严翼共享 企业级文件加密传输解决方案

全局审计：让传输全程可追溯、权限可管控

对于政府、金融、军工等对数据安全有严苛要求的机构而言，文件传输的核心诉求早已超越“成功送达”，更聚焦于“谁传了、传了什么、传给谁、能不能管”的全流程可控。严翼共享审计管理平台，精准匹配高安全场景需求，以“可追溯、可管控、可阻断、可审计”四大核心能力，筑牢文件传输安全防线，满足合规管控与风险防控双重需求。

一、全程可追溯：每一次传输，都有迹可循

严翼共享审计平台全程记录文件传输全链路信息，实现“每一笔传输有记录、每一个细节可追溯”，为合规审计与事后追溯提供坚实支撑：

- 发送方信息：精准记录发送方账号、登录 IP 地址、终端设备型号及系统信息，明确传输主体；
- 传输时间节点：详细留存传输发起时间、中断时间（如有）、完成时间，清晰呈现传输全周期；
- 接收方信息：完整记录接收方账号、IP 地址、设备信息，明确数据流向；
- 文件详情：精准记录文件名、文件大小、文件类型，实现文件传输全维度溯源；
- 传输结果：明确标注传输状态（成功、失败、中断、重传），同步记录中断/重传原因，便于问题排查。

所有审计日志长期安全留存，支持按时间范围、账号、文件名、传输状态等多维度快速检索，无需繁琐操作，即可快速定位目标传输记录，高效响应合规核查与事后追溯需求。

二、权限可管控：账号全生命周期，全程可控

审计平台提供精细化账号管理能力，覆盖账号全生命周期，实现“谁在用、用没在用、有没有异常”一目了然，从源头管控传输权限风险：

- 账号全量管理：支持组织内所有用户账号的统一添加、删除、编辑，实现账号集中管控，避免冗余账号带来的安全隐患；
- 角色权限分级：基于组织架构与业务需求，为不同角色配置差异化操作权限，实

现“权责对应”，杜绝越权操作；

- 异常紧急管控：发现账号异常登录、违规传输等风险行为时，管理员可一键强制用户下线，快速阻断风险扩散；
- 登录行为追溯：全面记录每个账号的登录时间、登录 IP、登录设备，精准识别异地登录、异常设备登录等风险，及时预警安全隐患。

三、内容可阻断：违规风险，提前防控

严翼共享审计平台突破“事后追溯”的局限，实现“事中管控、提前阻断”，将违规传输风险控制在萌芽状态：

- 文件分享封禁：管理员可针对违规文件、敏感文件，一键禁止其分享行为，避免敏感数据扩散；
- 黑白名单管控：灵活配置账号、IP 地址、文件类型黑白名单，精准允许或禁止特定主体、特定类型文件的传输，适配不同场景管控需求；
- 异常行为告警：系统自动监测批量传输、高频传输、跨地域异常传输等风险行为，实时触发告警，提醒管理员及时核查处置，实现风险早发现、早管控。

四、报表可导出：合规审计，一键达标

审计平台内置多维度统计报表功能，自动汇总传输数据与操作行为，适配内部审查与监管部门核查需求，轻松满足合规要求：

- 传输量统计报表：按账号、部门、时间维度，汇总文件传输总量、传输次数等核心数据，清晰呈现传输负载分布；
- 行为审计报表：详细记录所有用户的操作行为明细，包括登录、传输、权限变更等，全面呈现操作轨迹；
- 异常事件报表：汇总违规尝试、传输失败、异常登录等事件，明确异常类型与处置情况，便于风险复盘。

所有报表支持导出为 PDF、Excel 等常用格式，无需额外编辑，可直接用于内部安全审查或向监管部门提交，大幅提升合规审计效率。

五、核心总结

从“谁传了”的主体追溯，到“传了什么”的内容管控；从“能不能传”的流程保障，到“让不让传”的风险阻断，严翼共享全局审计平台实现了文件传输“可控、可查、可追溯”的全流程管理，为政府、金融、军工等高安全需求机构，提供合规、高效、安全的审计解决方案，守护数据传输全链路安全。