AnySecura

Document Control

Comprehensive document security solution

Monitor · Control · Protect · Audit

Module Overview

AnySecura Document Control integrates four core capabilities, providing enterprises with complete visibility and control over document activities to prevent data leakage and ensure secure document management.

Comprehensive Operation Logging

Tracks all document activities across storage locations with specialized audits for burning operations and ADB transfers.

Granular Operation Controls

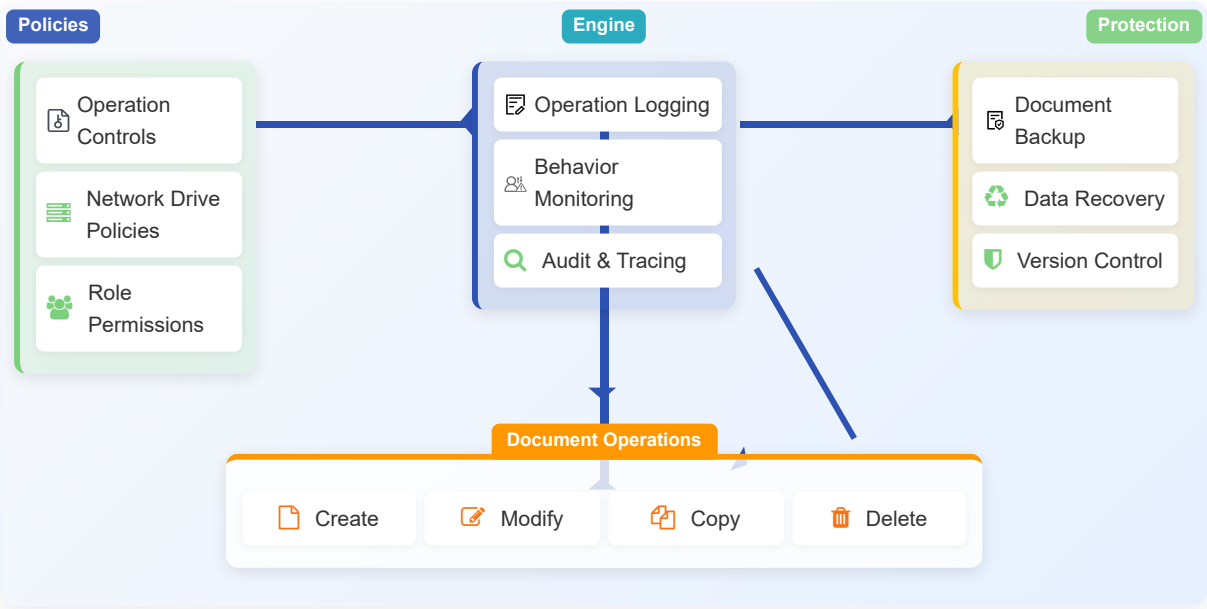
Manages permissions for document operations and regulates network drive copying through formal processes.

Critical Behavior Monitoring

Captures screen recordings during high-risk actions for security forensics and audit trails.

Protection & Backup

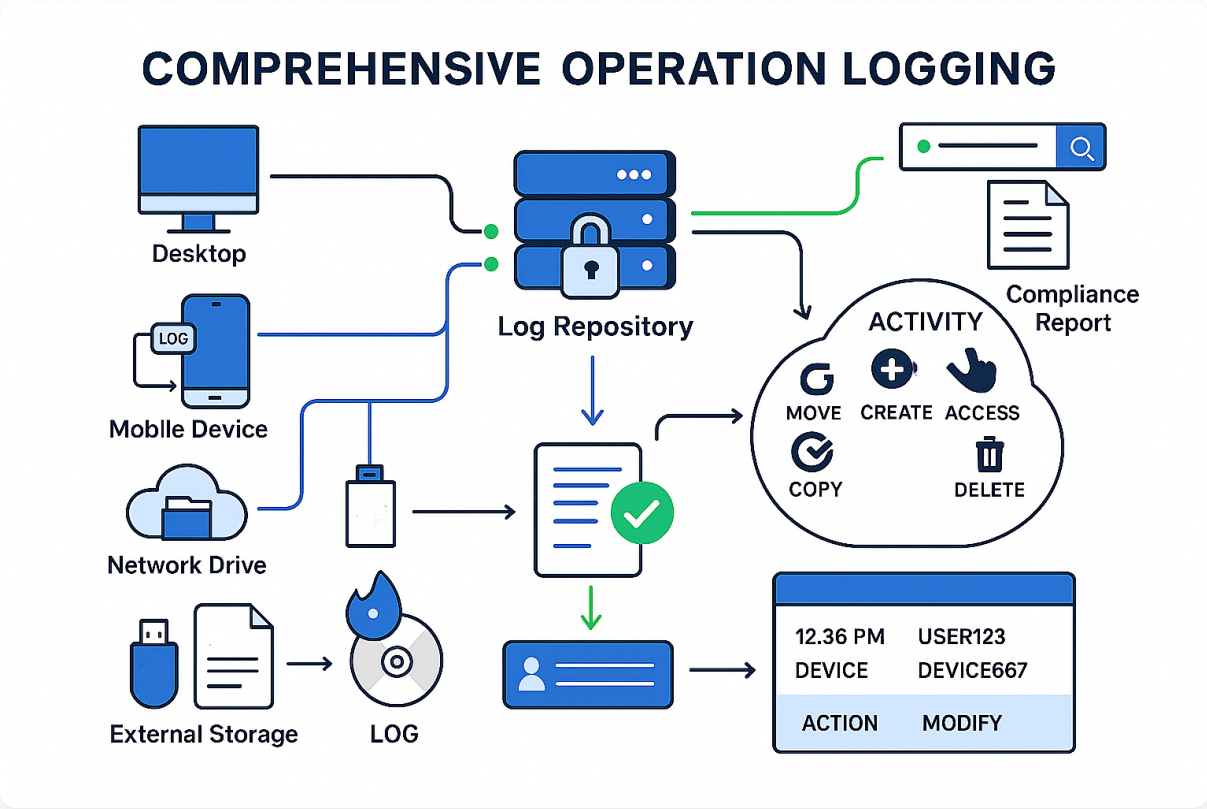
Automatically backs up important documents when tampered with or deleted, preventing data loss.



Comprehensive Operation Logging

Detailed tracking of all document-related activities across various storage locations and devices to maintain complete audit trails.

- **Core Activity Tracking:** Records creation, access, modification, copying, moving, deletion, recovery, and renaming of documents across all storage locations.
- **Multi-location Monitoring:** Tracks document operations on hard disks, mobile storage, network paths, and shared directories.
- **Burning Audit:** Logs CD/DVD burning details including user, device, file information, and number of copies with backup capabilities.
- **ADB Transfer Monitoring:** Records file transfers via external devices connected in ADB mode for mobile device security.
- **Forensic-Ready Records:** Maintains detailed logs with timestamps, user information, and device identifiers for investigations.
- **Centralized Log Management:** Aggregates all document activity logs in a secure, searchable repository for compliance reporting.



Granular Operation Controls

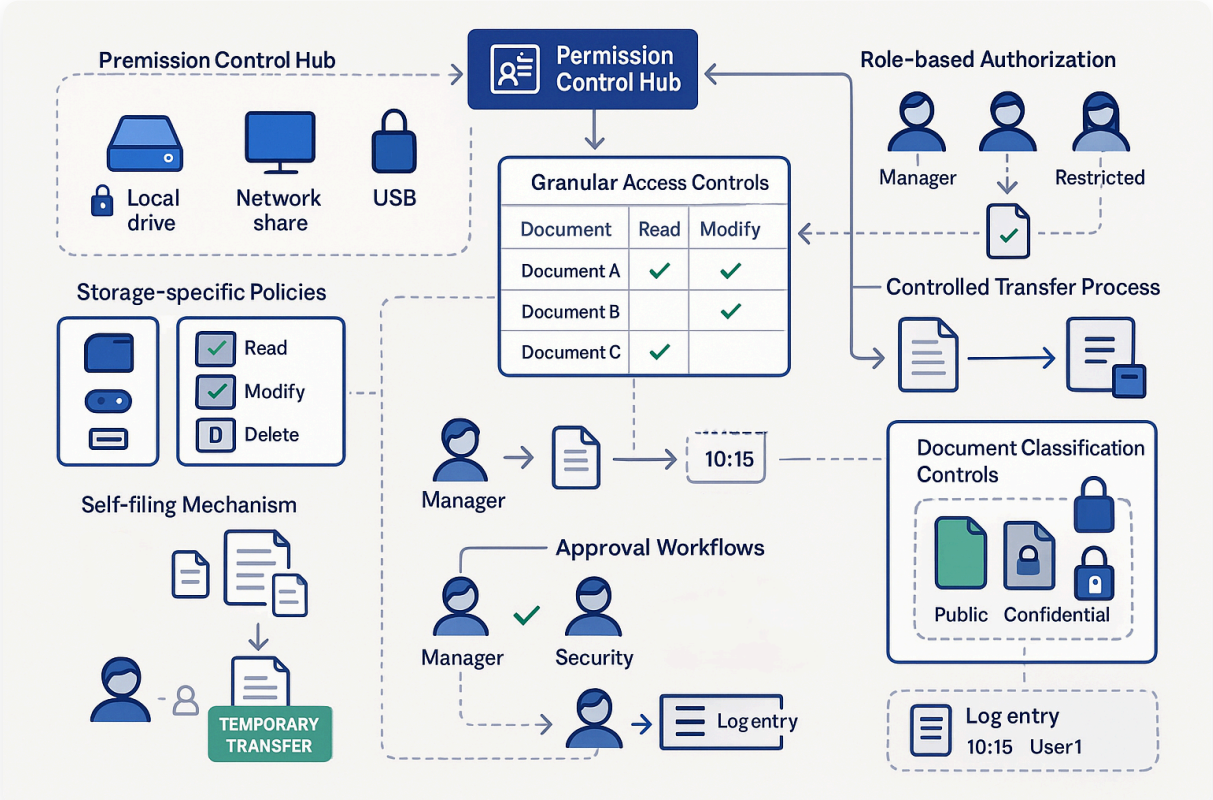
Precise management of document access and transfer capabilities to prevent unauthorized operations and ensure data security.

Permission Management

- **Granular Access Controls:** Regulates read, modify, and delete permissions for specified documents on targeted storage locations.
- **Storage-specific Policies:** Applies different permission sets based on storage type (local drive, network share, USB, etc.).
- **Role-based Authorization:** Assigns document operation permissions based on organizational roles and responsibilities.
- **Document Classification Controls:** Enforces different access rules based on document sensitivity levels.

Network Drive Management

- **Controlled Transfer Process:** Manages secure copying to network drives through formal application procedures.
- **Self-filing Mechanism:** Allows authorized users to copy documents after proper documentation and registration.
- **Approval Workflows:** Implements multi-level approval processes for sensitive document transfers.
- **Transfer Auditing:** Maintains complete records of all network drive transfers with user attribution.



Critical Behavior Monitoring

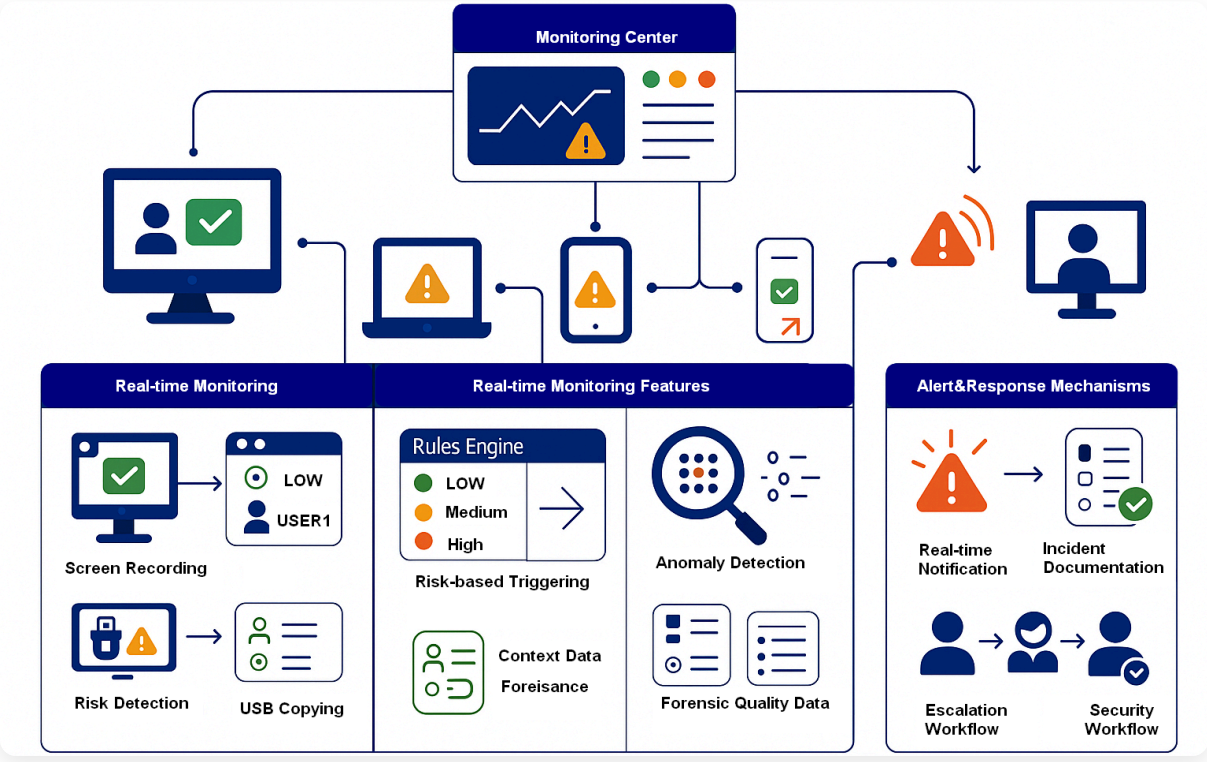
Proactive surveillance of high-risk document operations to prevent data leakage and support incident investigations.

Real-time Activity Monitoring

- **Screen Recording:** Captures video recordings during critical operations like file deletion or copying to mobile storage.
- **Risk-based Triggering:** Automatically activates monitoring based on predefined high-risk behaviors.
- **Context Preservation:** Records detailed context including user, time, location, and associated applications.
- **Forensic Quality Data:** Provides admissible evidence for investigations into potential data leakage incidents.

Alert & Response Mechanisms

- **Real-time Notifications:** Triggers immediate alerts for suspicious document operations requiring attention.
- **Anomaly Detection:** Identifies unusual document access patterns that may indicate security threats.
- **Incident Documentation:** Automatically compiles evidence packages for security incidents involving documents.
- **Escalation Workflows:** Follows predefined procedures for escalating critical security events to appropriate personnel.



Protection & Backup

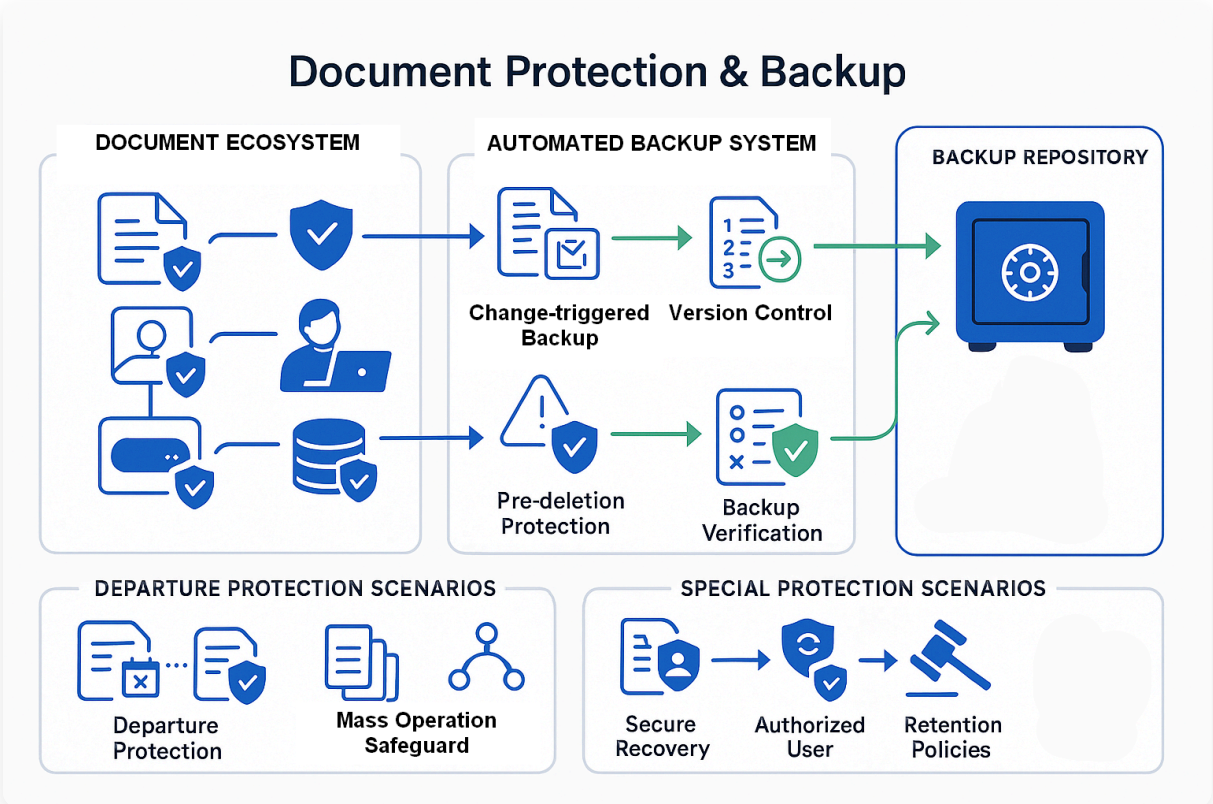
Comprehensive measures to prevent data loss and ensure recoverability of critical documents, even in cases of accidental or intentional damage.

Automated Backup Systems

- **Change-triggered Backups:** Creates secure backups automatically when documents are modified, deleted, or moved.
- **Version Control:** Maintains multiple versions of documents to restore previous states if needed.
- **Pre-deletion Protection:** Implements mandatory backups before critical files can be deleted.
- **Backup Verification:** Automatically validates backup integrity to ensure recoverability when needed.

Special Protection Scenarios

- **Departure Protection:** Activates special backup policies for employees leaving the organization to prevent data deletion.
- **Mass Operation Safeguards:** Detects and requires additional approvals for bulk document deletion or modification.
- **Secure Recovery:** Provides controlled access to backups for authorized personnel only with complete audit trails.
- **Retention Policies:** Enforces document retention periods based on business requirements and compliance regulations.



Application Scenarios

1. Audit Document Operations

The Challenge

A multinational corporation experiences frequent information leaks but lacks the ability to trace the source of leaked documents. They need visibility into how confidential files are being accessed, copied, and distributed across the organization.

The Solution with AnySecura

Implementing **Operation Logging** and **Behavior Monitoring**:

1. Track all document activities including access, modification, and distribution
2. Monitor USB copying and network uploads of sensitive documents
3. Record screen activities during high-risk operations
4. Generate detailed audit trails for investigation of information leaks
5. Create comprehensive reports on document circulation patterns

Results Achieved

- Successful identification of leakage sources in 92% of incidents
- 47% reduction in unauthorized document distribution
- Complete visibility into document lifecycle and circulation

2. Restrict Sensitive Document Operations

The Challenge

A financial institution needs to ensure only authorized personnel can modify or delete sensitive financial documents, while allowing read-only access for other employees who need information for client services.

The Solution with AnySecura

Implementing **Granular Operation Controls** and **Document Protection**:

1. Define role-based permissions for sensitive financial documents
2. Restrict modification and deletion rights to authorized personnel only
3. Allow read-only access for client service representatives
4. Implement approval workflows for network transfers of sensitive files
5. Create automatic backups before any deletion of critical documents

Results Achieved

- 100% compliance with financial data protection regulations
- Elimination of unauthorized modifications to financial records
- Balanced security and accessibility for business operations

Core Values & Benefits

Complete Visibility

Full visibility into all document activities across the enterprise with detailed audit trails and monitoring capabilities. Track document lifecycle from creation to deletion with comprehensive logs.

Enhanced Security

Prevent unauthorized document operations and data leakage through granular controls and proactive monitoring. Implement role-based access and prevent unauthorized transfers.

Data Protection

Ensure critical business documents are protected against accidental or intentional deletion with automated backup mechanisms and version control.

Compliance Assurance

Meet regulatory requirements with comprehensive audit trails, access controls, and data governance capabilities. Generate compliance reports with ease.

Ready to Secure Your Document Operations?

Learn More About Solutions

Contact Our Experts

www.anysecura.com

support@anysecura.com