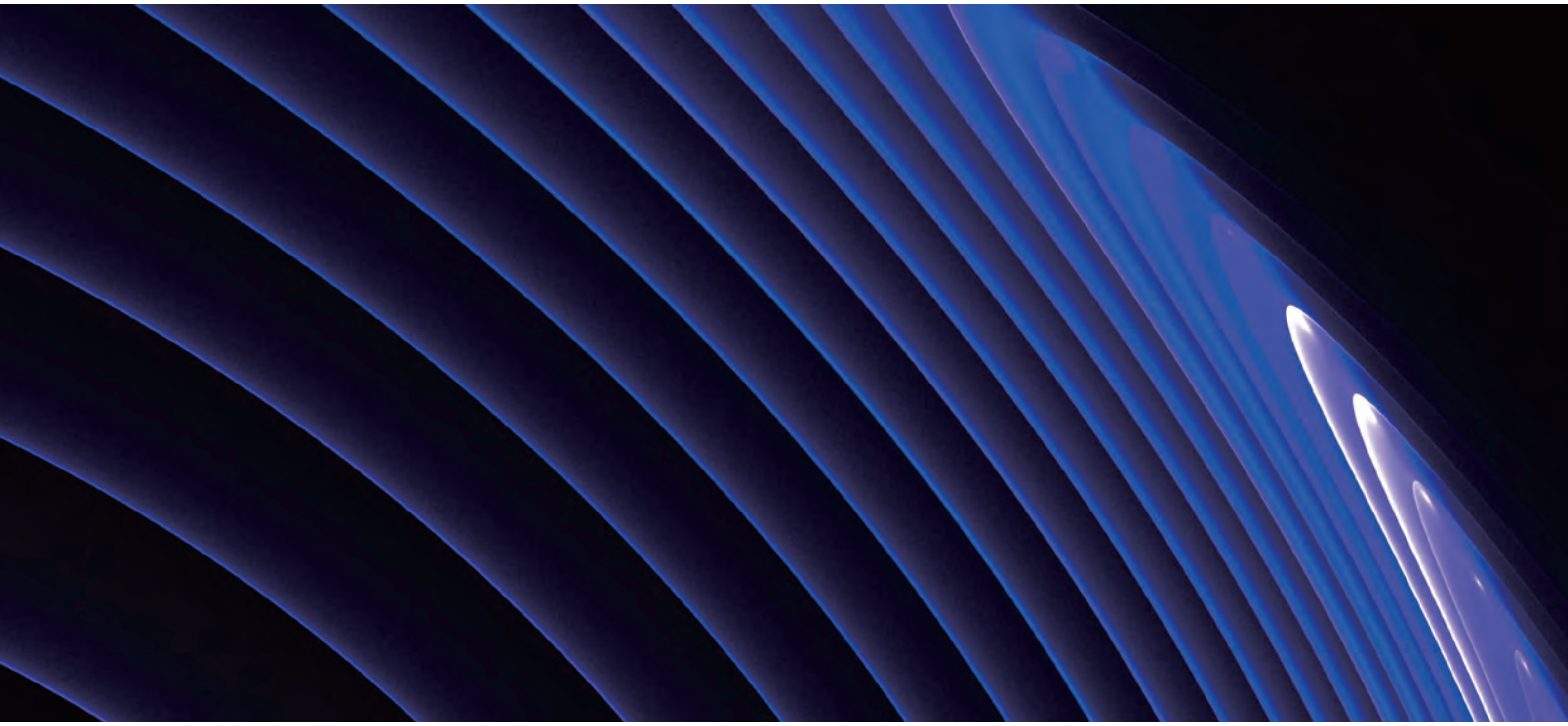
NSecsoft



All–in–One Platform for Endpoint Management and Data Security

Unified Endpoint Management | Data Loss Prevention | Managed File Transfer

About Us

NSecsoft is a cybersecurity software company specializing in Unified Endpoint Management (UEM) and Data Loss Prevention (DLP) solutions. Our mission is to help organizations gain full visibility and control over all endpoints—desktops, laptops, mobile devices—while securing sensitive data from unauthorized access, leaks, or misuse.

With a robust and scalable platform, we empower IT teams to streamline endpoint operations, enforce compliance policies, monitor user behaviors, and respond to threats in real time. Trusted by enterprises across various industries, our solutions are designed to meet modern security challenges with precision and agility.

Whether you are managing a remote workforce or navigating strict regulatory environments, our tools ensure your data stays secure—everywhere, every time.

Our Competitive Advantage

Certified with ISO/IEC 27001 (Information Security Management) and ISO 9001 (Quality Management). We are committed to protecting your data and delivering high–quality services globally.

Regulatory Compliance. Simplifies adherence to requirements.

Built for local admin rights. Just the features you need.

Ease of Use. Simple to deploy, manage, and maintain.

Cost Efficiency. Affordable per–endpoint pricing.

Information Security Management System ISO 27001 Certified

CERTIFIED ISO 9001:2015 COMPANY

NSecsoft Limited

✉ support@nsecsoft.com
🌐 www.nsecsoft.com

Ping32 Data Loss Prevention

Prevent data breaches and streamline compliance.

One platform that configures and enforces data security policies across web, cloud, email, network, and endpoint to help reduce potential data breaches and regulatory compliance violations.

Key Causes of Data Leakage

Data leakage often stems from gaps in visibility, human error, and evolving work models, making comprehensive protection essential.

Limited Visibility

Blind spots across endpoints and cloud increase exposure risks.

IP Theft

Confidential business data targeted by internal and external actors.

Insider Threats

Careless or malicious employee actions remain a top cause.

Remote Work Risks

Unmanaged devices and unsafe connections heighten threats.

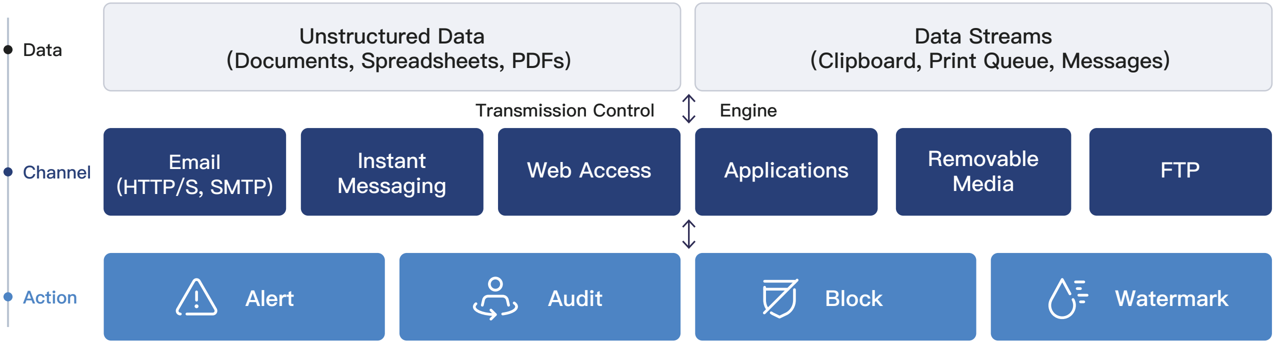
Benefits of Ping32 Data Loss Prevention

- Prevent data leakage across endpoints, cloud storage, and external devices without impacting user productivity.
- Detect and block sensitive content using intelligent content analysis and real-time behavior monitoring.
- Classify documents automatically based on predefined sensitivity rules powered by AI.
- Enforce granular security policies across different user roles, departments, and data types.
- Support compliance with regulatory standards such as GDPR, ISO 27001, and local data protection laws.
- Track and audit document access, modification, and transfer for full data traceability and defense.

Mitigating Insider Threats with Ping32

Insider threats, whether intentional or accidental, are one of the primary causes of data loss. Ping32 helps mitigate this risk by restricting unauthorized access, monitoring user behavior, and preventing the unauthorized transfer or sharing of sensitive data. It also provides detailed audit trails to support investigation and compliance efforts.

How data loss prevention works



Data

Unstructured Data
(Documents, Spreadsheets, PDFs)

Data Streams
(Clipboard, Print Queue, Messages)

Transmission Control ↕ Engine

Channel

Email
(HTTP/S, SMTP)

Instant
Messaging

Web Access

Applications

Removable
Media

FTP

Action

Alert

Audit

Block

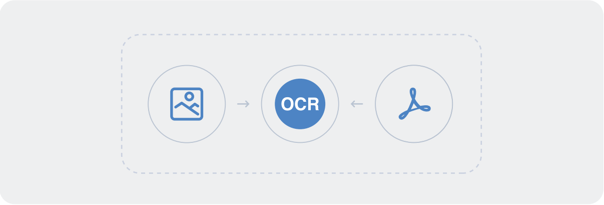
Watermark

Protect Your Business with Comprehensive DLP

Consistently discover, monitor, and protect sensitive data across every network, cloud, end–point, email, and user.

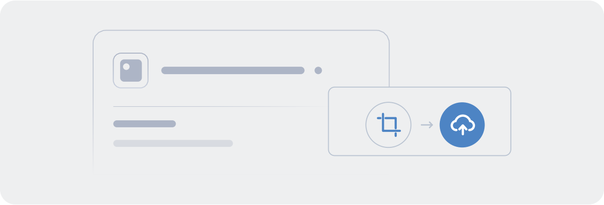
Policy Templates

Get started quickly with dozens of out of the box policies for common use cases and industry–specific requirements.



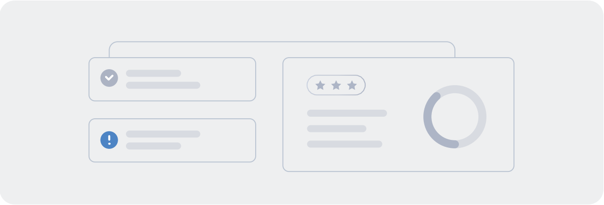
OCR Support

Extracts text content in image files and PDFs and supports use of this data in content–based policies.



Screen Capture

Screens can be recorded before an incident, with screenshots securely stored in the customer’s cloud.



Reports & Analytics

Includes out–of–the–box dashboards and a fully customizable reporting engine for advanced analytics.

NSecsoft
Unified Endpoint & Data Security

Ping32 Transparent File Encryption

Complete Protection for Sensitive Data Across Its Lifecycle

File encryption software protects sensitive data from unauthorized access, both at rest and in transit. It mitigates risks like data breaches, insider threats, and device loss while ensuring regulatory compliance and secure collaboration across environments.

One of the best ways to protect your data is to encrypt it—whether at rest or in transit.

Data Protection

Prevents unauthorized access and ensures information stays confidential.

Compliance

Helps meet legal and industry data security regulations.

Leak Prevention

Works with DLP systems to block unauthorized sharing or copying.

Why Should You Use File Encryption Software?

Without using file encryption software, your files are much more at risk, complying with regu–lations will ultimately be more difficult, and overall security will be weakened.

Stronger Protection, Greater Confidence

With the right encryption software, your data remains secure across devices—bringing peace of mind to you, your business, and every partner you work with.

Security across devices

File encryption software ensures that data is encrypted with the same protections in place, no matter if data is stored on a desktop or mobile device.

The secure movement of data

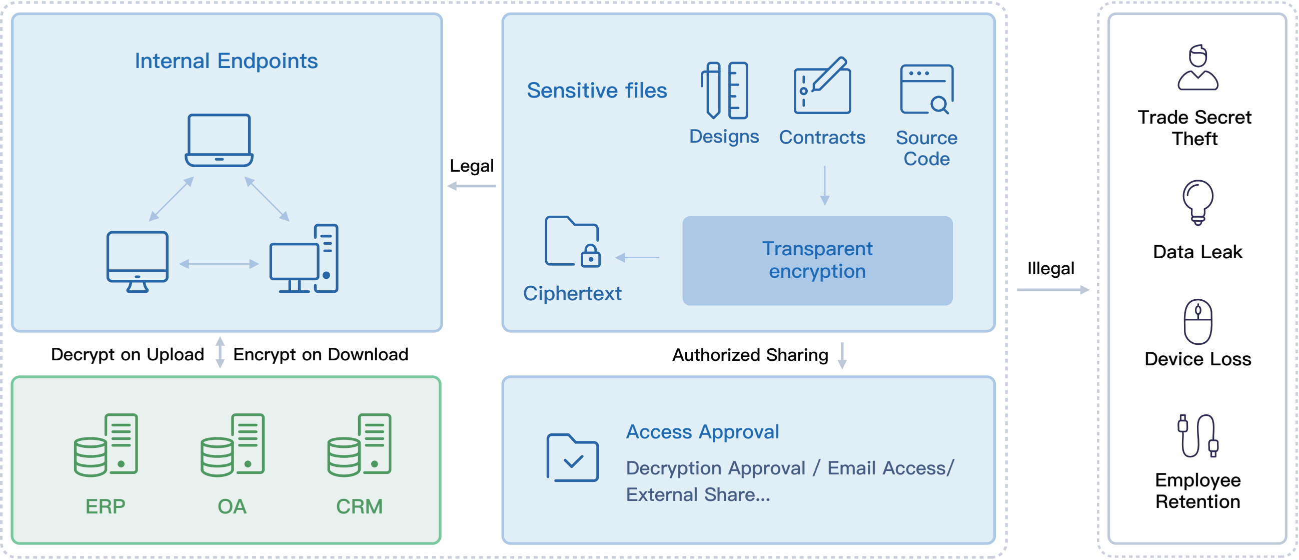
Effective file encryption software helps to ensure that data is protected no matter where it’s at in its journey.

Simplified compliance

File encryption software helps organizations to meet essential compliance regulations with its hefty security standards.

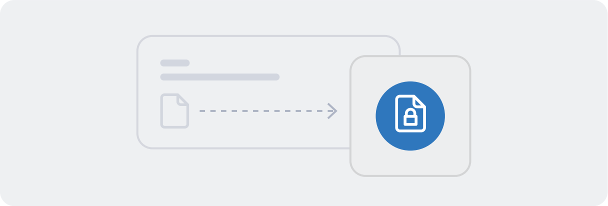
File Encryption and Access Control Architecture

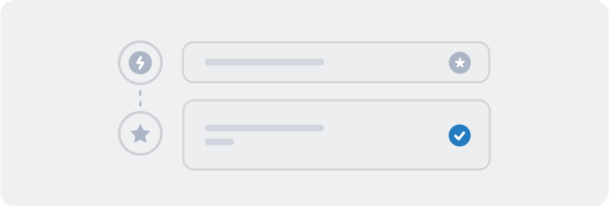
Transparent encryption secures sensitive data without disrupting access, enabling seamless protection and compliance.



Protect your data with file encryption

With tools like file encryption, you can protect sensitive data and information without adding extra steps to your workflow.





File–level Encryption

Encrypts files at the source to prevent unauthorized access or leakage, while allowing users to work without disruption.

Decryption Approval

All decryption actions follow a built–in approval workflow, ensuring traceability and strict access control for sensitive files.

Secure External Sharing

Supports encrypted file sharing with exter–nal parties via secure viewers, preventing unauthorized downloads, copying, or screen capture.

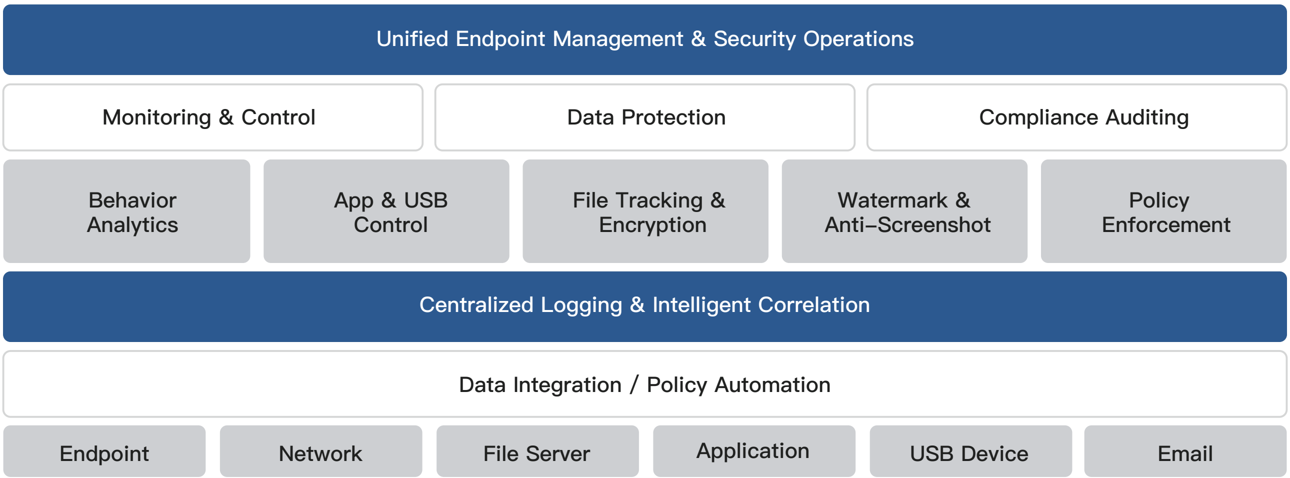
Full Path Encryption

Ensures encryption covers the full file path—including local folders, shared drives, and cloud storage—maintaining end–to–end data protection.

Ping32 Unified Endpoint Management

Ping32 is a comprehensive Unified Endpoint Management (UEM) solution designed for enterprise IT departments to efficiently manage, monitor, and protect endpoints across the organization. From employee behavior analysis to data loss prevention, Ping32 helps businesses enhance information security and operational efficiency.

Ping32 UEM Platform



Unified Endpoint Management & Security Operations

Monitoring & Control | Data Protection | Compliance Auditing

Behavior Analytics | App & USB Control | File Tracking & Encryption | Watermark & Anti–Screenshot | Policy Enforcement

Centralized Logging & Intelligent Correlation

Data Integration / Policy Automation

Endpoint | Network | File Server | Application | USB Device | Email

Manage all of your users and endpoints on one dashboard.

Increase visibility across your organization and detect threats in real–time.

Increase business productivity through automation.

One platform to manage them all

Deliver, manage and secure optimal user experiences across all devices, from managed endpoints to shadow IT remediation.

Windows

macOS

Linux
POWERED

Policy Execution Accuracy

99.9%

Automated enforcement of security policies across endpoints

Endpoints Managed

10,000+

Deployed across finance, manufacturing, healthcare, and more

Average Policy Response

30 sec

Fast policy delivery and execution at scale

Platform Uptime

99.99%

Enterprise–grade stability proven in mission–critical environments

Key Features

Real–Time Endpoint Monitoring

Monitor app usage, file activity, web access, and USB connections in real time.

Data Loss Prevention (DLP)

Prevent data leaks via email, USB, printing, and screen capture.

Device & Asset Management

Track hardware assets to ensure complete visibility and control.

Application Control

Allow or block applications based on policies to reduce risks.

Employee Productivity Insights

Monitor digital activity and identify productivity trends across teams.

Network Access Control (NAC)

Verify device compliance before granting network access.

Remote Support & Control

Provide real–time remote access to fix problems and reduce downtime.

Helpdesk & Ticketing

Streamline IT support with efficient ticket tracking and resolution.

Web Filtering

Block or allow website access based on URL, category, or content.

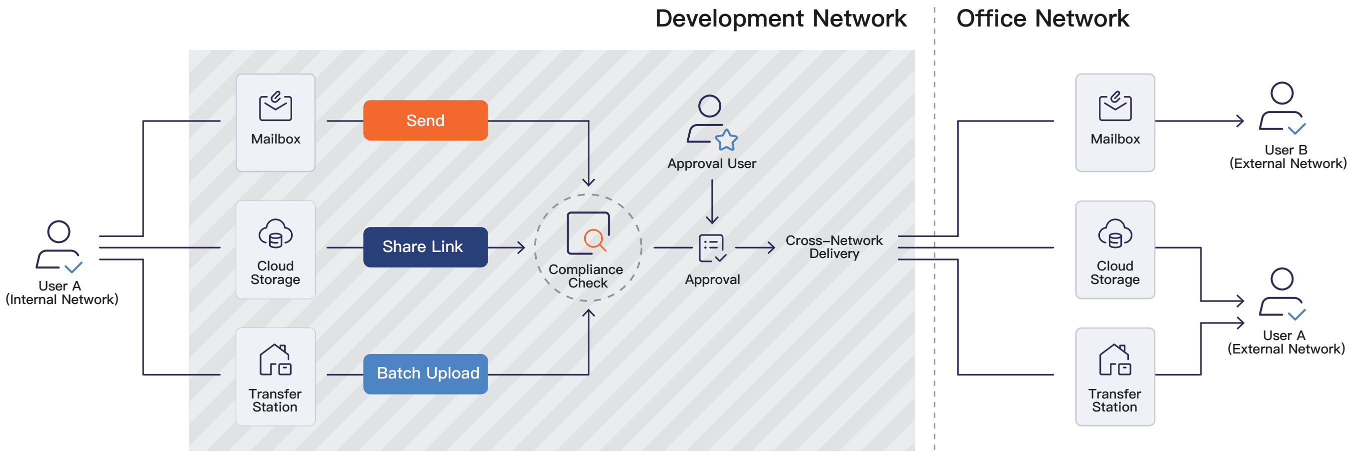
NSecsoft
Unified Endpoint & Data Security

FileLink Managed File Transfer

Secure Cross Domain File Transfer Solution

- FileLink enables secure file exchange in isolated network environments.
- It combines CDS principles to ensure safe cross–domain transfers.
- Advanced MFT features support automated, policy–driven workflows.
- All transfers are tightly controlled, traceable, and compliant.

● Between internal and external users



● Same user with internal and external identities

Key Features

Multi–Layered Security
Advanced threat scanning and access control ensure secure transfers.

Integrations
Connect with collaboration tools and file servers for automation.

Transfer Workflows
Support scheduled, on–demand, and rule–driven transfers.

Approval Flow
Enforce compliance with single or multi–level approvals.

Outbreak Prevention
Periodic rescans defend against zero–day threats.

Logic–Based Policies
Automate transfers using multi–condition rules, no scripting needed.

Easy Deployment
Quick setup for fast rollout in secure environments.

Audit & Reporting
Track transfers, user actions, and system events for compliance.

Secure File Sharing
Share with Control, Access with Trust

FileLink empowers organizations to send sensitive files to external recipients while maintaining complete control over how, when, and where they are accessed. Every file is protected by enterprise–grade security policies, ensuring your information remains safe even after it leaves your network.

Key Capabilities

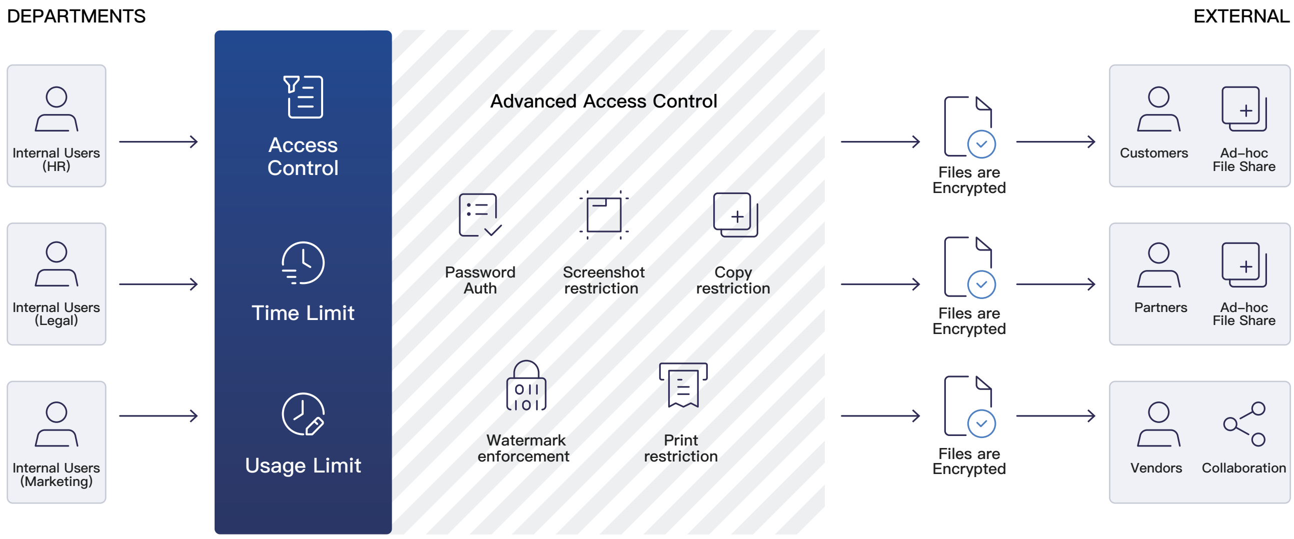
Granular Access Permissions — Define who can open the file, limit the number of views, and set expiration dates to automatically revoke access.

Content Protection — Apply dynamic watermarks, disable screenshots, and block text copying to prevent data leakage.

Strong Authentication — Require password verification before access and bind files to specific device IDs for maximum security.

Post–Delivery Control — Modify or revoke access at any time, even after the file has been shared.

File sharing and permissions — Advanced controls like passwords, expira–tions, and easy revocation ensure access only for the right people.



nsecsoft.com

NSecsoft may make changes to specifications and product descriptions at any time, without notice.

Simplicity is the ultimate sophistication.

Contact us : design–team@nsecsoft.com

NSecsoft Limited