SANGFOR 深信服科技

一体化安全架构在互联网+模式下的应用探讨

深信服医疗事业部副总经理 钟一鸣

国家对互联网+医疗的政策支持

SANGFOR 深信服科技

国务院

2018年4月

国务院办公厅发布关于促进“互联网+医疗健康”发展的意见

国家卫健委

2018年9月

《互联网诊疗管理办法（试行）》

《互联网医院管理办法（试行）》

《远程医疗服务管理规范（试行）》

密集的政策发布为中国快速发展的“互联网+医疗”指明了方向。

SANGFOR
深信服科技

互联网+医疗带来的变革

从安全的角度看医疗行业信息化特点

SANGFOR 深信服科技

敏感信息多	数据资产成为核心攻击目标	病历、用药、研究成果、涉及隐私的就医者信息；
网络庞大复杂	网络难管理、安全边界模糊	各分系统、子系统之间，即独立又有千丝万缕的联系；
共享要求高	业务安全、平台稳定难保障	各部门各系统的协同共享，与外联单位如：银行、医保等每个环节都关键；
威胁源众多	风险点众多，威胁难定位	医院的信息系统不是孤立的，而是众多合作单位甚至互联网都存在接口
管理难落地	安全管理的有效性不明确	管理存在疏漏或人员个人习惯的不同，导致对网络安全的有效管理缺失，给黑客留下可趁之机。

互联网+医疗模式下的业务发展趋势

SANGFOR 深信服科技

新型业务开展

- 为简化患者就医流程，预约挂号、移动支付等业务快速兴起

业务需要，医院内外数据共享

- 医院内外部业务数据共享，内网应用直接或间接与互联网连接

多机构业务协同作业

- 医院与卫生部门、第三方机构信息共享与业务协同作业

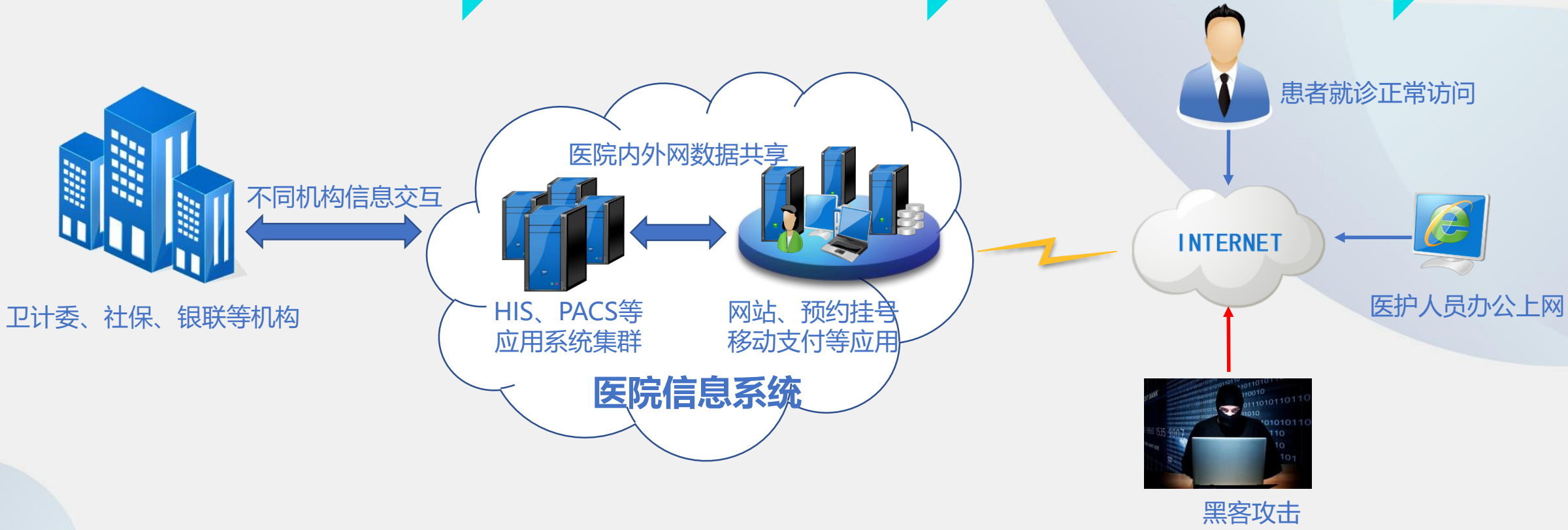
网络安全法、等保2.0

- 《网络安全法》要求医院作为网络运营者有责任保障患者个人信息安全，具备安全事件监测预警和应急处置的能力

互联网应用带来安全风险陡增

SANGFOR 深信服科技

信息共享与业务协同 → 医院网络愈加开放 → 安全威胁迅速增加



互联网+医疗模式下的安全痛点

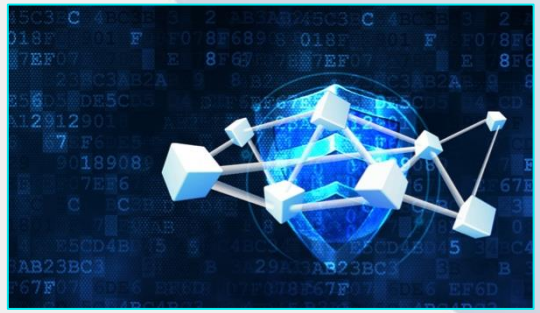
SANGFOR 深信服科技

融合安全

大量安全设备来自于不同的厂商，无论是设备功能还是安全服务都无法有效联动；

安全性

随着网络攻击手段的多样化，一台防火墙就解决问题的时代早就过去了；



扩展性

互联网+医疗的业务是逐步建设的，安全是否要一步到位？投入产出比谁来负责；

SANGFOR
深信服科技

安全的重新定义

一体化安全架构的引入

SANGFOR 深信服科技

第三方安全服务

深信服安全服务

安全合规手段服务化交付

高级防御服务

失控主机发现服务

高级防御服务

数据库审计服务

运维审计服务

基础防御服务

安全接入服务

失控主机发现服务

威胁情报服务

……

安全实力

虚拟化实力

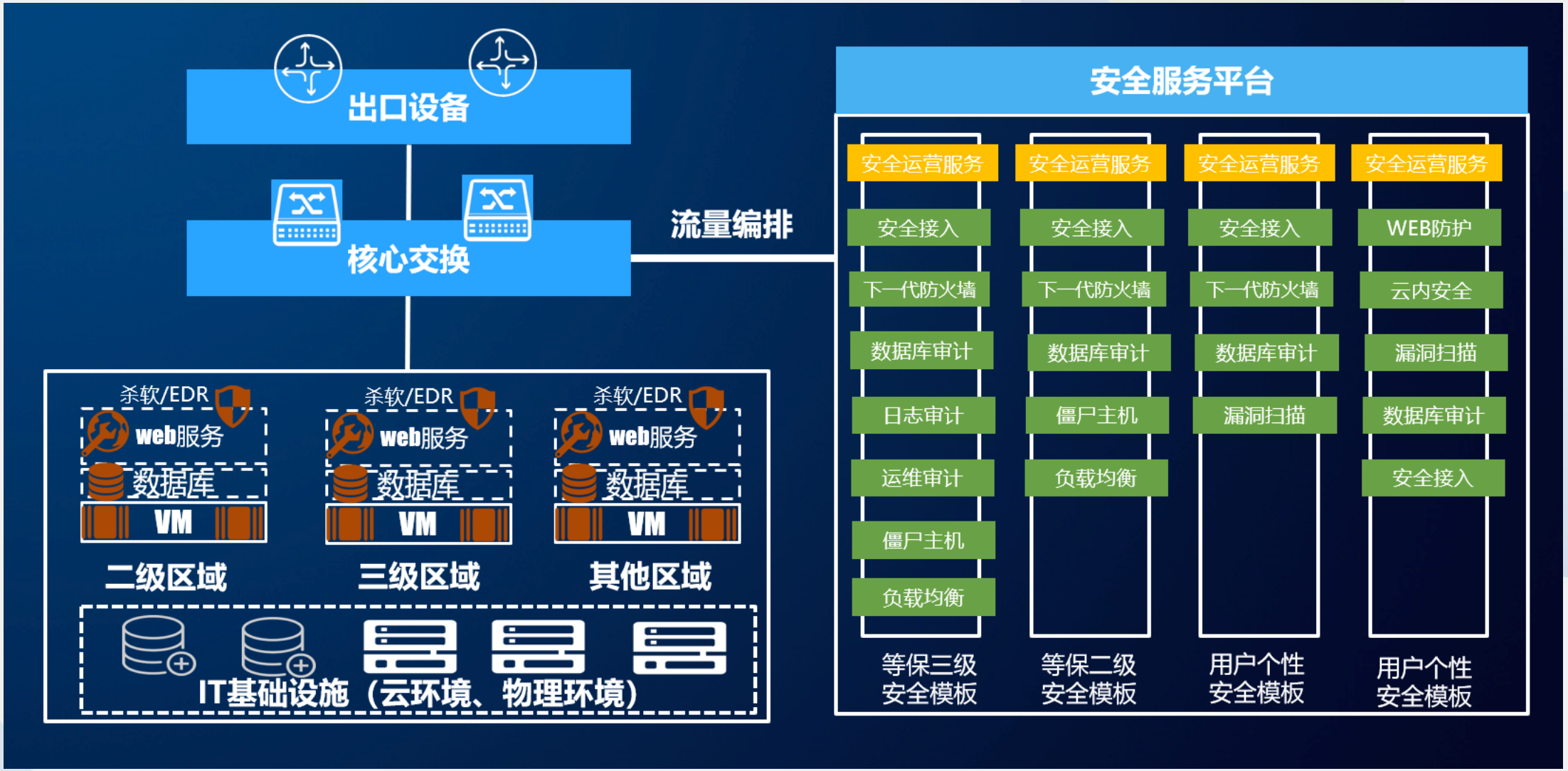
一体化安全架构

深信服超融合平台

标准X86服务器

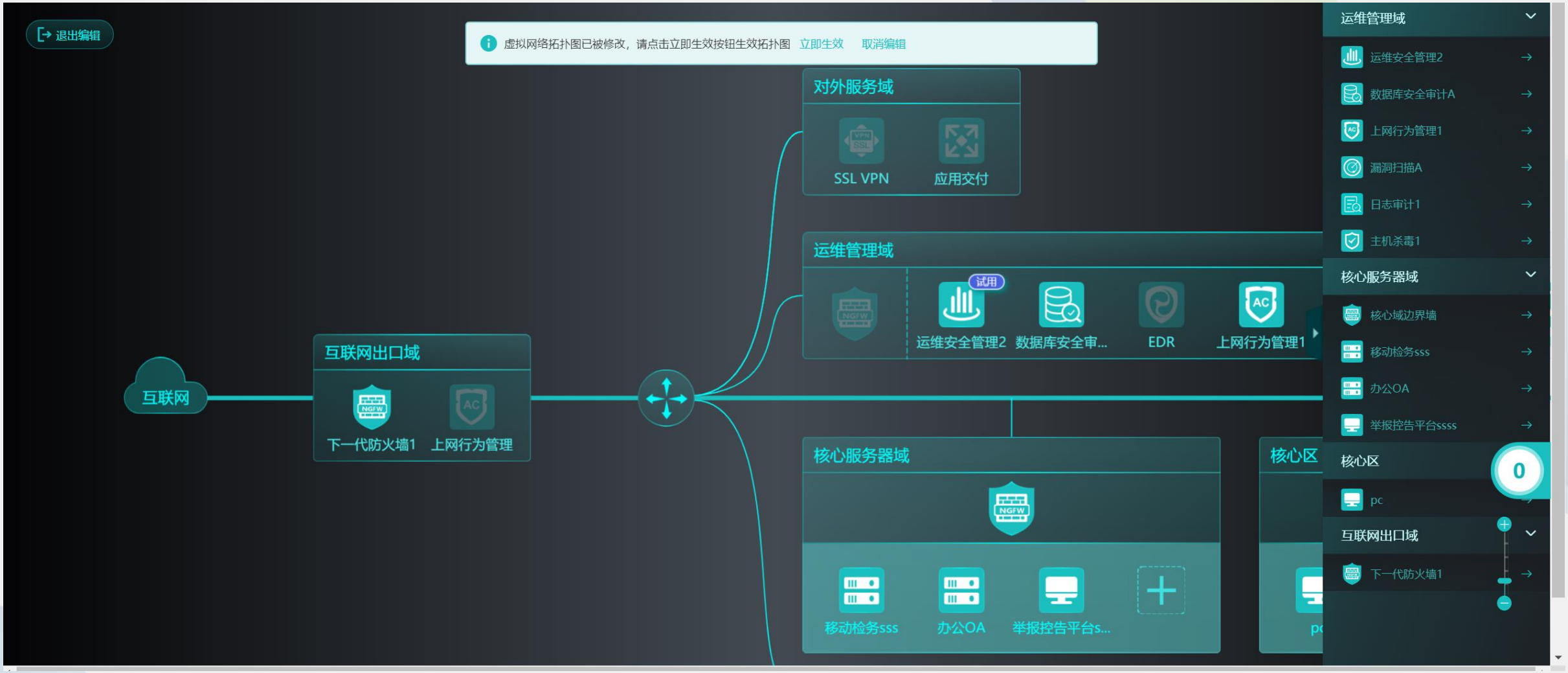
一体化安全架构硬件方案

SANGFOR 深信服科技



一体化安全架构软件方案

SANGFOR 深信服科技



一体化安全架构安全能力清单

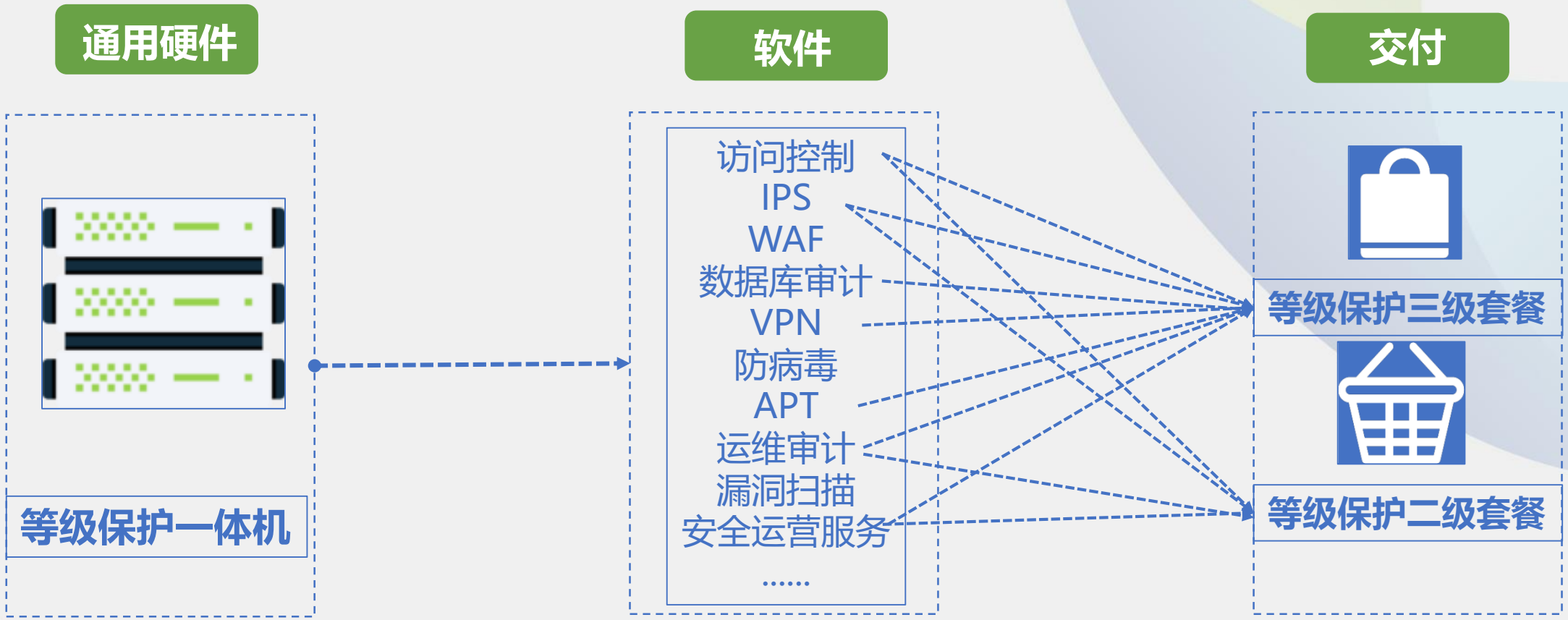
SANGFOR 深信服科技

服务/组件名称	服务内容	备注
主机安全	提供主机端的端点安全服务	深信服产品
下一代防火墙服务	提供FW、IPS、WAF、防篡改服务	深信服产品
数据库审计	提供数据库审计服务	深信服产品
失陷主机发现	提供僵尸网络发现、实时漏洞分析服务	深信服产品
上网行为审计	提供访问行为内容监测服务	深信服产品
安全接入	提供VPN接入服务	深信服产品
网络防病毒服务	提供提供网络病毒防护服务	深信服产品
漏洞扫描服务	提供系统漏洞扫描服务	第三方（如漏洞盒子等）生态产品；
安全检测服务	提供安全威胁检测服务	深信服产品，SaaS化服务
日志审计服务	提供日志审计服务	第三方（如聚铭科技等）生态产品；
主机防病毒	提供主机防病毒服务	第三方（如瑞星、江民等）生态产品；
CA证书	提供数字证书服务，包含私钥，公钥管理	第三方（如北京CA等）生态产品；
安全管理	提供全网安全集中统一管理	深信服租户安全门户；
容灾备份	提供数据容灾和备份服务	深信服服务，或第三方生态产品
邮件网关	提供邮件安全防护	第三方（如彩讯科技等）生态产品；
应用负载均衡包（AD）	提供应用服务负载均衡服务	自有服务包
DLP（终端防泄密）	提供终端数据防泄密和终端安全防护服务	第三方（如美创科技、中安威士等）生态产品；
安全能力不断增加中		

一体化安全架构在等级保护中的应用

SANGFOR 深信服科技

互联网诊疗管理办法（试行）：实施互联网诊疗的平台、网络、系统需要通过等保三级评测



一体化安全架构在等级保护中的应用

SANGFOR 深信服科技

受深信服科技股份有限公司委托，国家信息中心于 2018 年 7 月 9 日至 2018 年 7 月 17 日，依据 GB/T 22239-XXXX《信息安全技术 网络安全等级保护基本要求-试行稿》 标准中第三级的相关要求对 深信服云安全服务平台（等保一体机）CSSP V4.0 进行了产品标准符合性检测。本次检测的范围主要包括：网络和通信安全、设备和计算安全、应用和数据安全及云计算安全扩展要求。

经检测，深信服云安全服务平台(等保一体机)CSSP V4.0 基本符合 GB/T 22239-XXXX《信息安全技术 网络安全等级保护基本要求-试行稿》中第三级要求中网络和通信安全、设备和计算安全、应用和数据安全以及云计算安全扩展等部分的相关要求。结果统计详见下表：

安全层面	要求	检测项	通过	部分通过	不通过	不适用
网络和通信安全	安全通用要求	33	27	3	0	3
	云计算扩展要求	19	15	2	0	2
设备和计算安全	安全通用要求	26	3	12	1	10
	云计算扩展要求	16	2	1	1	12
应用和数据安全	安全通用要求	34	16	8	6	4
	云计算扩展要求	11	9	0	1	1
合计		139	72	26	9	32

一体化安全架构在不同医院中的应用

SANGFOR 深信服科技

通用硬件

等级保护一体机

软件

访问控制
IPS
WAF
数据库审计
VPN
防病毒
APT
运维审计
漏洞扫描
安全运营服务
……

交付

三级医院：
网上诊疗服务等；

二级医院：
网上挂号、网上支付等

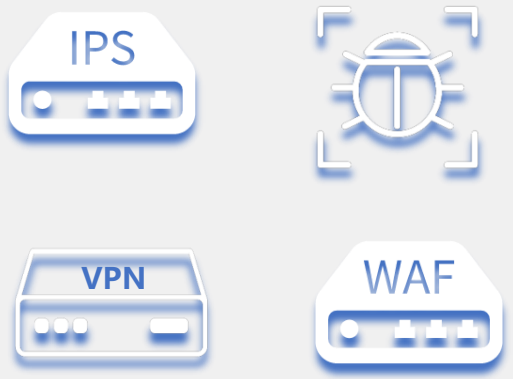
SANGFOR
深信服科技

一体化安全架构带来的价值

统一高效的管理

SANGFOR 深信服科技

硬件设备堆叠



……

安全资源化交付

- 下一代防火墙
- 安全接入
- 数据库审计

……

安全场景化交付

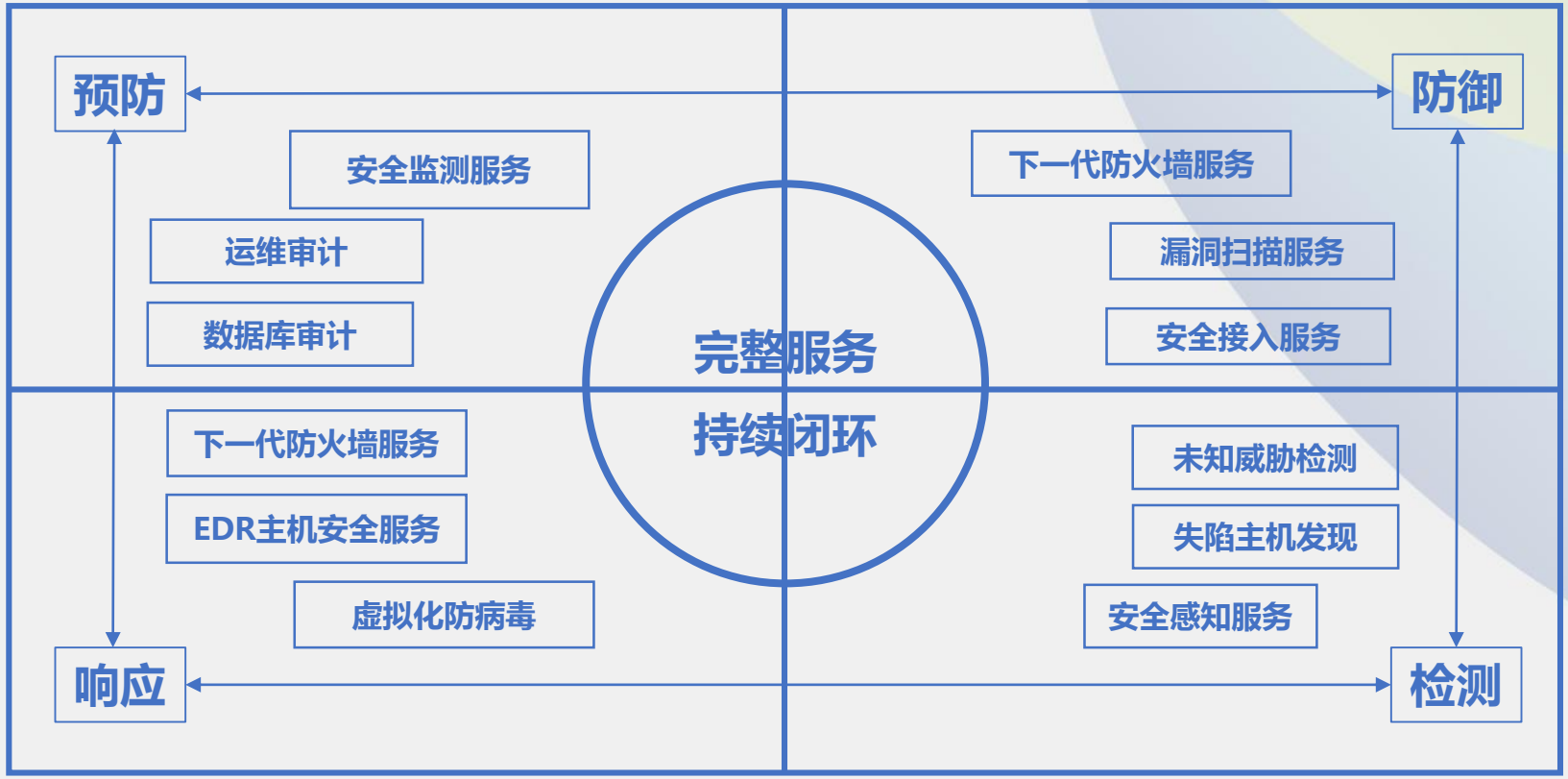
- 等级保护二、三级场景
- 勒索病毒场景
- 东西向安全隔离场景

……

向服务与场景化交付演进，安全功能组件统一管理

安全能力的持续闭环

SANGFOR 深信服科技



一体化的报表展示，安全不再割裂；

弹性扩展，随需而变

SANGFOR 深信服科技

- 硬件设备堆叠，建设复杂，周期长
- 设备割裂，运维管理复杂
- 架构固化，难以应对业务环境和政策变化

- 软件定义，快速交付
- 安全功能统一管理，减少硬件运维工作
- 组件化安全功能交付，弹性扩展，随需而变

SANGFOR
深信服科技

探讨小结

探讨小结

SANGFOR 深信服科技

价值呈现

- 有效提高IT部门及安全资源的生产力，真正发挥每一个安全产品的最大价值；

成本控制

- 极大的降低完整安全解决方案的采购成本；

安全体系

- 有效的构建了一个完整的安全防御体系；

高效管理

- 减少传统安全解决方案带来的复杂度，有效降低部署和运维的难度；

SANGFOR
深信服科技

THANK YOU

深信服科技股份有限公司