安全挑战



随着信息技术快速发展，大量的业务数据不断地迁移到网络环境中，企业日益依赖于信息技术来支撑业务的运行。业务数据成为组织的重要资产，不仅对业务具有价值，同时对组织的决策、商业智能，甚至战略规划都具重要意义。数据已成为组织重要的核心竞争力，数据型组织是必然的发展方向。

传统网络安全保护，难以匹配信息化的数据转型，数据外泄事件屡有发生，棱镜门、CSDN密码泄漏、如家开房信息泄漏、Sony个人信息泄漏等。这些事件，对组织造成重大的甚至无法弥补的经济损失与声誉损失。

很多企业对于各种业务敏感信息的创建，流转，存储等数据生命周期关键点缺乏安全管理和技术管控，没有有效的技术手段来监控敏感信息的流转过程。无法准确定义和查找相关的泄漏安全事件源头，不能分析、预警客户数据有意和无意的流失现象，更无法拦截资料的泄漏。

数据安全不仅涉及企业生产运营，还涉及个人隐私、国家利益等。国家、行业有关数据安全的法律、法规、制度也越来越多，数据防泄漏是要求的重点。

解决方案

数据的全生命周期包括数据创建、存储、使用、流转、归档、销毁等主要阶段。整体数据安全体系框架如下图所示：

**数据安全管理体系**

在企业数据安全防护目标的指引下，对客户信息数据进行梳理，建立敏感数据视图，进行分类分级保护；识别客户敏感数据全生命周期面临的泄露风险，进行闭环式风险管控；定义敏感数据使用和管理的相关角色、权限，并与用户组织结构、人员、岗位、职责进行关联；制定或完善数据安全管理体系文件，包括策略、制度、标准、流程等一系列管理文档；推动数据安全管理体系落地，并进行持续监督和改进。

**数据保护**

运用动态文档加密技术、身份认证技术、硬件绑定技术等多种技术对指定类型的文件进行实时、强制、透明的加解密。并对文档进行细分化的权限设置，确保加密信息在特定授权范围内进行指定操作。对文件的输出（包括外发、共享、打印、拷贝）的进行加密、脱敏、水印等方式管控。

针对存放在核心业务数据库系统中的客户敏感信息数据进行保护，包括数据库权限管理、数据库访问控制、数据库操作审计、生产数据脱敏（含动态数据脱敏和静态数据脱敏）等。

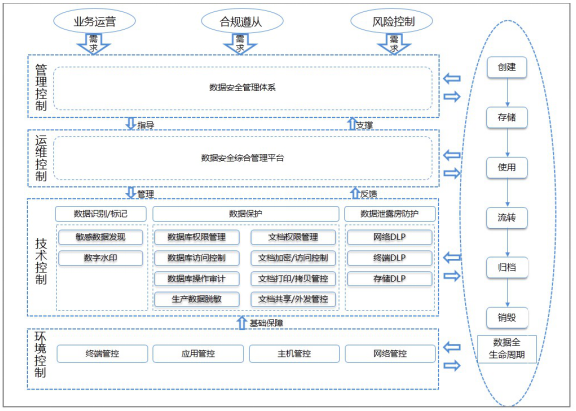
**数据泄露防护**

重点实现对产生、使用、传输中的数据进行泄露防护，包括：

网络数据泄露防护：即在网络出口或安全域边界识别、控制传输中的敏感数据，控制或监视通过邮件、WEB、FTP等网络协议传送敏感数据。

终端数据泄露防护：即发现、识别、监控计算机终端的敏感数据；对敏感数据的违规使用、发送等进行策略控制；对敏感数据的终端使用行为进行监控。

存储敏感数据发现：即对存储在服务器、数据库、存储库中的结构化数据和非结构化数据进行扫描，根据策略发现、记录敏感数据，并对违规存储事件报警。



方案价值



本方案加强对核心数据资产的安全保护，保障核心数据资产合理、高效共享的同时，防止核心数据随意扩散及泄密。

通过方案最终清晰了解敏感数据状态，识别数据风险状态，构建体系化的数据安全保护机制，降低法律法规合规风险，构建企业数据安全文化。