2023年南湖HIT论坛

数据驱动医院运营管理

2023年11月11日 嘉兴市

扫码观看视频直播

主办：HIT专家网

承办：北京和思凯文化传媒有限公司

支持企业：

美创 MEICHUANG | 18周年

数字化转型浪潮下的医疗数据安全风险与实践

数字化转型安全保障建设分享

目录

CONTENTS

01 数字化转型背景与机遇

02 数据安全风险与实践

数字化转型带来了哪些改变

数字化转型势在必行

数字化可使制造业企业成本降低17.6%、营收增加22.6%；使物流服务业成本降低34.2%、营收增加33.6%；使零售业成本降低7.8%、营收增加33.3%。

业务变化

业务互联网化，数量越来越多

复杂度越来越高

IT基础设施变化

业务与数据成倍递增

大幅度加大了基础设施的消耗

数据变化

数据海量化、资产化，数据量成几何倍数上涨

大数据又催生了新的业务

随着业务复杂度的增加，企业数据量成倍的递增，而大数据技术又催生了新的业务。数据海量化、资产化后，诞生了一系列的安全问题，用户内网管控、数据防泄密等需求越来越强烈。

数据安全法规提出了新的要求

相关法律有**52**部，行政法规**42**部，司法解释**50**部，部门规章**870**部，团体规定**43**部，行业规定**171**部

国家安全法

第二十五条 国家建设网络与信息安全保障体系……实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控。

2015年7月1日起施行。

等保2.0标准

标志着国家网络安全等级保护工作步入新时代。作为网络安全防御体系框架性指导标准与规划建设指南，指导用户开展信息系统安全等级保护的建设整改、等级测评等工作。

2019年12月1日起施行。

“十四五规划”

明确提出要**加快数字化发展，建设数字中国。**数据安全和个人信息保护是推进数字产业化、产业数字化以及发展数字经济的重要支撑。

关键信息基础设施安全保护条例

在《中华人民共和国网络安全法》确立的制度框架下，细化相关制度措施。内容更详尽、方法更具操行性、安全保护标准更严格。**2021年9月1日起施行。**

网络数据安全管理条例

为落实相关法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，由国家互联网信息办公室于**2021年11月14日发布征求意见稿**

2015.7 — 2017.11 — 2019.5 — 2020.4 — 2021.3 — 2021.6 — 2021.8 — 2021.8 — 2021.11 — 2022.9

网络安全法

标志着我国网络空间法治化进程的实质性展开，将等级保护上升为法律高度。**2017年6月1日起施行。**

“数字”生产要素

《关于构建更加完善的要素市场化配置体制机制的意见》是中央第一份关于要素市场化配置文件，**数据作为一种新型生产要素写入文件。**强调加快培育数据要素市场。

数据安全法

标志着数据安全上升到国家安全层面，自此数据安全建设有法可依。包括数据安全处理、建立健全各项制度、促进数据安全和发展、满足电子政务数据合理需求、保障国家安全。**2021年9月1日起施行。**

个人信息保护法

明确个人信息采集、使用的要求，完善投诉、举报工作机制……这部专门法律充分回应了社会关切，为破解个人信息保护中的热点难点问题提供了强有力的法律保障。**2021年11月1日起施行。**

数据出境安全评估办法

规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，切实以安全保发展、以发展促安全。

2022年9月1日起施行。

热点事件分析1-国内多家医院数据被窃，黑客牟利200余万

吴某某踩点接送

姜某某窃取

刘某某贩卖

安全事件回顾

- 2020年至2021年，刘某、姜某某、吴某某在多家国内医院内，多次通过技术手段秘密接入医院内网数据库，获取大量药品编码、数量、金额、单位等药品数据后出售，违法所得人民币200余万元。
- 姜某某于2021年2月2日在医院窃取数据时被当场抓获，刘某于2021年2月2日被查获，吴某某于2021年2月3日被查获。
- 经调查，三人共谋分工明确，姜某某窃取数据、刘某销售数据，吴某某负责开车接送姜某某到医院内窃取数据，此案三人分别获利刘某114.416万元，姜某某51.496万元，吴某某56万元。
- 经查，刘某、姜某某、吴某某采用黑客技术手段，非法获取多家医疗机构数据，系情节特别严重，其行为均已构成非法获取计算机信息系统数据罪，依法应予惩处。最终依法进行追缴和没收非法所得，并处四年至五年六个月有期徒刑，及四万到六万罚款。

① 如何绕过强大的网络安全层防御系统

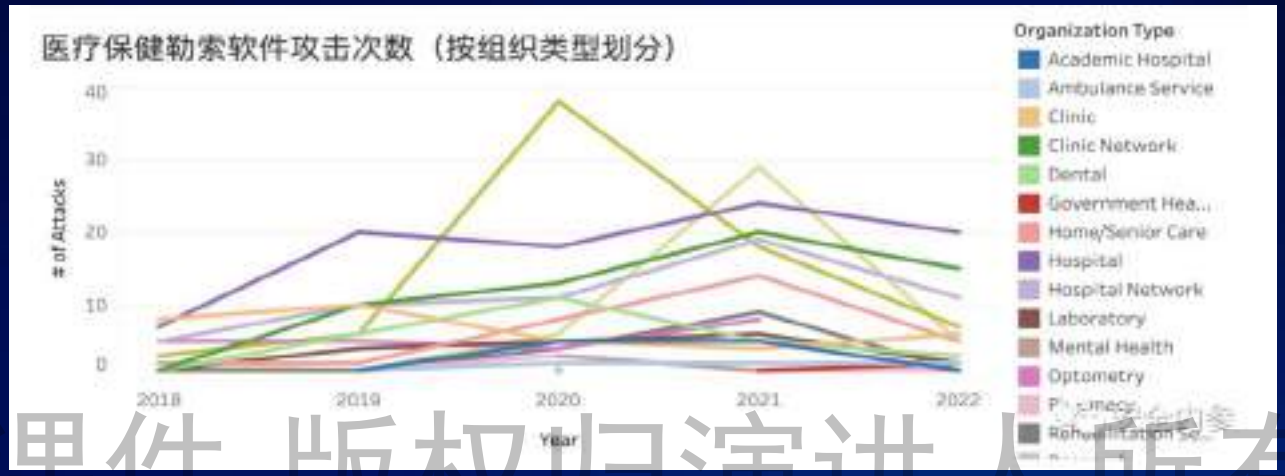
② 传统的防御堡垒机为何会频频失效

③ 仅仅依靠流量审计产品，进行时候审计，能够挽回损失吗

如果黑客从内部发起攻击，现有的网络层安全设备将会完全失效。而仅仅依靠堡垒机等传统内控产品，远远不足以进行降低数据泄漏风险。

而审计类产品，只能作为追责溯源的手段，一旦数据发生泄漏，数据将永久丢失，这意味着追责溯源永远也无法挽回已丢失的数据。

热点事件分析2-全球医疗机构因勒索软件攻击累计停机超7千天



安全事件回顾

- 自2018年以来，全球已发生**500**次公开确认的针对医疗保健组织的勒索软件攻击。凶猛的攻势导致近**13000**个独立设施瘫痪，并影响到近**4900**万份病患记录。据安全内参估计，黑客索取的赎金总额已超过**12**亿美元，受害医院已向黑客支付了近**4400**万美元赎金。
- 在多数情况下，勒索病毒攻击都会导致系统在数小时、数天、数周甚至数月之内无法访问。在某些极端情况下，系统甚至无法恢复正常。所有上报勒索软件攻击的停机总时长——结果为，全球医疗保健组织因停机而承受的业务中断总计**7381**天，相当于20多年。

不能单从赎金来计算损失，还需承担如因业务中断、法律程序、事件响应和补救、恶意软件发现和删除等造成的损失成本。尤其是，若因攻击导致关键系统和患者数据无法访问，可能造成严重延误甚至危及病患生命安全。

截至2020年，中国医疗卫生机构达到102.3万个，其中基层医疗卫生机构数量为97.1万家，占医疗机构总数量的94.9%。而大部分基层医疗机构数字安全意识相对薄弱、系统账号安全等级低、各类信息系统多而庞杂，容易遭到黑客的暴力破解、撞库、钓鱼邮件、木马病毒、**SQL**注入等攻击。

热点事件分析3-监管单位数据安全检查

公安机关持续进行净网行动

01

发现安全事件包括**侵犯公民个人信息案、非法获取计算机信息系统数据案**等。涉案数据达上亿条。

网信办持续开展APP专项检查

02

针对App非**法获取、超范围收集、过度索权等**侵害个人信息的现象。并对存在问题的App进行点对点通报，责令违规App限期整改。

行业监管单位开展安全检查

03

行业监管单位，**如卫健委**，针对行业内部的**数据安全保护情况进行检查**，如涉疫数据存储安全检查等。

目录

CONTENTS

01 数字化转型背景与机遇

02 数据安全风险与实践

医疗数据的高度敏感带来了哪些主要风险

- 数据安全场景，医疗行业数据敏感级别较高，因此面临的数据安全场景多种多样
- 数据安全测评，数据安全建设贯穿到了医院等级评审中，通过考核的方式促进医疗行业数据安全建设

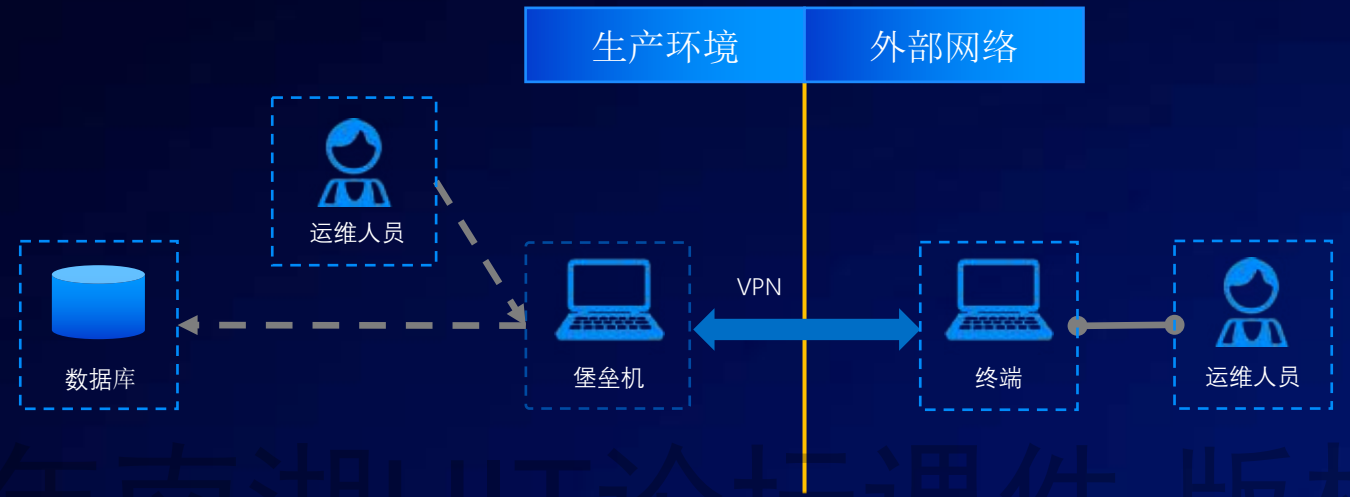
01. 医疗行业面临的数据安全风险

- 相较于传统行业，医疗行业数据敏感度较高，也面临了更多的安全威胁
- 部分地区的医疗行业缺乏必要的数据安全保护措施，进一步提高了风险

02. 医院等级评审带来的新的安全挑战

- 数据安全成为了医院等级评审中比不可少的一项检测要求
- 高等级医院需要花费更多的信息化投入到数据安全保护中

01.安全风险：医疗行业存量敏感数据管理风险



主要安全风险

- 大权限账号，越权及未经授权的访问风险
- 数据可能落地运维公司，甚至再次泄漏
- 远程运维从非安全区域直接访问敏感数据
- 远程工具漏洞让运维风险巨大

主要安全风险

- 一些老旧系统缺少运维，系统漏洞较多
- 新的系统带来了新的安全威胁
- 医疗行业数据价值高，黑客收益高
- 安全人员意识不足

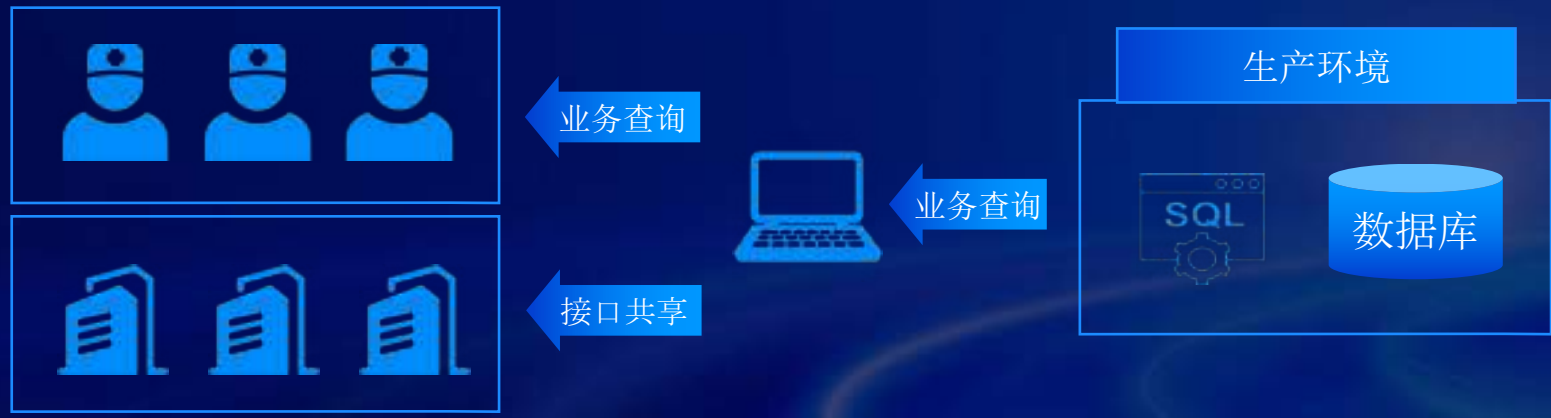
01.安全风险：医疗行业数据流动与共享风险

主要安全风险

- 业务变更和新业务上线频繁
- 用生产数据，甚至将数据被带回公司测试
- 脚本处理数据，测试效果差
- 数据流动到弱安全域、甚至外部网络，风险完全失控

主要安全风险

- 老系统原生安全薄弱
- 数据安全合规要求越来越高
- 隐私数据在操作界面突出展示
- 终端模式难管控，风险更大



01.安全风险：医疗数据其他数据安全风险场景

数据共享交换场景下的安全挑战

数据本质发生变化

集中存储　流转频繁　权责分离

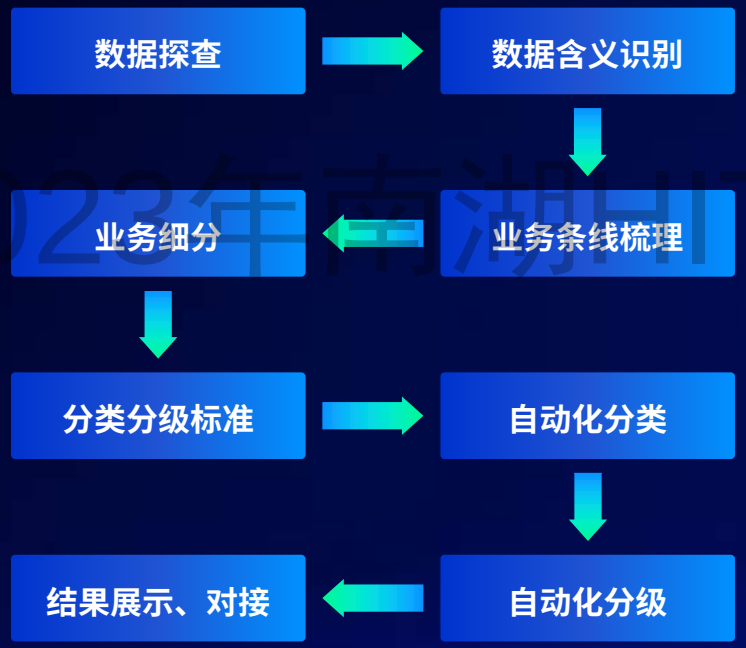
数据状况难看清	数据风险难监测	数据泄密难溯源
总量多少 分布在哪 是否涉敏 如何流转	权限风险 接口风险 行为风险 流转风险	什么数据泄密 什么人员泄密 什么时间泄密 什么方式泄密

共享建设不合规，出现问题要担责

序号	细分场景	主要挑战
1	回流数据场景	• 对数据通过API接口、批量等方式共享给使用方后的使用行为进行监管，需要对接口进行管控，防止数据违规导出、越权调用、数据泄露等风险行为。
2	数据多节点泄露	• 监测每个节点的数据流转情况，对数据泄露行为的预警或阻断，并在事件发生后进行有效溯源。
3	API接口二次封装	• 严格管控API接口共享，有效限制并监测二次封装、转发行为。
4	涉疫数据安全销毁	• 探索涉疫数据的及时、有效销毁机制，实现云上储存数据及过程数据的销毁。
5	数据全链路加密	• 针对流动数据中涉及到个人隐私的数据，如手机号、银行账号、身份证号等实现从采集到使用过程的全链路到加密。

01.解决方案：美创能提供的支持

支持一：数据探查分类分级(摸家底)
提升专业度



支持二：数据流动风险评估(识风险)
降低方案认可难度

支持三：数据安全运营体系(建体系)
解难题，提粘性

- 实现全链路数据安全监测
- 实现全周期数据安全管控

02.安全风险：医院等级评审带来的新安全挑战

国家卫健委在近年来陆续发布了一系列法律法规，法规针对医院重点建设的业务系统、如电子病例、医院智慧服务、分类分级等角度提出了数据安全建设要求。

“十四五”全民健康信息化规划	“十四五”国民健康规划	医疗卫生机构网络安全管理办法
中华人民共和国 基本医疗卫生与健康促进法	区域全民健康信息互联互通 标准化成熟度测评方案	医院信息互联互通 标准化成熟度测评方案
国家卫生健康委规划司卫生健康行业数据分类分级指南（征求意见稿）	电子病历系统应用水平分级评价 管理办法及评价标准	医院智慧服务分级评估标准体系

02.解决方案：医疗合规安全解决方案

医院信息互联互通标准化成熟度测评方案

DRCC、美创数据库透明加密、数据分类分级、数据脱敏、防水坝等

医疗行业网络安全管理办法

数据安全治理、分类分级、数据全生命周期安全加固等

电子病历系统应用水平分级评价标准

供数服务、数据汇聚、数据标准化、运营数据中心、决策分析、DRCC等

智慧服务分级评价标准

数据安全治理、数据分类分级、数据库防水坝等

其他主要风险

名称	要求	对象
密评存储加密建设	• 根据密评要求，存储层数据库数据需要通过国密算法进行国密改造，而一些传统数据库，如Oracle、Mysql、PG等，不支持国密算法加密。	• 医院 • 卫健委、疾控中心 • 各社区相关单位
涉疫数据安全保护	• 涉疫数据销毁，疫情结束后，疫情期间产生的涉疫数据分布在各业务系统、防疫人员办公电脑、终端上的数据需要进行摸排、销毁和销毁审计。	• 医院 • 卫健委、疾控中心 • 各社区相关单位
数据高铁建设	• 医疗行业数字化转型，需要实现医院内部不同系统之间的数据汇聚，或者医院到卫健委等多种场景下的数据汇聚，同时又要保障数据安全	• 医院 • 卫健委、疾控中心 • 各社区相关单位
数据出境安全	• 拥有跨境业务的医院，在开展业务过程中，涉及处理经营地地方敏感数据的，需要符合地方法规，在业务开展过程中，通过评估，发现安全问题，进行整改。	• 拥有跨境业务 • 医疗机构、科研机构等
业务系统容灾建设	• 业务系统在建设过程中，需要符合业务连续性要求。通过建设同城容灾和异地备份满足灾难恢复需求，保障以及符合等级保护级别需求	• 医院 • 卫健委、疾控中心 • 各社区相关单位

美创科技 懂数据、懂安全 的数据安全企业

理念先进

业界首个提出数据资产，零信任2.0理念、“韧性”数据安全防护体系，支撑产品不断前进

经验磨砺

作为数据安全领域专精型厂商，秉承18年数据领域安全经验，业界领先，经验磨砺品质

自主全面

自主研发数据安全、运行安全、数字化转型三大产线，提供最全面的数据安全整体能力

赛道领先

细分赛道第一厂家入选网安产业50强，是唯一入选CNCERT省级支撑单位的数据安全企业

用户广泛

服务全国12000+头部用户，覆盖政府、金融、运营商、医疗、教育、企业、物流交通等行业

引领发展

数十份产业报告的联合发布者，数十项国家行业标准牵头及参与者，引领产业发展

美创是一家从数据走向安全的公司

使命

让数据更安全更有价值

愿景

数据安全的领导者和引路人，
数字化转型的推动者

战略

聚焦数据安全，释放数据价值

价值观

创新、勇气、责任、成长

充足的产品和服务


政务


民生保障

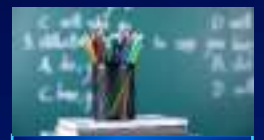

医疗健康


金融


物流交通


能源


通信


教育


企业

咨询

- 权限梳理
- 现状调研
- 环境评估
- 合规评估
- 能力评估
- 风险评估
- 跨境评估
- 分类分级
- 权限设计
- 策略设计
- 体系设计
- 制度设计
- 制度咨询
- 攻防演练
- 安全检查
- 安全培训

云端一体

洞察深微

精准即时

智能高效

管理域

- 数据安全运营平台
- 运行安全管理平台
- 流动安全管控平台
- 数据资产管理平台
- 数据安全管理平台
- 灾备集中管控平台
- 数据安全态势感知平台
- 数据支撑平台
- 暗数据发现及分类分级

安全管理 | 资产管理

访问域安全

身份、资产边界、资产活动

- 数据库防水坝
- 动态脱敏
- 数据库防火墙
- 防统方
- 数据库审计

流动域安全

界内、跨界、境内、边境流动

- 静态数据脱敏
- 水印溯源
- 诺亚星盾
- API监测与访问控制系统

存储域安全

封闭边界，减少暴露面

- 数据库透明加密
- 诺亚防勒索
- 全业务容灾
- 灾备一体机

公共基座

人、账号、终端、应用

- 统一身份管理

敏捷弹性

智能联动

全域覆盖

虚实一体

运营

- 设备巡检
- 补丁更新
- 策略调优
- 安全加固
- 远程专家
- 运维监测
- 智能工具
- 智能预测
- 资产治理
- 身份治理
- 风险治理
- 安全防护
- 应急演练
- 应急响应
- 事件溯源
- 培训宣贯

韧性理念

- 多重治理
- 行为建模
- 资产分层
- 全域身份
- 预测性
- 防御性
- 恢复性
- 适应性
- 可见性

零信任2.0

- 以人为中心的身份管理
- 动态访问控制系统
- 基于身份的行为模式识别
- 基于资产的边界定义
- 重构身份和资产边界
- 以加密重构新边界
- 流动中的边界和追踪

风险评估

- 脆弱性风险
- 合规风险
- 行为风险
- 存储风险
- 流动风险
- 访问风险

入侵生命周期1.0

- 探索发现
- 入侵和感染
- 探索感知
- 传播
- 持久化
- 攻击和利用
- 恢复

感谢聆听！