医药制造行业数据资产防泄密解决方案

1. 现状描述

医药制造业是根据医疗市场需要通过加工制造过程转化为可供人们使用的医疗工业品与消费品的行业，医药制造业包括医药产品的研发、生产和销售环节。近年来医药制造业主营业务收入保持持续增长，行业成长能力较强，也不断吸引国内外企业加入，市场竞争日趋激烈，这也促使了持续的产品研发和技术创新成为企业的发展核心，因此行业对科技发展的依存度较高，具有高投入、高产出、高风险和高技术密集型等特点。与此同时目前大部分药企经营过程中也面临如下风险：

新产品开发风险：新产品研发投资大、周期长，药品的研发失败后会有丧失市场的风险，将影响到公司前期投入的回收和效益的实现。

行业监管风险：国内对新药品的研发、注册与生产过程都有严格的合规控制，所有制药企业必须经过 GMP 认证，实行全面质量保证，确保药品质量。

市场竞争的风险：随着近年医药需求的不断增加吸引更多国内外企业加入，市场竞争也变得日益激烈，知识产权、经营策略、关键数据等作为核心资产要加强保护。

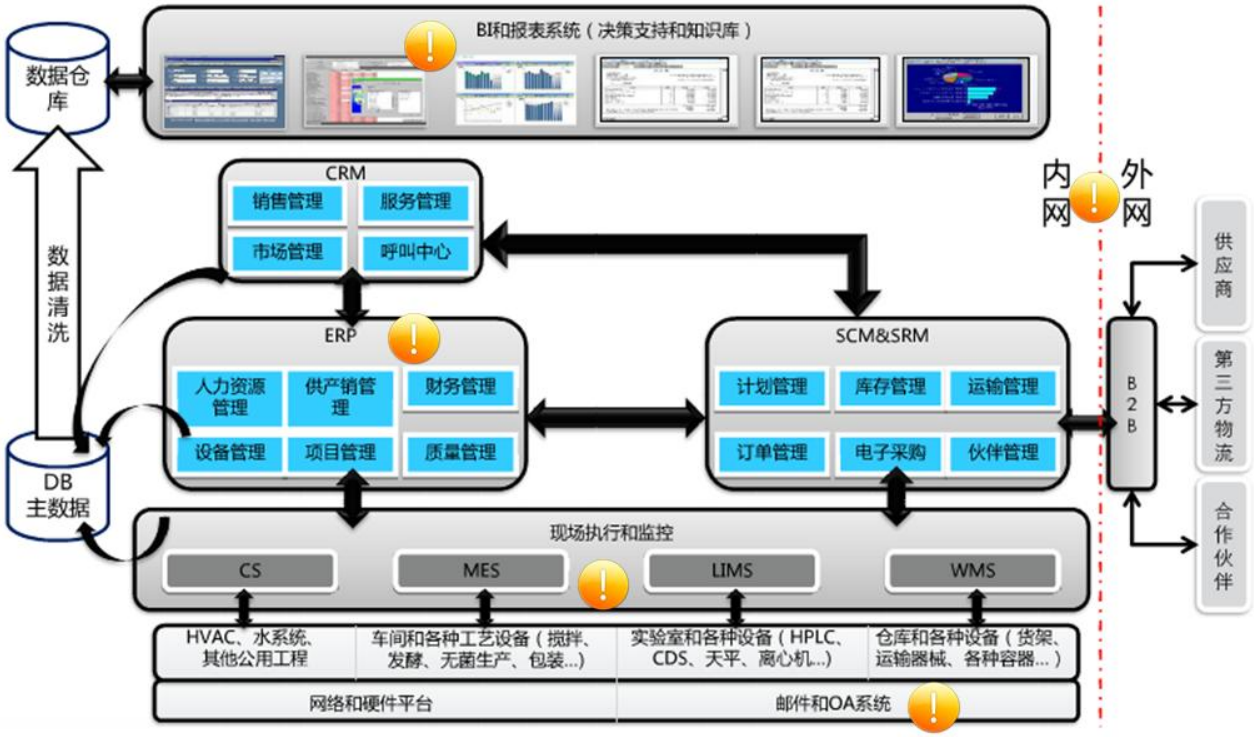
高速成长的管理风险：同时随着公司业务经营规模的扩大，如何建立更加有效内部风险控制体系成为公司管理中面临的挑战，其中信息安全风险应受到重视。

2. 面临问题

目前国内制药企业信息化建设规模、层次和水平都存在很大差距，其中尤其对于信息安全的重视程度和投入总体较低，防护能力和防护水平还有待提升。

随着办公信息化在药企中不断的成熟和深入应用，在药品研发、生产制造和销售过程中，企业对管理和经营都依赖于信息化平台，各种内部系统如 OA、ERP、LIMS(实验室信息管理系统)、生产管理系统、质量管理系统、CRM 系统等，这些系统之间集中存放和处理着大量的敏感业务数据，如中药保密配方、知识产权、临床分析报告、财务数据、销售数据、质检报告、管理经营策略等，作为药企核心信息资产，这些数据资产若被有意或无意泄密将对企业的持续运营造成经济、声誉损失甚至面临更为严

格的监管处罚。



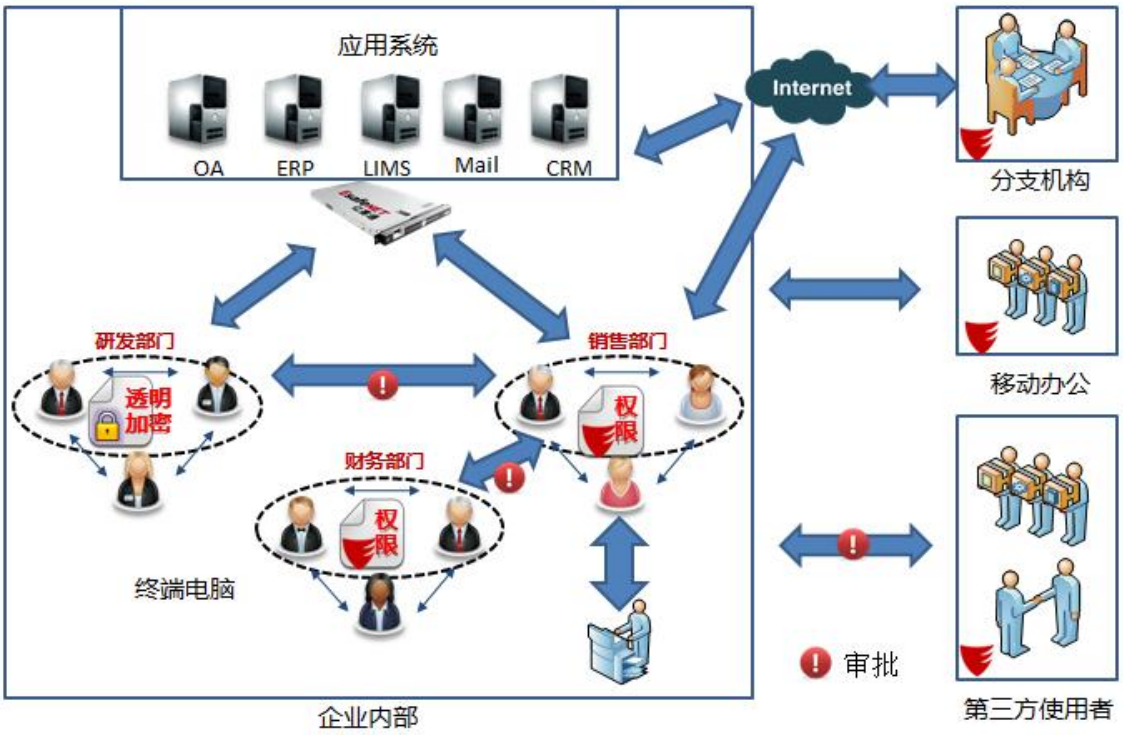
图：制药业 IT 基础架构图（图片源自 Loadstone）

面对日趋激烈的竞争环境，近年来如何保护这些数据资产在药企经营中的安全保护，已经成为不少制药企业的重点关注点。药企要想在经营过程中可持续性发展，就必须面对和解决以下问题：

- 新药品在研发过程中中药研发数据不同应用场景下如何保护？
- 国家级中药保密配方如何通过技术手段加密隔离访问？
- 如何确保药企与合作伙伴共同开发的相关药品数据安全？
- 员工企业终端和移动终端办公敏感数据如何防止泄密和失密？
- 因业务需要外发到第三方人员或组织的敏感数据如何受控？
- 如何防止企业内部人员有意或无意泄漏重要敏感数据？
- 内部 OA、ERP、LIMS 等系统内关键敏感数据资产如何集中防泄密？
- 集团化企业如何贯彻关键财务及审计数据的统一安全策略？
- 公司的信息安全保密制度如何才能有效落地？
- 敏感数据保护如何从被动防御到主动管理？

3. 解决方案

为确保药品从研发、制造到销售环节中敏感数据的安全，确保其在受控范围内安全的流转和使用，亿赛通通过多年的数据防泄密实践经验和产品，深入结合药企业务特点，制定了医药制造业的数据防泄密解决方案，协助药企保护关键资产安全，方案保护效果下：



图：制药业防泄密解决方案示意图

1） 终端数据保护：

- 通过亿赛通 DLP 平台的透明加密产品，建立数据安全边界，确保医药研发数据在研发部门内安全使用，防止内部人员有意或无意造成的泄密；
- 对非研发部门如财务、销售、生产部门采用 DLP 文档权限加密产品实现数据保护，可以控制敏感数据的用户访问范围、文档使用操作限制，对敏感信息的内部使用实现高细粒度控制；
- 对分支机构和移动便携办公人员终端数据泄密形成有效保护；

2） 应用系统数据保护

- 通过亿赛通第三代文档安全加密网关，实现对 OA、ERP、LIMS 等系统中敏感数据的集成保护，确保从这些应用系统下载的数据在终端加密受控流转使用；

- 终端加密数据数据上传到应用系统后可以自动解密，不影响使用习惯；
- 对于 ERP、LIMS、MES 系统后台采用明文数据存储，因此系统间的后台数据传递不受影响。

3） 数据外发安全保护

- 可以通过亿赛通文档外发管理功能实现市场、销售部门对外发送的敏感数据安全保护，防止合作机构或第三方人员有意无意扩散使用。

4） 业务效率保障

- 不改变或不过多改变现有业务流程效率及用户使用习惯；
- 通过加密网关实现终端与应用系统数据无缝集成；
- 系统内置单级和多级审批流程，让流转操作更快速容易；
- 通过邮件白名单可实现受信用户或伙伴数据自动脱密，降低沟通影响。

5） 敏感数据操作行为追溯：

- 对所有受DLP 系统保护的数据使用操作，提供审计机制，一旦泄密行为发生，可通过审计信息明确泄密责任，追究泄密行为。
- 对于DLP 系统角色实现三权分立和操作审计，同时针对解密管理员的解密操作执行过程跟踪审计。

4. 优势收益

通过本方案对药企敏感数据及业务系统现有的数据泄漏风险进行管控，加强药企数据产生源头、使用过程、对外发布整体的防护，为药企核心数据的安全提供保障，方案具备如下优势：

- 方案围绕数据全生命周期安全，纵深防御强化敏感数据安全防护
- 基于敏感数据流向分析，方案实现数据流到哪里，保护就执行到哪里
- 为药企关键应用系统的数据安全提供平台化保障
- 与业务应用系统集成实现敏感数据保护，不需要二次开发
- 数据保护实现从业务系统、终端电脑到移动终端的三重保护
- 方案灵活性和可扩展性强

通过亿赛通制药业 DLP 数据防泄密方案的部署实施，您将获得以下收益：

- 保护新药品研发周期内的数据安全，防止因数据泄密造成产品研发投入和市场竞争机会的流失
- 实现药品 GMP 认证中生产管理文件和质量管理文件的保护
- 满足来自上层监管要求保密中药配方保护的合规要求
- 落实药企 IT 安全风险管理，提升企业风险内部控制水平
- 深化药企员工的信息安全保密认知和意识
- 通过 DLP 系统引入降低总体合规管理成本