

互联网医院托管云解决方案

1 需求背景

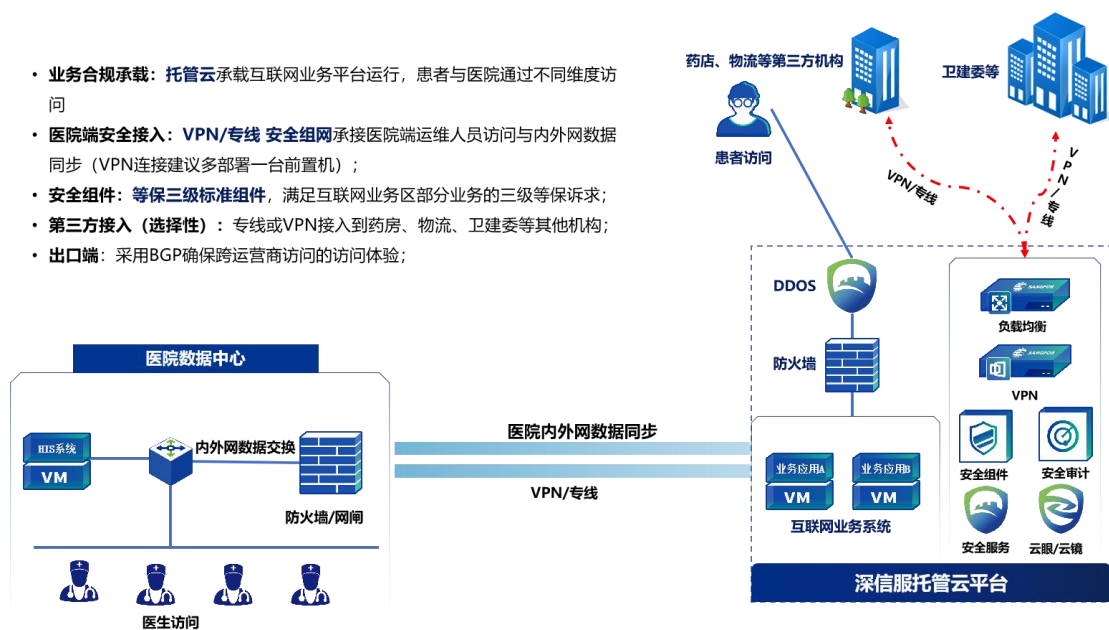
互联网医院就是通过互联网技术，把医疗资源跨地域、跨时间进行医疗服务，通过线上线下医疗服务的无缝对接，实现医患良性互动的目的。但针对互联网医院的信息化建设普遍存在以下问题：

现有的 IT 架构资源调度难、弹性扩容难：未来互联网业务升级以及互联网医院建设的 IT 资源需要具备灵活弹性扩容的属性，可以快速及时响应业务模块优化进行资源调整。

互联网区域信息安全风险，运营成本高：内网区域与外网之间直接通过防火墙直接连接，且需要满足等级保护要求，针对互联网侧易遭受攻击的特点，防护难度大、运营成本高。

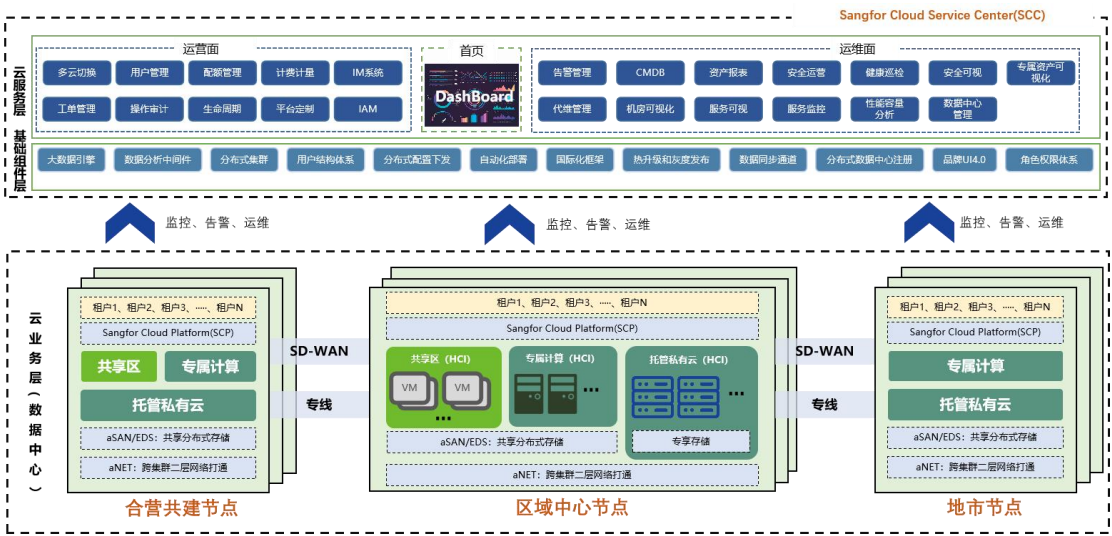
2 深信服解决方案

根据医院现有互联网区业务需求并且综合考虑互联网业务未来三年的资源演进路径，建设医院互联网业务区，可采用托管云形式，将医院互联网业务托管到指定云节点，实现内外网业务的强隔离，并且采购对应的安全组件与安全运营服务，以满足等保三级的安全建设要求。



按照数据中心安全区域等级划分，互联网作为承载对外提供服务的业务区域，处于整体数据中心的半安全区，通常会部署不被信任的系统，把敏感的内部业务系统网络和提供互联网访问服务的业务系统网络分开，阻止内网和外网直接通信，以保证内网安全。医院互联网业务区域通常会部署外网 OA，医院门户网站 Web 页面，外网邮箱以及互联网医院业务系统和数据库。互联网业务区应严格按照等级保护三级标准建设。

根据医院业务位置就近选择托管云数据中心节点，托管云数据中心全部部署在专业的托管机房，参照 T3 及以上的标准建设，拥有充裕的带宽资源，并预留了物理空间，满足快速扩展的需求；两路市电并配备发电机，完整的环境安全措施，包括防雷、防水、防静电、恒温恒湿、电磁、消防等；7*24 小时安保人员，多种访问控制体系、多重门禁系统自动识别进出人员身份，定期进行巡检及盘点等；部署统一运维接入平台实现用户对云平台操作管理的统一接入、统一认证、统一授权与统一审计；机房及云平台按照国家公安部三级等保标准设计。



3 方案优势

3.1 业务交付一体化

托管云一体机运行互联网医院业务，深信服提供一体化解决方案，无需客户对基础架构做额外设计、部署与运维。同互联网医院业务直接一体化交付给客户，互联网医院业务整体部署在云端，安全由深信服负责、业务由 isv 负责，让客户

无需对该类业务耗费更大精力，降低运维压力与安全风险

3.2 降低 TCO

通过托管云数据中心，控制和减少物理服务器的数量，明显提高每个物理服务器及其 CPU 的资源利用率，从而降低基础设施投资成本。降低运营和维护成本，包括数据中心空间、机柜、网线，耗电量，冷气空调和人力成本等。

3.3 服务实时响应

互联网医院作为医院少数完全对外访问业务，其自身还需要持续访问医院的核心数据（患者挂号、处方等数据）其安全风险远高于医院内网业务或其他外网业务。因此医院传统建设模式往往需要增购部分安全设备，并且安全检查中，互联网医院业务屡屡暴雷，通过托管云模式将安全建设全程托管，安全问题 5 分钟响应，对平台安全全流程负责，确保业务安全。

3.4 权责边界更明晰，医院聚焦内网安全

托管云协同软件厂商交付一体化方案，让外网业务的安全风险更加明晰，一旦发生安全问题可直接找到对应人员，不同于传统外网业务大量前置机、大量厂商与硬件导致权责难以划分，医院只需要聚焦精力放在内网的核心业务内，无需对互联网医院安全投入大量精力。

3.5 云内建安全体系结构

深信服托管云架构构建的私有云结合了自身在安全领域的技术领导地位，规避了传统架构极不灵活的网络、安全、存储体系结构，这种体系结构使用软件主导型网络和安全、存储虚拟化服务，获得云计算基础架构的全面敏捷性。

4 典型案例

成都市第六人民医院：通过服务化交付托管云上资源，业务主要分为三类：外联平台、微信平台、前置机业务。

广州市荔湾中心医院：通过托管云提供一站式云等保服务，为客户提供业务

安全评估，安全事件监测，专家应急响应等服务，进一步提高业务安全。

山东大学第二医院：互联网业务托管云上灾备建设；

上海市第九人民医院：互联网业务托管。