2023中国智慧医院研究报告：医院信息与网络安全篇

亿欧智库 https://www.iyiou.com/research

亿欧智库

目录

CONTENTS

亿欧智库

目录

CONTENTS

1.1 国家始终高度重视网络安全问题，二十大的顺利召开揭示其已达到国家战略层面

- “十二五”期间，中国颁布《国家安全法》，安全一词首次与国家生存发展联系起来，此后的“十三五”和“十四五”时期，国家先后出台并实施了《网络安全法》、《密码法》、《民法典》、《数据安全法》、《个人信息保护法》，**“五法一典”构成了中国信息与网络安全的法律法规体系。**由此可见，中国政府在网络安全的问题上始终保持高度重视，网络安全是国家安全的重要组成部分。
- 2022年10月，二十大在北京召开，紧紧围绕发展和安全两件大事，其中安全一词被提及91次，网络安全保障体系建设成为健全国家安全体系的重点任务之一，深刻表明**网络安全已经达到国家战略层面。**

亿欧智库：信息与网络安全相关法律法规

《国家安全法》：建设网络与信息安全保障体系，提升网络与信息安全保护能力；加强网络管理，防范、制止网络攻击、网络入侵等网络违法犯罪行为

《网络安全法》：加强网络安全管理，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改等行为；防止信息泄露、毁损、丢失

《密码法》：技术性、专业性较强的专门法律。密码作为网络与信息安全的核心保障技术和基础支撑，密码合规是企业网络安全与数据合规工作中不可或缺的部分

《民法典》：为我国未来个人信息保护法及数据保护的法律体系构建。不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息

《数据安全法》：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。开展数据处理活动应当加强风险监测

《个人信息保护法》：为数据安全法原则在个人信息保护领域的延申，在国家层面建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为

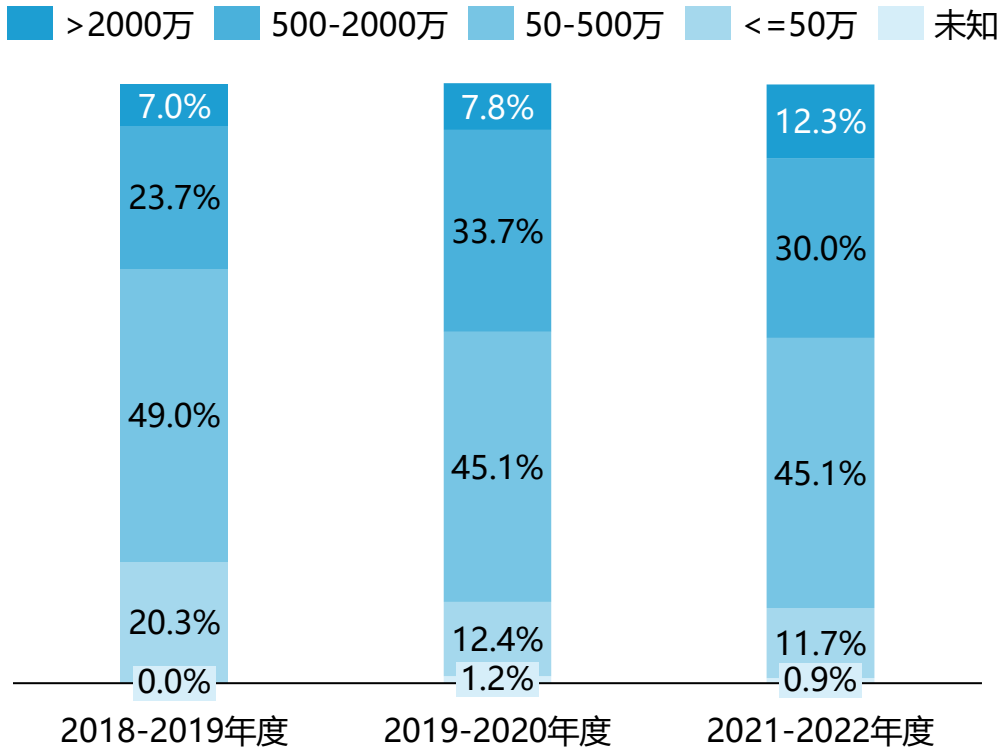
二十大报告指出在健全国家安全体系任务中，**网络安全保障体系建设**是重点任务之一，加快建设**网络强国，**健全网络综合治理体系，推动形成良好网络生态。同时最高院、最高检发声将促进数字经济、平台经济规范健康发展；推动健全大数据、人工智能、基因技术等领域**知识产权的保护规则。**相关代表们则表示数字技术“双刃剑”效应不断增强，成为诱发安全隐患的主要原因，需**加强维护网信安全的职责使命**，强化关键核心技术攻关

数据来源：公开资料、亿欧智库

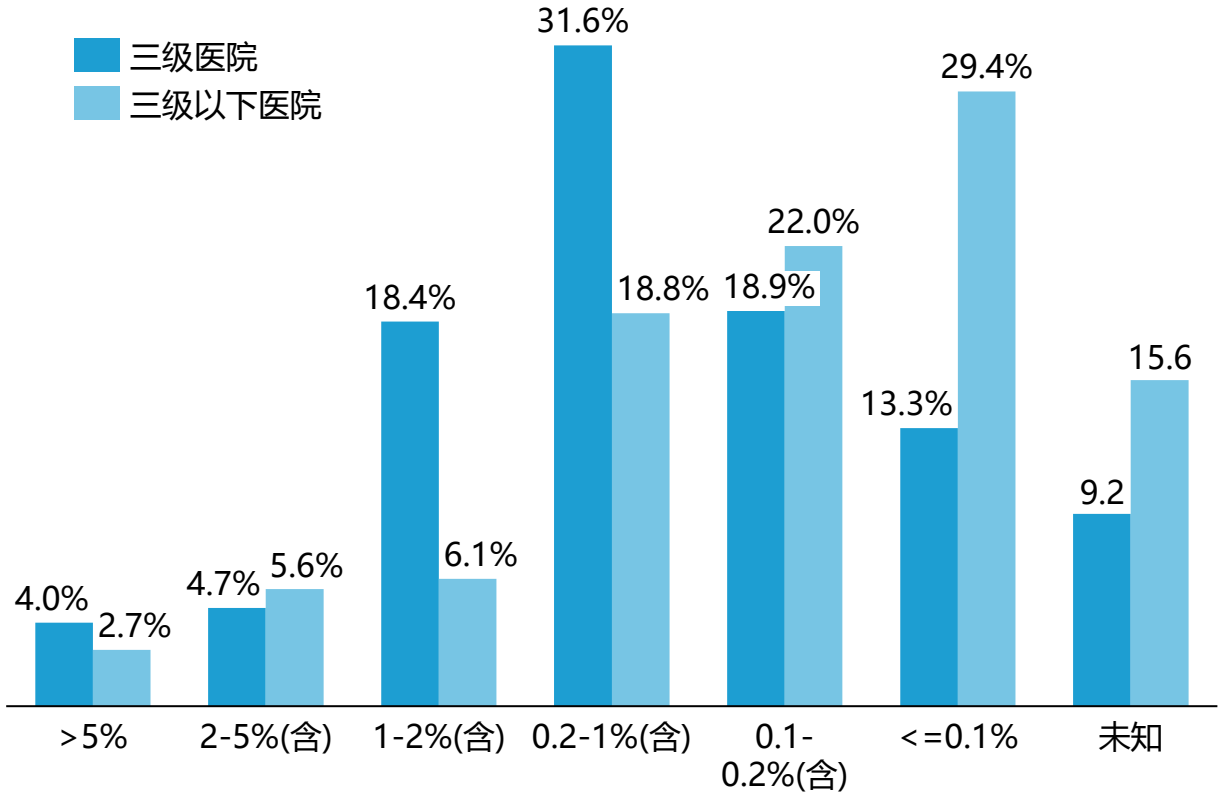
1.2.1 智慧医联体开始建立，医院信息化方面的投入金额持续上升，信息化建设不断深入

- 2023年2月国家卫健委和发改委等六部门联合发布《关于开展紧密型城市医疗集团建设试点工作的通知》，再次驱动中国智慧医院的发展，标志着中国开始探索建立智慧医联体，从单个医院的信息化整体架构设计和建设走向区域医疗的信息化，**同时网络安全也成为重点工作之一**。
- 据CHIMA统计数据显示，2021-2022年度12.3%的受访医院在信息化方面投入2000万元以上，11.7%的医院投入低于50万元，比2018-2019年度分别增加75.7%和减少42.4%，**凸显中国医院对信息化方面的投入愈发重视，各医院结合预算情况加大投入金额**。在信息化投入预算占总预算比例方面，不同等级的医院存在明显差异，中国三级医院整体投入占比高于三级以下医院，其中，4%的三级医院投入占比达到5%以上，接近30%的三级医院投入占比1%以上，而三级以下医院对此的比例分别为2.7%和23.6%，超过50%的三级以下医院投入占比为0.2%以下。

亿欧智库：2018-2022年中国医院 (%) 在信息化方面投入不同年度对比



亿欧智库：2021-2022年度中国医院 (%) 信息化投入预算占总预算比例



数据来源：CHIMA、亿欧智库

1.2.2 医疗机构网络安全事件频发，《医疗卫生机构网络安全管理办法》出台

- 医疗机构在信息化建设的不断深入中以及凭借其数据的高价值性和系统的脆弱性，一直频繁受到网络攻击，2021年针对全球医疗机构的勒索软件攻击在达到了166起，造成数百亿美元的损失，同时，据相关数据显示，黑客曾对医疗行业的暴露破解达到了单日80万次的高峰，因此，加强医疗机构的网络安全管理已经可不容缓。
- 在中国，2022年8月，卫健委等三部门为指导医疗卫生机构加强网络安全管理颁布《医疗卫生机构网络安全管理办法》，成为卫健委首个具体的医疗网络安全管理办法，其中提到需要保证医疗行业信息系统建设时**安全保护措施同步规划、同步建设和同步使用**，该管理办法将大力推动中国医疗行业信息与网络安全的发展。

亿欧智库：中国医疗机构网络安全事件举例

2019年1月 **河南安阳市某医院业务系统被攻击破坏**
因未履行网络安全保护义务，造成业务系统被攻击破坏，正常工作无法开展。

2019年5月 **重庆永川某私立医院业务全面“停摆”**
未安装边界防护设备、未安装日志行为审计设备，未设置数据安全备份策略等其他网络安全技术措施，使医院业务在互联网上长期处于为保护状态。黑客通过互联网攻破医院系统后植入勒索病毒，导致医院业务全面“停摆”。

2019年12月 **山西省忻州市某医院未履行网络安全等级保护制度**
该医院网络安全意识淡薄，未确定网络安全责任人，未制定网络安全应急事件预案，未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。

2020年4月 **青岛胶州某医院患者就诊名单泄露**
泄露信息包括患者姓名、电话、身份证号码、个人详细居住地址、就诊类型等，共涉及上千人。

中国医疗行业监管政策：《医疗卫生机构网络安全管理办法》

出台背景	随着高质量发展纵深推进，全国卫生健康领域迎来重要机遇期，信息化发挥着关键的支撑作用，医疗健康数据不仅是重要的生产要素，更是国家基础性战略资源，**而该数据一旦遭到篡改和泄露，对医疗机构和患者都会带来极大的负面影响。**《办法》的出台为医疗卫生机构指明了网络安全管理的总方向，防范网络安全事件发生，体现了统筹安全与发展的总体平衡。
要点总结	**围绕顶层设计** 在整体网络安全体系的基础上，依据数据的特性建构网络和数据安全顶层设计，落实安全责任分工，明确数据管理部门、业务部门、信息化部门在网络和数据安全管理工作中的权责。
	围绕制度保障 明确医疗卫生机构应建立健全安全管理制度、操作规程及技术规范，保障数据安全和数据应用的有效平衡，在实际运用中，应将总体安全策略拆解到具体安全管理要求，并通过安全技术实现管理要求，最终融入对应到安全运营体系中，形成融合管理、技术、运营三位一体的立体化网络安全管理模式。

虽出台相关管理办法，但行业整体的网络安全规范尚未形成体系，医疗作为“十四五”国家重点关注的行业之一，卫健委预计将会加强医疗行业的网络安全标准建设。

数据来源：公开资料、亿欧智库

1.3 医院信息与网络安全研究范围

- 医院医疗设备和信息设备种类繁多，各类业务系统（HIS、LIS、PACS等）和人员构成也相对复杂，因此医院信息与网络安全面临诸多隐患，常见的医院网络攻击方式包括网络钓鱼、勒索攻击、挖矿病毒、数据泄露等。
- 亿欧智库认为，医院信息与网络安全分为系统安全、数据安全和云安全三个方面。

亿欧智库：医院信息与网络安全研究范围

自主可控是实现医院信息与网络安全的手段，而国产化替代是自主可控的关键路径

医院信息与网络安全

系统安全
构建医院信息化建设中的网络安全体系，涉及基础软硬件和网络安全产品包括态势感知和各类安全服务，目的是用来预防网络遭受攻击

数据安全
保护数据在全生命周期中的各个环节免遭内部的外部威胁，防止数据泄露

- **院内应用**：数据在院内各科室各信息系统之间共享传输的安全
- **院外应用**：医院数据开放后在医院之间和各企业之间共享传输的安全

云安全
医院上云后，需要负责医院云平台中各个系统和数据的安全

*信创与国产化替代的关联：国产化替代是信创背后的核心逻辑，而信创相比国产化替代多了技术或应用上的突破与创新，本报告将主要关注国产化替换阶段过程中的医院信息与网络安全

数据来源：亿欧智库

1.4.1 “十四五”相关规划和地方政策驱动医院IT系统国产化替代的进程

- 在中国国产化替代的进程中，目前已经进入到软件、硬件联动，系统全面升级的阶段，国产化替代也意味着中国IT行业的发展战略调整为**自主可控取代借力发展**。
- “十四五”期间，国务院、卫健委等部门陆续发布《“十四五”数字经济发展规划》、《“十四五”国家信息化规划》和《“十四五”全民健康信息规划》等相关规划，皆在明确利用国产化替代来加速赋能数字化发展，构建数字中国。
- 2023年是中国信创的第四年，重点行业升级成为重中之重。医疗行业国产化替代速度远不及党政、金融、电力等行业，但2022年下半年起，随着各地逐步响应“十四五”相关规划，规定医院禁止采购进口设备的政策陆续出台，大力支持国产系统自主创新、自主研发，从而推动智慧医院网络安全关键技术发展。

亿欧智库：“十四五”相关规划梳理

创新发展 自主可控 安全可靠 提振市场信心

《“十四五”数字经济发展规划》 2021年12月
着力提升基础软硬件、核心电子元器件、关键基础材料和生产装备的供给水平，强化关键产品自给保障能力；加强面向多元化应用场景的技术融合和产品创新，提升产业链关键环节竞争力；数字技术自主创新能力显著提升，数字化产品和服务供给质量大幅提高，产业核心竞争力明显增强，在部分领域形成全球领先优势。

《“十四五”国家信息化规划》 2021年12月
十项重大任务中包括培育先进安全的数字产业体系、构建产业数字化转型发展体系和建立健全规范有序的数字化发展治理体系；到2025年，数字中国建设取得决定性进展，信息化发展水平大幅跃升，数字基础设施体系更加完备，数字技术创新体系基本形成。

《“十四五”全民健康信息规划》 2022年11月
以引领支撑卫生健康事业高质量发展为主题，以数字化、网络化、智能化促进行业转型升级，重塑管理服务模式的体系框架；推动我国自主技术与全球同步发展，探索国际健康医疗发展合作新模式，不断提升我国全民健康信息化应用水平、产业核心竞争力和国际影响力。

地方政府

亿欧智库：地方政府陆续出台相关标准政策

深圳市
2022年9月，深圳政府明确公立医院设备采购必须优先国产，因工作需要确需采购进口产品的，实行审核管理。

湖北省
2022年6月起，湖北省政府对于技术复杂、专业性较强的项目，包括需定制开发的信息化建设项目、采购进口产品的项目等，必须开展需求调查，进行可行性分析。

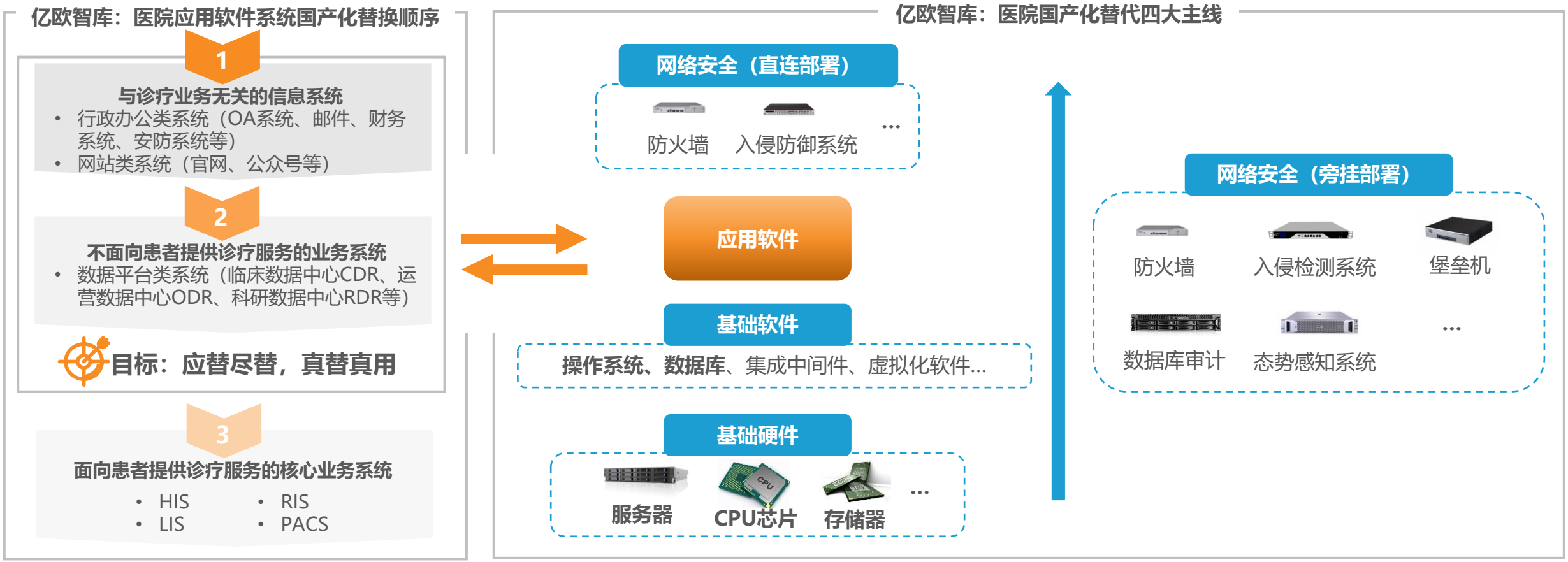
安徽省
2022年6月起，未经批准，公立医院禁止采购进口设备；对本土国产创新产品，政府采购要率先购买，不得以商业业绩为由予以限制。

北京、江苏、山东、海南、贵州、甘肃等省市政府集中采购目录及标准政策也都明确支持国产优先。

数据来源：公开资料、亿欧智库

1.4.2 医院各业务系统替换顺序为由边缘至核心，先易后难，逐步实现“应替尽替，真替真用”

◆ 医院国产化替代的顺序将**从不直接涉及医院诊疗业务的信息系统**开始，至**不提供诊疗服务的业务系统**。目前，这两类业务所对应的应用系统将和**行政办公类电脑终端设备**一起，率先完成国产化改造，**即承载该类业务的基础硬件、基础软件和网络安全产品将全部替换为符合信创要求的产品**，并达到“应替尽替，真替真用”的目标。



注：HIS等核心业务系统国产替换是指与HIS相连的医院各类设备均需要完成国产替代，因此难度极大

数据来源：专家访谈、公开资料、亿欧智库

1.4.3 医疗特殊性使医院IT设备国产替换难度高、周期长，保障信息与网络安全是重中之重

- 国产化替代政策对全国医疗卫生的影响受地域不同，目前国家已经开始进行区域试点，一些沿海城市的医院在2023年将会优先采购整套供应链均是信创名录中的产品来进行对与诊疗业务无关的信息系统的改造。
- 医院立足于民生，开展的各类业务与人的生命健康和幸福度密切挂钩。亿欧智库认为，医院完成国产化改造的最终目的是要加强对医院信息与网络安全的保障，但是结合医疗行业的特点，医院完成国产化改造之路仍很漫长，这其中，需要国产厂商加快**人才培养**，掌握关键核心技术，并完成**技术创新**和**协同合作**。

亿欧智库：使用国产设备V.S.国产化替代

使用国产设备

中国“壳子”外国“芯”

国产化替代

业务系统中使用的软硬件产品为国产，产品中的各类零部件也均为国产

医院信息与网络安全特点

1 **风险控制难度大**

医院业务系统和联网设备种类繁多，有些物联网设备甚至未在信息科管辖之下，随时都有黑客入侵风险。

2 **数据保护量大**

医院涉及大量个人隐私信息，如病历、病人信息等，且数据价值性高，数据的安全性、完整性、可用性都需要得到保障。

3 **追求方案的落地性和稳定性**

医院复杂的使用环境使进院IT设备的测试率极高，需要验证落地可行性。同时医院必须避免在治疗过程中由于网络安全问题而引发的医疗事故，同时也应避免终端设备故障而造成患者排队过长的现象等。医院始终以业务运行的稳定性作为优先保障。

4 **资金投入要求高**

医院信息化建设相比于其它行业来说相对滞后，在信息与网络安全方面的资金投入需求高，目前我国在该方面仍与发达国家有一定距离。

替换难点

产品适配难度大、要求高

医院各类系统零部件众多，需要适配芯片、操作系统与服务器、数据库，并最终与各类业务系统完成适配。**厂商需要考虑对于产业链上下游的兼容性。**

人才短缺

国产化替代意味着需要完成软件改造，设计软件基本架构，同时不断优化自身产品，让客户敢于去替换。**人才是对于国产化替代的最有力支持。**

医疗行业合适性有待验证

软硬件厂商众多，谁真正适合医疗行业还有待时间的检验。

资金来源、批准决策链复杂

医院体系复杂、种类多，包含属于医疗集团的医院、公益医院、武警医院等，国家政府对不同种类的医院的拨款仍有不足。

人才培养

技术创新

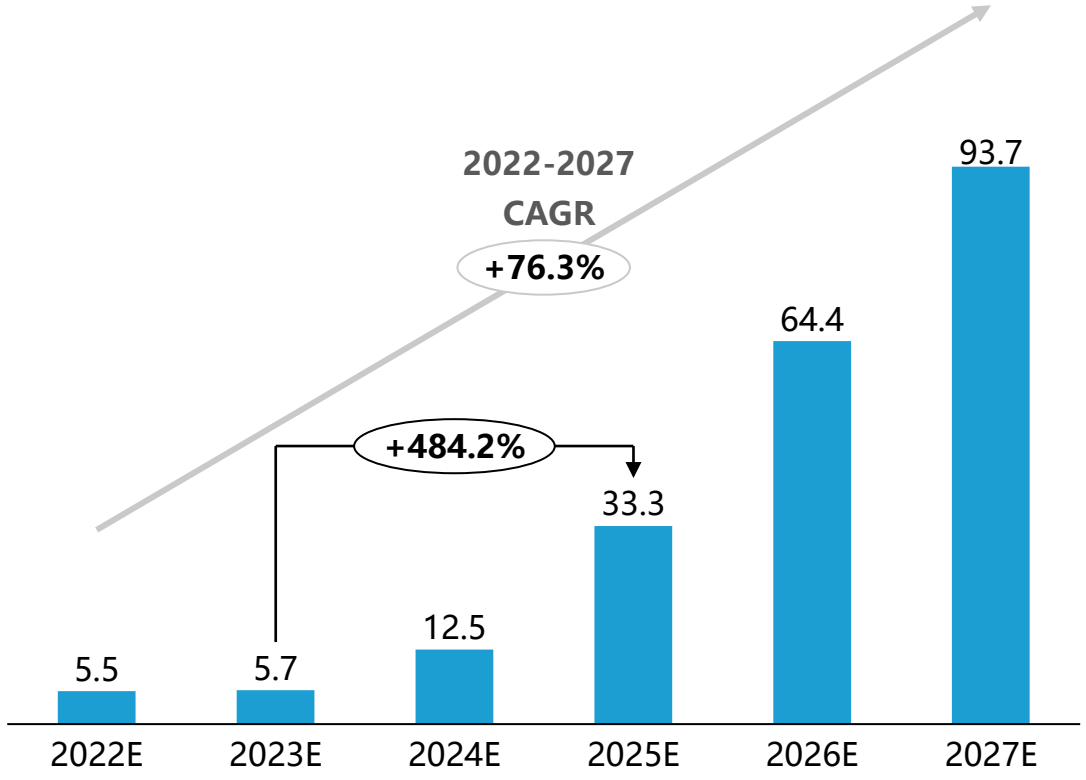
协同合作

数据来源：专家访谈、亿欧智库

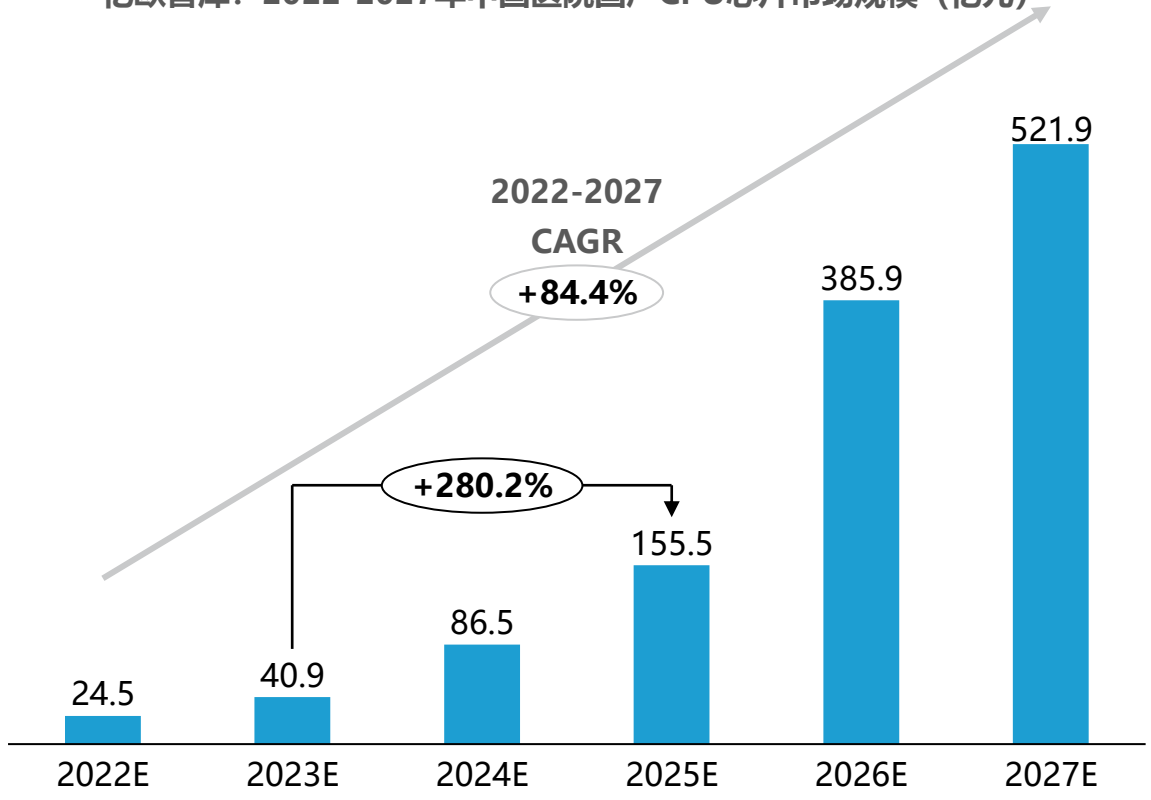
1.5 政策利好促进计算机信创行业在医院空间中的数百亿市场规模，国产厂商机会来临

- 亿欧智库认为，**国产化替代意味着国产厂商将产生数千亿规模的订单，面临千亿级的的市场空间**，正式成为中国IT行业发展的主力军。
- 在国家和地方政府的不断推动下，医院开始根据业务场景逐步对相应系统进行国产化替代，并逐渐从中小规模医院扩展至大型医院。因此，计算机信创行业将紧跟党政、金融等领域，**在医疗领域全面爆发，未来3-5年内，市场规模呈现指数级增长，其中在2025年后，进入全面爆发增长阶段。**
- 亿欧智库结合中国医院终端类和服务器类设备数量，预计2023年中国医院国产操作系统市场规模达到5.7亿元，此后受托于政策红利和技术的成熟保持高速增长，并于2027年达到近百亿规模。在中国医院国产CPU芯片方面，亿欧智库预计2023年市场规模达到40.9亿元，**而CPU芯片由于其更高的研发难度导致其前期增长率略落后于国产操作系统，2026年的增幅达到150%，并于2027年达到521.9亿元。**

亿欧智库：2022-2027年中国医院国产操作系统市场规模（亿元）



亿欧智库：2022-2027年中国医院国产CPU芯片市场规模（亿元）



数据来源：亿欧智库自主推算

亿欧智库

目录

CONTENTS

2.1 医院信息与网络安全企业图谱

医院信息与网络安全

传统网络安全集成商

Neusoft 东软 | SANGFOR 深信服科技 | 天融信 TOPSEC | 亚信安全 | 安恒信息 DAS-security | NSFOCUS | 奇安信 | H3C 数字化解决方案领导者

系统安全服务供应商

基础硬件

服务器：inspur 浪潮 | H3C 数字化解决方案领导者 | 中科曙光 Sugon | xFUSION

芯片：兆芯 | HYGON 中科海光 | 申威 | PHYTIUM 飞腾 | LOONGSON 龙芯 | Kunpeng

存储器：GigaDevice 兆易创新 | 长江存储 YANGTZE MEMORY

基础软件

操作系统：KYLINSOFT 麒麟软件 | 统信UOS | 德 中科方德 NFS-China 基础软件国家工程研究中心

数据库：达梦数据库 | KINGBASE 人大金仓

应用软件

LinkAPP 连用科技 | 金山办公 KINGSOFT OFFICE

安全服务

Neusoft 东软 | NSFOCUS | 奇安信

态势感知

Neusoft 东软 | SANGFOR 深信服科技 | 天融信 TOPSEC

云安全服务提供商

云服务厂商

腾讯云 | 阿里云 | HUAWEI 华为云 | 京东云

专注云安全服务商

安全狗 忠诚守护 值得信赖 | 青藤云安全 | 极御云安全 STOPDDOS | 德迅云安全

数据安全服务提供商

数据安全服务

LinkAPP 连用科技 | 慧盾安全 SmartSecuri | DBSEC 安华金和 | 中安星云 INTERSTELLAR SECURITY | 奇安信 | 全知科技 QUAN ZHI TECH

数据脱敏：观安 | 神州数码 Digital China | 美创 MEICHUANG

匿名化：美创 MEICHUANG | 洞见科技 INSIGHTONE

差分隐私：BaseBit.ai 翼方健数 | 锘崴科技 NUOWEI TECH

同态加密：Haitai 海泰方圆

院外应用安全涉及企业类型

互联网医院 | 制药企业 | 保险公司 | 医疗大数据公司 | 医疗器械公司 | ……

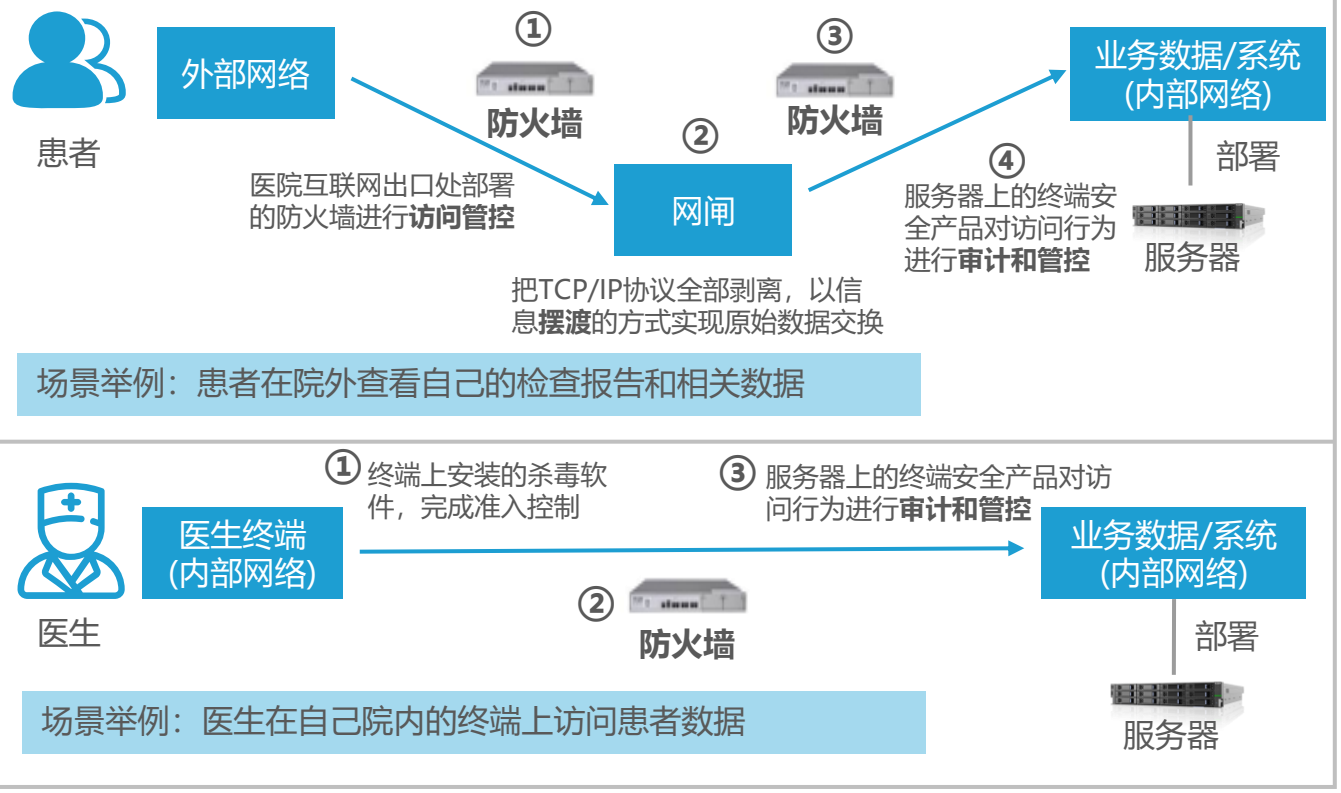
2.2.1 医院系统安全现状：保证医院系统安全需要建立多条防线，审计和管控不容忽视

- 医院常见的系统安全防线有内部网络防线、外部网络防线、应用程序防线和数据库防线等，为了建立这些防线，医院需要配备相应的软硬件设备，同时，**也需要指定相应的安全策略和流程，加强员工安全意识培训和管理**，以提高系统的**安全性、稳定性和可靠性。**
- 在访问路径上，医院常用的网络访问路径分为以患者为主要参与者的从外网到内网的访问路径以及以医院工作人员为主要参与者的从内网到内网的访问路径。

亿欧智库：医院常见网络防线及功能

防线	常见安全设备或措施	功能
外部网络防线 保护医院内部网络不受外部网络攻击和恶意软件的侵害	防火墙、入侵检测系统、网闸等	保障医院网络/应用程序/数据库的**安全、稳定和可靠**
内部网络防线 防止医院内部网络中的恶意软件和攻击行为对系统造成影响	网络隔离、访问控制、数据加密等	
应用程序防线 保护医院应用程序不受攻击和恶意软件的侵害	应用程序安全审计、漏洞扫描、代码审查等	
数据库防线 保护医院数据库不受攻击和非法访问的侵害	数据库审计、访问控制、数据加密等	

亿欧智库：医院常用网络访问路径举例



数据来源：专家访谈、公开资料、亿欧智库

2.2.2 合规驱动下，中国医院系统安全逐渐由“产品进入”过渡到“服务至上”

◆ 亿欧智库认为，目前三级以下医院在信息与网络安全的建设中仍处于“产品进入”的阶段，且存在较大的合规性需求，其中**产品需求大于服务需求**，这为**国内软硬件和安全设备厂商提供了产品开发、制造和销售的机会**，而三级医院在信息与网络安全的建设中**服务需求大于产品需求**。

合规驱动

阶段1
产品进入

阶段2 (过渡阶段)
发现问题：医院信息与网络安全未有很大提升，安全防护**仍旧存在痛点**

阶段3
服务至上

1

52.6%

2020年仅52.6%的三级医院通过等级保护三级测评

24.9%

2020年24.9%的三级以下医院通过等级保护三级测评

<50%

2022年“千县工程”名单中的医院少于50%通过等级保护三级测评

中国医疗安全建设的主旋律**围绕等保制度建设**，三级医院预算充足，集中采购防火墙、堡垒机、终端查毒软件和一些日志审计类的网络安全设备，而三级以下医院因政府资源倾斜等问题在网络安全上投入较少，近年来政府积极推动优质资源下沉，县级医院首要建设目标就是加快达到等保三级标准。

2

痛点分析

技术维度

网络安全设备齐全，却形同摆设，无法发挥真正价值。因为缺乏相关策略，资产梳理也非常困难，而医院也没有精力和能力管理诸多设备，因此迫切需要**专业人士**的帮助。

医院业务系统数量众多，同时医院开始使用APP如微信等开展相关业务，安全风险加大。医院迫切需要可以分析整体网络安全情况的系统，同时知晓资产梳理、准入控制、终端杀毒软件的使用和运营情况等。

管理维度

医院网络安全人才匮乏，也不愿意在培养该专业人才上投入过多

员工安全意识不足，不了解安全风险和防范措施。如未识别钓鱼邮件而造成财产损失。

医院缺乏安全管理制度和流程，导致安全管理混乱。

缺乏安全演练和培训，或未严肃对待，导致员工缺乏应对安全事件的能力。

3

>90%

2022年超过90%的三级医院通过等级保护三级测评

三级医院从采购网络安全设备上升到思考医院网络安全战略规划，以及对安全规划咨询、资产梳理排序等厂商提供的**一体化安全服务**和**态势感知**系统感兴趣。根据战略规划再添加购买新设备和建立院内制度。

数据来源：公开资料、专家访谈、亿欧智库

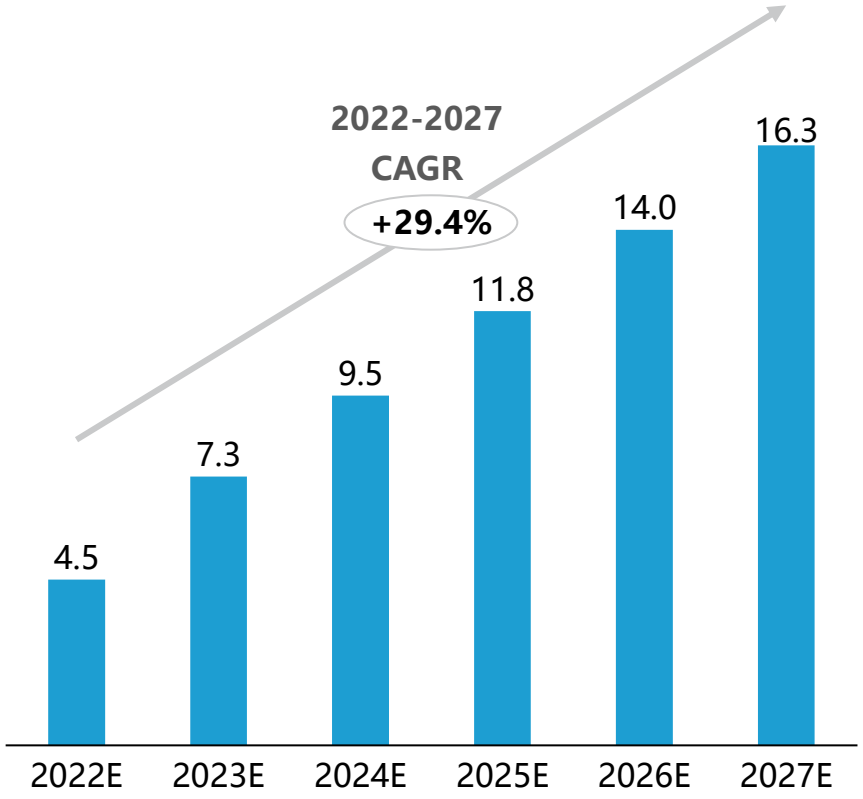
2.2.3 系统安全现状下的安全服务：态势感知和一体化安全服务的提供是国内厂商新的发力点

- 目前医院采购态势感知多数以包年的形式订购，分为基础版和含态势大屏的专业版。
- 态势感知提供全网络流量的分析，应用态势感知系统可以明确整个医院的网络安全状况，从全局视角提升对网络安全威胁的发现识别、理解分析和响应处置能力，进而进行决策与行动。医院开通态势感知服务需要若干台双网卡弹性云主机，其中一台云主机为态势感知系统（控制端），另外至少一台云主机为虚拟网关系统。态势大屏作为态势感知系统中的可视化工具，可以监控整个网络主机和关键节点的综合安全情况，提高分析深度和防御能力。亿欧智库认为，未来会有越来越多的医院选择包含态势大屏的态势感知版本。

Neusoft 东软 NetEye网络安全

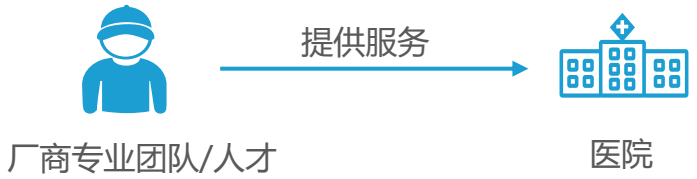
东软NetEye网络安全态势感知平台，面向医疗行业业务安全视角，实现新一代网络安全体系化防护方案，满足用户等保合规、安全运营、应急响应、护网、重保等场景安全需求。平台采用资产测绘、NDR、EDR、UEBA、AI安全分析、集中安全策略管理、SOAR等新型安全技术打造资产测绘管理中心、智能威胁管理中心、安全集中监管中心、安全能力中心、合规、HW支持中心五大安全中心，从宏观、微观各个视角评估网络的安全态势，实现历史态势回溯、实时态势评估、未来态势预测，全面提升企业的安全监控能力、分析能力、应急响应能力、自动化运维能力。

亿欧智库：中国医院态势感知市场规模（亿元）



注：该态势感知市场规模是指包含态势大屏的态势感知服务市场规模

亿欧智库：厂商一体化服务



目标：在厂商专业人士和专业团队的提供的服务下，有效解决医院信息与网络安全的痛点，加快实现医院网络安全顶层设计与规划，提升医院网络的安全性。

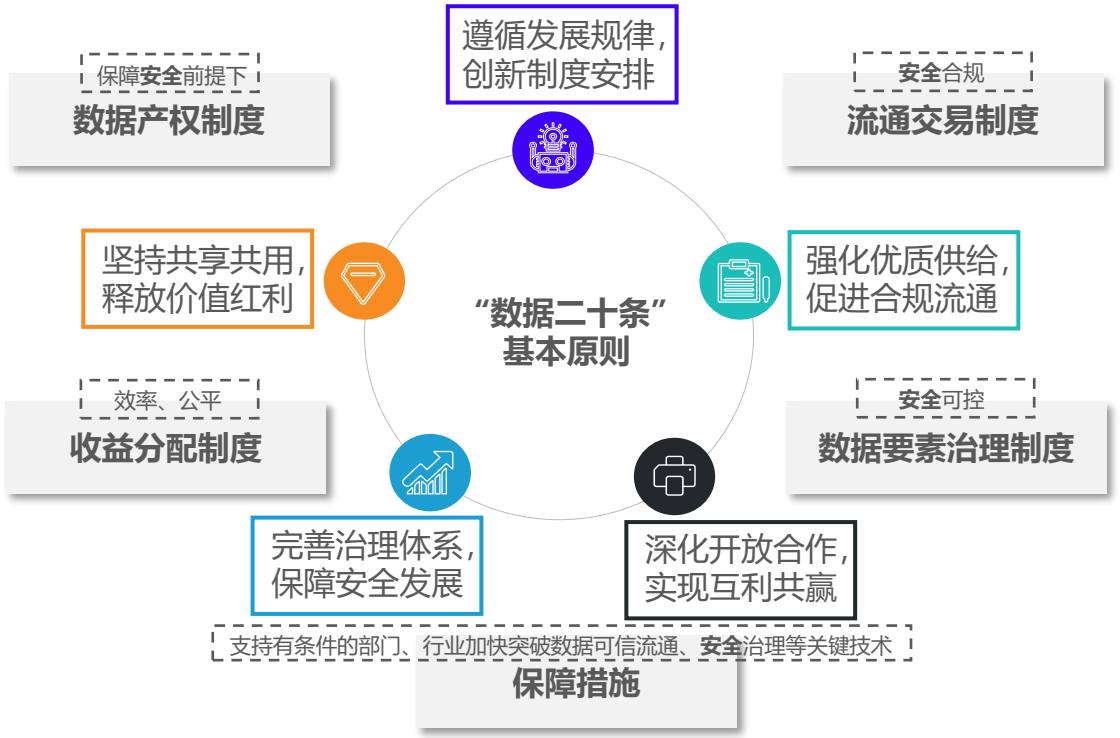
- 安全意识培训
- 产品使用培训
- 定期产品运维、检查
- 远程支持、辅助
- 网络安全咨询服务
- 医院安全战略规划
- ...

数据来源：东软内部资料、专家访谈、亿欧智库自主推算

2.3.1 系统安全的目的是全力保障数据安全，数据是医院最核心的资产之一

- 2022年12月，《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）对外发布。“数据二十条”以维护国家数据安全，保护个人信息和商业机密为前提，达到充分实现数据要素价值、促进全体人民共享数字经济发展红利的目的。由此看出，在政策和监管的需求下，数据安全安全始终作为国家发展数字经济的首要前提。未来，中国的数据安全政策也将在实践的过程中进一步明确。
- 系统安全是保障数据安全的关键步骤，数据是医院的最核心资产，也是各类系统的保护对象，医院中涉及众多数据类别，电子病历、健康档案、医学影像的产生过程中，也都会涉及大量的患者个人隐私数据，而正是因为医疗行为的特殊性，医院内部系统的安全性和可靠性必须是高级别，目的在于确保数据的安全以及确保数据不丢失，以此来发挥医疗数据的价值。

亿欧智库：“数据二十条”制度总结



“数据二十条”为基础建设确实是点亮了一盏灯，我们的前进道路确实有思想，知道怎么去做了，当然还有一些工作要完善细化。 ——王才有，中国医院协会信息专业委员会主任委员

亿欧智库：医疗数据类别汇总

数据类别	范围
个人属性数据	1）人口统计信息，包括姓名、出生日期、家庭成员信息等 2）个人身份信息，包括身份证、工作证、居住证、检查单号等 3）个人通讯信息，包括电话号码、邮箱账号等 4）个人生物识别信息，包括基因、指纹、面部特征等 5）个人健康监测传感设备ID等
健康状况数据	主诉、病史、家族史、症状、检验检查数据、基因测序、代谢小分子检测、人体微生物检测数据等
医疗应用数据	住院医嘱、用药信息、病程记录、手术记录、护理记录、入院记录、出院小结、转诊转院记录等
医疗支付数据	1）医疗交易信息，包括医保支付信息、交易金额、交易记录等 2）保险信息，包括保险状态、保险金额等
卫生资源数据	医院基本数据、医院运营数据等
公共卫生数据	环境卫生、传染病疫情、疾病监测预防数据等

产生数据

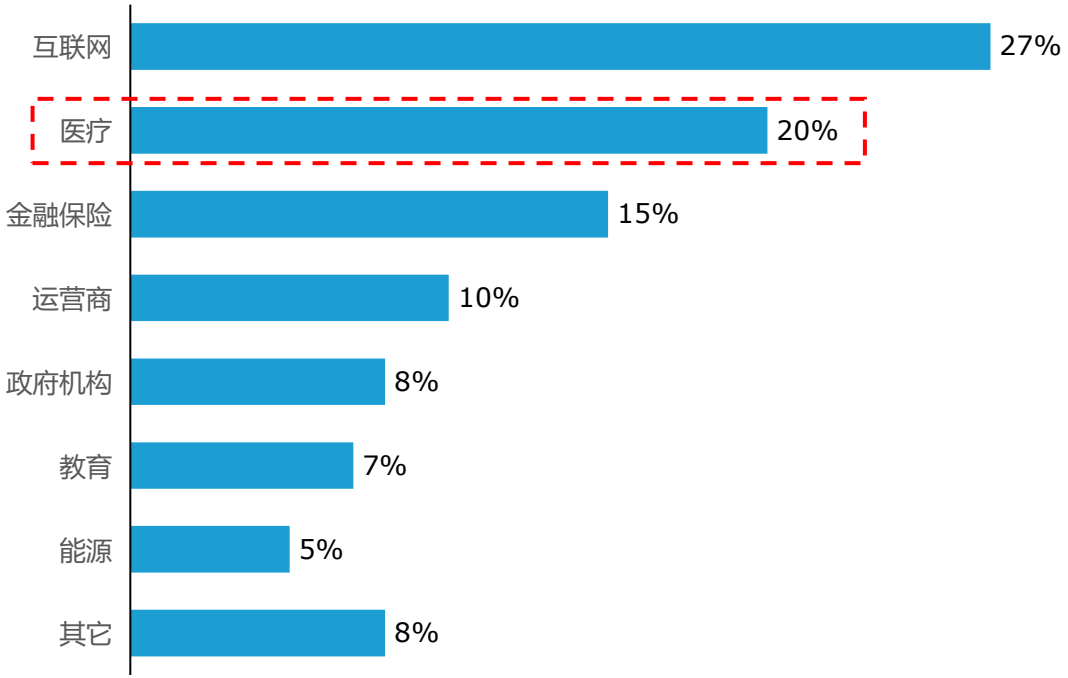
智慧医疗	智慧服务	智慧管理
电子病历、CDSS……	转诊服务、诊疗预约……	科室管理、后勤管理……

数据来源：《信息安全技术健康医疗数据安全指南》、公开资料、亿欧智库

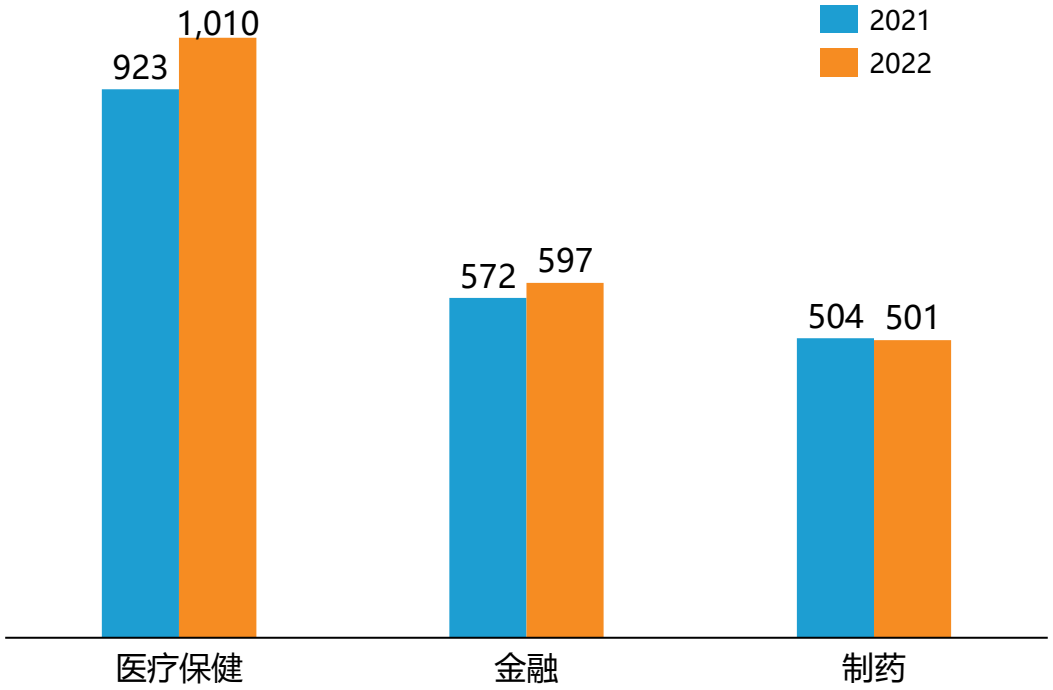
2.3.2 医院数据安全现状：医疗数据的高价值使其饱受攻击，高额的数据泄露成本不容小觑

- 医院数据的高利用价值使其一直受到黑客们的青睐。随着医院的业务范围逐年扩大，医院内患者的大量个人隐私数据一旦遭到泄露和被破坏，对医院品牌、日常运行和患者自身都会造成极大的负面影响。目前，医院内的数据保护仍然不是很乐观。
- 据IBM统计数据显示，医疗机构连续12年保持数据泄露成本最高，数据泄露成本是指安全事件发生到结束，组织业务系统完全恢复，前、中、后各个时期产生的所有支出。2022年医疗机构该数据高达1010万美元，与2020年相比激增42%，同时比排名第二的金融领域高出69%。医疗数据的高泄露成本主要是由于该行业收到政府部门的严格监管，法律层面的支出是其泄露成本的主要来源。

亿欧智库：2021年中国个人信息泄露行业占比



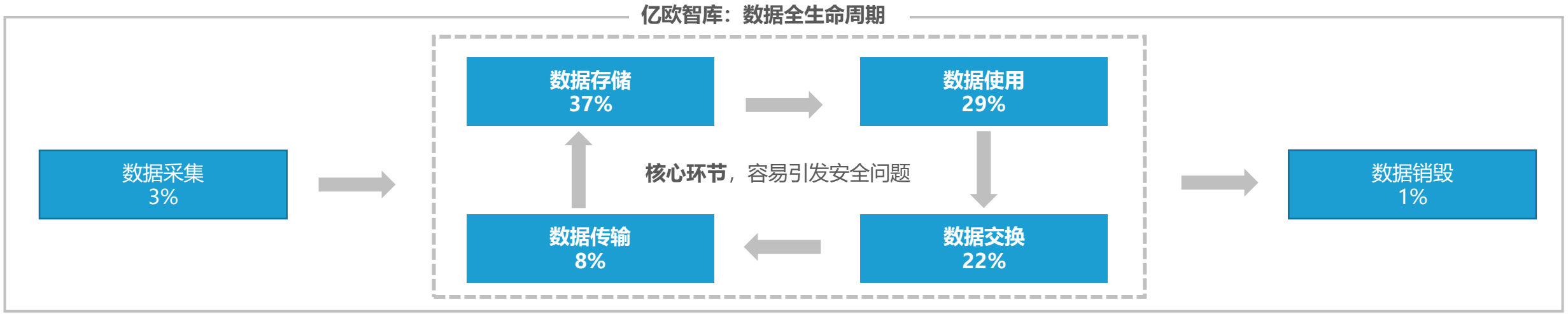
亿欧智库：2021-2022年全球平均数据泄露成本行业Top3（万美元）

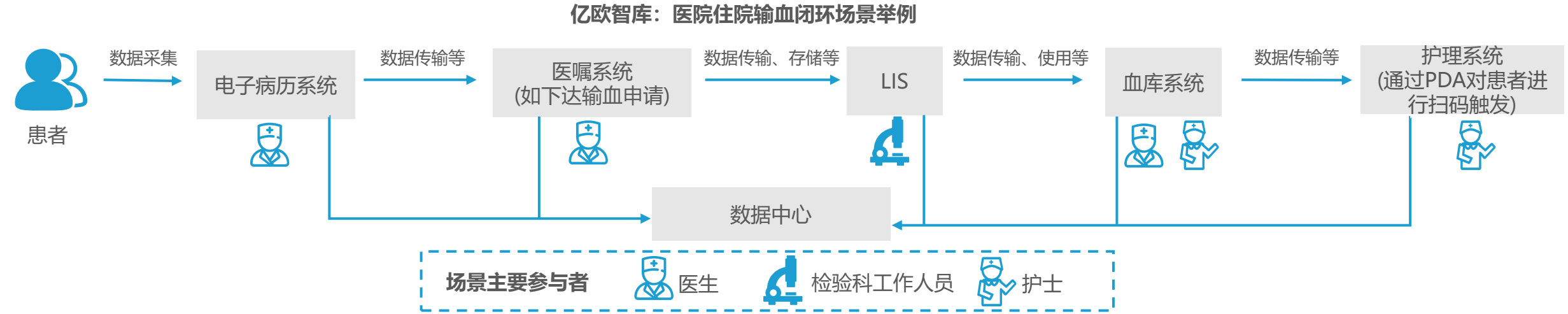


数据来源：IBM、Secsmart、亿欧智库

2.3.3 存储、使用、传输、交换是医疗数据泄露发生的主要环节

- 数据显示，2021年约有37%的数据泄露事件发生在数据存储阶段，其次为数据使用、交换、传输阶段。
- 从医院角度看，医院数据闭环管理是医院数据治理中的重要环节，**而存储、使用、传输和交换是数据形成闭环的关键步骤**，目前由于医院各部门对闭环建设的共识不足，以及同一家医院的HIS、EMR、PACS、LIS等系统由不同厂商生产开发，在数据存储方式、应用场景等方面存在差异，为数据闭环管理形成难题，因此数据在存储、使用、传输和交换环节存在相对较高的数据泄露可能性。





数据来源：Secsmart、专家访谈、亿欧智库

2.3.4 依托于健康医疗大数据区域中心，医疗数据共享和利用得到广泛关注

- 中国凭借人工智能、数据挖掘等新兴技术应用的日益成熟，健康医疗领域的数据积累被逐渐推动。一系列政策的颁发表明始终政府在为医疗数据交易做准备，想要通过流通共享来充分发挥医疗数据的价值性。
- 从2016年开始中国陆续出台医疗大数据应用相关政策和规划中国健康医疗大数据与区中心的建设。位于山东济南的国家北方健康医疗大数据中心是第一个落成并投入使用的医疗健康大数据区域中心，福建福州紧随其后。

亿欧智库：医疗大数据共享和利用政策

2016年10月　国务院《“健康中国2030”规划纲要》

加强健康医疗大数据应用体系建设。消除数据壁垒，建立跨部门跨领域密切配合、统一归口的健康医疗数据共享机制，实现公共卫生、计划生育、医疗服务、医疗保障、药品供应、综合管理等应用信息系统数据采集、集成共享和业务协同。

2018年7月　卫健委《国家健康医疗大数据标准、安全和服务管理办法》

加强健康医疗大数据的共享和交换，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系。责任单位应当依法依规使用健康医疗大数据有关信息，提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全。

2020年7-8月　四川省《健康医疗大数据应用管理办法（试行）》
山东省《健康医疗大数据管理办法》

推进医疗机构与公共卫生机构信息共享；开展服务过程中需对数据进行转移交接的，由交接双方签字确认，加密传输，确保数据在交接过程中的完整、安全。

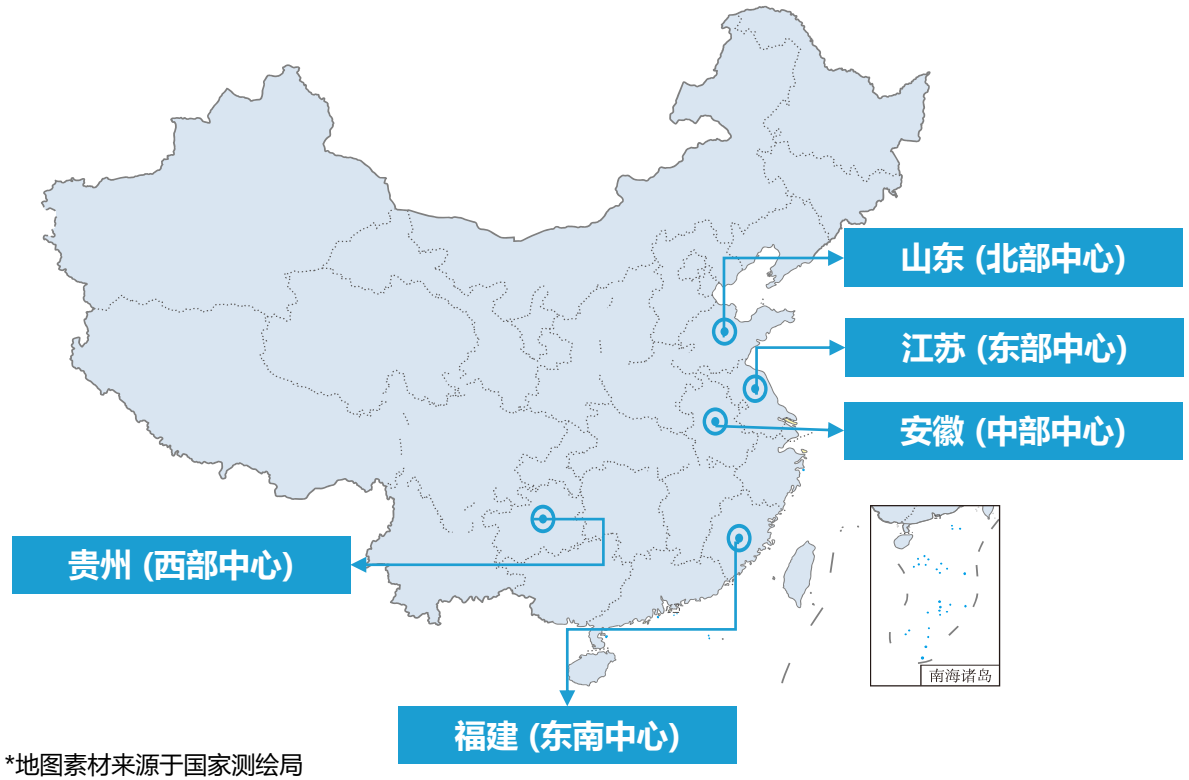
2022年3月　国务院《“十四五”国民健康规划》

推进各级各类医疗卫生机构统一接入和数据共享。探索建立卫生健康、医疗保障、药监等部门信息共享机制，通过全国一体化政务服务平台，实现跨地区、跨部门数据共享。

2023年3月　全国两会：加强健康医疗大数据共享和利用

应制定和完善相关的法律法规、规章制度，保障数据的共享和分析利用。政府可指定专门的机构或部门，制定工作机制和流程，负责数据共享申请的审批、督促、推进等工作，保障相关工作的顺利进行。

亿欧智库：中国五大健康医疗大数据区域中心



*地图素材来源于国家测绘局
审图号：GS(2008)1503号

数据来源：专家访谈、公开资料、亿欧智库

2.3.5 数据应用成必然，但医院开放数据存在明显阻力，技术储备需进一步完善

- 虽然医疗数据共享和利用得到广泛关注，但医院“数据孤岛”现象普遍以及诸多合规问题尚未解决，医院对开放数据的接受度非常低，达到最终目标仍有很长的一段路要走，其中，政府、厂商（技术）和医院都面临着诸多挑战。
- 亿欧智库认为，医院开放数据的阻力可以分为从政府端、技术端和医院端三个方面考虑。其中，政府所具有能力是最大的，另外，国家宏观要求为数据安全方案提供商提供了**生产研发的机会和广阔的市场空间，如何通过自身技术和措施保证数据是安全交易的，且不会被法律诉讼是厂商开展技术研发的核心目的。**
- 医院端来看，医院数据开放可能承担的风险成本远远高于医院在数据开放上投入的金额，因此考虑到风险和自身利益问题让医院自身不愿意开放数据。

亿欧智库：医院数据开放阻力

政府端

虽然《信息安全技术健康医疗数据安全指南》中将医疗数据可接受开放程度由高到低分为1-5级，**但并未结合数据分类出台统一数据分类标准**，同时若数据开放后出现数据泄露、数据篡改等安全事件，**责任主体**和**管理要求**并未被政府部门明确。

技术端

目前技术储备仍不完善不强大，还未做好可交易的准备。数据在传输存储等阶段中需要通过技术手段使人们无法通过数据拼凑出一个物理人，其中四大关键技术为**数据脱敏、匿名化、差分隐私和同态加密。**

医院端

相关利益让医院自身不愿意开放数据，政策和技术的不完善让医院也不敢轻易尝试共享数据。另一方面，不同医院根据行业标准对院内数据进行分级分类的标准也不统一，**存在同一类别的数据被不同医院划分为不同级别。**

亿欧智库：医院“数据孤岛”

指数据间缺伐关联性，数据库彼此无法兼容，缺乏数据间的互联互通。医院内系统出现的“数据孤岛”现象对其管理和服务的高效开展产生极大的负面影响。

打破“数据孤岛”可能性的前提

明确数据分类标准、责任主体，给予资金投入（最重要）

技术成熟

医院根据国家分类标准完成数据分级分类，统一各类数据重要程度、风险级别等

数据应用

医院数据共享合作对象

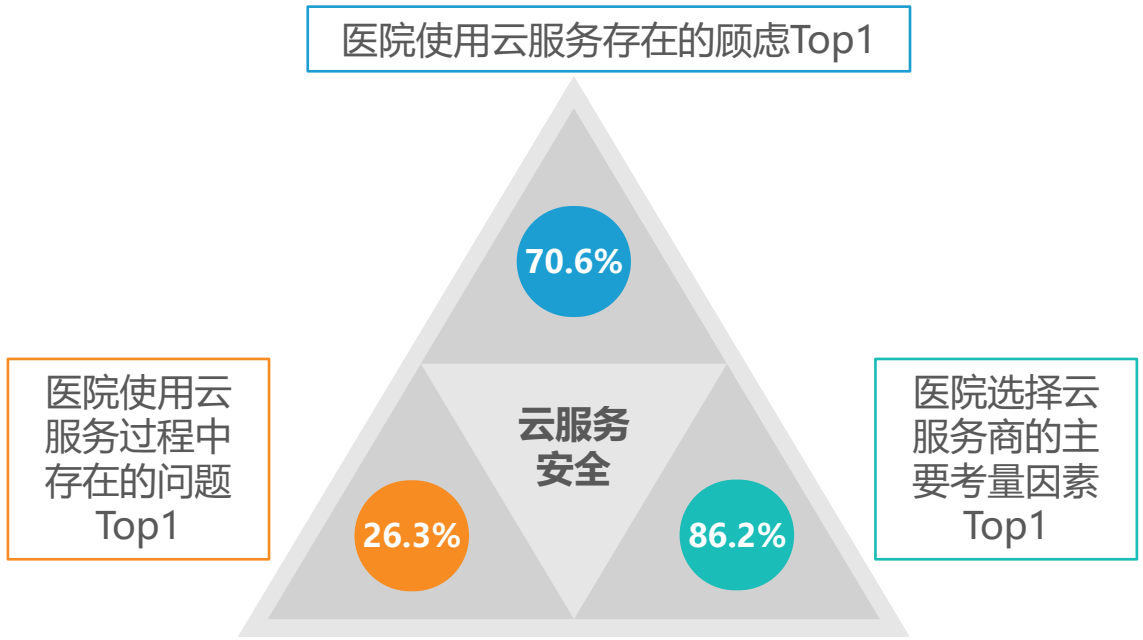
药企 | 保险公司 | 医疗器械公司 | 医疗大数据公司 | …

数据来源：《医院“信息孤岛”现象存在的问题与对策探讨》、专家访谈、公开资料、亿欧智库

2.4 “互联网+”促使医院上云意愿增强，但上云之路的进程将受到多方面因素影响

- 亿欧智库认为，虽然医院上云需求和意愿加强，但是随着国产化改造向越来越多的行业渗透，以及医院信息化建设的预算相对固定，目前医院的预算重心在对承载各类业务的基础硬件、基础软件和网络安全产品的国产化替代上，因此上云的落地性进程减缓，在云安全上的投入也有限，预计三年内医院云安全市场规模增速每年不超过30%，而在这之后增速加快，有望达到50%以上。
- 在公有云和私有云模式的选择上，互联网医院由于其需要具备医院资源随时补充进入等特点，因此依托公有云提供商来开展业务，而实体医院则由于内对内的访问较多，对弹性扩容的需求低，同时对云端环境和云上数据的安全性要求高，因此实体医院通过互联网来延伸业务通常会选择私有云。无论哪种模式被选择，云服务安全是众多医院的首要考虑因素，因此，云服务提供商需要保证一定的云安全。

亿欧智库：2021年中国医院中重点考虑云服务安全的比例



亿欧智库：互联网医院和实体医院上云模式倾向

01 互联网医院

汇集医院资源在公有云上开展医院业务，云服务提供商需要满足国家安全标准，并承担之后可能发生的安全责任，医院只需在网络边界上完成防护即可：

公有云 → 云安全问题责任承担主体 → 云服务提供商

02 实体医院

实体医院通过互联网来延申业务，往往有以下两种选择

- 自建上云服务器（难度大，性价比低）

医院自行配置需配置硬件设备、基础环境、网络、应用维护人员等，自行考虑平台冗余性、安全可靠性等问题，若受到**DOS攻击**，则医院面向互联网的业务无法开展。

- 采购私有云（在专业性、安全性、便利性与经济性上更胜一筹）

访问者 → **私有云**（提供网络安全防护，抵御DOS攻击等网络攻击） → **医院互联网入口** → 实体医院

数据来源：CHIMA、专家访谈、亿欧智库

2.5.1 深信服科技：释放数字健康价值、守护智慧医疗安全

- 深信服科技股份有限公司（下称“深信服”）创立于2000年，旗下有两大业务品牌——深信服智安全和信服云，与子公司信锐技术一起，在安全、云计算、IT基础设施与物联网领域中不断积淀、打磨、再创新，为用户数字化转型工作构筑稳固基石。
- 在医疗行业，深信服始终致力于洞察行业用户的业务需求，给用户提供简单易用的场景化解决方案。目前，深信服已服务于超过 13000 家医疗卫生机构，帮助超过3000家医院通过等级保护备案及评测，全情为用户业务保驾护航，全力推动智慧医疗体系高质量发展。

亿欧智库：深信服医疗行业部分安全业务介绍

深信服案例展示：某医院安全运营中心建设

用户需求

虽然医院已经顺利通过了三级等保测评，但在网络安全工作中仍面对**安全防护不全面、设备堆叠导致运维复杂、静态防御无法应对动态威胁、对绕过防御的残余攻击无法及时感知**等各种各样的困扰

建设目标

- 快速构建对医院内网安全持续检测的能力，做到风险和安全事件的全程管理，提升安全运维的效率和精度
- 有效地防御新型的病毒，一旦变种的病毒入侵，可以做到及时发现、定位和预警，并且联动安全设备进行处置

解决方案

深信服针对医院网络安全的建设诉求，在保证安全建设的等保合规基础上，**综合考虑到风险的预警、防护、处置等，提出了一套以“安全可视、动态感知、协同防御”为亮点的主动防御体系方案，结合“人机共治”理念**，形成医院安全建设的闭环管理

方案价值

- 整体安全能力的全面覆盖：利用**安全态势感知系统**
- 安全检测、预警、处置之间的协同响应：**安全感知平台可联动相关的安全设备**(比如防火墙、终端安全 EDR、MSS运营服务等)，在事件造成严重影响之前及时进行解决

数据来源：深信服科技、亿欧智库

2.5.2 东软：为医院信息化全生命周期安全赋能，让智慧医疗安全无忧

Neusoft东软 亿欧智库

- 东软集团（SH.600718）是行业领先的全球化信息技术、产品和解决方案公司，是产业创新变革的推动者和数字化转型的赋能者。东软成立于1991年，是中国第一家上市的软件公司。东软NetEye (网络安全) 于1996年成立，秉承多年的专业技术经验积累，持续为用户提供成熟、先进的网络安全产品，高效、完善的安全解决方案与服务，致力于成为全球领先的网络安全产品及服务供应商。
- 医院业务复杂，发展迅速，面临众多的安全风险。东软NetEye在提供一系列创新网络安全产品的同时，凭借优秀、诚信的服务能力和高效、可靠的质量控制管理方法为医院提供安全咨询、应急响应、渗透测试、安全加固、风险评估、安全运维、等级保护等全方位的安全服务，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，为医院提供基础全面的网络安全防护体系，助力医院业务稳定运行。

亿欧智库：东软以“咨询规划+安全服务” 模式助力江苏省某三甲医院开展网络安全工作

项目背景

江苏省某三甲医院基于其智慧医院建设的快速推进，业务连续性的重要性越发突出以及医院现有网络环境的变化等原因，医院早期部署的较为全面网络安全产品已无法满足医院的网络安全需求，综合分析医院还面临来如下三方面的需求：

- **安全产品存在堆叠现象，缺少全局视角下安全能力的认识**
- **用于支撑业务运行的IT资产风险不断增多**
- **医院人员网络安全意识淡薄，安全管理制度和协同处置机制不够完善**

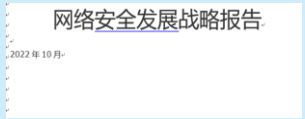
服务内容及输出成果

咨询规划服务　攻防演练服务　渗透测试服务

安全加固服务　应急响应服务　……

成果展示

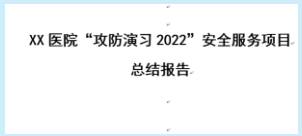
编制网络安全发展战略报告



制定十个闭环的管理制度

完成风险和能力的评估

完成攻防演练值守工作



客户价值体现

①**做信息中心的安全副总工**，通过五位一体的布局，形成务实的网络安全能力、高效的网络安全运营模式

②**明确**了清晰的安全发展战略　③**形成**了闭环的安全管理流程

④**规避**了重大的网络安全风险　⑤**强化**了全局的网络安全能力

⑥**建立**了高效的协同处置机制　⑦**确保**了业务的安全稳定运行

数据来源：东软集团、亿欧智库

亿欧智库

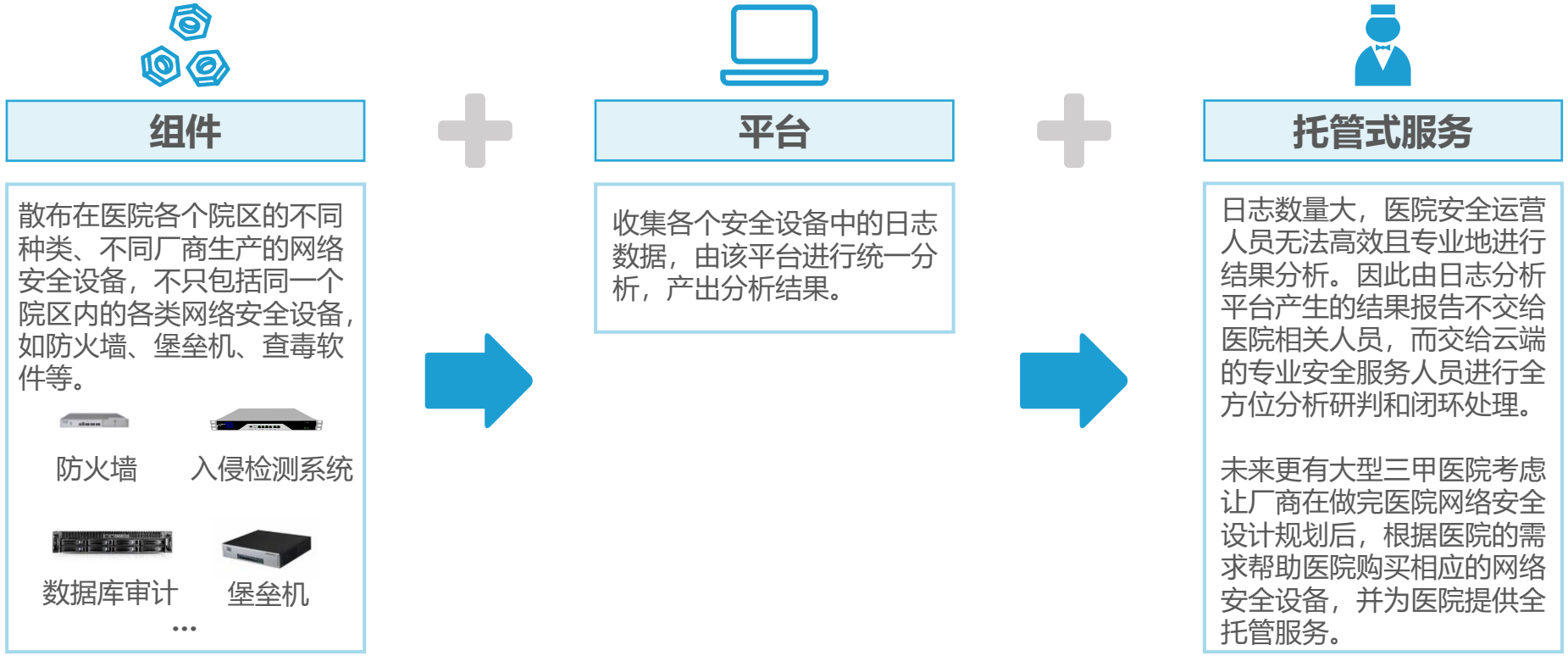
目录

CONTENTS

3.1 趋势一：“组件+平台+服务“三者联动模式成为医院网络安全技术突破口

- 医院工作人员由于时间和精力有限，加上医院IT专业人才配备少，网络安全设备买而不用的问题始终困扰着医院管理人员。在国产化替代的背景下，医院将迎来全新网络安全设备，**未来“组件+平台+服务”的模式将极大程度上帮助医院省时省力、高效利用各类设备，破解医院网络安全的技术缺失**。

亿欧智库：未来医院信息与网络安全防护模式

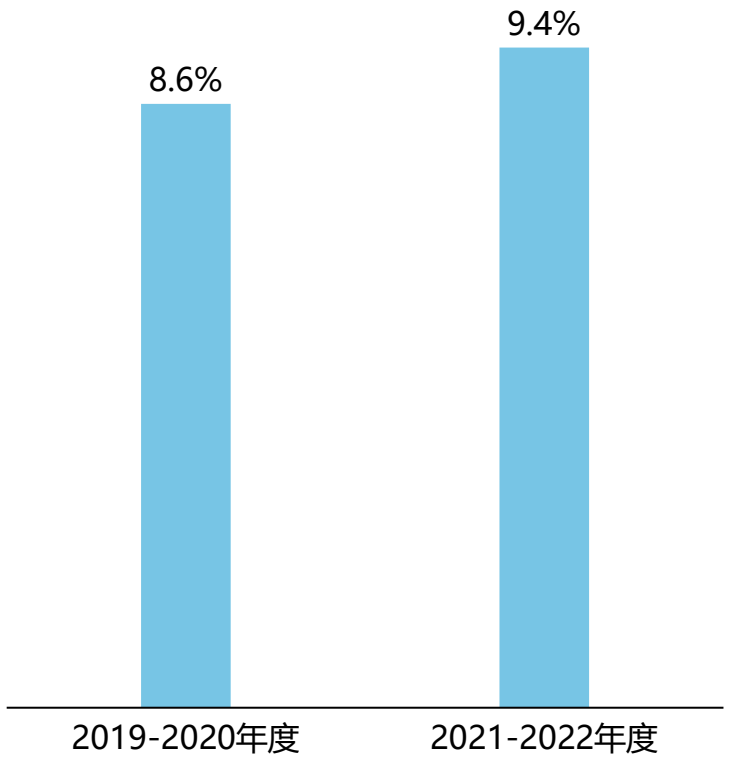


数据开源：专家访谈、亿欧智库

3.2 趋势二：中国医院信息安全类投入有望从9%逐渐上升到15%，促进行业高质量发展

- 据CHIMA最新数据显示，自2019年起，中国医院信息化建设中安全类投入占比稳定在9%上下，该平均值符合《医疗卫生机构网络安全管理办法》中对于新建信息化项目的网络安全预算不低于项目总预算的5%的标准。信息安全类投入包括对安全防护设备 (软件和硬件)和对安全服务的投入。
- 中国无论在医疗行业网络安全法规的细致度和出台时间上均落后于国外发达国家，因此导致中国医院对于网络安全的重视程度不及发达国家。据公开资料显示，美国2021财年IT总预算为922亿美元，网络安全预算占IT预算的比例为20.4%。
- 亿欧智库认为，未来伴随着外部政策因素和医院内部因素的驱动，医院信息与网络安全的投入占比将逐渐上升，促进行业高质量发展。

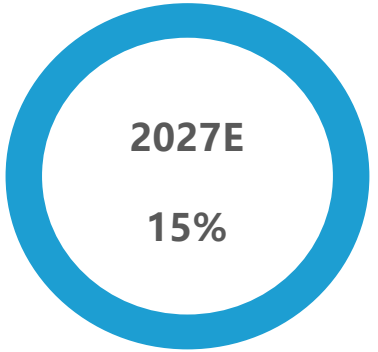
亿欧智库：2019-2022中国医院信息化建设中安全类投入所占比例



① 外部因素，未来中国医疗行业的网络安全管理办法将会更加具体和细化，也必然会对医院网络安全的投入占比提出更高的要求

②医院内部因素，医院信息与网络安全的隐患始终存在，随着医院线上业务的开展和数据量的积累，网络安全风险加大，医院自身也会从技术和管理角度加大对网络安全的重视程度

亿欧智库：2027年中国医院信息化建设中安全类投入所占比例

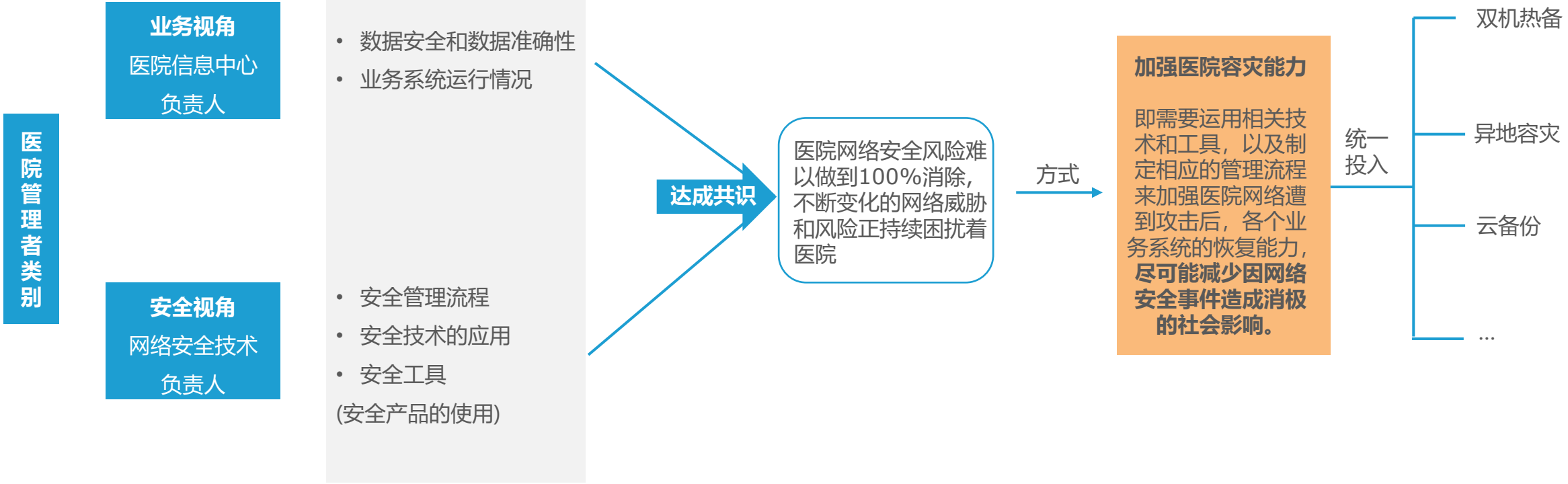


数据开源：CHIMA、专家访谈、亿欧智库

3.3 趋势三：容灾能力建设成为医院信息与网络安全领域的关注重点，医院容灾能力逐步加强

- 医院网络安全风险难以100%消除，因此医院管理者除了需要关注网络被攻击的风险从而不断地投入产品、人力和服务外，也在不断重视遭遇网络攻击后，医院业务系统的恢复能力和受影响的程度如何，即医院业务连续性，又称容灾能力。

亿欧智库：医院加强容灾能力的原因分析

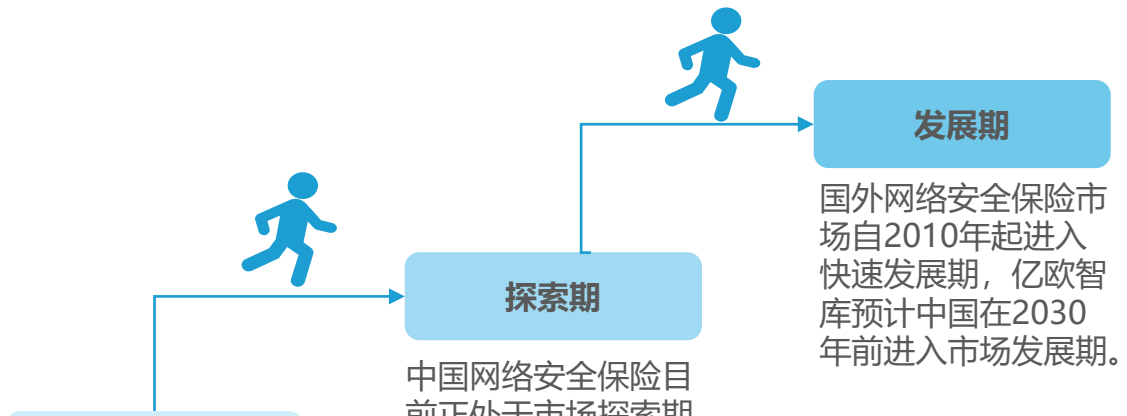


数据来源：专家访谈、亿欧智库

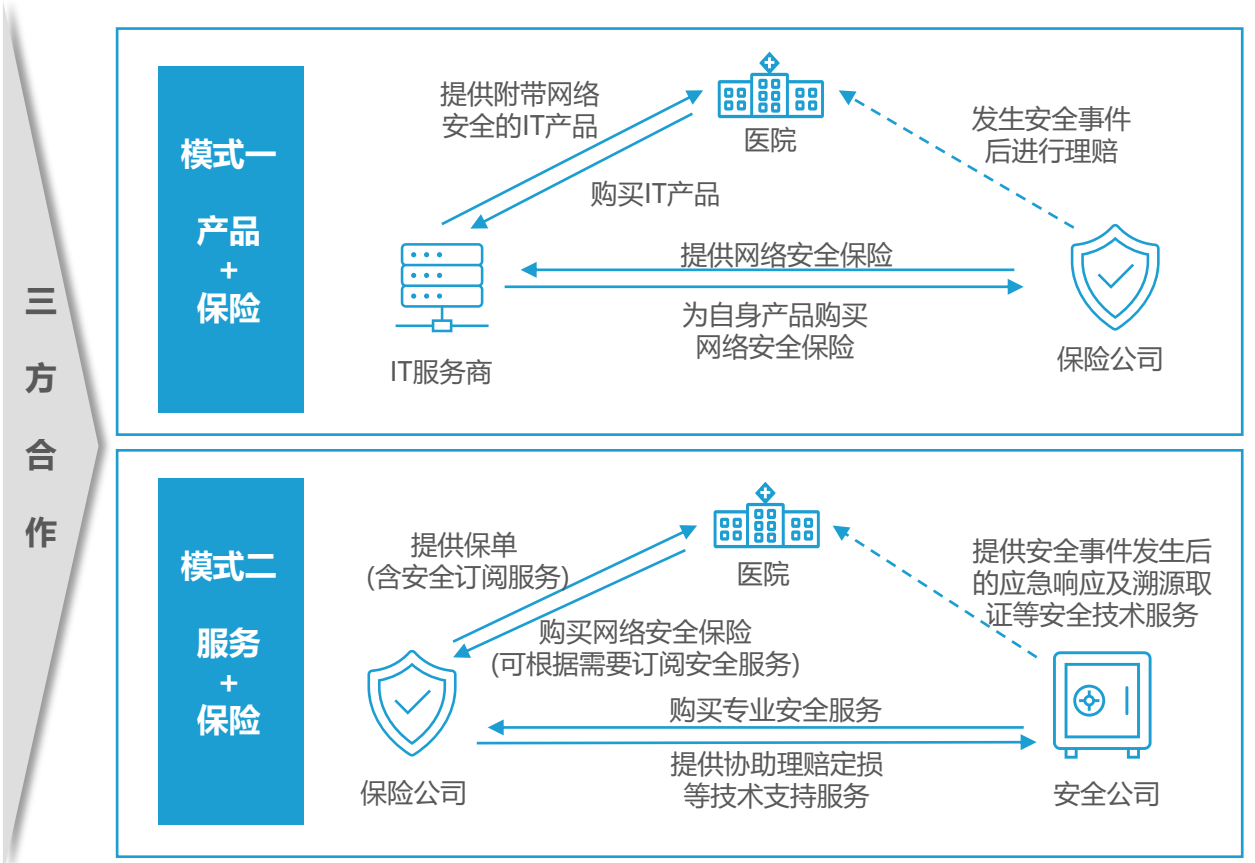
3.4 趋势四：商业生态逐渐丰富，网络安全保险逐步融入医院网络安全防护体系中

- 网络安全保险是承保与网络空间风险等相关风险的新险种，也是目前是全球财产保险市场中发展速度最快的细分领域之一，据慕再数据显示，到2025年全球网络安全保险市场的规模达到约200亿美元。
- 从医院管理角度来看，医院数据的高泄露风险和高泄露成本使医院对网络安全保险的需求不断加，该保险可以使医院和网络安全产品设备服务提供商免受巨大的经济损失，未来，保险公司将加快布局网络安全保险产品线，各大国内厂商将为自身网络安全产品购买保险后再提供至医院。亿欧智库预计，网络安全保险正在加速走进医院网络安全防护体系中，未来将有更多的医院选择带有网络安全保险的IT产品或服务。

亿欧智库：中国网络安全保险发展阶段



亿欧智库：医院网络安全保险主要参与者及业务模式



数据开源：专家访谈、公开资料、亿欧智库

医院信息与网络安全大咖说

张泉
东软集团
网络安全事业部
副总经理

从组织网络安全管理者的角度看，至少需要应对两方面问题，**第一个是合规性**，也就是组织在应对网络安全管理的内外合规性时，如何既能满足政府的监管要求，又能切实有效的提升组织的管理能力？**第二个是风险威胁**，也就是网络安全风险威胁对组织信息基础设施的攻击，以及伴随而来的业务信息系统瘫痪。

随着安全服务与产品的深度融合，组织的信息安全投资预算重心将从产品购买转向服务购买，**走向安全即服务的模式**，最大限度的发挥安全预算投入对组织业务系统的支撑和保障作用。

高昂
亿欧董事总经理
亿欧大健康总裁

医院信息与网络安全的未来发展趋势将是**综合性的**，包括技术、意识、管理、人力资源、应用等多个方面的提升，以应对不断增加的网络安全需求。

在未来，医院将更加积极、主动、自发地与自主可控的信息与网络安全供应商作伙伴**建立安全合作机制**，共同维护医院信息和网络的安全。同时监管部门也会对医院信息和网络安全提出更系统更全面的要求，这对医院内部管理来说将会是新的挑战。

致谢

- 亿欧智库经过桌面研究及对医院及相关企业、专家访谈后作出此份报告。报告重点对国产化替代背景下中国医院信息与网络安全的最新发展现状和未来发展进行研究分析，在此，亿欧智库感谢相关企业及业内专家的鼎力支持。
- 未来，亿欧智库将持续密切关注中国医院信息与网络安全领域，通过对于该领域的深度观察，持续输出更多有价值的研究成果，助力产业可持续创新发展。欢迎报道读者与我们交流联系，提出报告建议。
- 特别鸣谢

关于亿欧

◆ 团队介绍：

亿欧智库（EO Intelligence）是亿欧旗下的研究与咨询机构。为全球企业和政府决策者提供行业研究、投资分析和创新咨询服务。亿欧智库对前沿领域保持着敏锐的洞察，具有独创的方法论和模型，服务能力和质量获得客户的广泛认可。

亿欧智库长期深耕新科技、消费、大健康、汽车出行、产业/工业、金融、碳中和等领域，旗下近100名分析师均毕业于名校，绝大多数具有丰富的从业经验；亿欧智库是中国极少数能同时生产中英文深度分析和专业报告的机构，分析师的研究成果和洞察经常被全球顶级媒体采访和引用。

以专业为本，借助亿欧网和亿欧国际网站的传播优势，亿欧智库的研究成果在影响力上往往数倍于同行。同时，亿欧内部拥有一个由数万名科技和产业高端专家构成的资源库，使亿欧智库的研究和咨询有强大支撑，更具洞察性和落地性。

◆报告作者：

王若琛

亿欧智库 分析师

Email：wangruochen@iyiou.com

王思晗

亿欧大健康研究副总监

Email：wangsihan@iyiou.com

◆报告审核：

高昂

亿欧董事总经理，亿欧大健康总裁

Email：gaoang@iyiou.com

王辉

亿欧智库副院长

Email：wanghui@iyiou.com

关于亿欧

◆ 版权声明：

本报告所采用的数据均来自合规渠道，分析逻辑基于智库的专业理解，清晰准确地反映了作者的研究观点。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。本报告的信息来源于已公开的资料，亿欧智库对该等信息的准确性、完整性或可靠性作尽可能的追求但不作任何保证。本报告所载的资料、意见及推测仅反映亿欧智库于发布本报告当日之前的判断，在不同时期，亿欧智库可发出与本报告所载资料、意见及推测不一致的报告。亿欧智库不保证本报告所含信息保持在最新状态。同时，亿欧智库对本报告所含信息可在不发出通知的情形下做出修改，读者可自行关注相应的更新或修改。

◆ 关于我们：

亿欧是一家专注科技+产业+投资的信息平台和智库；成立于2014年2月，总部位于北京，在上海、深圳、南京、纽约设有分公司。亿欧立足中国、影响全球，用户/客户覆盖超过50个国家或地区。

亿欧旗下的产品和服务包括：信息平台亿欧网（iyiou.com）、亿欧国际站（EqualOcean.com）、研究和咨询服务亿欧智库（EO Intelligence），产业和投融资数据产品亿欧数据（EO Data）；行业垂直子公司亿欧大健康（EO Healthcare）和亿欧汽车（EO Auto）等。

亿欧服务

- 基于自身的研究和咨询能力，同时借助亿欧网和亿欧国际网站的传播优势；亿欧为创业公司、大型企业、政府机构、机构投资者等客户类型提供有针对性的服务。

- 创业公司

  亿欧旗下的亿欧网和亿欧国际站是创业创新领域的知名信息平台，是各类VC机构、产业基金、创业者和政府产业部门重点关注的平台。创业公司被亿欧网和亿欧国际站报道后，能获得巨大的品牌曝光，有利于降低融资过程中的解释成本；同时，对于吸引上下游合作伙伴及招募人才有积极作用。对于优质的创业公司，还可以作为案例纳入亿欧智库的相关报告，树立权威的行业地位。

- 大型企业

  凭借对科技+产业+投资的深刻理解，亿欧除了为一些大型企业提供品牌服务外，更多地基于自身的研究能力和第三方视角，为大型企业提供行业研究、用户研究、投资分析和创新咨询等服务。同时，亿欧有实时更新的产业数据库和广泛的链接能力，能为大型企业进行产品落地和布局生态提供支持。

亿欧服务

- 政府机构

  针对政府类客户，亿欧提供四类服务：一是针对政府重点关注的领域提供产业情报，梳理特定产业在国内外的动态和前沿趋势，为相关政府领导提供智库外脑。二是根据政府的要求，组织相关产业的代表性企业和政府机构沟通交流，探讨合作机会；三是针对政府机构和旗下的产业园区，提供有针对性的产业培训，提升行业认知、提高招商和服务域内企业的水平；四是辅助政府机构做产业规划。

- 机构投资者

  亿欧除了有强大的分析师团队外，另外有一个超过15000名专家的资源库；能为机构投资者提供专家咨询、和标的调研服务，减少投资过程中的信息不对称，做出正确的投资决策。

- 欢迎合作需求方联系我们，一起携手进步；电话 010-57293241，邮箱 hezuo@iyiou.com

扫码关注亿欧智库
查看更多研究报告

扫码添加小助手
加入行业交流群

亿欧智库

网址：https://www.iyiou.com/research
邮箱：hezuo@iyiou.com
电话：010-57293241

北京：北京市朝阳区关庄路2号院中关村科技服务大厦C座4层 | 上海：上海市徐汇区云锦路701号西岸智塔2707-2708
深圳：广东省深圳市南山区华润置地大厦 C 座 6 层 | 纽约： 4 World Trade Center, 29th Floor-Office 67, 150 Greenwich St, New York, NY 10006