



Protect Your Data, Keep Your Work Safe!

Theft | Loss | Disruption | Deletion
Leakage | Virus | Hacker | Malicious Insider





Briefly About **iCredible File Security**

A solution-focused company in the field of distributed file storage and encryption, appealing to a wide audience ranging from individuals and micro-businesses to corporations.

It has unique and cost-effective solutions than its competitors.

If your goal is file-based protection and transparency, iCredible File Security is the best choice for you!



Why **iCredible File Security**?



Distributed and Encrypted Storage

Your data is stored in a distributed manner and is resistant to data leaks due to being fragmented.



Immutable Logging

Critical system activities are also recorded on the blockchain and cannot be altered.



Pay-As-You-Go Model

Cost-effective, especially for individuals and SMEs.



Quick and Simple Setup

Setup is completed within minutes using a web panel and agent support.



Ransomware Protection

Your files are continuously protected and remain unaffected by ransomware attacks.

Target User Profiles

Individual Users: People who want to protect sensitive data against threats like theft, corruption, and ransomware.

Small and Medium Businesses: SMEs looking to optimize data security and backup costs.

Large Enterprises: Organizations seeking to secure critical files against internal and external threats.

Government Institutions: Public entities in need of KVKK/GDPR-compliant, immutable logging, and secure data storage solutions.



Competitive Advantages

Features

Distributed Storage

Immutable Logs

Pricing Model

Ransomware Protection

iCredible File Security

IPFS-based, geographically distributed, encrypted, and fragmented data storage

Blockchain-based logging ensures transparency and immutability

Pay-as-you-go (Individual and SME-friendly)

Files are continuously encrypted and backed up, making them immune to ransomware

Competitors

Mostly centralized storage, rarely distributed

Limited or centralized logging systems

Annual subscription, more expensive

Often focused on full-disk backup, limited file-level solutions

Competitive Advantages

Features

Data Leak Resistance

Ease of Setup

Compliance

iCredible File Security

Encrypted and distributed storage with fragmented, unmergeable pieces

User-friendly interface, simple activation, and 2FA-enabled approvals

KVKK/GDPR-compliant, meeting public and private sector requirements

Competitors

Higher risk of data leaks in centralized storage

More complex installations requiring technical expertise

Some competitors lack KVKK/GDPR compliance



Key Features

Real-Time Protection: Changes made to files are instantly encrypted and backed up on the server.

Dual Encryption: Files are encrypted using both user and application keys.

Immutable Backup: Stored files cannot be altered; previous versions are preserved.

Optimized Backup Costs: Only critical files are backed up instead of the entire disk.

Approval Workflow for Critical Actions: Security is enhanced with 2FA and authorization processes.





Distributed File Storage & SPOF

Critical digital assets like servers and databases are regularly backed up, but these backups, unless kept offline, remain a prime target for attackers. Your system is useless without your current data.



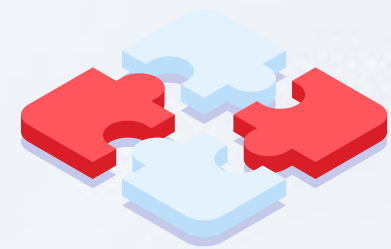
The more you securely back up your data in inaccessible and geographically diverse locations, the harder it becomes for a single point of failure to disrupt your system. In worst-case scenarios or successful attacks, recovery becomes significantly easier. That's why your critical files are protected and stored using IPFS-based, geographically distributed, decentralized systems with end-to-end encryption.

Client Backups & Immutable Storage



Servers often enjoy strong protection and frequent backups. However, end-user devices are either outside this protective shield or at their weakest point, often relying only on basic antivirus software. Their backups are either nonexistent or stored on the same disk via shadow-copy. However, critical data also exists on end-user devices.

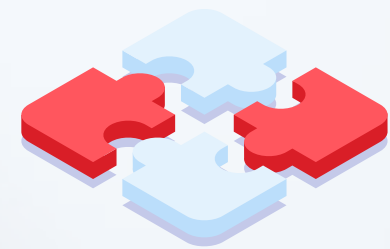
Devices always face risks like theft, disk failure, etc. In addition, ransomware is also becoming more widespread day by day.



To mitigate these risks, it is vital to ensure files are immutable and any version should be recoverable.

Storage Costs

Backing up end-user machines, establishing IT infrastructure, maintaining it, and providing sufficient storage space can be costly.



To minimize storage and transfer costs, the system should allow not only full disk backups but also selective protection for critical files only.



Dual Encryption Storage

While platforms like common cloud applications can be used for backups, your data is often stored openly, without privacy, and likely without backup. This is unacceptable for any organization.

Even if you avoid the cloud and use external drives, malware can reach your data the moment the drive is connected, rendering it inaccessible.

An illustration of a laptop with a blue shield icon on the screen and a red-bordered password field with asterisks. Below the laptop are several interlocking puzzle pieces in red and blue.

Therefore, files should be encrypted with personal keys and integrated with modern technologies such as Web3 for enhanced security.



Data Leakage

Although security tools like antivirus and EDR are used to protect end-user devices, a simple phishing email can bypass them. While you can restore corporate applications after an attack or failure, your most important asset—your data—remains at risk.

Internal threats pose an even greater risk because attackers familiar with system vulnerabilities can easily access servers or critical files, leaking sensitive data externally.



Relying on a single cloud backup is insufficient. Instead, distributed, fragmented storage across multiple servers ensures that, even in case of a breach, the data remains encrypted, fragmented, and nearly impossible to reconstruct.



Immutable Log Records

Once attackers gain access, they often delete log records to cover their tracks, making it harder to investigate and identify vulnerabilities.

Critical logs should be backed up and stored securely using blockchain-based solutions in addition to Elasticsearch to prevent tampering and preserve investigative integrity.



Device Management

In corporate environments, managing thousands of devices—including VIP users—requires sophisticated tools.



With Active Directory (AD) and LDAP integration, you can view and manage all digital assets, set policies, assign permissions, and handle storage and recovery.





Pay-As-You-Go

While large organizations can afford diverse security tools like Firewalls, EDR, DLP, and FIM, individuals and small businesses often face budget constraints.

The solution must scale with user needs, the number of users, storage requirements, and organization-specific management rules.

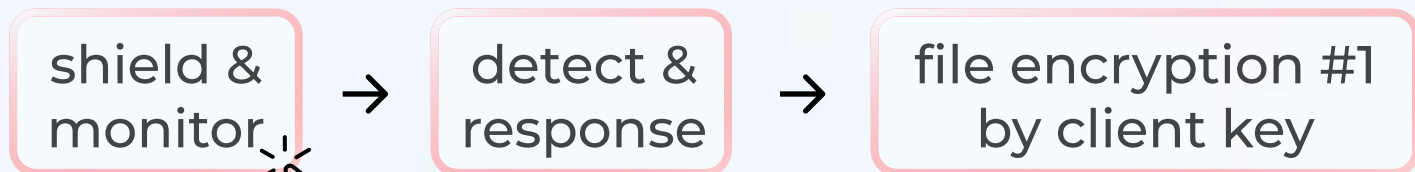
**A blockchain-based logging, cloud-distributed, encrypted, and immutable file security solution:
iCredible File Security**



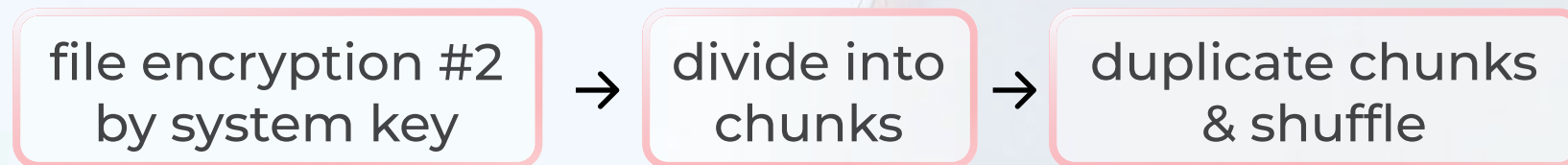
How It Works?

- ⊞ Works both on-premise and cloud-based.
- ⊞ An agent installed on your machine provides a seamless user experience or integrates with existing document management systems via API.
- ⊞ Each file is scanned for malware during upload and recovery.
- ⊞ Files are encrypted twice—once with a user key and again with an application key—then fragmented into smaller pieces.
- ⊞ Fragment copies are distributed randomly across server clusters.
- ⊞ Updated files are saved as new versions while previous ones are preserved. Uploaded files cannot be modified.
- ⊞ Files cannot be deleted, removed from protection, or recovered without passing additional security measures and 2FA, and deleted files can be recovered for up to 30 days.
- ⊞ Every access and modification is logged with timestamps and hashes.

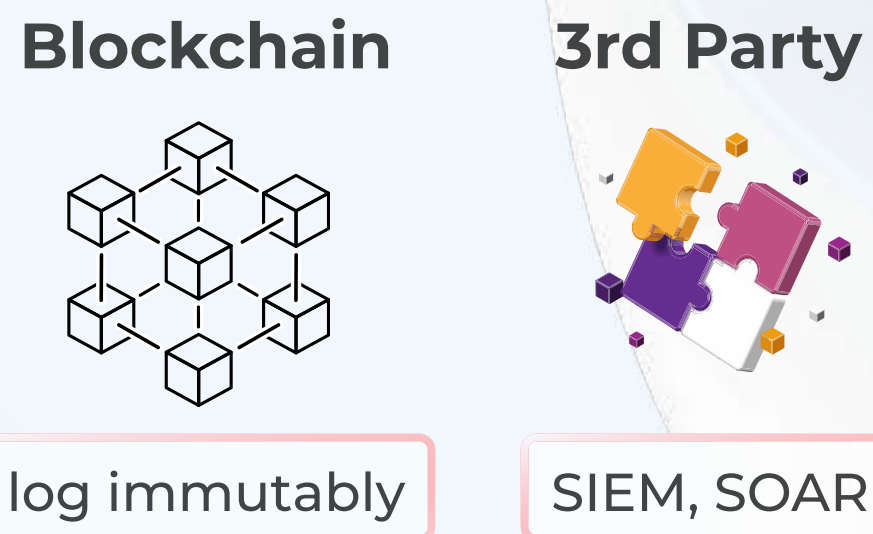
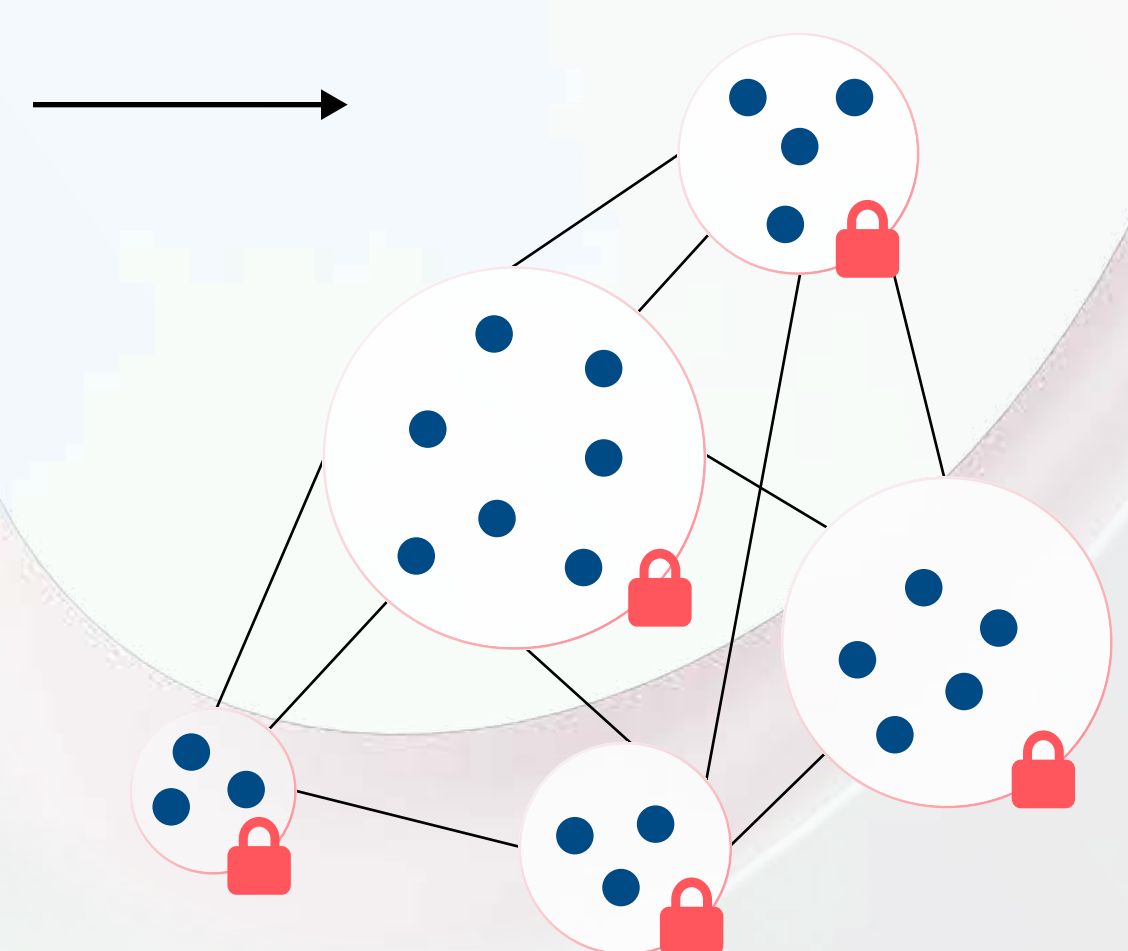
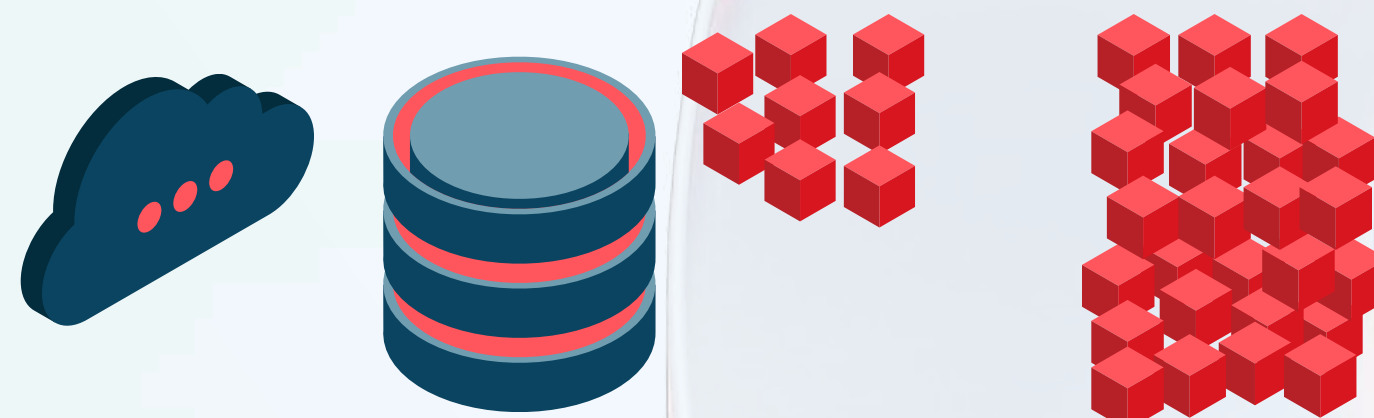
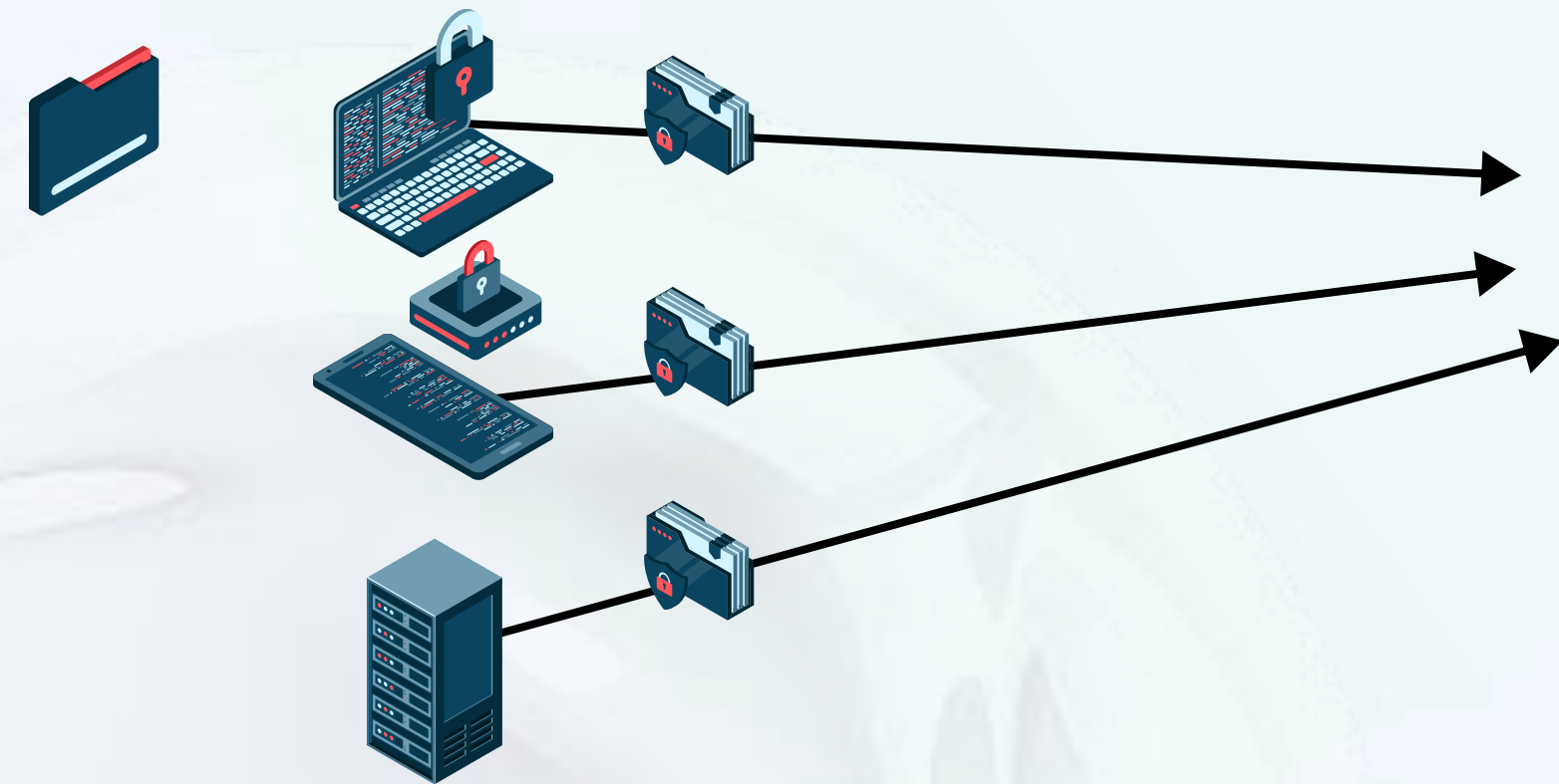
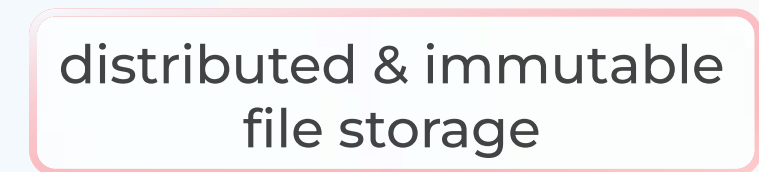
Endpoints

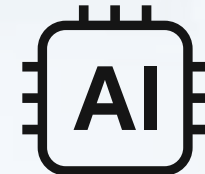


App Servers



Server Farm



-  **AI**
- monitor** files, folders, registry, logs and network
- detect** ransomware, malware and any suspicious activity
- response** alert, stop, isolate and report

- Disaster Scenarios**
- Different Locations & Providers
 - Redundancy
 - No SPOF
 - GDPR-Compliant

Thus, in the event of a server, disk, or file being targeted by ransomware or internal/external attacks, the integrity, currency, and accessibility of the compromised vector are preserved.

How to Use?

- ⑥ Create an account via the web management panel.
- ⑥ Download the agent compatible with your OS.
- ⑥ Generate an activation code via the panel.
- ⑥ Complete the setup effortlessly with the activation code.
- ⑥ A personal encryption key is created and stored on your OS.
- ⑥ Right-click on critical files/folders to “Shield” them for protection. They can only be “Unshielded” with 2FA.
- ⑥ All changes and access to these files are instantly encrypted and sent to the server.
- ⑥ Files are stored encrypted, distributed, and immutable – accessible only by the owner.
- ⑥ Use the management panel to list all files, configure permissions, and manage settings.
- ⑥ Recover files/folders individually or in bulk with 2FA.





Features at a Glance:

- Free account setup with unlimited use
- Folder/File protection
- Real-time protection and immutable backups
- File search and version history
- Automatic/manual restoration of selected file versions
- Storage space management
- Role-based access control
- 2FA for action verification
- Approval workflows for critical operations
- Team creation
- Device grouping and tagging
- Detailed log monitoring
- Logging of file, registry, and network changes
- Custom encryption key management
- GDPR/CCPA compliant

- Ransomware protection
- Resistance to data leaks
- AI-supported malware analysis
- Notification and isolation of suspicious threats
- API integration
- AD and LDAP Integration
- File Integrity Monitoring (FIM) module
- VirusTotal Integration



Who Should Use It?

- 📁 Devices without security beyond basic antivirus
- 📁 Individual users, small teams, and SMBs
- 📁 Cloud storage users
- 📁 Those prioritizing data privacy
- 📁 Companies neglecting backups for laptops or end-user devices
- 📁 Victims of ransomware like CryptoLocker or WannaCry
- 📁 Companies securing work-related files for employees
- 📁 Organizations seeking enhanced data security for executives
- 📁 Public institutions requiring privacy even during data leaks

Web Site:
[icredible.com](https://www.icredible.com)

Mail:
info@icredible.com