

# 县域医共体 / 医疗集团 / 千县工程整体解决方案及案例

## 需求背景

2019年8月30日，国家卫生健康委发布了《关于印发紧密型县域医疗卫生共同体建设试点省和试点县名单的通知》，发布了浙江、山西两个试点省份及全国567个试点县名单。以县中心医院为龙头的医疗共同体成为县域医疗行业的建设趋势。对于信息化要求实现集中部署建设、医疗协作网高效联动各个医疗机构，及整体的安全服务体系，并在22年有发布“千县工程”计划，推动上千家二级医院提升至三级医院的医疗服务水平，也看到了大量的医院进行了二生三和医共体的合并建设。

## 县域医共体 / 医疗集团整体解决方案

医共体一体化基础架构拓扑图



医共体建设按照“总体规划、分步实施”的原则，在信息基础设施的建设中应按照计划、分层次、分批实施，系统设计充分考虑可扩展性；同时一切建设以经济实用、适用为出发点，具体设计如下：



### Sangfor Cloud 保障核心业务稳定、安全运行

方案规划在中心医院搭建以超融合架构为基础的医共体云平台，提供整个硬件基础资源服务，通过“超融合架构”实现资源、业务、数据的集中承载和统一调度，构建全栈式医疗云平台。依照医共体各类业务系统众多且不一的需求，按需分配相应的计算、存储、网络等基础架构资源；同时还可根据业务应用情况，随时随需便捷扩展，实现医共体的“盆栽生态”。此外，Sangfor Cloud 超融合数据中心还具有云操作系统，通过该操作系统，运维人员可统一对医共体云平台数据中心进行资源管理调度和监控管理。



### SD-WAN 打造安全可靠的组网链路

医共体拥有多个基层医疗接入机构，在乡镇卫生院部署 SDWAN、WOC；根据需求选择性开启 VPN、防火墙、行为审计、广域网优化、虚拟前置机等功能；中心通过部署集中管理平台 BBC 实现全网可视化运维；智能管理分支网络设备、统一的策略配置和下发，保证整个医共体网络的健康运行。



### XSec 提供丰富的安全能力平台

医共体建设涉及到基层医疗机构的接入，网络安全不仅涉及到多基层医院接入的安全，还涉及到中心医院的网络安全，需要非常完善的安全能力。深信服通过设计软件定义的安全技术，匹配网络安全建设中的多场景建设需求，为医共体提供安全能力服务化交付平台 XSec。此外，方案还提供等保建设方案中要求的各种安全设备，实现“持续保护、不止合规”的安全防护效果。



### aDesk 构建统一的桌面办公资源池

深信服设计通过桌面云方式解决医共体办公桌面统一配置和运维问题。通过在医共体数据中心部署桌面云一体机平台 VDS，构建统一的桌面资源池；各乡镇卫生院、村卫生室则利用 aDesk 瘦终端，通过组网链路连接云桌面办公。医共体信息运维人员可以在中心医院，通过远程的方式对散于各乡镇村的终端进行集中管理，实现高效运维，提升业务效率。



### SIP 构建全网安全智慧大脑

鉴于医共体全网安全仍是割裂式的，缺乏统一平台对医共体全网流量、业务、资产、威胁、攻击和可疑流量等重要的网络安全信息进行有效监测和可视化展现。因此，本方案通过在中心医院部署安全感知平台，在各网络关键节点部署流量检测探针，对整体安全有全局的把控，真正看清网络现状、看到潜伏威胁、看懂风险影响面，并通过该平台对现网所有安全系统进行统一管理和策略下发。

## 方案优势



### Sangfor Cloud 保障业务稳定

- 超融合架构简单、医共体平台业务快速上线，扩容无瓶颈。
- 通过云管平台呈现统一可视化的管理界面，所有资源的管理和维护处理“即换即用”，实现便捷运营。
- 提升关键业务系统可靠性，多重技术保障数据可靠；通过应用交付，实现应用平滑迁移上云，业务访问零中断。



### SD-WAN 提供最佳访问体验的组网方案

- 实现基层医院 SSL 加密接入中心医院，保证业务数据交互传输的安全性。丰富的 NFV 组件，只需开通授权就可按需扩展广域网优化、下一代防火墙、上网行为管理、SSL VPN 等网络功能。
- 实现基层医院零 IT 运维，快速上线，即插即用；中心医院管理则更为敏捷，远程编排分支 IT，并基于 GIS 地图支持组网安全态势“秒级感知”，全网可视化运维。
- 通过应用级智能选路与加速技术保障关键应用，在广域网构建极致体验的医疗协作体验。



### XSec 满足安全建设丰富能力

- 不仅可向多个基层医院提供差异化的安全能力，而且能补充中心医院本级的安全能力的不足，提供从安全接入到整体安全运营全生命周期的安全服务。
- 通过简单的自助服务申请，开通流程即可快速获得对应的安全服务。云运营方可以像交付计算、存储资源一样进行安全服务资源交付。
- 方案涵盖了用户等保建设整改过程中所有技术方面的内容，实现南北向和云平台的東西向安全防护，满足最新等级保护标准要求。
- 旁路部署，不改变现有网络架构，部署更简单，广泛使用于物理环境和虚拟化环境下的等保建设。





### aDesk 办公的方便、安全、体验更好

- 提供更高效的桌面运维方式，可实现远程运维，尤其对于医共体终端分散的现状，桌面云可充分缓解运维压力。
- 集成了全方位安全策略，包括多种接入认证方式、全面的传输加密算法、灵活的安全控制策略、独创的个人盘加密技术等，实现医共体端到端的安全保护。
- IO 与缓存加速技术、SRAP 高效交付协议，让医共体桌面云启动和运行速度大幅提升。多媒体重定向技术、云终端硬件芯片解码技术，提供流畅播放高清视频，避免服务端资源占用。



### SIP 让安全可感知、易运营

- **防护新型威胁：**提供全面的威胁检测能力，不仅具备防护各类已知威胁能力，同时具备人工智能、机器学习、行为分析等技术防护各类未知威胁和异常行为，如勒索病毒等。
- **感知安全态势：**通过攻击趋势、有效攻击、业务资产脆弱性、业务外连风险、横向威胁等维度对全网安全态势进行整体评估，有效把控整体安全态势，进行安全决策分析。同时对内网横向攻击也做到全面检测，实时监测黑客跳板攻击与横向渗透行为，从而全方位感知整体安全态势。
- **简化安全运维：**平台对检测出的安全威胁不再单纯以安全事件展示，通过大数据技术，基于攻击链维度关联分析，以用户关注的业务和终端的视角呈现安全事件具体带来的危害，并对安全事件进行详细的举证，给出相应的处置建议，让用户一目了然，从而简化日常安全运维。
- **快速联动响应：**对发现的安全事件，通过各类安全设备与终端软件产品实现快速的响应处置，有效防护各类安全威胁。



## 精选案例——宝丰县人民医院



### 背景简介

宝丰县委、县政府高度重视卫生健康事业高质量发展，呼应民生健康需求，不断加强医疗卫生体制改革，推进紧密型医共体建设，成立了以宝丰县人民医院为龙头，覆盖全县医疗、预防、保健机构的医疗健康集团。作为牵头医院，率先先行、精准下沉，提升基层医疗服务能力，发挥县域龙头作用，以“信息化建设”为纽带，向上与城市三级医院对接，向下辐射乡镇卫生院和村卫生室，让“信息多跑路，群众少跑腿”助力打造宝丰县构建便民高效的县域新型卫生健康服务体系，推进区域医共体内外的信息共享和业务协同，让群众“小病不出乡、大病不出县”。



### 业务需求

平台涉及的业务繁杂，实时性要求高且业务不间断，安全可靠是用户对数据中心的首要需求，所有业务系统都没有高可用功能，业务连续性无法得到保障，只要服务器出现操作系统问题或是物理故障，业务就会中断。除 HIS 外，所有业务系统数据无容灾，一旦出现硬盘或存储故障，所有数据将会丢失，风险极大。



健康医疗大数据作为国家重要基础性战略资源，网络安全建设变得尤为重要，安全体系的建设必须保证全县医疗机构的相关数据安全。后续连接医共体的基层医疗机构后，由于机构地域分散，缺少网络防护设备，容易受到外部或内部侵入破坏，缺少相关防护措施，信息化管理、维护难度大。



### 深信服解决方案

**建设规模：宝丰县人民医院 +4 家县医院 +13 乡镇卫生院。**

- 使用 12 台超融合一体机承载东软的 HIS、PACS、EMR、医共体等全院业务，并采用本地容灾备份软件，可以达到秒级的 RPO，理论上可以恢复任何一秒的数据，满足数据中心对稳定性的要求。
- 使用 7 台分布式存储按照满足未来 5 年的资源消耗以及数据存储容量需求，采用两台以太网千兆交换机，并做多虚一，承载高容量区域的管理流量和 VXLAN 网流量，两种流量划分 VLAN 进行隔离管理。
- 等保按照三级等保设计标准，深信服提供完善的等保三级高性价比的建设方案，在安全管理区通过下一代防火墙与其他区域安全隔离，规划终端防病毒系统、全网安全态势感知、等保一体机等，实现全网安全可视，智能联动，统一运维。

## 用户收益



### 云化数据中心建设

通过超融合架构构建的全栈式医共体云平台，使业务快速上线，扩容无瓶颈；通过运管平台呈现统一可视化的管理界面，实现所有资源的管理和维护故障处理即换即用，减轻运维。



### 医共体安全防护

建立了可感知、可联动、可防护的主动防御安全体系，在满足现有安全的等级要求的前提下，将安全能力分散立体化部署于医共体系统中，进一步加强薄弱点的安全能力。

## 更多案例

客户名称	级别	客户名称	级别
江苏省金湖县医共体	二级甲等	湖北五峰医共体	二级甲等
云南南涧县医共体	二级乙等	浙江云和县医共体	二级甲等
宁夏贺兰县医共体	二级甲等	河北临城县医共体	三级甲等
山西省清徐县医共体	二级甲等	四川中江县医共体	三级甲等

