



# 安全云桌面技术在智慧医院的应用和实践

胡晓伟

锐捷医疗行业解决方案咨询顾问

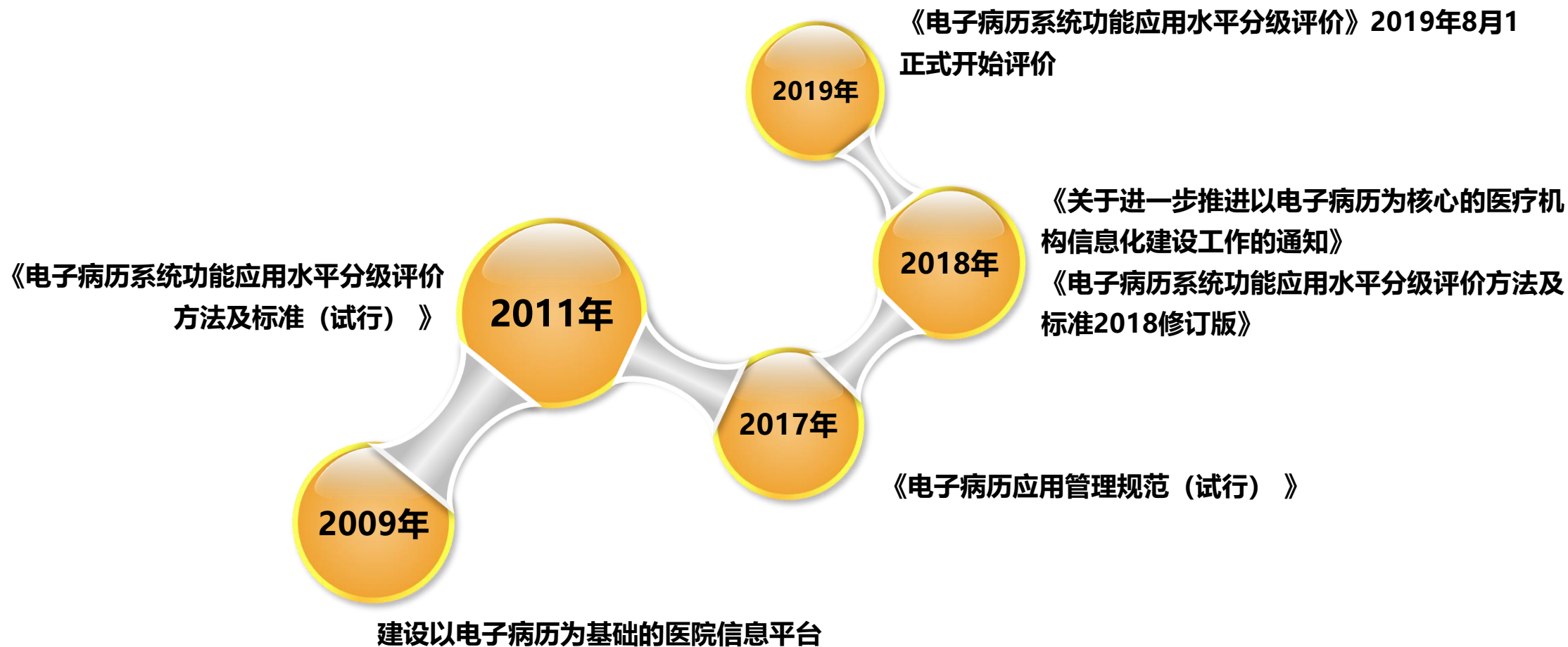
# 目录

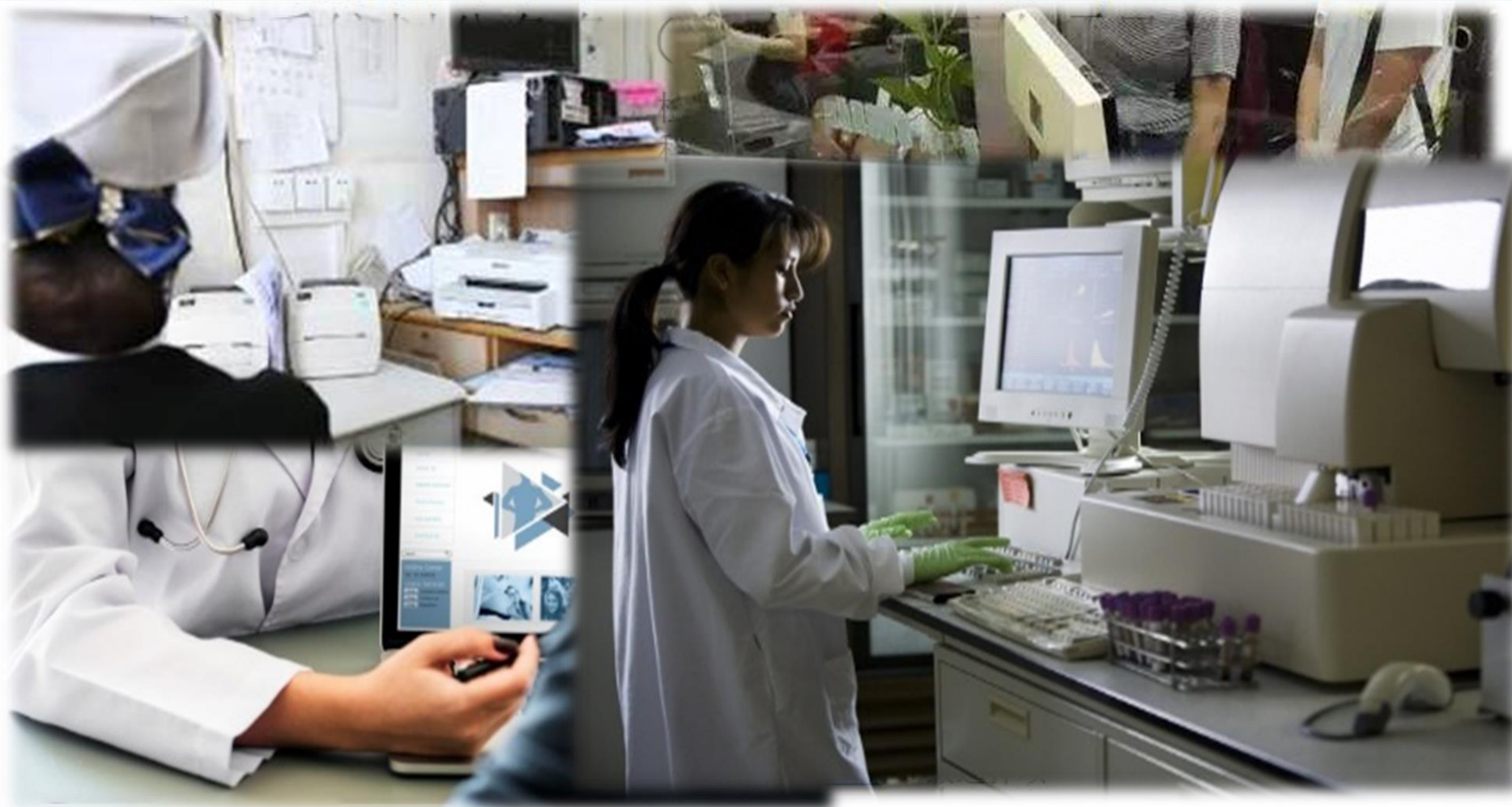
场景分析

解决方案

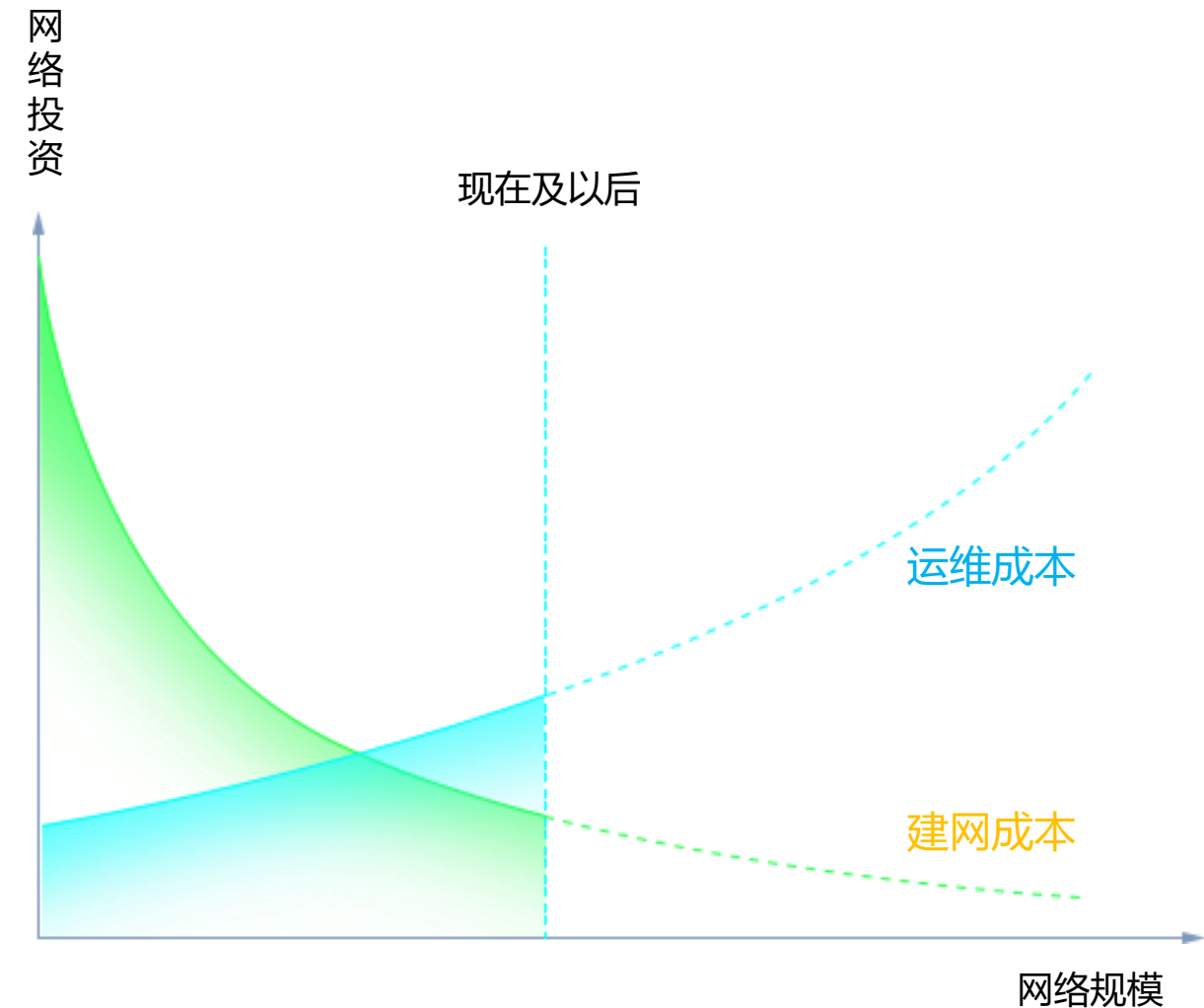
案例介绍







桌面终端成为电子病历和医院人员交互的重要载体和桥梁



### 新接入终端数量多

随着智慧医院评价、电子病历评价、互联互通评价等医院的桌面终端数量会越来越多；



### 业务增多变复杂

超过40%的医疗客户感受到了业务量增大、业务种类变多等变化，希望寻求更好体验来应对业务变化的挑战和机遇。



### 运营花费成本高

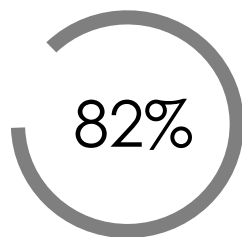
在运行网络的总成本中，硬件购买仅占到大约20%，而运营成本可占到50%或是更多。



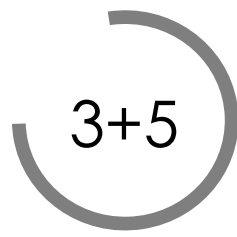
### 未知安全威胁日益频发

根据安全调查，有80%的安全漏洞出现在边界以内。这是传统边界安全防火墙无法防范的威胁。

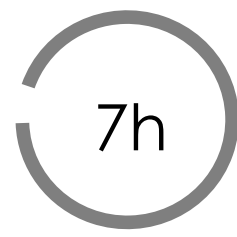




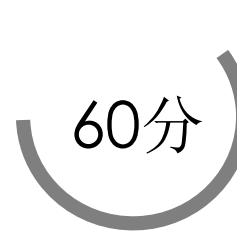
满意度调查



维护人员



日均工作时长



平均故障处理

工作站等应用安装

硬件故障处理久

业务系统配置修改

内网终端感染病毒

Windows故障

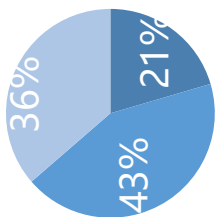
电脑外设接口管理



**PC+桌管无法解决操作系统层以下的故障**  
**特别是勒索病毒等对大规模PC的影响**

## 医疗终端操作系统调研

■ 纯XP ■ 有使用XP ■ WIN7或其它



### 微软宣布停止支持官方论坛Win7分版： 加速淘汰步伐

驱动之家  
百家号 | 06-11 14:54

目前，Windows 7已经结束主流支持，进入扩展/外延支持序列，也就是微软不会发布功能更新（即Service Pack），而仅仅只会有安全补丁，官方公布的截至时间是2020年1月。

## Window XP的不再更新：从第7代开始，Intel的CPU可能全面进入Win10时代

牵手一起梦 · 2017年08月25日 15:46 · 3915次阅读



当年在Skylake处理器发售的时候，微软曾经宣布过Win10将会是唯一一个得到该处理器支持的操作系统。当然微软这种作死的说法激怒了非常多的Windows7和Windows 8.1用户，大家都认为这是微软在强迫他们尽快的升级成最新的使用Windows10系统。随后微软因为压力等原因，表示老系统也将会得到这些处理器的支持，直到其生命周期结束。

去年，微软已经全部停止了对Window XP的更新，这也就意味着XP时代的彻底结束。对于中国来说这一消息还是值得惋惜的，特别是针对现在依旧使用着XP系统的公司来说，或许



## 新PC不支持XP和Win7，只支持Win10

## 医院的系统需要重新适配Win10 开发投入大

## 适配Win10后的稳定性还有待验证，风险较大



## 院领导：

- 简化IT维护成本
- 系统稳定、业务快速恢复
- 资产集中监控
- 节约能耗



## 业务科室：

- 易操作
- 外设的兼容
- 简化的数据备份
- 系统永不损坏



## 信息科：

- 统一管理集中配置
- 可信任的安全准入
- 远程协助
- 自动化运维



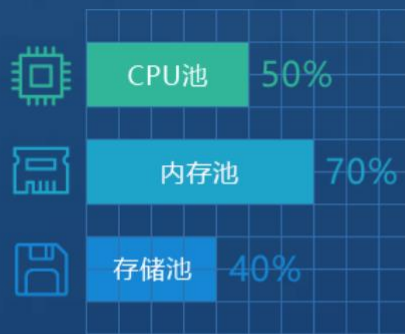
## VDI模式

数据不落地/动态性能分配

桌面漫游，随处办公



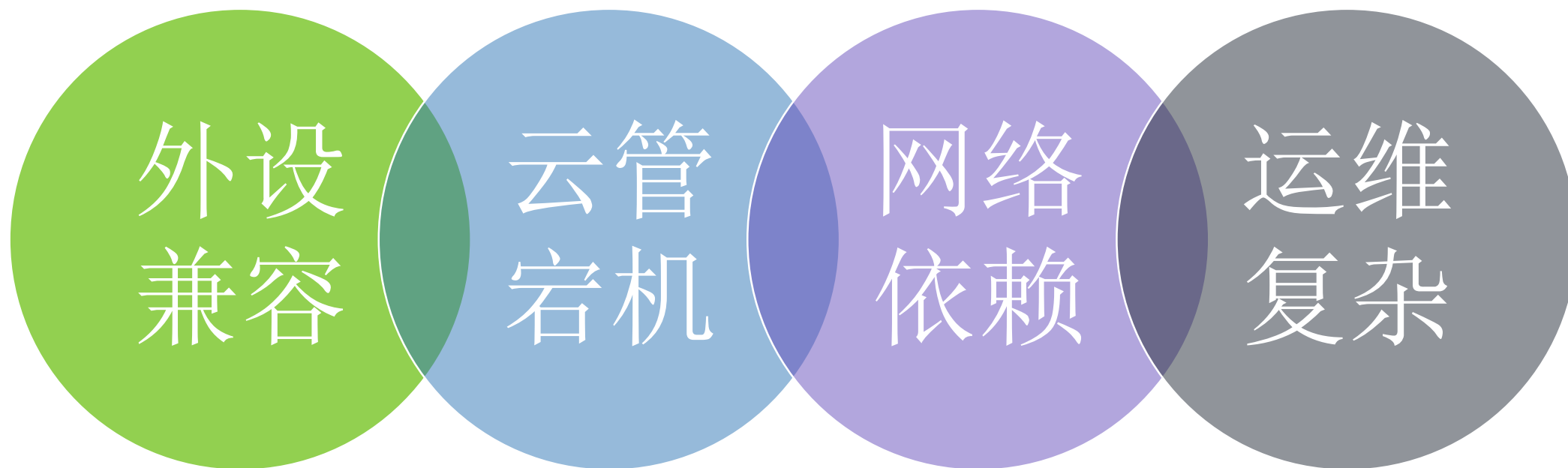
管理端配置



资源池按需配置



终端远程访问



因此给医疗客户带来了极大的不安全感;

## Network Business Artificial Intelligence 网络业务人工智能

### 智慧医院 智能网络

#### • 事前

##### ◆ 主动控制

边缘智能管理，做好安全访问控制的同时，做到极简易用，提升管理便捷性，通过提前干预，主动控制来提升反脆弱性

#### • 事中

##### ◆ 及时定位

发现网络中存在网络故障或者非法终端接入，以及环路问题，能及时定位问题和故障，主动控制和告警

#### • 事后

##### ◆ 快速恢复

设备零配置上线，环路自愈，快速恢复网络业务，提升医院信息化管理效率，提升医院的就医体验

稳定

安全

快速

简单

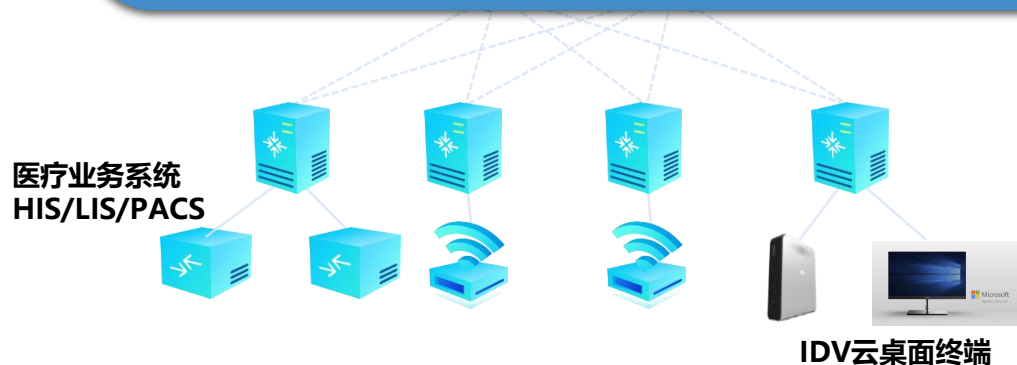


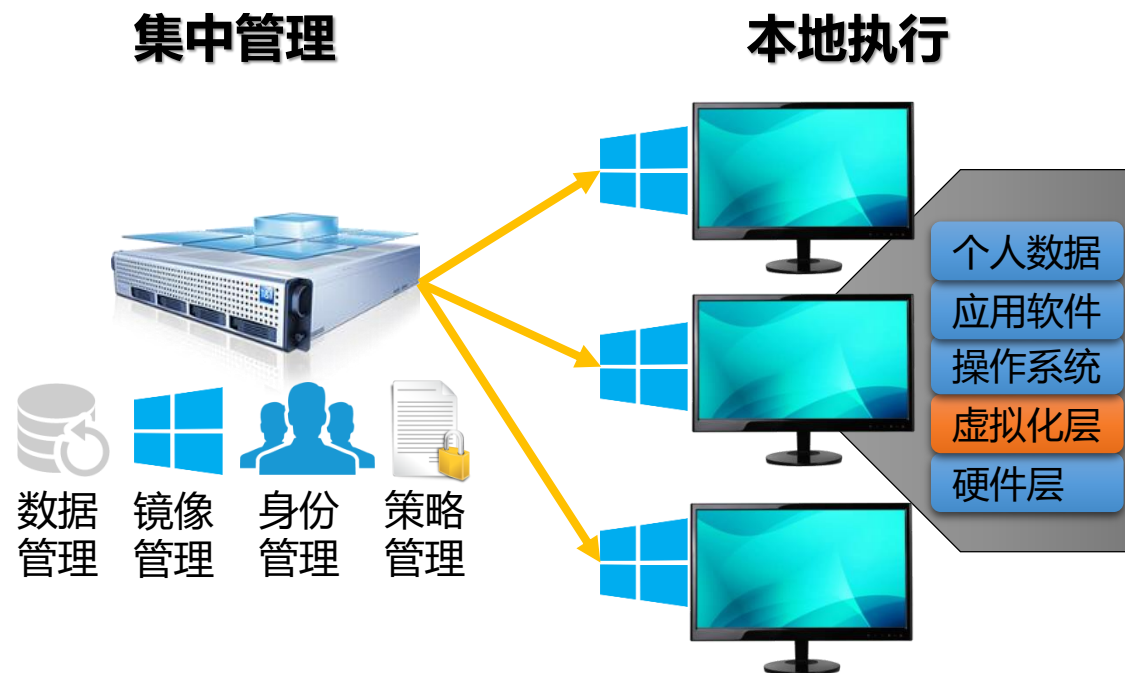


- 支持服务器离线使用、支持业务快速恢复、兼容

网络+终端双维度给医院云桌面提供安全防护；

堵风险交换机接口；





**IDV** 智能桌面虚拟化概念由Intel提出，通过支持本地虚拟化的软件+终端，实现了集中管理，分布式计算的效果。

**IDV架构采用本地虚拟化技术，虚拟机运行在本地运行，解决了VDI存在的集中故障风险**

## 全新ID元素

- ✓ 枪灰色金属喷漆，视觉更具质感
- ✓ 200\*200\*60mm 尺寸，外观更紧凑
- ✓ 无需支架，卧立两放

## 高性能平台

- ✓ 八代Coffee lake平台，主频高达3.7G，CPU性能提升166%，满足业务运行需求
- ✓ 8个USB口，方便连接更多外设

## 方便未来扩容

- ✓ 内置内存插槽，方便扩展内存
- ✓ 内置SATA硬盘插槽，方便扩展硬盘

## 提高管理效率

- ✓ 提供CT5200/CT5300两种规格，面对主流及低价用户选择
- ✓ CT6000系列一体机更高颜值



新一代IDV CT5000系列

**低主频CPU影响HIS系统运行**  
**3.7G主频保证业务软件运行顺畅**  
**8个USB口保证外设连接无忧**



人性化艺术感设计

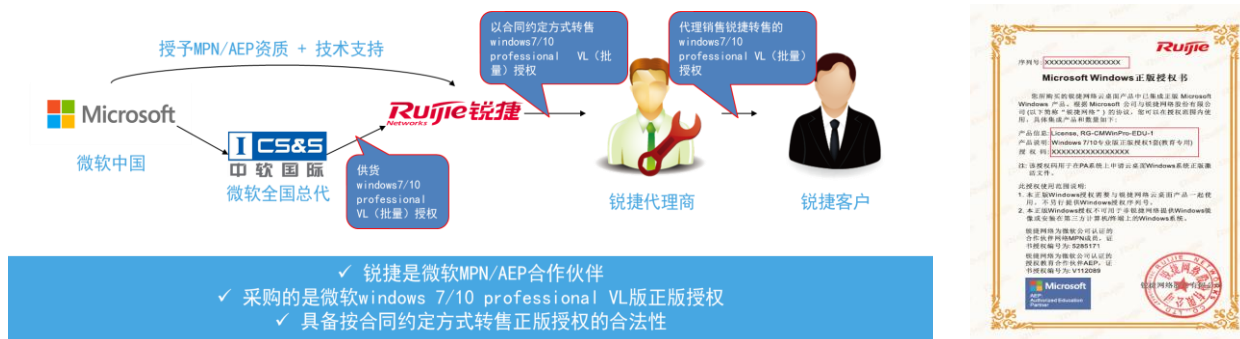


超高性能提升

## 兼容主流操作系统（XP、win7）



## 正版授权、放心使用



## 云化的打印模式，快速恢复



## 打包奇安信安全软件形成黄金镜像提高可靠性和快速部署



运维简单



中国移动

移动ONC

终端准入审批

Q 搜索MAC或IP

终端MAC	请求IP
f0:00:02:b1:a9:6c	10.105.1.226
f0:00:02:b1:a9:7b	10.105.1.241
f0:00:02:b1:a8:7c	10.105.0.242
f0:00:02:b1:a9:2f	10.105.1.165
f0:00:02:b1:a8:8b	10.105.1.1
f0:00:02:b1:a9:3e	10.105.1.180
f0:00:02:b1:a9:4d	10.105.1.195
f0:00:02:b1:a9:5c	10.105.1.210
f0:00:02:b1:a8:46	10.105.0.188
f0:00:02:b1:a8:59	10.105.0.207

中国移动

移动ONC

终端准入审批

终端(MAC) f0:33:02:b0:a8:6a

请求接入到 多承载业务网/大容量管控

申请IP地址为 33.1.1.222

IP冲突或ARP主机欺骗

终端名称

终端厂商

接入位置 192.168.184.26[Ag12]

端口 Ag12

Vlan 4000

首次请求时间 2018/04/25 09:13:49

最近请求时间 2018/04/25 14:11:41

同意

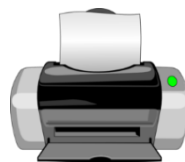
拒绝并加入黑名单

暂不处理

- 支持丰富的统计信息：终端IP、主机名、位置、品牌、状态、上线时间等，辅助资产管理
- 支持基于业务子网（VLAN）开启认证，可以和桌管配合形成最简单、最安全的准入方案



## 外设类型



打印机



扫描枪



读卡器



USB存储



4G网卡

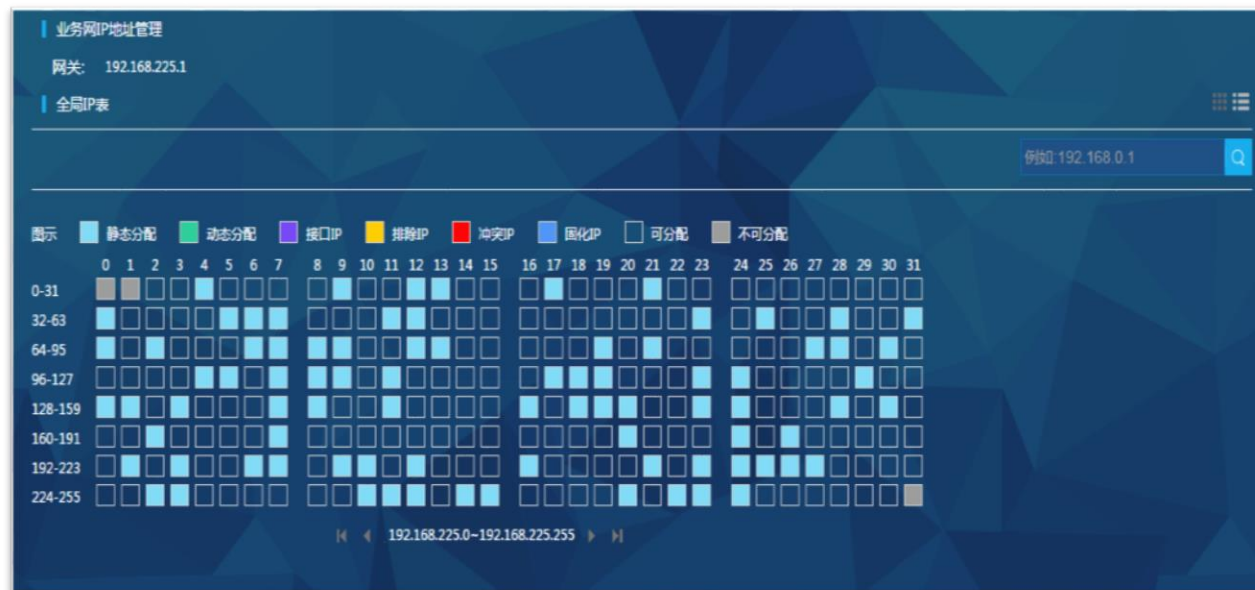
## 是否启用



管理员为不同用户/终端组制定不同的**外设策略**  
外设策略**跟随用户**，在不同终端上受同样的策略限制

## 终端准入日志信息

<input type="checkbox"/>	终端名称	IP地址	MAC地址	VLAN	接入位置	原因	厂商	创建时间	更新时间	操作
<input type="checkbox"/>		192.168.195.241	00:8c:fa:ed:95:d1	195	192.168.195.4[Gi0/17]	IP冲突	INVENTEC Corp...	2018-03-19 16:47:19	2018-03-19 17:24:30	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>		192.168.195.43	00:21:cc:72:78:88	195	192.168.195.4[Gi0/17]	IP冲突	Flextronics Ltd.	2018-03-19 15:23:03	2018-03-19 15:56:44	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>



IP地址可视化分配管理，  
像电影院选座一样直观便捷



管理维护人员



终端&用户管理



镜像管理



一键系统恢复



外设控制策略



IP可视化**管理**



云主机高可用



院领导



桌面用户



桌面漫游



高性能终端



远程桌面访问



(有线、无线)  
外设全兼容



支持离线运行



桌面无感准入



人力成本



固定资产管理



绿色节能



业务快速恢复





### ◆ 项目背景

中国科学技术大学附属第一医院（南区）隶属于中国科学技术大学，是一所集医疗、教学、科研、康复和急救为一体的省级三甲医院。随着医院信息化进程的深入，其桌面工作站呈现出爆发式增长。医护人员等对桌面工作站的可靠性、适用性提出更高的要求，IT运维人员面临巨大压力。

### ◆ 应用场景：VDI&IDV融合版解决方案

### ◆ 业务系统与外设：条码机、扫码枪、打印机、USB-KEY、摄像头、指纹仪等

### ◆ 问题与痛点

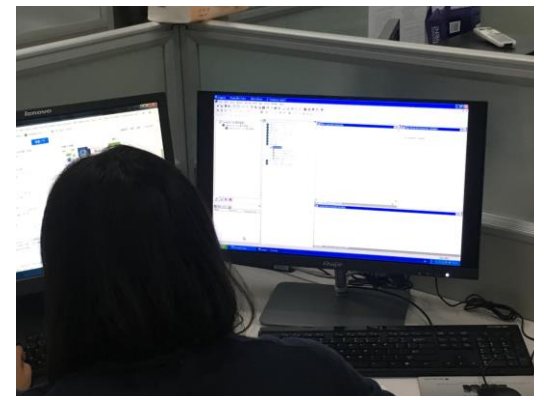
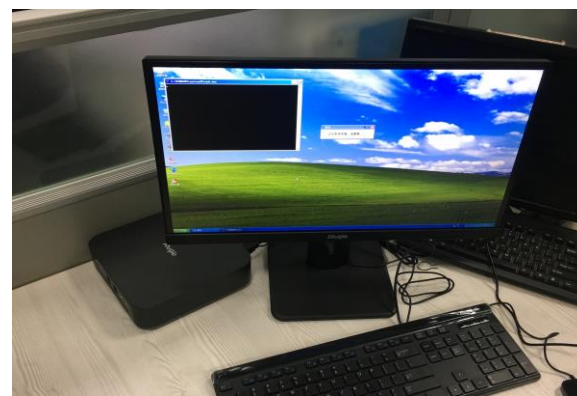
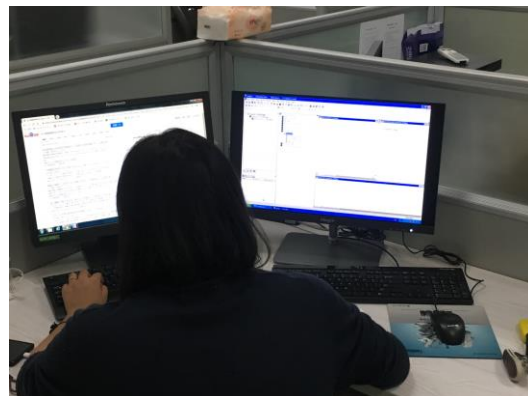
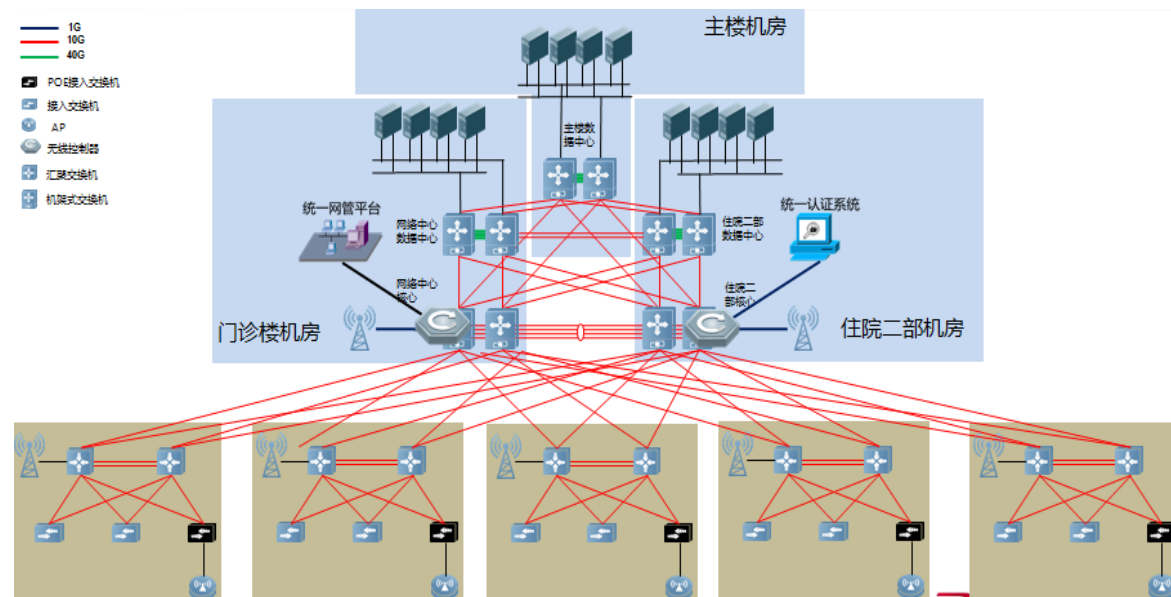
- 1) PC时常发生软件系统崩溃、配件损坏（硬盘、内存）等故障，随着PC日益增多，运维难度逐年增加。
- 2) 尝试过思杰VDI云桌面，维护难、离线不可用，业务恢复不及时

### ◆ 解决方案及价值：在医护工作站、医生办公室、分诊台、手推车、培训阅览室等全场景下部署了1100多台IDV智能桌面虚拟化终端和VDI虚拟桌面基础架构终端。

- 1) 桌面和资源的集中化，既可以减少设备硬件故障率，又能够显著提升IT运维效率。
- 2) IDV终端离线可用，释放了网络带宽，也保障了前端业务科室良好的使用体验。

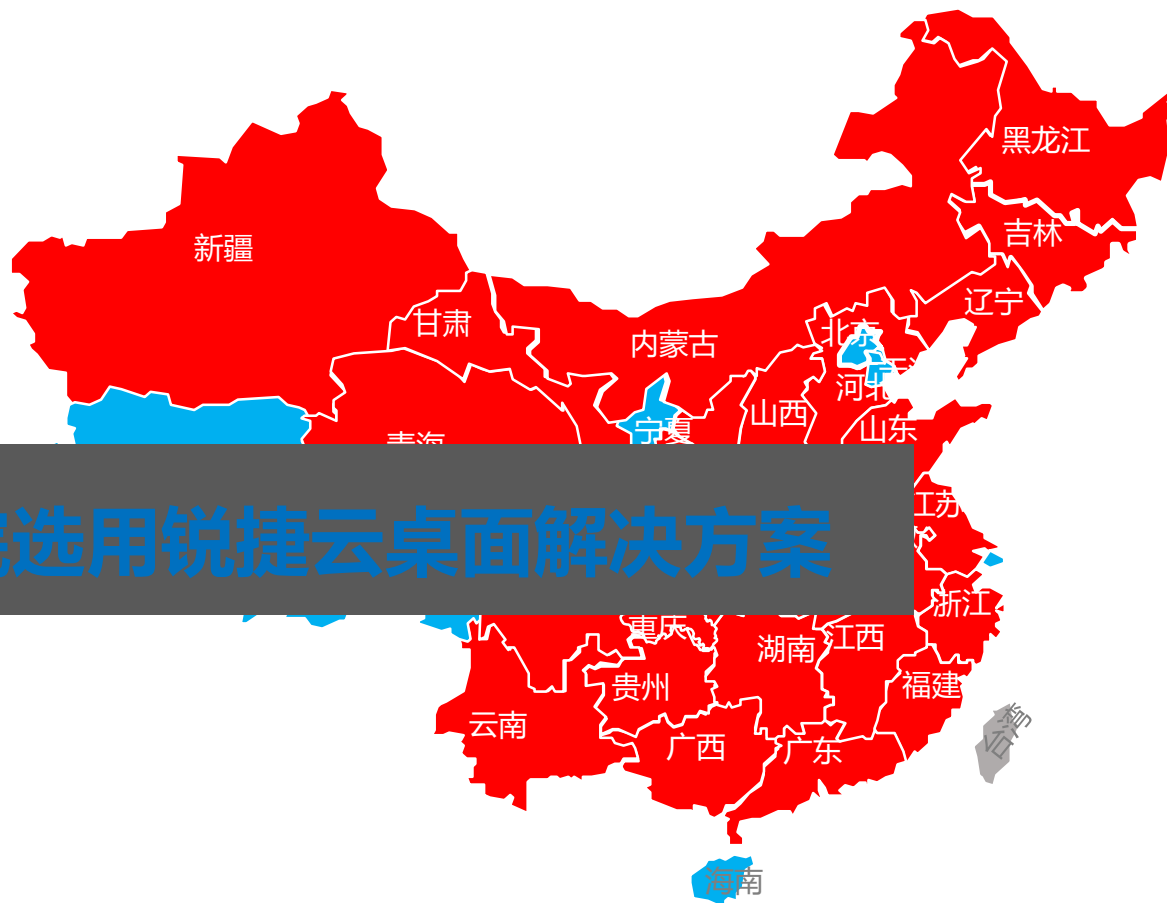







医院名称	医院级别
中国科技大学第一附属医院南区	百强
哈尔滨医科大学附属肿瘤医院	百强
宿州市立医院	三甲
青海大学附属医院	三甲
安徽医科大学第四附属医院	三甲
吉林省白城市人民医院	二甲
云南省景洪人民医院	三甲
内蒙古兴安盟科右中旗中蒙医院	三级
苏州口腔医院	三甲
重庆市人民医院	
兰州市第三人民	
四川达州大竹县	
南方医科大学 (	
石家庄中医院	三甲
广州中医医结合医院	三甲
鞍山中心医院	三甲
四川广安市前锋区人民医院	三级
宣城市人民医院	三甲
江西省妇幼保健医院高新分院	三甲
皖南医学院附属弋矶山医院	三甲
江苏省如皋人民医院	二甲
河北省中医院	三甲
山西省运城市中心医院	三甲
新疆克州人民医院	三甲
浙江省台州医院	三甲

近百家三甲医院选用锐捷云桌面解决方案





The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE