

场景式防泄密解决方案

◆ 解决方案

在《网络安全法》《数据安全法》《个人信息保护法》等法律法规施行，以及行业监管要求的背景下，企业面临诸多场景下的数据安全挑战。从保护企业内部商业机密，到满足个人隐私保护要求，再到维护企业声誉，场景式防泄密对于企业数据安全能力的建设与提升至关重要且迫在眉睫。由于每种技术都存在局限性，绝对安全难以实现，所以我们应抓住主要矛盾，兼顾安全与业务发展的需求，确保安全与效率的统一。具体而言，需对数据进行分类分层，并依据使用场景设计相应的保护方案。

◆ 解决方案

联软科技深入洞察企业多样化需求，紧密贴合角色、场景、位置、环境、终端以及数据类型等不同场景化要求，匠心独运地基于各类场景精心设计出全方位的控制、便捷、震慑手段。其创新性地突破单一技术局限，巧妙融合多种先进技术，有效减少系统维护工作量，助力企业业务领导轻松达成对重要数据的管控目标，精准界定管控范围，并确保管控手段的严格性，全方位守护企业数据资产安全。针对行业中的典型数据防泄密场景，特提供以下方案(不限于)：

金融类用户信息保护

基于数据分类分级规则精准识别敏感数据，依规将敏感文件存于文件保险柜，实现文件安全隔离和加密存储；

大型制造业数据防泄密

依据数据分类分级规则精准识别敏感数据，并实现联合敏感标签、智能加密以及外发通道管控等功能，为制造业用户提供便捷的防泄密策略制定方式；

软件开发场景防泄密

根据企业软件开发人员日常办公场景，利用透明加密技术、数据外发通道控制技术，严控内部代码库文件下载权限，并搭建合规的跨网数据交换安全通道，全方位守护企业核心数据资产；

应用系统数字水印

通过建设企业水印中台或将WEB业务集中发布至应用网关，为企业的应用系统提供统一规范的数字水印效果；

跨域取数与文档安全发布

专为用户解决多网隔离、重要文件分散存储、跨网文件交换频繁等复杂的文档安全需求场景。

◆ 业务价值与方案优势

精准适配不同场景，能够为企业提供高度定制化的数据防泄密解决方案，在不同办公场景（如办公室、外出办公、居家办公等）、不同网络环境（企业内网、外网、移动网络等）下，都能有相应的管控措施，确保数据安全策略的有效性和精准性。



全方位覆盖

基于各类场景精心设计出全方位的控制、便捷、震慑手段，从多个角度对企业数据进行保护。不仅关注数据的存储和传输安全，还考虑到员工使用数据的行为规范，通过控制手段防止数据泄露，便捷手段提高工作效率，震慑手段约束员工行为，形成一个完整的数据安全防护体系；



技术创新与融合

通过融合多种技术，如加密、访问控制、行为分析、水印技术等，可以实现优势互补，提高数据防泄密的效果和可靠性；



提升系统维护效率

有效减少系统维护工作量，降低企业在数据防泄密系统运维方面的人力、物力和财力投入。多种技术的融合可以使系统更加稳定、高效，减少因技术兼容性问题导致的故障和维护需求。同时，统一的技术架构和管理平台也方便企业对数据防泄密系统进行集中管理和维护，提高运维效率；



数据防泄密更专业

针对行业中的典型数据防泄密场景，如员工离职带走企业核心数据、合作伙伴违规使用企业数据、外部黑客攻击等，提供有效的解决方案。通过对这些典型场景的深入研究和分析，制定相应的数据防泄密策略和技术措施，能够有效降低数据泄露的风险，保护企业的核心竞争力；



提升企业整体数据安全水平

帮助企业建立起一套完善的数据安全防护体系，从数据的产生、存储、传输、使用到销毁，进行全面的保护和管理。这不仅能够有效防止数据泄露事件的发生，还能够提高企业对数据安全的重视程度和管理能力，提升企业整体的数据安全水平，为企业的数字化转型和发展提供有力保障。