



# AnySecura

## Sensitive Content Inspection

Advanced content analysis and protection solutions

Define · Discover · Classify · Monitor · Protect · Audit

### SENSITIVE CONTENT RECOGNITION





# Module Overview

AnySecura Sensitive Content Inspection is an enterprise-grade solution for intelligent content security management. It integrates six core capabilities to build a full-cycle protection system for sensitive information, helping organizations prevent data leakage and ensure compliance with security policies.



## Content Definition & Discovery

Define sensitive information through keywords and regular expressions, with local/remote scanning capabilities and backup functions.



## Tag Classification Level

Automatically add tags and classification levels to files containing specific sensitive content during creation or modification.



## External Transmission Management

Monitor and control external transmissions through multiple channels, with application and filing mechanisms for authorized cases.



## Local Storage Protection

Monitor local file operations and provide encryption, watermarking, and decryption warning for sensitive content.



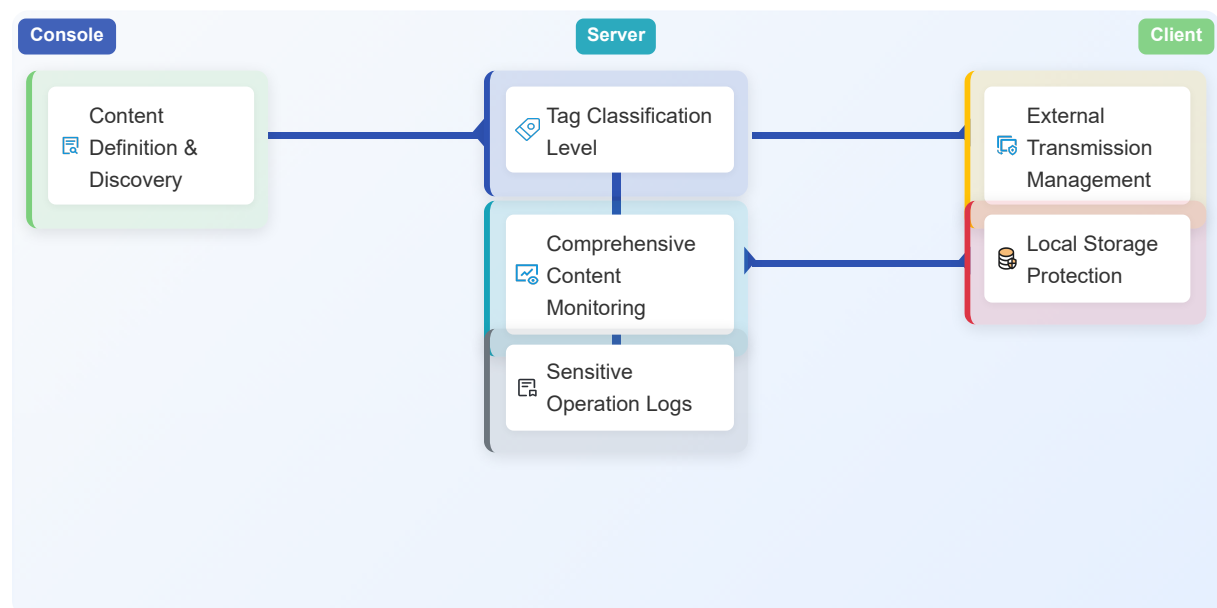
## Comprehensive Content Monitoring

Real-time monitoring of file operations, external transmissions, clipboard activities, and IM chats with audit capabilities.



## Sensitive Operation Logs

Detailed recording of all sensitive information operations including transmission, storage, and access activities.



## Content Definition & Discovery

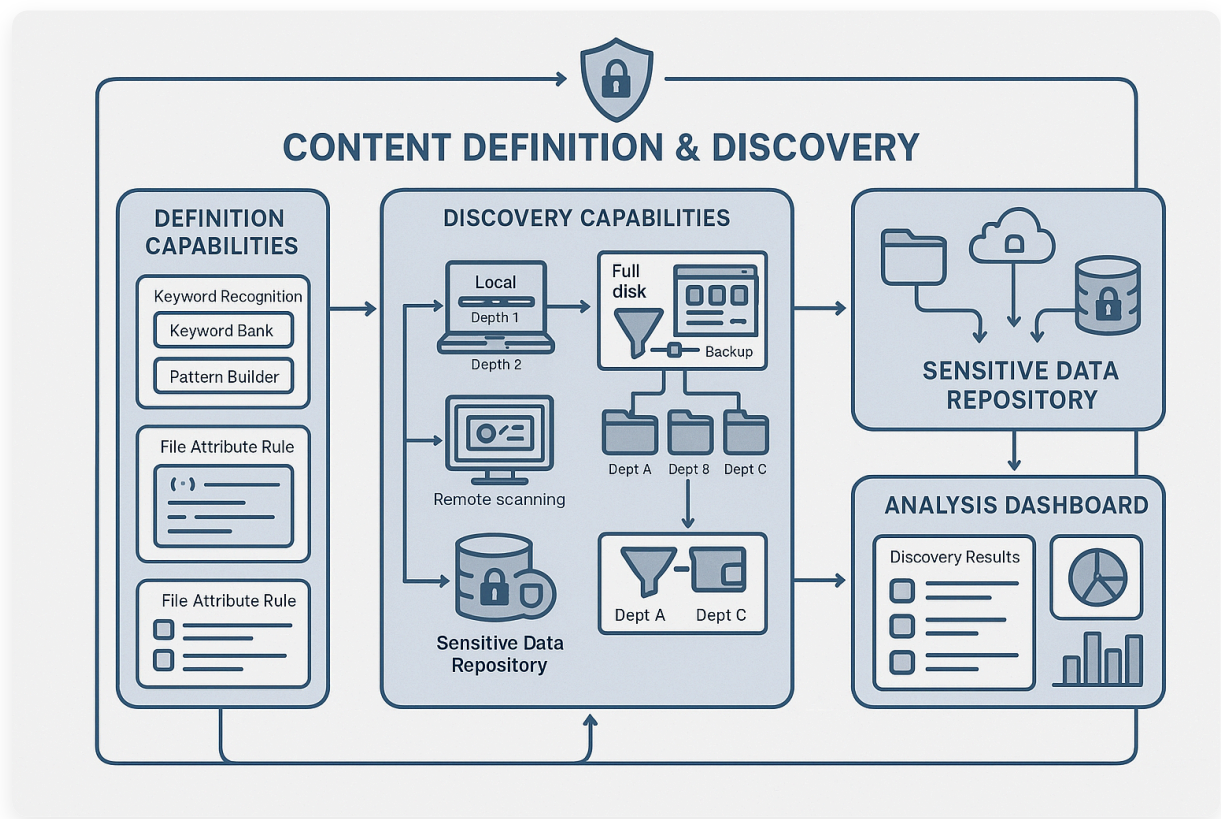
Comprehensive mechanisms to define and proactively discover sensitive information across enterprise data repositories.

### Definition Capabilities

- ✓ **Keyword Recognition:** Define sensitive information through specific keywords and phrases.
- ✓ **Regular Expressions:** Create complex pattern matching rules for structured sensitive data.
- ✓ **File Attribute Rules:** Define sensitivity based on file names, types, attributes, and sizes.

### Discovery Capabilities

- ✓ **Local Scanning:** Scan individual endpoints for sensitive content with configurable depth.
- ✓ **Remote Scanning:** Centrally initiate scans across multiple devices and departments.
- ✓ **Full-Disk Scanning:** Comprehensive scanning with backup for sensitive files discovered.
- ✓ **Targeted Discovery:** Scan specific departments (e.g., sales) for documents with sensitive keywords.



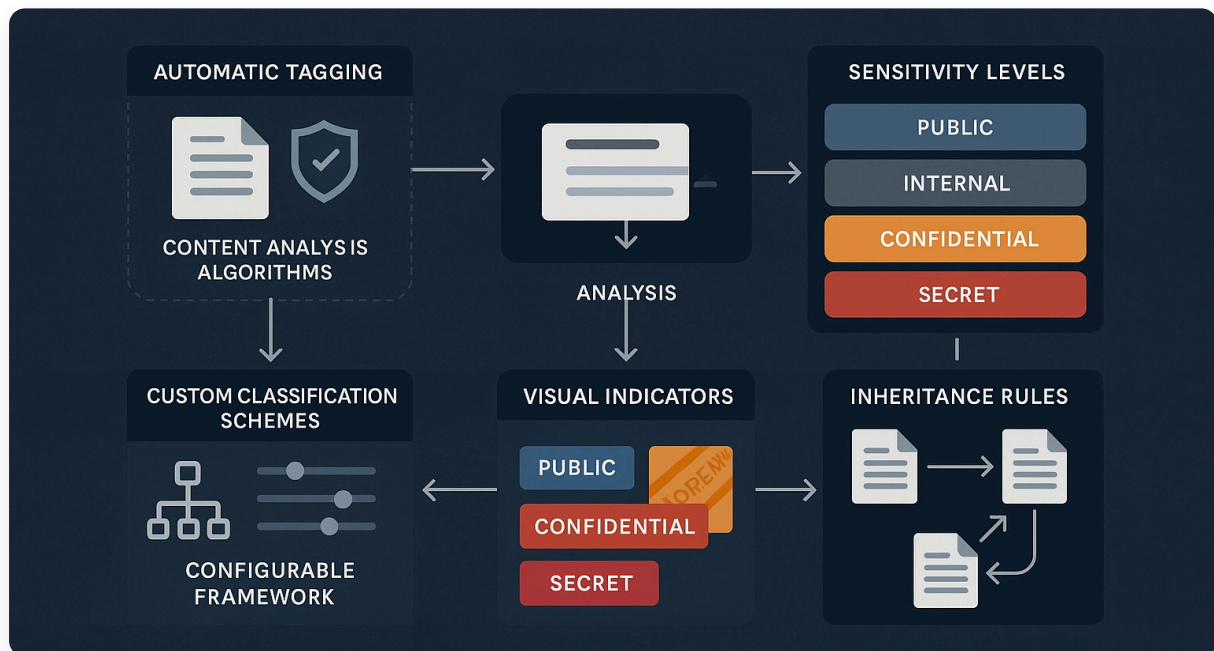




# Tag Classification Level

Automated classification system to manage sensitive content based on predefined levels and tags.

- **Automatic Tagging:** Add appropriate tags to files containing sensitive content when users create or modify documents.
- **Sensitivity Levels:** Assign classification levels (public, internal, confidential, secret) based on content sensitivity.
- **Visual Indicators:** Clear marking of sensitive content for users with classification labels and visual cues.
- **Custom Classification Schemes:** Support for organization-specific classification frameworks and taxonomies.
- **Inheritance Rules:** Automated propagation of classification levels through document relationships and hierarchies.





# External Transmission Management

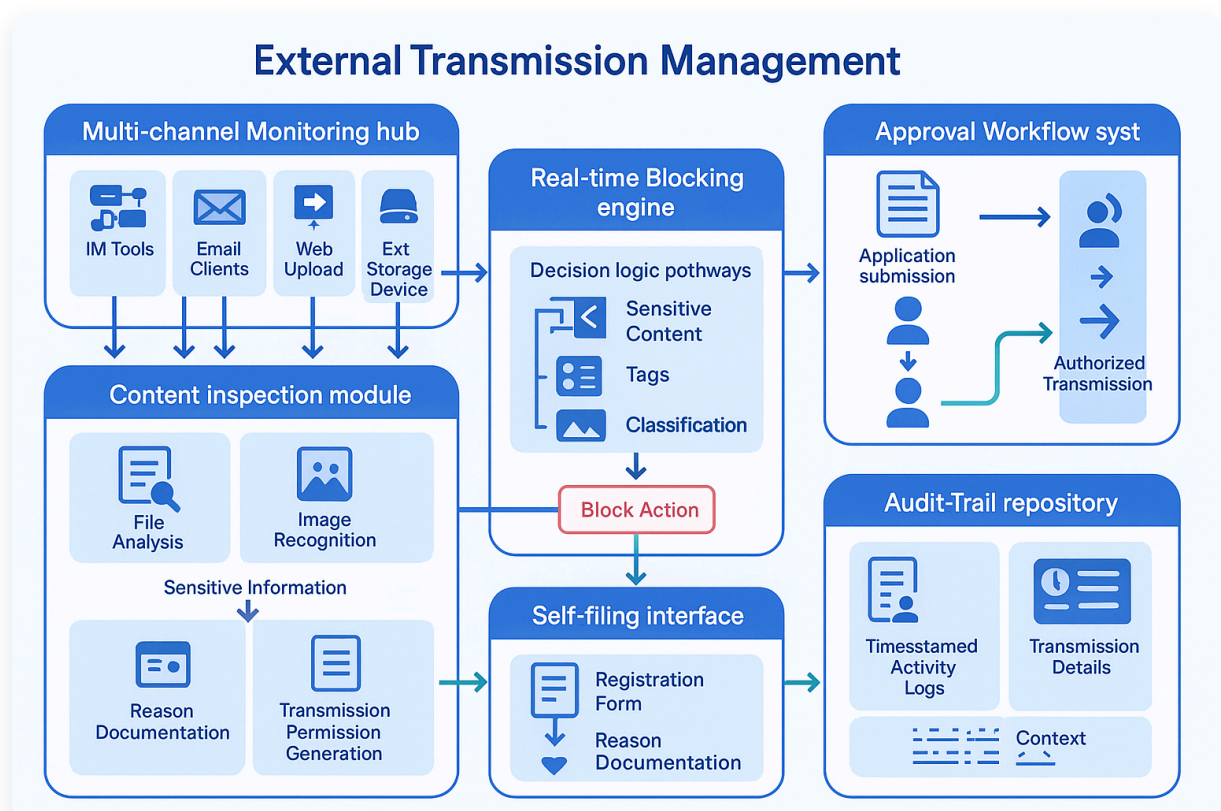
Comprehensive control over sensitive information transmission through various channels to prevent unauthorized data leakage.

## Transmission Control

- 🛡️ **Multi-channel Monitoring:** Monitor files transmitted through IM tools, emails, web uploads, network disks, and storage devices.
- 🛡️ **Real-time Blocking:** Automatically block transmission of files containing sensitive content, tags, and classification levels.
- 🛡️ **Content Inspection:** Analyze both files and pictures for sensitive information before transmission.

## Transmission Application and Filing

- 📄 **Approval Workflow:** Submit external transmission applications for sensitive files requiring legitimate sharing.
- 📄 **Self-filing Mechanism:** Allow transmission after self-filing and registration for traceability.
- 📄 **Audit Trail:** Record all approved transmission activities with complete context information.





# Local Storage Protection

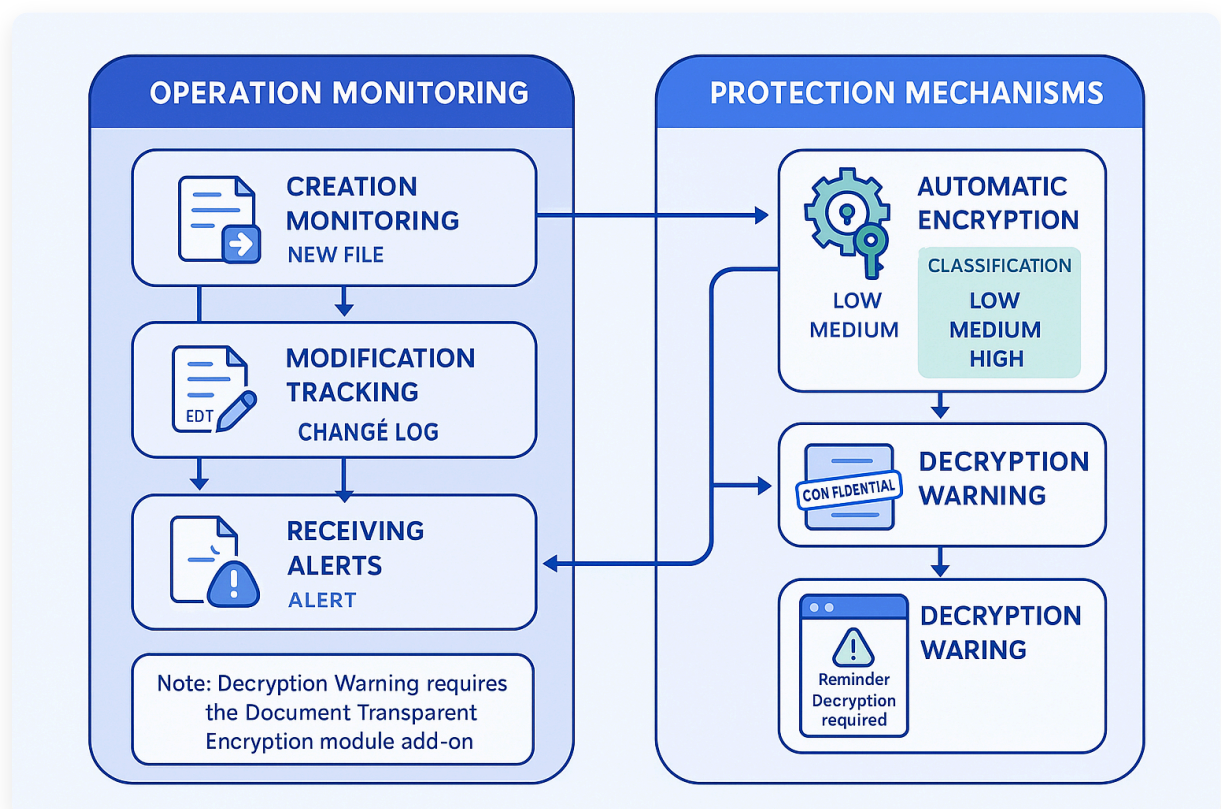
Comprehensive protection mechanisms for sensitive content stored on local devices and endpoints.

## Operation Monitoring

- 👁️ **Creation Monitoring:** Track the creation of new files containing sensitive content or classified information.
- 👁️ **Modification Tracking:** Monitor changes made to existing files with sensitive content or classification tags.
- 👁️ **Download Monitoring:** Track the downloading of sensitive files to local storage from network locations.
- 👁️ **Receiving Alerts:** Monitor files containing sensitive content received from external sources or other users.

## Protection Mechanisms

- 🔒 **Automatic Encryption:** Encrypt files containing sensitive content based on their classification levels.
- 🔒 **Watermarking:** Add identifying watermarks to sensitive documents to prevent unauthorized sharing.
- 🔒 **Decryption Warning:** Pop-up reminders about sensitive information classification during decryption attempts.
- 📌 **Note:** Decryption warning requires purchase of document transparent encryption module.





# Comprehensive Content Monitoring

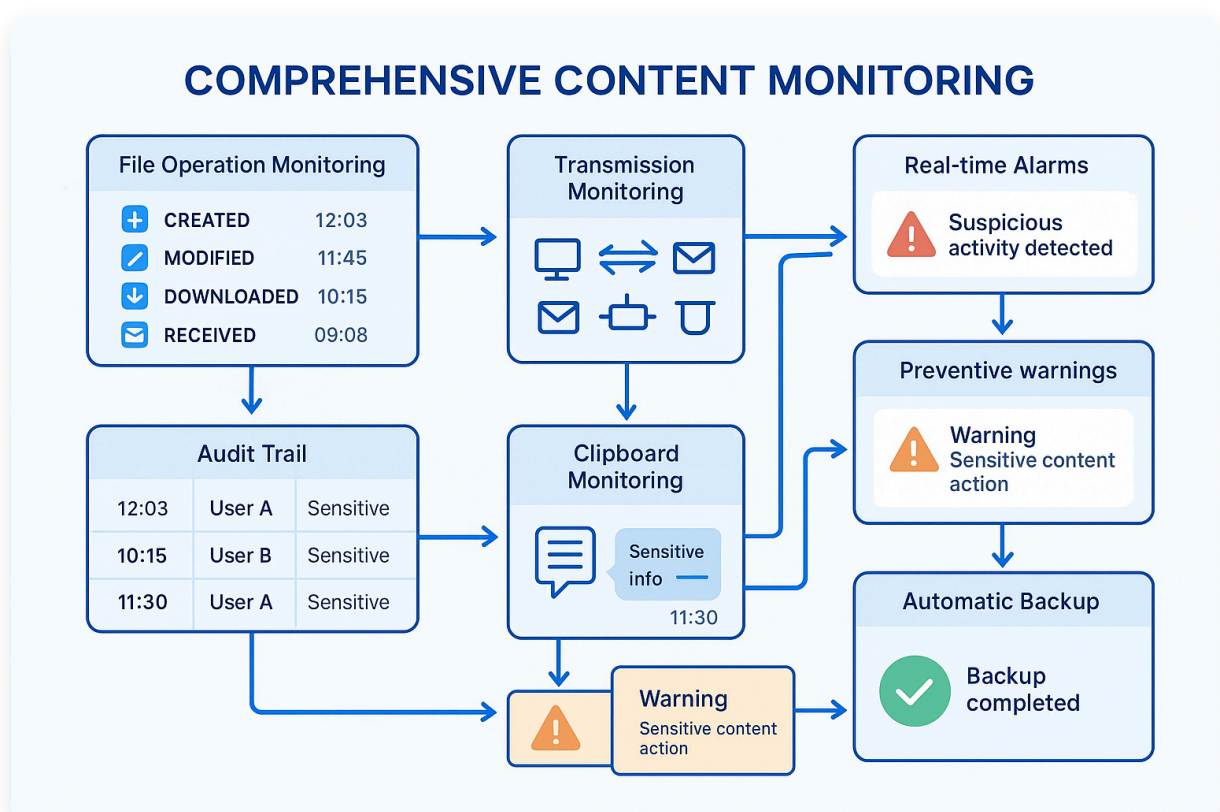
Real-time surveillance of sensitive content activities across all enterprise channels and operations.

## Monitoring Capabilities

- 👁️ **File Operation Monitoring:** Track creation, modification, downloading, and receiving of sensitive files.
- 👁️ **Transmission Monitoring:** Monitor external transmissions through various channels including printing activities.
- 👁️ **Clipboard Monitoring:** Real-time monitoring of clipboard content with sensitive information identification.
- 👁️ **IM Content Monitoring:** Monitor chat messages sent and received through IM tools with context recording.

## Response Mechanisms

- 🔔 **Audit Trail:** Comprehensive documentation of all sensitive content activities for compliance purposes.
- 🔔 **Real-time Alarms:** Instant notifications for suspicious activities involving sensitive information.
- 🔔 **Preventive Warnings:** Proactive alerts to users when handling sensitive content in potentially risky ways.
- 🔔 **Automatic Backup:** Secure backup of sensitive content before potentially risky operations.










# Sensitive Operation Logs

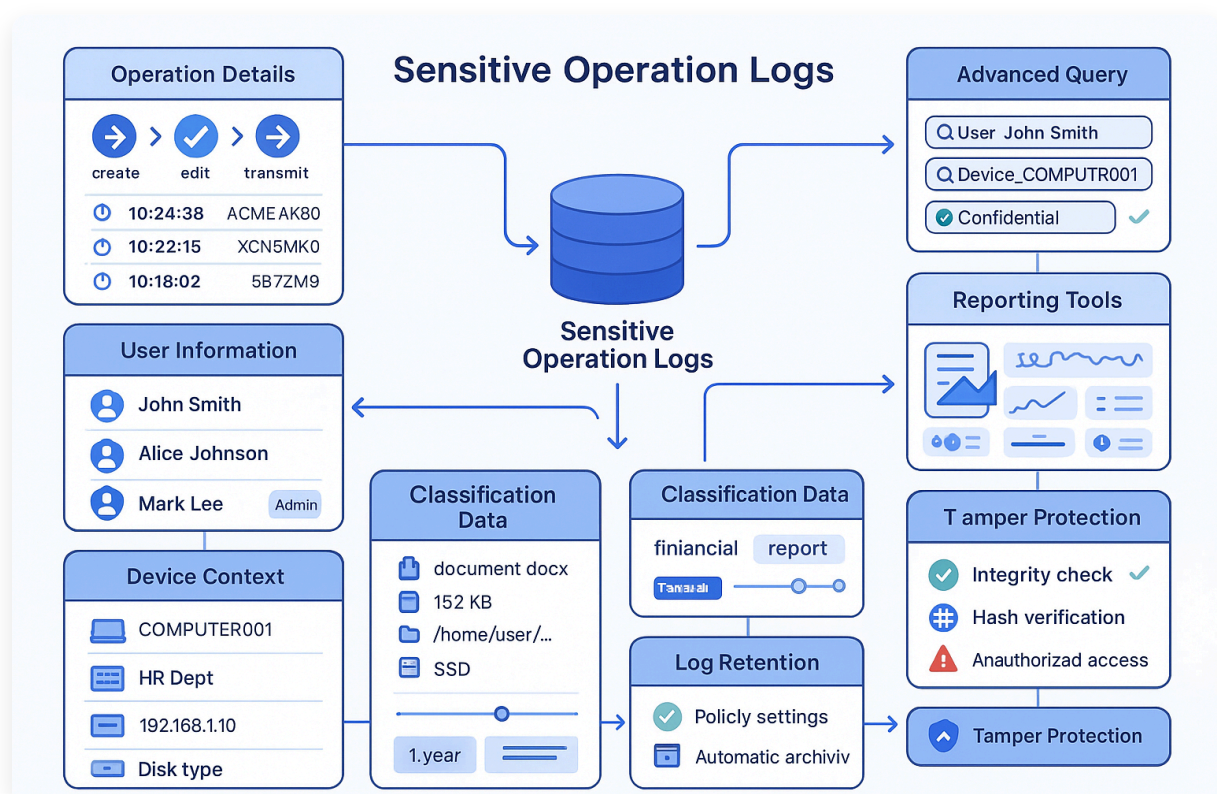
Detailed recording of all sensitive information operations for compliance and investigation purposes.

## Log Content

-  **Operation Details:** Record operation type, timestamp, and related system information for each sensitive content activity.
-  **User Information:** Document user and user group details associated with sensitive content operations.
-  **Device Context:** Log computer name, group affiliation, and network location for each operation.
-  **File Metadata:** Record file name, size, path, and disk type for complete traceability of sensitive content.
-  **Classification Data:** Log sensitivity levels and tags associated with the content being accessed or transmitted.

## Log Management

-  **Advanced Query:** Powerful search capabilities to quickly locate specific log entries based on multiple criteria.
-  **Reporting Tools:** Generate compliance reports and analytics on sensitive content activities.
-  **Log Retention:** Configurable retention policies to meet regulatory requirements for audit trail preservation.
-  **Tamper Protection:** Ensure log integrity with protection against unauthorized modification or deletion.





# Application Scenarios



## 1. Sales Department Data Protection

### The Challenge

A technology company's sales department handles sensitive customer contracts and pricing information. Management discovers that confidential documents are being stored on public computers and shared through unauthorized channels. The company needs to prevent data leakage while maintaining efficient sales operations.

### The Solution with AnySecura

Implementing **Content Discovery** and **Transmission Control** features:

1. Define sensitive information patterns for customer contracts and pricing data
2. Configure batch scanning to detect sensitive documents in the sales department
3. Set rules to prevent storage of sensitive documents on public computers with automatic alarms
4. Block unauthorized transmission through IM tools, emails, and USB drives
5. Implement comprehensive logging for all sensitive content operations

## Results Achieved

- ✓ 100% prevention of sensitive document storage on unauthorized devices
- ✓ 95% reduction in unauthorized file transmission attempts
- ✓ Complete audit trail for compliance and security investigations

## 2. Customer Service Information Security

---

### The Challenge

A financial services company's customer service team frequently handles sensitive customer data through various communication channels. Employees sometimes accidentally share confidential information through instant messaging or email attachments. The company needs to prevent data leakage while maintaining efficient customer support operations.

### The Solution with AnySecura

Deploying **Content Monitoring** and **Transmission Management** features:

1. Define sensitive financial information patterns and classification rules
2. Enable real-time monitoring of IM chats and email communications
3. Configure automatic blocking of messages containing sensitive customer data
4. Implement clipboard monitoring to prevent sensitive data copying to unauthorized applications
5. Set up approval workflows for legitimate external transmission needs

### Quantifiable Benefits

- ✓ 98% reduction in accidental sensitive data transmissions
- ✓ Enhanced customer trust through improved data protection
- ✓ Compliance with financial data protection regulations





## Core Values & Benefits



### Prevent Data Leakage

Comprehensive content monitoring and transmission control to prevent sensitive information from being shared through unauthorized channels.



### Discover Sensitive Content

Advanced scanning and discovery capabilities to identify sensitive information across enterprise data repositories and endpoints.



### Automated Classification

Intelligent tagging and classification system to automatically categorize sensitive content based on predefined rules and patterns.



### Compliance & Audit

Complete audit trail and compliance reporting for sensitive content operations to meet regulatory requirements and security standards.

## Ready to Protect Your Sensitive Content?

 [Learn More About Solutions](#)

 [Contact Our Experts](#)



[www.anysecura.com](http://www.anysecura.com)



[support@anysecura.com](mailto:support@anysecura.com)

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