Link-s Enterprise-Grade File Encrypted Transmission Solution

Global Auditing: Full Traceability and Permission Control for the Entire Transmission Process

For government, financial, military-industrial and other institutions with stringent data security requirements, the core demand for file transmission has long gone beyond "successful delivery". Instead, it focuses on full-process control over **who transmitted the file, what was transmitted, to whom it was sent, and whether it can be managed**.

The Link-s Audit Management Platform precisely meets the needs of high-security scenarios. With four core capabilities: **traceability, controllability, blockability, and auditability**, it builds a robust security barrier for file transmission and satisfies both compliance management and risk prevention requirements.

I. Full Traceability: Every Transfer Leaves a Record

The Link-s Audit Platform records the entire transmission chain in detail, ensuring **every transfer is logged and every detail is traceable**, providing solid support for compliance audits and post-incident investigation:

- **Sender information**: Accurately records the sender’s account, login IP address, terminal device model and system information to identify the transmission subject;

- **Transmission timestamps**: Detailed records of transmission start time, interruption time (if any), and completion time, clearly showing the full transmission lifecycle;

- **Recipient information**: Complete records of the recipient’s account, IP address and device information to clarify data flow direction;

- **File details**: Precisely logs file name, size and type, enabling full-dimensional traceability of file transfers;

- **Transmission results**: Clearly marks transmission status (success, failure, interrupted, retransmitted) and records the causes of interruptions or retransmissions for troubleshooting.

All audit logs are securely stored long-term and support multi-dimensional quick retrieval by time range, account, file name, transmission status, etc. Target records can be located rapidly without complicated operations, efficiently responding to compliance verification and post-incident traceability needs.

II. Controllable Permissions: Full Lifecycle Management of Accounts

The audit platform provides refined account management covering the entire account lifecycle, making **who is using the system, usage status, and abnormalities fully visible**, controlling transmission permission risks from the source:

- **Unified account management**: Supports centralized addition, deletion and editing of all user accounts within the organization, avoiding security risks caused by redundant accounts;

- **Role-based permission classification**: Configures differentiated operation permissions for different roles based on organizational structure and business needs, realizing **correspondence between rights and responsibilities** and preventing unauthorized operations;

- **Emergency risk control**: When abnormal login, unauthorized transmission or other risky behaviors are detected, administrators can force users to log out with one click to quickly stop the spread of risks;

- **Login behavior traceability**: Fully records each account’s login time, IP address and device, accurately identifying risks such as cross-region login and login from unrecognized devices, and issuing timely security alerts.

III. Content Blocking: Prevent Violation Risks in Advance

Breaking through the limitation of "post-incident traceability", the Link-s Audit Platform achieves **in-process control and proactive blocking**, containing unauthorized transmission risks at the source:

- **File sharing prohibition**: Administrators can ban the sharing of unauthorized or sensitive files with one click to prevent the spread of sensitive data;

- **Blacklist and whitelist control**: Flexibly configures blacklists and whitelists for accounts, IP addresses and file types to precisely allow or block transmissions from specific subjects and specific file types, adapting to diverse scenario requirements;

- **Abnormal behavior alerts**: The system automatically monitors risky behaviors such as batch transmission, high-frequency transmission and cross-regional abnormal transmission, triggering real-time alerts to remind administrators to verify and handle risks promptly.

IV. Exportable Reports: Achieve Compliance with One Click

The audit platform features built-in multi-dimensional statistical reporting, which automatically aggregates transmission data and operation behaviors to meet internal review and regulatory inspection requirements, easily fulfilling compliance mandates:

- **Transmission volume reports**: Summarizes total file transmission volume,

transmission times and other core data by account, department and time, clearly showing transmission load distribution;

- **Behavior audit reports**: Details all user operation records including login, transmission, permission changes, etc., fully presenting operation trajectories;

-**Abnormal event reports**: Compiles unauthorized attempts, transmission failures, abnormal logins and other incidents, clarifying anomaly types and handling status for risk review.

All reports support export to common formats such as PDF and Excel. They can be directly used for internal security reviews or submitted to regulators without additional editing, greatly improving compliance audit efficiency.

V. Core Summary

From subject traceability of "who transmitted the file", to content control of "what was transmitted", from process assurance of "whether transmission is allowed", to risk blocking of "whether it is permitted", the Link-s Global Audit Platform achieves full-process management of **controllable, searchable and traceable** file transmission.

It provides a compliant, efficient and secure audit solution for government, financial, military-industrial and other high-security institutions, safeguarding the security of the entire data transmission chain.