

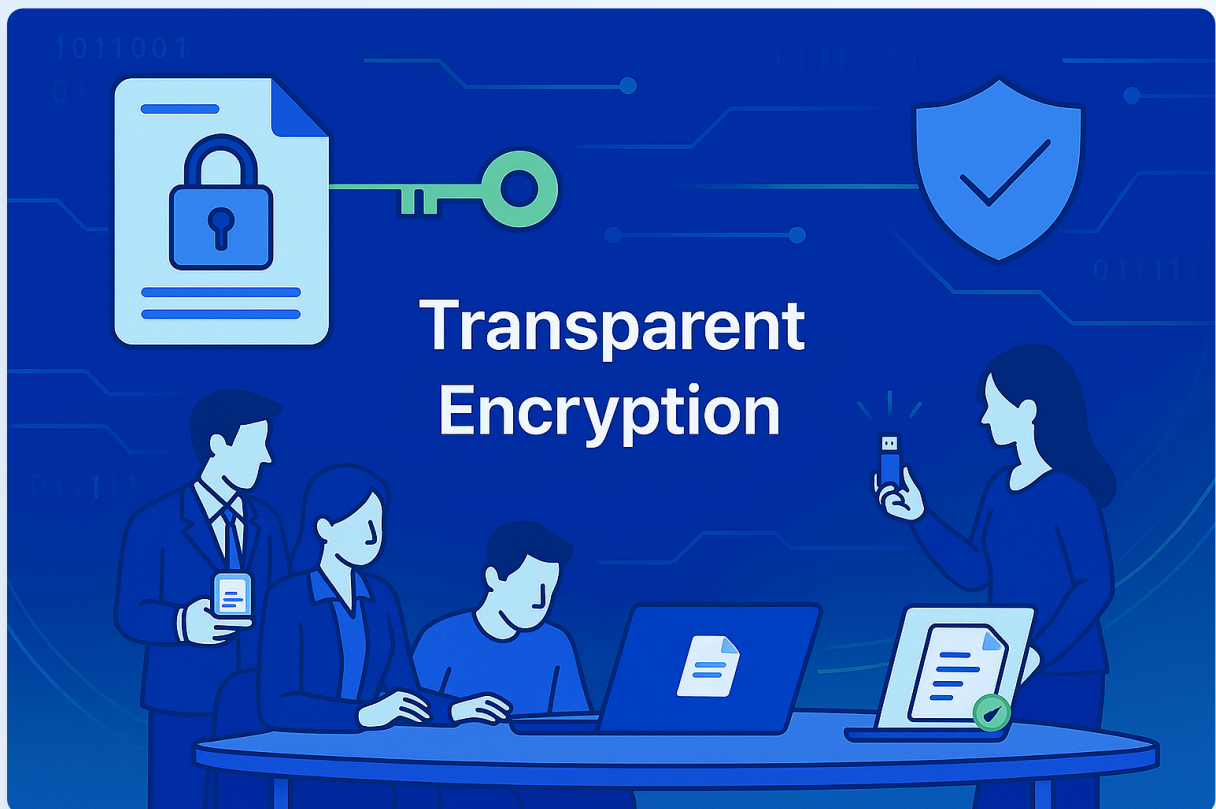


AnySecura

Transparent Encryption

Comprehensive document protection solution

Encrypt · Control · Secure · Share · Manage





Module Overview

AnySecura Transparent Encryption provides enterprises with comprehensive document security through transparent encryption technology, ensuring sensitive information remains protected across its entire lifecycle while maintaining user productivity.



Transparent Encryption

High-strength encryption that works automatically without disrupting user habits, with protection against clipboard, screenshot, and virtual printing theft.



Flexible Encryption Modes

Includes mandatory, intelligent, and read-only encryption options to meet diverse document security requirements.



Security Zones

Department and role-based document isolation with configurable security boundaries to prevent unauthorized access.



Classification Levels

Sensitivity-based document classification with appropriate access restrictions for each level.



Granular Permission Control

Detailed access rights management including reading, modifying, copying, printing, and decryption permissions.



External Distribution

Secure document sharing with external parties through controlled decryption and usage restrictions.



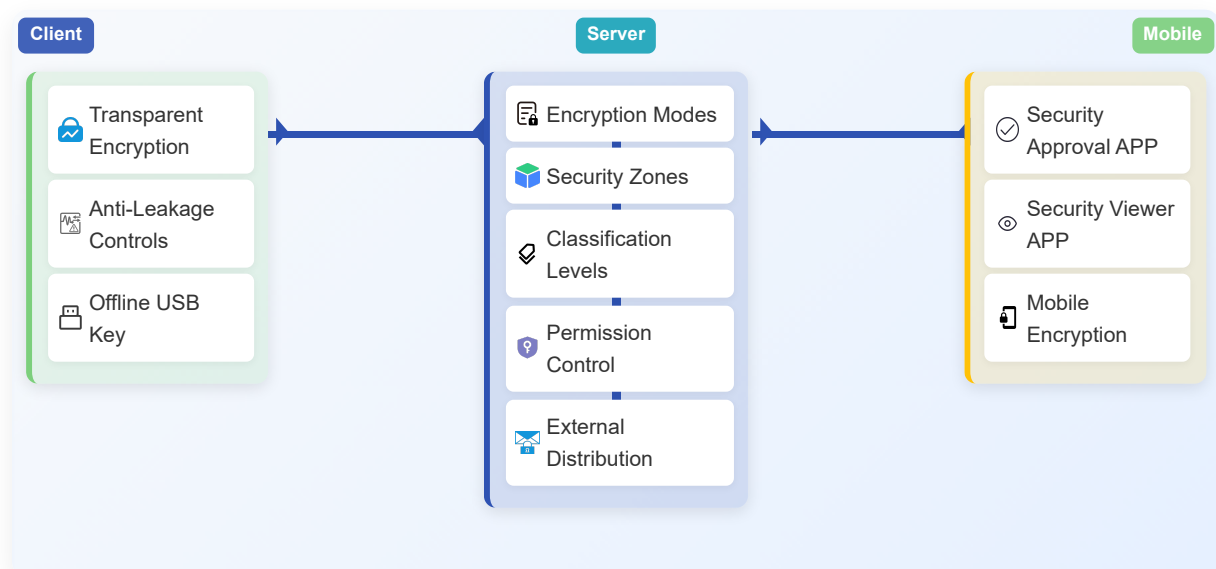
Offline Management

Secure offline access to encrypted documents through USB key authorization for business travelers.



Mobile Support






Mobile applications for document viewing, encryption, and approval workflows on iOS and Android devices.

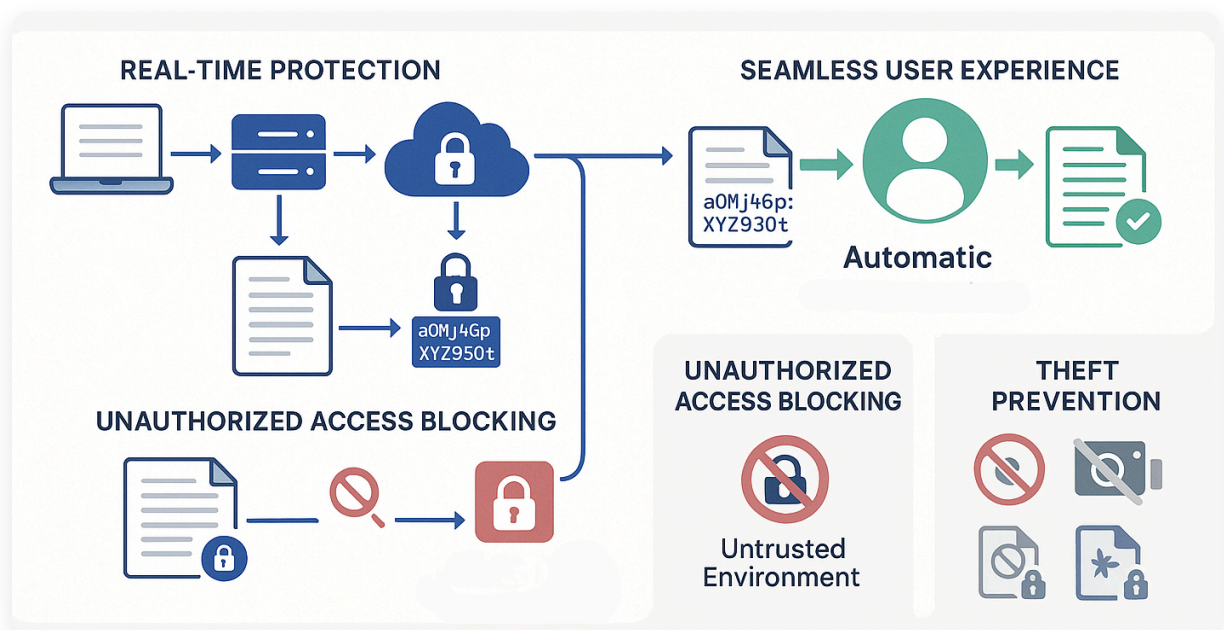


Transparent Encryption

Advanced encryption technology that protects documents without disrupting workflow, ensuring seamless user experience while maintaining robust security.

Core Capabilities

-  **Real-time Protection:** High-strength encryption keeps documents in ciphertext form at all times and locations, whether stored locally or on servers.
-  **Seamless User Experience:** Automatic decryption in trusted environments preserves normal usage habits without requiring additional user operations.
-  **Unauthorized Access Blocking:** Encrypted documents remain inaccessible in untrusted environments, preventing data leakage even if devices are lost or stolen.
-  **Theft Prevention:** Blocks content extraction via clipboard, screenshots, and virtual printing to prevent unauthorized copying of sensitive information.
-  **Comprehensive File Support:** Compatible with all major document formats including Office, PDF, CAD, images, and custom application files.





Flexible Encryption Modes

Multiple encryption modes to meet diverse business requirements, ensuring appropriate protection levels for different document types and usage scenarios.



Mandatory Encryption

- Automatic encryption for specified document types
- No manual intervention required
- Ideal for highly sensitive documents
- Prevents accidental unencrypted saving
- Customizable by file type and department



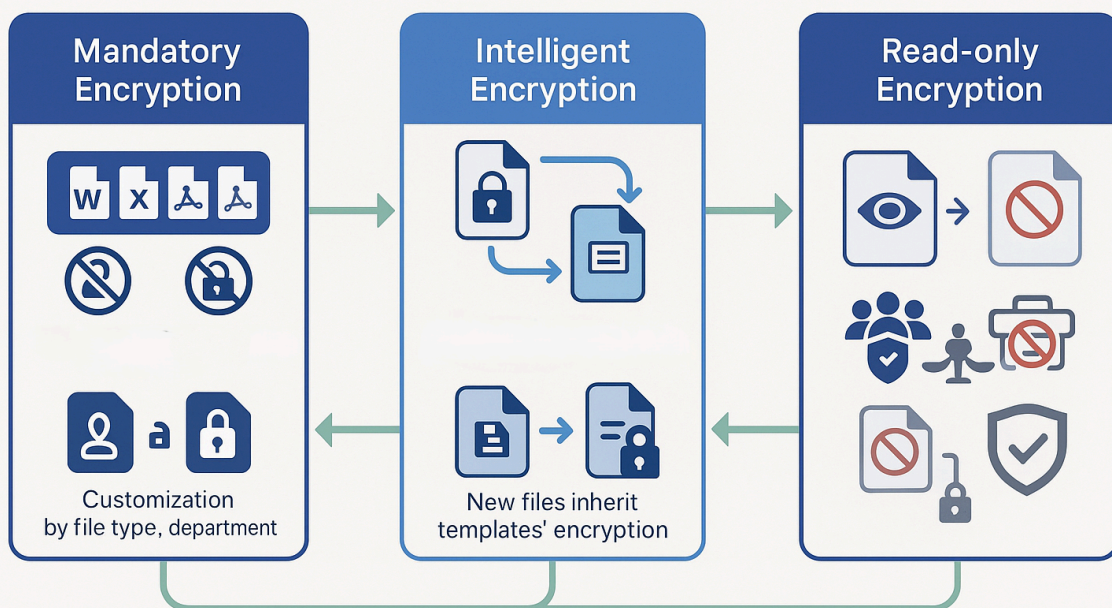
Intelligent Encryption

- Maintains encryption status through modifications
- New files inherit encryption from templates
- Preserves security during collaborative editing
- Adapts to user workflow patterns
- Balances security and usability



Read-only Encryption






- Allows viewing without modification rights
- Prevents unauthorized edits to sensitive data
- Ideal for reference documents and archives
- Can restrict copying and printing functions
- Maintain document integrity and authenticity

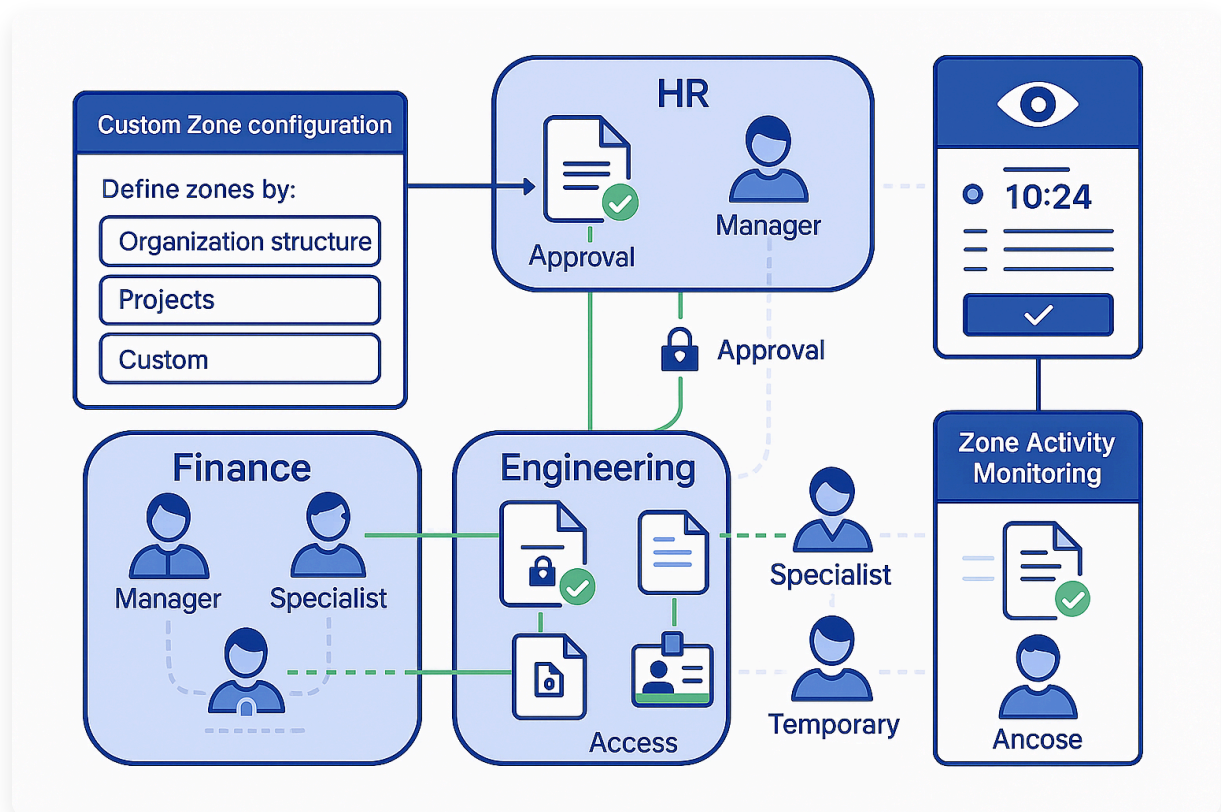


Security Zones

Department and role-based document isolation to prevent unauthorized cross-department access while enabling efficient collaboration within teams.

Zone Management Features

-  **Department-based Isolation:** Create separate security zones for different departments to prevent cross-department access to sensitive information.
-  **Custom Zone Configuration:** Define security zones based on organizational structure, projects, or any other business requirements.
-  **Role-based Access:** Ensure users only access documents appropriate to their department and position within the organization.
-  **Controlled Inter-zone Communication:** Establish secure channels for authorized document sharing between different security zones.
-  **Cross-zone Approval Workflows:** Formal processes for requesting and granting temporary access to documents in other zones.
-  **Zone Activity Monitoring:** Track document access and movement between zones for security auditing and compliance reporting.





Classification Levels

Sensitivity-based document classification with appropriate access restrictions for each level to ensure information is protected according to its importance.

Standard Classification Levels

1 Public Information

Information that can be freely distributed both internally and externally without restrictions.

2 Internal Use Only

Information intended for internal use within the organization but not containing sensitive data.

3 Confidential

Sensitive information that should only be accessed by authorized personnel within specific departments.

4 Restricted

Highly sensitive information with access limited to designated personnel with specific authorization.

5 Top Secret

Critical information with extremely limited access, typically restricted to executive leadership.

Classification Management

Customizable Levels: Organizations can define classification levels that match their specific security requirements.

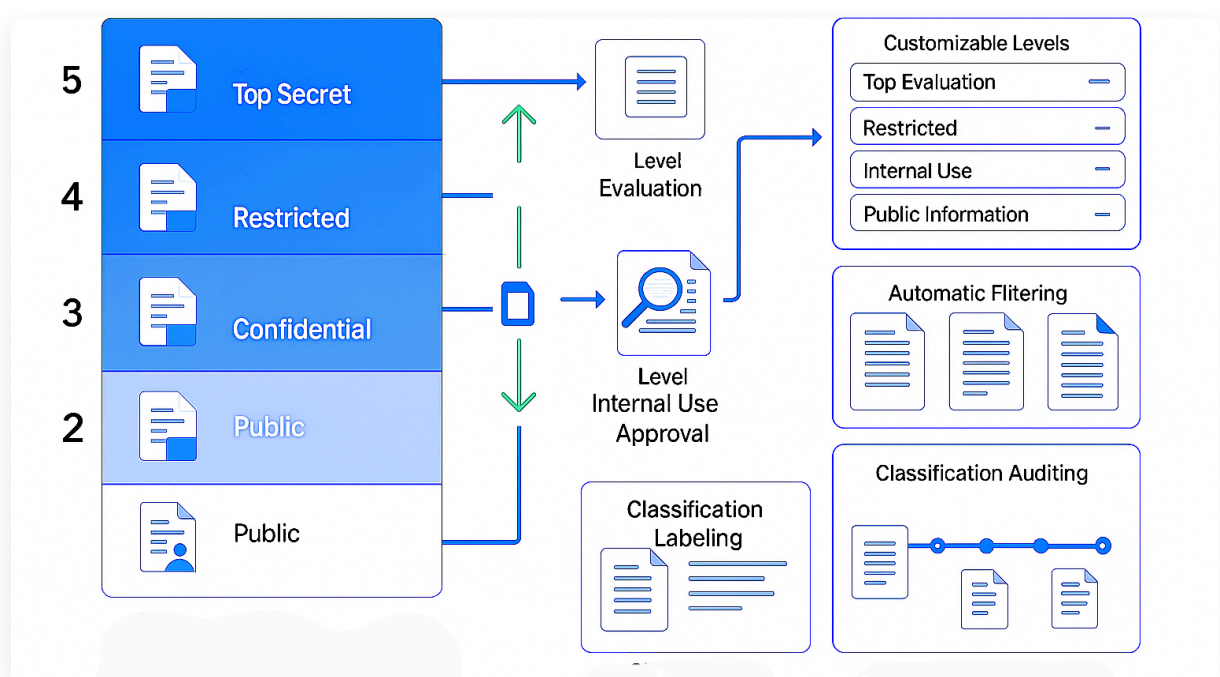
Level Elevation: Allow authorized users to increase document classification levels when sensitive information is added.

Level Reduction Approval: Formal processes for decreasing classification levels to maintain security integrity.

Automatic Filtering: Systems automatically identify and classify documents containing sensitive keywords or patterns.

Classification Labeling: Clear visual indicators of document sensitivity levels in all views and prints.

Classification Auditing: Complete audit trails of all classification changes and access to sensitive documents.








Granular Permission Control


Detailed access rights management to ensure documents are only accessed and used in authorized ways by appropriate personnel.


Permission Types


 **View Permission:** Ability to open and read the document content


 **Edit Permission:** Ability to modify document content


 **Copy Permission:** Ability to copy content from the document

 **Print Permission:** Ability to print the document


 **Save As Permission:** Ability to save copies under different names/locations


 **Share Permission:** Ability to grant access to other users


 **Decrypt Permission:** Ability to remove encryption from the document


 **Screenshot Permission:** Ability to capture images of the document


Advanced Permission Features

 **Granular Access Control:** Set detailed permissions for users based on document confidentiality and user roles.

 **Validity Period:** Set time restrictions for document access permissions, automatically revoking access after expiration.

 **Device Binding:** Restrict document access to specific devices for enhanced security of highly sensitive information.

 **Permission History:** Track all permission changes and access attempts for audit and compliance purposes.

 **Emergency Access:** Define emergency access protocols for authorized personnel to access documents during crises.

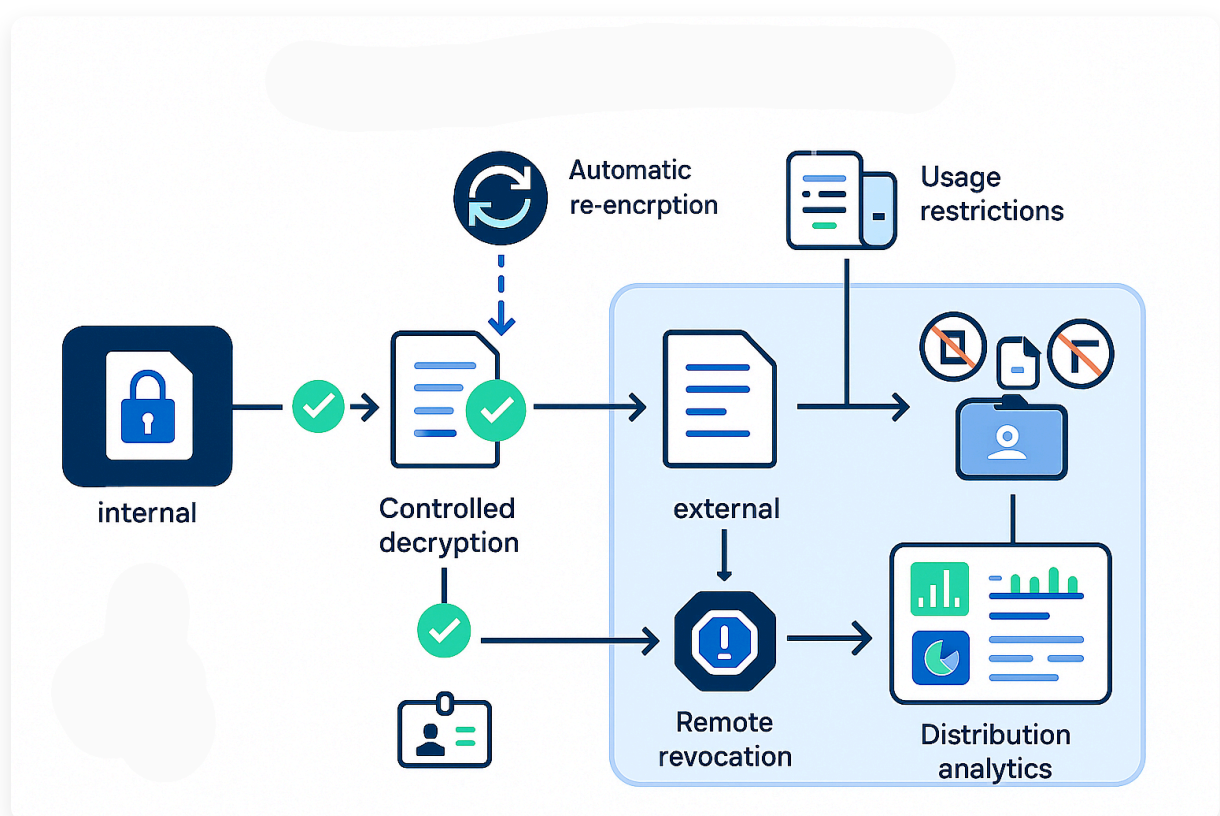


External Distribution

Secure document sharing with external parties while maintaining control over sensitive information and preventing unauthorized distribution.

External Distribution Management

- **Controlled Decryption:** Securely share documents with external parties through approved decryption methods while maintaining control.
- **Automatic Re-encryption:** Decrypted files can be set to re-encrypt after a specified period or upon completion of their intended use.
- 🕒 **Usage Restrictions:** Control viewing period, access count, and other permissions for externally shared documents.
- 🚫 **Secondary Leakage Prevention:** Prevent unauthorized sharing of sensitive documents by external recipients through copy and print controls.
- 👤 **Recipient Authentication:** Verify the identity of external recipients before granting access to sensitive documents.
- 📊 **Distribution Analytics:** Track how external recipients interact with shared documents, including access frequency and duration.
- 📄 **Remote Revocation:** Instantly revoke access to shared documents if circumstances change or security concerns arise.









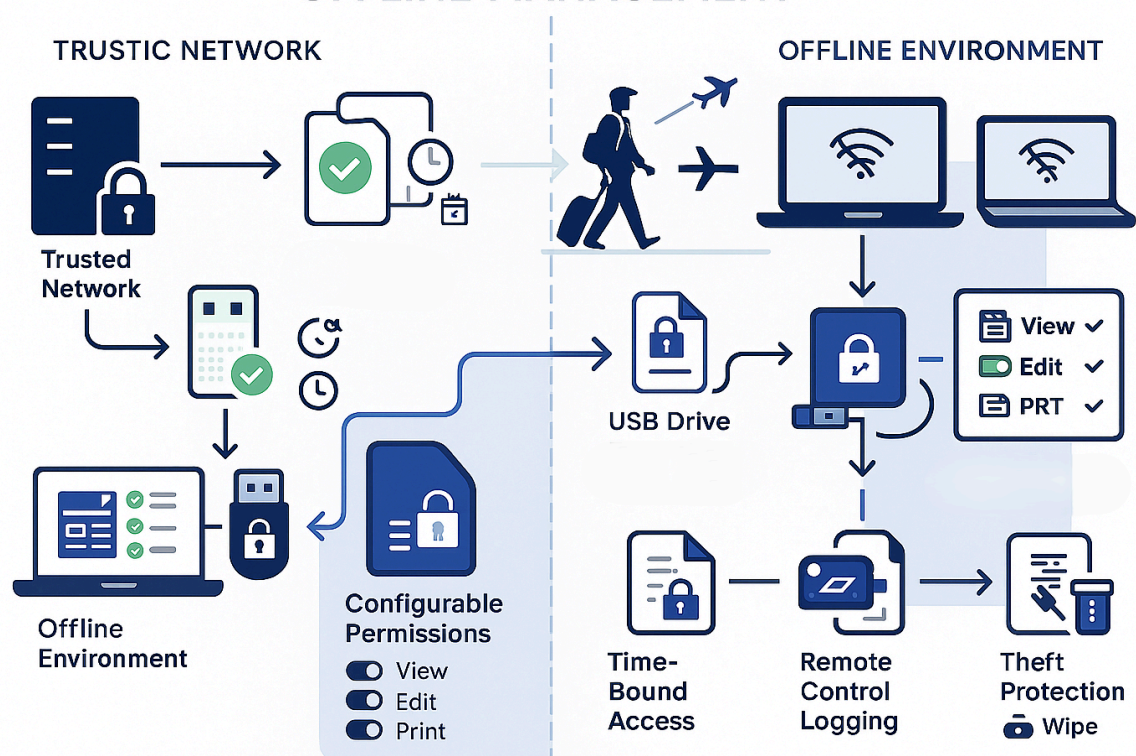
Offline Management

Secure offline access to encrypted documents for business travelers and remote workers while maintaining data protection standards.

Offline Access Solutions

-  **Offline Authorization:** Grant temporary access to encrypted documents outside trusted environments with configurable time limits.
-  **Offline Permission USB Key:** Maintain encryption functionality during business trips with hardware-based authorization for secure portable access.
-  **USB Drive Encryption Client:** Enable/disable encrypted file access using a USB drive without requiring additional software installation.
-  **Configurable Permissions:** Set specific document types and access rights for offline use based on business requirements.
-  **Time-bound Access:** Define precise time windows for offline access to ensure permissions automatically expire after the approved period.
-  **Offline Activity Logging:** Record all document activities during offline use for later synchronization and auditing when reconnected.
-  **Theft Protection:** Remote data wipe capabilities if offline devices are lost or stolen to prevent unauthorized access.






OFFLINE MANAGEMENT








Mobile Support

Mobile applications for document viewing, encryption, and approval workflows to support modern workstyles and business continuity.

Security Approval APP

-  **Instant Notifications:** Real-time alerts for pending approval requests directly to mobile devices.
-  **Quick Approval:** Approve or reject requests with just a few taps without needing to access a desktop computer.
-  **Document Preview:** Review relevant documents associated with approval requests directly on mobile devices.
-  **Approval Comments:** Add comments and instructions when approving or rejecting requests for clear communication.
-  **Approval History:** View past approval decisions and track the status of pending requests.

Security Viewer APP

-  **Encrypted Document Viewing:** Open and view encrypted documents directly on mobile phones and tablets.
-  **Mobile-optimized Viewing:** Documents automatically adjust for optimal viewing on different screen sizes.
-  **Mobile Encryption:** Encrypt or decrypt files directly on mobile devices to maintain security on the go.
-  **Offline Access:** Access previously viewed encrypted documents even when not connected to the network.
-  **Mobile Security Controls:** Prevent unauthorized copying, sharing, and screenshots of sensitive documents on mobile devices.

Mobile Platform Support



iOS Support

Compatible with iPhone and iPad running iOS 6.0 and above, with full support for the latest devices.



Android Support

Works with Android devices running version 4.0 and above from all major manufacturers.

Application Scenarios

1. Enterprise Confidential Document Protection

The Challenge

A large enterprise with multiple departments struggles to control access to sensitive documents. Confidential information frequently leaks between departments, and the company lacks visibility into document usage and distribution paths.

The Solution with AnySecura

Implementing comprehensive **Security Zones** and **Classification Levels** capabilities:

1. Create separate security zones for each department with controlled access points
2. Classify documents by sensitivity levels with appropriate access restrictions
3. Implement automated encryption based on document classification
4. Establish cross-department document sharing approval workflows

Results Achieved

- ✓ 95% reduction in unauthorized cross-department document access
- ✓ 100% visibility into document access and modification history
- ✓ 80% decrease in information leakage incidents

2. Secure External Document Collaboration

The Challenge

A technology company needs to share proprietary information with external partners and clients while maintaining control. Once documents are shared externally, the company loses visibility and control, creating significant IP protection risks.

The Solution with AnySecura

Leveraging **External Distribution** and **Granular Permission Control**:

1. Implement controlled decryption for external document sharing
2. Set time-limited access permissions for external partners
3. Restrict copying, printing, and further distribution capabilities
4. Monitor document access and usage by external recipients
5. Maintain remote revocation capabilities

Results Achieved

- ✓ Complete control over documents even after external distribution
- ✓ 100% visibility into external document usage patterns
- ✓ Elimination of unauthorized secondary distribution of sensitive documents

Core Values & Benefits



Comprehensive Security

End-to-end document protection across the entire lifecycle with multiple layers of security controls to prevent unauthorized access and data leakage.



Seamless User Experience

Transparent encryption that works automatically without disrupting established workflows or requiring users to change their habits.



Granular Control

Precise permission management and flexible security policies that can be tailored to meet specific business requirements and security needs.



Enhanced Collaboration

Secure information sharing both internally and externally while maintaining control, enabling efficient collaboration without compromising security.

Ready to Secure Your Sensitive Documents?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



www.anysecura.com



support@anysecura.com

© 2025 AnySecura SOFTWARE PTE. LTD. All rights reserved. Enterprise-grade security solutions.