C3安全峰会
CYBER | CLOUD | COMMUNICATION

医疗大数据时代网络信息安全概览

汪 鹏

陆军军医大学西南医院 2017.7.7

信息安全风险时有发生，信息安全管理形势严峻

C3安全峰会
CYBER | CLOUD | COMMUNICATION

近几年，随着我国医疗大数据战略的实施，以及互联网医疗的广泛开展，诸多医疗机构的内部业务系统正在逐步向外开放，数据利用的需求也在不断增长。然而，这些过程中，网络信息安全问题变得日益突出，已成为医疗数据共享、挖掘和深度利用的绊脚石。

- 物联网
- 移动互联网

被迫开放的医院网络信息安全体系

- 大数据
- 云计算

目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION

信息安全总体态势

C3安全峰会
CYBER | CLOUD | COMMUNICATION

2016年，医疗保健行业泄漏的数据总量（超过1594万条）比其他任何行业都要多得多，比例高达43.6%。

商业行业的违规行为总量虽是最多为495，但其数据泄漏总量却远低于医疗保健行业，只有567万条左右。

2016年数据泄漏报告中违规行为和数据泄漏总量最少的部门为银行 / 信贷 / 金融行业，只有52例违规行为，7万多条数据泄漏。

数据来源：Privacy Rights Clearinghouse

《2016年数据泄露报告》

2016 Data Breach Category Summary

How is this report produced? What are the rules? See below for details. Report Date: 1/18/2017

Totals for Category:	Banking/Credit/Financial	# of Breaches: 52	# of Records:	72,262
		% of Breaches: 4.8%	%of Records:	0.2%
Totals for Category:	Business	# of Breaches: 495	# of Records:	5,669,711
		% of Breaches: 45.3	%of Records:	15.5%
Totals for Category:	Educational	# of Breaches: 98	# of Records:	1,048,342
		% of Breaches: 9.0%	%of Records:	2.9%
Totals for Category:	Government/Military	# of Breaches: 72	# of Records:	13,869,571
		% of Breaches: 6.6%	%of Records:	37.9%
Totals for Category:	Medical/Healthcare	# of Breaches: 376	# of Records:	15,942,053
		% of Breaches: 34.4	%of Records:	43.6%
Totals for All Categories:		# of Breaches: 1093	# of Records:	36,601,939
		% of Breaches: 100.0	%of Records:	100.0%

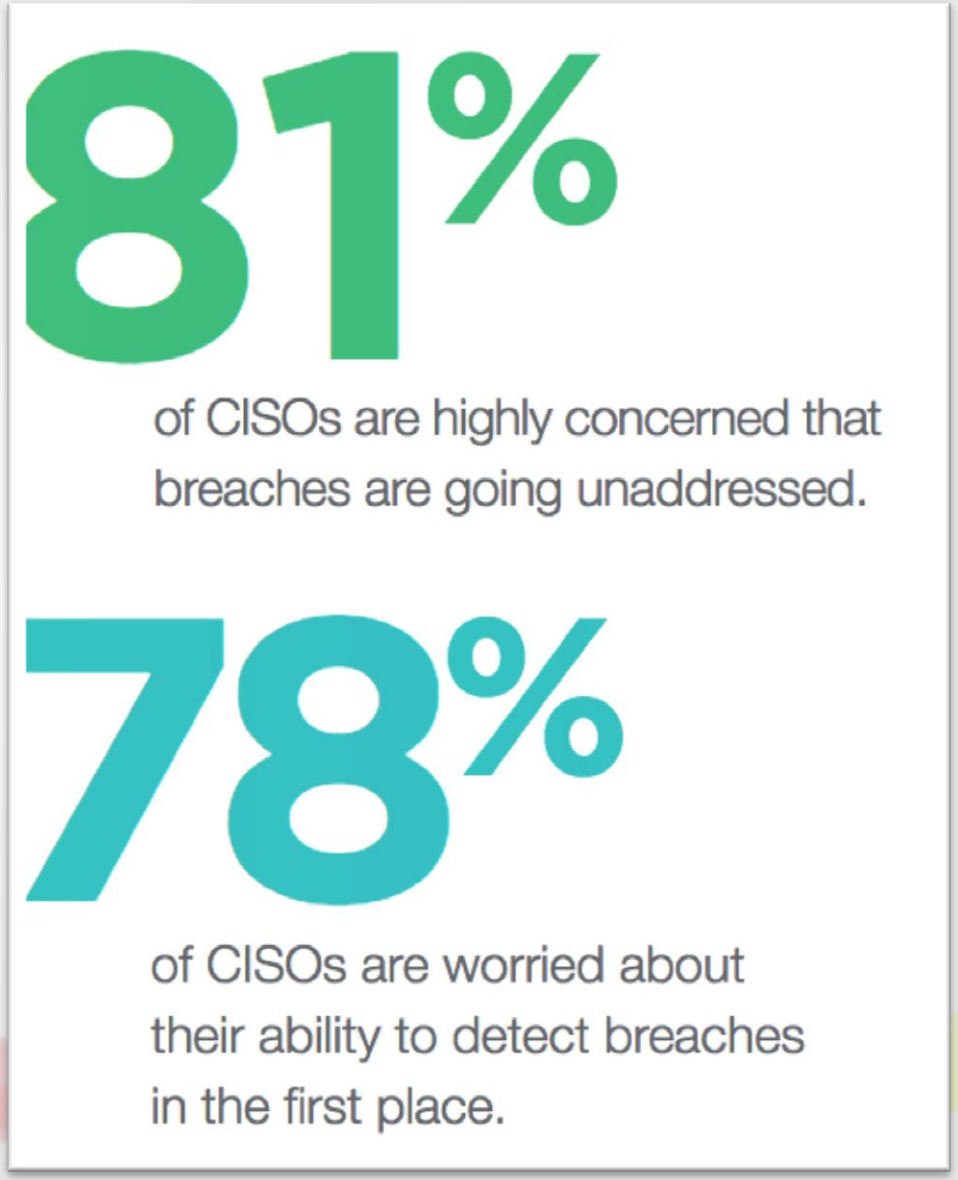
信息安全总体态势

C3安全峰会
CYBER | CLOUD | COMMUNICATION

《全球CISO研究报告》调查发现，超过80%的首席信息安全官对其组织检测到且尚未解决的违规行为表示高度关注。尽管有这样的担忧，但仍有56%的CISO认为他们的公司能够“有效地”阻止安全漏洞，另有19%的受访组织表示他们能够“非常有效地”阻止安全漏洞。

81%的CISO高度关注尚未解决的违规行为；78%的CISO对自己能否在第一时间检测出安全漏洞的能力表示担忧。

数据来源：《全球CISO研究报告》



国外医疗信息安全事件

2016年，英国NHS就因数据安全问题停止使用care data健康医疗大数据平台

2016年，洛杉矶好莱坞长老会医疗中心遭勒索软件攻击；

2016年，德国慕尼黑一家医院遭黑客攻击，病人监护仪和输药管系统遭入侵致系统瘫痪；

2017年，英国国家医疗服务体系（NHS）的至少16家医院和相关机构遭到了攻击

我国医疗信息安全事件

C3安全峰会
CYBER | CLOUD | COMMUNICATION

2016年，某医院因后台安全问题致使患者信息泄露；

2016年，白桦林全国联盟共接到来自30个省区市的275例艾滋病感染者因个人信息发生泄露而导致的诈骗；

2016年，某妇幼保健院，内部人员通过笔记本接入内网，将医院系统上存的母婴的信息窃取售卖；

2017年5月，我国多家医疗机构和高校遭到了勒索病毒攻击；

新时代医学大数据信息安全威胁

C3安全峰会
CYBER | CLOUD | COMMUNICATION

安全防护不到位

据美国非营利性组织身份盗用资源中心的统计数据显示，医疗健康信息系统成为黑客首要攻击目标，占漏洞总数的43.8% ；

安全意识不健全

我国相关的隐私保护等法律法规系统不完善，我国居民和相关机构对数据安全意识淡薄，并且各方面的基础建设也不足；

新技术新挑战

随着云存储、云计算、云服务、虚拟化等技术的广泛应用，过去的安全防护方案已成为制约数据安全的瓶颈；

国外医疗信息化安全战略规划

- 美国通过《2002年联邦信息安全管理法》
- 2010年美国颁布《2010年网络安全加强法案》

- 欧盟《欧盟数据保护法》
- 2013年颁布《国家网络安全策略—为加强网络空间安全的国家努力设定线路》

- 2012年英国成立数据战略委员会并颁布《开发数据白皮书》
- 2009年，英国成立“网络安全与信息保障办公室”
- 2011年11月，英国公布新的《网络安全战略》

我国医疗信息化安全战略规划

C3安全峰会
CYBER | CLOUD | COMMUNICATION

国内医疗大数据应用和安全保障起步稍晚，但近几年出现了蓬勃发展的态势。

2015年《国务院关于印发促进大数据发展行动纲要的通知》

助力完善法规制度和标准体系；
推进大数据产业标准体系建设；

鼓励开发网络数据安全保护和利用技术；

2016年《中华人民共和国网络安全法》

2016年，国家互联网信息办公室发布《国家网络空间安全战略》

建立大数据安全管理制度；
支持大数据信息技术创新和应用要求；

加强法规和标准体系的建设；
推进网络可信体系建设；
加强健康医疗大数据安全保障；

2016年国务院办公厅《关于促进和规范健康医疗大数据应用发展的指导意见》

我国医疗信息化安全战略规划

C3安全峰会
CYBER | CLOUD | COMMUNICATION

2014年8月26日，中央网络安全和信息化领导小组正式成立，习近平任组长

体现我国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展的决心。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

网络安全上升到国家安全战略

虚拟传播突破传统国界线

最高层统筹更加重视顶层设计

目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 专业技术队伍
- 巡查分析制度
- 等级保护与测评

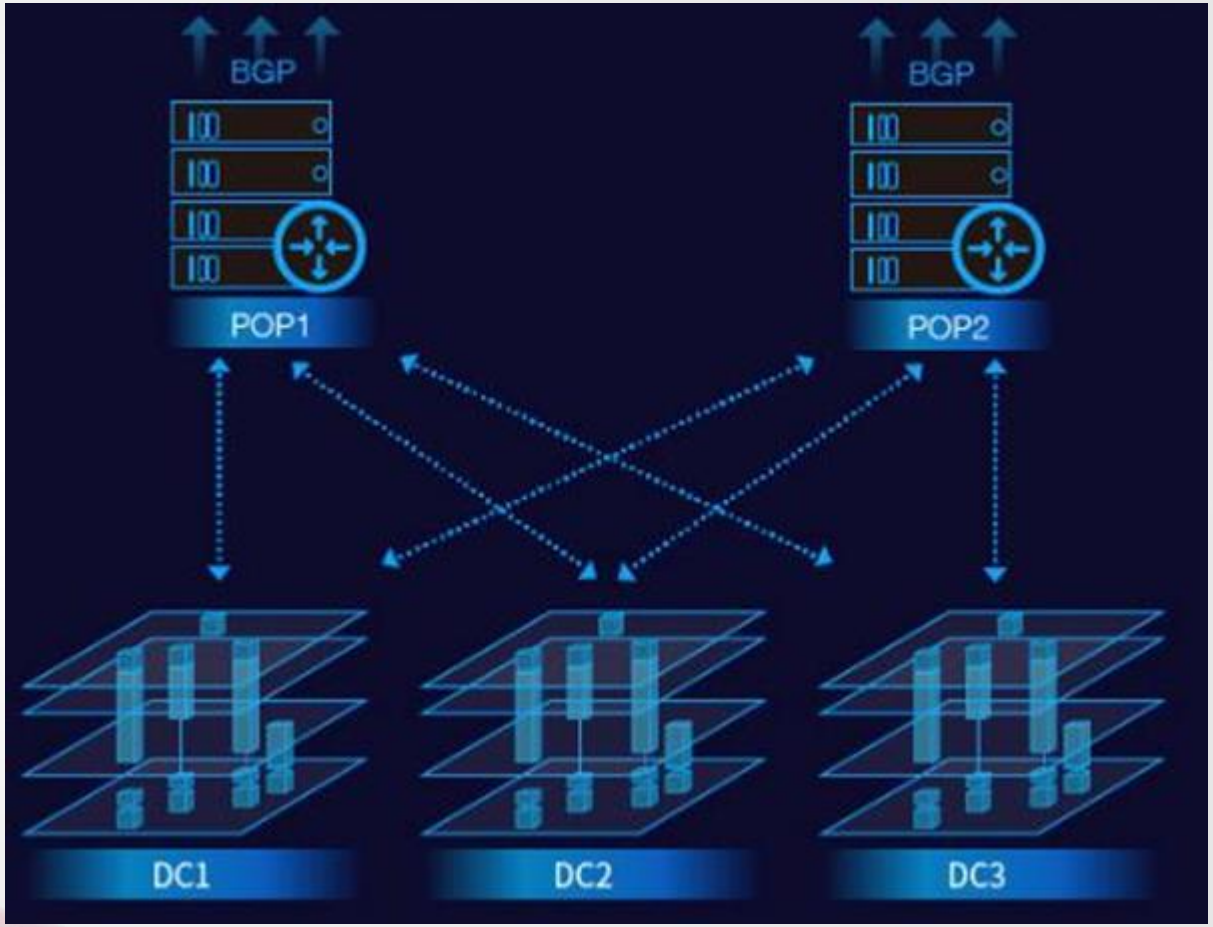
- 基础网络链路
- 机房设施设备
- 内外网防护交互
- 备份容灾体系

- 软件体系架构
- 数据管理维护
- 移动网络应用

基础网络链路安全

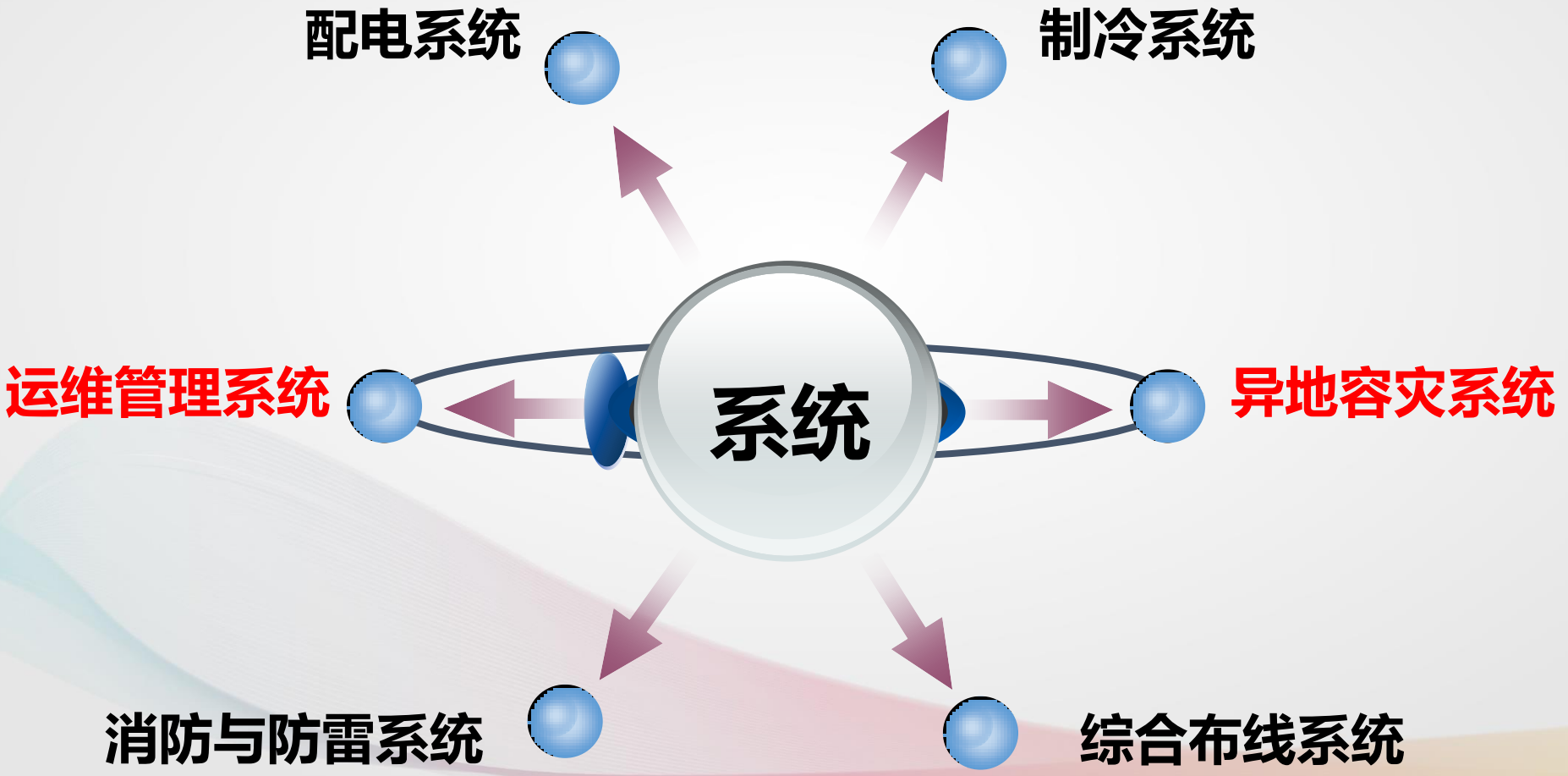
C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 核心网络设备**双机热备/双活**；
- 骨干**链路冗余**；
- 划分**虚拟局域网**；
- 网络**终端准入控制**；
- 网络链路与流量**可视化监控**；



机房设施设备安全

中心机房设计原则—标准化、安全性、扩展性、前瞻性



内外网防护与交互安全

建立实现内外网数据交互与应用的网络化平台，拓展对医院对外信息化服务，完善医院数字化建设起到积极作用。

安全设备

综合运用防火墙、网闸、入侵防御系统、堡垒机等网络安全设备，保障医院内网不受外部网络攻击；

专网

尽量使用专网完成如医保、区域医疗等系统数据的交互，减小网络攻击几率；

专用平台

综合建立内外网交换的数据交换平台，通过该平台完成内外网数据交互，保障内网数据的安全；

软件体系架构安全

C3安全峰会
CYBER | CLOUD | COMMUNICATION

应用软件体系架构的安全是一切应用安全的基础，必须高度重视，做好顶层设计。

软件架构安全设计

- 糟糕的架构设计有可能暴露出应用程序的许多安全漏洞。
- 最好的办法是在设计阶段就执行架构检查，避免在部署后再实施安全控制将花费高昂的成本和代价。

1

2

3

总体架构设计与文档：

- 开发语言、操作系统、三层架构、B/S与C/S、会话管理、配置与参数操作、例外管理等
- 架构图、网络图、安装手册、操作手册等

身份认证、授权与加密：

- 根据需求确定口令、CA、生物特征等认证方式及通讯协议
- 严格控制不同角色的授权，并考虑审计和日志
- 为保障存储数据的安全，或为保护在不安全的通道中数据传输的安全性，应考虑使用加密技术

软件系统间的数据共享与互操作：

- 越来越多的软件系统间的数据交互导致系统架构越来越复杂
- 必须适时考虑标准化、平台化的数据共享与互操作方式

数据管理维护安全

C3安全峰会
CYBER | CLOUD | COMMUNICATION

数据的延续性、准确性和高可用性是保证医院业务的正常运行的前提，也是做好医疗大数据应用的关键。

物理介质保障

- RAID、Dataguard、RAC、异地双活与备份;
- 构建虚拟化运行体系，从物理介质上增强冗余性;

管理机制保障

- 采用专业容灾备份恢复系统，定期进行检测验证；
- 不同部门用户的授权，限制用户对敏感数据的访问权限和读取功能;
- 部署审计系统，监控和审计用户对数据库中的操作，精确到SQL操作语句一级，并对违规行为进行记录、报警;

移动网络应用安全

移动医护、移动办公、医疗物联网等应用的逐渐普及，给传统有线网络带来新的挑战。应从网络访问控制、数据保密与完整性保护、抗干扰等方面加强管控。

医疗数据应用管理

医疗大数据技术的应用，带来了广泛的数据集中、高度的数据共享，快速的数据访问，将过去的许多不可能变为可能。但与此同时，也带来了前所未有的安全威胁和管理难度。

关键信息脱敏　　信息保密协定　　患者知情许可

基于Hadoop大数据平台的全院临床资料搜索，3秒内结果展现。

全jun电子病历共享

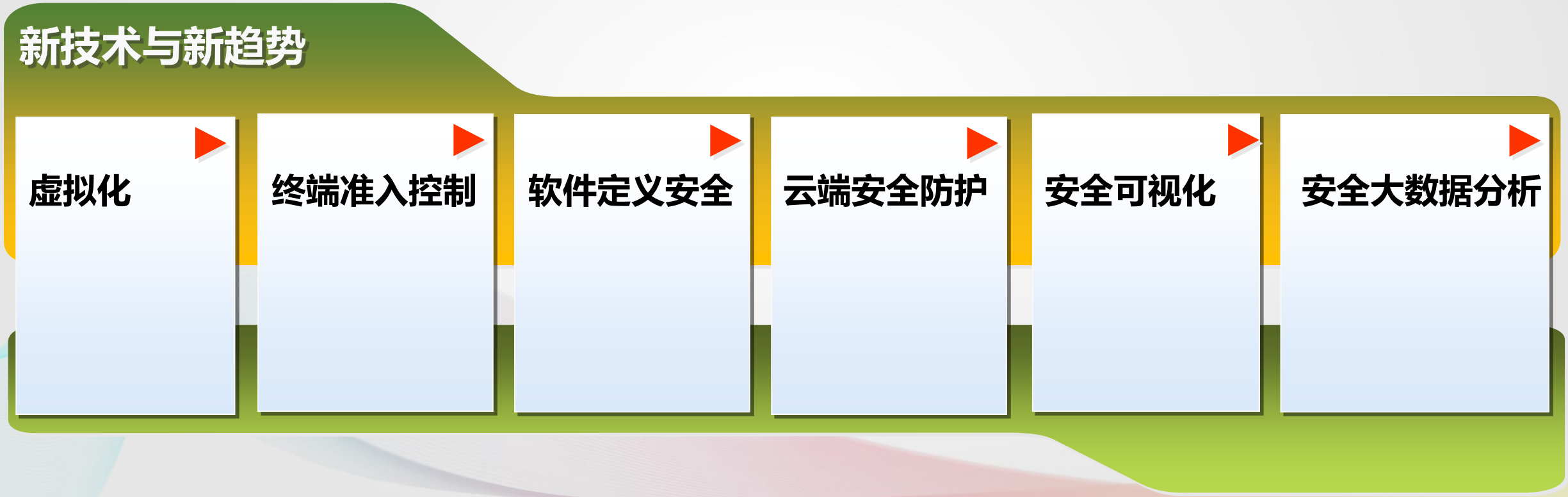
目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION

信息安全新技术与新趋势

C3安全峰会
CYBER | CLOUD | COMMUNICATION

最新的信息安全技术带来新的信息安全管理思路和方法，使得新时期的信息安全管理变得更加便捷、强大、智能。



虚拟化

C3安全峰会
CYBER | CLOUD | COMMUNICATION

虚拟化的实施应用是保障硬件资源冗余的有效举措，可以显著降低应用系统对硬件资源高可用的依赖性。

服务器虚拟化

更灵活迅速的部署、局部损坏不再可怕、灾难恢复能力更强、降低供电与制冷压力。

存储虚拟化

新旧资源整合利用、方便的数据复制快照与迁移、透明的存储扩展、自动精简配置。

网络虚拟化

核心网络资源的冗余、负载均衡提高效率、异地化多核心部署

桌面虚拟化

数据存放安全可靠、部署维护灵活便利、提高资源利用率、多类型应用终端

终端准入控制

C3安全峰会
CYBER | CLOUD | COMMUNICATION

实施全面有效的终端准入控制是构建安全防护堡垒的第一道关卡。

01

交换机上绑定MAC+端口或IP+端口模式严格控制非法用户接入

该方法对于那些拥有终端电脑数量比较多的大型医院来说，
技术人员实施起来比较麻烦，后期维护也很繁琐；

02

借助第三方软件终端准入控制系统

- 通过作为DHCP服务器模式或终端电脑安装客户端模式对有线或无线终端进行接入认证控制，防止非法用户接入内网窃取医院数据；
- 实施简洁快速，维护方便，可以为医院客户端的管控提供有效支持；

终端准入成为必需

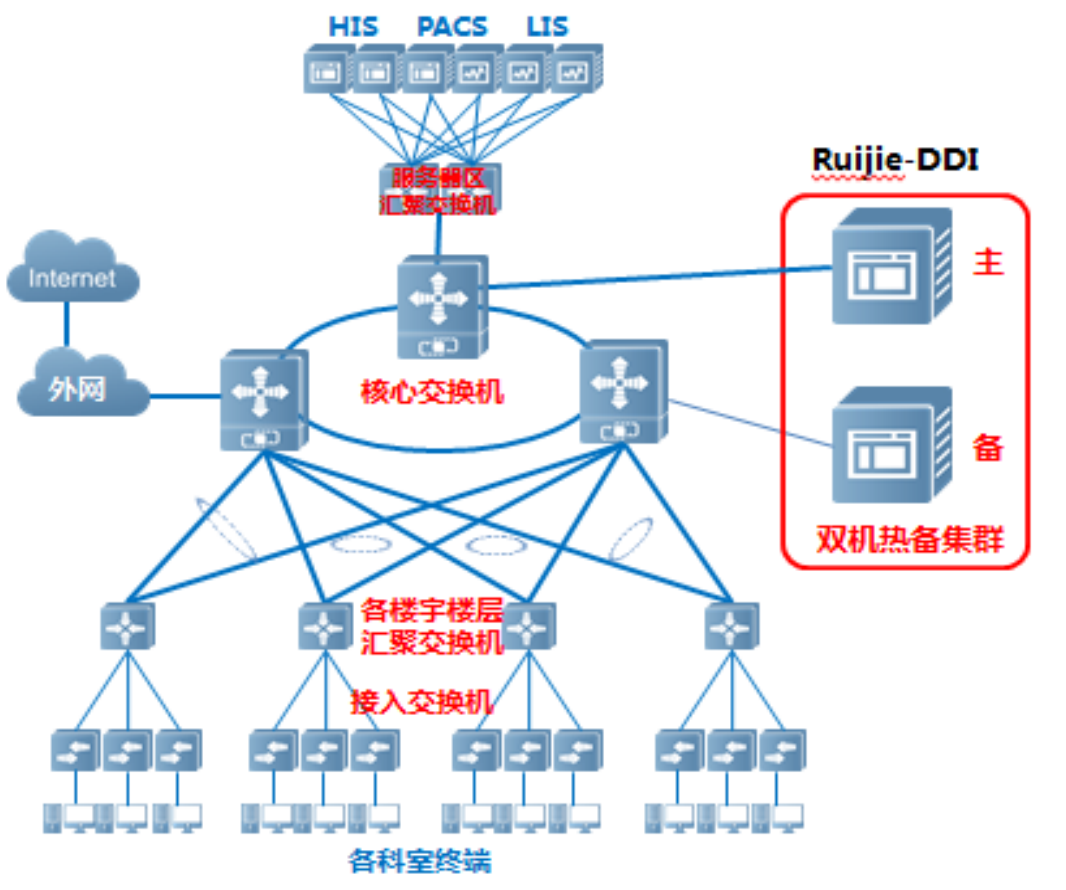
“等级保护基本要求”->“网络安全”->“边界完整性检查”

应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

内网无线是安全隐患，需要加强移动医疗终端接入管理

无线开放性特征，要求所有终端必须做认证接入。

通过一些第三方管理系统可以很方便的做到终端准入的可视化管理。



Step 1 → Step 2 → Step 3

终端动态获取地址

终端通过DHCP方式获取IP地址

DDI显示终端上线

RG-DDI能够检测到终端接入的交换机地址、VLAN、端口及终端MAC、主机名等信息

DDI一键授权终端接入

一键授权允许或者禁止终端接入，将终端MAC与IP地址或主机名或接入交换机绑定

通过CA电子签名技术进行访问控制也是保证医疗数据安全的有效举措。

每个使用公开密钥的用户发放一个数字证书

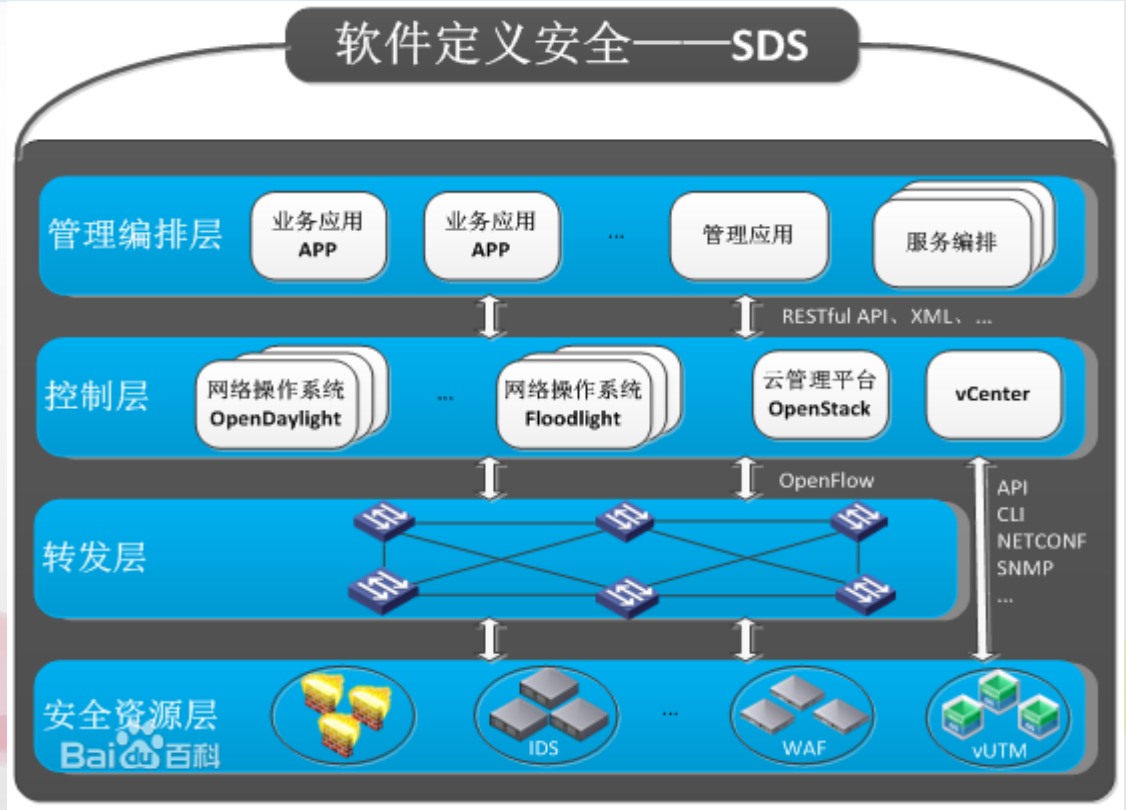
CA机构的数字签名使得攻击者不能伪造和篡改证书

软件定义安全SDS

C3安全峰会
CYBER | CLOUD | COMMUNICATION

软件定义安全（Software Defined Security，SDS）是从软件定义网络引申而来，原理是将物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，从底层构建安全资源池，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现一种灵活的安全防护。

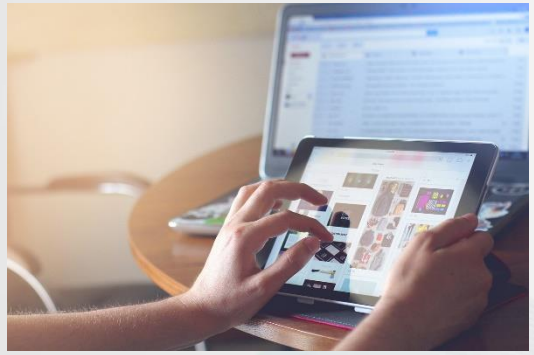
传统安全部署	SDS
• 安全设备部署过程繁复 • 不能区别处理流经的流量 • 安全防护范围僵化 • 安全设备成为单一故障点	• 安全功能部署灵活简单 • 细粒度区分流量 • 安全防护范围动态调整 • 维护网络高可靠性 • 安全功能易于创新



云端安全防护

C3安全峰会
CYBER | CLOUD | COMMUNICATION

随着云计算技术的逐步成熟，一些医院正选择将部分业务系统部署在云端，如影像云、健康管理云等。有的甚至全部放在云端，院内无数据中心。与传统IT解决方案相比云计算可能面临不同的风险，云端安全问题已成为医疗云发展的关键。



云资源访问控制/身份令牌

系统密钥/加密技术

数据隐私保护

安全大数据分析（Big Data Security Analysis，简称BDSA）

C3安全峰会 CYBER | CLOUD | COMMUNICATION

在大数据时代，网络信息安全数据也面临大数据化，如何将大数据技术应用于安全领域？

- 业务大数据的发展促使网络安全设备分析的数据包数据量急剧上升。
- 安全纵深防御使安全监测内容不断细化，合规监测、应用监测、用户行为监测、性能检测、事务监测等。
- 借助大数据安全分析技术，能够更好地解决海量安全要素信息的采集、存储和挖掘利用。

安全可视化

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 面对复杂的网络信息安全局面，需要更直观的管理与操作模式。
- 将安全态势感知与可视化技术结合，生成网络信息安全综合态势图，以多视图、多角度的方式与用户进行交互，实现对网络异常行为的可视化监测和分析。
- 可有效提高数据的综合分析能力与效率，降低误报率和漏报率。

- 数据中心运维可视化
- 信息资产监测可视化
- 安全日志分析可视化
- 网络安全决策可视化

机房关键设备可视化监控

目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION

迎接变化，拥抱新生

C3安全峰会
CYBER | CLOUD | COMMUNICATION

医院对信息化的依赖性不断增强

要求更安全的信息体系

医院信息系统越来越多的开放与交互

导致安全形势更为复杂

系列新技术、新模式的产生与应用

带来新的安全管理思路

安全管理方法同样需与时俱进

把握信息安全新趋势是关键

系统设计，分步实施

C3安全峰会
CYBER | CLOUD | COMMUNICATION

树立整体安全观

面向全局的科学设计是安全保障的基础

构筑立体防控体系

充分发挥硬件、软件和管理的联动作用

统筹规划、分步实施

从核心要素到全面管控逐步建设完善

应用驱动，安全可控

C3安全峰会
CYBER | CLOUD | COMMUNICATION

在信息安全的总体布局下

- 进行应用的设计和实施

在应用的建设发展中

- 不断完善信息安全管理策略

不可因噎废食，发展才是硬道理！

西南医院
SOUTHWEST HOSPITAL

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You