后疫情时代
医疗卫生网络安全
白皮书

HIT专家网
WWW.HIT180.COM

安恒信息
DAS-Security 安全中国

序

今年1月5日18:48，我在微信朋友圈发出：办公室繁忙工作间隙，因为专业身份而对一直关心的第三故乡武汉的疫情写几句；1、有关信息表明，应该是一种新的冠状病毒，且与SARS、BAT冠状病毒同源性都较高……

过去的四个月，全国上下，众志成城，与时间赛跑，让世界一次次见证中国速度、中国规模、中国效率！

过去的20年，是信息科技与通信技术发展最快的20年，也是我国从信息、通讯科技的落后者到跟随者，再逐渐实现弯道超车的20年。与此对应，我国各级医院的信息化应用意识和水平，也一直在快速提升。我清楚记得，2001年1月2日到杭州市拱墅区卫生局担任局领导，主抓的第一件事就是“升级全区所有医院信息系统，实现接入医保”。

业内人士一般认为，我国医疗信息化大致可以归纳为三个阶段：即HIS（医院信息系统）建设阶段、CIS（临床信息系统建设阶段）和数据整合阶段。伴随着近二十年的医院医疗改革创新，我国医疗信息化总体上第一阶段已经走完，目前基本处于第二阶段；部分发达地区和先进医院，已激情满怀迈入第三阶段。

近期出台的与疫情防控相关政策中，“医疗信息化”内容频频出现。国家卫建委连续发布“加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知”和“在疫情防控中做好互联网诊疗咨询服务工作的通知”，要求体制内外医疗机构大力开展互联网诊疗服务；国务院印发《关于开展线上服务进一步加强湖北疫情防控工作的通知》，提出加强远程医疗服务、推进人工智能服务等要求。今年3月27日，我应邀参加省发改委主办的“浙江省公共卫生领域补齐短板专家座谈会”时，与会领导和专家都对我提出的“后疫情时代医疗行业需要十分重视网络信息安全保障的更大挑战”表示十分赞同。

对于传统的安全层面，本报告基于“新冠肺炎”疫情期间全国医疗卫生行业网站安全抽样监测，总结归纳Top5的高危漏洞；同时，分析主要攻击方式与类型；后疫情期间，将会持续监测，进行实时分析并输出报告，全力支持全国医疗卫生健康系统最终打赢抗疫阻击战。

对于新型的安全层面，以云计算、大数据、物联网、移动互联、人工智能为代表的新一代信息技术日渐深入城市农村的生产与生活，医疗行业也在同步大面积创新应用过程中；新技术带来的网络信息安全有区别于传统的信息安全，有开放化、互联网化、云化、数据化的新四大挑战。

对于合规性的安全层面，本报告的编委会成员均来自多年在医疗卫生行业从事安全运营、安全咨询等服务的一线专家，从基础的合规等级保护建设，到行业监管建议，再到智慧安全运维，均给出实践中摸索出的针对建议与实践案例。

病树前头万木春，最美人间四月天！

网络信息安全作为医疗信息化的重要保障，今后将更加有效支撑医疗资源整合、系统互联互通、健康数据共享，智慧医疗共建、互联网医疗加速、生态化行业有序，乃至更进一步惠及百姓健康、经济发展、社会治理。

是为序！

俞荣

二〇二〇年五月二十日

Contents 目录

2019年12月以来，新型冠状病毒感染肺炎疫情在全国蔓延。国家卫生健康委办公厅为贯彻落实党中央、国务院关于新型冠状病毒感染的肺炎疫情防控工作的总体部署，充分发挥信息化在辅助疫情研判、创新诊疗模式、提升服务效率等方面的支撑作用，在总结各地典型做法的基础上，制定出台了《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》(以下简称《通知》)国卫办规划函［2020］100号。其中在第五部分12条中具体内容如下：

“加强网络信息安全工作，以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，畅通信息收集发布渠道，保障数据规范使用，切实保护个人隐私安全，防范网络安全突发事件，为疫情防控工作提供可靠支撑。”随着我国新型冠状病毒感染肺炎疫情逐步得到控制，社会对医疗卫生行业的信息化建设所起到的成效有目共睹，同时暴露出我国医疗体系中的一些短板，相信国家会推动医疗、医药领域的完善发展，这一领域有望出现大幅增长之势。一些细分领域，例如医疗信息化建设、“互联网＋”医疗等发展机遇可期。

2020年3月5日，《中共中央国务院关于深化医疗保障制度改革的意见》（以下简称《意见》）发布，《意见》提出我国未来5年—10年医疗改革的目标和任务。医疗信息化建设有望提速，《意见》出台的新意在于“高起点推进标准化和信息化建设”和“建立管用高效的医保支付机制”。

《意见》提出，高起点推进标准化和信息化建设。统一医疗保障业务标准和技术标准，建立全国统一、高效、兼容、便捷、安全的医疗保障信息系统，实现全国医疗保障信息互联互通，加强数据有序共享。2003年SARS之后医疗信息化行业迎来一轮建设高峰，政策对医疗事业高度重视。2003 年 4 月，卫生部发布《全国卫生信息化发展纲要 2003-2010 年》。该文件从建设内容、标准体系，到预算体系、阶段目标、考核机制等方方面面对医疗信息化建设进行了统筹性的规划，是行业发展的纲领性文件。自 2003 年后，我国院内信息化、公共卫生、区域医疗信息化迎来一轮建设高峰。医疗服务信息化是国际发展趋势，从政策的推出频率和力度来看，未来 2—3 年医疗信息化加速将是不可逆转的趋势。相比于欧美等发达国家，我国医疗机构信息化建设起步较晚，但是近年来国家政策支持力度加大。“十三五”将医疗卫生信息化纳入其中作为网络安全和信息化建设的重点。

“新冠肺炎”疫情期间全国医疗卫生行业网站安全抽样监测

疫情当前，共克时艰。面对新型冠状病毒疫情，安恒信息风暴中心第一时间做出响应，抽取医疗卫生行业1500余个网站，就2020年1月1日——2020年02月21日时间段的网络安全状态，进行实时分析并输出报告，全力支持全国医疗卫生系统抗击本次疫情。

经统计分析发现：

（1）在可用性方面，89.87%的重点医疗卫生行业的网站和系统可提供稳定服务，3.70%的网站出现了2小时以上的断网情况；

（2）在1500余家医疗网络系统中，存在网络安全风险漏洞的网站占比约10%，高危漏洞占比最高，约占风险漏洞总数的67.94%，其中跨站脚本成主要高危漏洞；存在高危安全事件105起，暗链为普遍攻击事件；

（3）重点医疗卫生行业的网站和系统总计接受8.03亿次访问，总计受到2843.71万次攻击，恶意user-agents占比较高，成主要攻击类型。

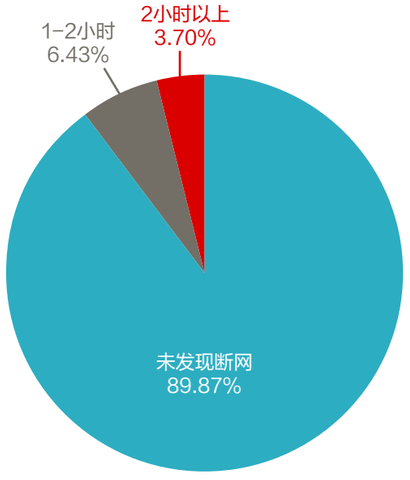
（一）可用性分析

可用性：88%以上网站可正常打开

疫情期间，医疗卫生行业的网站承担着重要的信息传播作用，能否保证这些网站能被全国各地、各个运营商网络的人民群众快速、准确地访问，关系到政府的公信力和社会的稳定。

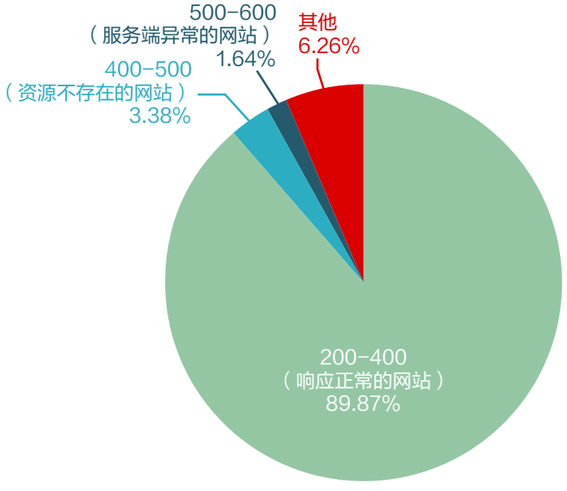
安恒信息利用分布全球的上百个监测节点，对1500多个医疗卫生行业网站进行实时主动监控，掌握网站运行情况，及时发现网站访问慢、无法访问、DNS错误解析等问题。经过监测发现，89.87%的网站不存在断网现象，有3.70%的网站出现了2小时以上的断网情况；通过站点响应码分析，88.72%的网站均可正常打开，其余站点响应码存在异常。

断网时长分布



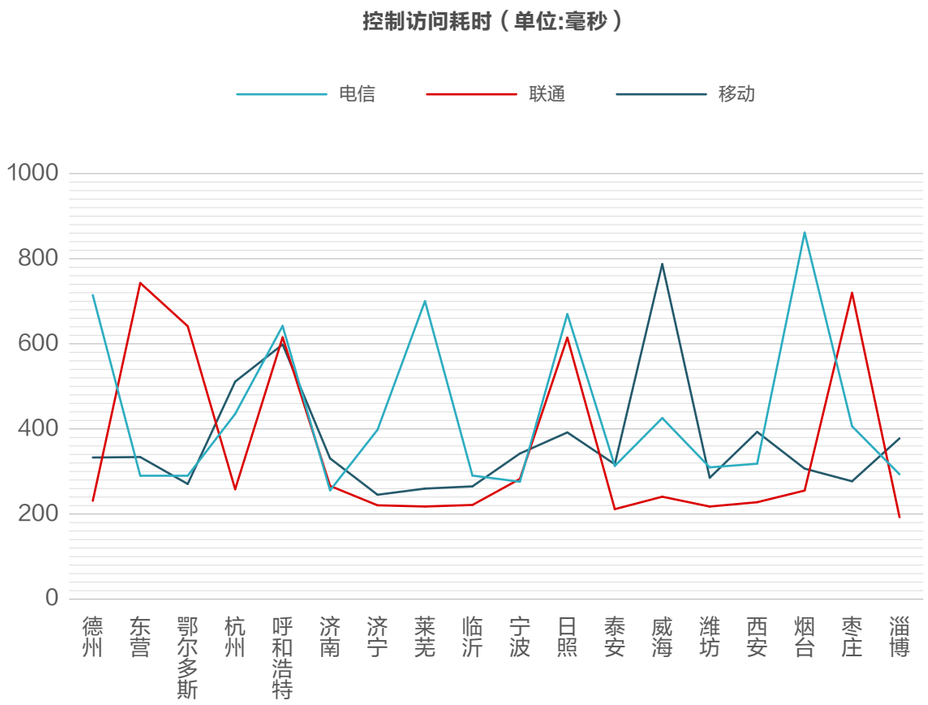
数据统计来自：安恒信息风暴中心

站点响应码分布



数据统计来自：安恒信息风暴中心

在所有可访问的网站中，绝大部分网站表现良好，61.45%网站的响应时间在100ms以内，19.96%网站的响应时间在100-200ms之间，只有2.41%的响应时间达到了1s以上。以下是3家国家级重点卫生单位，在部分地区三个运营商线路下的网站访问情况，总体表现良好：



（二）漏洞分布

10%网站存在漏洞，105起高危安全事件

2020年1月1日——2020年2月21日，安恒信息风暴中心监测发现在1500余家医疗网络系统中，存在网络安全风险漏洞约150余个，存在高危安全事件105起。

漏洞风险

疫情期间，安恒信息风暴中心监测发现在1500余家医疗网络系统中，存在网络安全风险漏洞约150余个，其中高危漏洞占比最高，约67.94%；其次是低危漏洞，占比约31.30%；中危漏洞占比约0.76%。通过进一步对高危漏洞进行深入分析，我们发现医疗卫生行业网站和系统中，排行top5的高危漏洞是跨站脚本、框架注入、链接注入、宽字符集跨站脚本和发现Apache Tomcat examples目录。

1) 高危漏洞top1：跨站脚本

主要危害：获取其他用户Cookie中的敏感数据、屏蔽页面特定信息、伪造页面信息、拒绝服务攻击、突破外网内网不同安全设置、与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。

2) 高危漏洞top2：框架注入

主要危害：恶意篡改网页内容、网页挂马。

3) 高危漏洞top3：链接注入

主要危害：获取其他用户Cookie中的敏感数据、屏蔽页面特定信息、伪造页面信息、拒绝服务攻击、突破外网内网不同安全设置。

4) 高危漏洞top4：宽字符集跨站脚本

主要危害：获取其他用户Cookie中的敏感数据、屏蔽页面特定信息、伪造页面信息、拒绝服务攻击、突破外网内网不同安全设置、与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。

5) 高危漏洞top5：发现Apache Tomcat examples目录

主要危害：未经授权状况下操作数据库中的数据、恶意篡改网页内容、私自添加系统帐号或者是数据库使用者帐号、网页挂马、与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。

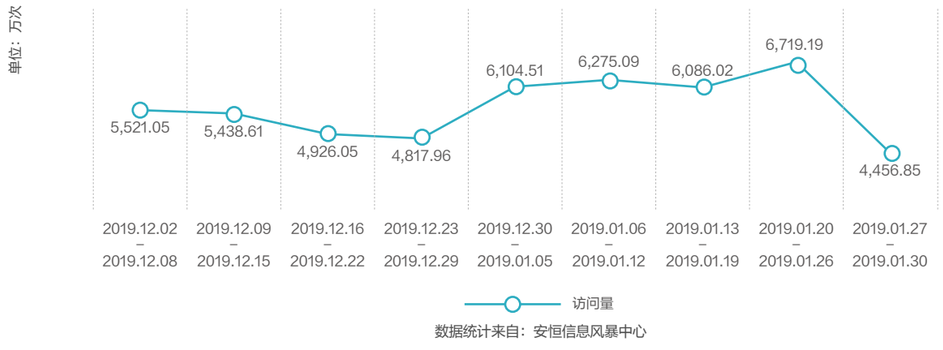
安恒风暴中心监测发现在1500余家医疗行业的网站和系统中，存在高危安全事件105起。通过进一步分析得出：医疗行业的网站和系统中主要存在暗链2828起、坏链152起、敏感内容112起、外链6起。

（三）攻击事件

2020年1月1日——2020年2月21日期间，风暴中心防护的重点医疗类网站和系统总计接受5.03亿次访问，总计受到1843.71万次攻击，恶意user-agents占比较高，成主要攻击类型。

风暴中心防护的重点医疗类网站/系统，在最近2月内总计接受5.03亿次访问，每周的访问量平均在5500万次左右，最高访问量出现在2020-01-20至2020-01-26期间，也是新型冠状病毒肺炎引起全国人民高度关注的时期。

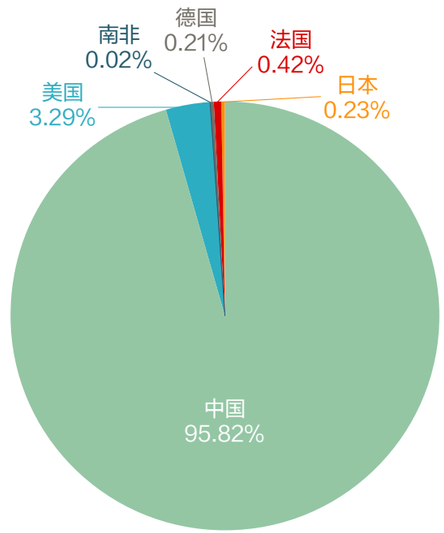
春节疫情期间 重点网站访问量统计



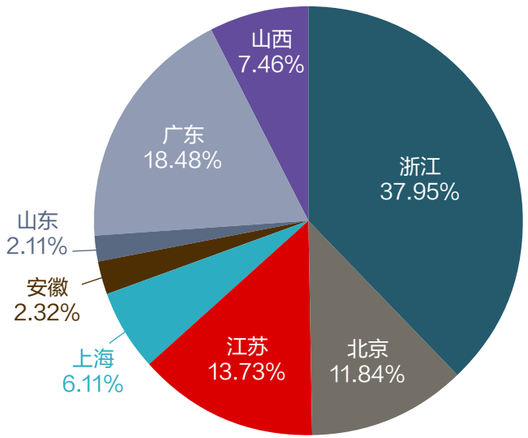
数据统计来自：安恒信息风暴中心

从国际访问源看，主要是来自中国的访问IP占比约95.82%，其次是美国、法国、日本、南非和德国；从国内访问源看，主要是来自浙江、广东、北京、江苏的IP，这四个省份的占比约在90%。

重点国际访问源

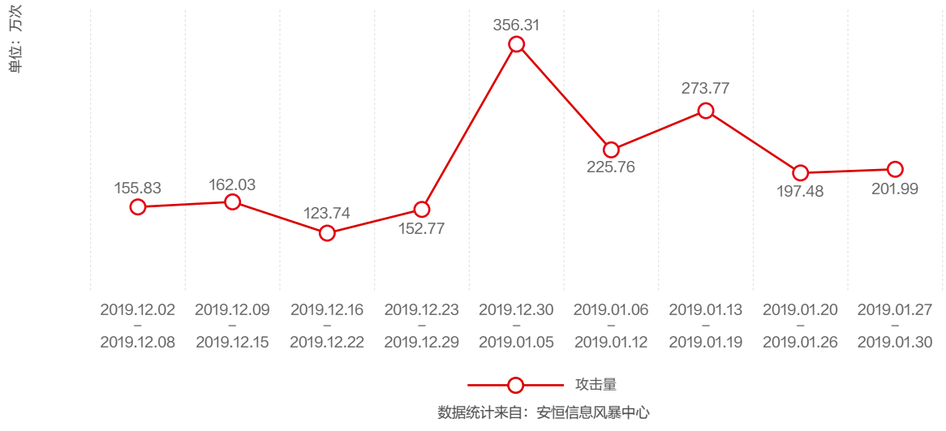


重点国内访问源



风暴中心防护的重点医疗类网站和系统，在最近2月内总计受到1843.71万次攻击。在2019年12月期间，攻击次数几乎稳定在平均每周140万次；从迈入2020年开始，特别是在2020年开年的第一周，攻击数据极速上升达到了356.31万次，其后2020年1月一直保持在200万次/周。

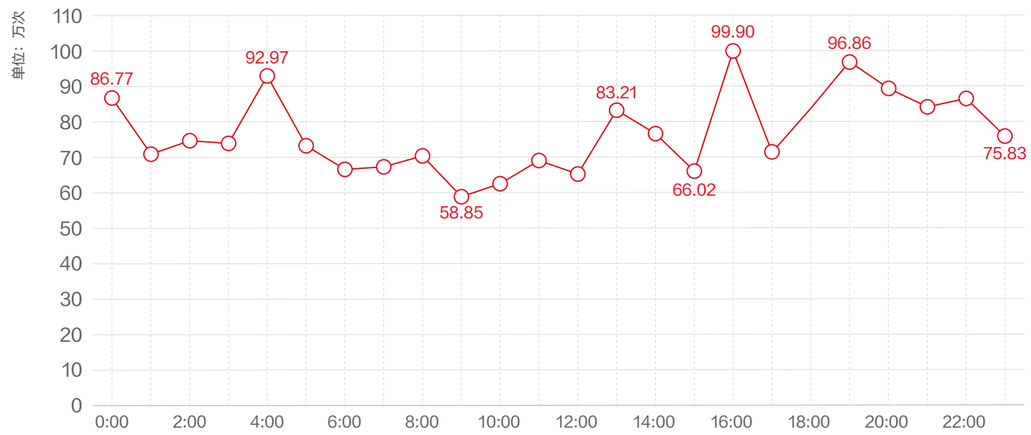
春节疫情期间 重点网站攻击量统计



数据统计来自：安恒信息风暴中心

接下来，安恒信息风暴中心对最近2月的攻击数据做了24小时节点剖析，我们发现在5:00-12:00期间，攻击趋势整体较为平稳，基本处于平均65万/次的水准，这期间9:00出现峰谷值。在13:00-0:00期间，攻击者对重要医疗行业的网站和系统发起的攻击较多，数据波动较大，整体呈现出2小时/周期的频率，其中13:00、16:00、19:00出现明显的高峰值。

第一时间节点 攻击数据

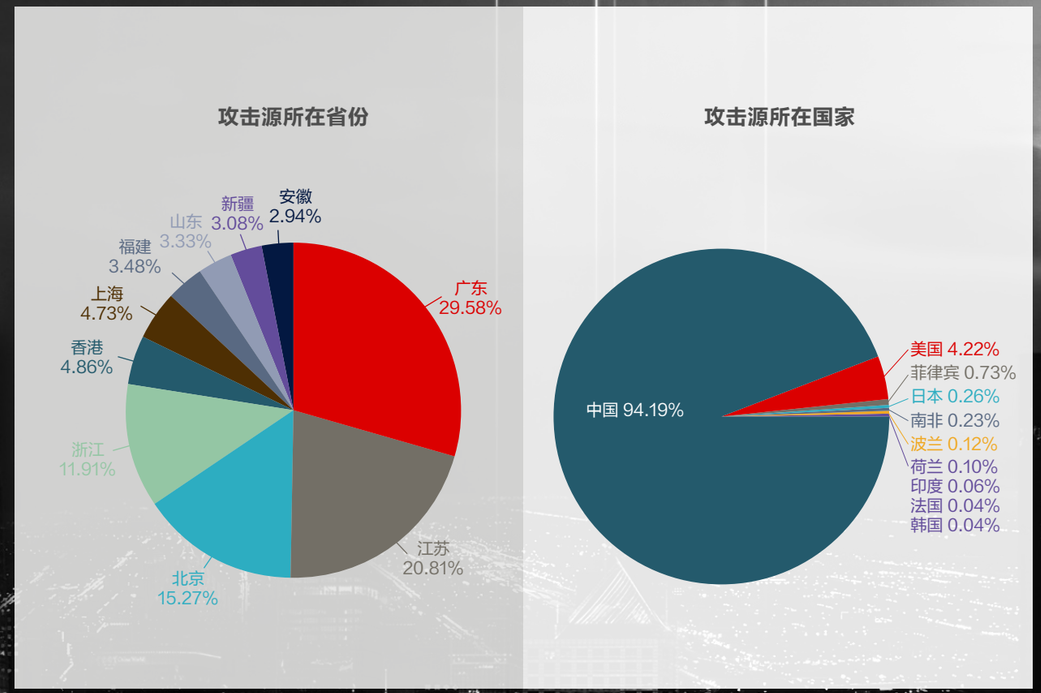


数据统计来自：安恒信息风暴中心

经安恒信息风暴中心攻击溯源分析，就全球攻击局势，由中国地区发起的攻击最高，占比约94.19%，其次是美国、菲律宾、日本等地区；就中国攻击局势，主要发起攻击的区域集中在沿海地区，如京广江浙沪，而具体的城市又以北京、汕头、南通、佛山、杭州、上海为主。

恶意user-agents、命令注入攻击、SQL注入攻击、协议违规、漏洞防护、疑似跨站攻击、文件限制、SQL盲注攻击、跨站脚本攻击和一句话Webshell等攻击类型，成为抗疫期间主要攻击类型。

以发展的眼光来看,网络安全是攻击方与防御方之间的动态博弈,新的攻击手段不断诞生,防御方法也不断升级。但是由于网络安全攻防双方的信息不对称,往往导致防御方难以预测攻击方将在何时、何处、以何种手段发起攻击。因此,防御方经常处于被动地位,防御升级会滞后于新的攻击。解决这个问题的根本方法在于消除信息不对称,这需要联合具备公共互联网观测能力的机构,以公共互联网安全观测和安全情报挖掘为基础,内外协同构建安全防御体系,从而构筑防护范围更为广泛的有效防御联动网络。



医疗卫生行业网络信息安全现状

伴随国内“疫情”状况得到控制，防控的主要关注点变成“输入性病例”，但在医疗卫生信息化建设，以及网络信息安全建设中，美国以及部分欧洲国家还是走在前列。当前全球信息化进程已进入全面渗透阶段,医疗卫生行业作为关乎国计民生的重要领域,是信息时代极力突破和改善的重点。从20世纪90年代开始，许多国家积极推动基于电子健康档案、以医疗信息交换为具体任务的区域医疗卫生信息化，如“欧洲电子健康行动计划”和美国的国家卫生信息网络等。与此同时,频发的医疗大数据泄露、医疗系统瘫痪等安全事件逐渐引发人们对医疗卫生行业信息化的安全思考。

我国网络信息安全建设伴随医疗信息化建设的节奏同步推进，目前信息化建设已步入智慧医疗建设阶段，电子病历、预约诊疗、智能导诊、电子支付等网络信息技术在健康医疗便捷普惠、医疗资源压力释放、医疗资源优化配置、数据信息开放共享等方面发挥了重要作用。近几年，伴随着互联网的发展和政府的重视，也取得了一定的进展。

国内医疗卫生行业信息化发展与安全保障四大挑战

随着信息化新技术的不断发展与国内居民在自身健康需求关注度的逐渐提升，国内各级医疗行政管理机构、公共卫生管理机构、以及以医院为主的各级医疗服务机构为了提升我国居民医疗健康的管理与服务水平，通过信息化手段例如远程诊疗、移动诊疗、医疗物联网的方式拓展了各类医疗信息化的应用场景，互联网医院的开展，也改变了传统线下就诊的服务模式，云计算、大数据的不断深化应用也让医疗信息化不再受传统IT服务架构的桎梏，医疗数据的价值进一步得到提升，上述内容使得我国医疗信息化出现明显的开放化、互联化、云化、数据化特征，而在这背后也存在着亟待解决的一些安全风险与问题。

首先是开放化与互联化，我国越来越多的公立医院在国家卫健委的指导下开展了医院智慧服务评估、电子病历应用分级评估与标准化的信息化建设工作，在医院运营模式上也逐步开展了医联体或医共体的区域医疗服务模式，在这样的大环境下，医院加强了各类互联网挂号及在线诊疗、慢病管理相关业务应用的建设，医院间的数据交互更是成为了开展分级诊疗、远程会诊等业务协同的基本需求，打破了医疗行业原有相对封闭的应用及数据使用环境。在医院的线下与线上诊疗服务中，更多的智能自助服务终端、移动设备终端、医疗物联网终端加入到了诊疗服务管理流程当中，通过有线网络、无线网络、物联网络的方式相互连通依赖并提供各项服务，在拓展了医疗管理抓手的同时也造成了不小的安全风险，不安全的数据使用及共享方式、不安全的医疗设备与物联网终端设备，都会给医院带来很大的运营风险，轻则造成经济名誉损失，重则威胁人们的生命安全。

其次是云化，云计算已经成为了各个行业在进行IT服务架构选择时的一般首选，公有云能够快速敏捷的提供SaaS\PaaS\IaaS化服务，使得用户在降低拥有成本的情况下快速发布业务，私有云更是医疗行业用户的主要建设方式，其灵活的可扩展性、高可用性、资源高利用率特性都使得医疗行业应用系统更方便的进行部署、升级与扩容改造，医疗行业用户更可以在两种云计算方式中根据PACS大容量场景、数字化应用场景、大数据AI场景中灵活的选择适合的云服务提供方式，在使用云计算方式大规模替代传统物理IT服务架构的同时，其平台自身的安全性（包括镜像安全、资源隔离）、租户业务应用数据的安全性，在云化之后也成为了主要的问题之一，由于传统的软硬件安全能力对云计算的基础适配能力不足，导致医疗行业的云上业务安全成为了我们亟待解决的问题之一。

最后是数据化，医疗行业内各级医院、区域卫生信息平台拥有大量的医疗卫生信息系统及数据，其往往记录着关于居民的各类个人基础信息、以及电子病历及电子健康档案等敏感信息，同时也记录着关于医院处方、科研等重要医院运营管理数据，而且随着大数据技术在医疗行业的应用，这些基础数据不断被进行二次汇总及大数据分析，分析结果往往用于临床诊断以及公共卫生决策，其价值较原始数据又有了更高的提升。医院间、监管机构、第三方应用对数据的交换及使用的普及也促进了医疗数据的共享。在医疗数据价值凸显的背后医疗行业数据泄露事件却频频发生，大量的病人数据、处方数据通过非正常渠道方式流通到医疗产业、黑色产业的各个链条，数据倒卖行为、非法统方行为屡禁不止，如果在医疗行业数据安全方面不加以重视，将给我国居民、医疗行业乃至国家社会带来非常严重的不良影响。

国内医疗卫生行业的外部威胁形势观测

医疗行业近年成为了黑色产业关注的主要对象，2017年爆发的勒索病毒，据统计有29%发生在医疗行业，而医疗行业与其他行业有所不同，其医疗信息系统之间往往存在连带性质，其中任何一个环节如果出现问题，对医院正常开展诊疗服务都会造成不同程度的影响，例如叫号系统，看似这个系统不太关键，但是如果叫号系统出现故障，医院的门诊业务将会受到极大的影响，而且一旦勒索病毒感染关键应用业务或数据库服务器，其加密行为将会导致核心业务系统不可用甚至严重的造成数据的不可逆损毁与丢失，给医院的运营带来灾难性的后果。与勒索蠕虫类似，挖矿病毒也同样在医院网络环境中肆虐，其危害性表面看起来没有勒索病毒严重，但是其隐蔽性的特点在不断消耗着医院信息系统的计算资源，加上医院信息系统繁杂，信息中心管理人员往往很难注意到挖矿病毒的存在，导致病毒逐渐啃噬着医院信息系统，可能到最后计算资源消耗殆尽出现系统连续性影响才被重视。另外随着智慧医疗、互联网医疗概念的普及，医院开展的各项业务触手越来越长，其业务系统从院内服务逐步向个人终端、互联网以及先关机构覆盖，但是同时暴露的攻击面也越来越大，不规范的应用开发导致的漏洞越来越多，例如应用程序中包含的第三方组件可能原生存在漏洞、对输入数据不进行格式内容校验、对个人信息数据的采集不符合国家规定标准等，但是这些应用又承载着患者、医生、医院的重要敏感数据，一旦被不法分子利用漏洞进行进一步的渗透及破坏，会造成严重的数据泄露事件发生。另一方面，漏洞并非全部是多么高深的漏洞发现和利用技巧，而是相关人员缺乏安全基本意识造成，例如直接通过端口映射的方式在互联网发布关键服务、启用了不使用的系统服务、弱口令、由于业务敏感疏于打补丁等也是医疗行业存在大范围外部攻击包露面的主要原因。如果说勒索挖矿病毒与漏洞利用攻击是黑产链条趋利的原因所致，那么医疗行业还面临着APT这一强劲对手，不论从医疗数据相关市场层面还是国家战略层面，医疗数据属于目前国家级别的重要战略资源，是掌握着国家居民健康状况的命脉，我们的居民健康数据、基因数据、医疗科研数据都面临着极大的泄露风险，一旦被不法分子或者敌对势力进行渗透窃取，会对我国社会造成严重的不良影响。因此如何发现APT攻击的各类漏洞利用及隐蔽渗透、钓鱼行为并进行阻止，也成为了医疗行业网络信息安全的一个主要话题。

国内医疗卫生行业的内部安全管理难题

在面临各类外部威胁的同时，医疗行业也面临着各类内部管理问题，虽然按照等级保护、以及各项医院信息化建设标准要求建立了初步的纵深防护体系，但是在实际医疗行业安全运营角度下仍然存在一些安全管理上面的难题。

首先是缺乏体系化的合规能力建设，医疗行业用户的网络安全建设较为松散，没有形成完整的统一安全体系，在各层威胁与攻击面的识别上面还有不少漏洞，目前在网络安全检测与防护能力上都缺少基本的合规能力满足，例如终端上只部署了单机版的杀毒软件且覆盖不全，应用安全只使用防火墙进行基本的访问控制，数据安全更是属于裸奔，针对不同的公共医疗数据、医疗科研数据、个人敏感数据场景没有制定基本的防护措施。同时在安全管理制度上，由于缺乏单独安全管理制度、数据安全管理制度等专项策略规程以及安全专岗人员能力和数量问题，导致由于非技术类安全问题时有发生，上述各类原因导致医院安全管理人员无法有效开展以网络安全和核心的运营工作。

第二点是IT资产繁杂，医院场景下不同于传统办公场景，除了医生护士站以及服务器办公终端、打印机外，还拥有大量的智能自助服务终端、移动设备、医疗物联网设备，可谓设备种类多、数量多，管理起来非常复杂，而且目前大多数智能物联网设备、医疗设备多是基于定制操作系统以及开源第三方组件进行开发，其自身可能携带漏洞或者弱点入网，也给医院网络及其他相关系统、设备带来了风险，传统的SOC使用SNMP和日志收集的方式对全网设备进行管理，这样对于哑终端、智能物联网设备由一定的管理盲区，对传统设备也只能做到简单的汇总数据管理。

第三点是高级威胁发现能力弱，之前提到由于医疗行业数据价值高，不法分子也将关注点放在了以提供医疗服务为主，数据集中且真实程度高的医院，使用APT等攻击手段长期潜伏在医院数据中心。高级持续性威胁的特点是：目

的性非常强，攻击目标明确，持续时间长，不达目的不罢休，攻击方法经过巧妙地构造，高级的攻击者们往往会利用社会工程学的方法或利用技术手段对被动式防御进行躲避。而传统的安全技术手段大多是利用已知攻击的特征对行为数据进行简单的模式匹配，只关注单次行为的识别和判断，并没有对未知网络行为、文件的检测手段，也缺乏长期的潜伏式攻击行为链进行有效分析。因此对于高级持续性威胁，无论是在安全威胁的检测、发现还是响应、溯源等方面都存在严重不足。

第四点是安全能力与安全数据分散，院网络承载的业务越来越复杂，各种审计信息、安全措施的告警信息独立存放，缺少基于攻击者与安全视角的统一安全管理与分析。基于单一视角的安全管理员往往面对的是海量的安全设备告警，无法快速准确发现安全问题并且及时准确掌握网络系统的整体安全态势。在这种情况下，投入了大量资金建设的安全防御体系也成了摆设，同时各级安全能力设备系统无法有效联动，各自为战的情况下只能通过管理员逐一排查安全设备与日志并进行手工的配置处理，很难有效地对紧急网络安全事件进行合理及时的处置。

最后是缺乏统一高效的安全运营运维能力，医疗行业用户针对业务系统缺乏周期性及实时性的安全评估，针对威胁预警、安全事件研判、应急响应及安全管理决策，缺乏可提供技术支撑的有效数据与实施专家。同时尚未建立成熟的信息安全人才队伍，无法开展持续可靠的安全运营工作，如果过只是通过传统的远程桌面和表单记录运维工作结果，将会带来不小的工作量与运维控制中造成各类恶意、误操作安全风险。

国内医疗卫生行业网络信息安全典型事件

近年来针对医院等医疗系统的网络安全风险和网络攻击一直处于活跃状态且呈现持续上升态势，其中，在我国多地医院持续检测出勒索病毒，有些医院出现患者信息被盗等情况。2018年全国三甲医院中，有247家医院检出了勒索病毒，被勒索病毒攻击的操作系统主要以Windows 7为主Windows 10次之，以及停止更新的Windows XP。

医疗卫生行业网络信息安全建议

网络安全等级保护制度进入2.0时代

面对新的要求，新的挑战，网络安全等级保护制度进入2.0时代，内涵丰富和措施完善，进一步明确网络定级及评审，备案及审核，等级评测，安全建设整改，自查等工作要求；增加了风险评估等与网络安全密切相关的措施纳入等级保护制度并加以实施。

医疗行业合规面临问题

1) 计算环境安全

弱口令：网络设备、安全设备、操作系统、数据库等存在空口令和弱口令账户；

系统补丁漏打:互联网直接能够访问到的网络设备、安全设备、操作系统、数据库等，存在高危端口开放；

校检机制缺失：由于校检机制缺失导致的应用系统存在如SQL注入、跨站脚本、上传漏洞等漏洞；

应用安全漏洞：应用系统所使用的环境、框架、组件等存在可被利用的高风险漏洞；

防恶意代码软件缺失：操作系统未安装防恶意代码软件，未进行统一管理。

2) 数据安全

明文传输重要数据：用户鉴别信息、个人敏感信息数据、重要业务数据等以明文方式在不可控网络中传输；用户鉴别信息、个人敏感信息数据、重要业务数据等以明文方式存储，且无其他有效保护措施；

数据备份措施缺失：未提供任何数据备份措施，一旦遭受数据破坏，无法进行数据恢复；

存在单点故障：未采用热冗余技术提高系统的可用性，核心处理节点存在单点故障。

3)个人信息保护

违规采集存储个人信息：在未授权情况下，或超范围采集、存储用户个人隐私信息；

违规访问使用个人信息：未授权情况下将用户信息提交给第三方处理，未脱敏的情况下用于其他业务用途，未严格控制个人信息查询以及导出权限。

4) 网络架构

设备业务处理能力不足：核心网络设备性能无法满足高峰期需求，存在设备宕机导致业务中断隐患；

未划分不同网络区域：未按照不同网络的功能、重要程度进行网络区域划分。

网络单链路：网络链路为单链路，核心网络节点、核心网络设备或关键计算设备无冗余设计。

5) 通信传输

无通信完整性保护：数据在网络层传输无完整性保护措施。

6) 边界防护

无线网络接入未限制：内部核心网络与无线网络互联，且之间无任何管控措施。

7) 入侵防范

未检测网络攻击行为：关键网络节点（如互联网边界处、核心服务器区与其他内部网络区域边界处）未采取任何防护措施，无法检测、阻止或限制互联网或从内部发起的攻击行为。

8) 恶意代码和垃圾邮件防范

无恶意代码检测措施：主机和网络层均无任何恶意代码检测和清除措施的，无法对来自互联网的恶意代码攻击、病毒等进行检测和拦截。

9) 安全审计

无安全审计措施：在网络边界、重要网络节点无任何安全审计措施，无法对重要的用户行为和重要安全事件进行日志审计。

10) 系统管理

运行监控措施缺失：无任何系统监测措施，发生故障时难以及时对故障进行定位和处理。

11) 审计管理

日志存储不满足要求：相关设备日志留存时长不满足网络安全法相关要求。

12) 集中管控

安全事件发现处置措施缺失：未部署相关安全设备，识别并告警网络中发生的安全事件（网络攻击事件、恶意代码传播事件等）。

安全建议

安全防范对策的思考

挖掘自身需求原动力-借助国家管理外驱力-依靠专业服务支撑力-形成协同一致持久力。

定级备案梳理：合理开展重要业务系统、新业务系统的定级备案工作；

安全技术防护：在等保建设中采用新技术新手段，加强安全技术防护、安全态势感知等能力建设，重点防范特种木马或新型网络攻击；

日常运维加强：加强日常安全运维，引入安全设备、技术手段，提升安全管理和运维效率；

主动防御加强：加强风险分析和主动防御能力，完善医院网络安全建设短板，从而降低安全风险，提高信息系统健壮性；

安全服务采用：适当选择安全厂商提供的安全服务，弥补运营单位专业安全技术人员缺失的问题，降低因网络安全事件而导致业务应用中断和管理成本增加的风险。

建立结合高质量威胁情报的大数据分析及态势感知防御能力

层出不穷的网络安全案件表明，原有的单纯以等保合规为目标的安全建设已经很难防御当前面临的勒索病毒等高级威胁；同时，监管机构仅通过漏洞通告等传统手段，也难以实现对下辖单位的安全威胁进行感知和及时预警。要提高监管机构的预警能力，建议通过建立结合高质量威胁情报的大数据分析及态势感知防御能力，以及安全分析团队，建设态势感知与预警平台。

当前，医疗卫生行业网络安全工作针对局部信息系统的被动性、应急性安全保障，需要向网络空间安全整体规划，主动积极防御转变，以应对日益严峻的安全形式。根据中央网信办制定的《关键信息基础设施安全保护条例（征求意见稿）》，医疗卫生行业信息化建设作为国家关键信息基础设施的重要组成部分，面临着严峻的网络安全形式，需加强网络安全监测、感知和预警工作。医疗卫生行业网络安全态势感知系统可采取分布建设、数据集成、信息分享、逐步完善的建设思路开展建设，在条件成熟的医疗机构建立微观动态感知系统，构建区域态势感知平台，逐步完善医疗卫生行业宏观态势感知。

医疗卫生行业部门多、医院多、资产多、问题多，有多少资产不清楚，只有备案资产清单，还有一些没有备案私自发布的网站和系统，出现问题难以快速定位，有些资产没有联系人。对于建立医疗卫生行业关键信息基础设施态势感知能力需满足SaaS化服务，依靠高质量威胁情报，行业资产一键梳理，监管目标覆盖系统、设备、终端，网站漏洞、安全事件、违法与不良信息、主机漏洞一网打尽，而在复杂信息系统环境中，存在大量异构多样化数据需利用大数据技术实现，全网流量处理、异构日志集成、核心数据安全分析、办公应用安全威胁挖掘等智能安全威胁挖掘分析与预警管控能力。

应用安全层面

随着互联网+医疗的发展，越来越多的医院借助 Web、患者APP、第三方医疗服务平台等形式，提供网上预约挂号、网上缴费、网上查 询报告等多项线上医疗服务。更便利的是，第三方医疗服务平台还可同时为多家医院提供线上挂号预约、体检预约以及医生咨询等服务。传统网络层安全防护措施和防御体系在安全管理中相当重要，但在面临数据被泄露的安全问题中，应用安全的防护能力更加重要。一种基于风险评估模型及“事前+事中+事后”的安全理念的结合传统网络层防护措施的新型应用安全解决方案，将有效降低应用安全风险和出现被泄露信息的风险。

风险评估与加固层面

威胁一个信息系统的风险可能来自不同的层面，从网络层、系统层到应用层，都有可能形成对信息系统直接或间接的威胁。通过风险评估对整个信息系统进行有效地安全评估，发现信息系统技术与管理方面存在的威胁。通过专业安全团队的加固，减少或降低威胁对系统造成的影响，避免因存在的威胁造成的信息泄密影响。

事前安全防范层面

当前绝大多数外网业务系统缺少必备的Web安全和数据库安全的评估工具，难以实施事前的风险评估。专业的安全产品需要有效的安全策略才能发挥应有的功能，而事前的安全评估则显得尤为重要。外网业务系统业务系统最重要的资产集中在Web应用层和数据库系统，因此长期有效的保障外网业务系统的安全，安全运维人员应有必备的安全评估工具及技术实力。

事中安全防护层面

安全的信息系统需要涉及物理层、网络层、主机层、应用层方方面面的安全防御措施。目前绝大多数的外网业务系统基本上把信息系统的相关主机托管至IDC机房，根据IDC的不同等级分别具备了物理层安全和网络层安全。但外网业务系统尚缺少有力的安全防御措施，例如专业的远程安全接入主机的VPN，网络防火墙，Web应用防火墙等安全设施，应切实建设相应的安全防御措施，提高系统的抗风险能力。

事后安全审计层面

外网业务系统核心数据库存储有大量的用户信息，以及大量的有价值的其它信息资产。如果处理不当，敏感的数据库信息被窃取将会导致极大的信誉危机，对外网业务系统造成重大影响。本项目中应部署专业的数据库审计系统，实现对数据库访问的详细记录、监测访问行为的合规性，针对违规操作、异常访问等及时发出告警，同时可通过与应用层关联审计发现前端的请求与后端的数据库操作关联性，争取将安全风险控制在最小的范围之内。

数据安全层面

数据安全对每个单位来说尤其重要，数据在广域网线路上传输， 很难保证在传输过程中不被非法窃取和篡改。拥有先进技术的黑客或一些工业间谍会通过一些手段，设法在线路上做些手脚，获得在网上传输的数据信息，造成的泄密对用户来说是决不允许的。

1. 数据可用性风险

静态存储数据的可用性问题:关键数据的存储设备自身是否可靠，设备是否有充分的冗余措施，如果因存储设备物理损坏或其他原因导致在线数据丢失或破坏时，数据是否能够可靠地被恢复;

实时处理数据的可用性问题：在进行实时业务处理过程中，业务处理终端通过本地或远程网络查询、修改业务服务器上 存放的业务数据时，通信线路、网络交换设备、路由设备以及业务服务器主机等任何一个环节上的性能下降或中断，都会对数据的可用性造成直接的影响。

2. 数据保密性风险

存储保密问题：对于存放在服务器上的数据，其所存在的网络、系统平台自身是否具有足够的控制和监视手段来防止 信息泄露;对于存放在工作人员的计算机硬盘上的数据，用 户是否会有意、无意的把数据存放目录共享给网络邻居任意 访问，或者主动将数据通过网络或物理手段传播给非法接收者;

传输保密问题：如果敏感数据采用明文在网络上进行传输，攻击者能够通过线路侦听等方式，获取传输的信息内容，造成信息泄露；非法用户可以利用"中间人攻击"或"会话劫持"的手段，模拟正在通信的两台计算机中一方或双方的身份和行为，插入到正常的通信过程中，截取正在传输的数据。

3. 数据完整性风险

静态存储数据的完整性问题：对于存放在服务器上的数据，其所存在的网络、系统平台自身是否具有足够的控制和监视手段来防止信息被篡改;

网络传输数据的完整性问题：攻击者在截获网络上传输的数据报文后，即可对报文内容进行修改，造成收信者的错误理解；或者通过删减信息内容等方式，造成对信息的破坏，导致信息的严重失真;还可以通过重新发送收到的数据包的方式，进行重放攻击，而对于一些业务系统，特别是数据库系统，这种重放攻击会造成数据失真以及数据错误。

安全运营体系建设层面：

从安全技术而言，网络安全要靠一个包括防火墙、入侵检测、访 问控制、防病毒、安全审计、身份认证、加密等多项技术的安全体系来实现。而数据中心各个Web服务器、应用服务器、数据库服务器及 相关的应用系统是构成了最核心的信息资产，这些服务器、应用信息 系统的运行状况通过管理员手工的被动查看和管理，难以做到业务系统安全持续运行。

因此，对于数据中心运维管理缺少一个集中式的管理平台来对信 息资产进行总体配置、调控这个多层面、分布式的运维管理系统。缺 少对各个核心服务器平台、应用平台、数据库平台以及网络安全产品的运行情况的自动监控，不能全面掌握整个信息系统的运行态势，无 法做到事前预防业务故障。缺少对各种网络安全资源的集中监控、统一策略管理、智能审计及多种安全功能模块之间的互动，使得网络安 全管理工作由繁变简，效率较低。

行业实践案例

某三甲医院等级保护建设实践案例

1. 建设背景

等级保护工作是三甲医院建设的重要内容之一。《三级综合医院评审标准实施细则（2011 年版）》（卫医管发【2011】33号文）第六章对三甲医院有如下要求：“实施国家信息安全等级保护制度，实行信息系统操作权限分级管理，保障网络信息安全，保护患者隐私，推动系统运行维护的规范化管理，落实突发事件响应机制，保证业务的连续性。”对信息系统的安全措施、防病毒、防入侵、安全监管、安全运维及安全保护等级等做出了详细规定。 在此背景下，开展了等级保护安全保障体系建设工作，以提升信息系统安全防护水平，并满足相关监管要求。

2. 建设内容

某三甲医院的HIS、LIS、PACS、OA等系统是本单位信息化管理的重要组成部分，根据《信息安全等级保护建设指南》，HIS系统和LIS系统定为三级，PACS和OA系统定为二级，整体网络按照三级要求进行安全建设。 结合某医院的实际情况，从技术、管理、服务三个层面，对HIS、PACS和OA等核心业务系统的安全进行整改和建设，形成完善的等级保护安全保障体系。

安全技术体系建设

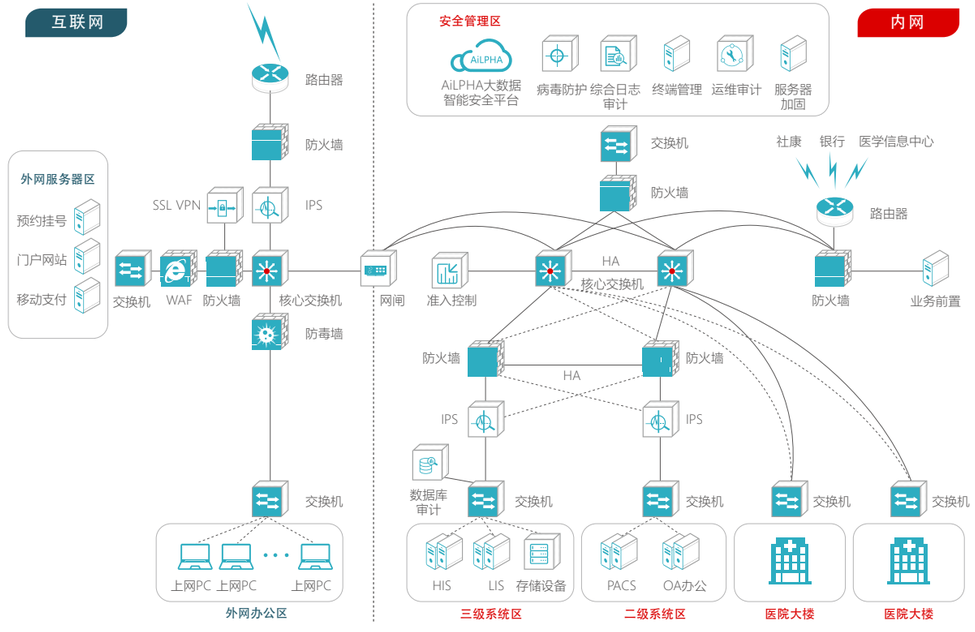
安全技术体系是通过相应的安全技术手段补足，控制策略细化等措施弥补等保基本要求之间的差距，并围绕防范来自内部、外部的攻击及病毒等安全威胁等进行建设。通过防火墙、入侵防御、漏洞扫描、安全审计、病毒防护、Web信息防篡改、终端安全管理等基础安全产品的部署和设置，在统一安全策略的基础上，通过大数据安全管理平台实现安全态势感知和安全运营。

安全管理体系建设

安全管理体系包括总体策略、规章制度、法律法规、安全标准。本次安全建设为医院设计总体安全策略以及安全管理制度，并通过多次培训保障相关制度的落地。

安全服务体系建设

为适应上述安全体系的建设，安全服务团队的参与到项目的建设过程中，将网络安全风险评估工作贯穿到信息系统的整个生命周期中，并结合安全加固、安全预警和应急处置服务，保障医院信息系统的持续、安全、稳定运行。



3. 建设价值

1) 符合医疗卫生行业等级保护工作要求

通过对安全技术体系，安全管理体系和安全运行体系建设，使该医院的信息系统安全保障水平符合《信息安全等级保护建设指南》的要求，并通过等级保护测评。

2) 构建纵深防御体系

针对该医院的通信网络、区域边界、计算环境，综合采用访问控制、入侵防御、恶意代码法防范、安全审计、防病毒、终端管理等多种技术和措施，实现业务应用的可用性、完整性和保密性保护，并在此基础上实现综合集中的安全管理，并充分考虑各种技术的组合和功能的互补性，合理利用措施，从外到内形成一个纵深的安全防御体系。

3) 实现集中的安全管理与态势感知

通过建设大数据安全管理平台，实现对医院所有IT资产的安全事件、安全风险、访问行为等的统一分析与监管，使管理人员能够迅速发现问题，定位问题，实现医院整体安全态势感知，有效应对安全事件的发生。

某省卫建委网络安全监测预警通报及大数据平台建设

1. 建设背景

作为重要网站及信息系统运营单位，全省医疗卫生信息安全工作的指导监管单位，某省医疗卫生委员会（简称：省卫健委）在已完成的网络与信息安全通报预警服务平台基础上建立一套功能更加全面的覆盖全省卫生医疗计生体系及各级医疗卫生计生单位的重要网站和信息系统安全进行态势感知、预报预警、数据直报、大数据智能分析以及应急处置的通报预警及数据分析平台。实现信息安全数据的标准化统一采集、规范化管理、历年信息安全状况可追溯，同时与国家医疗卫生信息安全平台信息安全数据的互联互通。

2. 建设内容

某省卫健委网络安全监测预警通报及大数据平台要遵循统一管理、统一标准、统一设计，并要考虑与省电政办、省委机关业务系统等相衔接。本着实用性、可靠性、先进性、经济性、开放性、可扩展性、易维护性和安全性的原则，充分考虑系统的整体性、科学性和可持续发展性，采取充分论证、试点运行、分步实施、全面推广的方法，紧密结合本项目实际，务求实效，以发展的眼光建设系统。

3. 建设目标

1) 建立网络与信息安全信息通报预警处置机制

为了保证全省医疗卫生系统覆盖通报预警处置机制，以平台为依托推进和完善网络安全态势感知监测通报手段、信息通报预警及应急处置体系建设。通过续建网络安全态势感知监测通报平台，继续实现对门户网站和网上重要信息系统的安全监测、通报预警、应急处置、态势分析、安全事件（事故）管理、督促整改等功能，为开展相关工作提供技术保障。

2) 建设医疗卫生信息安全数据直报平台

针对各级医疗卫生行政管理机构、各级卫生医疗机构的卫生信息安全数据集中管控平台，主要功能有：上报提醒、数据上报、数据质控、数据管理，统计分析、数据发布等。

3) 建立医疗卫生信息安全数据管理平台

包括申报管理、数据管理、报表管理、消息提醒、报送提醒、基础数据管理等功能。让省级信息安全管理人员可以监控全省信息安全数据的报送，实现全省信息安全数据的电子化管理。

4) 建立信息安全数据资源库

通过系统化的信息安全数据采集，积累完整、全面、实时、可靠，覆盖全省各级医疗卫生行政管理部门和卫生医疗机构的信息安全数据，形成全省信息安全数据资源库。

5) 实现医疗卫生信息安全数据共享平台

各级管理人员可以通过共享平台了解辖区及兄弟单位的信息安全管理工作，共同推进信息安全建设工作及促进信息安全管理工作的规范化。

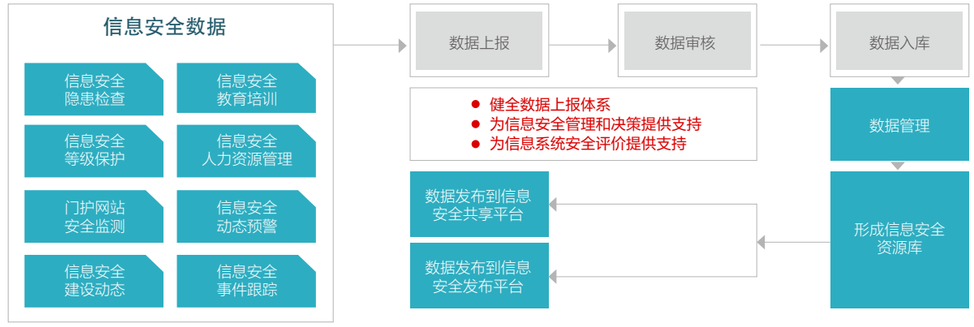
6) 实现卫生信息安全数据发布平台

快速响应国家卫健委信息安全管理平台及其他相关安全主管部门对我省医疗卫生行业信息安全数据的需求。

7) 与卫生其它应用系统在流程、信息、数据上实现无缝衔接

比如OA、网站、财务系统等，使得信息安全工作管理更加规范、更加科学、更加高效，推动我省医疗卫生信息化业务安全可靠地建设与发展。

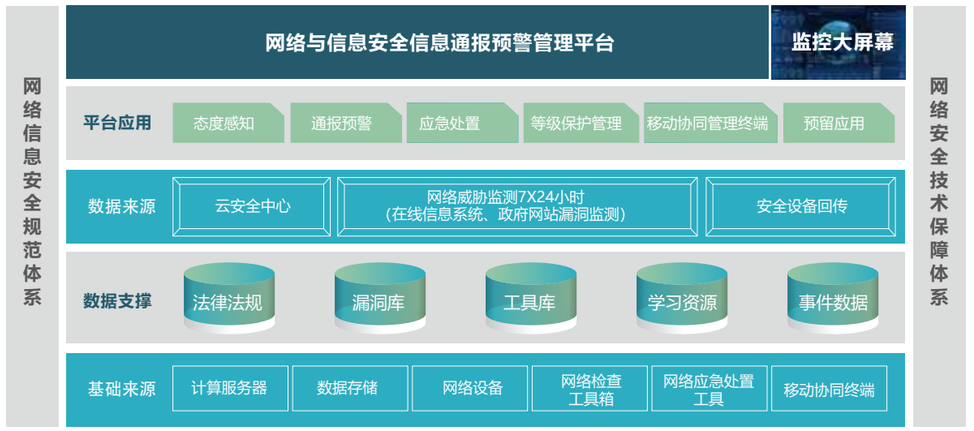
◎卫生健康信息安全数据管理流程分析



① 重要网站安全事件监测管理

信息安全网站监测平台采用远程监测技术对网站应用提供7*24小时实时安全监测服务。通过对网站的不间断监测服务，实行网站漏洞监测、网页木马监测、篡改检测、可用性监测与关键字监测，提供详尽的数据与分析报告，从而全面掌握网站的安全态势，可有助于提升网站的安全防护能力和网站服务质量，并通过安全监测平台的事件跟踪功能建立起一种长效的安全保障机制，令动态且变化不定的网站安全态势尽在掌控之中。

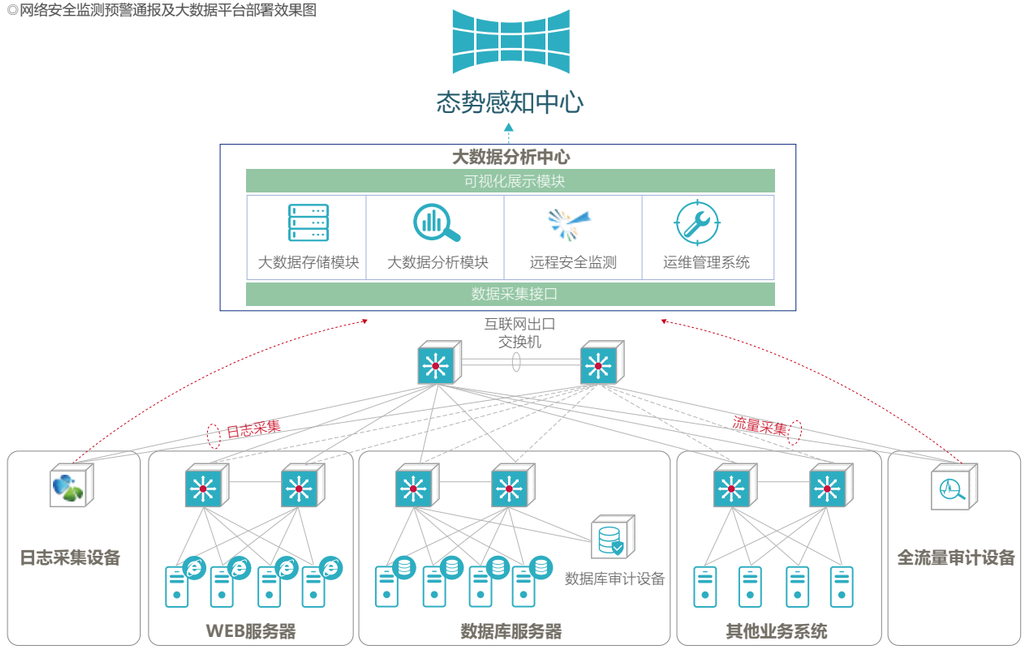
◎网络安全监测预警通报及大数据平台架构设计及部署效果图



② 系统核心流程

某省卫健委网络安全监测预警通报及大数据平台核心流程。其功能是：通过对网络中系统、主机、网络、服务数据采集，进行多源异构网络数据的处理，通过数据融合，生成综合的、全局网络安全态势图，进行多视图、多角度、多尺度的可视化显示，为用户决策提供支持和保障。

◎网络安全监测预警通报及大数据平台部署效果图



4. 建设价值

随着网络安全管理工作要求的提高，有必要继续建设和优化网络与信息安全通报预警服务平台，并在此基础上扩建大数据智能分析平台。该系统的建设，可以全方位管理、监督、预警、防范各类信息安全事件的发生，能感知全省信息安全的态势，帮助省卫健委掌握当前形式下的安全形势、安全问题与各地的安全水平，做到信息安全建设心中有数、保障有度、行动有据、管理有法、防范有措，真正做到为人民群众的生命健康保健护航，提高人民的卫生管理参与程度及满意度。

某医院核心数据安全防护实践案例

1. 建设背景

随着医院信息化的迅猛发展，信息的高度集中使得核心数据泄密的隐患也越来越突出，在利益的驱使下非法统方行为时有发生，严重影响了医院的公众形象，也严重损害了患者的利益。鉴于问题严重性，卫生管理部分也引起了高度的重视。 目前医院工作的开展对信息系统的依赖性越来越强，致使信息系统越来越庞大，各业务系统关联性越来越复杂，核心数据泄密的隐患也越来越突出。

2. 建设内容

医院对数据库的审计包括两个方面:

医院对数据库的审计包括两个方面:

Plan-1

HIS系统

对核心数据库（HIS系统）全审计并且配置统方规则实现防统方

门诊病人诊疗收费明细

医生信息字段：ORDERED_BY_DOCTOR	存在于表：OUTP_ORDER_DESC
描述：ORDERED_BY_DOCTOR（开单医生）	OUTP_ORDER_DESC（开单记录）
药品信息字段：ITEM_CODEITEM_NAME	存在于表：OUTP_BILL_ITEMS
描述：ITEM_CODE（项目代码）	
ITEM_NAME（项目名称）	OUTP_BILL_ITEMS（门诊病人诊疗费用项目）
数量信息字段：COSTS AMOUNT	存在于表：OUTP_BILL_ITEMS
描述：COSTS（费用）	
AMOUNT（数量）	OUTP_BILL_ITEMS （门诊病人诊疗费用项目）
时间信息字段：VISIT_DATE	存在于表：OUTP_BILL_ITEMS
描述：VISIT_DATE（就诊日期）	OUTP_BILL_ITEMS （门诊病人诊疗费用项目）

住院病人收费明细

医生信息字段：DOCTOR	存在于表：ORDERS
描述：DOCTOR（开医嘱医生）	ORDERS（医嘱）
药品信息字段：ITEM_CODE ITEM_NAME	存在于表：INP_BILL_DETAIL
描述：ITEM_CODE （项目代码）	
ITEM_NAME （项目名称）	INP_BILL_DETAIL （住院病人费用明细记录）
数量信息字段：COSTS AMOUNT	存在于表：INP_BILL_DETAIL
描述：COSTS （费用）	
AMOUNT（数量）	INP_BILL_DETAIL（住院病人费用明细记录）
时间信息字段：BILLING_DATE_TIME	存在于表：INP_BILL_DETAIL
描述：BILLING_DATE_TIME（计价日期及时间）	INP_BILL_DETAIL（住院病人费用明细记录）
药品处方（药品处方明细记录）	
医生信息字段：PRESCRIBED_BY PRESC_NO	存在于表：DRUG_PRESC_MASTER
描述：PRESCRIBED_BY（开方医生）	
PRESC_NO（处方号）	DRUG_PRESC_MASTER （药品处方主记录）
药品信息字段：DRUG_NAME DRUG_CODE	存在于表：DRUG_PRESC_DETAIL
描述：QUANTITY（数量）	
COSTS（费用）	DRUG_PRESC_DETAIL（药品处方明细记录）
时间信息字段：PRESC_DATE（处方日期）	DRUG_PRESC_MASTER（药品处方主记录）
医生信息字段：DOCTOR	存在于表：ORDERS
描述：DOCTOR（开医嘱医生）	ORDERS（医嘱）
药品信息字段：DRUG_CODE DRUG_SPEC	存在于表：DRUG_DISPENSE_REC
描述：DRUG_SPEC（药品规格）	
DRUG_CODE（药品代码）	DRUG_DISPENSE_REC（摆药记录）
数量信息字段：DISPENSE_AMOUNT	存在于表：DRUG_DISPENSE_REC
描述：DISPENSE_AMOUNT（摆药数量）	DRUG_DISPENSE_REC（摆药记录）
时间信息字段：DISPENSE_DATE_TIME	存在于表：DRUG_DISPENSE_REC
描述：DISPENSE_DATE_TIME（摆药日期及时间）	DRUG_DISPENSE_REC（摆药记录）

对核心数据库

HIS系统 LIS系统 PACS系统

Plan-2

满足条件审计
设置增删改查铭感表规则

- **从根源解决防“统方”难题**
  从数据库级别进行防控，从根源上彻底控制统方数据信息的泄露，为医疗信息化打好底层基础。

- **医疗行业防统方规则包真正贴合用户需求**
  结合数十家医院的实施经验，形成了丰富的防统方知识库，通过强大、细粒度的规则设置功能，形成了医疗行业防统方规则包，准确识别非法统方行为。解决统方行为特征提取困难、规则设置难度大、规则误告警等问题，帮助客户轻松部署防统方系统。

- **应用改造零代价**
  安恒解决方案的实施，对于现有应用系统完全透明，无需改造，原有数据库核心特性均可继续使用。

敏感数据规则组

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
敏感数据清空操作	对象组=敏感数据业务表	操作类型=truncate	无	无	高	所有
批量更新敏感数据（大于1000行）	对象组=敏感数据业务表	操作类型=update 影响行数1000	无	无	高	所有
批量删除敏感数据（大于1000行）	对象组=敏感数据业务表	操作类型=delete 影响行数1000	无	无	高	所有
批量查询敏感数据（大于1000行）	对象组=敏感数据业务表	操作类型=select 影响行数1000	无	无	高	所有
非业务系统访问数据库	所有对象	操作类型=select/delete/insert/update/create来源ip不等于业务系统ip来源用户名不等于应用系统用户	无	无	高	所有

数据库性能规则组

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
执行时间超过5秒	所有对象	执行时间大于等于5秒	无	无	高	所有
执行时间超过10秒	所有对象	执行时间大于等于10秒	无	无	高	所有
模糊查询语句	所有对象	无	报文关键字 (? !)select[\s]*.*[\s]*where[\s]*.*[\s]*like[\s]*.*	无	高	所有

权限管理规则组

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
授权操作	所有对象	操作类型=grant	报文关键字=grant[\s]+.*	无	高	所有
权限回收行为	所有对象	操作类型=revoke	报文关键字=revoke[\s]+.*	无	高	所有
删除用户行为	所有对象	操作类型=drop	报文关键字=drop[\s]+user.*	无	高	所有

Oracle数据库备份与恢复

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
数据库物理备份和恢复行为	所有对象	数据库账号=sys来源IP，来访客户网络=xxx, xxx, xxx客户端工具=rman.exe	无	无	高	所有
数据库逻辑恢复行为	所有对象	客户端工具=imp.exe	无	无	高	所有
数据库逻辑备份行为	所有对象	客户端工具=exp.exe	无	无	高	所有

Sql执行失败规则组

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
Oracle错误代码ORA-00904：标示符无效	所有对象	无	执行结果关键字=ORA-00904.*?	无	高	所有
Oracle错误代码ORA-01920：发生冲突	所有对象	无	执行结果关键字=ORA-01920.*	无	高	所有
Oracle错误代码ORA-00942：表现视图不存在	所有对象	无	执行结果关键字=ORA-00942.*	无	高	所有
Oracle错误代码ORA-01031：权限不足告警行为	所有对象	无	执行结果关键字=ORA-01031.*	无	高	所有
Oracle错误代码ORA-01017：登录失败行为	所有对象	无	执行结果关键字=ORA-01017: invalid username/password; logon denied	无	高	所有

数据清理删除操作

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
数据清理删除	所有对象	无	(?!) (truncate | drop)[\s]+.*	无	高	所有
全表删除业务数据	自定义表	操作类型=delete	delete[\s]+from[\s]+app_table_01[\s]*$		高	所有

合规性规则组

规划名称	应对对象	触发条件	特殊触发条件	白名单	规划等级	业务主机群
非法账户的访问行为	所有对象	用户名不等于XX，XX，XX，XX	无	无	高	所有
非DBA账号的DDL操作	所有对象	用户名不等于root操作类型=create、alter、drop	无	无	高	所有
非法IP地址的访问行为	所有对象	IP地址不等于XX操作类型=所有操作类型	无	无	高	所有

3. 建设价值

- 双向审计，对医院统方行为全面监控、精确定位、实时响应
- 简洁直观的统方界面并附带中文翻译，方便纪检部门使用
- 定期评估数据库漏洞，防止数据库密码破解
- 丰富的审计报表，满足纪检部门审计需求 短信、邮件告警，第一时间了解违规统方行为

某医院应用安全实践案例

1. 建设背景

为了进一步提升系统的运行效率，加强信息安全，最大程度保障系统的数据安全和高可用性。因此工程实施业务压力及可用性方面均有极高的要求；同时，该系统涉及国家其他数据中心的业务平台接口和零宕机数据迁移，工程实施风险非常大。包括公安厅网监部门在内的各方专家已经对安全防护进行了相应的指导与论证，根据专家的相关意见提出了适合CLTR系统的安全解决方案，方案最终做到专家要求的“系统进不来，进来了拿不走，拿走了看不懂”的防护原则。

2. 建设内容

传统网络层安全防护措施和防御体系在安全管理中相当重要，但在面临数据被泄露的安全问题中，应用安全的防护能力更加重要。使用基于风险评估模型及“事前+事中+事后”的安全理念结合传统网络层防护措施的新型应用安全解决方案，将有效降低应用安全风险和出现被泄露信息的风险。

风险评估与加固层面

通过风险评估对整个信息系统进行有效地安全评估，发现信息系统技术与管理方面存在的威胁。通过专业安全团队的加固，减少或降低威胁对系统造成的影响，避免因存在的威胁造成的信息泄密影响。

事前安全防范层面

专业的安全产品需要有效的安全策略才能发挥应有的功能，而事前的安全评估则显得尤为重要。外网业务系统业务系统最重要的资产集中在Web应用层和数据库系统，因此长期有效的保障外网业务系统的安全，安全运维人员应有必备的安全评估工具及技术实力。

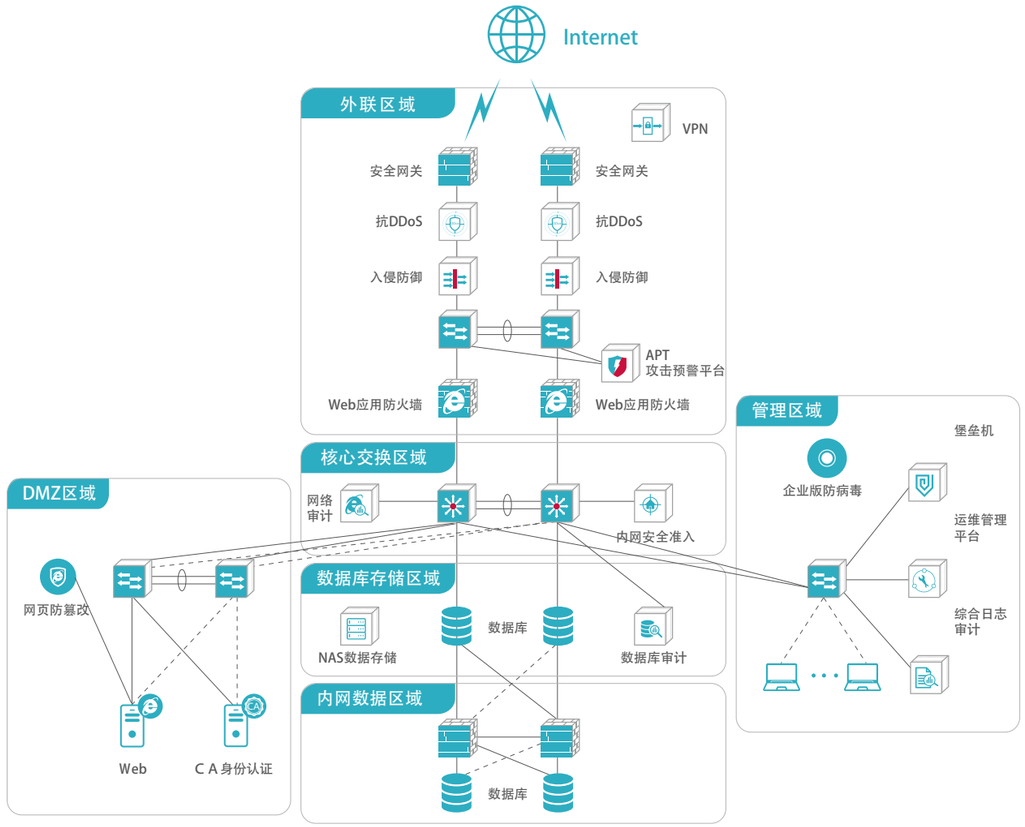
事中安全防护层面

目前绝大多数的外网业务系统基本上把信息系统的相关主机托管至IDC机房，根据IDC的不同等级分别具备了物理层安全和网络层安全。但外网业务系统尚缺少有力的安全防御措施，例如专业的远程安全接入主机的VPN，网络防火墙，Web应用防火墙等安全设施，应切实建设相应的安全防御措施，提高系统的抗风险能力。

事后安全审计层面

应部署专业的数据库审计系统，实现对数据库访问的详细记录、监测访问行为的合规性，针对违规操作、异常访问等及时发出告警，同时可通过与应用层关联审计发现前端的请求与后端的数据库操作关联性，争取将安全风险控制在最小的范围之内。

◎项目拓扑图



3. 建设价值

整体安全

- **风险管理**

  本方案是集预警、检测、防护、响应为一体的安全集成方案。

- **合规管理**

  针对国家法律法规及行业标准规定，网络审计、数据库审计、日志审计提供合规性审计及管理。

- **配合协作统一管理**

  安全管理中心提供对终端管理、漏洞扫描、运维审计、防火墙等安全设备的集中管理、统一日志分析，提高网管效率。

- **全方位的生命周期防护**

  信息安全事件的发生，通常都会经历事前、事中、事后三个生命周期过程，不同的阶段我们可以有针对性地采取安全措施，即事前预防为主，事中有效防护，事后追溯审计提供持续安全服务。

某医院智慧医疗网络安全建设实践案例

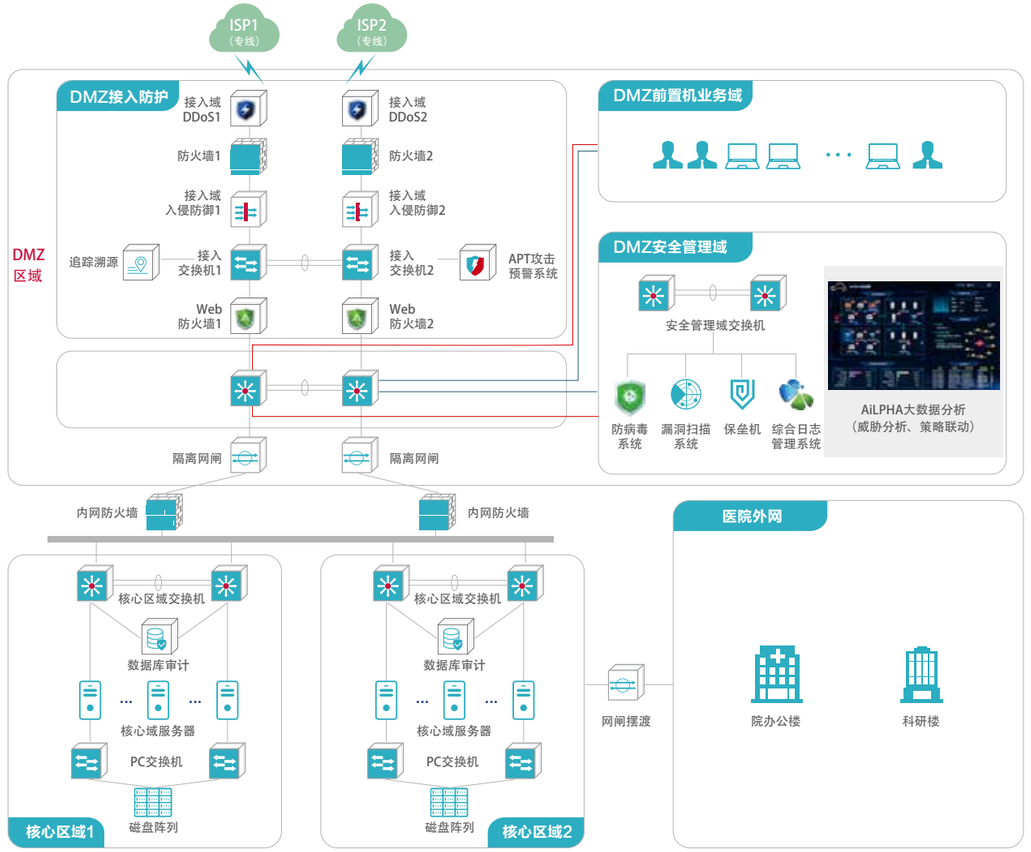
1. 建设背景

伴随信息化的发展，医院逐步建立起依赖于网络的业务办公信息系统，比如门户Web应用、HIS系统、LIS系统、电子病历系统、PACS系统等等。网络信息功能和内容以及网上预约挂号、网上查询检查结果等等一系列工作是通过Web来实现的，但医院Web应用的公众性质使其成为攻击和威胁的主要目标，给医院的服务形象、信息网络和核心业务造成严重的破坏。一个优秀的Web应用安全建设是医院信息化是否能取得成效、充分发挥职能的基础，而合规、有效、全面的信息安全体系建设对保障其正常运行至关重要。

2. 建设内容

根据等级保护要求以及前期分析了解的结果，对某医院信息系统安全存在的弱点提出相关的整改意见，结合等级保护建设标准，并最终形成安全解决方案。

◎安全解决方案示意图



1) 区域安全防护设计

根据某医院业务安全需求和等级保护三级对入侵防范的要求，本项目整体安全建设方案将建立网络层纵深防御体系强化应用层的防护措施，实现新型应用层解决方案。

建立边界访问控制防御能力

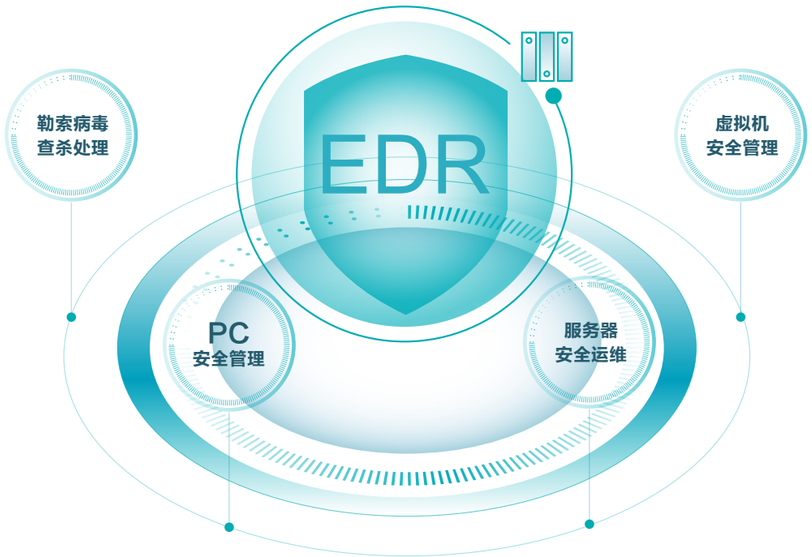
通过部署下一代防火墙和抗DDoS设备，对该区域提供边界攻击防护，同时有效预防、发现、处理异常的网络访问，确保该区域信息网络正常访问活动。

建立网络入侵防御能力

通过部署入侵防护产品，实现在入侵检测的基础上对攻击行为进行阻断，实现对入侵行为实时有效的防范。入侵检测/保护产品部署于DMZ区防火墙之后，是继防火墙边界访问控制后的第二道防线。

建立Web防护安全监控机制

通过在DMZ区域部署Web应用防火墙（WAF）设备，对Web应用服务器进行保护，即对网站的访问进行7X24小时实时监控。可以解决Web应用服务器所面临的各类网站安全问题，防止网页篡改、被挂木马等严重影响形象的安全事件发生。



建立网络安全隔离系统

通过部署安全隔离网闸，对内网实现按需数据同步，可以为访问提供更高的安全性保障。实现“协议落地、内容检测”，既从物理上隔离、阻断了具有潜在攻击可能的一切连接，又进行了强制内容检测，从而实现最高级别的安全。

建立APT沙箱技术提供网络攻击行为检测机制

通过部署APT预警平台采集器，采集互联网中的网络流量、电子邮件流量实现对流量的实时检测，采集和分析网络流量数据，包括：Web流量、文件流量、邮件流量等，通过特征匹配、行为匹配、规则匹配来实现对APT攻击威胁检测和预警。

2) 终端安全防护设计

前置机系统终端作为DMZ网络区域最核心的业务支撑点，因为其为外网与内网方位的连接点，同时涉及转发核心敏感数据，因而成为黑客和病毒制造者的攻击目标，导致其成为DMZ网络中最危险的一环。

通过部署主机安全及管理系统（以下简称EDR），可以将常见服务器操作系统提升至等保三级要求，从根本上免疫现有的各种针对操作系统的攻击行为，具有进程保护、病毒、后面查杀、漏洞防护、防端口扫描等功能，可在非法攻击开始侵入系统之前就切断其连接，禁止其下一步行为。

3) 运维管理安全设计

建立安全漏洞检测系统

通过部署系统安全检测管理系统有效的实现了对DMZ区域内网络设备、主机系统、应用系统进行漏洞扫描、配置核查的全生命周期管理，将技术和管理以及等级保护合规有效地融合在了一起，为用户信息系统整体风险评估提供有力的支撑。

建立运维审计管理系统

通过建立运维审计管理系统整合DMZ区域各类系统的运维行为管理，将运维操作集中可视化管控，通过基于唯一身份标识的集中账号与访问控制策略，实现与各服务器、网络设备等无缝连接，一站直达，解决多种设备类型带来的管理问题，快速发现和处置违规事件。

建立日志审计收集分析系统

通过部署综合日志审计设备，可以全面收集网络设备（路由器、交换机等）、网络安全设备（防火墙、入侵检测系统，补丁系统等）、应用系统等运行日志和安全事件日志，平台对日志进行归并、关联分析等操作，为管理人员提供直观的日志查询、分析、展示界面，并长期妥善保存日志数据以便需要时查看，使管理员能够在综合日志审计平台上就可以了解整个数据中心的安全态势。

建立全流量深度威胁分析及溯源追踪系统

通过部署全流量深度威胁检测平台，对流量采集并深度还原解析，发现流量中的应用会话行为和潜在威胁，并提供了全流量审计及攻击溯源追踪分析能力。

建立大数据智能化安全分析平台

大数据智能分析平台通过建立安全大数据中心，实现网络安全类、管理类、流量数据以及资产、用户的基本数据的采集、标准化和集中化存储，并在安全大数据中心的基础上建立安全态威胁分析与预警平台，实现全网的安全要素分析、安全威胁事件联动分析、异常行为快速发现的能力以及实现整体网络的安全态势可视化能力和整体网络环境安保能力综合评估。

3. 建设价值

整体防护更安全更可靠

整体安全解决方案以业务系统及数据流向为整体防护目标，侧重于立体式全局防护，从业务访问请求的检测防护到人员的访问管控，以及人为设定逻辑的数据安全边界，保证数据合法合规的使用，从整体到局部避免了防护的短板，真正实现全生命周期无死角的安全防护，保证数据安全更安全。

多重内控访问边界更合规

整体安全解决方案通过边界防护、Web防护、APT、全流量DPI设备进行多级控制和检测，确保内部人员访问更合规，避免内部合法人员和非授权用户的非法数据泄露事件的发生。

多级联动无缝防护更智能

整体安全解决方案均采用厂商同品牌防护设备，整个平台在研发初期已同各个安全防护设备约定数据共享联通接口，通过内部API自动完成防护策略设定及动作响应，彻底解决之前多品牌防护都是独立工作安全防护孤岛，安全数据无法共享无法协同的问题，使数据安全防护更智能。

分块安全防护更专业

整体安全解决方案从整体规划，局部落地防护，即保证整体的安全防护无短板，单个数据处理单元防护更加精准，保证每个节点的防护采用，无防护短板，保证每个数据处理单元都有业内专业级的防护实行精准的安全防护，让数据安全防护更专业。

全业务流审计更具威慑力

整体安全解决方案具有全局的事件审计取证能力，通过全面的事件调查取证能力对内部能形成极大的威慑，从心理上威慑内部各种维护、管理、开发人员肆意的数据泄露行为，极大的降低数据泄露的可能。

典型场景分析检测更准确

整个安全防护系统集中了各种各样的数据、告警急日志，以典型场景为导向重点分析特定威胁场景安全威胁更加准确，通过大数据对这些日志进行智能的建模关联挖掘分析，剔除噪音日志，使的安全预测更加准确，彻底解决传统安全防护设备大量误告警日志。

安全预警数据展示更直接

采用统一的数据安全分析平台，对安全域内业务系统相关的日志、资源使用情况、告警异常数据、审计数据统一展示，解决之前日志分散不容易监控等难题，人机交互界面非常友好直观，让数据展示的更加明了直接。

某医院信息系统安全服务项目案例

1. 建设背景

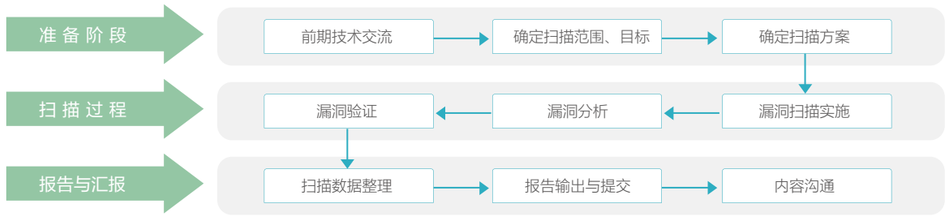
近几年来，随着网络安全威胁的越来越复杂，医疗行业面临着网络安全重大考验，信息安全防御面临着越来越严峻的考验，信息安全建设维护已成为医院的首要任务之一，防止外部恶意攻击导致内部重要信息数据丢失，或者业务系统瘫痪影响正常办公。为保障医院信息化安全已经在网络架构设计及Web安全防御上做了相应保护措施，本次项目主要是为了防止目前多种多样的外部恶意利用攻击。

2. 建设内容

采用安全评估技术手段检查医院官网及核心信息系统存在的安全隐患，针对安全隐患进一步加固，防止黑客借助系统漏洞攻击系统及数据。

1) 漏洞扫描服务

- 漏洞扫描是脆弱性识别的重要手段，能够帮助医院发现设备和系统中存在的严重漏洞，了解技术措施是否有效执行，并通过及时修补完善，避免对信息系统造成严重影响。
- 扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题，提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案。



2) 安全配置检查服务

- 采用人工现场设备检查的方式对指定系统和设备等进行全面的安全配置核查和分析，发现配置的不合规项，并结合行业实际需求提出系统整改建议，输出报告。

检查对象	类型
主机	WINDOWS、LINUX、AIX、HP-UNIX、SOLARIS
数据库	MSSQL、ORACLE、SYBASE等
中间件	IIS、APACHE、WEBLOGIC、JBOSS等
网络/安全设备	防火墙、路由器、交换机等

3) 渗透测试服务

- 渗透测试作为检验目标系统安全性最有效的服务，需要服务人员通过智能工具扫描与人工测试、分析的手段，以模拟黑客入侵的方式对服务目标系统进行模拟入侵测试，识别服务目标存在的安全风险。

信息收集类
配置管理类
（HTTP方法测试、应用中间件测试、信息泄露、异常错误等）

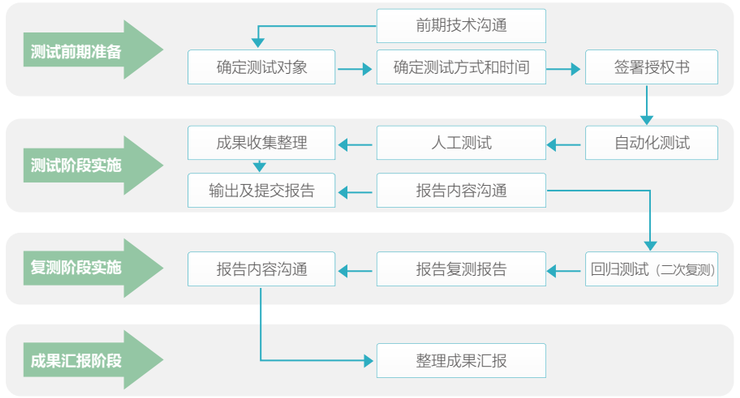
认证类
（用户枚举、密码猜解、密码重置、密码策略测试等）

会话类
（cookie测试、session会话测试等）

授权类
（越权访问、路径遍历、任意文件下载、逻辑缺陷测试等）

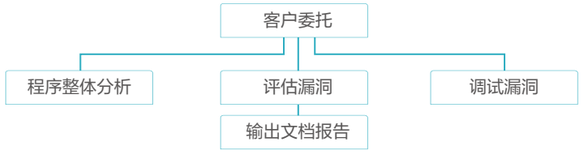
数据验证类
（SQL注入、跨站脚本、代码注入、URL跳转、文件上传测试等、输入输出校验绕过、数据篡改）

系统应用漏洞
（溢出、0day漏洞等）



4) 移动APP安全测试服务

- 移动APP安全测试服务是由资深安全服务工程师以人工分析为主，漏洞检测工具为辅的方式，对APP进行安全分析，在保证整个安全测试过程都在可以控制和调整的范围之内，全面发现Android、IOS、微信应用等程序可能存在的安全缺陷，并提供安全测试报告和改进建议，最大程度地为保障北京大学口腔医院APP的程序安全。



成果输出汇总		
项目阶段	工作内容	交付成果报告
全安评估服务阶段	漏洞扫描服务	《 漏洞扫描报告 》
	渗透测试服务	《 渗透测试报告 》
	APP渗透测服务	《 APP渗透测报告 》
	安全配置检查服务	《 安全配置检查报告 》
	应用系统梳理	《 应用系统级别梳理 》

3. 建设价值

技术支持服务期内，为了解决医院业务系统运营过程中遇到的各种问题和困难，设立了安全服务咨询热线，提供7*24小时的远程安全技术支持服务、常见信息安全问题咨询服务。

参考文献

1. 国家卫生健康委办公厅.国卫办规划函〔2020〕100号:关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知 [OL].http://www.nhc.gov.cn/xcs/zhengcwj/202002/5ea1b9fca8b04225bbaad5978a91f49f.shtml
2. 新浪财经，巨丰投顾： 巨 • 研究 | 医疗信息化大势所趋 本次疫情将带来下一个发展高峰 [OL].http://finance.sina.com.cn/wm/2020-02-11/doc-iimxxstf0460609.shtml
3. 豆丁网：提高认识积极探索大力推进卫生信息化建设 [OL].http://www.docin.com/p-1029509766.html
4. 国防科技要文：美国发布《2019 2022年国家卫生安全战略》 [OL].https://xw.qq.com/cmsid/20190123A0MUXA00
5. 中华人民共和国卫生部.卫办发〔2011〕85号: 卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知 [OL].http://www.nhc.gov.cn/wjw/gfxwj/201304/994583c125e842549d75aae22f67c05c.shtml