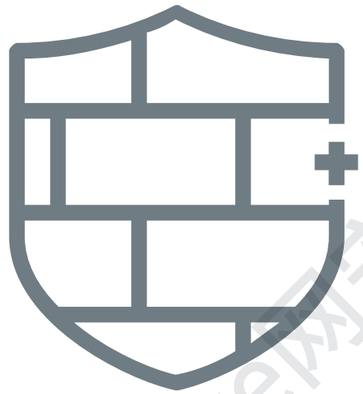


东软NetEye医疗行业网络安全白皮书

医院篇

Neusoft

东软网络安全官方微信

产品咨询热线：

400-655-6789

中国辽宁省沈阳市浑南新区新秀街2号 东软软件园
邮编：110179
电话：(86 24) 8366 7788
传真：(86 24) 2378 2700

neteye.neusoft.com

NetEye1907

CONTENTS 目录

东软NetEye
医疗行业网络安全

医疗行业政策背景

2009年3月17日中共中央国务院办公厅印发《中共中央国务院关于深化医药卫生体制改革的意见》，标志着新医改正式施行。《意见》提出"2009年到2020年是我国全面建立小康社会的关键时期，医药卫生工作任务繁重"，近期目标是切实缓解"看病难、看病贵"的问题，长远目标是"建立健全覆盖城乡居民的基本医疗卫生制度，为群众提供安全、有效、方便、价廉的医疗卫生服务"。为推动落实这两个目标，中共中央国务院下发了一系列政策文件。

2013年中共中央国务院办公厅印发《中共中央关于全面深化改革若干重大问题的决定》，《决定》从公共卫生服务体系、医疗服务体系两个方面，解决"看病难"的问题，从医疗保障体系、药品供应两个方面解决"看病贵"的问题，主要改革措施如下所示：

- 医疗服务体系从基层医疗卫生机构和公立改革两方面落实。基层医疗卫生机构健全网络化城乡基层医疗卫生服务运行机制。公立医院建立科学的医疗绩效评价机制和适应行业特点的人才培养、人事薪酬制度。
- 公共卫生服务体系主要工作目标是充分利用信息化技术完善分级诊疗模式、加强区域卫生公共服务资源整合两方面促进优质医疗资源纵向流动。
- 药品供应体系改革包括取消以药补医，理顺医药价格，建立科学补偿机制三个方面。
- 医疗保障体系主要任务是改革医保支付方式，健全全民医保体系。加快健全重特大疾病医疗保险和救助制度。同时完善中医药事业发展政策和机制。

2015年中共中央国务院办公室印发《国务院关于积极推进"互联网＋"行动的指导意见》，《意见》提出推动在线医疗卫生新模式。基于互联网技术完成医疗数据共享，落实便民服务，提高医疗数据应用水平，持续解决"看病难"的问题同时向医疗健康的方向发展，具体落实措施如下：

- 构建医学影像、健康档案、检验报告、电子病历等医疗信息共享服务平台，逐步建立跨医院的医疗数据共享交换标准体系。
- 提供在线诊疗、候诊提醒、划价缴费、诊疗报告查询、药品配送等便捷服务。
- 引导医疗机构面向中小城市和农村地区开展基层检察、上级诊断等远程医疗服务。
- 建立医疗网络信息平台，加强区域医疗卫生服务资源整合，充分利用互联网、大数据等手段，提高重大疾病和突发公共卫生事件防控能力。
- 积极探索互联网延伸医嘱、电子处方等网络医疗健康服务应用。鼓励有资质的医学检验机构、医疗服务机构联合互联网企业，发展基因检测、疾病预防等健康服务模式。

2016年12月，中共中央国务院印发了《"健康中国2030"规划纲要》，提出"共建共享、全民健康"的战略主题，推动健康中国建设，最终实现医疗到健康的转变。《"健康中国2030"规划纲要》进一步提出了医疗行业发展方向，包括全面建成统一权威、互联互通的人口健康信息平台，规范和推动"互联网＋健康医疗"服务，创新互联网健康医疗服务模式，持续推进覆盖全生命周期的预防、治疗、康复和自主健康管理一体化的国民健康信息服务，实施健康中国云服务计划，全面建立远程医疗应用体系，发展智慧健康医疗便民惠民服务。

国家卫健委积极响应国家政策，具体落实医改工作，采取了"以评促建、以测促用"的工作方式。推动医疗机构信息化建设，最终建立统一规范的医疗信息化体系。2017年8月国家卫健委印发《国家医疗健康信息区域（医院）信息平台标准化成熟度测评方案（2017年版）》。通过测评指导并规范各地区开展区域信息平台标准化建设，以卫健委为中心推动医院与医院、医院与医疗职能部门、医疗职能部门之间信息共享协同，同时以患者为中心，推动医院系统之间、医院与第三方机构的信息共享与协同。《国家医疗健康信息区域（医院）信息平台标准化成熟度测评方案（2017年版）》旨在实现医疗资源的整合，提高医疗诊疗水平和医疗服务水平。

2018年12月国家卫健委印发《关于印发电子病历系统应用水平分级评价管理办法（试行）及评价标准（试行）的通知》提出："地方各级卫生健康行政部门要持续推进电子病历信息化建设，组织辖区内二级以上医院按时参加电子病历系统功能应用水平分级评价。到2019年，所有三级医院要达到分级评价3级以上；到2020年，所有三级医院要达到分级评价4级以上，二级医院要达到分级评价3级以上"。电子病历以患者为中心，将门、急、住系统进行集成，将急救和居民健康档案联系起来。电子病历系统建设是"一把手"工程，由院长领导，医院处负责，业务科室参与，信息科技术支持，解决了信息化建设和改造过程中建设不统一、业务与安全冲突等问题。

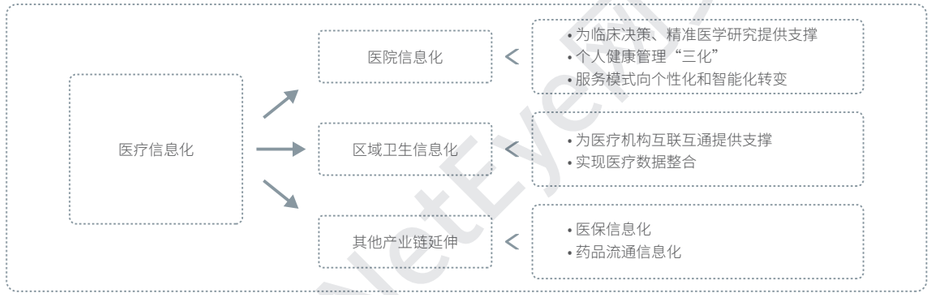
医疗行业现状分析

患者与医疗机构的供需关系驱动着医疗行业业务发展方向，信息化是医疗行业业务发展的核心措施。近几年医疗行业信息化飞速发展，为医疗机构人和物之间的互联互通提供了全方位的可能，医疗信息系统似乎与医疗执业单位越来越远，与患者越来越近。然而在信息化建设过程中带来了更多的网络安全风险，同时医疗行业早期的网络安全建设存在漏洞，最终导致网络攻击事件频发，为医疗行业信息化发展带来了阻力。

(一)医疗行业信息化现状分析

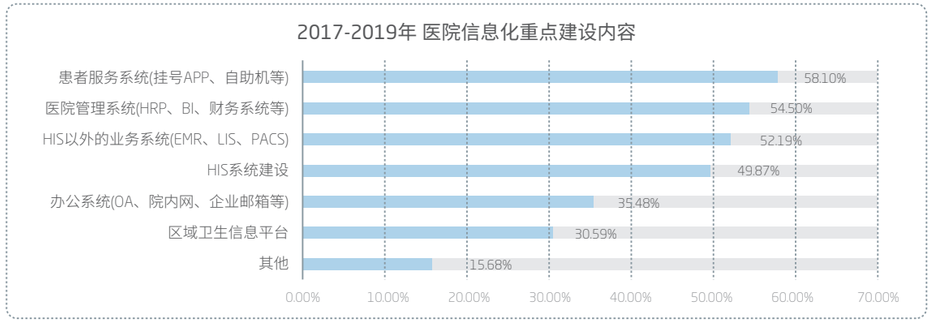
1. 医疗行业信息化现状

随着技术的快速发展，信息化正改变着每一个行业。在医疗行业，信息化正迅速从边际效率的驱动者转变为创新和价值创造的推动者，信息系统成为了医疗执业单位的基础设施，是核心竞争力，是医疗执业单位向前发展的内驱力。医疗行业信息化主要解决患者与医疗执业单位之间的供需问题，解决“看病贵、看病难”的问题，同时以精准医疗为代表提高医疗水平，从治疗转向预防。围绕着这一目标，医疗行业投入了大量资金进行信息化建设，已经基本解决“看病贵”的问题，“看病难”的问题也有所改善。现阶段医疗行业信息化建设主要围绕医院信息化、区域卫生信息化和其他产业链延伸三个方向落实。以优化医疗资源和提高医疗质量为信息化建设的重点，提高整体医疗水平，实现“以医院为中心”到“以病人为中心”的转变，最终在解决“看病难”的基础上实现全民健康。



2. 医院信息化现状

医院作为医疗行业关键单位，其信息化的水平直接关系着医疗行业信息化发展。经过对多家医院进行走访调查，结果表明随着医院以患者为中心服务理念的逐步落地，患者服务系统已成为近年来及下一步医院信息化建设的重点之一。同时，医改政策的实施和医院绩效考核的加强推动越来越多的医院将建设重点转向医院管理系统（HRP、BI、财务系统）等，助力医院实现精细化管理。随着医院HIS系统的普遍应用，EMR、LIS、PACS等系统的建设也提到了大部分医院的信息化建设日程中来。



图片来源：中国医院协会信息专业委员会发布的2019年《CHIMA医院信息安全调查报告》

(二)医疗行业网络安全挑战

挑战1—国内网络安全环境挑战

国内网络安全环境整体发生变化，各个行业面临持续的安全威胁。对安全市场进行了调研分析，发现需要防护的环境和设备越来越多、网络边界消亡、安全工具激增、网络犯罪日益复杂是国内各行业在网络安全方面普遍面临的挑战。

需要保护的环境和设备越来越多

信息化发展依托于硬件设备组成的基础环境，信息化建设越完备硬件设备越多。为了解决硬件设备扩充带来的数据迁移问题，各部门开始采取虚拟化形式部署，预测2019年将有29%的新服务器以虚拟化形态销售。这样庞大数量的设备同时也形成了大量的IT环境，保证这些设备和环境稳定运行，成为了信息部门的首要任务。

网络边界消亡

以前的网络环境主要是局域网环境，信息系统是在局域网相对安全、相对封闭的环境中运行的。现在放到了互联网+这个大环境，是个陌生的环境，是个万物互联的环境，是个不安全的环境，在这个环境里面很多的东西都在发生变化。同时各机构之间网络的互联互通、云计算的大面积应用促使网络边界的扩大和消亡。打破了传统的内网环境，为边界防护带来了巨大挑战。

安全工具激增

由于业务信息化快速发展产生了众多新的安全需求，对于新的不同类型的安全工具的需求也在激增。在许多情况下，这些工具仅仅是解决某个时期特殊安全问题的产品，在不久的将来，这些产品将被纳入传统的安全产品集。越来越大的安全工具为信息安全从业者带来了更多的挑战，产品的盲目使用将有可能导致新的安全风险。

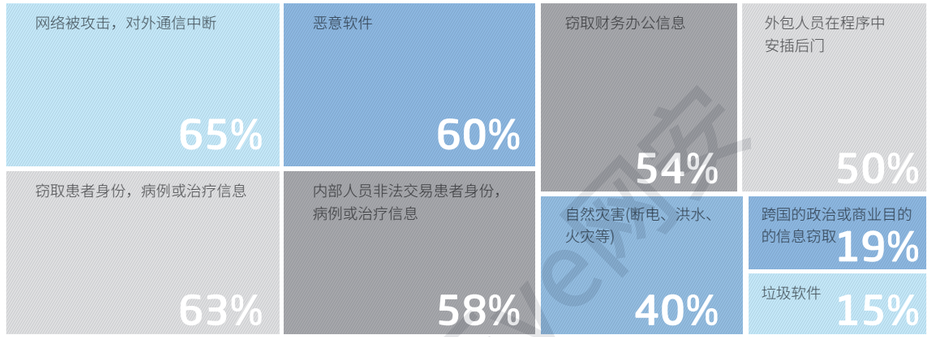
网络犯罪日益复杂

网络安全已经上升到了国家层面，更多网络攻击是有组织的网络犯罪，使用混合攻击方法攻击最终目标。同时越来越多的攻击者将繁多而复杂的技术变成网络攻击工具，以扰乱与他们的政治或意识形态观点不一致的组织。

挑战2–医疗行业面临的外部风险

医疗行业信息化快速发展带来的是运营效率的提高和收入的增长。然而信息化发展意味着IT系统不再是孤立的业务支撑系统而将与业务深度结合，业务越来越依赖于信息化系统。对于攻击者而言，高价值的目标则意味着高收益，因此医疗行业成为了黑客攻击的主要目标。根据对医疗机构的调研分析，医疗执业单位担心的来自外部的威胁主要包括通信中断、数据泄露、恶意软件等方面。

威胁(来自外部的攻击行为)

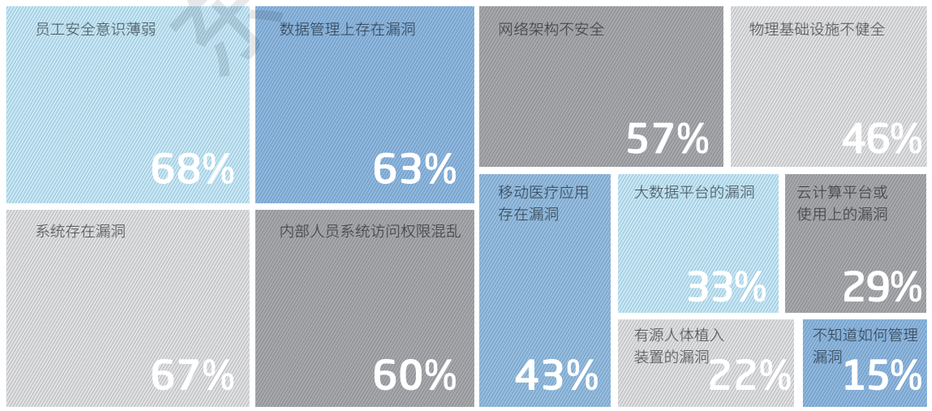


图片来源：东软NetEye联合安全牛发布的2018年《医疗行业信息安全调查报告》

挑战3–医疗行业面临的内部风险

单纯的外部威胁并不能造成真正的网络攻击。内部资产的弱点是导致网络攻击的另一个因素，攻击者识别内部的弱点，利用内部的弱点进行针对性的攻击是目前最常见的攻击方式。从医疗机构的角度，其认为目前内部资产弱点主要包括员工安全意识薄弱、数据管理漏洞、系统漏洞、内部访问权限混乱等方面。

威胁(来自外部的攻击行为)



图片来源：东软NetEye联合安全牛发布的2018年《医疗行业信息安全调查报告》

(三)医疗行业信息安全防护困境

面对日益严峻的网络安全形势，医疗行业应当将信息安全建设作为医疗行业信息化发展的基石。只有保障医疗执业单位的网络安全才能确保业务的稳定运行和持续发展。然而目前大多数的医疗机构在信息安全建设方面仍然存在不足。

困境1–安全预算不足

医疗机构更注重信息化发展，将更多的资金投入到对业务有直接帮助可以产生效益的系统建设上，而在网络安全建设投入较少。网络安全建设的预算应当是基于医疗执业单位面临的安全风险和安全需求，评估应落实的安全建设成本。漫长的求证与审核非但不能节约开支，反而丧失最佳的时机，制约业务的发展。

困境2–基础设施建设难

由于物理环境限制、业务系统连续性和预算不足等原因导致医疗执业单位基础设施建设不到位。强健的基础设施是应对一切安全风险的根本，无论我们的人力、应用和流程是怎样的完备与敏捷，当面对难以预测的攻击时也只能束手就擒。应对攻击最好的方式是“保证资源具备弹性和空间”。

困境3–安全治理落实难

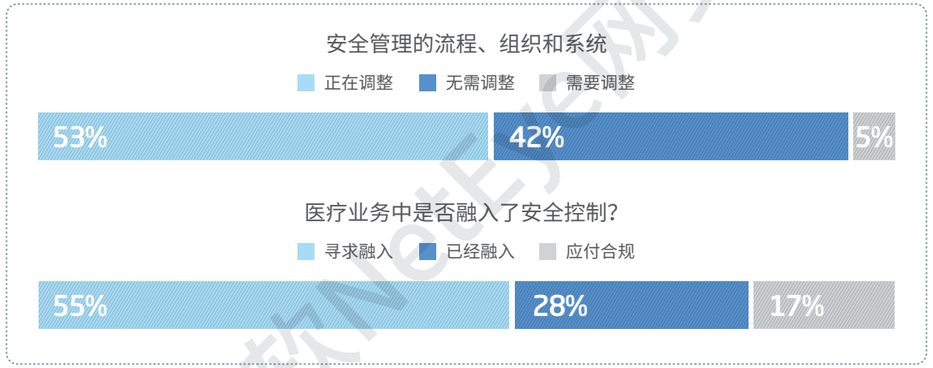
大部分医疗机构并未树立正确的安全治理观念，网络安全建设仍然处于盲目建设阶段。完善的安全治理组织和流程，可保证医疗执业单位实施安全防御的措施，去直面不断变化的威胁。这些措施不是面面俱到，而是根据自身的发展战略、风险评测、业务导向，并在满足合规要求的前提下，发挥资金的最大价值。良好的安全治理流程，不会成为敏捷特性的羁绊，只会在积极的防御中让医疗执业单位更加的高效和专业，避免沦为游击式的发挥。这样持续化的安全治理不断锤炼，能确保医疗执业单位持续修复弱点，树立信心去开拓更多的业务。安全管理者需要持续的向领导传达这个理念并获得承诺与支持。

困境4–防御体系效果差

近年来很多医疗机构不断遭受网络攻击，勒索病毒攻击事件，数据泄露事件持续增加，尤其是在新兴技术广泛应用的背景下，安全问题将会持续呈现增长趋势。这一现状表明传统的安全防御体系已经难以有效的保障医院的业务。据统计，传统的安全防御体系失效主要包括以下几个原因：

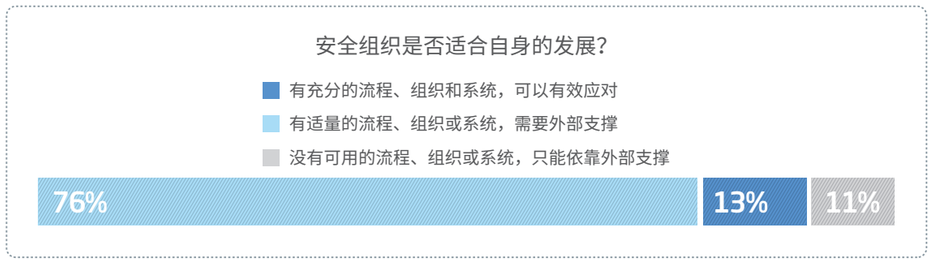
设计出发点错误

医疗执业单位安全防护体系设计规划时间短，建设落实时间短，导致安全防护体系无法起到真正的防护作用。安全防护体系建设并不是通用的，针对不同机构和业务情况应定制符合其安全需求的安全防护体系。同时安全防护体系建设也不是一蹴而就的，应结合信息化发展情况和能力逐步建设逐步完善。然而安全体系设计之初医疗执业单位并未重视这些问题，导致安全组织建设不适合自身的发展，安全措施没有结合实际医疗业务。目前大多数的医疗执业单位正在寻求调整安全体系的方式，解决安全体系设计不合理带来的问题。



建设思想落后

传统网络安全防御体系建设思想落后，通常采用单点防护的思维，以安全产品为主要落实手段，忽视了安全防御体系建设的关键问题，降低了安全防御体系的防护效果。单点的防护措施忽略了产品之间的配合与联动，降低了产品的防护效果。以安全产品为核心的落实措施，忽视了安全管理的重要性，只有将产品与管理结合持续运维才能到达理想的防护效果。



防御技术迭代速度慢

网络空间已经成为继陆海空天外的第五维空间，人民的生活与之息息相关，在各种利益的驱使下，黑色产业的攻击持续不断。攻击方与防御方之间的博弈愈演愈烈，技术的迭代速度决定着谁能够获取短暂的胜利。传统网络安全防御体系中，安全防御技术迭代速度较慢，因此遭受攻击概率持续增加。

困境5–专业信息安全人员缺失

对网络安全担忧的日益增长和不断变化的IT架构正在推动着各单位对经验丰富的网络安全专业人士的需求。网络安全人才储备不足导致网络安全人员工资的上升，小型医疗机构难以为此支付更多的成本，导致缺乏专业的信息安全人员。没有匹配的人员安全素质，先进的体系、平台和工具的效益将大打折扣。

(四)医疗行业网络安全事件

医疗行业信息化的快速发展导致安全形势日益严峻，面临的安全风险与日俱增，同时医疗行业前期安全防护建设不足。这些因素最终导致近年来医疗行业网络攻击事件层出不穷。勒索病毒导致业务系统瘫痪，数据泄露对医疗机构形象和患者利益受损是近年来医疗行业发生的主要安全事件，为医疗行业带来了极其严重的影响。

1. 国际医疗行业网络安全事件

- 2014年10月，波士顿儿童医院卷入一起有争议的14岁病患监护权案件。此案的敏感性刺激了黑客主义者团体“匿名者”发起DDoS攻击，长达1周时间的持续攻击为波士顿儿童医院造成了约30万美元的损失。

- 2015年7月美国食品和药物管理局对Hispira公司发出警告，强烈建议医院不要使用Hospira公司的Symbiq输液系统，因为该系统存在安全漏洞，可能被利用发动网络攻击进而实现对该系统的远程控制。

- 2017年8月美国食品和药物管理局发布了一项警告。警告称由于网络安全漏洞，召回健康公司Abbot的46.5万个心脏起搏器。

- 2017年5月英国国民健康服务体系（简称NHS）受到勒索病毒攻击，至少16家NHS信托机构受到冲击，IT系统被攻破，病人健康受到威胁。NHS医疗系统遭受勒索病毒攻击在英国范围内引起了热烈的讨论。

- 2017年6月美国最大制药商之一的默克（Merck）公司和宾夕法尼亚州西部经营两家医院的医疗网络系统——Heritage Valley健康系统也成为新勒索病毒攻击的牺牲品。

2. 国内医疗行业网络安全事件

- 2016年7月中国疾控中心数据泄露，31个省区127个地区498例艾滋病感染者接到诈骗电话，11位艾滋病感染者被诈骗数额共122083元。有两例因隐私暴露，所在单位知情后被迫辞职。

- 2017年5月“永恒之蓝”勒索软件对成都市部分医院造成影响，为防止勒索病毒攻击，根据国家卫健委和四川省卫健委指示，紧急切断了医院与外网的联结。

- 2018年2月，湖南省儿童医院遭受勒索病毒，导致全院所有医疗系统瘫痪22个小时，给医院造成了极大的经济损失和极其恶劣的影响。

- 2018年1月四川警方破获了一个非法信息买卖案件。成都市某社区卫生服务中心的工作人员徐某利用职务之便，进入妇幼信息系统下载全市新生婴儿和预产孕妇的50多万条信息。这些信息被层层转卖，用于向新生婴儿家庭推销甚至诈骗。

- 2018年3月，湖北某医院内网遭到挖矿病毒疯狂攻击，导致该医院大量的自助挂号、缴费、报告查询打印等设备无法正常工作。由于这些终端设备为自助设备，只提供特定功能，安全性没有得到重视，导致挖矿病毒集中爆发。

- 2018年6月，上海市医疗保险系统发生故障，医保结算业务瘫痪将近4小时。全市各家医院医保实时结算普遍受到影响，由于只能采用现金结算，导致医院各个窗口前的结算服务进行缓慢，人流难以疏通。

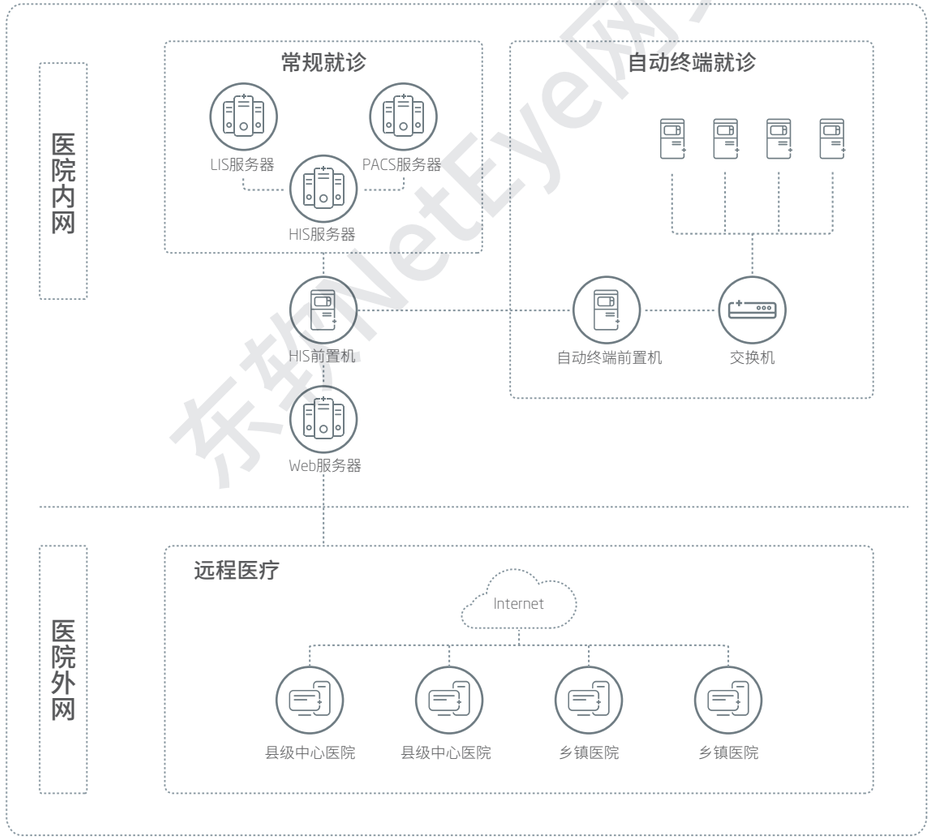
医疗行业典型场景风险分析

目前，为了提高工作效率和医疗水平，医疗行业快速进行信息化建设，医疗业务对于信息系统的依赖性越来越强，信息系统已经贯穿于医疗活动的全生命周期。医院依赖于HIS、LIS、PACS、手麻、OA等信息系统完成病人从入院到出院的全部业务，病人的各项检查数据、病人与医院的经费往来费用等等均存储在信息系统服务器中。医保局依赖于医保系统实现医保报销、医保与医院的结算等业务。卫健委依赖于区域卫生信息平台、智慧医院监管平台等信息系统实现医疗资源的整合和医院业务监管的职责。由此可见，医疗执业单位已与信息系统有着密不可分的关系，信息系统的稳定运行成为了医疗行业业务开展的关键。

东软NetEye深入解读医疗行业政策文件，紧跟医疗行业发展步伐，依据《卫生行业信息安全等级保护工作的指导意见》、《互联网医院管理办法》、《省统筹区域人口健康信息应用功能指引》、《国家医疗健康信息区域（医院）信息平台标准化成熟度测评方案（2017年版）》等国家关于卫生行业的安全要求，结合多年来在医疗行业的项目经验以及各医疗机构的反馈，站在医疗从业者的角度对医院业务场景进行分析，识别各场景中的安全风险。医疗信息化建设是不断优化持续改善的过程，由于各地区物理环境限制、经济投入限制等原因导致医疗信息化存在较大差异，各医疗机构应结合自身的信息化情况识别安全风险建立防护措施。

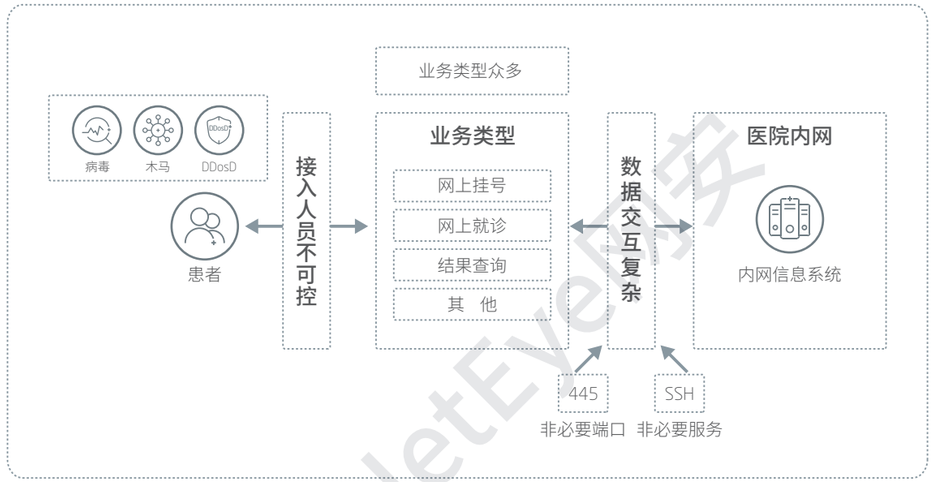
(一)典型场景1–就诊场景安全风险

患者到医院就诊的过程中，抱怨最多的问题往往是就诊过程时间太长，挂号候诊排队、检查取报告排队、缴费报销排队。医院为了解决就诊时间长的问题，结合《国务院关于健康服务业发展的若干意见》指导相关要求，从提高医院就诊效率和基层医院就诊水平两个方面入手。通过互联网挂号、转诊服务推动传统就诊效率，通过发放就诊卡、部署自助服务终端设备开展自助就诊方式。让患者可以自助完成挂号、取化验单、结算等业务提高医院就诊效率。通过开展远程诊疗服务让患者可以在基层医院接收大医院的诊疗服务提高基层医院的诊疗水平。就诊场景的系统部署和网络连接如下图所示：



1. 一般就诊

为了减少医院挂号窗口的工作，提高患者就诊体验，医院基于互联网开展了线上诊疗服务。患者可以在网上进行挂号、就诊、查询检查结果等业务，为患者就诊带来了极大的便利。医院开展互联网业务使医院的内网不得不与互联网进行连接，导致医院面临了新的安全风险，主要体现在以下几方面：



医院内网边界安全

开展网上就诊服务，内网服务器需要向外网提供数据保证患者可以查询数据，同时挂号等数据要写入医院内部服务器。因此外网需具备内部服务器的读写权限，然而互联网上的攻击多种多样，木马、病毒等可以通过互联网进入医院内网服务器导致医院网络瘫痪，通过互联网可发起DDoS攻击影响内部网络，导致网络拥堵。

互联网业务安全

随着患者需求增加和医院信息化发展，医院开展的互联网业务越来越多。攻击者可能利用某一个互联网业务的漏洞横向攻击其他互联网业务，导致医院互联网业务全面瘫痪。

患者数据安全

医疗数据一直是黑产市场上的重点交易对象，随着精准医疗、医疗数据整合等业务的开展，医疗数据价值显著提高，互联网业务为患者提供查询数据的同时也为黑客提供了一条盗取数据的路径。

2. 自助终端就诊

自助终端设备为患者自助办理和发放医院诊疗卡，患者持医院诊疗卡/社保卡/居民健康卡等介质进行挂号/预约号取号/打印检验报告/打印门诊清单/打印住院费用清单/信息查询等自助式服务，使用银行卡/社保卡进行充值缴费和住院预缴等自助式服务，解决患者就诊过程中的排队问题。

为了实现上述自助式服务，自助终端设备需要与医院内部HIS系统连接实现挂号、结算等功能，与LIS/PACS系统连接实现检查报告打印功能。在自助终端系统建设中为了规范标准、节约资源和保障信息安全，部署了医院自助终端前置机。自助终端统一与自助终端前置机进行通讯，自助终端前置机通过医院内网与医院的HIS前置机系统通讯。

自助终端设备的使用解决了患者就诊排队的问题，减轻了医院人工窗口的压力，但是自助终端设备在安全管理方面却存在一些问题，主要体现如下：

数量多

根据各医院对于自助终端设备使用需求不同，医院采购的自助终端设备数量不同。据统计，普通三级甲等医院大约采购80~100台，就诊人数多的大型三级甲等医院使用数量可达到200台左右。

部署分散

具备不同功能的自助终端设备部署在医院的各个位置，例如挂号、缴费功能的自助终端设备主要部署在医院一楼，而检验结果打印自助终端设备部署在检验科室附近，费用查询功能的自助服务终端设备在住院部每个楼层都有部署。

风险处置难

市面上常见的自助终端设备大多采用Windows XP系统，低版本操作系统本身容易出现安全漏洞，并且更新系统补丁或使用更高版本系统可能导致硬件的不兼容，影响自助终端设备的正常使用，因此无法及时修复漏洞。

防护效果差

自助终端设备在建设和部署过程中仅考虑系统连接等问题，常常忽略安全防护问题。即使考虑了安全防护问题，也仅仅是在自助终端前置机与医院系统之间部署防火墙。这种单点的、粗粒度的安全防护措施无法解决终端设备本身的安全漏洞，也无法达到整体防护效果。

3. 远程医疗服务

远程医疗是一方医疗机构（邀请方）邀请其他医疗机构（受邀方），以提升医疗服务为目的，运用通讯、计算机及网络技术为医疗机构诊疗患者提供技术支持的医疗活动。远程医疗服务一般由卫健委搭建远程医疗信息资源中心，为受邀方和邀请方提高统一业务平台支撑具体远程医疗应用，同时邀请方和受邀方通过专线、MPLS VPN、Internet、3G/4G、卫星等多种手段接入远程医疗信息资源中心。

远程医疗服务主要存在以下安全问题：

共享机构多

病历共享是远程医疗信息系统的核心需求，多部门的数据交互与共享增加了数据泄露的安全风险，同时基层医疗机构由于环境限制常常使用互联网进行传输。患者隐私数据的泄漏直接侵犯患者利益，影响医院的声誉；远程医疗信息等在传输和存储过程中被篡改或丢失将直接影响会诊结果，情况严重将导致医疗事故。

防护水平差

参与远程医疗的专业机构需要在机构内网与远程医疗外网之间进行部分连接与限定的信息交互，其他大量内网信息则不能外泄。远程医疗机构的安全防护水平参差不齐，使得医疗机构内网安全面临新的挑战。

业务稳定要求高

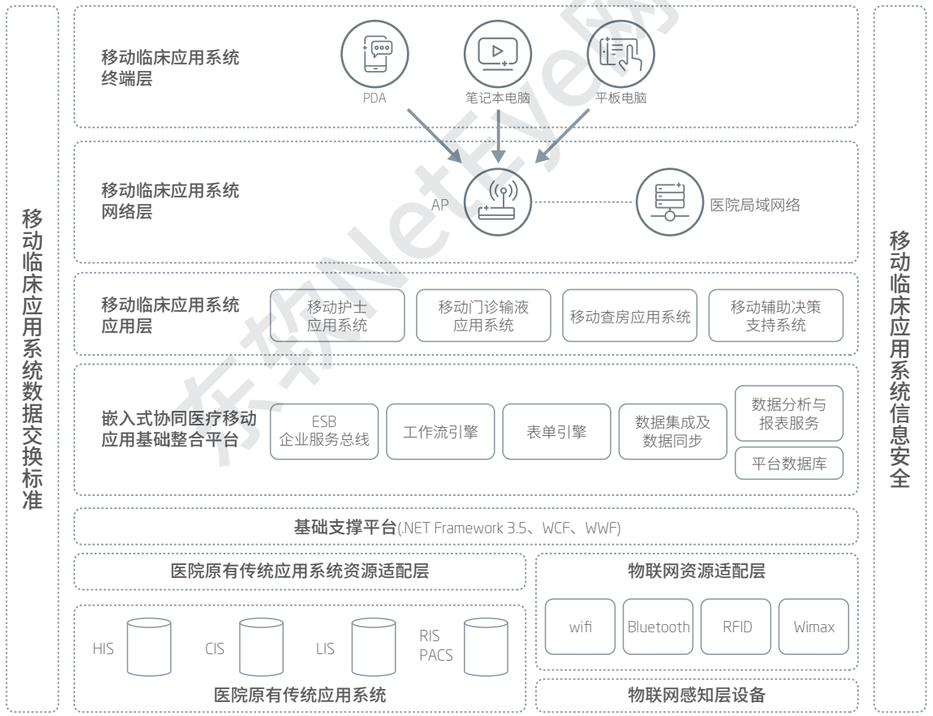
远程医疗信息系统包括远程会诊、双向转诊、远程重症监护、远程手术示教等多项功能。系统应提供7×24小时连续运行，平均年故障时间小于1天，平均故障修复时间小于30分钟。系统在日常使用过程中不会出现运行错误、无法执行等现象影响正常使用。

(二)典型场景2–住院场景安全风险

1. 移动终端

为了更好的监控医嘱执行效果，实现"以病人为中心"的管理理念，解决传统HIS使用中医生在病区日常工作中查看患者病历、获取化验结果和下发医嘱不及时等问题，避免了护士在执行医嘱过程中抽血及用药错误等问题，医院引进了移动应用系统。

移动应用系统的架构设计将系统分为无线移动终端、无线网络、移动临床信息系统应用软件、嵌入式协同医疗移动应用基础融合平台、基础支撑平台、医院原有传统应用系统资源适配、医院原有传统应用系统七个层次，以及移动临床应用系统数据交换标准、移动临床应用系统信息安全两个支撑平台，如下图所示：



然而，移动医疗系统在实际使用中对提高医疗效率、医护质量控制管理有显著作用的同时，也不容忽视随之而来的数据安全风险性。

目前移动医疗系统网络安全存在以下几方面问题：

移动医疗的接入方式

医院本地区域内的移动医生终端、移动护理终端等设备通过分布在楼道或病房的无线AP接入医院网络。AP通过局域网线接入到楼层交换机，楼层交换机通过光纤连接到汇聚交换机，再经过核心交换机连接到中心机房。在连接过程中，无线AP的接入方式具有开放性和隐蔽性，任何一个未经授权允许的终端设备都可能接入，并访问内部保密数据引起数据泄露。

通用性与非法攻击安全隐患

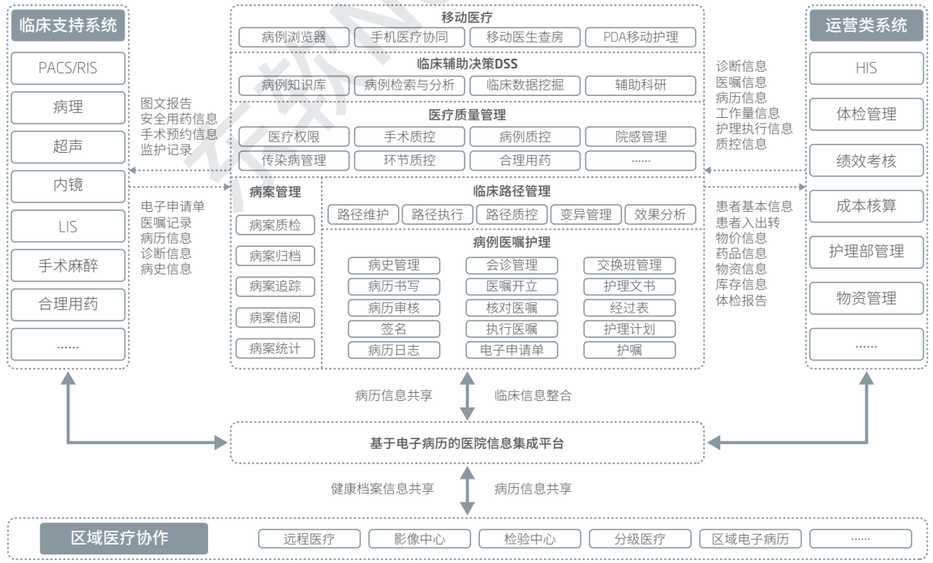
移动医疗主要使用Windows操作系统，但由于其易用性导致网络黑客可能进行全面而深入的研究，并利用发现的系统安全漏洞进行攻击。

管理措施执行

根据统计按照一个病区配备4至5台移动护理设备，普通三甲医院移动护理设备数量将达到300至400台，这样大的数量给移动设备管理带来了极大困难。管理问题主要体现在移动医生终端、移动护理终端权限划分不到位，存在越权现象。

2. 系统融合

为实现医院信息系统与各类业务应用的动态整合、信息数据规范共享的目标，提高医院工作效率。基于电子病历的医院信息平台将医院的系统进行资源整合以实现共享的目的，负责与区域卫生信息平台等各部门的信息交互。在系统数量多、种类复杂且高度集成的医院信息平台中如下图所示：



目前基于电子病历的医院信息平台网络安全存在以下几方面问题：

身份假冒、口令窃取威胁

医院信息系统的登录方式大多采用“用户名+口令”方式，存在身份假冒威胁等，一旦医护人员的身份被窃取，将直接影响到患者信息、电子病历等的安全性和隐秘性。

数据泄露和破坏威胁

医院信息平台中存在大量隐私信息，包括个人健康信息、统计信息等，而这些信息在存储和传输过程中极易被窃取或监听。一旦数据丢失或被篡改，将造成很大的影响。另一方面，随着便携式数据处理和存储设备的广泛应用，由于设备丢失而导致的数据泄漏威胁也越来越严重。

计算机病毒威胁

病毒是系统最常见、威胁最大的安全隐患，主要表现为利用系统软件或应用软件中的程序错误或安全漏洞来获得对计算机系统的非法访问和攻击。医院终端数量众多包括医生工作站、医技工作站、护士工作站等，人员安全意识薄弱，设备管理困难极易导致病毒入侵。一旦将计算机中的病毒或木马引入医院信息系统中，将可能造成严重的系统瘫痪及资源的泄漏。

系统漏洞威胁攻击

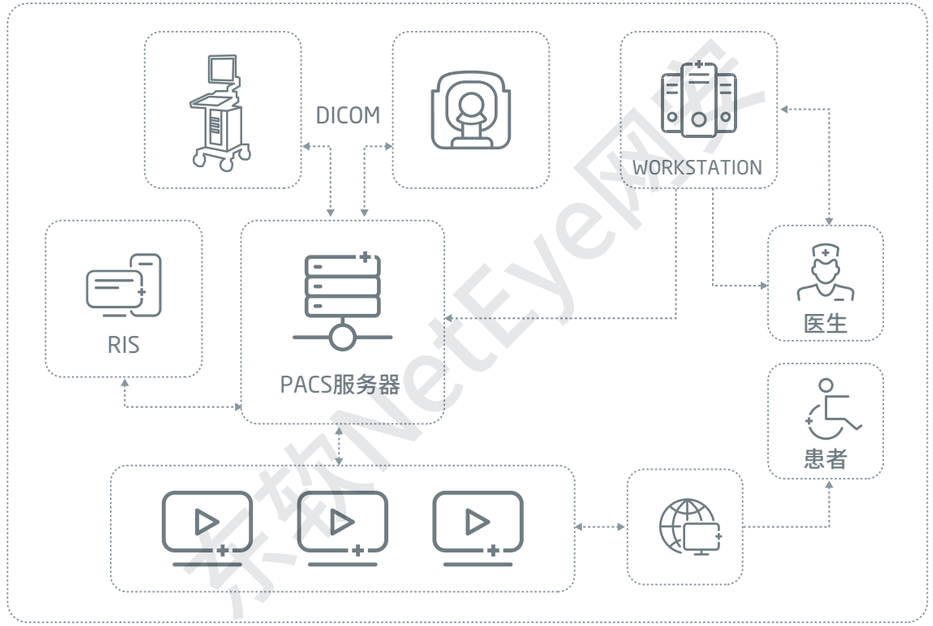
医院信息化发展迅速，系统更新迭代速度快。医院信息平台集成了大量的系统很有可能存在着可被攻击者利用的安全弱点、漏洞以及不安全配置等安全隐患，主要表现在操作系统、网络服务、TCP/IP协议、应用程序（如数据库、浏览器等）、网络设备等几个方面，正是这些弱点给蓄意或无意的攻击者以可乘之机，一旦系统的漏洞被利用成功，势必影响到系统的稳定、可靠运行，更严重的导致系统瘫痪和数据丢失，从而影响医院的公众形象。

通讯业务流传输侦听威胁

医院信息平台作为医院内部跨系统的数据交互平台，网络中存在大量的信息交互，非法人员可以通过对信息流向、流量、通信频度和长度等参数的分析，获取平台内部的隐私信息。

(三)典型场景3–检查场景安全风险

医院采用PACS系统把各种数字化信息（包括CT/MR/DSA/CR/DR等）通过各种（模拟、DICOM、网络）以数据化的方式海量保存起来，把B超、内镜等非数字化图像经过信号转换器转换成数字化图像信息进行保存，当需要的时候在一定的授权下能够很快的调回使用，同时增加一些辅助诊断管理功能，PACS工作流程如下图所示：

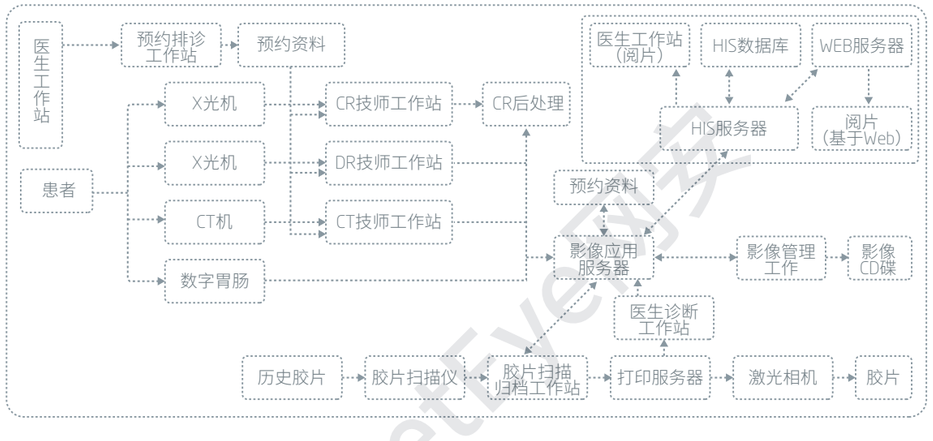


这种系统实现了各种数字化医学设备影像的连接，可以在影像科范围内进行图像的数字化存储和网络传输，我们称之为科室级PACS。科室级PACS的影像管理还是以传统的“灯箱+胶片”的方式为主，这些影像设备没有与医院的HIS系统进行连接，这给医生的工作效率、医院的全面信息化管理带来了诸多不便：

- 不能同步患者在HIS系统中的报告申请信息，需重复录入患者资料，增加了医护人员的工作量。
- 患者做了多项影像检查之后，需要回到各科室等待、领取影像报告。
- 由于各影像设备没有联入医院信息网络，影像数据不能实时共享，使教学、科研等各类后期应用难以开展。
- 在影像数据量不断增长、分散式的数据管理模式下，数据安全存在诸多隐患。

1. 全院级PACS

为了解决上述问题，多家医院上线全院级PACS，实现了影像科室与临床各科室之间的医学影像数据的网络传输、信息共享和数字化诊断，同时达成影像系统与HIS系统之间的信息互联互通。使得HIS临床医生下达的医嘱能够通过网络送达影像医技科室的登记台，提高登记速度和准确率，避免和减少手工重复录入和减少人为的输入错误，全院级PACS流程如下图所示：



由于影像设备和PACS系统在设计时只考虑了其应用型而在安全方面的考虑却非常的欠缺，所以在实现信息互联互通的同时，也不可避免的出现了很多安全问题，主要体现在以下方面：

- 影像设备使用FreeBSD、VxWorks等操作系统，这些操作系统漏洞发布不及时，导致风险发现不及时。
- 影像数据使用DICOM、HL7等医疗行业专有的传输协议，这些协议存在安全风险的可能性。
- 全院级PACS将影像数据与HIS系统进行连接，各科室均可在线阅览，而各科室的权限以及数据出口存在安全性问题。

全院级PACS实现了影像数据的整合，但是全院级PACS系统使用的是医院内部局域网，无法通过网络进行数据传输。每家医院的PACS系统存储平台接口不一样，而从DICOM接口来进行数据共享不仅技术难度较大，而且会大量改动PACS应用。同时随着近年来数字成像技术的迅猛发展，尤其是多排CT、高场强磁共振等设备的普及，PACS系统所承载的数据量呈几何式增长，给数据存储带来了极大压力。

基于传统的数据存储方式，目前PACS系统在存储数据方面存在以下几个问题：

目前的存储架构很难实现PACS影像数据长期、可持续的支撑

国内一个中型医疗机构平均每天新增几十GB的影响数据，每年200天总计新增十几到几十TB的医疗影像数据。很多PACS上线较早的医院几乎每一两年就需要进行一次存储扩容，不仅投资巨大，而且每次扩容的实施难度很大，而性能却越来越低。

PACS系统硬件维护成本高

PACS系统本身硬件存储设备日常要进行维护，要定时升级，不仅会造成医院业务中断，且运营维护成本贵。

没有足够的安全性考虑

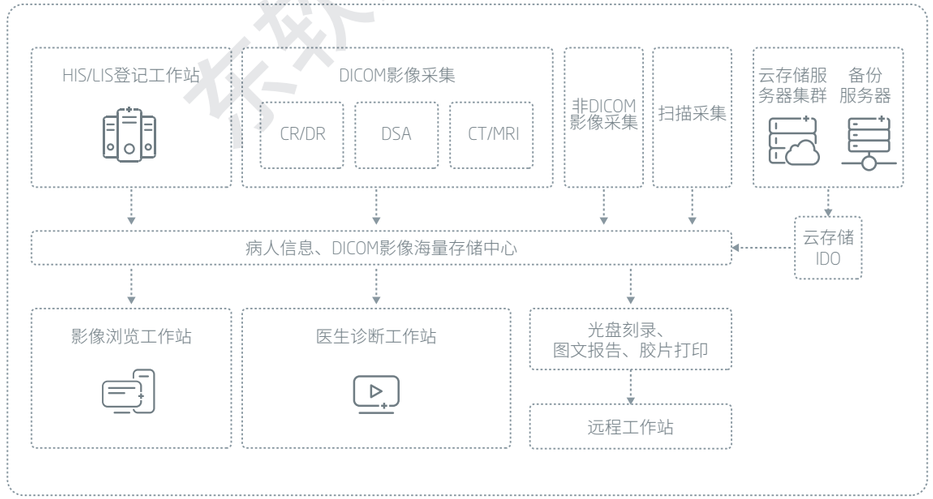
很多PACS系统中，连最基本的防病毒措施都没有，往往PACS存储系统成为医院最大的"毒窝"，很多终端因此而反复感染病毒。包括数据的备份，存储冗余等基本的措施都没有，PACS系统实际上处在一种非常脆弱的状态中，一个简单的存储故障就可能导致整个PACS系统完全瘫痪，而一个硬盘的故障可能会导致PACS影像数据的大量丢失，甚至永远无法恢复。

缺乏对前端透明的数据生命周期管理

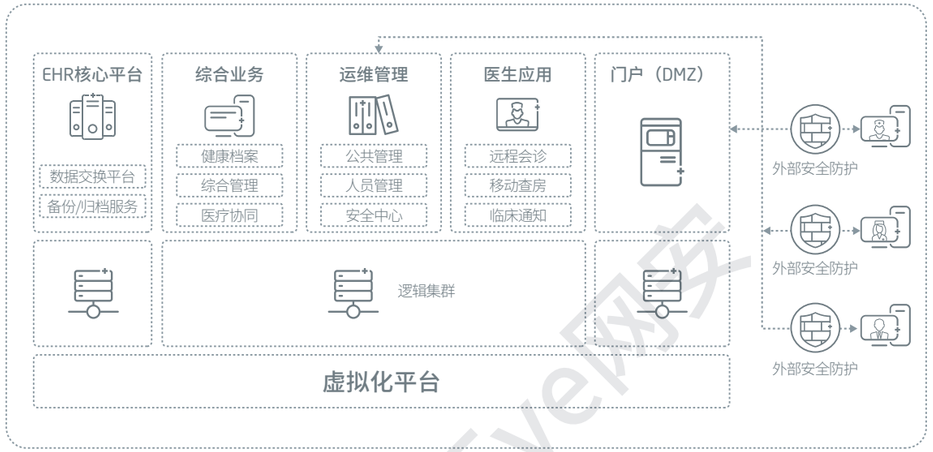
现有的存储系统对PACS影像的管理几乎都是把所有数据放在同一级别上的粗放式管理，没有根据数据生命周期进行合理的分配，或者是有一些简单的分级措施，但对前端影响太大，往往导致历史查询很困难，数据丢失等情况时有发生。

2. 企业级PACS

综合以上现状，站在PACS系统长期发展和区域信息共享的角度，提出了PACS云存储平台，一方面，云及虚拟化技术的引入降低了医疗行业核心业务的运营开支；另一方面，医疗行业具有数据量大、复杂性高等特点，云及虚拟化技术的引入将加速数据运算的处理能力，拓扑图如下图所示：



根据《中共中央国务院关于深化医药体制改革的意见》要求，实现医院内部数据整合，同时也为智慧医院建设打好基础，在医院中云存储不仅仅存储影像数据，包括医生应用、运维管理等数据也搬到了云平台，如下图所示：



在云及虚拟化外部的安全防护手段已经无法解决内部安全需求，出现的安全问题如下：

- **如何能对虚拟机之间的异常行为进行有效阻断?**
- **虚拟机之间流量传递怎样才能直观呈现?**
- **平台迁移过程中的安全策略能否随之迁移?**

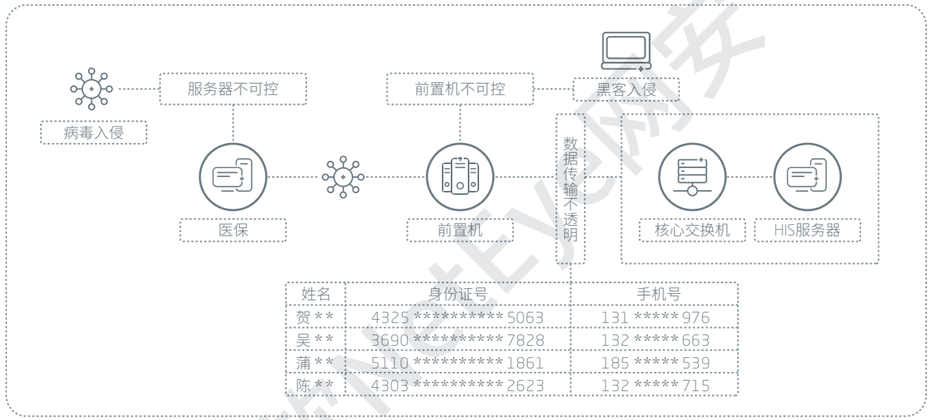
3. 数据跨院共享

以分级诊疗为手段优化医疗资源配置是目前医疗行业主要发展方向。实现分级诊疗的前提是保证患者数据的共享，避免患者重复检查。根据各地区医疗机构调查显示，部分地区乡镇卫生院等基层医疗机构通过专网将患者检查结果传输到当地区县医院。卫健委作为数据中转和汇聚中心，负责各区县医院与其他大型医院的数据共享。这种传输方式实现了医疗数据共享与整合，但是，接入机构众多增加了网络安全隐患，而且各地区医疗机构众多，信息化水平和安全建设水平存在较大差异，不同的医疗机构需要面对如何保障自身的网络安全的问题。

(四)典型场景4–结算场景安全风险

1. 医保结算

医院在对城镇居民提供医疗服务的同时，需要与该地区的社会保障部门进行信息交流，主要是为了享受社会医疗保障的居民提供个人医保的提交、缴费等一系列数据，因此各地医院大部分通过光纤专线接入和拨号专线接入等方式接入地方医保网络，如下图所示：



姓名	身份证号	手机号
贺**	4325**********5063	131*****976
吴**	3690**********7828	132*****663
蒲**	5110**********1861	185*****539
陈**	4303**********2623	132*****715

医保网络是一个非常复杂的网络结构，管理难度大，因此，也相应地增加了安全风险。从目前实际情况分析，医院HIS与网络互联中存在的主要风险概括为"3个不可控、1个不透明"。

- **网络安全环境不可控**

医保信息中心是一个异常复杂的网络环境，除了自身管理的网络以外，还要和银行、社区街道、药店等其他单位互联。由于医保网络接入终端数量多、分布广，给病毒、木马传播提供了便利的途径。

- **网络范围不可控**

医保信息中心通常通过城域网的"专线"与医院HIS网络互联，而由于数字网络的特点，实际上，这种"专线"仅仅是医院HIS网络到城域网机房之间的"专线"，并不是我们想象中的医院网到医保网络的"专线"。真实的情况是，医院网和医保中心之间仅仅是通过在城域网交换机上设置虚拟局域网（VLAN）来实现逻辑上的"专线"。目前最常见的是采用MPLS技术实现虚拟专线，这种专线从理论上讲可以通过人为设置进行改变，甚至允许任何节点访问。

核心服务器主机安全不可控

放置在医保网络与医院网之间的前置机，在实际工作中是由医保网络方面进行管理和配置，医院方面对该服务器没有控制权。前置服务器安装了Windows操作系统、医保应用软件等，可能存在大量系统漏洞，并且由于网络原因，其补丁更新非常不及时。从目前该服务器的配置管理情况看，它能够直接访问医院网内部所有服务器和PC，这样任何黑客都能够以该服务器为跳板攻击医院内网，窃取、破坏资料。

信息采集不透明

截至目前，我们并没有任何手段能够掌握医院向医保中心传输了哪些信息，是否存在敏感信息。虽然在硬件结构上医保网络与医院通过"信息缓冲区"实现隔离，但由于运行在"信息缓冲区"上的前置机的应用程序、运行在医院各电脑上的数据交换接口等完全封闭在医保网络提供的整套软件环境中，整个通讯过程完全由医保网络控制。从业务数据的层面看，医保网络完全进入了医院的HIS网，并取得了数据传输的控制权。

2. 第三方平台支付

在早期医院信息化建设不完全的阶段，医院结算中，现金支付占据着相当大的比例。门诊和住院使用HIS系统进行收付款处理（包括检查、药品的收费和住院预交金及结算收费）。所有终端配有刷卡器，但不能受理银行卡，只能采用现金方式，费用从几元的零头到上万元，需清点现金并验证真伪，虽然有点钞机，但是遇到钞票皱折破损，点钞机不能正常工作，反而会延长浪费更多时间，同时需准备零钱，各个环节都会导致错误，例如多找、漏找零钱。工作人员需要更多的时间精力放在清点现金和找钱环节上，数目不正确、收到假钞，工作效率低等问题明显。为了受理银行卡业务，有的医院直接安装POS终端机来处理刷卡。所有收费窗口，除了计算机，还摆放着POS机。医院部署前置机与银行进行信息交互，银行网络安全体系建设时间早投入巨大因此对于医院网络安全影响较小。

然而随着医院业务的发展和日益增加的门诊量，为了提高结算的效率，很多医院将HIS系统和第三方支付平台如微信、支付宝进行连接，实现了手机支付功能。2016年，移动支付业务共257.1亿笔，金额共157.55万亿元。同比分别增长85.82%和45.59%，保持快速健康增长。互联网式的就医支付体验，符合消费者逐渐改变的消费习惯，有效提升就医体验，同时也极大的改善了医疗环境、提高了医护质量。但互联网支付也给医院的业务系统带来了很高的安全风险。

(五)典型场景5–数据安全风险

随着“互联网+”时代的到来，医疗行业开始加快推进信息化建设，加速实施基于电子病历的医院信息平台、区域卫生信息平台、影像共享中心等的整体建设，大量诊断记录、用药信息、患者信息等汇聚到各种平台内，这些信息中含有病人的身份标识信息包括姓名、家庭住址、邮箱地址、生日，病人的诊疗信息包括保单号码、检验结果、诊断结果等敏感信息，数据聚合或二次加工后产生的基因信息和公共信息。然而大部分医疗组织和机构在数据安全管理和数据保障措施方面相对落后，安全意识相对薄弱，因此导致医疗行业信息泄密事件频发。

1. 业务层面

医疗行业各部门之间数据传输共享的行为越来越普遍，增加了数据传输风险，同时增加了数据管理难度。为了提高患者就诊效率快速查询,医疗行业各部门分别开展了网上查询业务，增加了数据爬虫等风险。医疗行业信息系统高度集成，实现了数据互联互通扩大了数据的使用范围，增加了非法查询的风险。

2. 运维层面

信息化建设中涉及到大量信息化设备的引入，由于资源限制，一方面运维过程中通常会找寻第三方人员进行维护；另一方面院内运维人员通常有较大的运维权限，缺少有限监管，而底层设备往往直接连接着医院的核心敏感数据，如何对内外部的运维过程进行有效监管，成为了保障数据安全的难点。

3. 保障措施层面

医疗行业现有安全防御手段多以被动防御措施为主，市场上出现很多基于权限管控、终端管理、运维管理和数据库审计等安全类的防护产品，但这些防护手段依旧停留在被动防御的阶段，那么，在数据流转过程中，如何才能全面掌握核心敏感数据的安全状况，如何在第一时间精准有效的对数据访问者进行定位、跟踪，并对敏感数据的非法调阅进行实时阻断，成为了医疗行业数据安全急需解决的问题。

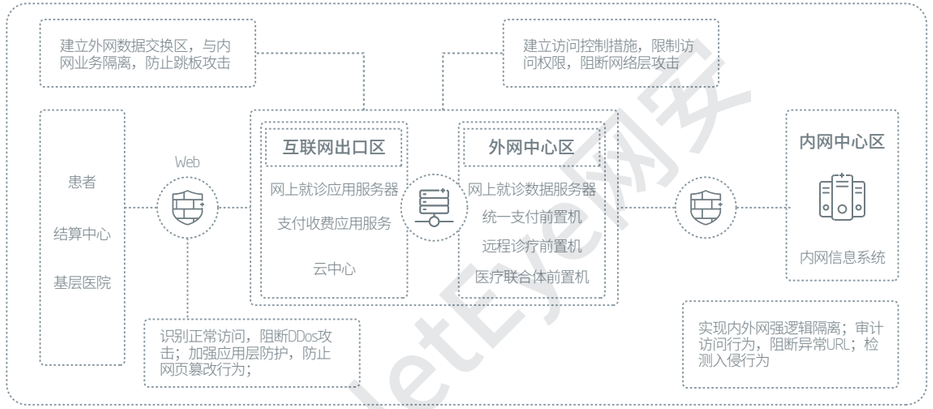
基于场景的医疗行业网络安全防护措施

基于不同场景的安全风险构建医院安全防护体系，从安全产品部署、安全策略制定、安全组织构建和安全运维四个维度思考医院安全防护体系建设，旨在为医院提供全方位、一站式的网络安全解决方案，帮助医院搭建符合实际需求、具备落地能力的网络安全防护体系。

(一)就诊场景安全防护措施

1. 传统就诊解决方案

互联网攻击多种多样，难以保证绝对安全，因此互联网防护措施宜采取多层防护，针对不同区域的业务类型的安全风险建立不同的防护措施，同时持续监控安全风险，逐渐完善的防护体系。部署图如下所示：



降低资产价值

具备条件的医院可以建立互联网交换区，单独部署互联网业务应用服务器和数据库服务器，定期将内网部分时间段的数据同步到互联网服务器中，降低对外提供的资产价值。不具备条件的医院可将前置服务器等对外提供服务的设备集中部署在前置服务区，便于内网服务器访问控制措施落实。

多级访问控制

访问控制措施是网络防护的第一步，也是最重要的一步，采取"最小必要原则"建立多级访问控制措施，保障各级服务器安全，防止病毒传播扩散。互联网用户仅允许访问互联网应用地址，互联网应用仅允许访问前置服务器。基于业务系统使用端口情况，建立访问控制白名单，仅允许前置服务器访问内网核心服务器指定端口。

多层防御措施

互联网访问量巨大，其中夹杂着众多非法访问，给医院的网络和设备带来极大的负担。因此应对访问流量进行过滤，阻断恶意访问行为。优先过滤阻断网站攻击，包括网站篡改等，维护医院形象。进行用户身份验证，防止数据盗取、网页爬虫等行为，同时对网站的连接行为进行防护，防止DDoS攻击行为导致网络拥堵，影响互联网业务开展。最后对病毒进行全面检查和过滤，防止病毒进入内网核心区域，保证内网业务稳定运行。

持续安全审计

随着黑客技术的发展和医院业务发展，不同阶段面临着不同的网络安全风险。因此应持续审计网络流量，识别可能存在的恶意行为，对恶意行为进行分析，调整安全防护策略，持续优化安全防护体系。

2. 自助终端解决方案

网络安全领域，漏洞是重点。没有漏洞，也就没有了可被攻击的弱点。但是漏洞本身并非活跃威胁，而且漏洞数量实在太多，用户难以分辨需解决什么漏洞，又该按何种顺序处理。同时，漏洞修复后是否会影响自助终端设备功能正常运行也是医疗领域一大问题。针对这些问题，可通过风险识别、诊断分析、攻击阻断、漏洞修复四个步骤做到风险可知、安全可控保证自助终端设备全生命周期安全运行，部署图如下所示。

风险识别

全面扫描自助发卡机、打印工作站、多功能一体机、挂号缴费机等各类自助终端，检查设备存在漏洞生成漏洞扫描报告，为用户提供增强网络安全性的解决方案。从结果分析来看，国外的同类产品在漏洞判断上通常会有上千条的报警，但这里面不全是真正能成功的注入点，会产生大量的噪音，给管理员带来很大的压力。自助终端防护仅报告真正意义上风险点，让管理员更能集中精力来解决问题。

诊断分析

快速识别各类网络攻击，通过智能分析发现被攻击主机、攻击类型以及被利用的漏洞。打破传统监控类平台因采集到的数据无法互相沟通、彼此关联所造成的各司其职的尴尬状况，站在运维人员关注风险变化的视角，将所有采集的数据统一整合并建立科学的时间轴前后关联分析策略，将安全监控与IT系统各种细微变化联系在一起，以至于将安全风险监控深入到每个细节。

攻击防御

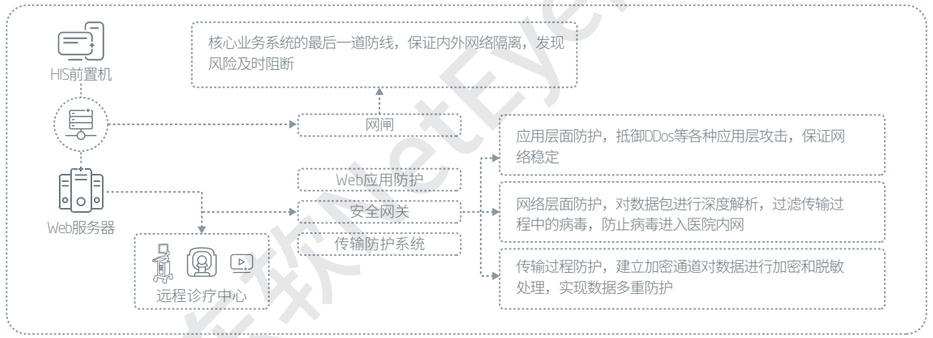
通过诊断分析结果确定被攻击主机和详细的攻击类型，攻击类型显示出基于哪种漏洞进行了攻击，发现后及时阻断攻击源头，避免病毒扩散，保证整体业务不受影响，并记录被攻击漏洞。

漏洞修复

通过机器统一下发或者人工操作的方式对所有终端设备的被利用漏洞进行修复。考虑自助终端设备的应用性，漏洞修复需要结合管理措施进行落实，其中管理措施主要包括安排专有人员与自助服务终端设备厂商进行联系，及时协调进行漏洞修复。

3. 远程医疗解决方案

远程医疗服务实现了多个医疗机构间的网络互联互通和信息共享，因此防护的核心在于保障医疗机构内网安全、防止数据泄露和保障业务的稳定性。东软NetEye结合多年的医疗行业经验从边界防护、业务保障和数据防护三个维度设计了一整套远程医疗安全解决方案。



边界防护

通过网络分区，明确不同网络区域之间的安全关系，在不同中心之间数据共享关口设置安全设备，保障网络的高扩展性、可管理性和弹性，达到了一定程度的安全性；用网闸隔离各安全区域实现阻断网络中的异常流量，应用系统间访问控制功能。

业务保障

远程医疗信息系统数据中心的出口采取防DDoS措施进行安全防护，对于进入数据中心的流量采用实时检测和清洗的方式，能够有效防御针对web、视频等远程医疗业务系统的应用DDoS攻击。

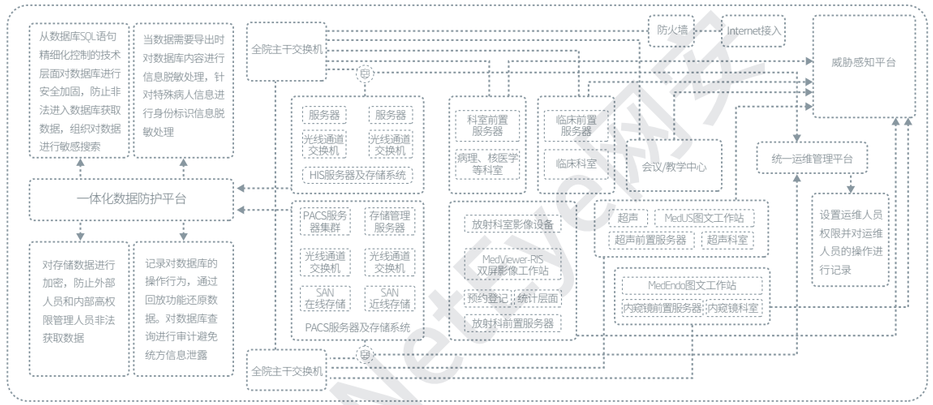
数据防护

采用符合国密标准的密码技术进行数据加密传输，保证了数据传输过程中的安全。

(二)检查场景安全防护措施

1. 全院级PACS解决方案

为保证影像设备安全运行和影像数据安全，应对影像设备传输流量进行监控，在核心数据出口处全面检测数据包及时发现并阻断异常流量，在数据存储区域建立一体化数据防护措施，全面记录数据库操作行为，及时阻断异常操作行为，对核心数据采取加密和脱敏措施防止数据泄露。



核心数据出口边界防护

在核心数据出口边界限制访问核心服务器源IP地址、访问的端口等，限制对外提供服务的核心服务器。同时对进出的数据包进行解析，识别异常数据包，包括病毒、异常脚本等，及时阻断攻击行为，保障核心数据边界安全。

数据存储区一体化防护措施

在数据存储区采取一体化防护措施，建立多层数据防护措施。对存储数据进行全库静态加密，防止拖库导致数据大面积泄露。审计数据库操作行为，针对异常登录行为、异常查询行为进行告警，防止敏感数据泄露。对临床科研、第三方机构研究等数据进行脱敏，防止患者敏感信息泄露。同时对数据库SQL等语句进行精细化控制，及时阻断数据库异常操作。

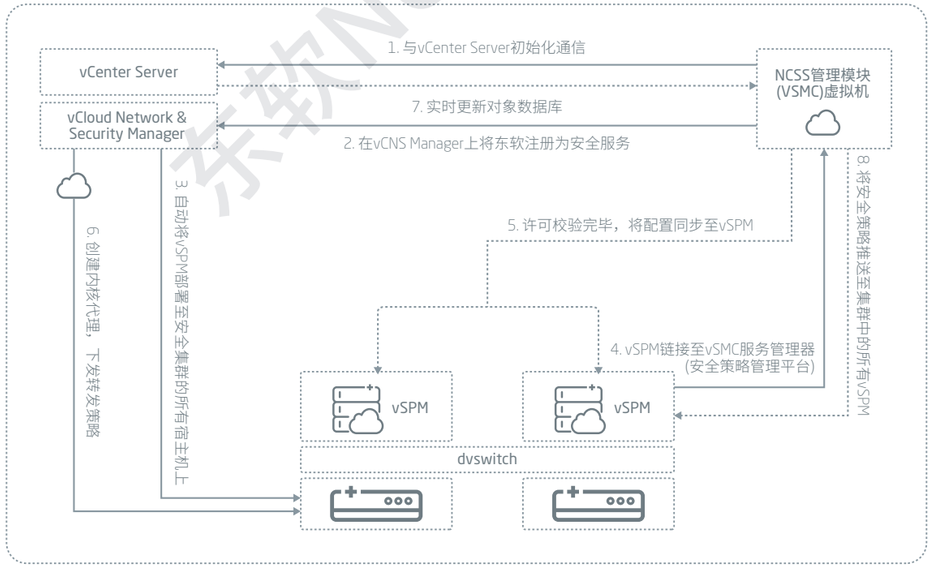
全面运维管控

威胁感知平台收集网络出口的流量，同时监控核心设备的运行状态。识别分散的攻击行为之间的关系，感知整体的网络风险，建立主动防御体系。同时通过统一运维管控平台全面识别运维人员的操作行为，防止越权访问、非法操作等异常运维行为。

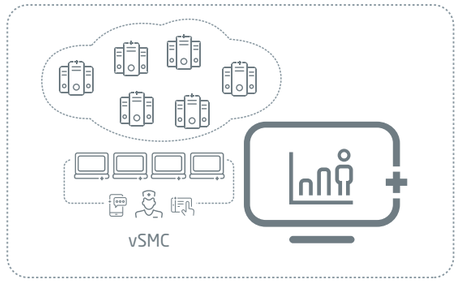
2. 企业级PACS解决方案

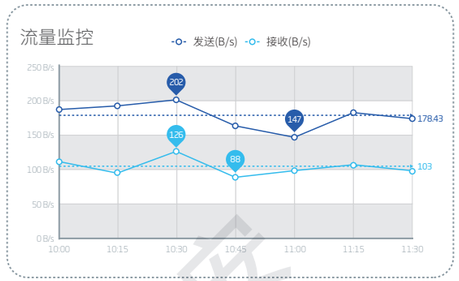
大量的医疗系统部署在了云环境中，云环境打破了传统的网络边界，病毒在不同系统间传播，不同系统间的非法访问都成为了医疗行业云环境下的安全风险。针对医疗行业云及虚拟化环境下产生的安全问题，在医疗行业的云计算中心建立内外一体化的安全防护体系，防止攻击行为在云内部各系统之间传播，同时建立负载均衡措施保证资源合理利用。

基于虚拟机的访问控制实现云内部各系统之间的流量管控，对同一VLAN下虚拟机中不同系统之间的流量进行管控。通过引流技术，将虚拟机流量牵引至虚拟安全防护模块（vSPM），发现并阻断不同系统之间异常流量的安全威胁，阻止攻击在云平台内横向蔓延，同时，综合运用DoS/DDoS攻击防御、入侵防御、应用协议识别与控制等多项安全技术。



在云内部可视化方面，通过虚拟安全管理模块（vSMC）实现云平台内部流量及应用可视化，可以细粒度的展现虚拟机的实时流量、应用排名统计、IP地址排名、系统日志、IPS日志等可视化模型。





通过管理平面与业务平面分离的架构设计，完美的支持了虚拟机在云内的迁移，实现动态实时安全防护。

为保证大量使用者对医疗行业云及虚拟化环境中业务的正常访问，通过负载均衡系统将客户端流量进行分流，对服务器端的负载进行智能调节，从而最大限度地提高服务器的工作效率。负载均衡系统通过链路探测功能，自动检测服务器的工作状态。管理员开启会话保持功能后，当负载均衡系统接收到数据流时，首先检查该数据流是否属于已建立连接的会话。如果属于已建立连接的会话，那么数据流仍将被转发到与该会话建立连接的服务器。否则，会依据管理员的配置处理。

3. 数据跨院共享解决方案

单向访问

由于不同机构的访问需求不同，需要基于业务需求建立单向访问控制措施。基层医疗机构向区县医院上传数据，区县医院不会主动访问基层医疗机构的系统，因此基层医疗机构应阻止区县医院访问其网络。基于此思路，应确保上级机构无法访问访问下级机构，保证了下级机构安全。

访问白名单

根据下级医疗机构的IP地址和需要访问的系统建立访问控制白名单。采取"最小必要原则"仅允许指定的IP访问指定系统的指定端口，保证上级医疗机构被访问的安全性。

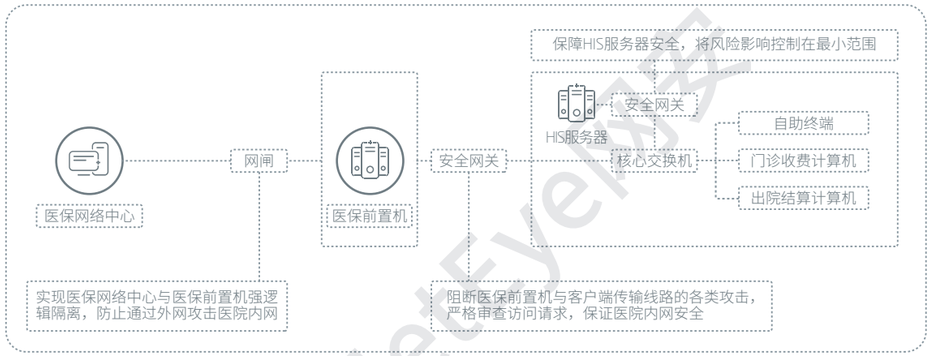
网络攻击检测

单纯的访问控制无法识别流量的安全性。因此建议在核心交换机位置部署入侵检测系统，帮助网络系统快速识别网络攻击事件，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测系统通过旁路部署模式实时获取原始网络数据包，不影响业务的正常开展，同时可以发现网络攻击、入侵、滥用等恶意行为，在提供分析证据的基础上，对可疑的访问行为进行报警。

(三)结算场景安全防护措施

1. 医保结算

在结算场景中，医院涉及与医保局进行数据传输，传输过程中网络结构的安全是网络安全的前提和基础，应根据医疗行业对外提供服务的需求对整体网络进行合理规划，在外网区与内网区之间建立安全访问路径，同时，网络平台根据实际使用情况增加外联区和安全管理区，打造对外的专属公众服务区，和对内的专属应用服务器区。



根据对外业务需要在前置服务器与外部网络数据出口处部署双向网闸实现内外网之间的"物理隔离"，在实现数据交互的同时保证攻击的一定阻断。

在医院与前置机数据出口部署入侵防御系统，识别和阻断来自外部网络的入侵行为，并通过在对外网区部署流量分析与响应系统，对网络数据的采集、分析、识别，实时动态监测信息系统的网络通信内容、网络行为和网络流量。

内网中的外联区部署入侵防御系统，识别和阻断来自外联单位网络的入侵行为，同时利用VPN技术实现与外联单位的可靠连接，保证数据交互的可靠性、有效性、保密性。

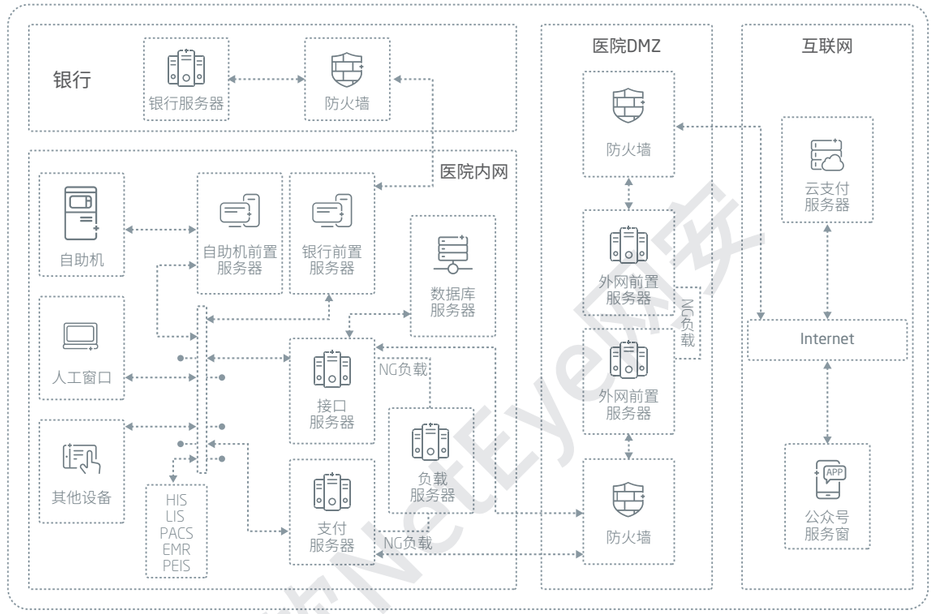
2. 第三方平台支付

网络分离

根据安全级别，将网络划分为互联网、医院外网和医院内网。互联网到医院外网采用Https协议，数据加密，保证数据传输时的安全，防火墙追加授信IP的验证。医院外网到医院内网通过网闸或防火墙将网络划分为外网区和内网区，在隔离内外网业务的环境下，实现数据的安全交换。

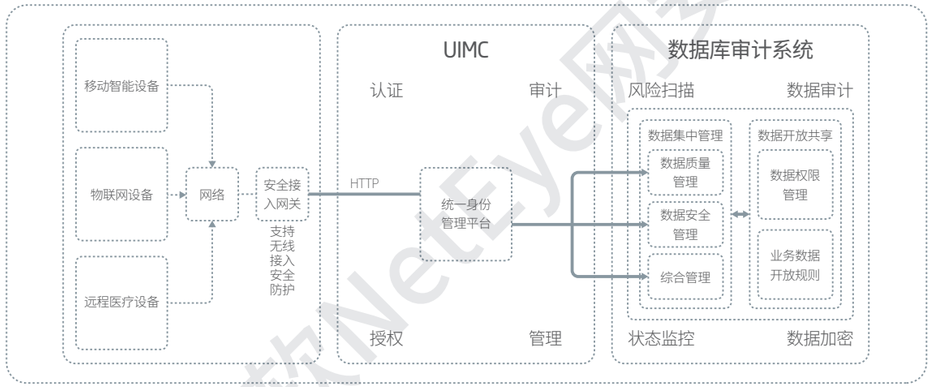
安全机制

对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，完成对医院网络流量和用户行为数据的统计、分析和报表输出。

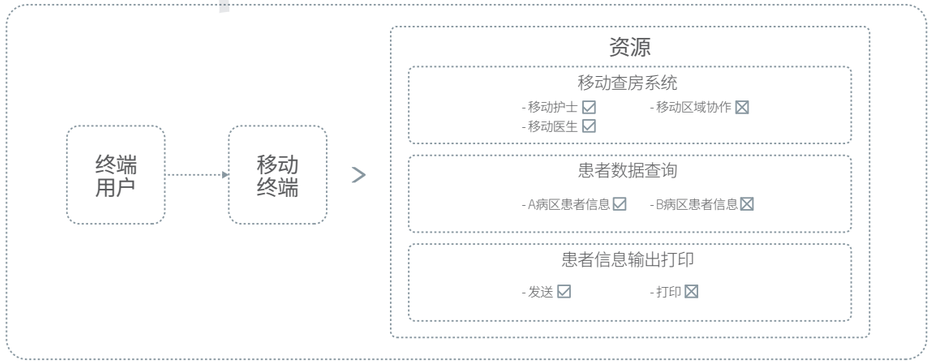


(四)住院场景安全防护措施

基于医疗行业无线安全边界增加产生的安全风险，打造具有有线和无线网络一体化防护的安全接入网关，来保证用户在移动设备进行网络访问时的安全，为用户有线/无线网络提供防病毒、反垃圾邮件、URL过滤、入侵防御和深度检测等应用级别的安全防护。针对当前流行趋势，增加Wireless功能，支持 802.11 a/b/n/g 协议，支持AP、Client、Bridge、Repeater和Router等多种工作模式，支持3G/4G移动网络接入，适用于不同的无线网络环境，并且提供无线网络环境下的各种安全防护功能，能够确保移动终端通过无线访问网络过程中的安全，同时支持与AC设备进行无缝对接，实现无线接入点的实时定位与监控。



针对大量无线手持设备的接入，为避免非法接入产生的安全风险，通过统一身份管控系统，加强移动终端的接入管理、认证、授权、审计，同时结合病人和医护人员对应关系进行无线终端的映射，避免移动终端的越权查看操作。



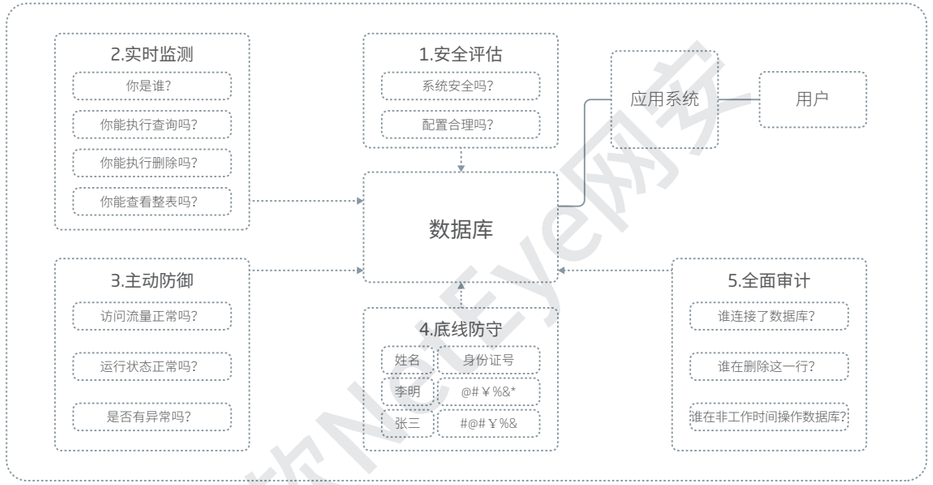
为了保证远程诊疗数据的传输可靠性、有效性、保密性，利用VPN的高效数据加密机制使远程接入更加安全可靠，同时支持多种移动终端设备实现安全、便捷的远程数据传输。

"互联网+"环境下的数据具有数据量大、种类多、实时性高的特点，这些碎片化的数据聚合后,原有数据属性将发生根本性变化，数据属性将被重新定义，所以，应加强数据的管理，对数据质量进行检查和评估，同时，提升数据安全的健壮程度，利用数据库审计系统对数据库进行风险扫描和状态监控。

"互联网+"环境下的数据开放共享的权限管理及规则面临空前难题，应结合新的数据属性进行数据分类，并根据数据的重要程度进行分级标记，依照访问角色的不同本着最小化授权原则加强数据开放共享的权限管理，同时，结合业务使用特性制定以业务数据为核心的开放规则，利用数据审计系统对不同级别的数据进行加密和审计。

(五)数据安全防护措施

结合医疗相关业务进行数据库结构设计，根据医疗药库、药房管理、药品字典维护、药品统计、非药统计、就诊信息查询等业务的运维操作特点并与普遍的医疗行业数据安全风险结合，进行深入分析，建立全面的一体化数据防护平台。为客户提供上帝视角，对数据进行全方位监控和管理。



1. 安全评估

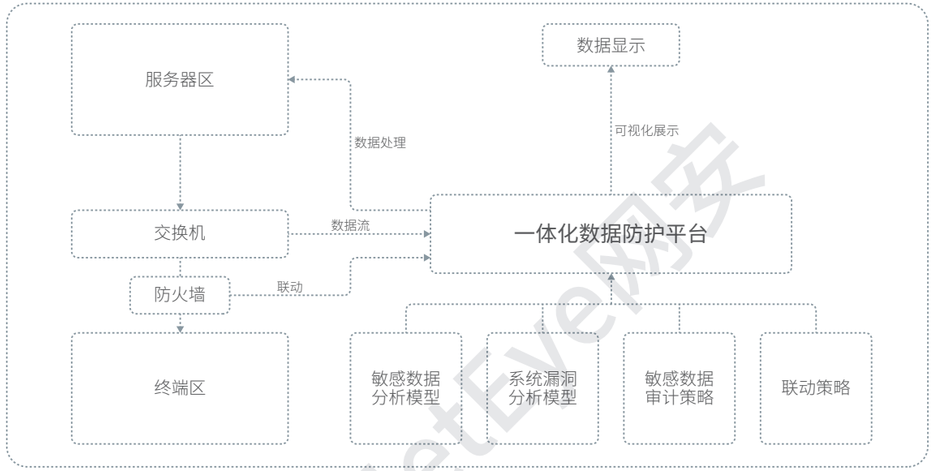
着重分析数据库的安全漏洞和缺陷配置，通过扫描工具和人工方式不定期进行数据库风险扫描，针对数据库扫描所得的弱点和漏洞，采取多种方式进行安全加固，在考虑系统稳定性的同时提升数据库自身健壮性，帮助数据库抵御外来的入侵和袭击，使数据库可以长期保持在高度可信的状态。

2. 实时监测

针对医院内外部数据的使用和运维操作行为，进行统一运维操作管理。通过账号管理、权限分配、登录认证、操作审计、账号托管等功能实现人员、账号、权限对应。摆脱传统数据安全防护手段的单一性，运用以数据监管为中心的安全运维平台，对数据流转过程中所涉及的全部信息进行统一收集，包括医院人员访问行为、操作日志、设备硬件情况、核心敏感数据调取信息等。利用关联分析技术，构建基于数据调取人物画像方法与数据操作行为分析方法。针对敏感数据的调取，实现精准定位，快速识别操作人员身份、操作时间、操作主机等信息，针对敏感数据的操作，实现及时告警和操作过程完整回现。

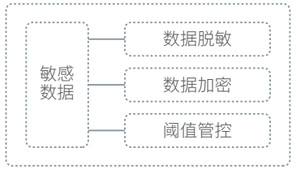
3. 主动防御

对数据流转的全过程进行检测，通过对数据传输中的源地址、目的地址、源端口、目的端口进行检查。根据数据包属性监控数据的流向，确保数据在相对安全的范围内流转，当发现敏感数据越境传输或非法传输时，将与防火墙、集成安全网关、入侵防御等访问控制类产品进行实时联动，有效阻断。



4. 底线防守

针对医疗行业底层核心数据的访问，设定固定的阈值，在固定范围内对数据进行查询和导出。当超过设定值时，主动阻断越界操作，防止拖库等数据盗取行为。数据库审计不仅仅审计指定数据对象的访问行为，而且还将通过其它技术手段进行辅助检测，防范个别内部人员通过数据库内部机制进行间接统方。



5. 全面审计

以第三方的角度观察数据操作行为，全面记录数据操作行为，包括登录方式、登录时间、操作账号、操作内容等。用户自定义筛选条件，快速定位异常操作行为，及时恢复数据，并为追责、定责提供证据。

东软NetEye
医疗行业网络安全能力

东软NetEye成立于1996年，是我国实现网络强国进程中最早的网络安全厂商之一。二十余年来，东软NetEye累积了8000余家行业客户，通过对各行业业务的深入研究，将业务与安全紧密融合，提出了东软NetEye网络安全业务安全框架，帮助客户制定描述企业组织内部和组织之间关系的企业安全架构，并根据企业安全架构灵活选择与之匹配的业务安全解决方案。

面对医疗行业，东软总结多年来的医疗行业项目经验，将医疗信息系统、医疗设备与网络安全深入融合，旨在建设符合医疗行业业务发展的安全防护体系。东软对全国多家医疗机构进行调研访谈，联合安全牛编制《医疗行业信息安全调查报告》、联合IDC编制《保障业务安全 护驾数字化企业高速发展》，参与由清华大学主导编制的《健康医疗数据安全指南》。旨在以此深入了解医疗行业客户安全需求和安全发展方向，帮助医疗行业客户解决实际的安全问题，助力客户业务稳定发展。

(一)东软NetEye医疗行业解决方案

医院业务复杂，发展迅速，面临众多的安全风险。如何建立整体的网络安全防护体系，避免重复建设，消除安全孤岛，提高医院的安全防护水平，同时在关键需求和核心风险上加强防护，成为了医院网络安全防护体系建设的难点和关键。东软NetEye对医院安全需求进行分析总结，得出医院现阶段面临的安全需求主要包括安全合规需求和业务保障需求。

1. 安全合规解决方案

从医疗行业政策和实际发展需求出发，现阶段医疗行业安全合规要求主要包括国家卫生健康委颁布的《电子病历系统功能应用水平分级评价方案和标准》、《国家医疗健康信息医院信息互联通标准化成熟度（医院信息互联互通）测评方案（2017年版）》两个评级标准和国家卫生健康委一直在推动的医院信息安全等级保护体系建设以及医院为了提高竞争力指导信息化建设进行的HIMSS电子病历评级四个方面。

各评级标准评级的侧重点不同，安全要求也不尽相同。东软NetEye深入解读评级标准，以等级保护体系为指导思想结合评级要求，制定符合业务发展与评级要求的整体防护体系，采取分阶段建设的思想，确保安全体系建设与各等级信息化建设同步。助力医疗执业单位完成各评级安全部分要求同时保障业务稳定运行。

《医院等级保护合规性方案》

2011年《卫生行业信息安全等级保护工作的指导意见》要求重要卫生信息系统安全保护等级原则上不低于第三级，包括三级甲等医院的信息系统、卫健委卫生信息平台、国家级数据中心等。《电子病历系统功能应用水平分级评价方法及标准》要求安全功能评分达到6分及以上时等级保护不低于第三级。部分地区医院等级评审明确要求二级、三级医院必须通过等保三级测评。

信息安全等级保护制度作为中国在网络安全非涉密领域的安全防护制度，是网络安全体系建设的权威指导标准。依据信息安全等级保护制度可以建立全面的网络安全防护体系，阻断安全风险，因此等级保护标准是医院网络安全建设的基础。东软NetEye深入解读等级保护体系，编制的《医院等级保护合规性方案》，在满足等级保护建设的基础上参考等保2.0的建设要求和医疗行业的业务属性，为医院建设基础的全面的网络安全防护体系。

项目	序号	类别	数量	备注
安全技术建设	1	安全集成网关	2	部署在服务器边界区域，完成安全隔离工作
	2	防火墙	1	隔离安全管理区和核心交换区
	3	入侵检测系统	1	部署于核心交换区，完成入侵检测发现功能
	4	日志审计系统	1	部署于安全管理区，完成全网的统一日志收集和分析功能
	5	运维审计堡垒机	1	部署于安全管理域，完成对各类主机、网络设备等资产的人员授权与审计功能
	6	漏洞扫描	1	部署于安全管理域，完成对全网资产漏洞脆弱性的评估
	7	网闸	1	部署于外联区域对网络进行隔离，有利于后续其他单位外联网络接入
	8	终端准入管理系统	1	部署于核心交换区域，实现对终端准入的控制
	9	准入服务器	1	
	10	备用数据库服务器	1	

《电子病历系统功能应用水平分级评级方法和标准合规性解决方案》

2011年由国家卫健委医政医管局发布，在2018年得到大力推广，要求二级以上医院要全部按时参加分级评价工作。到2019年，辖区内所有三级医院要达到电子病历应用水平分级评价3级以上，即实现医院内不同部门间数据交换；到2020年，要达到分级评价4级以上，即医院内实现全院信息共享，并具备医疗决策支持功能。《电子病历系统功能应用水平分级评级方法和标准》更符合中国的医疗行业现状和发展需求，从信息化覆盖程度进行分级，包括单机阶段、部门内部信息互联互通、部门间信息互联互通、全院信息互联互通等等，共涉及9个等级，10个角色，39个评价项目，并且明确提出了基础设施与安全管控的评价要求。

《电子病历系统功能应用水平分级评级方法和标准合规性解决方案》从信息化覆盖程度出发，将评级要求与等级保护要求进行融合。站在全局的角度围绕医院信息系统闭环和使用，制定完整的安全防护体系。同时深入分析各级别信息化建设的内容，区分不同阶段的网络安全风险，并结合标准中的安全管控要求为每个定级制定安全防护措施并保障防护措施的落实。

评价内容 / 功能评分	物理安全	网络安全	主机安全	应用安全	数据安全
0分	--	--	--	--	--
1分	--	--	计算机防病毒	--	--
2分	--	部门级局域网	服务器防病毒	--	--
3分	服务器专用房间	局域网部门间互联互通	计算机、硬件管理制度	--	--
4分	独立的信息机房	局域网全院联通 网络管理制度	服务器独立安全防护区域	--	--
5分	机房、设备和配线架标识	划分不同业务独立网络区域 无线局域网安全接入	--	--	--
6分	信息机房具备不间断 电源、空调、消防设施	物联网设备安全 接入局域网 防止设备非法外联	关键网络设备、链路冗余设计，核心设备无单点故障	时间戳及守时系统	--
7分	B级机房要求 局域网布线 符合GB50311要求	--	电子病历系统核心硬件 设备集中监控、报警 网络设备及服务器操作审计	电子病历系统核心软件 集中监控、报警	集中管理日志，保留 时间不低于六个月
8分	--	内网与区域健康网络连接 互联网安全传输通道	--	互联网业务的信息系统	--

重要信息安全等级保护不低于第三级

《国家医疗健康信息医院信息互联互通标准化成熟度测评解决方案》

《关于促进"互联网+医疗健康"发展的意见》（国办发[2018]26号）提出二级以上医院要健全医院信息平台功能，整合院内各类系统资源，提升医院管理效率。三级医院要在2020年前实现院内各诊疗环节信息互联互通，达到医院信息互联互通标准化成熟度测评4级水平。互联互通作为医疗行业资源整合的关键，从医院和医疗执业单位两个角度出发。医院互联互通以患者为中心，实现数据标准化、信息系统连通、与其他机构连通，最终达到医院内部流程信息化闭环，实现信息的互联互通。

东软NetEye从互联互通的角度出发，考虑信息化格局变化后的网络安全风险，并结合互联互通在基础设施建设方面的标准，提出了互联互通的整体解决方案。互联互通安全防护应从两方面进行，一方面实现医院互联互通后在网络边界的安全防护保证医院内部网络和核心系统的安全，另一方面从数据角度考虑互联互通后的数据使用安全。

《HIMSS电子病历应用模型合规性解决方案》

2006年美国医疗信息和管理系统协会（HIMSS）提出病历系统概念以及系统构成，为国内电子病历发展提供参考。2009-2010年国务院、卫生部相继发文推进医院信息化建设，明确以电子病历为医院信息化工作重点。由此，电子病历系统进入由政府推动的快速发展期。HIMSS电子病历应用模型包括门诊和住院两个部分，共7级。HIMSS是基于系统的重要程度进行建设和评级，并在每一级提出了网络安全需求，因此应结合不同等级建设的系统进行网络安全建设，保证网络安全建设与信息化建设同步，逐渐完善最终形成整体的网络安全防护体系。

HIMSS Analytics EMRAM（住院急诊）电子病历应用模型	
级别	电子病历应用模型累积能力要求
7级	全面的电子病历；外部健康信息交换；数据分析能力，灾备，治理，隐私与安全
6级	基于技术手段的用药、输血和母乳闭环；风险评估与报告
5级	医生文书，含结构模板；入侵监测、设备防护
4级	电子医嘱，含临床决策支持（CDS）功能；护理和辅助科室文书；基本业务连续性
3级	护理和辅助科室文书；电子用药记录（eMAR）；基于角色的信息安全
2级	临床数据中心（CDR）；内部互操作性；基本信息安全
1级	3个主要医技科室系统全部上线，包括检验科、药房和放射科系统；放射和心脏放射PACS；非DICOM格式影像存储
0级	3个主要医技科室系统部分或全部未上线

2. 业务保障解决方案

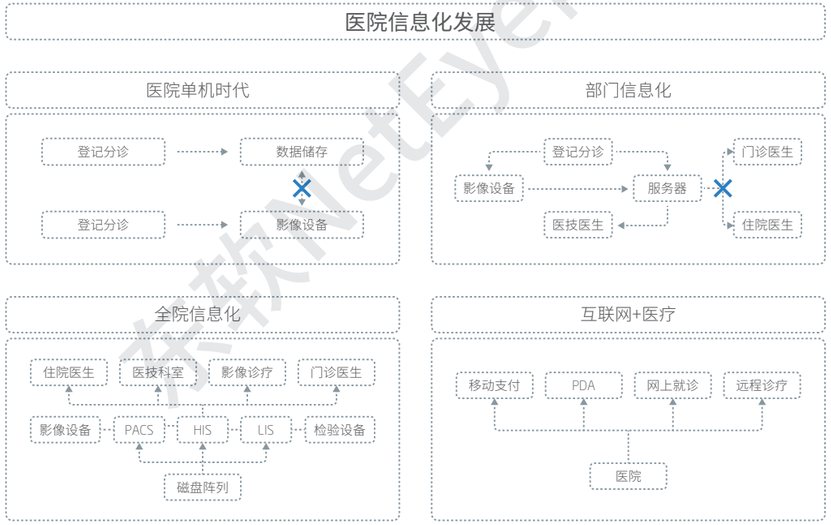
医疗行业信息化经历了不同阶段同时导致了业务形态的改变，而在不同的信息化发展阶段和不同的业务形态上都呈现出来不同的安全风险。同时由于各等级各区域医院的信息化建设程度存在较大差异，因此东软NetEye提供了全面的医院业务安全解决方案，旨在帮助不同阶段的客户解决不同的安全问题。

《新时代下医疗业务安全》

医院信息化建设的方向由于地域、需求等因素导致医院信息化程度和建设方向存在极大的差异。即使近几年卫健委发布了众多标准引导医院的信息化建设方向，但由于系统历史原因，仍然存在差别，因此医院面临的安全风险也存在极大的差异。《新时代下医疗业务安全》结合东软NeyEye多年的医疗行业经验累积，从就诊、检查、住院、结算场景出发，全面分析医院所有可能面临的安全风险并结合医院的业务优先级和实际情况制定解决方案。通过比对的方式帮助用户识别自身的安全风险。

《医院网络安全解决方案》

不是所有的安全风险都是核心安全风险，因此并不是所有的安全风险都需要解决。东软NetEye结合多年医疗行业项目经验对医院的业务场景和安全风险进行了提炼，总结了医院核心业务需求、安全风险、防护的原则和解决方案。



《分级诊疗解决方案》

分级诊疗是医疗行业着重推动的业务。以医共体、医联体建设为主要抓手。建设医共体将基层医疗机构整合实现区县医院资源下沉，整体提高乡镇卫生院医疗水平。建设医联体实现大型医疗机构联通，实现大型医疗机构的资源下沉和医联体内部的资源共享。《分级诊疗解决方案》站在主导医院的角度考虑整体安全建设，根据开展业务形态制定防护措施，确保各医疗机构网络边界安全和接入安全，考虑数据流通过程中的完整性、可用性和保密性。

(二)东软NetEye安全资质

网络安全是业务稳定运行的保障，可信赖的网络安全厂商为客户提供更可靠的安全产品和更专业的安全服务。东软为全国众多的医疗机构提供安全产品和服务，是网络安全体系建设中可信赖的网络安全厂商。

国家密码管理局
- 商用密码产品生产定点单位证书
- 商用密码产品技术鉴定证书
- 商用密码产品销售许可证

工业和信息化部省软件认定办公室
- 软件产品登记证书

国家保密局
- 涉密信息系统集成证书
（系统集成/软件开发/运行维护)(甲级)

中国信息安全认证中心
- 中国国家信息安全产品认证证书
- 信息安全服务资质认证证书 应急处理资质
- 信息安全风险评估服务资质
- 信息安全服务资质认证证书
信息系统安全集成服务资质

中国人民解放军信息安全测评认证中心
- 军用信息安全产品认证证书

国家版权局
- 产品著作权登记证书

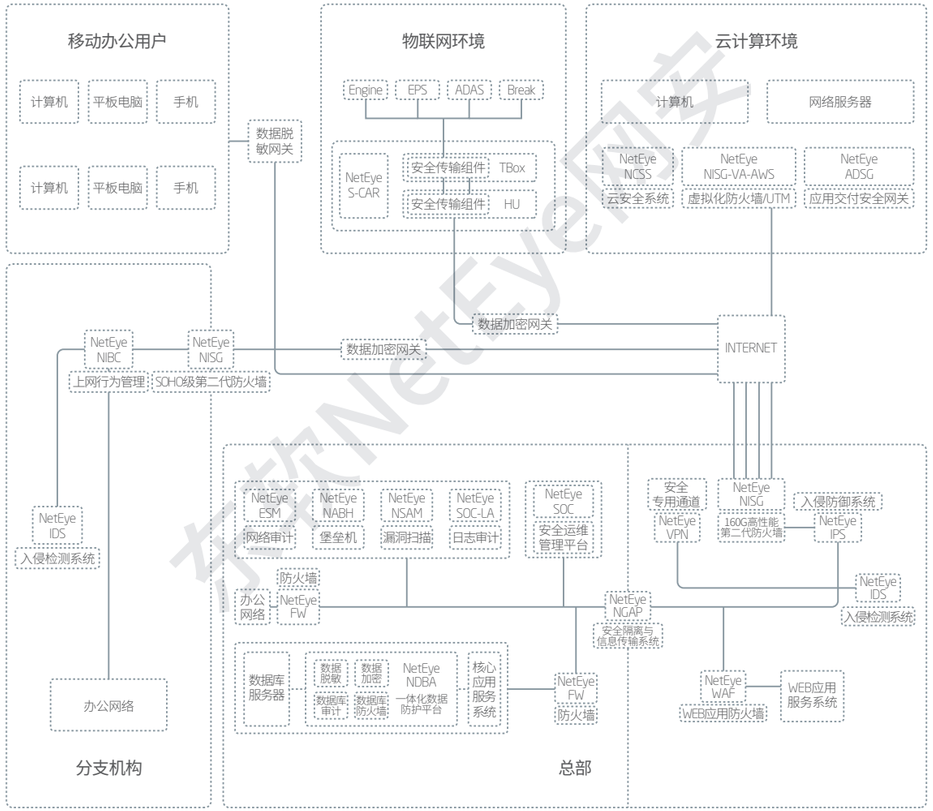
中国信息安全测评中心
- 国家信息安全认证产品认证证书EAL3+级
- 国家信息安全测评信息技术产品自主原创测评证书
- 国家信息安全测评信息安全服务资质证书(安全开发类)
- 国家信息安全测评信息安全服务资质证书(安全工程类)
- 国家信息安全测评授权培训机构(注册信息安全人员培训机构)

国家保密科技评测中心
- 涉密信息系统产品检测证书

中华人民共和国公安部
- 计算机信息系统安全专用产品销售许可证
- 信息安全等级保护安全建设服务机构

(三)东软NetEye安全产品

网络安全产品是网络安全体系落实必不可少的一部分，稳定可靠的安全产品可以保障业务顺利开展，减少运维人员工作负担。东软NetEye自1996年开始研发并生产网络安全产品，为客户提供全方位的网络安全产品，帮助客户建设和完善安全防护体系。



访问控制类

- NetEye防火墙（FW-X86、龙芯、飞腾、兆芯）
- NetEye入侵防御系统（NISG-IPS-X86、龙芯、飞腾、兆芯）
- NetEye集成安全网关（NISG）
- NetEye智晟系列下一代防火墙
- NetEye VPN网关系统（VPN）
- NetEye Web应用防火墙（WAF）
- NetEye上网行为管理（NIBC）
- NetEye安全隔离与信息传输系统（NGAP）
- NetEye业务安全网关
- NetEye基于物联网环境的车联网安全系统（S-CAR）
- NetEye基于业务场景的业务安全网关（ElvaEye）
- NetEye基于云环境的虚拟化安全网关（NISG-VA）
- NetEye基于云环境的应用交付安全网关（ADSG）
- NetEye基于云环境的云安全系统（NCSS）

检测审计类

- NetEye入侵检测系统（IDS-X86、飞腾、龙芯、兆芯）
- NetEye数据库审计系统（NDBA-X86、飞腾）
- NetEye网络审计系统（ESM）
- NetEye安全评估和检测系统（NSAM）
- NetEye日志审计系统（SOC-LA）
- NetEye统一身份管理系统（NABH）

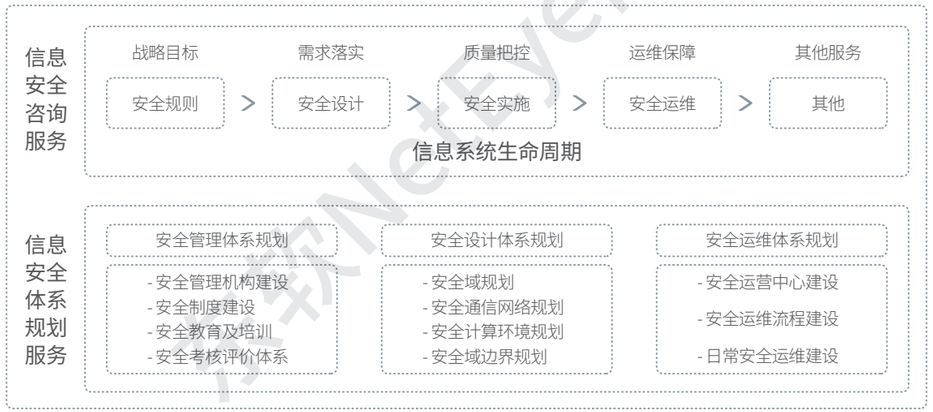
运维管理类

- NetEye安全运维平台系统（SOC）
- NetEye安全服务（NSS）
- NetEye安全运维平台系统（SOC-支持涉密专用服务器）

(四)东软NetEye安全服务

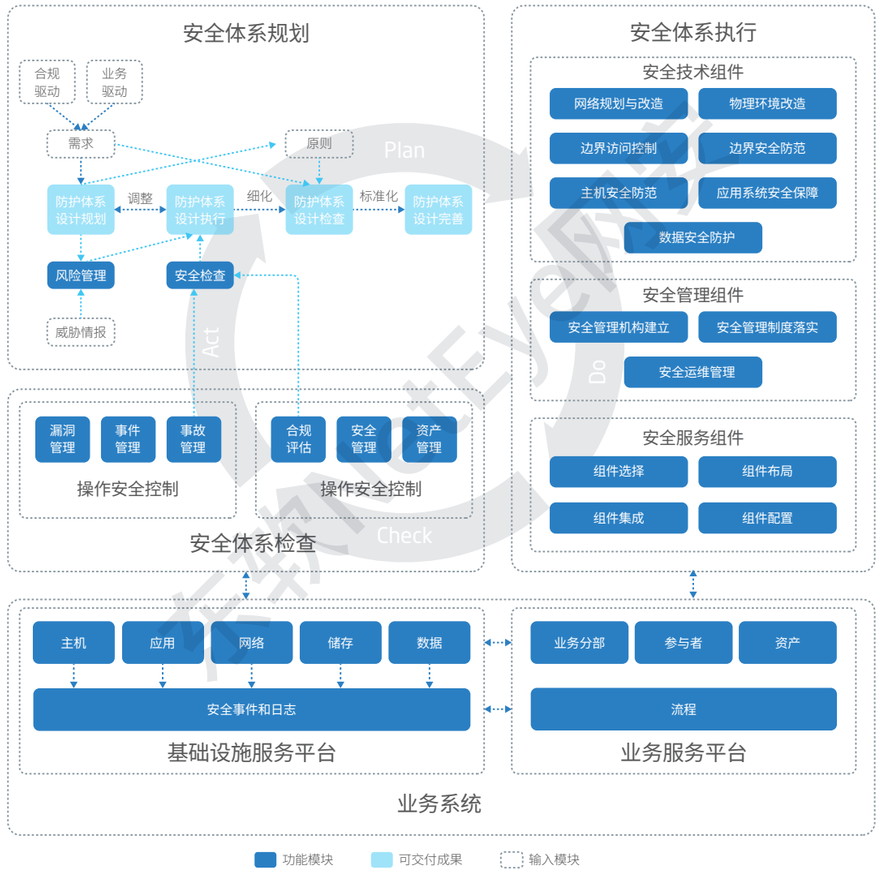
东软NetEye站在业务的角度考虑，认为制定完善的网络安全解决方案只是网络安全防护体系建设的第一步，如何将网络安全解决方案落地，保证网络安全和业务的平衡，如何持续完善网络安全防护体系，保证网络安全防护体系与业务发展的同步，是网络安全防护体系建设的关键。

东软NetEye通过全面专业的服务为医疗行业信息安全从业者赋能。通过信息安全咨询服务为医院网络安全管理者赋能，提供网络安全防护体系建设的建议，使医院网络安全管理者可以制定符合其安全需求的网络安全防护体系和长期的医院网络安全规划。通过信息安全体系规划服务为医院网络安全实施人员和服务提供商赋能，指导其识别日常的网络安全风险，落实和完善网络安全防护措施，提高安全体系运维效率。



以等保体系为中心构建有效可执行的医院安全防护体系是典型的信息安全服务方案，从咨询服务和规划服务的角度，落实等级保护体系，建立符合医院实际需求，能够解决医院安全问题的典型的信息安全防护体系。

以等保体系为中心构建有效可执行的医院安全防护体系，利用东软业务驱动安全模型建立完善的安全体系执行流程，通过信息调研、人员检查、漏洞扫描等方式识别网络中的安全风险，输出风险识别报告和差距分析报告。以此为依据设计全面防护重点加强的等级保护防护体系，通过安全产品选择、策略配置、管理制度建立、管理机构建立落实防护体系。最后通过定期的安全检查和持续运维不断完善安全防护体系，使其与信息化发展和业务发展同步，调整安全防护体系修复安全漏洞。



东软NetEye
医疗行业典型案例

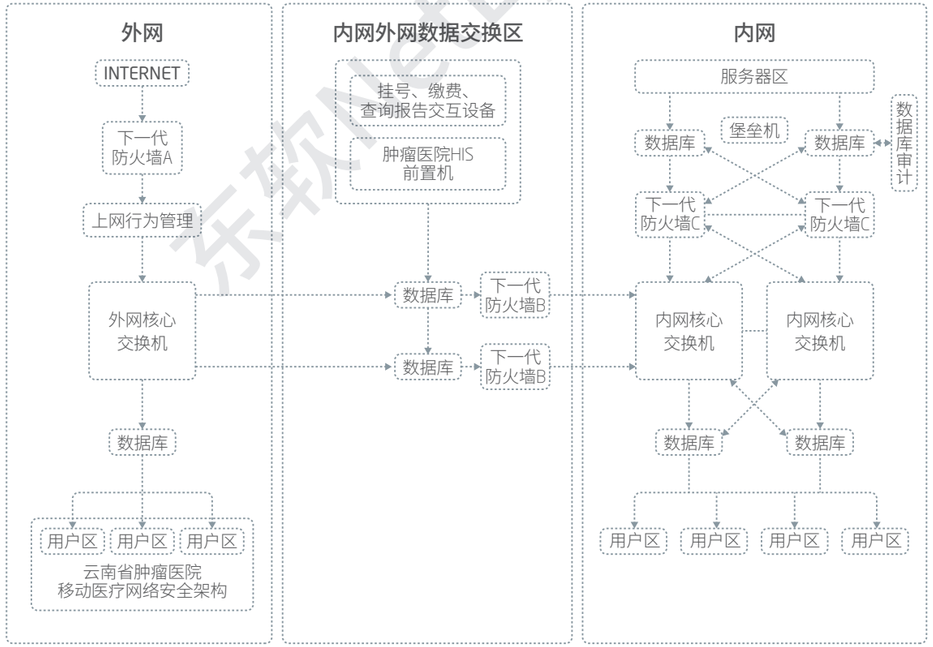
(一)云南省肿瘤医院

1. 项目背景

2009年，为了保证医院业务安全，云南省肿瘤医院实现了内外网物理隔离，内网作为医院的业务网络，使用HIS、LIS、PACS、EMR等业务系统；外网主要访问互联网、内外网是两张完全独立的网络。在2014年云南省肿瘤医院率先上线了支付宝"未来医院"项目、微信移动医疗患者服务平台，向移动互联网时代医院患者平台迈出了具有里程碑意义的第一步。但在利用微信、支付宝支付方新IT环境下，基于业务需求，内外网必须有数据交互，因此，原有的安全防护机制已经无法适应新的IT部署环境，基于业务需求带来的安全挑战出现了。

2. 解决方案

东软网络安全团队通过对新业务需求的深入分析，与云南省肿瘤医院共同构建出安全保障的七道防线：边界安全防护、应用行为防护、Web应用防护、关键路径防护、核心区域防护、数据安全防护和管理安全防护，如下图所示：



第一道防护：边界安全

实现互联网边界防护，通过NAT、IP策略、访问控制策略、轻量级的防病毒、WAF、IPS功能保障业务系统的边界安全。

第二道防护：应用行为防护

通过深度包检测和深度状态检测技术，对全网PC进行互联网行为管控，保障网络应用行为级的安全和审计。

第三道防护：Web应用防护

通过WAF，保护移动互联网医院对外发布的EB站点的安全，同时进行实时监控。

第四道防护：关键路径防护

针对WAF与内网核心交换机之间的重要路径，通过IPS、WAF、DLP数据防泄漏等安全策略加强防护并实时监测。

第五道防护：核心区域防护

在内网核心交换机与服务器交换机之间，通过IPS、WAF、DLP数据防泄漏、应用控制等安全策略加强防护并实时监测。

第六道防护：数据安全防护

在服务器区实时记录网络上的数据库活动，对数据库访问行为严格管控，检测并防范内外部对数据库的入侵。

第七道防护：管理安全防护

在服务器区，通过堡垒机加强内外部在运维层面的管理，防患于未然。

3. 价值体现

云南省肿瘤医院网络安全建设是院方基于自身业务的变化而制定的，通过缜密测试、反复验证后选择了安全服务提供商及所需的安全产品，其价值如下：

业务需求驱动的安全建设降低安全防护的TCO

云南省肿瘤医院的网络安全建设是围绕业务发展而持续更新的，与大而全的网络安全解决方案相比，围绕业务需求，因地制宜的设计、评估、建设使得医院在安全方面的投入恰如其分。

为医院数字化转型提供有力保障

实现移动支付是云南省肿瘤医院数字化转型进程的重要里程碑，采取微信、支付宝等支付方式提升了医院的运营效率，缩短了患者的就诊时间。数字化转型打破了原有的内外网物理隔离的网络架构，会给医院网络带来极大的安全风险。在2017年WannaCry勒索病毒大规模爆发的时候，很多医疗机构不幸感染病毒，而云南省肿瘤医院在勒索病毒爆发之前，就已经将勒索病毒传播的443端口封堵，并且在事发前两个月就通过内外补丁服务器将勒索病毒对应的补丁推送到了服务器。

(二)上海曙光医院

1. 项目背景

上海曙光医院是一个信息和技术密集型的行业客户，其信息网络满足高效的内部自动化办公同时需保证对外界的通讯畅通，同时因为医院信息系统访问人员复杂，所以保证医院网络系统中的数据安全问题尤为重要，信息安全建设重要性不容忽视。便捷、开放的网络环境，是医院信息化建设的基础，在数据传递和共享的过程当中，数据的安全性要切实地得到保障，才能保障医院信息化业务的正常运行。以医院的HIS、LIS、RIS、PACS、体检、临床路径、心电图系统等信息系统的现有基础设施为基础，建设并完成满足等级保护三级系统基本要求的信息系统，确保整体信息化建设符合相关要求并迈向新的台阶。

2. 解决方案

东软NetEye为落实卫生部《卫生行业信息安全等级保护工作的指导意见》，维护医院信息安全保障和促进医院信息化建设的健康发展，依照国家《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等标准，以及医院对信息系统等级保护工作的有关规定和要求，协助并参与医院信息安全等级保护建设：

- **协助医院按信息系统编制了定级报告和定级备案表、提交定级材料备案。**
- **对照差距分析，制定整改方案，提供整改措施，通过产品部署及服务协助医院完成等级保护技术体系建设。**
- **建立健全信息系统安全管理制度，根据信息安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。**
- **制定保障医疗活动不中断的应急预案。按可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保医疗活动持续进行。**
- **为医院信息化技术人员提供信息安全相关专业技术知识培训，满足安全运维的基本需要。**

3. 价值体现

东软NetEye医院信息系统安全等级保护整体解决方案，满足物理安全、网络安全、主机安全、应用安全、数据安全五个方面的基本技术要求；满足安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个方面制定基本管理要求。通过上述两个方面的建设使得医院信息系统最终既可以满足等级保护的相关要求，又能够全方位为医院的业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

(三)河北省人民医院

1. 项目背景

河北省人民医院为了提高医院的管理与业务工作水平,提高信息安全保障能力和防护水平，建立面向医院、面向社会公众和患者、面向卫生行政部门的高效、快捷、方便、优质的医疗卫生信息共享与服务体系，充分利用医疗卫生资源，利用信息化的战略先进性，努力提高河北省人民群众的健康水平，启动了医院网络安全建设工程。

医院考虑到自身的应用和硬件储备量、设备处理能力以及如何最大化节省成本等运营战略。对硬件资源规划资源池，进行动态的统筹划分，以便发挥现有硬件整体效能的同时保证虚拟化安全防护且满足合规性要求。

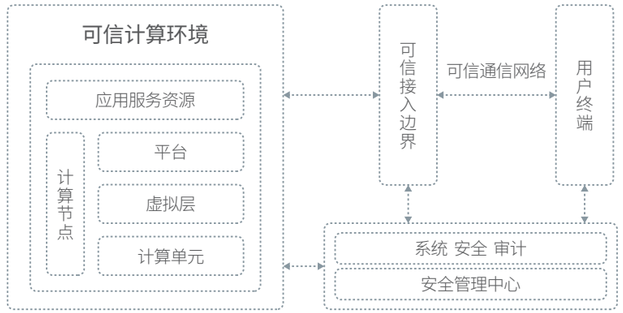
2. 解决方案

虚拟化的广泛应用打破了传统数据中心基础支撑环境模式，越来越多的医院已经搭建私有虚拟化环境。针对传统的安全技术手段已不适应虚拟化的环境，数据中心中基础虚拟化平台作为数据中心的支撑，需保护虚拟化技术的安全性、虚拟化操作系统的安全性、虚拟机的安全性以及整个虚拟化平台的完整性，需要通过安全技术手段对虚拟化平台的非法入侵、篡改、资源非法调用、资源非法消耗、虚拟机文件安全、Hypervisor层安全进行综合安全防护。

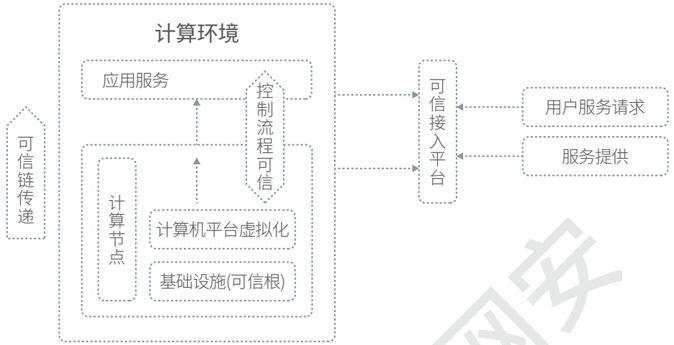
IT信息化中心由传统的环境向虚拟化环境迁移，应用系统数据依然是最核心的资产，同时虚拟化平台自身的数据库、操作系统数据、虚拟机文件等也要适用于等级保护的技术要求，对于数据完整性、保密性以及数据的备份与恢复同样也要遵循等级保护的的相应技术要求。

虚拟化技术是指计算元件在虚拟的基础上而不是真实的基础上运行，它可以扩大硬件的容量，简化软件的重新配置过程，减少软件虚拟机相关开销和支持更广泛的操作系统。计算系统虚拟化是一切服务与应用的基础。

虚拟化环境的安全保护策略：按照1个“安全管理中心”支持下的“计算环境”、“区域边界”、“通信网络”的3重防御体系实施方案。

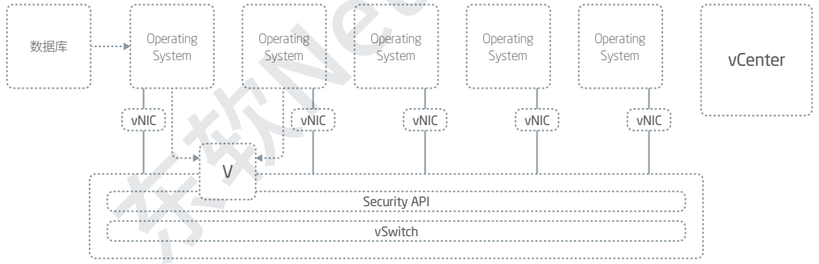


虚拟化环境安全建设要点包括：整体安全、环境内部共享、互联机制安全、环境资源访问控制等，从基础设施可信出发，度量基础设施、计算平台，验证虚拟计算资源可信，支持应用服务的可信来确保计算环境可信。



南北向流量安全防护

虚拟防火墙就是完全运行于虚拟环境下的防火墙，与主机防火墙概念是相对立的。它如同一台虚拟机，一般运行于虚拟机监控器中，对虚拟机网络中的数据包进行过滤和监控。它可以是主机中的一个内核进程，也可以是一个带有安全功能的虚拟交换机。



东西向流量安全防护

NCSS云安全系统是以软件的形式部署，安装在VMware虚拟机内，无需占用机柜空间，实现云平台内部业务系统之间、虚拟机之间的安全防护、威胁检测与隔离。

3. 价值体现

虚拟化为用户提供便捷服务和良好用户体验同时也暴露出一些安全风险，东软NetEye网络安全整体解决方案可解决主要的安全风险包括：数据泄露、数据丢失、账户或服务流量劫持、不安全的接口API、拒绝服务、恶意的内部人员、云服务的滥用、不够充分的审查和共享漏洞等。在得到国家层面的相关安全标准及法律法规支撑的同时有效应用安全技术，解决安全问题，才能更好的完善信息安全防护。

(四)四川省人民医院

1. 项目背景

四川省人民医院信息网络建设起步早，体系相对完善。为了充分利用已有的安全设备，减少安全事件发生，保障信息系统正常运行，深入评估信息系统的安全现状，根据信息系统的安全防护现状与国家等级保护要求之间的差距，确定等级保护安全建设需求。从而更好的提升网络安全保障高效性，为医院业务提供更卓越的信息支撑价值。

2. 解决方案

协助医院完成设备的选型、采购、安装、策略配置等规划建设工作，采用渗透测试、安全加固等技术和服务手段，协助医院搭建完善的技术防护系统和安全管理体系，保障重要核心业务系统等信息系统的安全稳定运行。

咨询服务

按照上级主管部门相关指导性文件，结合各信息系统实际应用状况，梳理策略并收集分析文档资料。

安全风险评估服务

通过调研信息系统相关数据和属性并从整个系统服务来分析各业务系统所承载业务的业务类型和服务对象，以及网络覆盖范围和网络性质，有针对性的对网络、主机、应用安全等层面进行评估。

安全整改加固服务

制定安全加固实施方案和安全整改实施方案，通过合理的人员和工期安排，实施整改内容和部署新增设备，优化整体安全策略，梳理管理体系。

应急响应服务

应急响应服务是应对突发和重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。东软NetEye在服务期间提供现场或远程的服务，并在重大敏感时间提供现场的值守与应急处理，应急小组在接到应急请求时，立即启动应急服务流程进行应急。

3. 价值体现

安全保障体系是一个技术、管理、服务及相关支撑平台相结合的综合保障体系。其中技术保障体系是核心，涉及安全技术开发，安全系统应用，构建综合防护系统等问题。运行管理体系是关键，包括人员管理、技术管理和风险管理等内容。服务体系由安全管理服务、安全测评服务、应急响应服务和安全教育培训等构成。四川省人民医院在如何保障医院信息数据机密性、完整性、可用性、可控性和不可否认性等方面建立了完善的安全体系、系统、策略、流程制度及工作措施。

东软NetEye安全服务解决方案以层次化的网络系统作为支撑平台，使各种信息安全技术功能合理地作用在网络系统的各个层次上，从技术和管理上保证安全策略得以完整准确地实现，安全需求得以满足。

东软NetEye
医疗行业客户名录

东软NetEye医疗行业客户名录

中日友好医院	中国人民解放军第305医院
北京医院	浙江医科大学第一附属医院
四川省人民医院	上海中医药大学附属曙光医院
苏州市第一人民医院	华中科技大学同济医学院附属同济医院
天津市第一中心医院	武汉大学中南医院
北京大学首钢医院	上海市第五人民医院
沈阳市第五人民医院	陕西省第四人民医院
中山大学附属第一医院	山东省肿瘤医院
太原市阳曲县人民医院	云南省第一人民医院
武汉市结核病医院	青海省第五人民医院
绍兴市第六人民医院	西安交通大学第一医院
银川市第一人民医院	西安市第四医院
韶关市第一人民医院	重庆儿科医院
新疆克拉玛依市中心医院	武汉市儿童医院
烟台市中医医院	渭南市第二人民医院
昆明医学院第一附属医院	襄樊市中心医院
山西医科大附属第二医院	山西省运城市中心医院
山东省千佛山医院	无锡市第七人民医院
义乌市中医院	济宁市第一人民医院
济南千佛山医院	济宁医学院附属医院
合肥市105医院	广西中医学院第一附属医院
贵州省黔西南州人民医院	桂林医学院附属医院
广西梧州市工人医院	广东省农垦中心医院
齐齐哈尔中医院	河北省人民医院
青岛市第七人民医院	喀什地区第一人民医院
山东省妇产医院	连云港第一人民医院

九江市第一人民医院	邯郸市第一医院
海南医学院附属医院	邯郸市中医院
河北医科大学第三医院	重庆市西南医院
普洱市中医院	黑龙江省医院道外分院
黔西南州人民医院	东南大学附属中大医院
垫江县中医院（重庆）	山西省煤炭中心医院
黑龙江省农垦红星隆管理局中心医院	广东省韶关市铁路医院
湖州吴兴区人民医院	齐齐哈尔医学院附属第一医院
临沂市肿瘤医院	阳泉市第一人民医院
邯郸市第一医院	桂林医学院附属医院
南京市溧水区中医院	黑龙江双鸭山煤炭总医院
上海市闵行区吴泾医院	宽甸满族自治县中心医院
临沂市人民医院	七台河市人民医院
青岛大学附属医院	包钢职工医院
黑龙江省医院道外分院	浙江省台州医院
砀山县人民医院	浙江省口腔医院
铜川市人民医院	阳泉市第一人民医院
海宁康华医院	六安市世立医院
商都县医院	银川市第一人民医院
伊犁哈萨克自治州奎屯医院	安徽省太和县人民医院
徐州市铜山区中医院	宜昌市第二人民医院
东山县医院	商河县人民医院
保定京南医院	唐山市曹妃甸区医院
内江市市中区人民医院	吴忠市红寺堡区人民医院
深圳市龙城医院	富阳中西药结合医院