数字经济的安全基石
The security cornerstone of digital economy

安恒信息
DAS-security 安全中国

科创板：688023

大健康行业信息安全
解决方案

2020年网络安全
上市公司双增速第一

极致责任的创新者
国家级核心安保单位

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11月5日正式登陆上交所科创板股票上市，股票代码：688023。自成立以来一直专注于网络信息安全领域，以云安全、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方向为市场战略。凭借强大的研发实力和持续的产品创新，已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全平台以及网络信息安全服务，各产品线及业务线在行业中均形成了强大的竞争力。

在医疗卫生行业，安恒信息专注于为医院、基层医疗卫生机构、卫健委、医保局等不同行业客户构建专业的信息安全保障体系。在互联网+医疗、智慧医院建设、中小医院信息化建设、区域卫生健康信息平台建设，医保信息平台建设等前沿场景，安恒信息均可提供完整可靠的信息安全解决方案，全方位保护行业信息化建设成果，支撑“智慧医院”“智慧医保”“智慧卫健”的安全落地。

目前，安恒信息已经为超过1000+医院、150+卫健监管部门、20+医保局客户提供优秀的网络安全产品与服务，致力于成为医疗卫生行业值得信赖的网络安全专家。

7个研发基地

25个办事处

1000+技术服务人员

重保**0**事故

7*24响应服务能力

目录

01

智慧医院信息安全建设方案

智慧医院建设背景

2020年5月，国家卫健委印发《关于进一步完善预约诊疗制度加强智慧医院建设的通知》。通知中，对智慧医院建设提出明确要求，包括智慧服务、智慧医疗、智慧管理、互联网医院等。具体解读如下：

智慧服务

智慧服务是智慧医院的抓手，2019年国家卫建委发布《医院智慧服务分级评估标准体系（试行）》，明确6个等级，包括电子预约、信息推送、电子病历随诊、药剂配送等17个评测项目，形成覆盖诊前、诊中、诊后的智慧医院服务体系。

智慧医疗

围绕临床，为医护提供信息共享、辅助决策等服务，简化临床工作，建设医护一体、临床一体、智慧决策等机制。

智慧管理

以HIS数据为支撑，核算为基础，对数据进行实时分析，对医院各科室、部门的人、财、物、事等进行综合资源管理，建设医院运营管理平台，具备业务运行、绩效考核、财务管理、成本核算、后勤能耗、廉洁风险防控等能力。

互联网医院

依照《互联网医院管理办法（试行）》等文件建设互联网医院，针对常见病、慢性病人形成互联网咨询、诊疗、监测、会诊、医保结算、药品配送等完整的互联网医疗服务闭环。

智慧医院面临主要威胁

接入终端安全挑战

勒索病毒

医院由于其数据资产价值高、对业务连续性要求高等特点，日渐成为勒索病毒投放的“冤大头”，医院成为勒索病毒攻击重灾区之一。

医疗设备脆弱性

大量PACS、LIS医疗设备采用非标准Windows作为系统内核，存在大量已知的安全性及稳定性漏洞，却无法及时更新补丁，成为安全体系中资产价值高但防护能力差的薄弱环节。

物联网资产缺乏管理

除了PC、医疗设备外，医院会使用大量物联网设备来构建智慧服务，包括信息大屏、排号机、摄像机、自助服务终端等，这些资产繁冗复杂，其安全性无法得到有效监测与管理。

数据中心安全挑战

数据中心云化挑战

云化数据中心有独特安全需求，如平台自身的安全性（包括镜像安全、资源隔离）、租户业务应用数据的安全性等。传统软硬件安全能力对云计算的基础适配能力不足，导致云端数据防护能力不足。

内部人员数据泄露

数据访问控制问题，控制粒度过粗、无法区分账号共用等；数据存储管理问题：未加密、缺乏全生命周期管理等；第三方开发运维人员行为管控问题：权限过高且行为不受控、缺乏高级审计手段等。

外部攻击者窃取

互联网医院业务开展后，外部暴露面增大，外部攻击者通过SQL注入、撞库等互联网攻击手段对数据进行渗透；通过钓鱼、鱼叉攻击渗透外网，穿过网闸攻击数据中心。

互联网安全挑战

DDoS/CC攻击

互联网业务普遍遭受的难以有效防护的攻击类型，攻击者能够以较低的技术成本达到业务崩溃的严重后果。

SQL注入

互联网端攻击者可通过SQL注入方式进行脱库，造成数据集中泄露。

爬虫

爬虫对未经保护的短信认证接口、业务数据接口进行信息爬取，造成核心文本信息泄露或短信轰炸。

网页篡改

根据相关报告，疫情期间医院网站篡改类攻击相比2019年11月增长明显，幅度达到44.92%，造成挂马、散布谣言、发布反动言论等严重后果。

物联网安全挑战

物联网设备脆弱性识别及修复问题

由于物联网设备厂商更加注重功能实现，产品可能存在大量脆弱性问题，包括系统及应用漏洞、不安全的安全配置、大范围端口开放等。由于产品往往不具备或很少具备升级更新功能，脆弱性问题很难有效解决。

非授权设备通过物联网非法接入问题

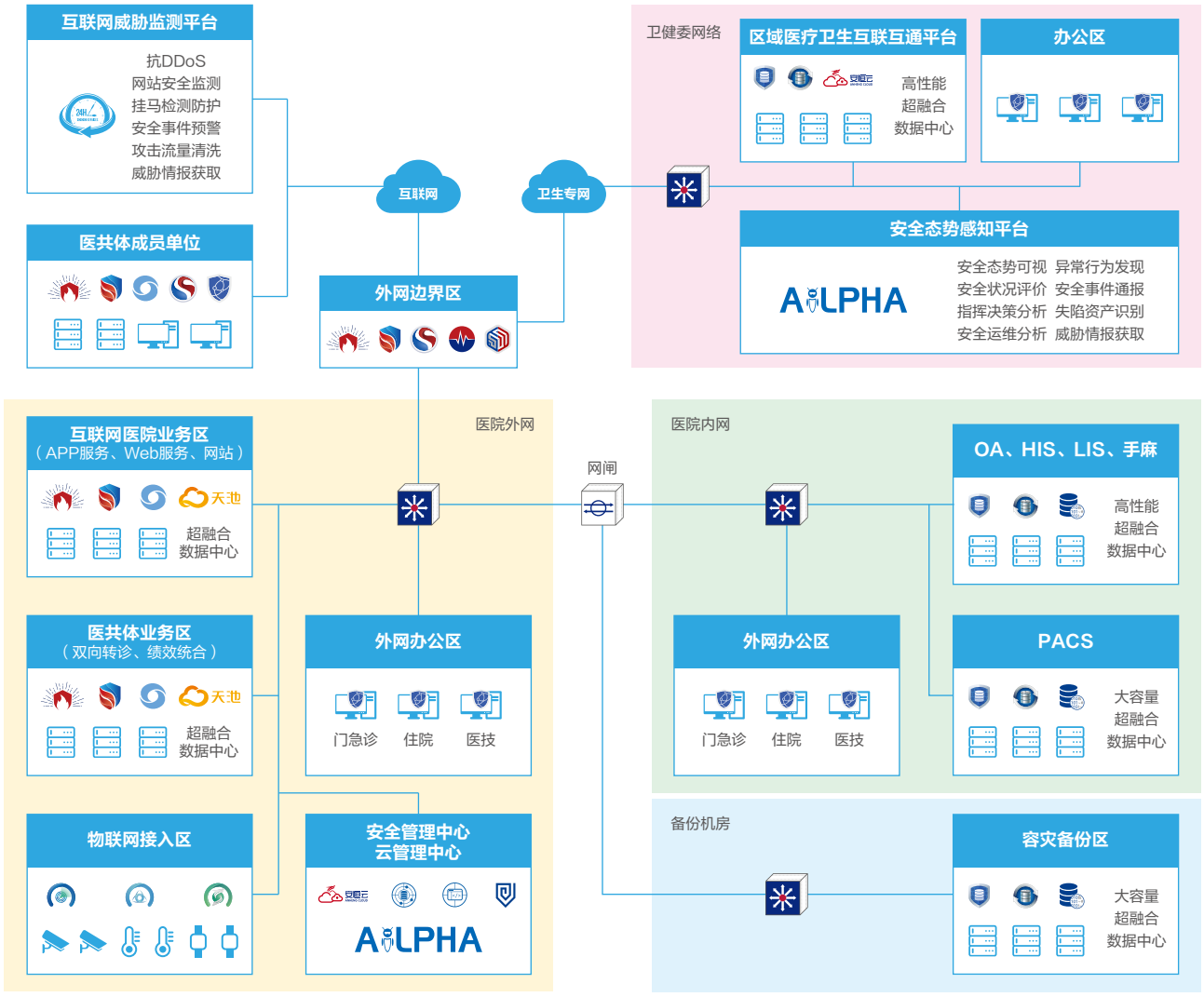
物联网设备往往通过wifi或5G无线网路接入医院外网，医院通常对这些设备缺乏认证手段，容易出现攻击者将PC伪装为物联网设备接入并实施破坏或窃取数据的问题。

物联网设备安全管理的问题

医院会使用大量物联网设备来构建智慧服务，其设备安全性无法得到有效监测与管理。

安恒智慧医院信息安全建设方案

安恒智慧医院信息安全建设方案通过安恒云作为智慧医院数据中心信息化的“底座”，可同时承载安恒SaaS化的安全能力与HIS、LIS、PACS等医疗信息化软件。其上，构建云管中心、安管中心实现统一的运算基础资源与安全资源调配，构建智慧安全大脑。通过在医院各个部门（门/急诊、住院部、医技支持、体检中心等）部署NGFW、EDR、日志审计、堡垒机、WAF、物联网监测等安全产品，形成安全能力的全覆盖。在互联网端通过玄武盾监测平台实施对互联网医院的7X24小时监测与防护。



医院内网

- 医院主要信息系统均部署在内网，因此整个内网数据中心均可部署在安恒云上，提供计算、存储、网络的完整云化能力。同时，数据安全是内网安全建设的重点。在内网通过数据库审计、日志探针抓取数据，在AiLPHA安管中心构建UEBA为核心的数据安全行为模型，对外部黑客统方、内部账号失窃、运维人员脱库等行为进行有效识别和发现。同时部署EDR，对服务器系统进行防勒索保护。

医院外网

- 医院外网PC众多，也是勒索病毒重灾区，通过EDR完成勒索病毒的针对性加固。同时，在DMZ区通过轻量化的超融合承载邮箱、OA、医共体等外网业务的同时，通过等保一体机的形式完成NGFW、WAF等边界安全能力的部署。物联网接入区中应通过物联网监测、态势感知、安全心、物联网接入网关等一系列产品完成物联网至医院外网的安全接入建设。

互联网医院

- 互联网医院的出现对信息中心带来了前所未有的挑战。DDoS、爬虫等一系列互联网安全威胁是医院从未接触过的。通过玄武盾平台，对部署在互联网上的业务系统进行7X24小时监测，有效遏制DDoS、CC攻击、挂马、爬虫、SQL注入等互联网威胁。同时，可通过安恒云提供完整的基础架构与等保合规保护。

方案价值与优势

架构先进，省钱省心

通过安恒云大面积运用超融合及云化架构，横向扩展能力节省大量部署运维成本，服务节点自愈能力保障业务高可用，快照技术保障数据高可用。

安全大脑，智慧决策

通过安全管理中心构建智慧医院的安全大脑，自动化分析、编排、响应、管理，无需高额技术和成本投入即可拥有身边的“白帽子”。

能力丰富，面面俱到

在终端、网络、数据中心、互联网均具备相应的识别、防御、检测、响应能力，网端联动、云端联动、云网联动，实现发现早、防得住、看得清、响应快。

02

中小医院及基层医疗卫生机构信息安全建设方案

中小医院信息化现状

在中小医院信息化发展过程中，预算投入受限、团队人手不足、技术手段贫乏等问题普遍存在。因此，信息化发展呈现两种不同的发展路线：

对院内信息化进行逐步规划升级

医院以向三级医院进行升级作为目标，在现有信息化基础之上，以三级医院信息化作为标杆（如高等级互联网互通、电子病历系统等），以评促建，对HIS、电子病历等核心系统进行升级，支撑医院运营与临床工作。此路线下，医院“以我为主”的建设思路能够得到落实，但对医院规划和建设能力要求较高。

采用云HIS等云化系统快速满足需求

以满足现有医院云化需求为根本，快速低成本在云端部署云HIS等系统，院内仅保留PC、移动终端进行接入，核心信息系统与数据资产均在云端，院内网络无隔离。此路线下，能够迅速完成信息化系统的部署，前期投入成本低，但医院在功能迭代、架构升级等方面会面临“受制于人”的状况。

中小医院信息安全需求

两种信息化路线下，安全需求侧重点有所不同：

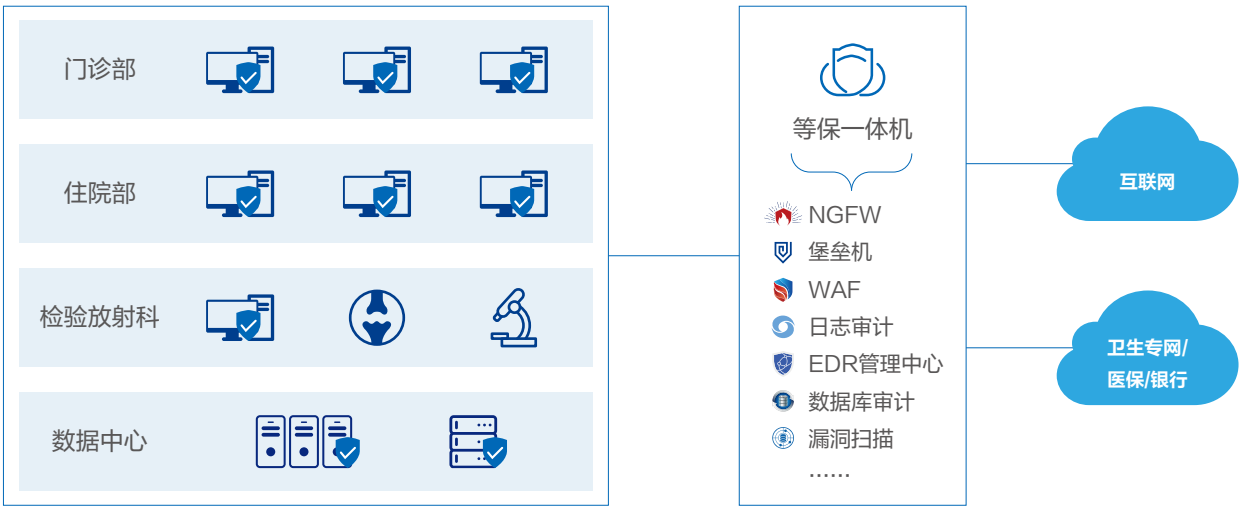
院内信息化路线

以保护院内核心信息系统与数据资产为第一目标，充分考虑等级保护与医院信息化安全建设方面的合规需求，重点解决勒索病毒、院内外数据窃取、运维安全漏洞、上级监管部门通报等问题。

云端信息化路线

云端系统在互联网上暴露面会更大，因此云平台自身安全与云上业务安全需求成为关注的重点。包括云平台对DDoS、爬虫等攻击的防护、云平台不同租户的隔离性、医院自身业务的访问控制与审计、业务系统漏洞的解决方案，安全事件发生后的应急响应机制等。

安恒院内信息化路线的安全建设思路及方案优势



思路：通过等保一体机满足安全合规与纵深防御需求

- 等级保护是安全建设的基础。通过等保一体机内置九大安全能力（下一代防火墙、WEB应用防火墙、主机安全卫士（EDR）、网页防篡改、APT、漏洞扫描、日志审计、数据库审计、堡垒机），完整覆盖等保二、三级要求具备的网络及终端的安全措施。和传统堆叠盒子建设方案相比，等保一体机能够将过剩的硬件资源利用起来，以较低的成本就能够完成安全能力的部署。

优势：在安全建设投入有限情况下具备基本完整的安全防护能力

- **一机多能，安全能力完善**

  完全符合等保2.0的“一个中心，三重防护”的技术要求，安全能力覆盖通信网络、区域边界和计算环境，通过构建覆盖事前监测、事中防护、事后审计的全生命周期的安全体系，快速实现等保合规建设落地，全方位满足业务系统多样化的安全需求。

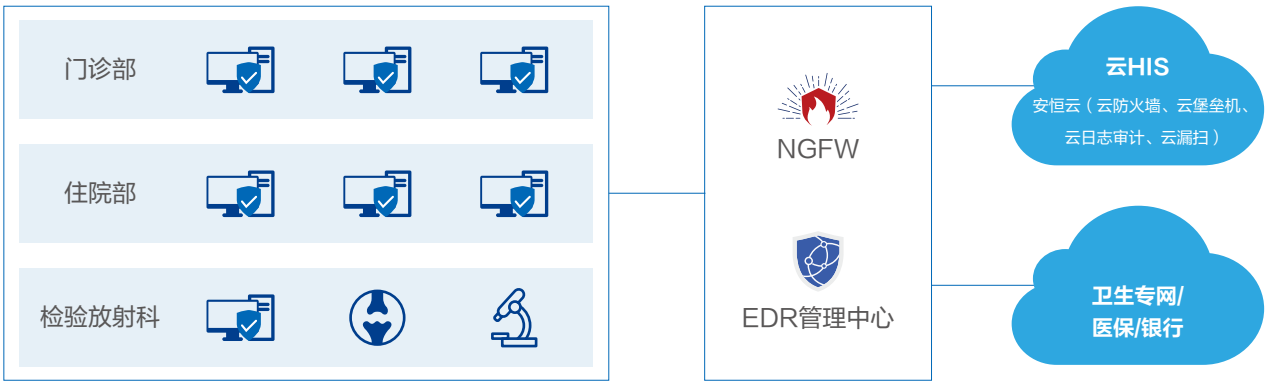
- **敏捷部署，节约信息科管理运维成本**

  单机交付，旁路部署，免去传统等保方案各类设备复杂的部署过程，广泛适用于物理环境和虚拟化环境下的等保2.0建设，不影响已有的网络架构，智能引流，部署更简单，使用更高效。内置等保二级、三级套餐，安全能力一键上线。

- **弹性扩容，帮助医院信息化升级后无需增加相应的安全投入**

  等保一体机能够实现各类安全组件服务化交付。用户可基于自身业务特点与需求，灵活选择与搭配安全服务，按需获取安全资源。自定义安全资源的种类、规格、数量、使用时长、配置等，提升安全资源的利用率，避免资源过度占用造成浪费。随着安全业务的扩展，等保一体机可以为用户提供安全资源池和安全产品的动态扩展能力，当硬件资源不足时，等保一体机支持纵向扩容内存、硬盘等资源，提升整体资源池的性能，实现安全资源的弹性扩展和灵活调度。

安恒云端信息化路线的安全建设思路及方案优势



思路：通过安恒云完成云端安全能力构建

云HIS模式下，医院核心数据与应用系统被转移到云端，安全保护对象由院内转向云端。在云安全方面，需要依照等保2.0云计算扩展要求，与云服务提供商一起对平台与业务系统进行安全建设。在云服务提供商选择方面，医院需要验证其平台是否具备符合相应等保要求的安全措施。在业务搭建层面，应重点关注以下方面：

- **网络和通信安全：**采用在云内虚拟边界部署防火墙、入侵检测防御、WAF等产品完成云内边界构建，形成基本访问控制能力；同时采用密码技术进行云端业务访问。
- **计算环境安全：**通过应用漏扫与安全审计完成计算环境脆弱性发现与业务流程的安全可追溯。同时通过EDR等产品保障系统对恶意代码的免疫能力。
- **应用和数据安全：**对业务应用进行7X24的安全监测，分析安全威胁，并通过安全管理中心进行安全管理。通过渗透服务，具备接口安全情况的感知能力。
- **采用安恒云一键完成安全防护：**NGFW等产品可通过镜像共享的方式将虚机NGFW部署在VPC内。EDR、网页防篡改、数据库审计等产品可部署Agent到云主机上，通过安恒云进行统一管理和配置。其它安全能力如云扫描、云WAF、云堡垒机等产品只需网络可达即可实现对应的安全防护效果。

优势：专业、快速的云安全解决方案

- **丰富多样的安全服务能力：**为云环境中的医院用户提供全方位基于“安全云”的安全保障服务能力。用户可以自行选配。灵活使用，最终建设形成自有的云内业务系统安全解决方案，覆盖事前、事中、事后的全方位安全防护。
- **等保标准一键落地，快速合规：**为医院用户的不同业务提供满足等保合规的安全能力，用户只需按需自助申请开通和配置使用即可，帮助用户快速满足等级保护要求，业务合规。
- **开放兼容各类主流云平台：**安恒云可无缝对接阿里云、华为云、腾讯云、Ucloud、百度云、青云等主流公有云平台，通过统一门户实现对多云资产的统一管理、统一运维、统一运营，实现“云+安全”一体化实践。

03

互联网医院信息安全建设方案

互联网医院建设背景

经过数年发展，“互联网+医疗”成为医院信息化的新热点。通过互联网技术打破时间空间桎梏，让患者高效便捷获取医疗服务，让医疗资源合理流动，互联网医院利用信息技术为患者、医院、医生打造了一个三方共赢的创新点。

互联网医院业务建设主要是终端接入层，包括患者端APP与小程序的搭建。同时在私有云或公有云上搭建互联网业务服务层，包括入口、医生工作台、远程咨询、远程诊断、远程监测、远程会诊等子系统。同时，需要搭建电子处方系统，与社会药房对接，完成药品下单、配送的闭环。底层的临床、管理、电子病历数据均来自医院现有HIT体系。医保及费用结算在医院业务层完成。

互联网医院信息安全需求

根据国家卫健委《互联网医院办法（试行）》的要求，所有互联网医院安全建设应达到等保三级。同时，医院模式下的互联网医院建设，通常分为三层：终端接入层、互联网业务层、医院业务层，三层在等保框架内，均有不同的安全需求：

终端接入层

本层主要载体是APP、小程序和Web前端，是互联网医院的“接待大厅”，主要的安全问题包括：

- **前端系统脆弱性：**针对APP、小程序及Web前端的代码漏洞，恶意攻击者可在本地文件中获取系统信息及用户数据，进而对业务端发起跳板攻击。
- **中间人攻击及窃听：**在网络通信层面，监听前端流量，甚至冒充合法用户对服务端进行访问。

互联网业务层

本层是互联医院主要业务的承载体，包括远程咨询、远程诊疗、远程监测、远程会诊等，通常采用私有云或公有云方式部署在互联网上，主要的安全问题包括：

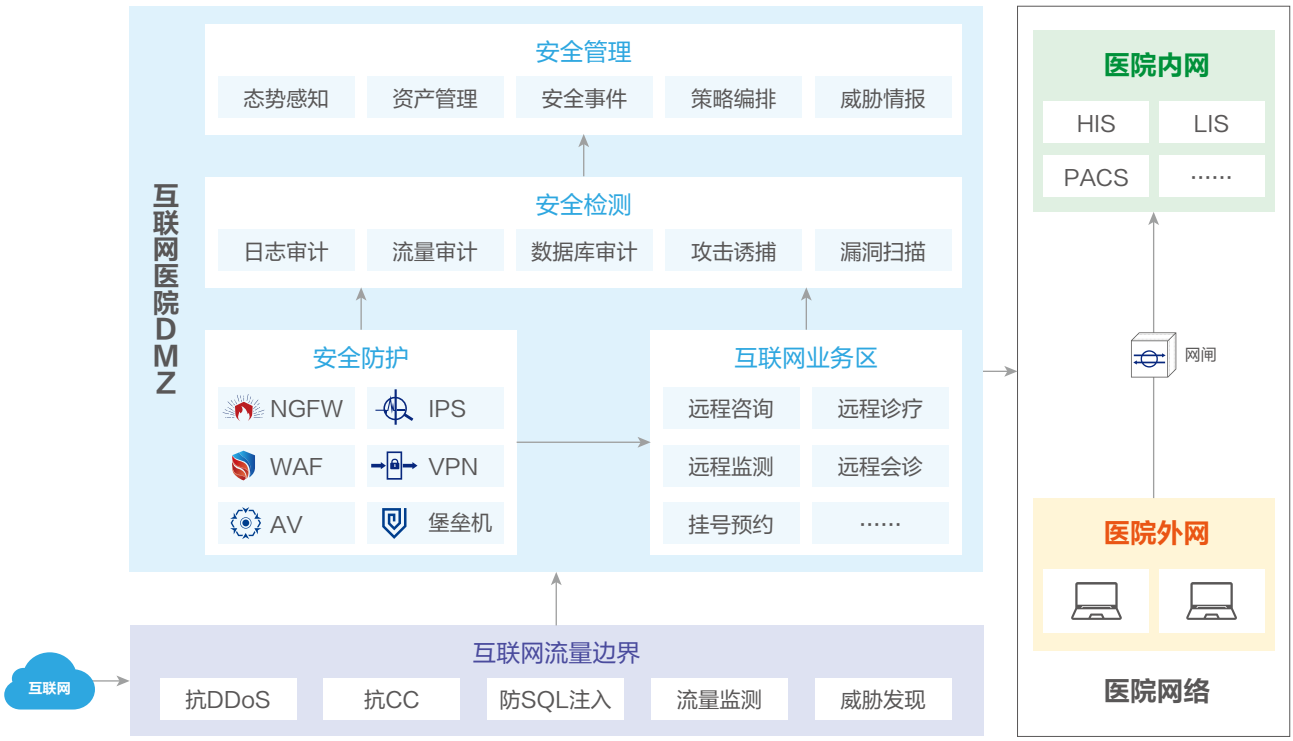
- **DDoS/CC攻击：**互联网业务普遍遭受的难以有效防护的攻击类型，攻击者能够以较低的技术成本达到业务崩溃的严重后果。
- **爬虫：**爬虫对未经保护的短信认证接口、业务数据接口进行信息爬取，造成核心文本信息泄露或短信轰炸。
- **数据泄露：**互联网端通过SQL注入方式进行脱库，造成数据集中泄露。

医院业务层

本层主要承载医院内网业务，包括HIS、LIS、PACS、RIS等，主要安全问题包括：

- **勒索病毒、挖矿软件：**医院最迫切解决的安全问题。
- **数据泄露：**数据的内部非法访问是医院数据安全的最大问题，也是医院最关注的安全问题。

安恒互联网医院信息安全解决方案



安恒信息为互联网医院提供“互联网医院DMZ上云”的整体安全解决方案，包含5个组件：

- **云安全组件**
  可同时提供云平台安全防护能力与云上安全能力。采用云防护中心、云检测中心、云安管中心的三中心设计，完整满足等保2.0（三级）要求中移动互联网扩展要求、云安全扩展要求。

- **互联网流量边界**
  提供抗DDoS、抗CC、防SQL注入等安全功能，完成对互联网访问流量的防御与清洗。

- **前端代码安全服务**
  通过代码安全审计、上线前渗透检测等安全服务，帮助客户对APP、小程序等前端入口进行脆弱性检测与分析。

- **医院终端安全组件**
  通过EDR针对性解决勒索病毒、挖矿软件、终端管理混乱等一系列终端安全问题。

- **医院数据安全组件**
  针对数据安全需求，通过数据库审计+数据库网关+数据脱敏+堡垒机等产品提供完整的数据安全防护与审计能力。

方案价值与优势

完整满足等保2.0三级相关要求

安恒互联网医院信息安全建设方案充分参考等保2.0三级基本要求与云计算要求，在完整满足等级保护相关要求的基础之上，为互联网医院信息系统提供立体、纵深的安全保障防御体系，保障互联网医院系统健康运行。

针对互联网威胁的一体化防护

安恒信息具备10余年互联网安全技术研究经验，在互联网暴露面管理、互联网信息系统安全监测、访问流量分析与清洗、失陷资产发现等领域具有独特技术优势。

同时满足公有云+私有云互联网医院安全解决方案

安恒信息为部署在公有云上的中小互联网医院提供完整的云安全解决方案，通过安全资源池的云WAF、云NGFW、云堡垒机、云审计、云EDR等多个组件，形成默认适配、一键开通、迅速部署的安全能力集合。同时，针对私有云化的互联网医院，安恒信息通过等保一体机全面的安全能力以及SaaS化的互联网信息系统监测与流量清洗方案，保障互联网业务安全不中断。

04

区域卫生健康信息安全监管与建设方案

区域医疗信息安全监管迫在眉睫

《网络安全法》出台后，保障信息安全不仅是医疗机构与公安、网信部门的职责所在，政府行业监管部门同样应在职责范围内对辖区内医疗机构肩负指导、监管责任。另一方面，勒索病毒层出不穷、大规模医疗数据泄露频发，针对大型三甲医院及科研院所的网络攻击激增，这一系列重大网络安全事件让医疗行业处在网络安全的“风口浪尖”。因此，对于卫健委等政府监管部门，医疗行业信息安全监管迫在眉睫。

医疗信息安全监管需求分析

评价区域医疗机构安全建设情况

从漏洞、弱口令、安全配置基线等脆弱性数量、分布及危险程度评价各地网络安全建设情况。从安全事件响应速度，处理结果评价各地应急响应制度建设情况。

主动发现、通报、处理安全隐患

化被动为主动，前期能预警、中期能控制、后期能恢复，是态势感知平台建设的重要目标。掌握安全态势后，针对下辖医疗机构，区域医疗平台等系统进行针对性安全建设加固。查缺补漏，提升地区医疗行业网络安全整体建设水平。

跟踪干预大规模医疗数据泄露等重点安全事件

针对来自境内外大规模网络攻击等重点网络安全事件能够进行识别、锁定、跟踪。能够对下属单位进行安全预警、通报、事件督办、结果验证，动态掌握处理情况。

安恒区域卫生健康信息安全监管与建设方案

加强内网态势感知与安全管理能力

卫健委建设医疗行业安全态势感知平台，利用大数据及人工智能技术，从防御侧视角采集分析全网安全数据。平台可发现安全隐患，评价安全建设成果、跟踪安全事件、加强安全管理，化被动为主动提升全行业网络安全水平。

建设互联网医院安全监测与流量清洗能力

互联网+医疗大势所趋，卫健委应对区域内互联网医院网络安全情况进行持续监测。同时从攻击侧视角定位外部网络攻击，在安全事件初期对辖区内各医院、单位进行预警通报，具备流量清洗等干预处置能力，有效降低损失。

安恒信息通过内网态势感知平台+互联网监测与流量清洗平台+安全评估及应急响应服务，三位一体全面解决区域医疗卫生网络安全监管“看不清、搞不懂、控不住”等问题。

内网态势感知平台——通过大数据分析技术为不同角色提供不同分析视角与建议

- **为主管领导提供指挥决策视图**：支持安全建设成果展示、安全威胁统计可视、下属单位能力评价、关键系统安全状态可视、实现资产发现、重大安全事件处置进度、违规人员定位等。
- **为运维人员提供安全可视化运维视图**：支持安全事件定位、调查、取证、溯源和处置等功能。
- **为上级主管部门提供安全态势报告**：通过对安全态势数据的周期性归纳总结、统计分析，定期形成全网安全态势分析报告。

互联网监测与流量清洗平台——通过7*24的监测预警与流量清洗保障互联网应用的安全与高可用

- **提供安全漏洞检测服务**：通过大数据漏洞扫描技术，定期对目标网站进行全面的安全漏洞扫描，发现系统存在的各类安全隐患，并持续跟踪漏洞修复情况。
- **提供安全事件监测服务**：对Web系统进行页面资源与指纹信息的分析，通过监测技术对各类安全事件进行全面分析感知，包括篡改、暗链、黑页、挂马、后门等，并向相关部门和人员进行定向安全通报。
- **提供内容监测服务**：对Web系统中的非法及不合规的内容进行筛查，包括敏感外链监测、敏感词监测、错链坏链监测等
- **提供系统可用性监测服务**：对于重点系统，采用分布式节点进行数据监测，以多链路多点监测形式，发现在不同区域内网站系统的多线路访问可用性情况。网站服务质量实时监测，提供目标站点的域名解析可用性、网站服务可用性、以及网站内容可用性监测，能够较为全面的实时了解网站可用性状况。

安全评估及应急响应服务——定期的全面体检与紧急状态下的外部介入

- **系统安全评估：**对辖区内特定范围信息系统及管理制度进行全面的安全性评估，如系统漏洞情况、安全配置合理性情况、源代码漏洞情况、安全制度漏洞情况等。
- **安全事件响应分析：**在系统出现系统恶意入侵、恶意资源消耗、病毒爆发及其他各类安全事件时，安恒信息会在规定的安全应急响应时间内，派出应急响应人员对安全事件进行分析和处理。
- **安全事件灾难恢复：**当系统由于出现安全事故，造成系统无法正常对外提供服务时，安恒信息会在服务要求中规定的安全应急响应时间内，派出应急响应人员协助客户完成包括但不限于，系统安全恢复、应用服务安全恢复、数据安全恢复、网络性能安全恢复，网络病毒灾难恢复等在内的灾难恢复工作。
- **安全事件入侵追踪和取证：**在系统出现各类型安全事件后，安恒信息负责对安全事件进行分析，开展安全事件入侵追踪、犯罪取证、事后安全分析和处置服务。

05

医保局医保信息平台信息安全建设方案

医保信息平台建设背景

根据国家医疗保障局规划，在全国稳步推进“建设一套全国统一的医疗保障信息系统，搭建国家医保信息平台和省级医保信息平台，提高全国医保标准化、智能化和信息化水平，重点推进公共服务、经办管理、智能监管、分析决策四类医保信息化应用”的信息化建设工作。其中医保信息平台是医保工作全国一盘棋的重点所在。

医保信息平台信息安全需求

安全合规需求

在国家级及省市级医保信息平台建设过程中，需充分考虑等级保护以及国家医保局《医疗保障核心业务区网络安全接入规范》、《医疗保障信息平台-云计算平台规范》等信息安全相关法律法规及政策文件的指导要求。

云平台安全需求

与传统信息化建设不同，医保信息平台大规模采用了云计算等相关技术。云安全是平台建设的基石，需重点考虑，包括DDoS防御、流量监测、XSS、SQL注入等网络漏洞攻击防御等。

网络安全需求

网络是平台能够体现价值的重要通道，因此在平台建设过程中应充分考虑网络相关安全问题。在网络规划建设时需充分体现纵深防御思想。

数据安全需求

医保信息具有极高的真实性与敏感性，更由于其覆盖范围广数据价值极高。因此，数据安全保护是平台设计建设前就应充分考虑的重点问题，例如多方数据交换的安全问题、数据使用的审计问题、数据访问的控制管理问题等。

安全运营管理需求

安全不是“一锤子买卖”。网络威胁持续存在，那么平台建设应充分考虑长期运营过程中的安全问题，包括持续的安全监测、漏洞发现、安全事件应急处理、运维安全等。

安恒医保局医保信息平台安全建设方案

- **网络安全能力建设**

  根据国家医保局相关要求对网络进行规划。通过横向边界与纵向边界进行外部单位的安全隔离，边界中部署防火墙、入侵检测、审计、防病毒、身份鉴权等网络安全能力；同时设计核心业务区与公共服务区，中间通过网闸等安全设备进行数据隔离交换。安恒NGFW具备完整的网络侧安全威胁防护能力。

- **云安全能力建设**

  通过安恒云内置的各类安全能力（如云WAF、云NGFW、云堡垒机、云审计），从云监测、云防护、云审计三个维度全方位保障云平台及云上业务安全。安恒云安全能力兼容主流云平台，并适配支持开源云计算技术，具备安全能力一键开通、全可视化防护、安全资源生命周期管理等特色。

- **终端安全能力建设**

  通过安恒EDR部署终端安全能力，具备勒索病毒专杀及预防加固能力，同时能够对服务器及终端主机的安全状态、漏洞情况进行检查修复，具备失陷主机发现与隔离能力。

- **数据安全能力建设**

  通过安恒数据安全岛，对医保信息平台与外部单位进行数据交换的全过程进行安全保障，利用区块链、联邦学习、同态加密等技术，实现数据交换可审批、可审计、可追溯、可控制，解决数据共享场景下各方安全互信问题。同时，结合数据脱敏、数据加密、数据库网关、数据库审计、数据水印等一系列的产品，为医保数据全生命周期提供完整保护。

- **安全管理能力建设**

  利用安恒安管中心作为抓手，将安全运营全流程融入安全管理，在预测、识别、管控、防御、响应、恢复、追溯等各个节点部署相应的处理流程与能力。结合AI自动化编排能力，实现安全状态一目了然、已知威胁自动处理、未知威胁分析建议、安全策略统一调配等安全目标。

方案价值与优势

完整合规，面面俱到

通过安恒信息完整的产品线，在网络安全及平台安全部分均可提供优秀的解决方案，完整满足等保及文件要求。

安全大脑，智慧管理

云安全、云管理一体两面，通过安管中心构建智慧安全大脑，自动化分析、编排、响应、管理，无需高额技术和成本投入即可拥有信息安全的AI专家辅助决策。

全流程保障数据安全

在数据生命周期的存储与访问阶段，提供加密、身份认证、访问控制、审计方案，同时在流转阶段提供基于联邦计算、区块链等前沿技术的跨网数据交换方案。

合作客户（部分）

- 北京医院
- 北京大学人民医院
- 北京大学口腔医院
- 复旦大学附属华东医院
- 复旦大学附属儿科医院
- 复旦大学附属金山医院
- 上海交通大学附属第一人民医院
- 上海交通大学附属第六人民医院总院
- 同济大学附属肺科医院
- 中国福利会国际和平妇幼保健院
- 上海市第一妇婴保健院
- 上海市同济医院
- 上海市浦东医院
- 浙江大学医学院附属第二医院
- 浙江大学医学院附属邵逸夫医院
- 浙江大学医学院附属口腔医院
- 浙江大学医学院附属儿童医院
- 广东省人民医院
- 中山大学附属第一医院
- 中山大学附属第二医院
- 中山大学附属第三医院
- 南方医科大学南方医院
- 南方医科大学附属第三医院
- 湖北省人民医院
- 湖北省中山医院
- 武汉市中心医院
- 武汉儿童医院
- 武汉雷神山医院
- 郑州大学第一附属医院
- 青岛市妇女儿童医院
- 青岛市中心医疗集团
- 青岛大学附属心血管病医院
- 青岛市口腔医院
- 青岛西海岸新区中医医院
- 芜湖市第二医院
- 安徽医科大学第一附属医院
- 宿州市立医院
- 蚌埠医学院第一附属医院
- 宣城市人民医院
- 浙江省卫生健康委员会
- 浙江省疾病预防控制中心
- 湖南省疾病预防控制中心
- 新疆维吾尔自治区医疗保障局
- 新疆生产建设兵团医疗保障局
- 聊城市医疗保障局
- 济宁市医疗保障局
- 青岛市黄岛区卫生健康局
- 青岛市疾病预防控制中心
- 中国人民海军疗养院
- ……

* 以上合作客户排名不分先后

安恒信息
DAS-security 安全中国

为行业客户量身打造
网络安全+N个细分行业

找行业解决方案
上行家小程序

如何精准查找大健康行业信息安全解决方案？

数字经济转型
5G边缘计算
零信任
APP安全认证
云计算
《个人信息保护法（草案）》
打击网络犯罪
网络安全审查
网络安全防护
新型智慧城市
路网协同
《数据安全法（草案）》
大数据轨迹查询
智能安全

网络安全行家
有需求，搜一下

电子版阅读或下载请扫码进入

行家 1+n 你的内行专家
网络安全行业资料线上整合平台

快 懂需求，按图索骥
准 懂场景，一键直达
特 懂技术，不再有鸿沟

19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

让安全更智能 • 让智能更安全

Make security more intelligent • Make intelligence more secure

杭州2022年第19届亚运会官方网络安全服务合作伙伴

杭州安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

官网：www.dbappsecurity.com.cn
电邮：info@dbappsecurity.com.cn
客服专线：+86-400-6059-110
直通专线：首席客户成功官　沈亚婷　18100188999
　　首席客户成功官　刘蓝岭　18100189888

安恒信息官方微信

杭州总部
地址：杭州市滨江区西兴街道联慧街188号安恒大厦
座机：0571-88380999/28860999
传真：0571-28863666

科创板：688023