

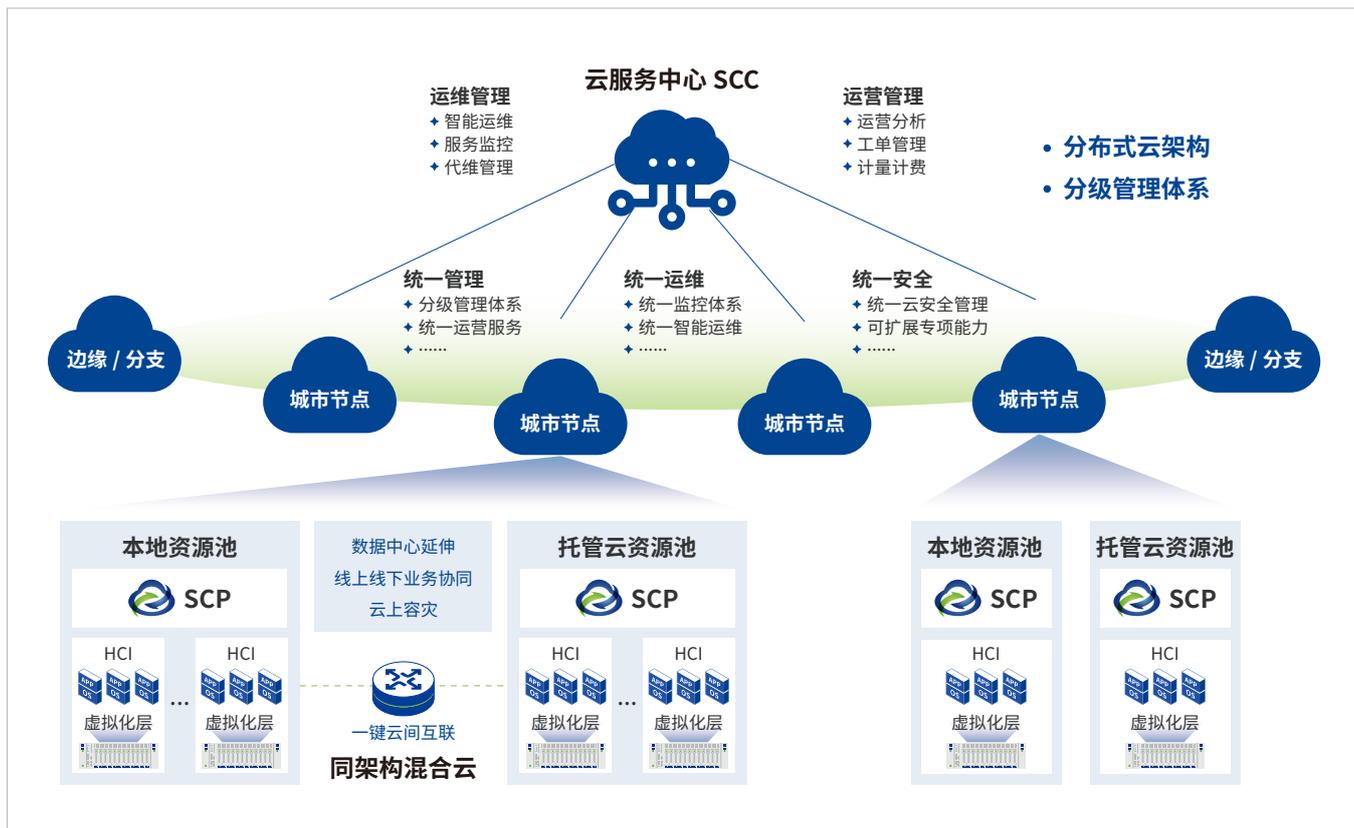
# 医院托管云解决方案及案例

## 现状与挑战

随着智慧医院建设步伐加快，医院的新型业务也不断增加，比如互联网医院、便民就医、远程诊疗等互联网类业务。但传统信息化建设之中的应用和资源是紧耦合的，使得底层架构缺乏弹性，难以快速适应医院业务的发展。数据中心本地设备品牌众多，使得信息科室很难对基础设施实行统一的监控和管理。尤其是现在互联网业务、新型应用不断增加，医院的安全防护逐步从传统的“合规建设”走向了“安全效果”建设，更好地保障安全服务、安全效果是医院数据中心建设的首要前提。

## 深信服解决方案

托管云是一种新的云服务模式，以租用的方式为用户提供计算、存储、网络、安全资源以及全生命周期的业务托管服务，实现“资源专属”、“安全防护专属”、“专业服务保障”，通过服务交付，帮助用户快速、轻松地构建属于自己的云化数据中心。托管云能够让用户获得如自建机房的资源，以及提供如公有云般的资源扩展灵活性和服务能力。除此之外，还能获得专业服务体验。



托管云分布式云整体架构

计算	云主机	专属计算	托管私有云	
存储	块存储	文件存储	对象存储	备份&容灾
	CDP	云盘		
数据库	RDS MySQL版	RDS Oracle版	RDS SQLServer版	Redis
	MongoDB	RDS GaussDB版	RDS PostgreSQL版	
网络与 CDN	弹性IP	NAT网关	私有网络VPC	应用交付
	CDN加速	VPN	IPv6改造服务	专线接口
安全	DDoS防护	下一代防火墙vAF	数据库审计DAS	基线核查
	日志审计	堡垒机OSM	EDR	数据安全
	云WAF	云镜	CWPP	态势感知SIP
	SSL证书	内容安全		
大数据	大数据	X-Search	X-HD	Dipper
	Clickhouse			
容器与中间件	容器服务	Kafka	RabbitMQ	RocketMQ
企业应用	短信服务	平台定制		
贴心服务	设备支持服务	智能安全防护	数据库专业服务	

托管云服务目录

## 优势及亮点



### 贴心服务

首先托管云是在用户整个业务生命周期内，为用户提供“一站式省心服务”。托管云的服务，有三个维度的核心特点：第一是“预警式主动服务”，比如平台会免费为用户提供业务拨测，一旦业务中断或者时延超出阈值会自动生成工单下发给管家，管家会及时的联系用户并闭环处置问题；第二是“千人千面的服务体验”，深信服联合本地合作伙伴，线上线下结合的根据不同用户的业务诉求和服务诉求提供更好的服务体验；第三是“高性价比的专业服务”，目前深信服已经推出了更多的高阶服务，比如容灾备份演练、高可用架构升级等等来满足用户不同业务场景的服务诉求。





### 安全有效

从用户业务上托管云开始到用托管云的过程中都为用户提供较高的安全水位线，而且当用户真的发生安全事件时还会为用户进行数据兜底。先说“构建业界领先的安全水位线”，深信服托管云从用户业务上线开始就会帮助用户进行安全基线检查，如病毒扫描、漏洞扫描、弱密码检查、高危端口等等，而且在后续业务运行和管理过程中也会保持。另外，托管云给用户提供“面向关键业务的数据兜底”，当业务数据因病毒或其他原因导致数据破坏，深信服团队会协助用户最大程度恢复数据；当前，托管云已经具备“更丰富的安全解决方案和服务”，比如一站式等保、重保值守、安全托管等一系列的高级安全服务都可以按需选择购买。

#### 提供安全高水位线

上线前提供一套完善的安全基线方案，并帮助客户进行正确的安全配置、最大化收缩暴露面；运行中我们会持续跟踪业务变化进行配置更新、更新病毒库、并对热点漏洞关联业务进行分析，对高风险的攻击路径进行主动阻断



#### 数据兜底服务

对于核心业务和关键数据我们通过存储快照进行保护兜底，协助客户进行灾难恢复，比如发生勒索病毒的时候



#### 丰富的安全解决方案

提供丰富的安全解决方案和服务，如：一站式等保服务、护网重保服务、密评服务、MSS 服务



### 业务数据专属可控

深信服托管云通过资源隔离给用户提供“全栈专属云”，而且本地化接入数据不出省/市，能够保障数据私密性。另外在代维、协管、权限划分等各类管理举措上都还给用户，让用户真正能掌控资源。



#### 专属资源物理位置透明

- 所属机房位置
- 设备的机架信息
- 设备的上架时间
- 设备占用的空间
- 设备运行时长

#### 专属设备状态透明

- 设备的规格参数
- 剩余可用资源
- 实时的负载压力
- 网络拓扑信息

#### 业务代维可控

- 代理权限最小化
- 实时在线直播，录播重播
- 随时中断，防止突发运维事故
- 操作留痕，满足审计合规

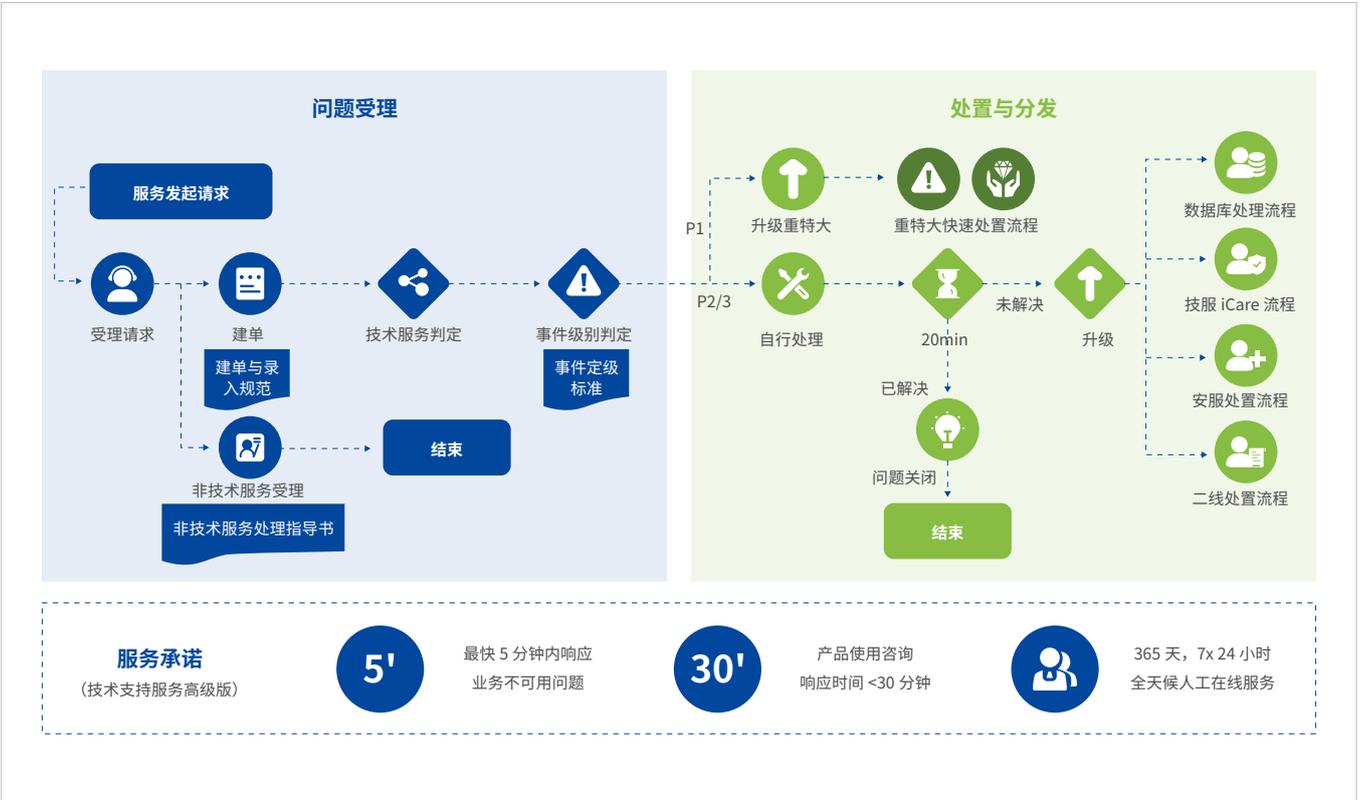
#### 权限可控

- 像私有云一样管理权限、实现资源分配、基础设施的变更
- 提供协管员功能，可以分配协管员的权限



### 实时响应的 IT 服务

深信服提供明确的服务响应时间窗口，除标准的 IT 咨询服务外，还提供包括：等保咨询服务、运维巡检服务、数据库运维服务、安全服务等 IT 全流程服务。医院可根据自身现状，自由订阅相应服务，真正实现医疗服务定制化。



服务响应流程与服务承诺



## 精选案例——内蒙古中医院（全院级上云）



### 医院简介

内蒙古自治区中医医院，集医疗、教学、科研、康复、保健、制剂、养生于一体的自治区级三级甲等综合性中医医院，并入选国家中医药传承创新工程项目建设单位。编制床位 1000 张，医院设有临床科室 45 个，医技科室 9 个，病区 26 个。

### 业务需求

#### 降低运维压力、扩容虚拟化资源

医院目前运维人员较少，大量基础硬件设备面临更新换代，并且随着医院业务的逐步增加，数据中心原有的大量异构品牌的设备也给医院运维带来了许多附加工作。医院当前的虚拟化资源冗余较少，出于对未来业务的承载考虑，医院也需要对底层云平台进行扩容。

#### 等保三级建设、勒索病毒防范

处于政策合规与等保新评分的趋势之下，以及针对内蒙区域医疗行业的勒索病毒攻击层出不穷，医院急需对安全建设进行更新升级。

#### 业务容灾建设

目前内蒙古中医院仅有一个数据中心，并未建设异地容灾中心，一旦医院数据中心遭受不可抗力导致数据中心停止运行，将给医院业务带来无可挽回的损失，并且面临患者数据丢失的风险。因此容灾建设是医院下一步 IT 规划的核心目标之一。

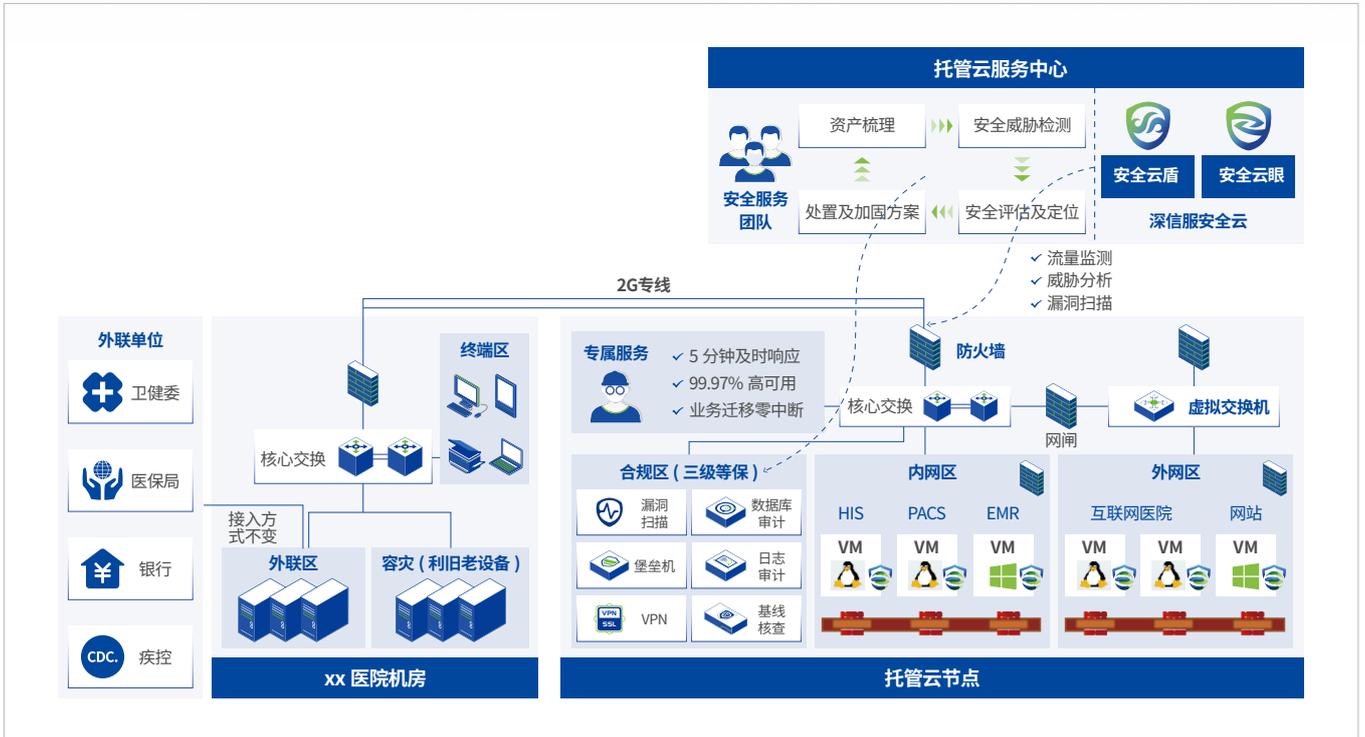
#### 信息化统一建设

从医院信息化管理者角度出发，当前医院的信息化预算主要以信息科和各个业务科室申请为主，缺乏统一的信息化管理平台与制度，信息化建设事倍功半，因此医院也迫切希望能够尽快建立统一的云计算管理平台实现对 IT 建设的精细化管理。

### 深信服解决方案

托管云承载内蒙古自治区中医院全院信息化业务系统，为全院 60+ 系统提供底层支撑与对应的云服务，支撑内蒙古中医院本院的相关临床业务开展，包括医院的外网业务与创新业务承载。

整个项目采用 13 台医疗云服务器进行配置，并与本地数据中心实现主备容灾建设，云节点配备 2 条万兆专线直连医院与医疗托管云机房。



医院信息系统上云迁移过程：



**第一阶段：**

2个月时间将医院外网虚拟化中对应业务虚拟机迁移至云平台。



**第二阶段：**

利用6个月时间将医院内网虚拟化中对应业务虚拟机迁移至云平台，其中利用两节点专属系节点搭建 Oracle RAC 数据库进行 HIS 数据库的迁移。



**第三阶段：**

业务迁移完成后，利用中医院现有服务器资源（HIS 新增一台、磁盘阵列物理搬迁）、网络资源、存储资源重新规划，部署备份容灾环境，定期进行备份还原、应急演练和故障恢复等操作。

部署完成后，用户可通过托管云管理平台对云上云下的双数据中心进行资源管理、监控、计量计费、维护等操作，支持组织或用户在线自助申请、使用虚拟资源，实现数据中心由“简单的虚拟化”向“云计算”飞跃。



## 用户收益



### 等保三级与容灾建设

通过云上构筑等保三级安全解决方案，满足医院业务的安全基线要求。同时形成了业务云上、云下容灾的建设模式，即便由于不可抗力导致任一数据中心出现故障，也能实现 15 分钟内的业务切换，数据近乎零丢失的容灾效果。



### 兜底服务

专属管家式服务、5 分钟内快速响应、问题闭环处理、专业的团队 / 标准化的流程 / 丰富的实践案例。



### 业务迁移服务

业务上线后，提供免费专家级安全体检、巡检报告、代维服务、高级专家服务。

## 方案价值

对比价值	自建/上云方案	托管云方案
<b>50%↓</b> 首年资金投入	一次性投入 <b>超 1000 万</b> 资金，还无法 <b>满足等保、T3 机房</b> 等配套要求	单年投入不足 <b>300 万</b> ，配套满足等保安全要求；并且 <b>无需一次性</b> 购买全部服务器
<b>100%</b> 运维公司不变 业务运维熟悉程度有保障	运维公司负责医院数据中心本身运维	<b>与医院原有运维公司合作，运维人员、业务熟悉程度有保障</b>
<b>5 分钟</b> 及时响应	传统上云方案仅有工单提醒，问题响应不及时 ( <b>1 天左右</b> )	1 对 1 专属项目经理； 7*24 小时 + <b>5 分钟</b> 内响应
<b>100%</b> 安全事件全处理	一周基础设施平均运维时间超 <b>15 个小时</b> <b>勒索病毒自身处理</b>	一周平均运维时间不到 <b>2 小时</b> <b>提供专属安全服务</b>

## 精选案例——成都市第六人民医院（DMZ 区上云）



### 医院简介

成都市第六人民医院是一所集医疗、科研、教学、急救、保健、康复为一体的国家三级甲等综合医院。医院曾先后获得“四川省十佳城市医院”、“四川省职工职业道德建设先进单位”、“成都市精神文明单位”、“成都市模范单位”、“成都市诚信示范医院”等荣誉称号，现为西南医科大学、遵义医学院、川北医学院、成都医学院等多所医科大学的教学基地及硕士联合培养点。

### 业务需求

#### 已有 IT 资源不足

现有互联网业务资源量难以满足后续医院业务扩容与升级所需，资源扩容势在必行。

#### 内外网业务未隔离，存在安全风险

医院互联网业务与本地内网核心业务都运行在一套超融合平台之上，通过逻辑隔离进行相应的访问权限控制。但互联网业务主要是面向复杂的外网环境，大量的访问带来的是大量网络安全风险。一旦外网业务失陷，可能会导致内网业务受到一定程度的影响。

#### 需建设可统一管理的混合云平台

医院当前已有两个数据中心，完成数据中心初步云化。互联网区业务平台需要能够实现与已有云平台兼容，并且能借助云管平台进行统一管理。

### 深信服解决方案

#### 成都市第六人民医院的托管业务主要分为三类

外联平台

微信平台

前置机业务

#### 为两类群体服务

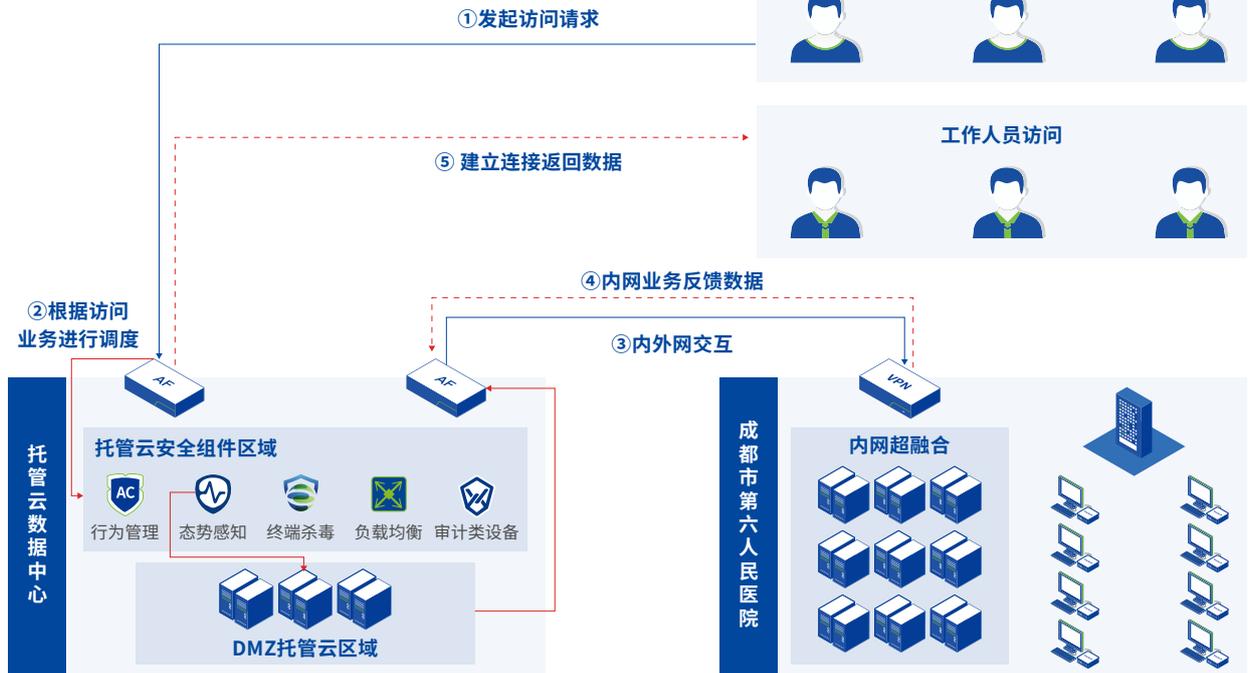
就诊患者微信挂号

工作人员访问前置机数据进行日常办公

就诊患者通过微信公众号等平台进行就诊服务时，通过互联网访问到成都市第六人民医院托管云数据中心的挂号平台，获取医疗服务。若挂号平台需要和医院内网业务如 HIS 等系统进行数据交互，则通过托管云数据中心和医院内网数据中心边界的 IPSec VPN 组网设备组建的加密隧道进行数据传输。

工作人员需要进行合同审批、HRP 系统调阅医院运营数据时，通过互联网访问到成都市第六人民医院托管云数据中心的 HRP 等业务系统前置机，然后前置机直接将数据返回给工作人员。若前置机需要和医院内网业务（如 HRP 等系统）进行数据交互时，则通过托管云数据中心和医院内网数据中心边界的 IPSec VPN 组网设备组建的加密隧道进行数据传输。

成都市第六人民医院  
DMZ 区托管云业务访问流程示意图



通过云管平台纳管本地超融合集群以及托管云互联网业务集群，监控本地与云端的业务系统与容灾系统的运行情况。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。

**用户收益**



**内外网业务隔离**

托管云实现内外网业务跨数据中心部署，对外访问全部基于托管云，内网只进行必要的业务交互，降低了由于互联网攻击导致内网业务受影响的风险。



**高性价比的安全防护**

采用云端安全组件给外网业务提供全方位防护，用户无需在本地购买硬件设备，在保障安全效果的同时减少了 DMZ 区的安全投入。



**业务迁移服务**

业务上线后深信服提供免费专家级安全体检、巡检报告、代维服务、高级专家服务。

## 方案价值

对比价值	自建/上云方案	托管云方案
<b>50%↓</b> 安全建设投入	原有缺乏 DMZ 区专属安全方案，整体建设与内网业务混合，如新建 DMZ 区投入超过 <b>70 万</b>	单年投入不足 <b>30 万</b> ，配套满足等保安全要求；并且无需购买服务器
<b>100%</b> 资源独享与数据可控	传统方案多为共享区资源，一旦医院业务增长，非常可能面临资源抢占。数据安全也难以保证	<b>资源全独享，性能有保障 数据可溯源，拔盘可拿走</b>
<b>5 分钟</b> 快速响应	DMZ 区面临大量互联网安全攻击，一旦业务停顿直接影响临床业务 ( <b>1 天左右</b> )	1 对 1 专属项目经理； 7*24 小时 + <b>5 分钟</b> 内响应
<b>80%</b> 运维时间	一周基础设施平均运维时间超 <b>15 个小时</b>	仅需定期查阅巡检报告即可； 一周平均运维时间不到 <b>2 小时</b>

## 更多案例

客户名称	级别	解决方案	客户名称	级别	解决方案
山东大学第二医院	三级甲等	互联网业务托管 云上灾备建设	上海市第九人民医院	三甲医院	互联网业务托管
石嘴山第二人民医院	三级甲等	全院业务上云	株洲市第二人民医院	三级医院	全院业务上云
徐州医科大学附属医院	三级甲等	互联网业务托管	复旦大学 附属耳鼻喉科医院	三甲医院	互联网业务托管
安乡县人民医院	三级甲等	全院业务上云	保定市第七医院	二级医院	全院业务上云
.....	.....	.....	.....	.....	.....

