2022年医疗行业网络安全报告

2023-1

数说安全研究院有限公司

医疗行业报告

- 医疗行业信息化和政策概况
- 医疗行业市场概况
- 医疗行业供给侧分析
- 总结

医疗行业概况

- 研究主体
- 医疗行业构成
- 医疗行业信息化进程
- 医疗行业网络安全政策环境
- 医疗行业市场规模
- 医疗行业需求简要分析

• 研究主体

我国的医疗健康体系主要包括医疗机构、医药、医保三类，其监管部门分别为国家及各地卫生健康委员会、国家药品监督管理局和国家医疗保障局。医疗机构主要包括各级别的医院、基层医疗机构、公共卫生机构、医联体等。医疗信息化指医疗服务的数字化、网络化、信息化，狭义上的医疗信息化包括医院管理信息化、临床管理信息化和区域信息化;广义上的医疗信息化还应包括医保信息化和药品流通信息化。本报告主要探讨的是医疗机构和医保局信息化的进程及带来的网络安全的需求，医药信息化不在此报告讨论。

卫健委

医疗服务市场的整体秩序，医疗服务资质的合法合规，医疗质量及其安全性等

- 医院
- 基层医疗
- 公共卫生机构
- 医联体
- 其他医疗机构

医保局

负责医保支付

- 各地医保局

药监局

负责药品、医疗器械的监管

- 药企
- 医疗器械

• 医疗机构构成

2021年末，全国医疗卫生机构总数1030935个，比上年增加8013个。其中：医院36570个，与上年相比，医院增加1176个，基层医疗卫生机构增加7754个。

医院中：三级医院3275个（其中：三级甲等医院1651个），与上年相比三级医院增加279家，三级甲等医院增加71家；二级医院10848个，一级医院12649个，未定级医院9798个。

专业公共卫生机构中：疾病预防控制中心3376个，卫生监督机构3010个，妇幼保健机构3032个。

疾病预防控制中心（3376个）	卫生监督机构（3010个）	妇幼保健机构（3032个）
• 省级31个 • 地（市）410个 • 县（区、县级市）级2755个	• 省级25个 • 地（市）级315个 • 县（区、县级市）级2487个	• 省级26个 • 地（市）级377个 • 县（区、县级市）级2554个

表 1　全国医疗卫生机构及床位数

机构类别	机构数（个）		床位数（张）	
	2020	2021	2020	2021
总计	**1022922**	**1030935**	**9100700**	**9448448**
医院	**35394**	**36570**	**7131186**	**7412566**
公立医院	11870	11804	5090558	5206065
民营医院	23524	24766	2040628	2206501
医院中：三级医院	2996	3275	3002503	3228967
二级医院	10404	10848	2718116	2743079
一级医院	12252	12649	712732	726054
基层医疗卫生机构	**970036**	**977790**	**1649384**	**1712115**
#社区卫生服务中心	9826	10122	225539	239139
#政府办	6848	7042	177263	188550
社区卫生服务站	25539	26038	12804	12581
#政府办	10482	10631	2704	2238
乡镇卫生院	35762	34943	1390325	1417410
#政府办	35259	34494	1370674	1402629
村卫生室	608828	599292	-	-
诊所（医务室、护理站）	259833	271056	564	1343
专业公共卫生机构	**14492**	**13276**	**296063**	**301566**
#疾病预防控制中心	3384	3376	-	-
专科疾病防治机构	1048	932	42323	40611
妇幼保健机构	3052	3032	252920	260132
卫生监督所（中心）	2934	3010	-	-
计划生育技术服务机构	2810	1588	-	-
其他机构	**3000**	**3299**	**24067**	**22201**

注：#系其中数。以下各表同。

数据来源：卫生健康委网站

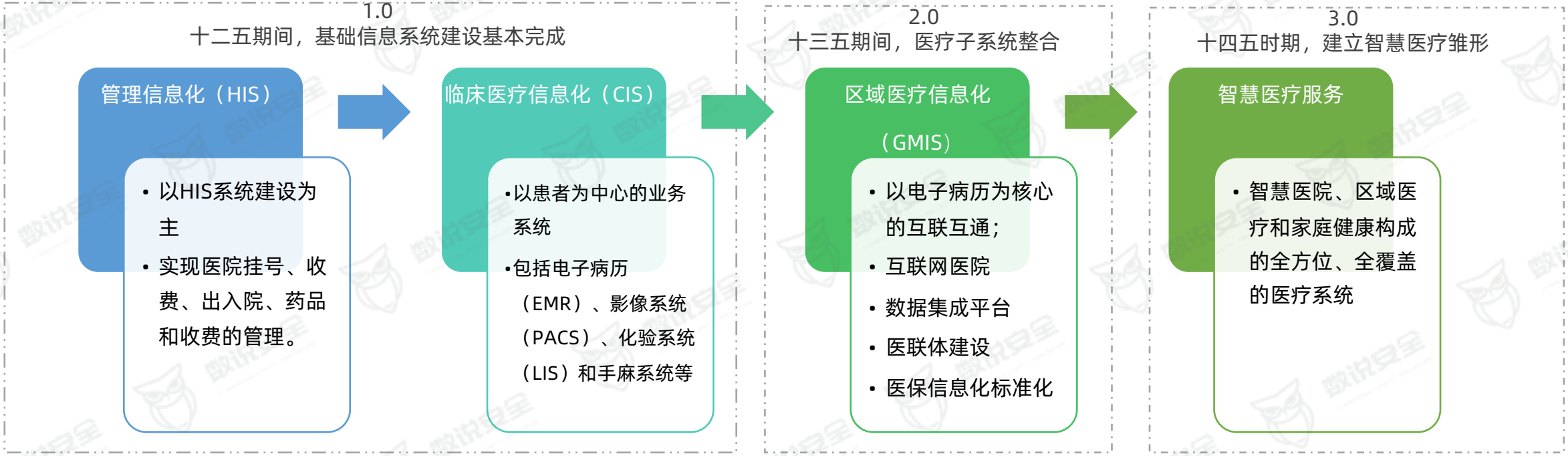
• 医疗行业信息化现状

我国信息化建设30余年，主要分为三个阶段：

1.0阶段：基础信息系统建设：我国医疗信息化起始于20世纪70年代，当时医院信息化建设以单机版为主，HIS系统应运而生，主要是简单的管理应用。随着网络技术和计算机技术的普及以及技术的成熟，医院信息化建设也逐渐从单机版向网络版发展，HIS系统以门诊、住院收费为基础，逐步扩展到收费管理、药品数据等。2010年掀起了HIS建设热潮，目前在全国范围内部署渗透率较高。 21世纪初，我国医疗行业开始引进以患者为中心的CIS系统，自此信息化建设向临床信息化转移，主要包括EMR、PACS、LIS等诊疗系统，实现患者诊疗环节全部流程信息化，提升临床医疗效率。十二五期间，基础信息系统建设基本完成。

2.0阶段：区域医疗信息化：十三五期间，国务院推动分级诊疗建设，开始强调电子病历等核心医疗数据的共享。但是医疗信息化建设涵盖诸多子系统，每个系统都有不同的供应商，不同产品之间的数据端口和格式不统一，为了解决院内信息系统的互联互通和数据管理的问题，医院构建了信息集成平台和数据集成平台。随着互联网应用的深入，“互联网”+医疗健康发展迅猛，2019年开始智慧服务分级评估，二级以上公立医院建设互联网医院成为标配。2018年以来卫健委、医保局等部委出台了大量的医疗信息化政策，主要集中在电子病历升级、医联体建设、互联网诊疗、医保信息标准化和医保收费制度改革5个领域。

3.0阶段：智慧医疗服务：中国医疗信息化建设的最终目标是智慧医疗，由智慧医院、区域医疗和家庭健康构成的全方位、全覆盖应用场景广泛的医疗系统。



• 医疗行业信息化现状

数说安全

政策

医院：院内系统：三位一体智慧医院建设，“以评促建”政策体系搭建完成

2018.12月《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）》；2019.3月《医院智慧服务分级评估标准体系（试行）》；2020.8月《医院信息互联互通标准化成熟度测评方案》；2021.3月《医院智慧管理分级评估标准体系》

互联网+医疗健康配套文件完善

国务院指导文件：《关于促进“互联网 + 医疗健康” 发展的意见》(国办发〔2018〕26 号)；卫健委配套文件：《互联网诊疗管理 办法(试行)》和《互联网医院管理办法及标准(试行)》以及《远程医疗服务管理规范》，管理办法要求医疗机构开展互联网诊疗活动，应当具备满足互联网技术要求的设施信息系统、技术人员以及信息安全系统，并实施第三级信息安全等级保护。

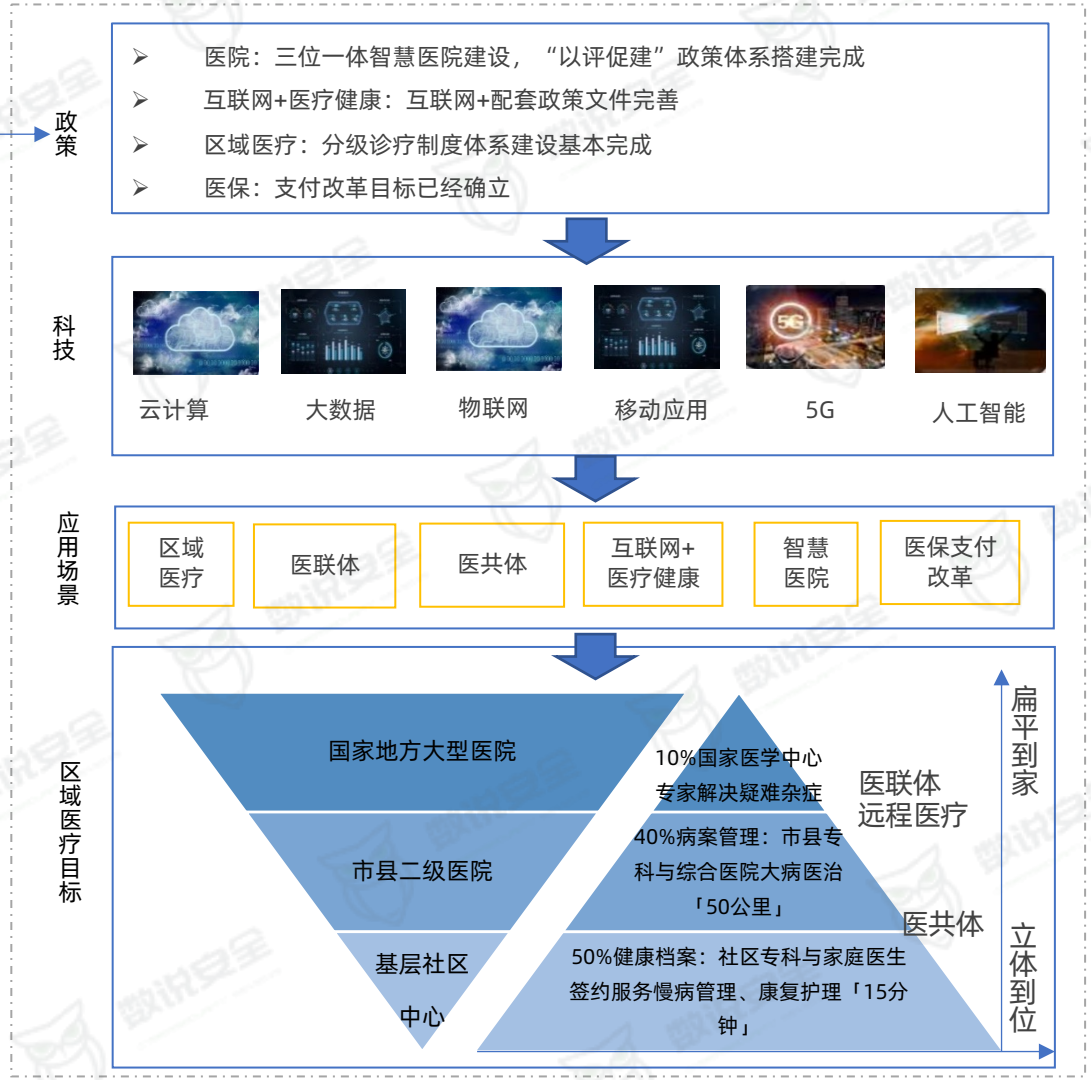
区域医疗：分级诊疗制度体系建设基本完成

- 2017年8月国务院办公厅印发《关于推进医疗联合体建设和发展的指导意见》将我国医联体分为四种组织模式：城市医疗集团、县域医共体、专科联盟、远程医疗协作网。
- 2019年《国家医学中心和国家区域医疗中心设置实施方案》，提出在全国建设高水平的国家医学中心和国家区域医疗中心，进一步完善医疗服务体系顶层设计，优化优质医疗资源布局，提升区域医疗服务保障能力，减少患者异地就医。
- 2020年7月，《医疗联合体管理办法（试行）》，文件提出加快推进医联体建设，逐步实现医联体网格化布局管理，并印发了《紧密型县域医疗卫生共同体建设评判标准和监测指标体系（试行）的通知》。
- 2021年，《“十四五”优质高效医疗卫生服务体系建设实施方案》，提出2025年各地建设120个左右省级区域医疗中心。
- 自此我国分级诊疗制度体系建设逐渐完善，一是国家层面设置国家医学中心和国家区域医疗中心，建立国家、省、地市、县四级医疗卫生服务体系；二是，加强和规范医联体建设，推广远程医疗服务，深入开展城乡医院对口支援，特别是增强县级医院的综合服务能力。

医保局：支付改革目标已经确立

2021年10月国家医疗保障局《印发DRG/DIP 支付方式改革三年行动计划的通知》国家医保局依托全国统一的医保信息平台制定DRG/DIP 相关信息系统标准和规范。

十四五期间医疗行业信息化趋势



• 医疗行业网络安全建设政策背景

十二五期间，我国医疗机构基础信息系统基本建立，信息安全需求开始产生，原卫生部在等保1.0基础上发布等级保护指导意见，提出三级甲等医院的核心系统必须通过等保三级测评。

进入十三五期间，医疗行业信息化建设发展如火如荼，卫健委加强医院、基层医疗和公共卫生信息化规范建设，并在规范中对未来5-10年的信息安全建设提出建议与要求。**十三五期间医疗行业信息化建设规范已经初步形成，医疗行业网络安全规范尚未形成体系，滞后于信息化建设。十三五期间医疗行业网络安全主要围绕等保合规建设。**

进入十四五时期，卫健委和医保局都提出了要加强网络安全和数据安全的指导意见，**2022年8月29日，卫健委推出了医疗行业首个关于网络安全的管理办法，《医疗卫生机构网络安全管理办法》，其文件为医疗卫生机构网络安全管理提供了工作指南，**对医疗行业网络安全和数据安全发展具有重要意义。

总体而言，十三五以来从国家对网络安全和数据安全逐渐重视，陆续推出多部法律使安全有法可依。相应地，医疗行业监管部门也陆续推出相应的管理办法促进医疗行业网络安全的发展，但整体而言，医疗行业的网络安全规范尚未形成体系，根据卫健委的十四五规划，预计十四五期间，卫健委会加强医疗行业网络安全和数据安全的标准建设。

“十二五”时期（2011-2015）

国家层面：

2015年7月《国家安全法）；

行业监管层面：

2007.公安部等四部门发布等保1.0管理办法：为信息安全建设提供了框架标准的具体要求。

2011. 卫生部《卫生行业信息安全等级保护工作的指导意见》：明确提出三级甲等医院的核心系统必须通过等保三级测评。

“十三五”时期（2016-2020）

国家层面：

2017年6月1日，《网络安全法》正式开始施行；

2020年1月，《密码法》，开始实施；

行业监管层面：

公安部：

2019.5公安部发布《信息安全技术网络安全等级保护基本要求》：

卫健委：

2018.4《全国医院信息化建设标准与规范（试行）》对二级及以上医院的数据中心安全、终端安全、网络安全及容灾备份提出要求。

2018.9《国家健康医疗大数据标准、安全和服务管理办法（试行）》：明确责任单位应当落实网络安全等级保护制度要求，对健康医疗大数据中心、相关信息系统开展定级、备案、测评等工作。

2019.3《关于印发全国基层医疗卫生机构信息化建设标准与规范》明确了基层医疗卫生机构未来5-10 年信息化建设和信息安全的基本内容和要求。

2020.12《全国公共卫生信息化建设标准与规范》着眼未来5-10年全国公共卫生信息化建设，对信息安全提出要求。

2020.9《关于加强全民健康信息标准化体系建设的意见》完善加强推进对网络安全、数据安全、应用安全标准体系建设。

医保局：

2020.2《关于推进新冠肺炎疫情防控期间开展“互联网+”医保服务的指导意见》要求不断提升信息化水平，同步做好互联网医保服务有关数据的网络安全工作，防止数据泄露。

“十四五”时期（2021-2025）

国家层面：

2021年1月，《个人信息保护法》开始实施；

2021年9月，《数据安全法》正式实施；

2021年9月，《关键信息基础设施保护条例》；

2022年2月，《网络安全审查办法》；

行业监管层面：

医保局：

2021.4《关于加强网络安全和数据保护工作的指导意见》明确提出到2022年基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制，到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。

卫健委：

2022.1《“十四五”卫生健康标准化工作规划》强调健全卫生健康信息标准体系，完善基础类、数据类、应用类、技术类、管理类、安全与隐私类等6类信息标准的制定。

2022.8.《医疗卫生机构网络安全管理办法》是卫健委首个具体的医疗网络安全管理办法。

• 《医疗卫生机构网络安全管理办法》总体架构

数说安全

出台背景：

随着互联网+医疗健康、医疗系统互联互通、智慧医院的建设的推进，医疗网络不再封闭，安全风险也进一步加大。

而医疗卫生机构的医疗健康数据关系国计民生，一旦遭到篡改、破坏和泄露，对医疗机构的声誉、对患者的治疗都会有极大影响。随着新冠疫情的爆发，全球医疗机构遭受网络攻击数量倍增。在我国，疫情防控期间医疗卫生系统、科研机构也频繁遭受网络入侵攻击。

在这样的背景下，《医疗卫生机构网络安全管理办法》发布，《办法》将进一步规范医疗卫生机构网络和数据安全，促进“互联网+医疗健康”发展，加快推动卫生健康行业高质量发展进程。

第一章 总则

制定目的 | 基本原则 | 适用范围 | 各方责任

第二章 网络安全管理

总体要求

等保合规 | 监测预警

应急实战 | 安全自查

人员管理 | 安全运维

业务连续性 | 新技术安全

医疗设备安全 | 密码安全

供应链安全 | 报废管理

第三章 数据安全管理

管理总则

组织建设 | 分级分类

制度规范

全生命周期安全管理

组织建设 | 分级分类

存储安全 | 使用安全

交换安全 | 人脸识别

销毁安全

第四章 监督管理

监督管理

检查督导

上报机制

事件通报

执法协助

第五章 管理保障

总体保障 | 人才培养 | 经费保障 | 考核机制

第六章 附则

• 《医疗卫生机构网络安全管理办法》要点

数说安全

一：细化网络安全管理颗粒度

- 成立网络安全和信息化工作领导小组，由单位主要负责人任领导小组组长，每年至少召开一次网络安全办公会；
- 等保第二级以上：应在网络安全保护等级确定后10个工作日内，报备公安、上级行政部门；网络撤销或变更等级；10个工作日内报备。
- 第三级以上：每年至少一次开展网络安全等级测评；二级系统中涉及10万以上个人信息：至少三年开展一次；其他的网络：至少五年开展一次；新建的网络上线运行钱应进行安全性测试；

二：覆盖数据全生命周期的管控

数据收集	•明确业务部门和管理部门的主体责任 •采取数据脱敏、加密等防控措施
数据传输	•重要数据加密传输 •加强传输接口安全控制
数据存储	•境内存储，涉及云存储，评估风险 •重要数据加密存储
数据交换	•对外提供数据需严格审核 •数据共享遵循最小化原则
数据销毁	•销毁数据确保彻底清除 •关注数据残留及备份风险

三：强调检测预警与应急处置协同

- 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；
- 通过建立完善应急预案、每年组织应急演练等方式，有效出来网络中断、网络攻击、数据泄露等安全事件。

四：与国家法律法规实现有效链接

- 等级保护方面：要求落实《关键信息基础设施安全保护条例》和网络安全等级保护制度要求。
- 要求落实《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。

五：融合管理、技术、运营三位一体

总体策略拆解到具体安全管理要求，并通过安全技术能力实现管理要求，最终融入对应到安全运营体系中。

① 建立网络安全管理制度体系

② 加强网络安全保护

③ 运营过程中，每年开展文档核验、漏洞扫描、渗透测试等多种形式的安全自查。新建信息化项目的网络安全预算不低于项目总预算的5%。

六：构建防护监测处置保障四个体系

① 安全防护方面：要求建立实战化、体系化、常态化的安全防护体系，形成动态防御、主动防御、纵深防御、精准防御、整体防控、联防联控的安全防护态势；

② 安全监测层面：鼓励三级医院探索态势感知平台、及时收集、汇总、分析各方面网络安全信息，并与国际及行业平台对接；

③ 安全保障方面，通过统筹领导和规划设计、在人才培养、安全培训、经费保障等方面实现全方面保障；

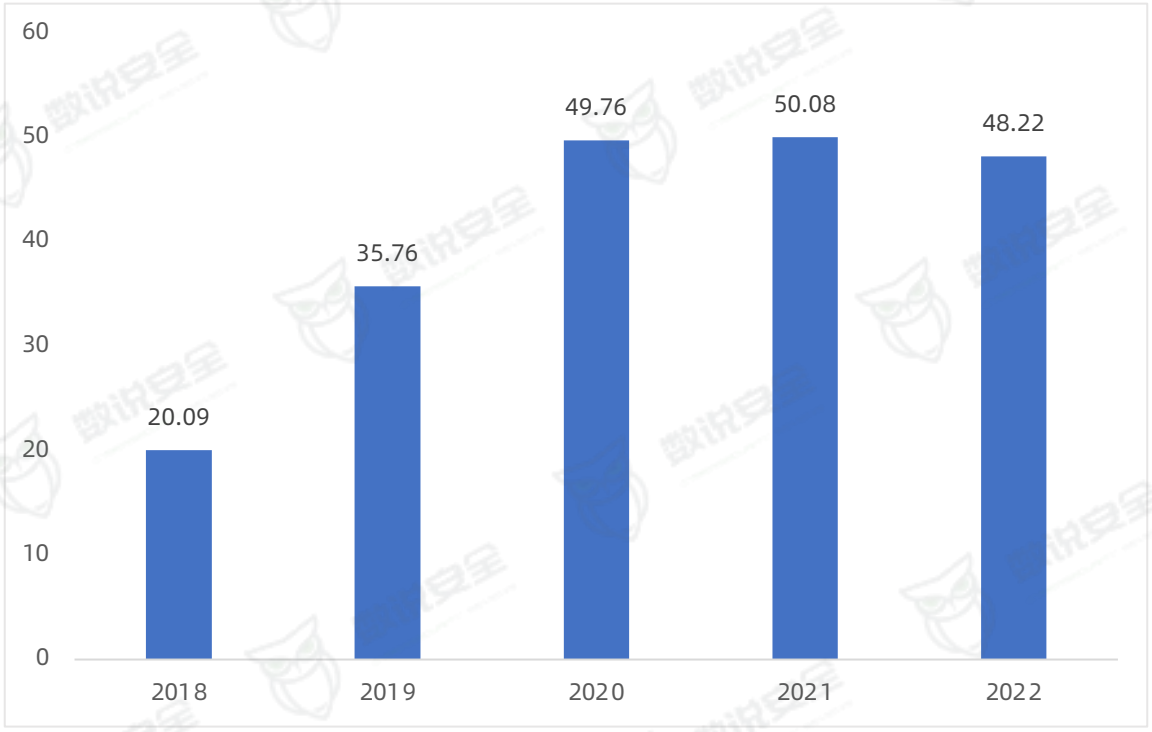
④ 安全处置方面：形成监督管理、安全检查、应急预案、联防联控系统体系。

• 医疗行业市场规模受到疫情影响

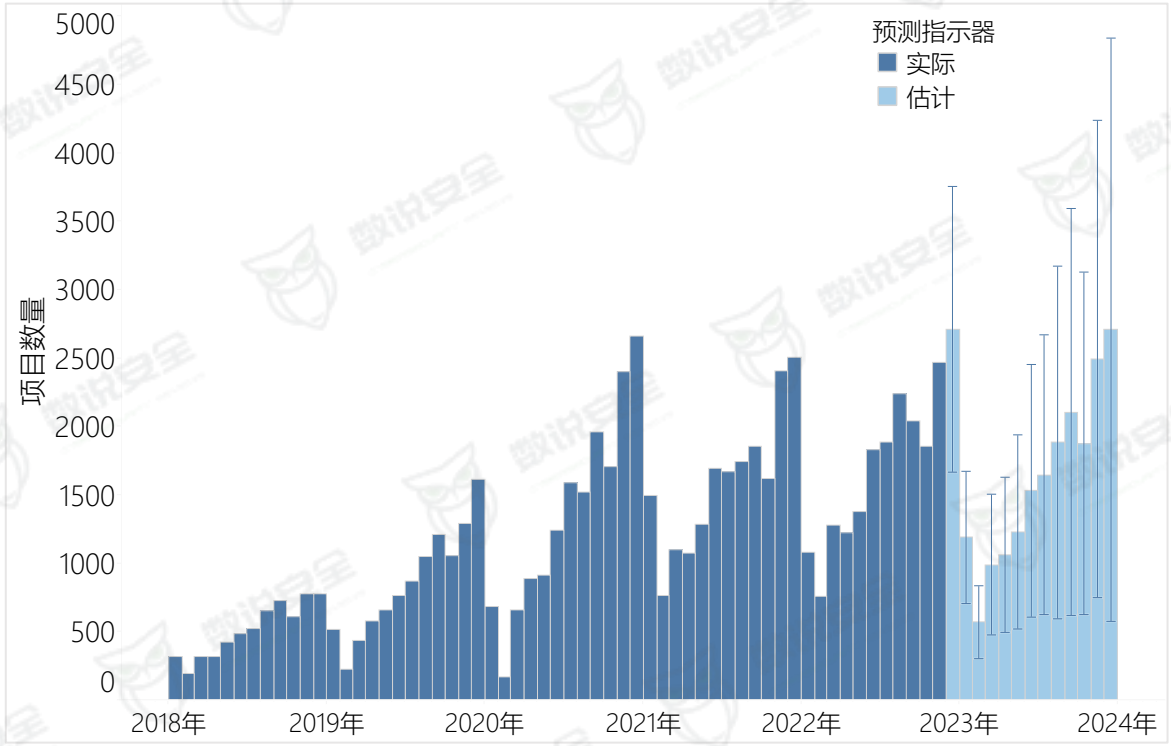
医疗行业在等保2.0正式实施以后，行业需求迅速增加，市场规模扩大。根据数说安全商业分析平台测算，2018-2020年以来医疗行业市场规模分别为20.09、35.76和49.76亿元，2019-2020年分别增长78%和39%。2021年-2022年由于疫情影响，行业整体规模增速放缓，甚至有所下滑。2022年医疗行业市场空间为48.22亿元，相较于2021年同比下滑3.7%。

随着5G、云计算、物联网等新兴技术与传统医疗系统的不断深化融合，我国医疗信息化程度越来越高，逐步向数字化、智慧化医疗演进，蓬勃发展的信息化也使医疗行业面临的安全风险逐渐增多。近年来医疗行业勒索病毒频发、医疗数据频频泄露等问题促使医疗行业客户对网络安全愈发重视，叠加政策的推动，未来医疗行业网络安全的市场规模会进一步扩大。

2018-2022年医疗行业网络安全市场规模（亿元）



2018-2022年医疗行业网络安全项目数量



• 医疗行业市场需求分析

数说安全

等保2.0发布以来，医疗行业以等保合规为基础搭建了网络安全框架，未来十四五期间，以等保合规的网络安全建设依然是医疗行业的保底需求。而不同的医疗客户由于信息化建设的趋势和进度产生了新的安全需求。

<table>
<tr><th>建设方</th><th>信息化</th><th>十三五期间</th><th>十四五发展趋势</th><th>网络安全需求</th><th>共同的需求</th></tr>
<tr><td>卫健委</td><td>区域信息化</td><td>全面健康平台</td><td>区域医疗中心
医共体建设</td><td>1）监管职能的需求：对下属单位的网络安全监管需求提升
2）区域中心建设的安全需求：十四五期间为了均衡区域医疗资源，各地卫健委在全民健康平台的基础上继续打造区域医疗中心，并推动医共体建设，在一定区域内实现居民医疗信息互联互通。区域信息系统的搭建一般项目体量较大，对网络安全和数据安全也产生较大的需求。</td><td rowspan="4">1、安全运营和服务需求提升：
随着医疗信息化进程的蓬勃发展，信息系统应用范围逐渐拓宽。而医疗信息系统运维工作面临着需维护的设备和种类繁杂、业务系统覆盖面较广，运维难度加大，而自主运维存在高维护成本和高维护的风险等挑战和问题。因此近两年医疗行业客户对安全运营和服务的需求大大提升。

2、数据安全需求开始起步：
随着医院业务范围不断扩大，医院系统存在海量的个人信息和健康医疗数据，一旦数据泄露和被破坏，对医院品牌和正常业务系统运行产生极大影响。目前，各级医疗机构在数据安全方面还处于起步阶段，产品采购主要集中在数据库防护和防泄漏等传统产品。随着监管单位加强对数据安全的监管叠加医院业务的需求，未来医疗机构对数据安全的需求会逐步增加。</td></tr>
<tr><td rowspan="3">医院</td><td>临床信息化</td><td rowspan="2">以电子病历为核心的互联互通</td><td rowspan="2">“三位一体”智慧医院建设；远程医疗建设；县级医院综合能力提升；</td><td rowspan="2">1）智慧医院建设带来较强的网络安全能力提升：二级以上公立医院为达到智慧医院评级标准，会对院内电子病历系统、院内管理系统进行升级，建立互联网医院和搭建互联网平台，满足患者的在线服务，另外还需要建立远程医疗服务，对区域的县级医院进行帮扶。根据促进行动，二级以上公立医院都需要建立互联网平台，而建立互联网平台的医院都需要满足等保三级的需求。因此，未来智慧医院评级会带来较强的院内网络安全的升级需求。
2）勒索病毒频发促使医疗机构加强网络安全建设。近年来，由于医疗行业的重要性与业务的特殊性，以及对信息化的程度依赖较高，使其成为勒索病毒的重要攻击目标。 根据Check Point Research（CPR）最新报告显示，医疗行业成为勒索软件攻击的头号重灾区，每个组织平均每周遭受109 次攻击。因此近两年来医院客户对网络安全也愈发重视。
3）“互联网+”促使医院上云意愿的加强：由于医疗机构传统的数据中心临着建设投资大和运维压力大的问题，很难满足医疗信息化未来发展的需求。另一方面，受到疫情影响和国家政策的推动力，以及互联网诊疗的业务特点驱使，互联网+以及互联网诊疗成为了医院上云意愿的最强驱动力。
4）医疗联网设备增加，安全风险增加。物联网技术在医疗领域中应用越来越普遍，涉及从医疗信息化、身份识别、医院急救、远程监护、药品与耗材领域、以及医疗设备和医疗垃圾的监控、血液管理、传染控制等多个方面。而医疗物联网设备的安全性却很薄弱，由于设备联网以及设备的远程运维方式多样，导致风险暴露面积增加。整体来看，医院对联网设备的安全投入较低，需求尚处于起步阶段。</td></tr>
<tr><td>管理系统信息化</td></tr>
<tr><td>互联网医院</td><td>挂缴查医疗咨询</td><td>构建以个人健康为中心三医联动体系过渡</td></tr>
<tr><td>医保局</td><td>国家、省、地市三级医保信息平台</td><td>建立医保局信息平台</td><td>DRG/DIP改革</td><td>医保信息平台成立后对网络安全和数据安全会产生较大的需求</td></tr>
</table>

供给侧分析

- 医疗行业网络安全市场竞争格局
- 解决方案展示

• 医疗行业网络安全市场竞争格局

在医疗行业具有强竞争力的厂商需要具备两点条件：
第一，对医疗机构的业务具有深刻的理解；
第二，覆盖全国的销售网络。

第一梯队：
两者兼备的综合性厂商；一些进入医疗行业较早的综合性厂商，对医疗行业有较深的理解，且具有覆盖全国的销售网络，因此在医疗行业拥有较强的竞争力。

第二梯队：
进入医疗行业时间较短或近两年才把医疗行业当做重点行业进行深耕的综合性厂商；这类厂商医疗行业的案例积累和业务理解相较于第一梯队厂商有所缺乏，但这类综合性厂商拥有覆盖全国的销售网络，只要不断在医疗行业积累经验，有机会涌入第一梯队。

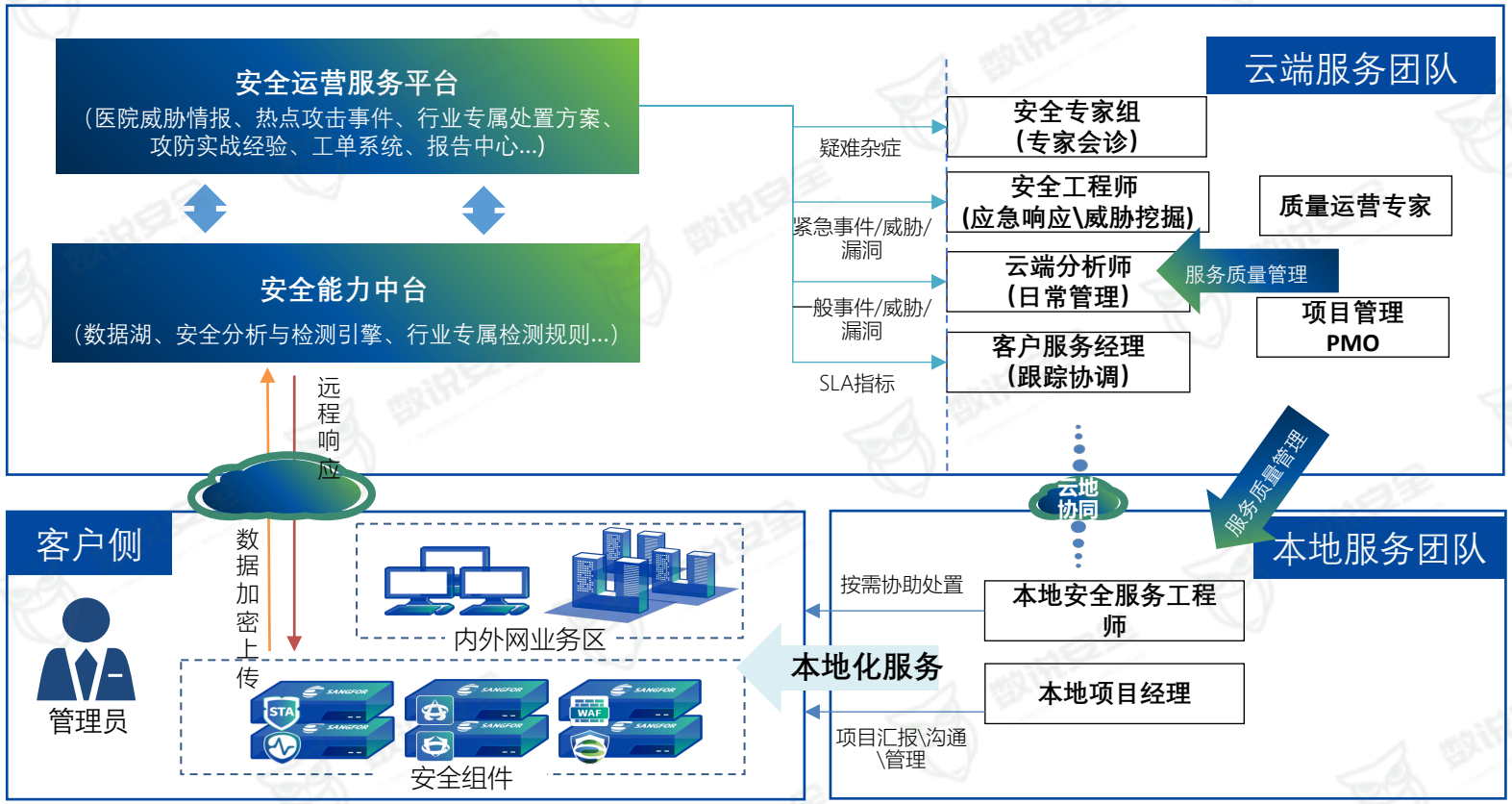
第三梯队：
专注于医疗行业的厂商。这类厂商进入医疗行业时间较久，对医疗行业的业务理解深刻，尽管没有综合性厂商的销售网络覆盖广泛，也可以通过丰富的医疗行业经验为客户提供优质的解决方案和服务。

• 深信服-医疗行业专属安全运营中心（成都）

深信服科技股份有限公司是专注于企业级网络安全、云计算、IT基础设施及物联网的产品和服务供应商，拥有深信服智安全和信服云两大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让每个用户的数字化更简单、更安全。目前，深信服员工规模超9000名，在全球有50余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业等。

深信服医疗行业专属安全运营中心（成都），目前核心技术团队规模50+（含服务专家、应急响应和威胁狩猎专家），作为安服BG的核心部门，承担着安全托管服务的高质量交付任务，致力于为全国医疗用户提供专业、省心的云化安全服务。

项目情况



项目亮点

两大属性：

1、可视化可衡量可监督
- 可视：基于攻击路径的可视化溯源分析
- 可衡量：多维度的结果总结
- 可监督：监督机制与调查结合提升服务质量

2、行业专注
- 专注医疗：行业属性的加持，更好和客户“对话”
- 专注医疗：行业情报的集中整合，早发现早治疗

三大能力：

1、7*24小时守护，快速响应
- 7*24h守护，风险快速响应
- 安全专家15分钟响应，平台联动组件自动化响应
- 专属服务经理，全天候持续监测

2、风险管控，有效预防
- 组织安全策略应用既有效
- Usecase过滤96%无效告警，专家研判确保99%准确
- 业内首个风险预防库，全面检测系统脆弱性
- 资产管理环境梳理，提前发现脱缰设备

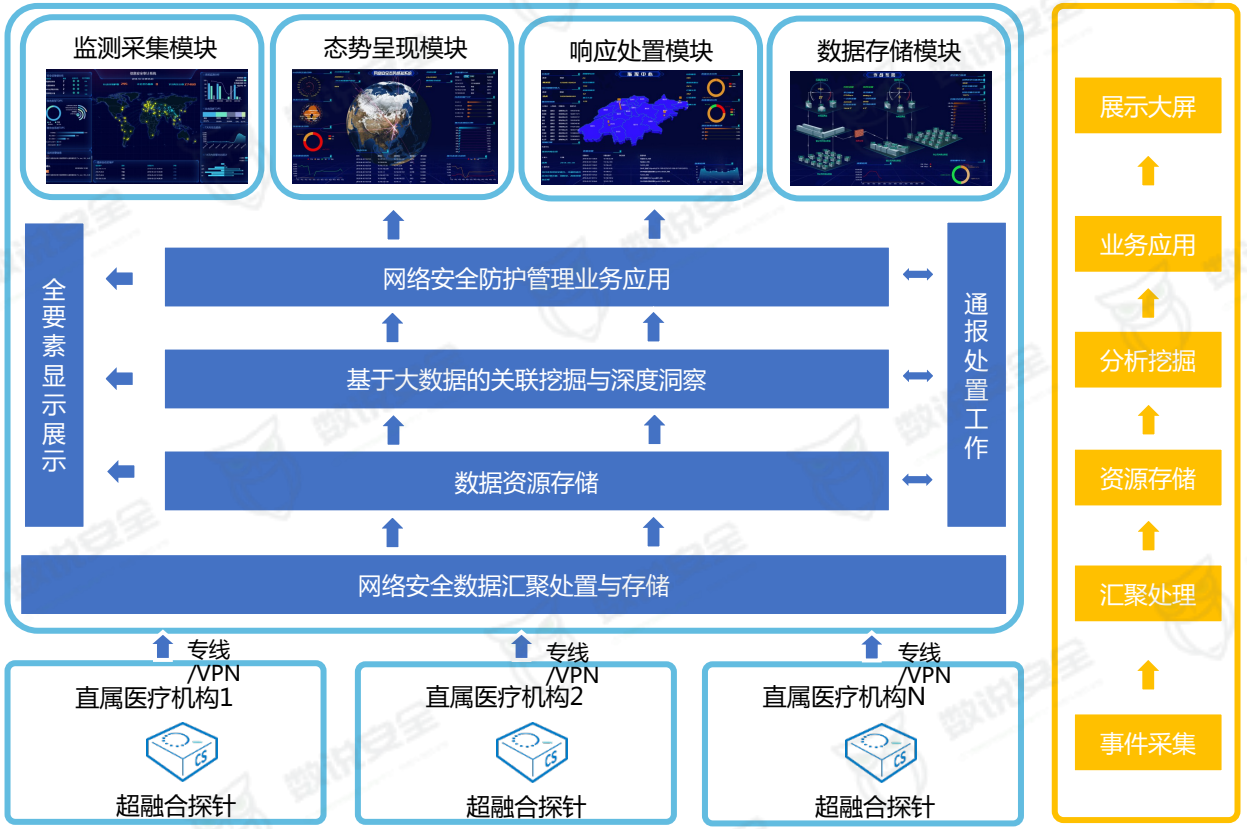
3、主动闭环，持续提升
- 勒索专项风险排查与加固
- 流行风险预测，早一步发现安全隐患
- 线上专家团支撑服务经理/安服工程师修复风险-组织力量

• 启明星辰-某省医疗卫生行业网络安全监测预警平台

数说安全

启明星辰信息技术集团股份有限公司成立于1996年，总部位于北京，公司于2010年在深圳A股中小板上市，是国内极具实力的、拥有完全自主知识产权的网络安全供应商。启明星辰集团依托核心技术优势、丰富实践经验和前瞻性发展战略，通过安全原生创新和场景化创新，不断引领数据安全、工业数字化安全、新算力安全等板块的高增长，致力于打造自主可控的安全生态体系，为用户提供安全服务，客户覆盖政府、运营商、金融、税务、能源、交通、制造、医疗等多个行业领域。

项目情况



项目亮点

需求背景：

搭建集预防、监测、分析、处置为一体的省级医疗卫生行业网络安全预警监控平台，对全省范围内各级卫生医疗机构进行实时网络安全监管，实现由被动防御向主动防御转变、静态防御向动态防御的转变、分散防御向协同防御的转变，逐步构建覆盖全网纵深协同网络安全防御体系。

建设意义：

1. 落实国家政府和医疗卫生行业政策法规要求，有效满足网络安全等级保护新标准的要求
2. 提升某省医疗卫生行业网络安全监测预警能力，落实行政监管服务职能
3. 贯彻全天候全方位感知网络安全态势的要求
4. 抵御新型网络安全攻击，促进协同联动防护能力
5. 强化网络安全应急响应、重要时期安全保障技术支撑能力

• 安恒信息-医共体解决方案

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于2007年，于2019年登陆科创板。作为行业领导者，安恒信息秉承“构建安全可信的数字世界”的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，参与了近乎全部国家重大活动网络安保，实现零失误。2020年11月23日，安恒信息正式成为2022年杭州第19届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

项目情况

方案价值

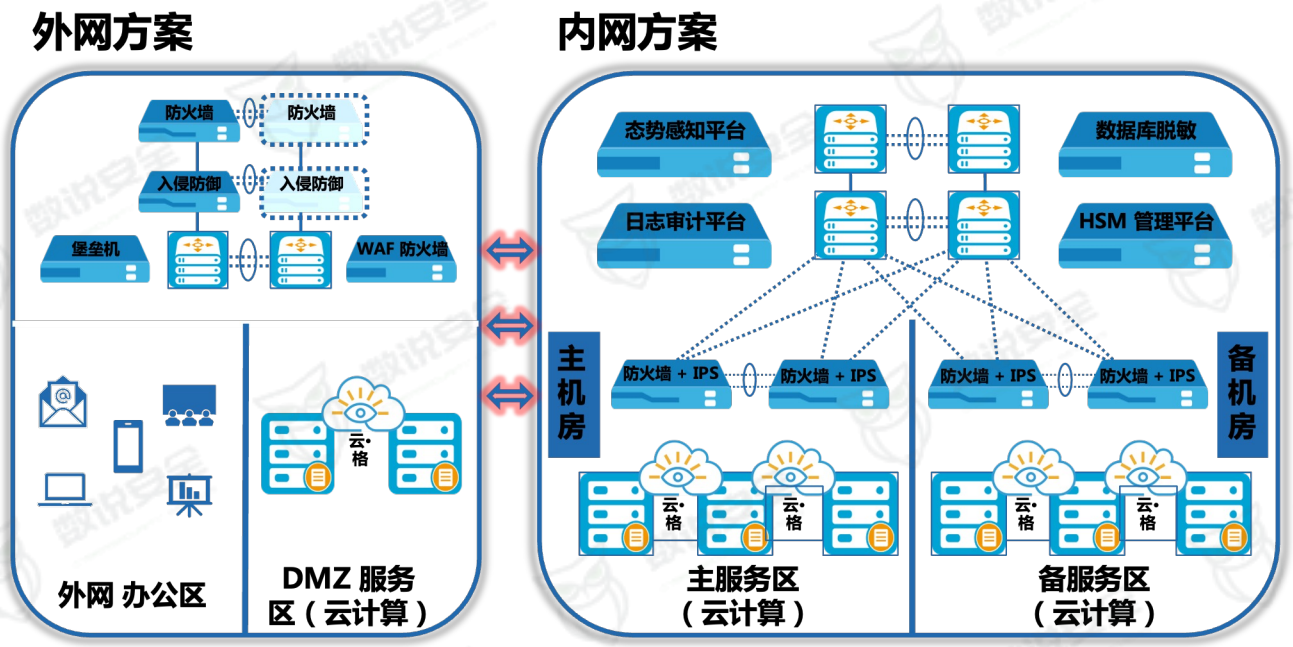
安恒信息为医共体打造全网合规智能防护，安全统一管理的医共体安全解决方案通过分支边界统一防护管控，构建安全可视的系统边界；通过终端管控，行为管理，建立统一安全基线；牵头医院建立“一个中心，三重防护”的安全防护体系，实现分支安全统一管理，全网态势可视可控，清除医共体系统安全薄弱点，保障核心系统安全无忧。

- **满足政策合规要求：**方案满足等级保护第三级及医共体相关政策要求，满足相关法律法规，帮助医共体规避合规安全风险，护航医共体信息系统安全运行。
- **全网资产一体化安全管控 ：**下一代防火墙与EDR高效联动，安全能力彼此赋能，南北向流量管理防止病毒侵入，东西向流量隔离防止病毒横向扩散，资产漏洞扫描情况统一处置，实现医共体系统资产一体化安全管控 。
- **建立医共体统一安全基线 ：**安全漏洞统一管理，终端安全策略统一配置，系统状态统一监控；规范成员上网行为，设置口令策略，限制风险操作；统一实现入网认证，未安装EDR禁止入网，高风险资产禁止入网，建立医共体统一安全基线。
- **整体安全状态清晰感知 ：**通过威胁情报及大数据分析技术，关联分析网络侧与终端侧告警，威胁定位更精准，安全事件更真实；全盘攻击态势可视化呈现，终端，边界安全状态统一体现，医共体整体安全状态清晰感知。

• 山石网科-某省大三甲医院数据中心建设（国家区域医疗中心）

山石网科成立于2007年，专注于网络安全领域前沿技术的创新。目前已经形成并具备“全息、量化、智能、协同”四大技术特点的方案理念，涉及边界安全、云安全、数据安全、业务安全、内网安全、智能安全运营、安全服务、安全运维等的八大类产品服务，50余个行业和场景的完整解决方案。公司迄今已为金融、政府、运营商、互联网、教育、医疗卫生等行业，覆盖50多个国家和地区，累计超过23,000家用户提供产品服务，高效稳定支撑客户业务的可持续安全运营工作。山石网科在苏州、北京和美国硅谷均设有研发中心，于2013年、2016年和2019年成功申报国家高新技术企业。

项目情况



外网建设： 通过防火墙、IPS（入侵防御）、堡垒机、WAF防火墙等安全设备，基于等级保护要求分别落实办公区、DMZ区、管理区、出口区等分区准则，确保各区域流量合理检测、分析等问题；

内网建设： 通过态势感知、日志审计、数据库脱敏、HSM安全管理平台以及数据中心级防火墙（含IPS模块），以分析、防护、审计等思路严格落实管理和技术防护机制；

云计算建设： 通过微隔离安全防护技术，基于云格产品实现虚拟主机的立体化防护，确保流量可视、威胁可检测、应用可管控的安全管理与防护需求；

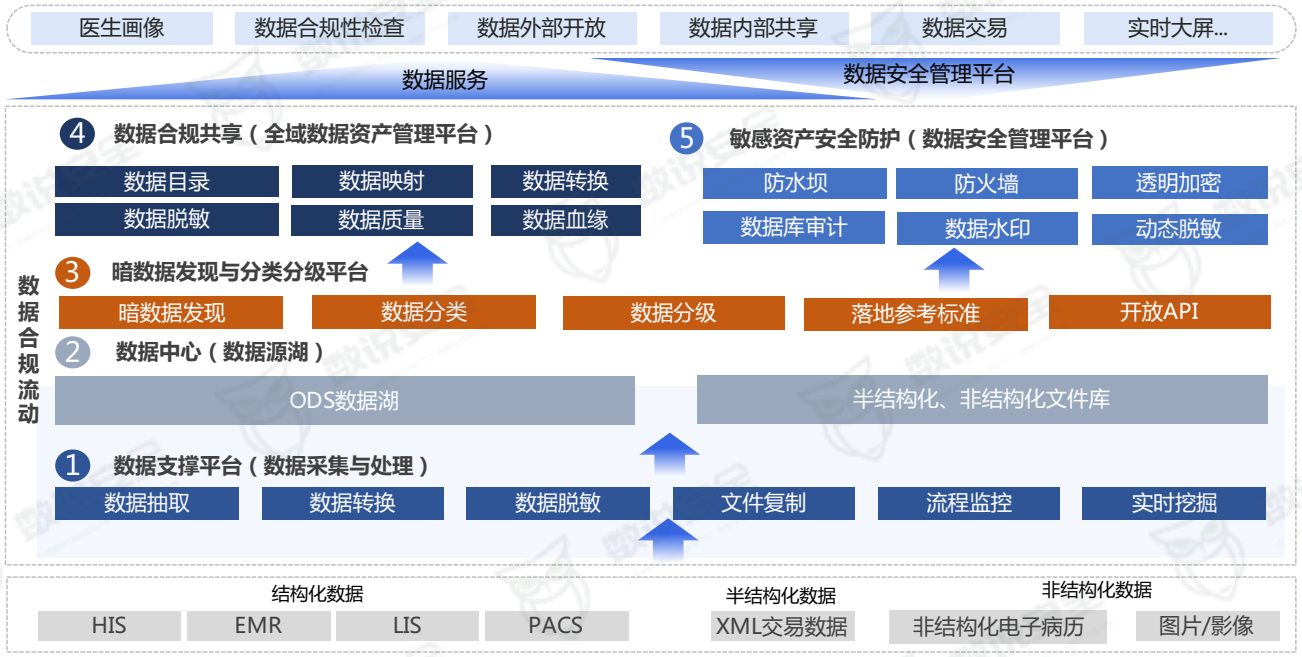
方案价值

- **合规管理能力：** 基于安全咨询、安全设计、安全建设等环节，助力客户在落实国家安全政策的要求下，不断具备等级保护 2.0 的能力塑造，为信息化可持续发展提供基础；
- **纵深防护能力：** 基于分区分域保护原则，针对边界防护、运维管理、安全审计、云内防护等层面，以智能 AI、边界NDR、XDR体系等新兴技术的产品实践化助力客户实现纵深防护体系建设，解决未知的、高潜伏性的网络安全威胁与攻击；
- **安全管理能力：** 基于态势感知平台、威胁探针和相关安全组件关联分析，协助客户网络安全决策性工作，将勒索病毒、APT攻击等行业突出安全问题“ 防范于未然 ”；

• 美创科技-某三甲医院基于分类分级的数据安全防护建设实践

杭州美创科技股份有限公司成立于 2005 年，总部位于浙江杭州，专注深耕数据安全领域十数年，拥有数据安全、数字化转型、运行安全三大业务及技术运维和安全运营服务，研发形成数据分类分级、数据安全防护、数据安全审计、数据安全运营、数据资产管理、可视化应用、数据库运行安全、灾备集中管控等 30 余款产品，并率先落地实践数据安全治理服务。客户数量过万，覆盖32个省市的医疗卫生、政府、教育、金融、能源电力、物流交通等行业。

项目情况



项目亮点

• 体系化的数据安全防护

从全局性策略出发，以互联互通的安全技术为保障，以平台化的管理工具为支撑，搭建出真正能够有效对抗威胁，保障应用的数据安全体系。

• 智能精准的数据分类分级

通过智能化敏感数据分类分级平台与专家服务团队的支持，持续帮助用户对全院数据资产中的敏感数据进行识别发现与分类分级。

• 纵深防御的防护构建

针对医院核心系统综合采用泄露防护、入侵防护、风险内控、安全审计等多种技术和措施，实现数据的可用性、完整性和保密性保护，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，保障信息系统整体的安全保护能力。

• 联软科技-终端一体化解决方案框架建设

深圳市联软科技股份有限公司（简称“联软科技”）创立于2003年，专注于企业级网络安全市场，主营业务是为政企客户提供网络安全产品和服务。围绕端点安全、边界安全和云安全，为客户打造了网络准入控制、终端安全管理、数据防泄露、数据安全摆渡、软件定义边界、网络入侵检测、移动端安全管理、云主机安全管理、互联网安全监控SaaS 平台、网络空间资产测绘、终端检测与响应等产品的综合安全解决方案。18年来，联软科技从全球较早的网络准入控制厂商之一，成长为中国企业端点安全领域的领导者、国产自主可控的网络安全新基建领军厂商、并成为国内率先落地基于“零信任安全”产品的厂商之一。

项目情况

联软端点安全一体化平台

分级安全管理	安全管理流程	可视化展示引擎	大数据智能引擎
可信	**可管**	**可控**	**可防**
适应复杂网络	安全基线管理	敏感数据发现	数据采集分析
资产发现管理	安全加固管理	数据安全保护	威胁响应处置
基于场景接入	统一策略管控	外发通道管控	攻击欺骗诱捕
威胁持续检测	运维响应支持	泄密溯源取证	用户行为分析

管控对象

内部员工	LAN/WAN	PC终端	内部数据	Windows服务器
访客	无线网络	移动终端	互联网数据安全导入	Linux服务器
外部人员	VPN接入网	IoT终端	打印 / 截屏	中间件/数据库

方案价值

该方案实现对医院内部各种操作系统和各种终端的集中管控，在同一个平台中集中实现网络准入控制、补丁管理、桌面管理、安全加固、U盘管理、网络行为审计、敏感数据管理、数据防泄漏、移动终端管理等多项管理要求，相比传统方案：

- 一个平台、多种技术、综合解决信息安全问题，降低运维工作量和学习成本；
- 16年终端安全管控经验，管理超过2300W终端，卓越的终端兼容性确保项目落地；
- 满足卫健委规范要求和网络安全等级保护要求；
- 全量网络资产发现，协助院内快速进行终端运维工作；
- N合1的解决方案，减少院内在终端安全方面的重复投资。

• 贝格通-某医院核心业务系统保障防御平台解决方案

山东贝格通软件科技有限公司成立于2015年，运营中心设在青岛、研发团队在北京。贝格通以安全运维服务支撑+安全产品工具营销为核心。持续打造自主知识产权的网络安全产品线。随着数字中国战略的推进，贝格通科技在医疗行业以面向实战化的安全场景，不断推出适应新场景的安全产品和解决方案。作为用户背后的网络安全专家，贝格通科技一如既往以自强不息、持续创新、优质产品、专业服务，提供行业一流的网络安全服务，成为备受用户信赖的网络安全公司。

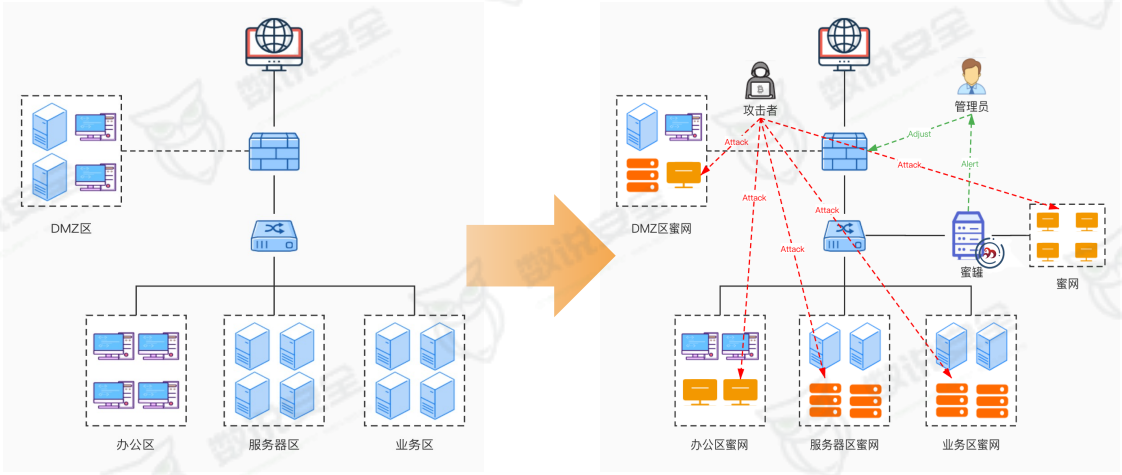
项目情况

需求背景：

为了保障医院的平稳发展，必须加强医院针对核心业务系统的防御建设，从而实现医院安全管理信息化，进一步提高医院的运行效率。

通过对业务的仿真，构建虚假业务的蜜网，通过蜜饵主动引诱攻击者攻击处于蜜网的虚假业务系统，捕获攻击行为并进行告警。实现阻止网络攻击，混淆攻击目标，从而保护真实业务系统，实时定位攻击源，使被动防御变为主动防御，提高防御能力及应急响应效率。

建设方案：



用户收益

- 贝格通医院核心业务系统保障防御的建设为医生搭建了一个安全、稳定的诊疗环境，为医务工作者提供高效的业务看诊环境，使医务人员能够迅速地对病人的病情作出诊断，从而使病人得到更及时、有效的救治。
- 通过全院覆盖的标准化、智能化的仿真安全管理控制措施，使医疗活动得到最大化的效益，防止医护人员在诊疗过程中出现因网络环境问题导致的意外情况，从而减少医疗事故的发生，全面提高医疗质量。
- 贝格通医院核心业务系统保障防御平台通过全医院业务系统的覆盖仿真，使外来黑客等攻击者无法定位真实核心业务系统，从而无法进行加密、勒索等非法操作，将医院业务系统的安全风险降低至最低点，保证全医院稳定、高效的运转，从而提高医院的整体经济效益。

• 盛邦安全-某省卫健委互联网资产普查及网站安全监测案例

盛邦安全专注于网络空间安全领域，以“让网络空间更有序”为使命，为客户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。公司倡导“安全有道，治理先行”的发展理念，秉持精准识别、精确防御、深入业务场景的“两精一深”的研发战略，聚焦漏洞及脆弱性检测、应用安全防御、溯源管理及网络空间地图等技术领域，致力于从网络空间视角剖析数字世界，构建数字世界的网络空间地图，赋能行业用户的数字化安全转型，护航国家网络空间安全战略的实施落地。

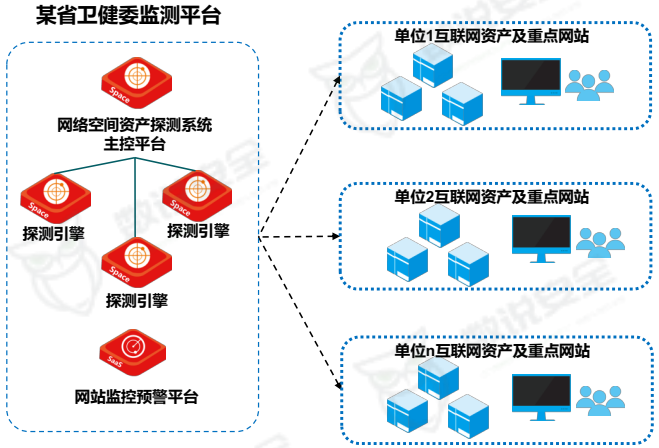
项目概况

需求背景：

落实《关于促进“互联网+医疗健康”发展的意见》，通过对当前全省医疗卫生行业的安全状况和安全事件分析，结合现阶段网络与信息安全监控保障工作的实践与经验总结，如何全面掌握全省范围内互联网资产整体情况和全面监控重点保障网站的安全情况，是目前最为迫切的需求，同时对网站的可用性（访问延时）进行监控，并分析网站访问延时产生的原因，也是网站监测的重要目标。

建设方案：

（1）互联网资产存活探测与资产识别画像；
（2）互联网资产脆弱性检测及漏洞验证；
（3）网络资产拓扑绘制与可视化分析；
（4）网络资产统一监控管理
（5）多级分布式部署
（6）重点网站（安全性、合规性、可用性）7*24 小时实时监测预警



方案优势和用户价值

方案优势：

（1）“全”，丰富的资产指纹库，识别准确率高
（2）“准”，多样化漏洞标准，PoC 检测误报率低
（3）“快”，高性能采集技术，全网单端口探测 2 小时以内
（4）“深”，协议深度解析数据深度挖掘，网络资产纵深全面掌控
（5）“实”，全面掌握网站风险情况，实时监控网站安全状态

用户价值：

（1）帮助用户快速摸排互联网资产暴露情况，发现未知资产，排查敏感信息泄露，减小威胁暴露面。
（2）特定漏洞快速普查，重大安全事件，高风险精准定位，各个击破定点加固，如勒索病毒、struts2安全漏洞，6小时完成检测和绘制报告，评估影响面。
（3）绘制完整的网络地图、资产拓扑图，资产线索链条清晰，实现安全事件精准定位、灾情范围快速定界、预警通报及时准确、执法检查证据清晰。
（4）完善资产管理及安全建设体系，为统一监管提供技术依据和关键指标。
（5）提升重点网站安全实时监测预警能力
（6）通过自动化的技术手段，降低运维成本

• 指掌易-某知名三甲医院移动终端安全项目

北京指掌易科技有限公司是成立于2013年的高科技软件企业，总部位于北京，分别在北京、南京、大连设立研发中心，业务覆盖全国所有省份以及部分海外市场。指掌易顺应数字化转型大势，针对万物互联场景，以各类数字化终端及业务为切入点，以零信任和移动化为技术基础，提供数字化安全、数字化联接、数字化智能与体验等软件产品和方案，打造更安全更易用的数字化工作环境，充分服务于医疗、政府、金融、国防、运营商、能源、交通、制造等行业的数字化转型。

项目情况

项目亮点和项目价值

项目亮点：

- 开展移动应用标准化的生命周期管理建设。实现对 APP 从测试、推广、上线发布、版本更新、应用下架整个生命周期的安全管控。
- 构建移动应用安全监测与运营分析机制。通过构建统一的移动安全监测服务平台，实现能够及时发现应用安装情况、启动崩溃情况、使用热度、使用时长、违规情况等，填补医院对已投产上线客户端环境安全、可信监测等需求的空缺。
- 构建自适应的移动端数据安全防护。通过对接入终端特征信息绑定，用业界领先的自动封装虚拟安全域技术，在一套平台上，完整实现对配发终端从设备，应用，数据，上网行为等全方位强管，保护个人隐私的同时解决办公应用数据的安全。
- 建立移动安全相关管理制度规范。针对应用发布、应用更新、应用下载使用、数据使用、终端管理等方面建立相关制度规范。

项目价值：

- 移动医生、移动护理方案在医院顺利实施，助力推动医院移动化建设，大幅度提升了院内医护人员的协作效率，保护了医患数据安全。

总结

• 总结

数说安全

信息化趋势

以公立医院为中心的医疗服务模式

数据流通弱

医联体、医共体、区域医疗、互联网医院等
医疗服务主体增多

以患者为中心的医疗服务模式

数据流通强

监管侧趋势

弱 → 强

需求侧趋势

时间节点：2011年《卫生行业信息安全等级保护工作的指导意见》

1.0：等保合规是基本需求

时间节点：2016年《网络安全法》颁布

2.0：体系化安全运营成为主流

时间节点：2021年《数据安全法》颁布

3.0：数据安全时代开启

2011年至今，医疗行业以等保合规建设为中心推动网络安全建设，目前三级医院已普遍完成等保合规建设，未来等保合规依然是医疗行业基本需求。

随着《网络安全法》的颁布，以及护网的常规化运行，促使体系化的运营逐渐成为主流。与此同时，大部分医疗客户已经满足了合规要求，但存在安全产品堆叠，运维工作量大，内部安全人员不足等挑战。因此持续有效的安全运营和服务成为了医疗行业客户的重要需求。

2021年《数据安全法》颁布，医疗行业对数据安全的关注度大幅提升，但也面临着医疗行业内数据分类分级标准不完善，数据安全成功的实践经验尚少等问题，当前医疗行业购买数据安全还是为了满足合规要求。随着智慧医疗体系的建设，数据在院内、院外、区域之间的流通加剧，如何保障数据安全与患者隐私将成为医疗行业的重要议题。

供给侧趋势

能力要求：
业务理解
行业属性
服务能力

等保合规时代，不需要对医疗业务有较深的理解，标准化的产品就可以满足大部分客户的合规需求。

当前阶段医疗行业对供应商的要求提高，供应商需对医疗机构的业务理解加深，安全防护产品需要和业务系统融合，因此提供的解决方案和服务的医疗行业属性逐渐加强。

在医疗数据互联互通建设的信息化趋势下，数据安全与业务高度融合。因此从数据分类分级到相应的数据安全策略的匹配都需要供应商对医疗业务有深刻的理解，同时也要求供应商提供适配医疗系统的解决方案和产品。目前供应商提供的医疗数据安全解决方案和服务的成熟度尚不够高，需要累积案例经验不断提高数据安全的解决方案成熟度。

低 → 高

THANK YOU

以数据为基础的网络安全产业研究平台

关注“数说安全”公众号，私信回复“医疗安全报告”，获取报告完整版