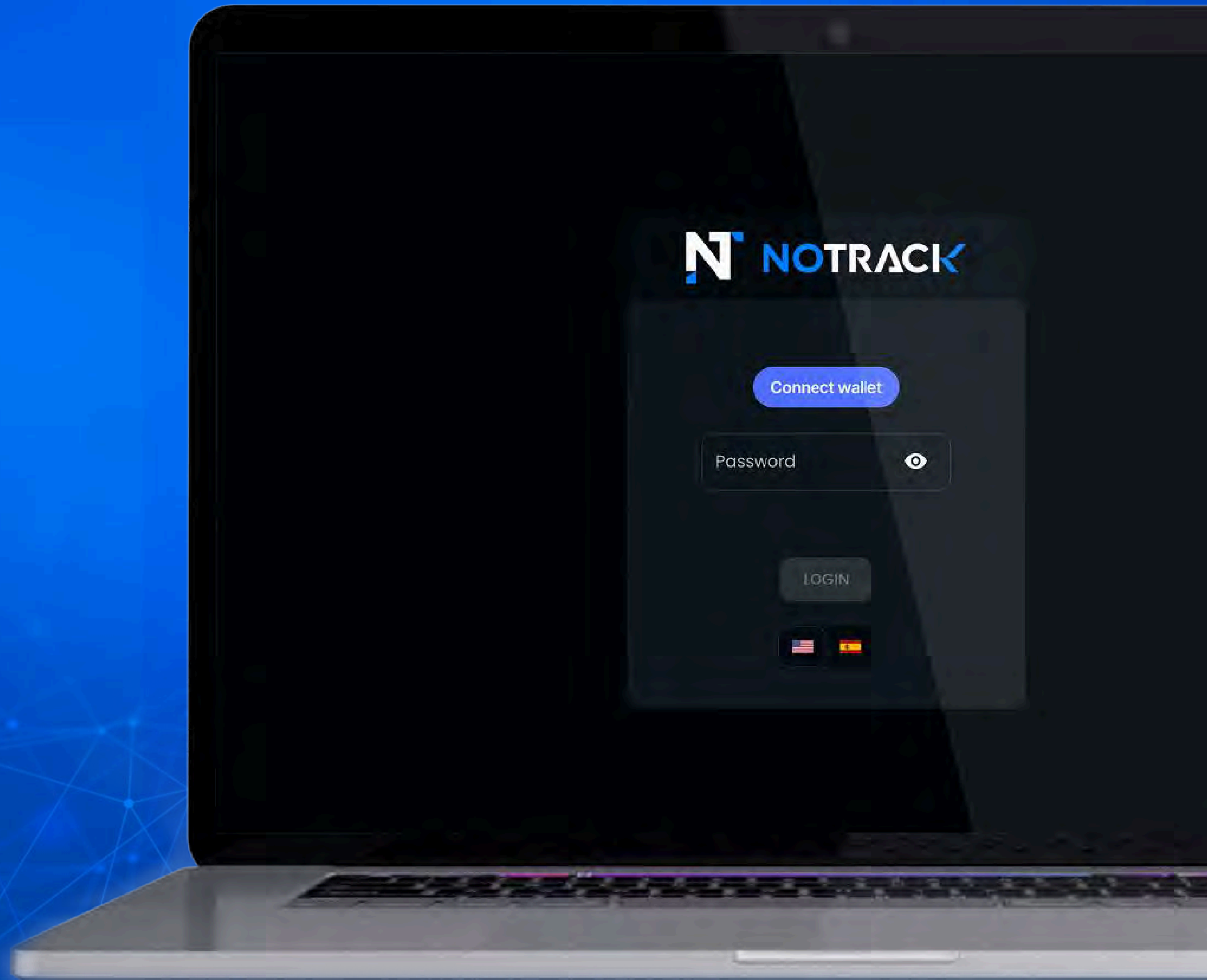
Our Solution

Key Features:

Hidden Access: Access is achieved through a "screen" web interface that conceals the true entry to Web3.0.

Dynamic Access: The access URL changes daily following a predefined logic known only to the administrator, significantly complicating unauthorized access.

Multi-Factor Authentication: Access requires:
- Wallet address.
- Password.
- Scanning a QR code with the phone linked to the wallet.

Smart Contract Validation: A Smart Contract validates user access by verifying the provided information and granting access to content based on permissions defined by the administrator.
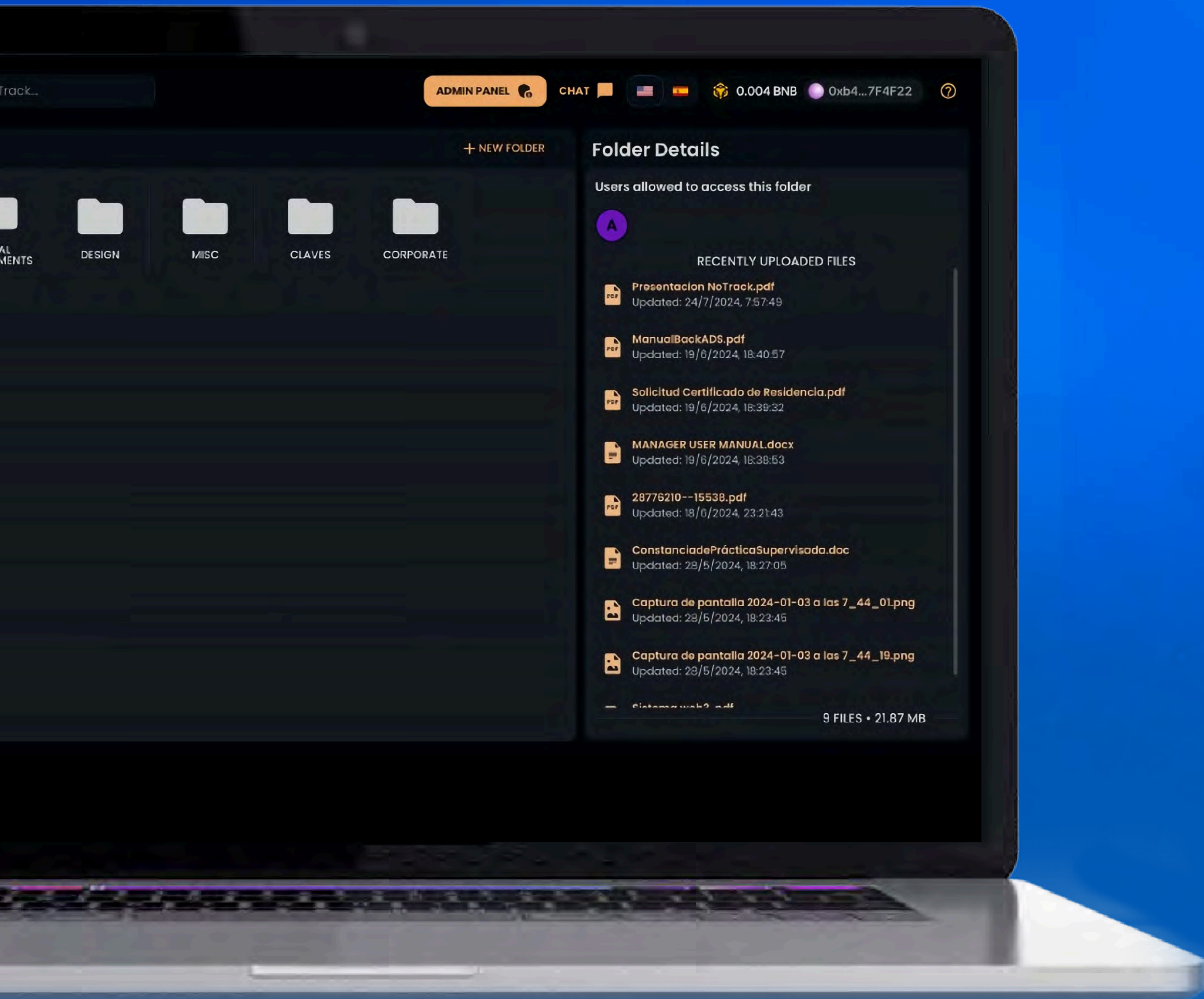
Our Solution

Key Features:

___

File Encryption: Files stored on the server are encrypted, adding an extra layer of security.

Periodic Server IP Change: The server's IP address hosting the encrypted files can change periodically, making its location even harder to pinpoint.

Inactivity Control: A configurable inactivity timer (3, 5, or 15 minutes) is implemented. If the user does not interact with the system within this timeframe, the session is automatically closed, preventing unauthorized access in case of unattended devices.

Secure Infrastructure:
- Hosted on secure servers.
- Exclusive access through a private VPN (single allowed IP).
- Communications protected with JWT (JSON Web Tokens) for all endpoints, except login, which is verified via the Smart Contract.

Advantages and Disadvantages of NoTrack

Strengths:

- **Extreme Security System** with Multiple Layers: Blockchain, encryption, and 2FA authentication.
- **Advanced Role and Permission Management:** Enables granular control over user access.
- **Exclusivity and Personalized Access:** Rotating URLs and wallet-based restrictions enhance privacy.
- **Unique Capabilities:** Encrypted chat and secure online editing.

Opportunities:

- **Increased Privacy Regulations** (e.g., GDPR): Rising demand for robust security solutions to comply with strict data protection laws.
- **Growing Demand from Businesses**: More companies are seeking integrated solutions to safeguard sensitive data.
- **Expansion in Tech and Legal Markets**: Opportunities in sectors where security and data protection are top priorities.

SWOT
NoTrack

Weaknesses:

- **Requires Technical Knowledge:** Advanced configurations demand a higher level of technical expertise.
- **Dependence on Blockchain Stability**: Certain operations rely on the stability and functionality of the blockchain network.
- **High Initial and Maintenance Costs:** More expensive compared to basic solutions, due to advanced infrastructure and security features.

Threats

- **Competitors with More Affordable Solutions:** Lower-cost alternatives or solutions with established integrations .
- **Resistance to Change:** Businesses relying on traditional methods may hesitate to adopt advanced systems.
- **Initial Distrust in Blockchain Technology**: Certain sectors may view blockchain with skepticism, slowing adoption.

Advantages and Disadvantages of Using NoTrack

Advantages:

- **Superior Data Protection**: Multi-level security with encryption and temporary sessions.

- **Real-Time Audit and Traceability**: Track changes instantly and accurately.

- **Prevents Information Leaks:** Integrated and secure system ensures data confidentiality.

- **Ideal for Key Sectors**: Tailored for industries like legal, financial, and technology development.

Disadvantages:

- **Learning Curve for New Users**: May require time to familiarize with the platform.

- **Internet Connection Requirement:** The system depends on stable internet access.

- **Wallet Access Needed for Login**: Users must have a wallet to authenticate and log in.

Problems Addressed by Its Implementation

Data leaks and vulnerabilities:

- **Solution:** Full protection through blockchain, encryption, and limited access.

Difficulty in managing roles and access in large teams:

- **Solution:** Advanced management of permissions and roles tailored to each user.

Loss of sensitive data due to theft or cyberattacks:

- **Solution:** Full encryption and automatic backups.

Regulatory concerns about data protection:

- **Solution:** Regulatory compliance through robust security standards.

Potential Competitors of NoTrack

Cloud Storage Solutions

Google Drive / Dropbox Business:
- Widely used in businesses and individual users.
- Focus on collaboration, but with less emphasis on advanced security such as blockchain.

Microsoft OneDrive:
- Integration with Microsoft 365 tools.
- It offers encryption in transit and at rest, but does not include systems like 2FA blockchain.

Secure Collaboration Platforms

Slack (with encryption)
- Internal communication tool with encryption options for messages and files.
- It does not have the robustness of an integrated data management system.

Microsoft SharePoint:
- Designed for companies with collaborative workflows.
- It offers advanced security, but does not integrate blockchain or wallet-based authentication.

Encrypted Data Managers

Tresorit:
- Enterprise-level security with end-to-end encryption.
- Focused on companies seeking high privacy in storage.
- It does not include blockchain authentication or dynamic access features.

Proton Drive:
- Offered by the company behind ProtonMail.
- Strong focus on privacy, but lacks advanced features like rotating URLs or custom roles.

Document Management Solutions

Box:
- Provides secure collaboration with data encryption.
- Lacks unique features like end-to-end encrypted chat and access through smart contracts.

Egnyte:
- Hybrid solution for cloud and local storage.
- Focused on businesses, but without innovations like blockchain or dynamic access like NoTrack.

Potential Competitors of NoTrack

Advanced Security Platforms

Vera Security:
- Granular control over file access and real-time encryption.
- **Focus on secure document management, but without blockchain functionalities.**

BlackBerry Workspaces:
- High security for business collaboration.
- **It offers traceability and control, but lacks blockchain multi-factor authentication like NoTrack.**

Specific Blockchain Solutions

Storj:
- Decentralized storage system based on blockchain.
- **Good focus on privacy, but less oriented towards businesses and end users like NoTrack.**

- Filecoin:
  - Decentralized cloud storage platform.
  - **Lacks a comprehensive approach for roles and permissions management.**

Differentiating Features of NoTrack

Despite the mentioned competitors, NoTrack stands out for:

1 Daily dynamic URL and logic known only by the administrator.

2 Access through authorized wallets and smart contracts.

3 End-to-end encryption with temporary decryption.

4 Encrypted chat exclusive for authorized users.

5 Advanced role and permission management (Admin, Manager, Viewer, Corporate, etc.).

Why NoTrack?

Blockchain 2FA

Authentication is based on a two-factor (2FA) system with blockchain. Users are linked to a smart contract through an authorized wallet, confirming the login through it. The contract verifies the user's status, and a password is required, blocking access after three failed attempts.

File Encryption

Uploaded files are encrypted and sent to a secure server of the administrator. They are only accessed through the application, temporarily decrypted during use, and re-encrypted afterward. This prevents third-party access, even by service providers.

Full Control

The administrator controls the application, managing user permissions, folders, file restoration, and the suspension/shutdown of the application.
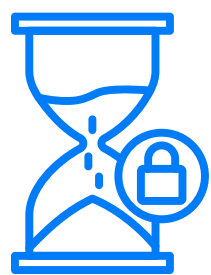
Encrypted Chat

An end-to-end encrypted chat is offered for users with authorized wallets. Messages are encrypted on the sender's device and decrypted only on the recipient's device, ensuring privacy.
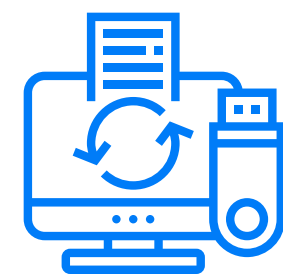
Why NoTrack?

Extreme Security gives the administrator full control against threats. It offers two options:
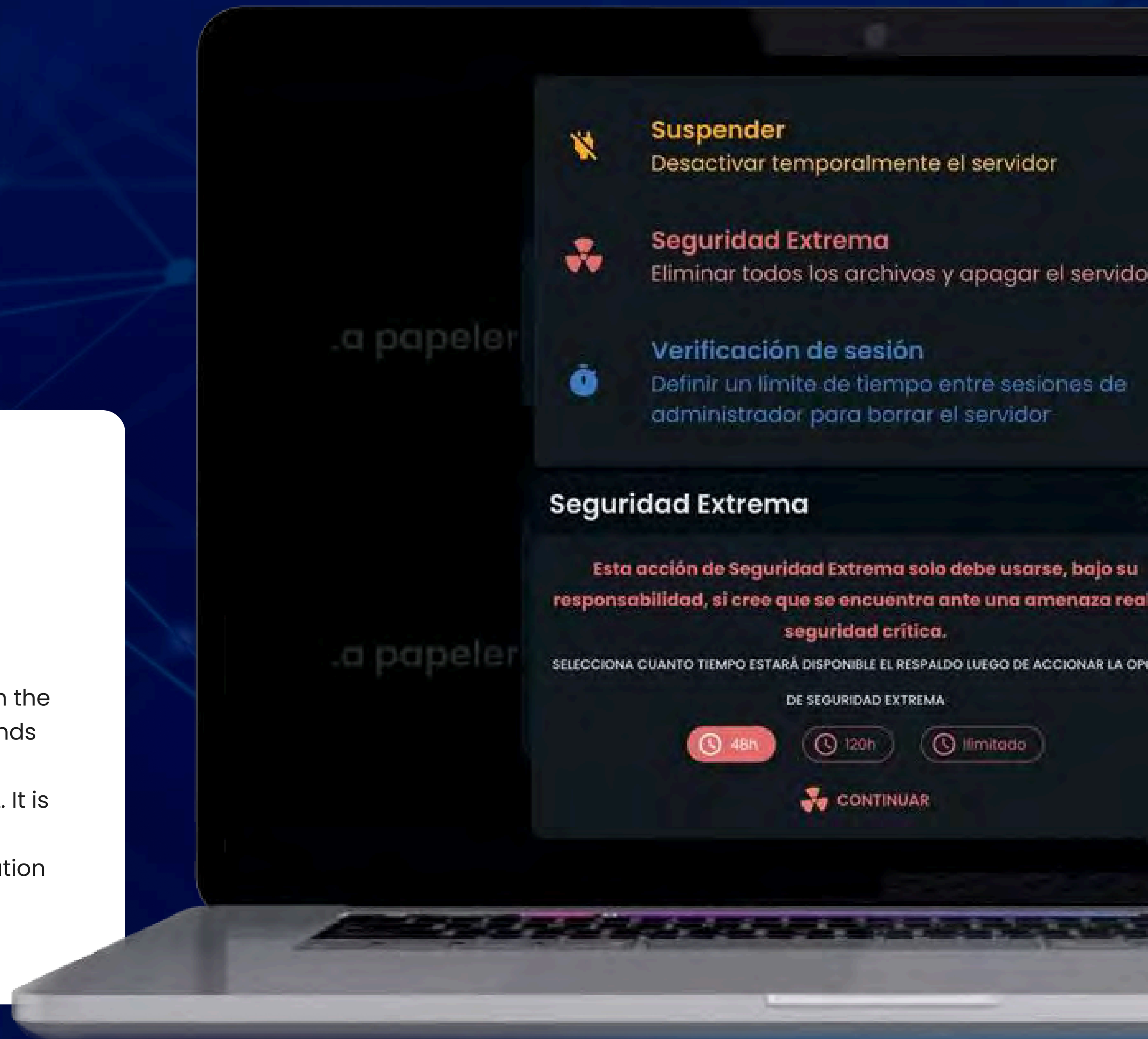
Temporary Lockout

It suspends access to the files, keeping them inaccessible until the administrator restores them. It is a quick measure to "freeze" access in case of suspicion.
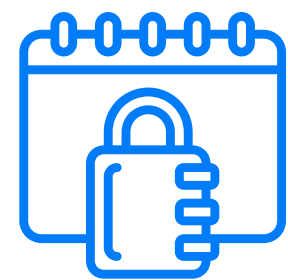
Deletion and Backup

It deletes the information from the server and simultaneously sends encrypted backups to the administrator via a secret URL. It is a drastic measure for major threats, ensuring the preservation of data.


Suspender
Desactivar temporalmente el servidor

Seguridad Extrema
Eliminar todos los archivos y apagar el servido

Verificación de sesión
Definir un límite de tiempo entre sesiones de administrador para borrar el servidor

Seguridad Extrema

Esta acción de Seguridad Extrema solo debe usarse, bajo su responsabilidad, si cree que se encuentra ante una amenaza rea seguridad crítica.

SELECCIONA CUANTO TIEMPO ESTARÁ DISPONIBLE EL RESPALDO LUEGO DE ACCIONAR LA OP DE SEGURIDAD EXTREMA

48h   120h   Ilimitado

CONTINUAR

Why NoTrack?

Different ACCESS URL every day:

Our platform introduces an additional level of security through access URLs that change daily. This unique feature means that the URL parameters to access the login page are modified each day, following an algorithm known only to the ADMIN. This added layer of security ensures that access to the platform is extremely difficult for unauthorized users, thereby strengthening the protection of sensitive data and the platform's infrastructure.
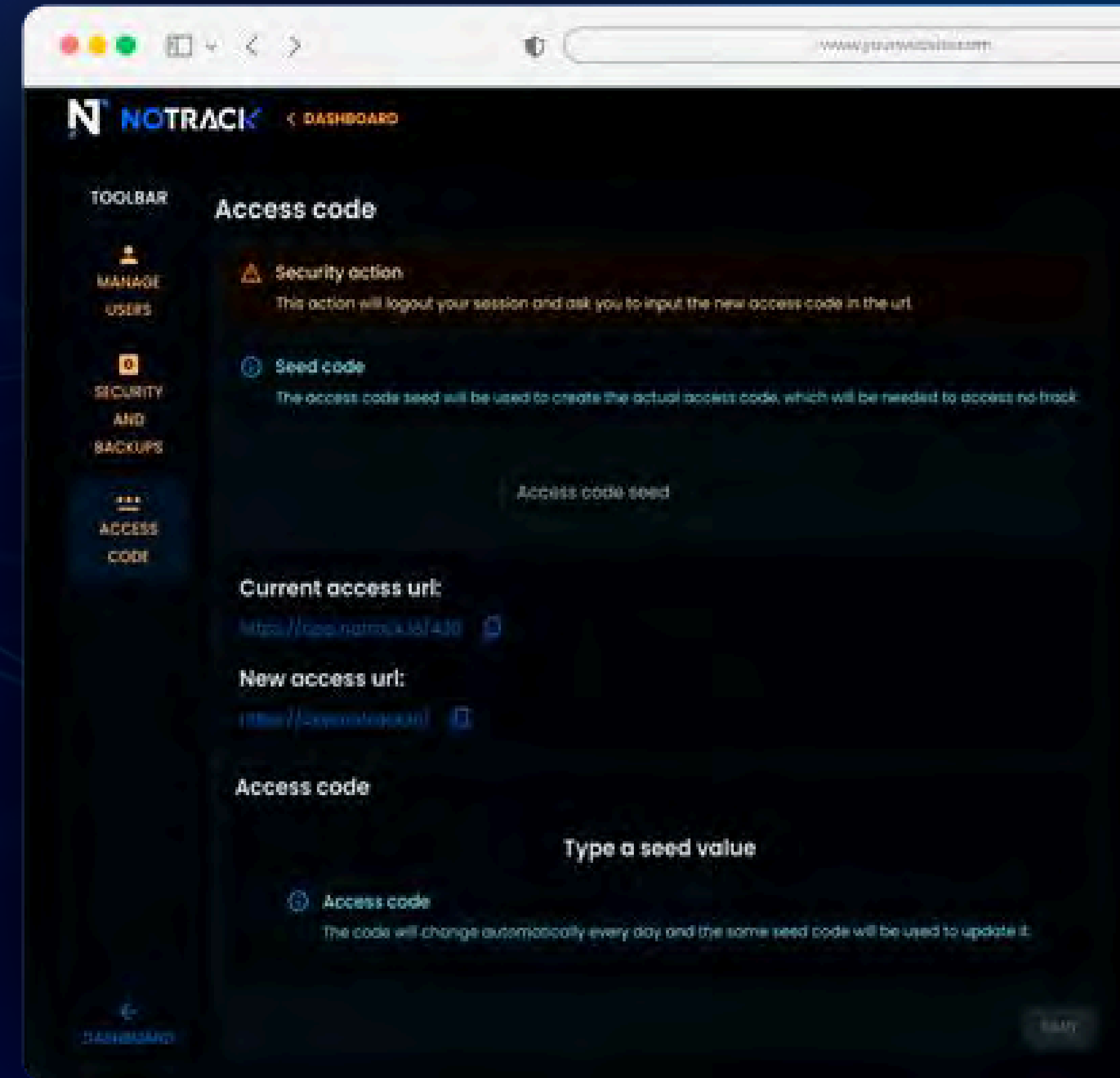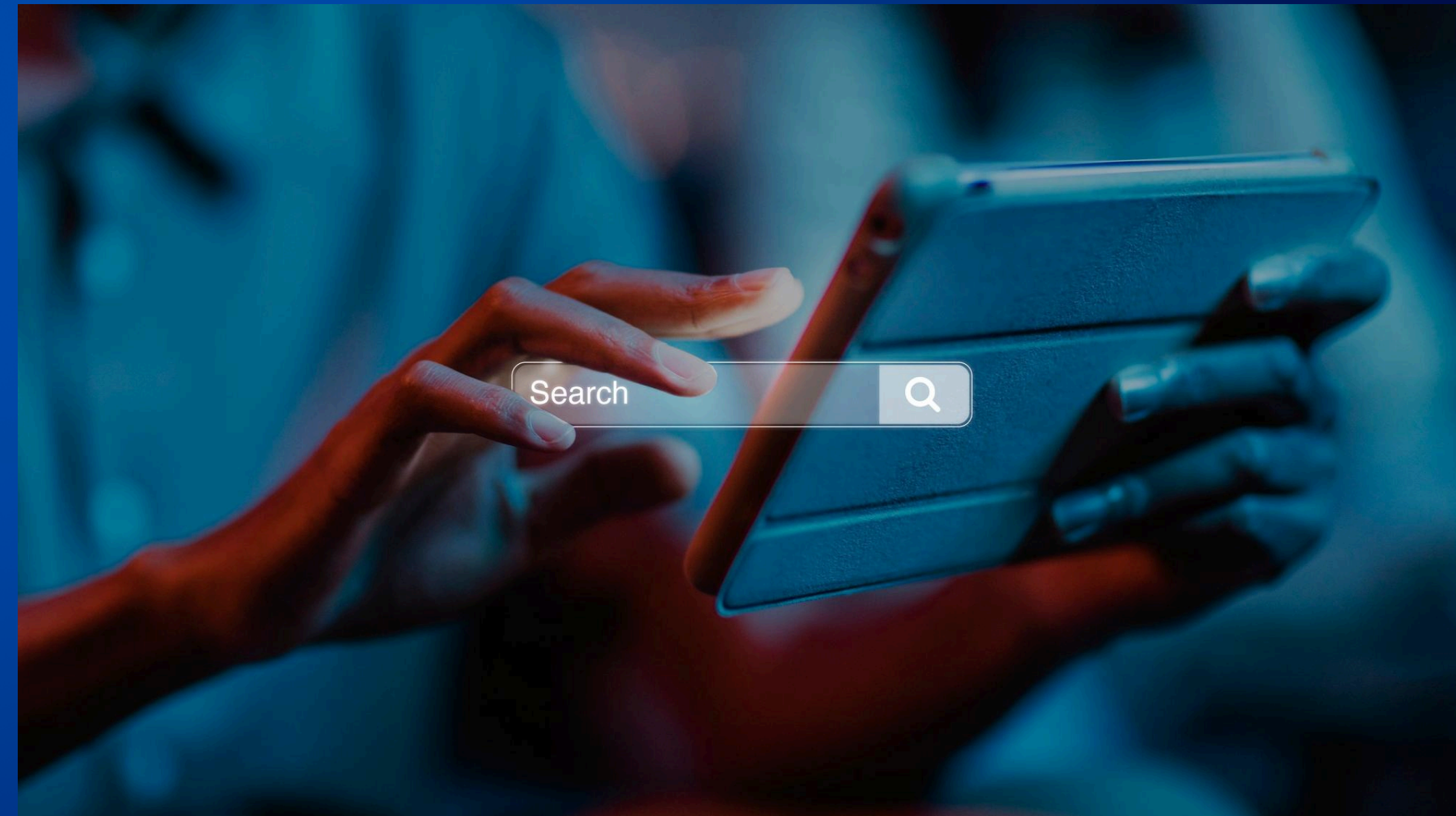
NoTrack Browser

The platform optionally includes its own web browser, specifically designed to access the URL where the platform is hosted. This browser is optimized to ensure maximum security, allowing only the input of the parameters necessary to access the login page.

A key feature of this browser is its privacy policy: it does not store cookies, browsing history, or any other type of data. This ensures that each session is completely private and secure, eliminating any trace of activity once the browser is closed, thereby reinforcing protection against any attempts to recover private information.

Antivirus

The platform includes an antivirus that meticulously scans every file uploaded to it. This feature is designed to detect and block any type of malware or malicious content. If the antivirus identifies a threat in a file being uploaded, it automatically prevents the upload, ensuring the platform remains free of harmful software.

This guarantees that all files on the platform are safe and free from any harmful code or programs, maintaining the integrity and reliability of the digital environment.

Proof of Life

The "Proof of Life" feature enhances security through an inactivity timer configured by the ADMIN. If there is no access to the platform within the set period, the system is suspended. After a second period (also defined by the ADMIN), all files are deleted, and a secret URL is generated for backup download. Optionally, if configured, a notification is sent to the backup email address. This feature protects information in the event of prolonged inactivity.
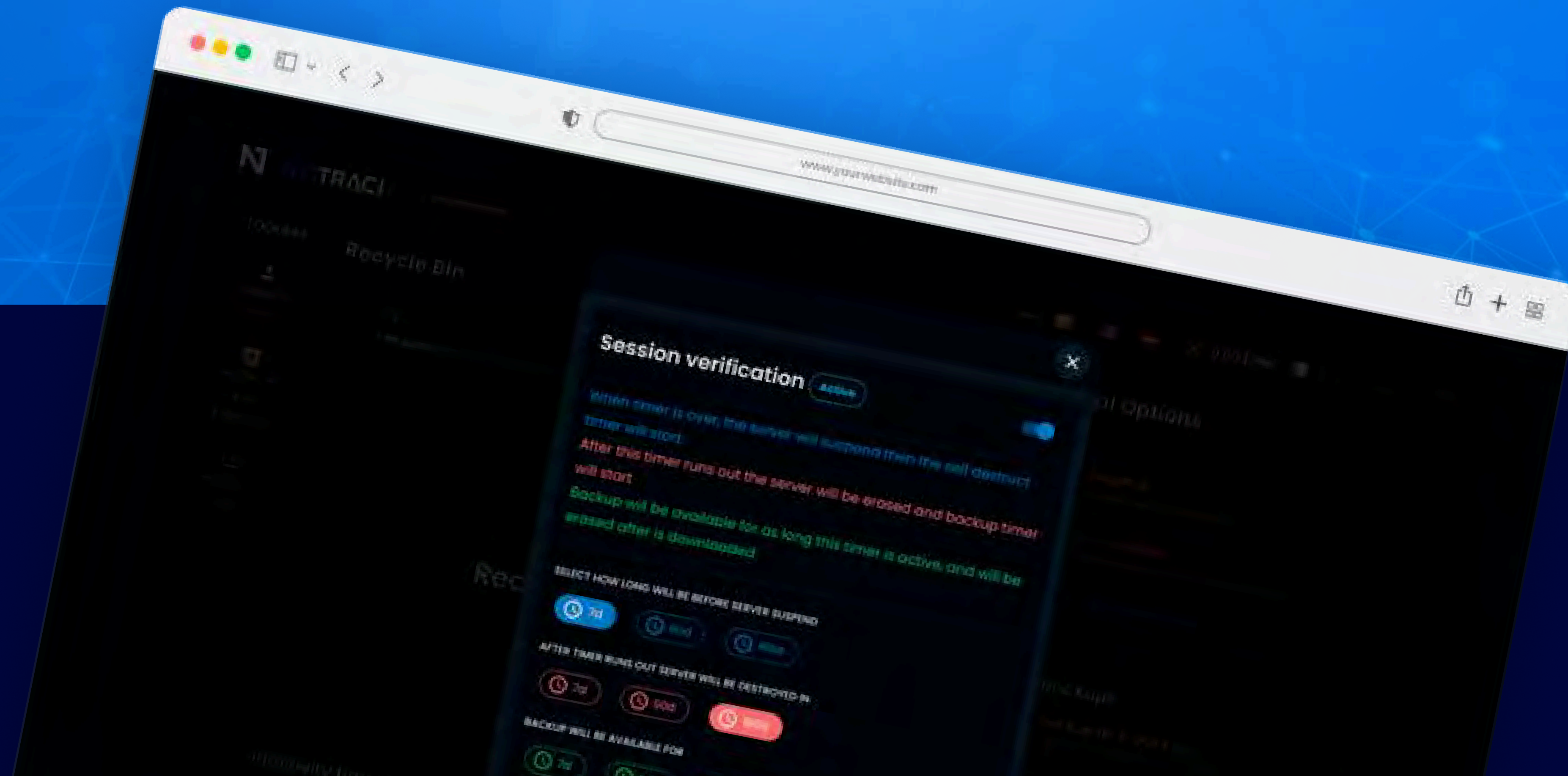
User and Permissions Management

The platform offers user role management that allows control over access and permissions. In addition to the Administrator role, there are three additional roles: Manager, Corporate, Editor, and Viewer, each with different levels of access.
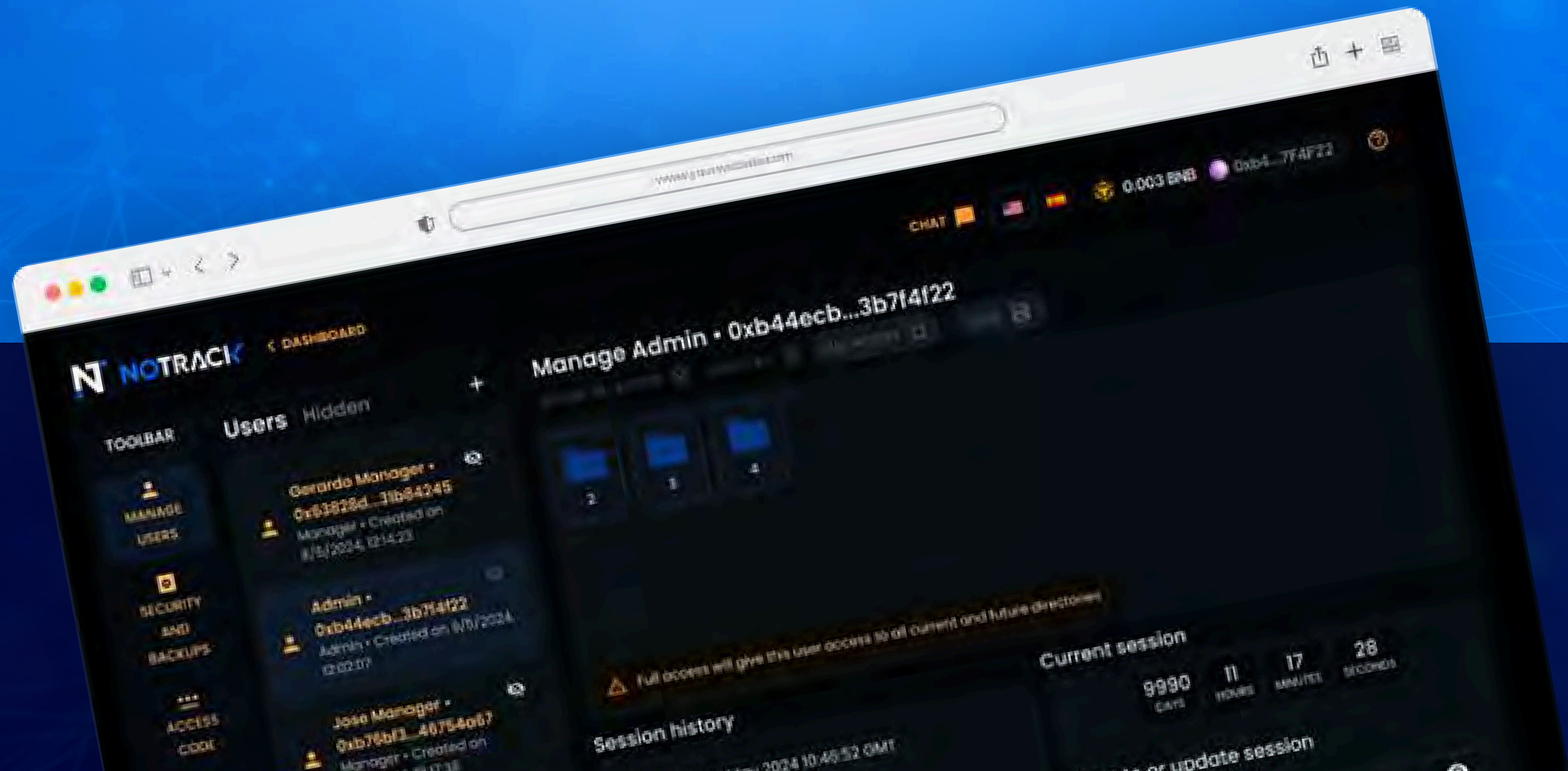
User and Permissions Management

User Types

Admin

Has full access and complete management of the files uploaded to the platform. Can control access for other users, change roles, revoke permissions, and access system settings. Has access to the support CHAT and can execute the FORCE MAJEURE function.

Corporate

Corporate is a special user role designed to work securely with companies (clients, suppliers, advisors, or any other individuals with a secondary connection to the project) or collaborators outside the core group of users around the Administrator. This role allows the user to fully manage the bidirectional handling of files uploaded to the shared folder between the administrator and this user. Additionally, if desired by the admin, it includes an exclusive chat channel with both the administrator and any other authorized user.

Manager

They will have access to the folders the Admin has granted them access to, view the files within, edit them, download them from the platform, upload new files, delete them, and restore backups. They will also be able to execute the FORCE MAJEURE function.

Editor

They will have access to the folders the Admin has granted them access to, view the files uploaded in them, edit them, save them, and upload new files.

Viewer

They will have access to the folders the Admin has granted them access to. They can only view the files uploaded to those folders; they will not be able to edit, download, or upload new files.

Important:

• For security, the access permission time during which a user can log into the platform is set by the Administrator. Once this time has passed, the user will not be able to connect to the platform.

• The system has a Change History, where changes to the files are saved and logged, recording who made the change and when.

Target Audience

Sectors and entities that, in general terms, have a critical need for solutions like NoTrack due to the sensitive nature of the data they handle:

Professional Associations:
- *Bar Association*: They handle confidential client information, legal cases, defense strategies, etc. Confidentiality is essential in their practice.
- *Medical Association*: They store medical histories, patient information, diagnoses, treatments, sensitive personal data, etc. Patient privacy is paramount.
- *Notary Association*: They safeguard legal documents, deeds, wills, powers of attorney, etc. Legal security is essential.
- *Accountants Association*: They manage financial information of companies and individuals, tax filings, audits, etc. The accuracy and confidentiality of financial data are critical.

Government Entities:
- Departments that handle classified information and sensitive citizen data.

Insurance Companies:
- They handle sensitive client information, policies, claims, medical histories, etc. Confidentiality and data security are essential for the business.

Private Companies:
- Companies that handle confidential data, such as technology, finance, consulting, and auditing firms.

Financial Institutions:
- Banks, fintechs, and other institutions that handle transactions, personal data, and sensitive strategies.

Individuals:
- People interested in protecting personal information, legal documents, and private multimedia content.

Educational and Research Sector:
- Universities and research centers that need to protect academic data, patents, and projects.

Potential Clients

Corporate Sector:
- *Legal firms and financial consultants*: Ensure confidentiality and traceability of their documents.
- *Technology companies*: Owners of source code, trade secrets, and customer data.
- *Financial Institutions*: Banks and fintechs that need to protect customer data and critical operations.

Startups and PYMEs:
- Growing technology and financial businesses looking for scalable and accessible solutions.

Government and Public Entities:
- Critical departments such as national security, tax areas, and citizen privacy policies.

Education and Health:
- Universities, hospitals, and clinics that manage academic and medical records.

Specialized Insurance Companies:
- Protection of policies, customer data, and critical claims.

Creative and Media Industry:
- Audiovisual production companies, publishers, and agencies looking to protect intellectual property and exclusive content.

Our Plans

ESSENTIAL

5.000 USD
$300 Monthly maintenance fee

Features

We use a new instance of our server and website for access.

They have new smart contracts and exclusive, encrypted file storage on the server.

Up to 6 users.

Antivirus

Optional:

NoTrack Browser
NoTrack Wallet
QuickNode: Private RPC
Add extra users

The client accesses the solution at notrack.io/client/seed

PRO
QUOTE

Features

Total independence and full control of the platform, hosted on their servers and managed by their resources.

Custom URL + "Screen" Web

Customization of look & feel to match their branding.

Unlimited users

NoTrack Browser

NoTrack Wallet

Antivirus

QuickNode: Private RPC

A complete clone of the project, maintaining look & feel, server, and the client's domain.

PLUS

10.000 USD
$300 Monthly maintenance fee
+ Server cost

Features

We use a dedicated server and the client's own login webpage.

They have new smart contracts and exclusive, encrypted file storage on the server.

Custom URL + "Screen" Web

Up to 10 users

Antivirus

Optional:

NoTrack Browser
NoTrack Wallet
QuickNode: Private RPC
Add extra users

The client accesses the solution through their own URL, but the look and feel of NoTrack is maintained.

NOTRACK

We protect your documents and respect your privacy.

Audited in Security by

DragonJAR®
SEGURIDAD INFORMÁTICA

www.dragonjar.org

NOTRACK

Are you ready to transform the security of your data?
Discover how NoTrack can protect what matters most.
Contact us today.

Gerardo Manuel Prieto

CEO & DIRECTOR

+34 685692 132 / +54 9 341 311 8773

gerardo@fanaticoins.com