

金融行业数据安全解决方案

全面保障金融数据全生命周期安全

方案优势

- 构建从远程接入、研发、办公、运维到文件交换，全流程安全管控的立体数据防护体系，严防数据泄密
- 部署实施不改变现有架构，不造成业务中断；管理员图形化操作，运维简化；用户端影响小，不改变原有用户习惯
- 针对数据全生命周期提供完善日志记录，可审计、可追溯，满足国家及行业监管要求

大数据、人工智能、云计算等新技术在金融业的深入应用，推动金融数据和业务上云，给企业机构业务开展和用户交易行为带来极大便利。同时，也催生数据泄露、被滥用和篡改等恶性安全事件的频发，不仅对金融机构、企业和用户造成极大经济损失，甚至于影响到国家安全、社会秩序、公众利益和金融市场稳定。如何强化数据安全保护能力，保障数据合规使用、安全流动成为金融行业当前亟需解决的问题。

需求与挑战

- 政策监管提出审计等合规需求：为保护用户与金融机构敏感数据信息的安全，国家层面及行业监管机构出台了多个相关政策法规、指引与标准规范，对数据存储、使用等全生命周期的安全提出严格要求，如要求运行系统至少保留6个月的审计日志，以便进行日常审计和事后查证工作。
- 数据集中管理需求：金融新增大量分支机构、营业厅、外置终端和外包团队等让网络架构变得庞大、分散，管理难度增加，敏感数据需要更有效的统一、有序、集中的管理手段、机制。员工、合作方、外包商等多种身份人员频繁访问内网，用户终端易留存大量的业务资料、客户数据、交易数据等核心数据资料，安全性无法保证，数据泄密风险大。因此，金融机构亟需建立整体的数据安全保障体系。
- 多网数据安全合规交换需求：金融行业业务多元复杂，对网络隔离要求高，且面对多头监管，在数据流转层面，既要满足行内的数据流转需求，还要考虑到和同行间的业务合作，并可接受审计。如何确保内网数据流转安全、外发共享数据安全和合理的授权使用已成越来越多金融机构所关注的重点。
- 部署运维简单，支撑业务稳定运行：金融行业业务范围广，覆盖用户量庞大。企业和机构IT系统繁多且复杂，对稳定性要求非常高，一旦出现故障，导致业务延迟高甚至中断，带来用户负面影响大。

服务客户



关注志翔

北京志翔科技股份有限公司

www.zshield.net

电话：400-819-8880

邮箱：contact@zshield.net

地址：北京市海淀区学院路35号世宁大厦1101

邮编：100191

解决方案

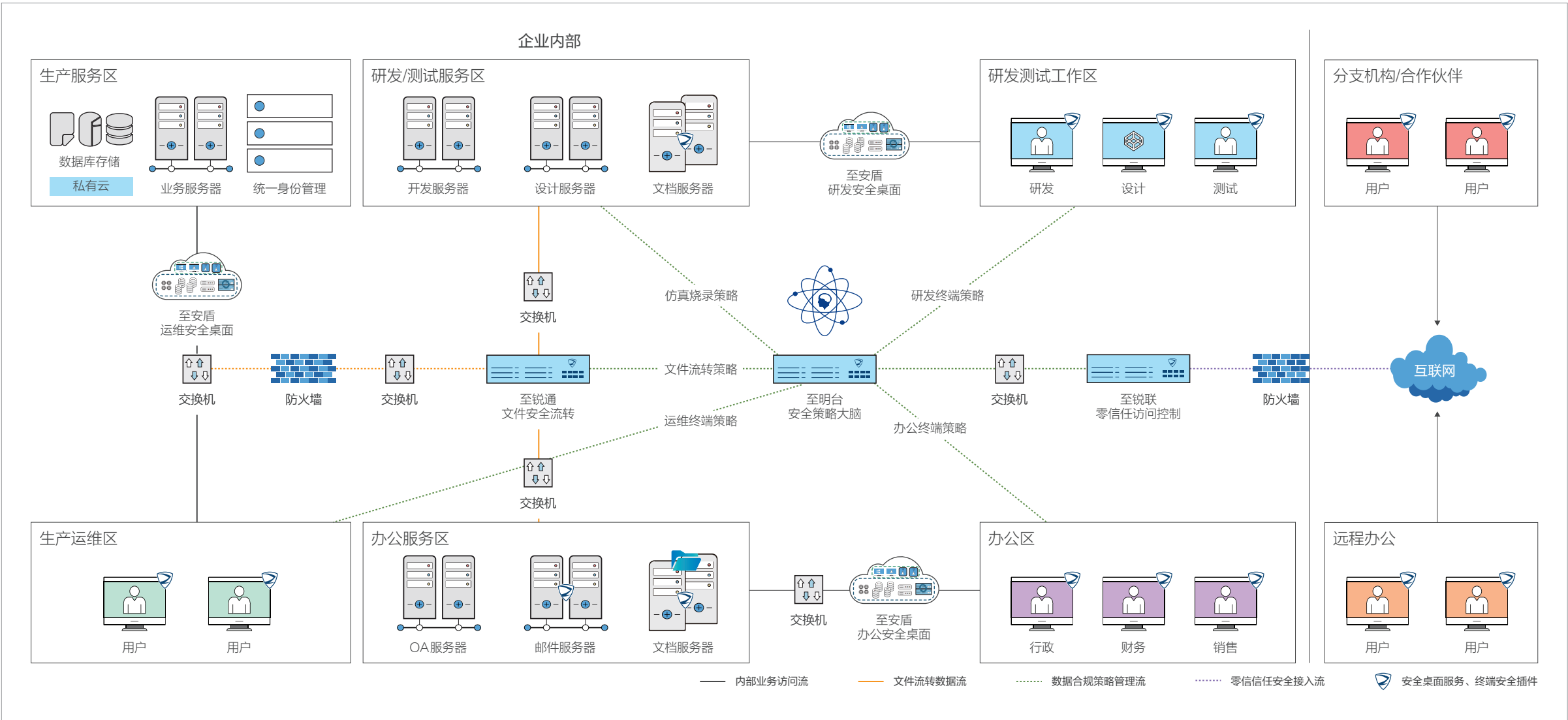
志翔科技金融行业数据安全解决方案采用模块化设计，以数据的安全和流转为核心，平衡考量核心数据安全和业务运行效率。为金融机构远程研发、远程运维及办公、外包等多种应用场景构建安全可靠、稳定高效，且简单易用数据安全保护体系。

至锐联：零信任访问控制系统，以授权终端为边界，或针对特定资源的虚拟网络安全边界，提供基于用户身份的最小化访问权限。

至明台：全面保障终端数据安全，提供对终端文件的识别、内容扫描、权限管控、加密及追溯等。

至锐通：提供多个网络隔离区域间的跨区数据安全交换，集隔离、交换、网盘、审批、审计于一体。

至安盾：安全云桌面作为内网办公、业务、研发、运维等操作的统一入口，确保数据不落地。



应用场景

-  **跨网业务数据提取：**金融行业企业机构内部通常将内网划分为多个网络，如生产网、办公网、开发测试网等，各网相互隔离，日常业务开展过程中常有跨网数据提取使用需求。方案通过部署至锐通，可在网络隔离的前提下，实现数据交换流程的“可管、可控、可审”，确保跨网业务数据提取的安全性和合规性。
-  **生产数据脱敏流转至测试环境：**金融机构企业通常将生产网与测试网隔离，生产网的重要数据需要流转到测试网进行相关业务程序测试。方案会按需将生产数据进行脱敏，并采用至锐通审批流转到测试网，流转过程日志全记录，满足可审计、可追溯的安全合规要求。
-  **分支行数据下发：**在银行业务中，分支行为了更好的提升业绩，需要总行的业务数据或者综合分析数据做支撑，而这些数据都是核心且高机密的数据。方案采用至锐通提取业务数据，并审批流转下发到分支行指定的专用数据接收终端。数据流转全程数据不落地，审批审计一体化，同时满足数据提取和下发的安全性和传输的高效率。

-  **研发、办公数据安全：**方案通过至安盾为研发人员、办公人员构建统一云桌面，运维人员统一对资源和权限进行调配管理，研发人员、办公人员通过桌面访问后端资源，数据不落本地。
-  **安全远程接入：**方案通过至锐联为用户提供安全的访问通道，大幅收敛互联网暴露面，精细化管控用户访问权限，持续监测动态授权。为金融企业机构解决远程办公、远程研发、远程运维安全接入需求。
-  **终端敏感数据防泄漏：**方案基于至明台产品，可对行内终端进行全面数据资产梳理，满足“谁，何时，用哪台终端，经哪个程序，对哪个文件有哪些操作，造成了什么结果”的分析需要，同时可根据梳理结果进行相应的管控策略下发，从而构建终端数据的全面安全防护体系。

除此，方案还可以应用于营业厅分支网点、金融呼叫中心、内外网混合办公、内网协同办公、研发测试中心、外包管理等多个金融行业机构和企业常用场景，全面保障金融数据安全。