医院安全改造（轻咨询）解决方案

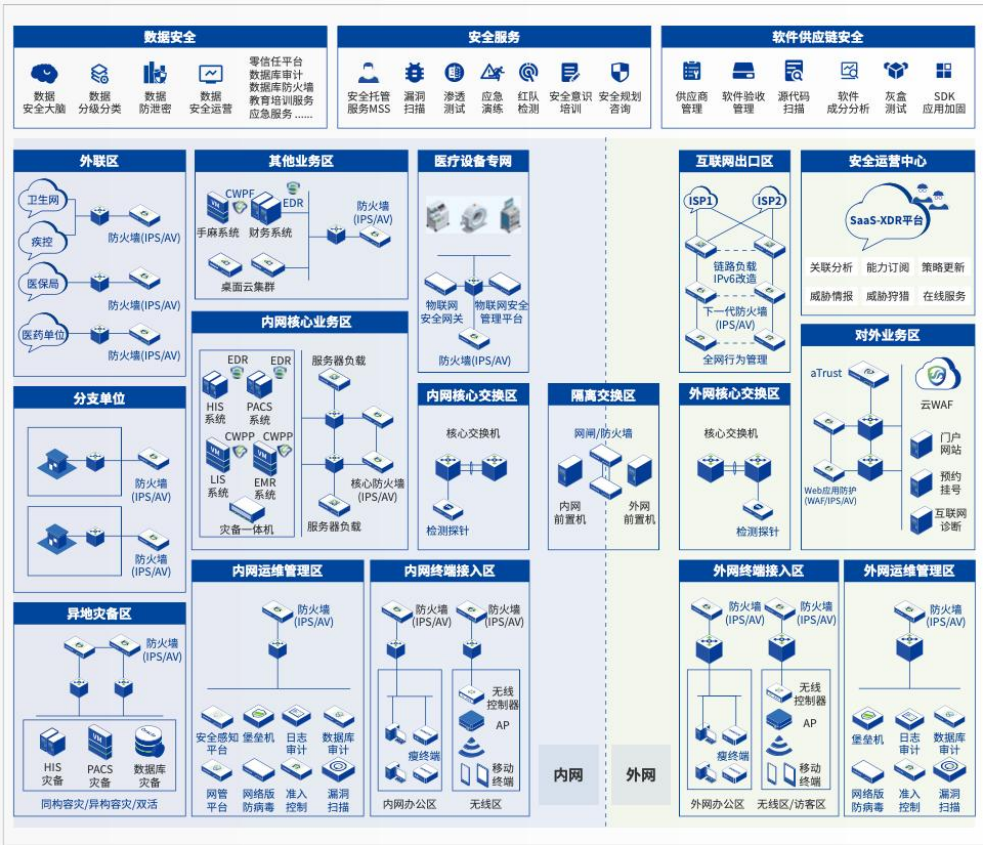
1 需求背景

2017 年国家《网络安全法》的颁布，医院掀起等保建设浪潮，很多医院开始基于合规要求的角度开始建设，但缺少了从医院整体网络架构进行考虑和建议，导致很多医院过了等保依旧出现安全事件。

现阶段医院网络安全建设主要还是“头痛医头、脚痛医脚”的建设模式，在不断的攻防之间，医院疲于应付、缺乏明确的规划。医院应当真正结合建设现状和建设方向（标准），提前做好规划应对未来的安全风险，化被动为主动。

2 深信服解决方案

结合行业主要政策及众多三甲医院实践经验，深信服以“为医院量身打造的、符合实际情况的、能落地可执行的、分年度分批建设的”为原则，设计了能够帮助医院进行差距分析并完成建设的轻咨询安全加固解决方案。



序号	重点场景	建设依据（业务+政策）	匹配内容	阶段
重点场景	边界安全加固（网络权限）	**业务：**区域边界是安全建设基础，精细化的区域隔离（核心交换机与服务器、科研服务器区、无线控制器、医联、医保、卫生局及安全运维管理区等）能有效降低终端感染后造成的扩散现象，降低安全风险， **政策：**符合《医疗卫生机构网络安全管理办法》实行分区分域管理，区域间进行安全隔离和认证，实现由外到内、从边界到核心的多重保护，以及对攻击的层层防护要求。	AF、EDR	一期
	安全运营体系建设（托管）	**业务：**以建设安全效果为目标，结合安全技术、安全工具、安全服务，搭建符合医院的网络安全运营体系，解决“看不清、看不懂、难处置”的问题，实现“早发现，早治疗”的安全目标； **政策：**符合《医疗卫生机构网络安全管理办法》鼓励三级医院探索态势感知平台建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作的要求，同时也符合三化六防中，全天候的态势感知与安全运营的要求；	SIP、安全托管服务	一、二期
	勒索病毒专项防护	**业务：**医疗行业是勒索病毒的重灾区，每年由于勒索病毒导致医院业务停摆的事件屡有发生，医疗为国家重点民生行业，为保障正常的医疗秩序，勒索病毒防护时医院安全建设的重中之重，以往安全建设大而泛，医院在真正回答最为担心的勒索病毒防护措施时，往往“心里没底”，医院目前需要精细化勒索防护及可承诺的安全效果； **政策：**《GBT22239-2019 等级保护基本要求》中提出，应采用免受恶意代码攻击的技术措施及时识别入侵和病毒行为，并将其有效阻断（在医疗行业，特指勒索病毒）	勒索病毒专项服务+理赔保险	一、二期
	医疗零信任	**业务：**医院终端网络复杂化、业务变化、攻防变化，导致安全风险剧增，同时由于医院互联网+业务的发展，网络边界模糊化、接入形式多样化、用户角色多样化，导致医院不得不开放部分边界，如何解决业务需要带来的边界敞口问题，也称为当下安全建设的主要矛盾；	aTrust、aES	一期
	终端安全相关	服务器作为承载业务的最终载体，安全建设依旧停留在等保合规的层面，导致漏洞被通报、装杀毒软件依旧中毒的问题，核心还是在于客户端对于端点安全的关注度不够，导致”安全最后一公里“没有得到妥善保障；	aES	一期、二期

3 方案优势

（1） 安全规划指引建设经验丰富

✓ 深信服参编国家卫健委统计信息中心主导的《新一代医院数据中心建设指导》、参编《医院网络安全建设指引》等

（2） 医疗行业用户经验丰富

✓ 深信服安全业务覆盖广泛，医疗行业头部医院、三级医院及区县医院覆盖率第一，积累大量用户实践经验及各地检查和政策发文解读，从而不断优化和完善深信服行业化解决方案

（3） 打造创新服务模式

✓ 目前深信服通过“云网端”架构的不同组合方式，增加安全防护的效果及性价比，打造数字化转型下的技术路线。

4 典型案例

广州医科大学肿瘤医院	昆明市儿童医院
上海市口腔医院闵行院区	中山大学附属第六医院
河北医科大学第一医院	上海交通大学医学院附属瑞金医院