

vinchin

医疗影像云新规灾备“硬指标”

国家医疗保障局《“医保影像云”基础规范》



目 录

PART 01 医保影像云规范解码

PART 02 合规灾备方案

PART 03 案例分享

PART 01

医保影像云规范解码





首页> 政府信息公开> 法定主动公开内容> 通知公告

视力保护色: ☐ ☐ ☐ ☐ ☐ ☐

名称:	国家医疗保障局发布《“医保影像云”基础规范》		
索引号:	2026-04-00061	发文字号:	-
发布日期:	2026-06-22	发布机构:	

国家医疗保障局发布《“医保影像云”基础规范》

日期: 2026-06-22

访问次数: 10557

字号: [大 中 小]

为更好维护医保参保人权益,切实解除群众疾病医疗后顾之忧,加快推进医保影像云高质量建设,构建“患者本人可阅、医疗机构可调、医保部门可核”的影像检查数据服务平台,国家医保局组织开展了医保影像云系列规范研究,制定《“医保影像云”基础规范》,现予以公开发布。

附件: “医保影像云”基础规范

国家立法与行业标准双重驱动，构建全方位医疗数据合规监管体系

《网络安全法》《数据安全法》《个人信息保护法》
从国家层面明确了数据安全的法定责任、合规底线与处罚标准

标准升级 · 独立考核

GA/T 2380-2026新规，将数据安全提升为独立考核维度，指标更细、标准更严。数据安全不再是系统建设的附加项，而是具备“一票否决”效力的核心指标，倒逼医疗机构从被动合规转向主动建设。

行业规范 · 统一落地

国家医保局《医保影像云基础规范》，对全国影像数据的存储、共享、加密与权限管控提出统一技术要求，解决了跨区域、跨机构数据流通的标准不统一问题，同时为医疗云服务的安全合规提供了明确的实施指南。

监管趋势：从“事后补救”到“事前预防”，数据安全已成为医疗信息化建设的前提与底线，合规能力将直接决定医疗机构的数字化发展上限。

《医保影像云—业务应用规范》
一、适用范围
二、定义
三、总体建设要求
四、总体建设架构
五、适用场景
六、影像中心技术要求
七、前置机端技术要求
八、个人端技术要求
九、安全规范
十、影像中心、前置机端影像检查图像浏览工具要求
十一、个人端影像检查图像浏览工具要求

《医保影像云—基础设施技术规范》
一、适用范围
二、定义
三、物理环境要求
四、硬件设备要求
五、基础平台要求
六、云服务要求
七、网络要求
八、安全防护要求
九、容灾备份要求
十、存储介质处置要求

《医保影像云—业务人员、设备及图像基础要求》
一、适用范围
二、定义
三、业务人员要求
四、医学影像设备要求
五、影像检查图像基础要求



图 1 总体架构图



物理环境筑基

明确机房等级、选址标准及双路供电保障，夯实系统运行的物理底座。



硬件性能规范

规范服务器算力、存储IO及网络设备吞吐，匹配业务高并发需求。



专网建设要求

搭建医保影像云专用网络通道，保障数据传输的高速与低延时。



全域安全防护

覆盖数据中心、网络边界及终端的立体化防护，严防数据泄露。



容灾备份（核心）

明确RTO/RPO量化指标，建立“本地+异地”多副本灾备机制。



介质管理（核心）

实施数据分层存储，规范介质全生命周期管理与销毁流程。

三、物理环境要求

(一) 机房基础

1.建设等级

数据中心机房规划与建设应遵循GB 50174-2017《数据中心设计规范》相关规定。等级划分要求如下:

(1) A级标准: 适用于国家医保影像云;

(2) B级及以上标准: 适用于各省级医保影像云、三级定点医疗机构;

(3) C级及以上标准: 适用于三级以下定点医疗机构。

五、基础平台要求

(一) 服务器虚拟化

1.具备虚拟化集群管理、虚拟机在线迁移、克隆等核心功能;

2.具备宿主机故障时,虚拟机自动重启或迁移的高可用性(HA)功能;

3.宜具备分布式资源调度能力,实现计算资源的动态负载均衡;

4.宜支持网络虚拟化,实现灵活的网络策略定义和微分段。

(二) 存储虚拟化

1.采用分布式架构,实现单节点故障不影响数据存储的完整性和业务连续性;

2.支持统一提供块、文件、对象等多种存储服务类型。

四、硬件设备要求

(一) 服务器设备

在满足功能、性能、安全、可靠性及兼容性要求的前提下,服务器宜优先选用主流国产芯片及国产品牌。

1.各省医保影像云服务器应满足如下要求:

平台服务器配置需符合市场主流参数标准,具备高可用、高并发、低延迟、易扩展等特性,能够满足全国范围内医保影像数据7×24小时持续调用的业务需求,同时支持虚拟化平台、数据库、中间件等多种应用服务的统一部署。平台存储总可用容量需满足医保影像数据未来3—5年的增长需求,并保证日常运行水

3.专线带宽

各省医保影像云应依据日均异地就诊转入和转出人口数量中的较高值，参考下表进行专线带宽基线选型，具体可结合实际情况上调。

表 1 医保影像云专线带宽要求对照表

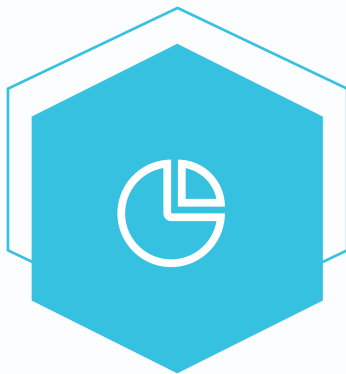
日均异地就诊转入/转出人数	最低网络带宽要求（Mbps）
≥100000	≥4200
≥80000	≥3300
≥50000	≥2100
≥30000	≥1200
≥10000	≥400
≥5000	≥200
≥2000	≥100

注：表中未列出数值，可参照已有数据按比例进行估算。



医保影像云数据中心

对网络防火墙、入侵防御系统、Web 应用防火墙、日志审计系统、数据库审计系统、运维审计系统、漏洞扫描设备、态势感知与综合安全管理平台、数据防泄漏系统和传输安全等十个方面做出详细说明



网络边界与通信安全

网络隔离：通过部署网络防火墙或安全隔离网闸，实现不同安全等级网络区域（如互联网接入区、应用服务区、数据核心区、运维管理区）之间的有效隔离和访问控制。

流量控制：宜部署流量控制设备，对网络流量进行分析和管控、告警，具备用户行为分析、应用带宽限制、应用带宽保障、链路监测、自动告警等功能。



终端安全

应采用至少两种组合鉴别技术，终端设备通过公共网络访问业务系统时，须采用基于国密算法进行加密保护，所有接入网络的终端应安装统一管理的防病毒软件，建立完善的密钥全生命周期管理体系，包括密钥生成、分发、存储、轮换和销毁。核心数据加密，宜采用经过国家密码管理部门认证的硬件加密机进行密钥安全保管。

九、安全规范

医保影像云建设须通过国家信息安全等级保护第三级测评，保障系统运行、存储、传输及个人信息安全。

《规范》确立医疗业务灾备硬性考核标准

01 业务恢复：RTO ≤ 4小时

要求核心业务系统在故障发生后4小时内恢复运行。这意味着必须摒弃传统的人工恢复模式，建立基于自动化技术的业务接管机制，确保医疗服务不中断。

02 数据保全：RPO ≤ 1小时

数据恢复点目标要求数据丢失量严格控制在1小时以内。传统定时快照备份难以达标，必须部署CDP实时数据保护技术，实现数据的持续捕获与零丢失保护。

03 实施保障：异地多副本机制

严格执行“3-2-1”备份原则，核心数据必须建立异地备份机制。同时需定期开展灾难恢复演练，不仅要确保数据能备份，更要验证数据能随时恢复可用。

合规与价值并重：建立高标准的容灾备份体系，不仅是满足《规范》的合规要求，更是医疗安全的底线保障。在突发硬件故障、网络攻击或自然灾害等极端情况下，完善的灾备能力能确保患者数据不丢失、诊疗业务不中断，为生命救治提供坚实的信息化支撑。

01 超长周期数据留存硬性指标

规范明确了医疗影像数据的底线存储时限：门（急）诊影像数据需**至少存储15年**，住院影像数据需**至少存储30年**。这不仅是满足医疗法规与追溯需求的基础，更对存储系统的容量规划、数据可靠性及长期归档能力提出了极高要求。

02 热-温-冷三级分层存储策略

为平衡性能与成本，需构建分级存储体系：

- 热存储**：采用全闪存/SSD，保障临床秒级调阅；
- 温存储**：使用大容量磁盘阵列，存储中频访问数据；
- 冷存储**：通过磁带库或蓝光库，低成本归档长期离线数据。系统需具备智能生命周期管理，自动完成数据的分级迁移。

6.存储分层策略

自影像检查完成时起，门（急）诊影像检查数据须存储15年，住院影像检查数据须存储30年，影像检查数据可采用分层存储策略：

（1）热存储：用于存储近期（如1年内）影像数据，应采用全闪存阵列或 SSD/SAS/SATA 混合阵列；

（2）温存储：用于存储中长期（如1至3年）影像数据，宜采用大容量NL-SAS/SATA磁盘阵列；

（3）冷存储：用于长期（3年以上）影像数据归档，宜采用磁带库、虚拟带库或蓝光光盘库等低成本、高持久性介质。

《医保影像云》规范 vs 等保2.0（三级）

01 核心灾备指标：更高的业务连续性门槛

等保2.0: $RPO \leq 2\text{小时}$ / $RTO \leq 12\text{小时}$ (参考性数值)

医保规范: $RPO \leq 1\text{小时}$ / $RTO \leq 4\text{小时}$

解读：灾备能力要求提升50%以上，精准匹配医疗业务“零容忍”的连续性需求。

02 数据存储期限：首次明确超长周期

等保2.0: 无针对医疗影像的统一强制存储年限规定

医保规范: 门诊影像 $\geq 15\text{年}$ / 住院影像 $\geq 30\text{年}$

解读：倒逼医院构建低成本、高可靠的海量数据分层存储与长期归档体系。

03 备份策略：从“存在”到“有效”的质变

等保2.0: 仅原则性要求建立异地备份机制，重形式

医保规范: 自动化备份 + 定期恢复演练 (常态化验证)

解读：强调备份的有效性，从被动合规转向主动保障，确保数据“可恢复、可使用”。

04 政策导向：安全护航数据互联互通

等保2.0: 通用的网络安全合规基线，侧重防御

医保规范: 强制数据共享 + 高标准安全兜底

解读：安全不再是业务发展的阻碍，而是支撑“全国影像数据互通共享”的基石。

《医保影像云》规范 & GA/T 2380-2026 协同要求

vinchin

01 安全等级：合规准入的硬性门槛

国标要求：确立等保三级为行业安全基准线。

规范深化：明确系统上线前必须通过等保三级测评认证。

协同价值：实现国家强制标准与行业准入条件的无缝衔接。

02 数据存储：加密与长周期归档

国标要求：存储强制加密，存储期限不超授权，防止越权留存。

规范深化：门诊影像存15年/住院存30年，明确超长留存期。

核心：建立长期、分层、合规的归档策略，兼顾安全加密与使用的长期调阅需求。

03 数据使用：隐私保护与价值挖掘

国标要求：严格遵循最小权限原则，严控访问范围。

规范深化：AI训练/科研等二次利用场景，必须执行去标识化。

协同价值：在合规前提下，规范医疗大数据的科研应用路径。

04 灾备要求：业务连续性量化指标

国标要求：强制实施异地备份，定期开展恢复演练。

规范深化：定期自动化备份，明确量化指标。

核心：将灾备原则转化为可考核的业务连续性标准。

05 数据安全：强国密加密，放丢失篡改

国标要求：强制使用密码技术，防窃取篡改。

规范深化：传输/存储双重加密，推荐国密算法

核心：必须支持国密算法的端到端加密，确保数据安全。

06 审计安全：操作留痕与溯源

国标要求：全操作行为审计，确保数据可溯源。

规范深化：日志留存≥6个月，覆盖数据库审计。

核心：事前防御+事后溯源的全方位审计。

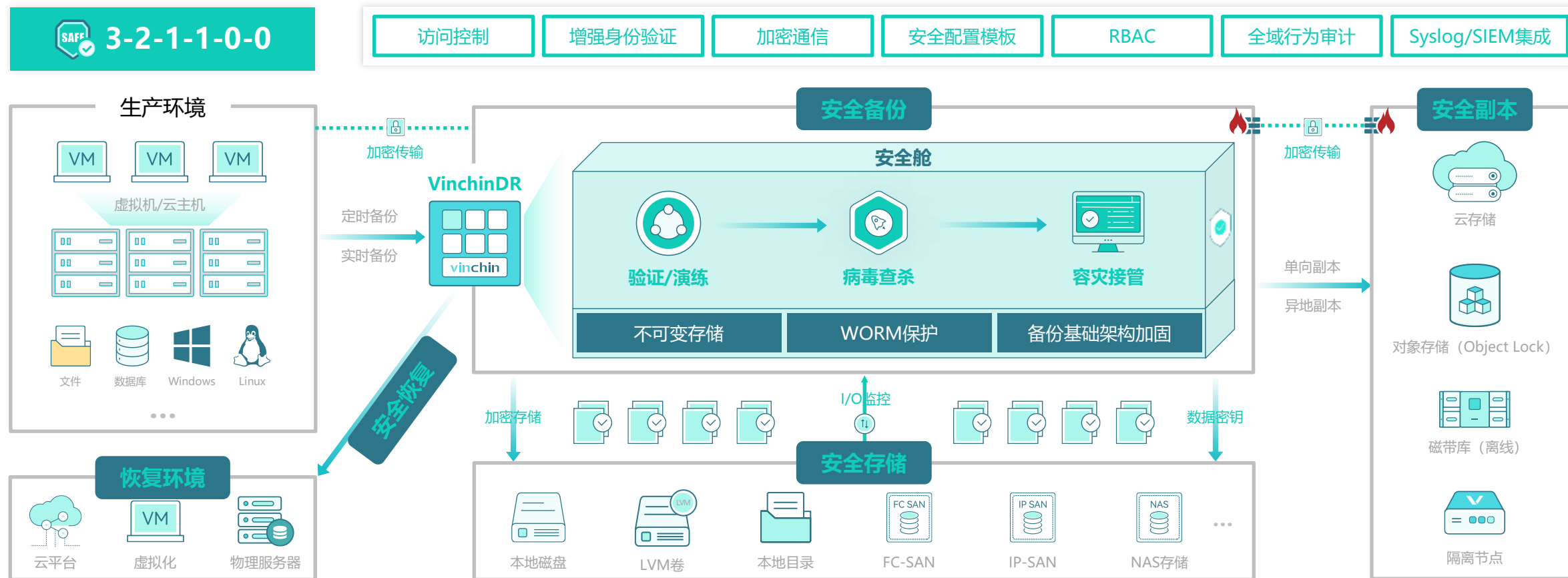
PART 02

云祺解决方案



存储安全与全生命周期管理

vinchin



全程加密防护

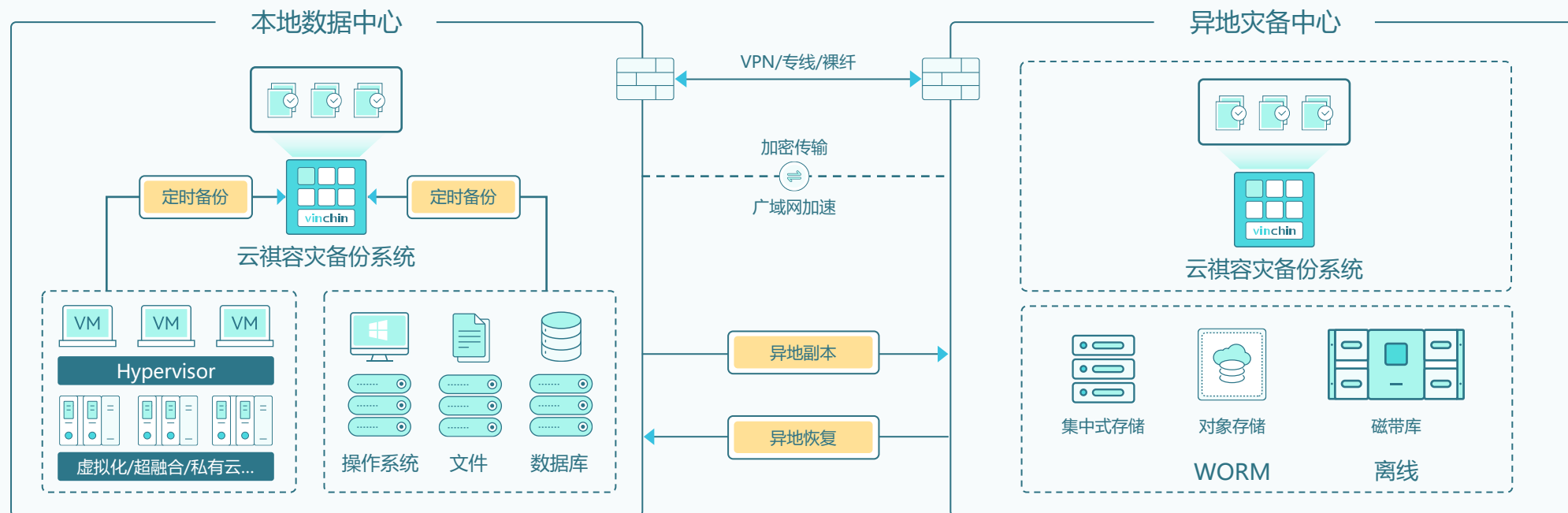
WORM 防篡改

异地副本容灾

全生命周期归档

异地副本数据容灾方案

vinchin



数据异地副本

定期将最新备份数据自动传输到异地数据中心，避免机房级灾难，支持广域网加速与加密传输。

窄带宽异地传输

通过源端压缩、断网续传以及永久增量副本等技术适合窄带宽场景，提升传输效率。

统一管理

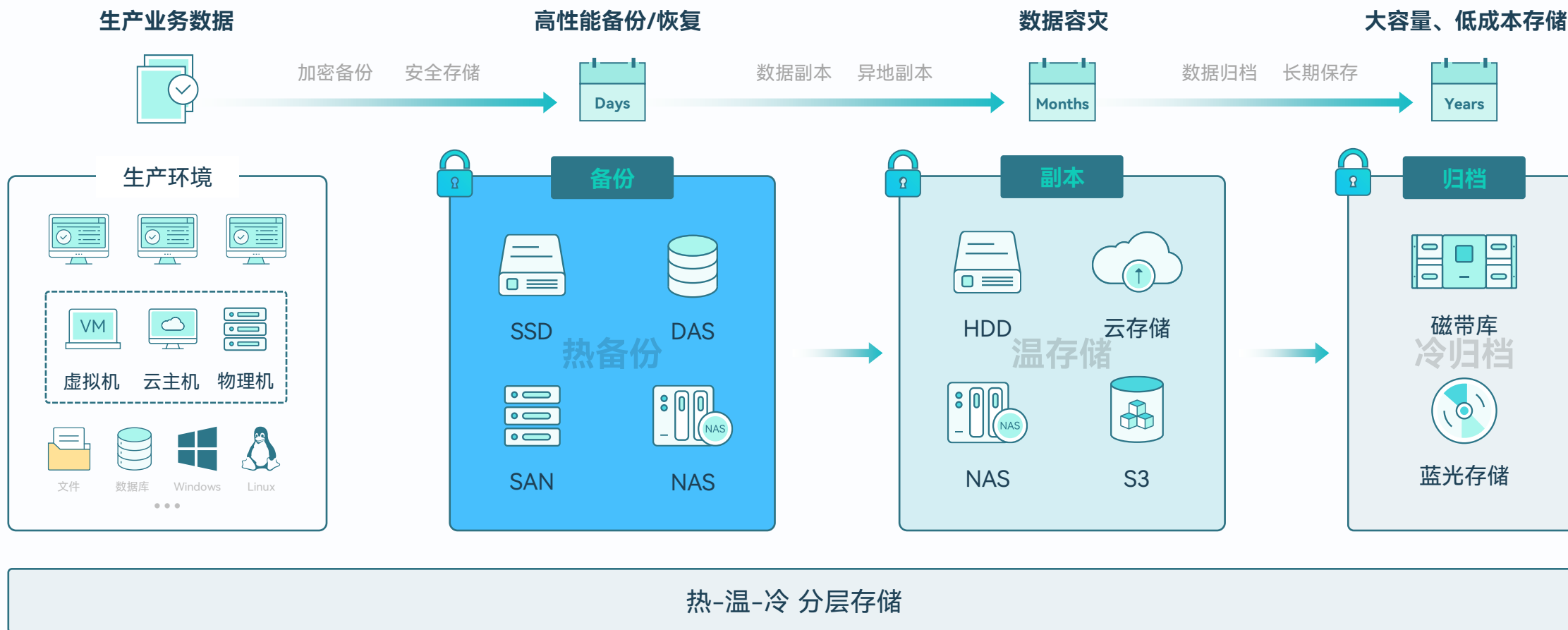
一个平台统一管理两地本地备份、异地副本，结合可视化大屏实现轻松监控运维。

数据库实时保护

vinchin

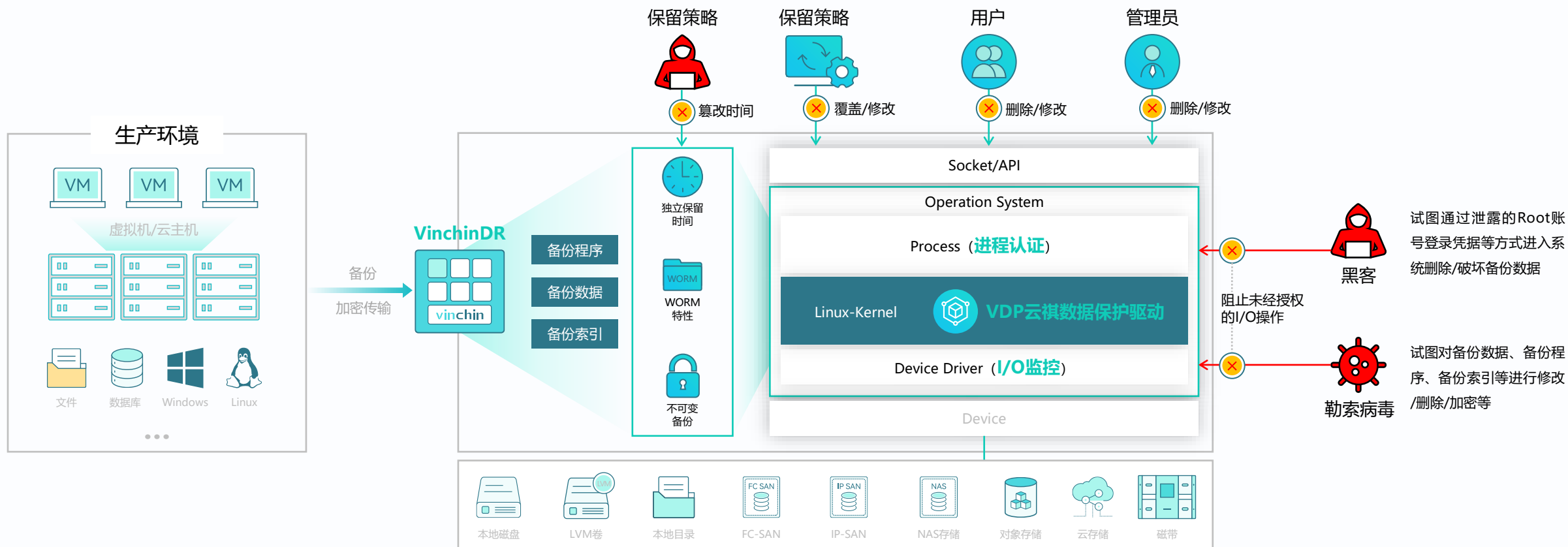


数据分层管理



不可变存储，以不变应万变

vinchin

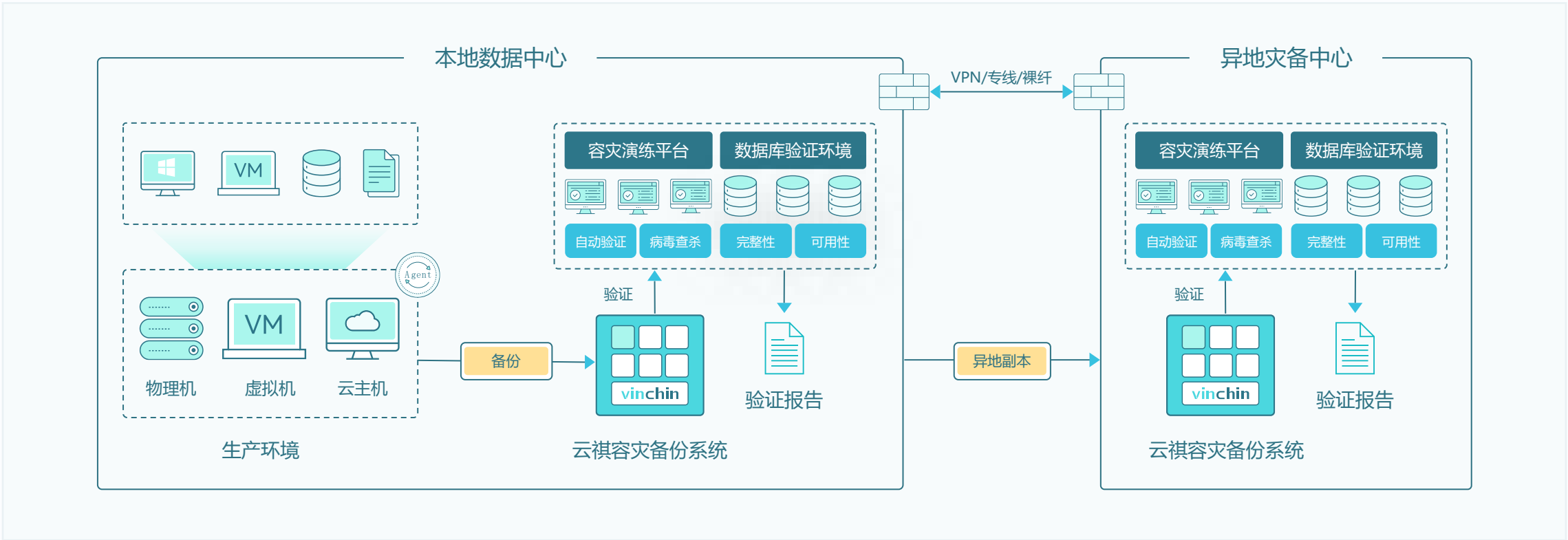


勒索防护：内核级防勒索加固，阻止恶意软件从后台破坏备份程序、备份数据、备份索引等关键数据和组件

进程认证：进程必须经过认证才可进行存储I/O操作，实时监控后台进程，第一时间阻断异常行为

不可变存储：使用原生不可变存储或对象存储Object Lock、物理磁带离线存储等实现备份数据不可变特性

WORM保护：保留时间独立计算，防止root账户、备份管理员非法删除、篡改备份数据



隔离环境病毒查杀

验证过程全程与生产环境隔离，结合第三方杀毒软件，在隔离环境对备份数据进行查杀。

降低验证成本

使用内置容灾演练平台可直接拉起系统环境进行数据验证，减少用户隔离环境搭建成本。

安全合规

通过定期进行容灾演练，生成数据验证以及病毒查杀报告，企业可以大大增强其安全合规性。

可视化验证报告

自动生成验证报告，确保验证结果可视可见，可发送到邮箱，支持自定义报告模板。

PART 03

案例分享



业务挑战：

业务平台多



众多信息化系统都由虚拟化平台承载，平台压力大，容错能力低。

数据增量



业务系统每日产生大量数据，对数据访问频率高。

面临风险多



医疗行业近年来频发勒索病毒入侵事件，建立安全保障机制刻不容缓。

云祺方案价值



虚拟机整机备份

使用云祺备份整个虚拟机，备份过程中无需关机，不影响业务运行。



重复数据删除

通过重复数据删除技术，只备份虚拟机有效数据，减少备份数据量。



LAN-Free 备份

通过 LAN-Free 方式备份数据，不占用业务系统带宽，降低医院生产网络负载。



瞬时恢复

秒级时间内瞬时恢复任意备份点数据，恢复医院业务系统运行，减小业务中断风险。



多种时间策略配合

支持多种备份模式，配合时间策略，解决业务系统数据增量大的问题。

业务挑战：



异构虚拟化平台

医院采用不同虚拟化平台承载业务，大量虚拟机都运行在虚拟化平台中。



网络情况复杂

面对大量数据增量和即将占用生产带宽的备份流量，医院业务网络负载较重。

云祺方案价值



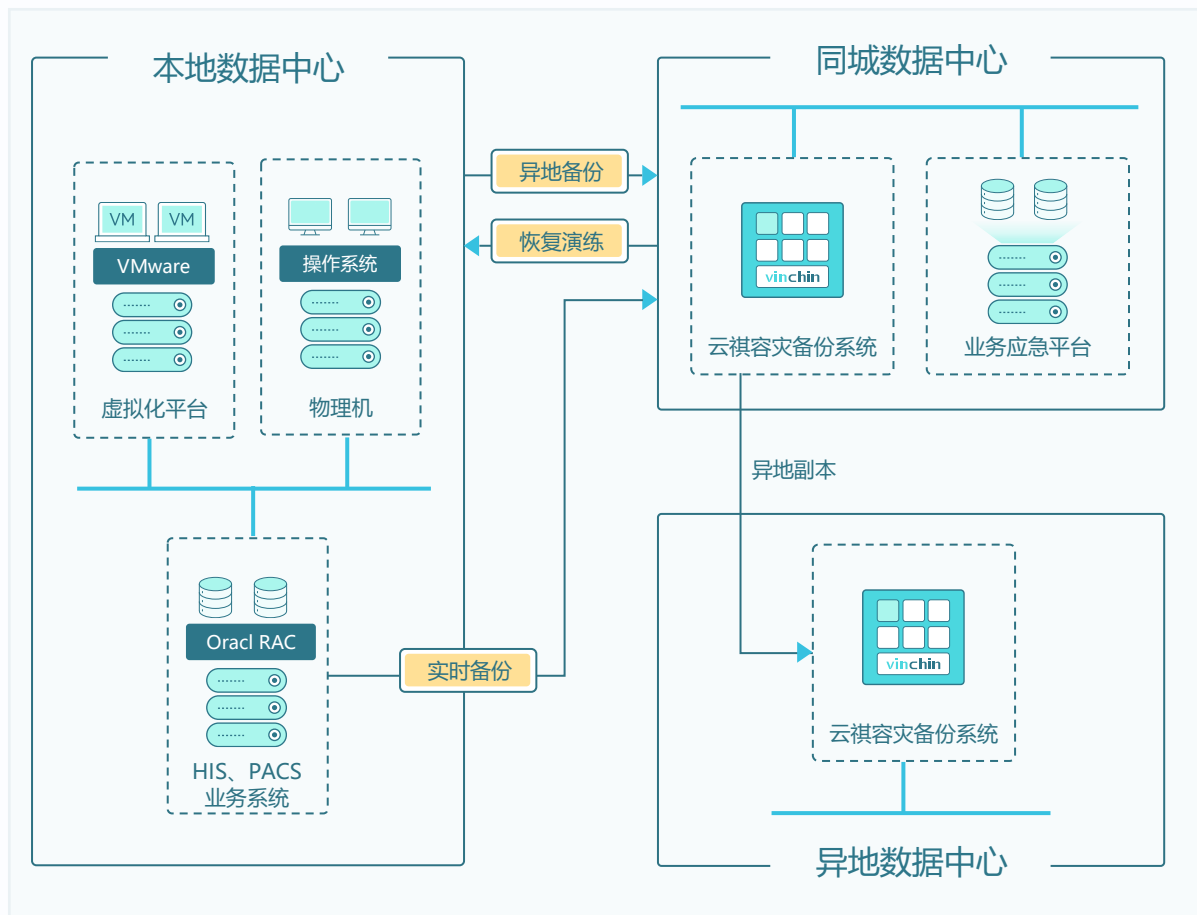
跨虚拟化平台统一保护

云祺备份软件同时支持国内外主流虚拟化平台的备份，和众多虚拟化厂商展开合作，可以完美对应多虚拟化平台数据保护难题。



业务快速恢复能力

云祺备份软件提供丰富的业务恢复方式，提供瞬时恢复，秒级恢复业务运行，直接接管业务；支持细粒度恢复，快速恢复特定文件数据。



现状及需求

- 对数据中心虚拟化平台的虚拟机以无代理的方式进行备份，且支持文件、业务应用、操作系统等数据类型。
- 极端情况下对核心HIS业务系统故障时，需减少业务停机时间，保证核心业务的连续性；
- 核心业务数据要实现异地备份（同城以及异地），同时需要满足异地业务快速恢复及接管的需求；
- 合法合规，要满足等保三级要求，能及时提供相关的资料，需要满足电子病历相关评审要求。

云祺方案价值

- 通过融合方案，对医院相关信息系统的保护，实现了文件数据、应用数据、系统数据的多重保护机制；
- 采用异地备份的方式将医院数据中心数据备份上云，同时通过副本数据功能将备份数据同步到异地数据中心实现跨城异地数据备份；
- 经过相关业务系统灾难演练，提供电子病历系统灾难恢复体系相关依据，协助医院进行电子病历五级评审；