医疗

www.ruijie.com.cn

立体防护 安全可视

锐捷医疗安全解决方案

如有疑问
扫一扫在线咨询

Ruijie Networks 锐捷

方案背景

安全失陷日益突出

某医疗机构1

某医院在互联网被发现可利用的前置机入口点,前置机没有经过IPS防护，搭建socks代理进入DMZ，成功从DMZ区跳转到内网区，通过挂号服务器接口获取到部分诊疗信息，并利用struts2反序列化漏洞拿下医院Vcenter，搭建二层跳板进入内网，通过弱口令获取到数据库服务器权限并抓到域管理员哈希，通过域管理员哈希传递获取域控服务器最高管理权限。

某医疗机构2

某医院测试系统连上公网测试，存在弱口令被猜解，存在SQL注入漏洞，通过数据库提权，可以获取该医疗机构病人、收费等信息，同时通过代码审计，发现在线客服系统存在任意文件上传0day漏洞，成功获取服务器权限；发现目标系统存在越权，可以越权查看万级病历信息。

某医疗机构3

某医院在攻防演习中发现网站apache版本低，通过渗透提升系统权，限搭建多层代理跳板获取该目标系统一、目标系统二、某核心业务系统、邮件系统等权限，并通过ITSM运维监控管理平台/堡垒机可以控制数十台内网服务器系统权限。

某医疗机构4

某医院在攻防演习中发现通过渗透搭建代理跳板经由互联网→DMZ区→内网，PACS影像服务器存在弱口令，通过获取PACS核心数据库权限、查询缓存服务器权限，可实时查询近万条PACS影像数据。

某医疗机构5

某医院测试系统连上公网开展测试，时间紧，未对防火墙策略做细致调整，对内部远程桌面简单变更端口后放通，测试完毕后未关闭端口，在攻防测试中被发现：远程桌面端口存在未修复的漏洞被成功侵入，侵入方通过提权控制服务器，并将服务器作为跳板获取了内网其他服务器管理权限。

典型失陷案例	失陷主要原因分析
软件版本旧	软件组件版本低　存在低版本容易入侵
账号弱口令	弱口令有规则性　猜解过程没能监测到
搭建跳板	DMZ区策略问题　搭建反向代理进内网
人为错配置	安全策略不清晰　策略执行效果不预知
架构不合理	网络划分不合理　存在监测不到的流量
端口暴露	公网暴露端口多　端口漏洞没有被修复

方案构建目标

锐捷医疗安全解决方案，通过引入“网络+安全”的立体防护策略，实现安全可视化，降低对管理人员的精力消耗。主要体现在四个方面：

提供
精准预报

全面联动
堵疏漏

快速处置
排除风险

为客户
构建安全环境

锐捷医疗安全解决方案

安全管理中心	安全通信网络	安全区域边界	安全计算环境
大数据安全（流量+日志）	下一代防火墙	下一代防火墙（防病毒+立即邮件）	入侵检测/防御
IT运维管理	VPN	入侵检测/防御	数据库审计
堡垒机	路由器	上网行为管理	动态防御系统
漏洞扫描	交换机	安全沙箱	网页防篡改
WMS		动态防御系统	双因素认证
等保建设咨询服务		身份认证管理	漏洞风险评估（渗透+漏扫服务）
		流量探针	杀毒软件
		WEB应用防护	

建设要点

- 对安全进行统一管理与把控
- 集中分析与审计
- 定期识别漏洞与隐患

建设要点

- 构建安全的网络通信架构
- 保障信息传输安全

建设要点

- 强化安全便捷防护及入侵防护
- 优化访问控制策略

建设要点

- 强调系统及应用安全
- 加强身份签别机制与入侵防范

锐捷医疗安全解决方案参照等保要求，通过1中心3防御的架构提供网络安全设备
参照医院信息化架构内、外、设备三网规划，从网络架构层面保障医疗信息化基础架构的安全

方案价值

安全计算环境：大数据安全集成漏洞扫描，定位高危资产

支持的数据采集方式

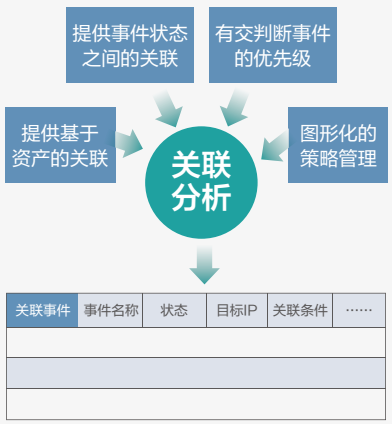
SYSLOG
SNMP Trap
WMI
SMB
数据库
文件
… …

适用场景

网站攻击
信息泄露
网页篡改
异常行为分析
带宽资源滥用
Dos、DDos攻击
钓鱼欺诈
… …

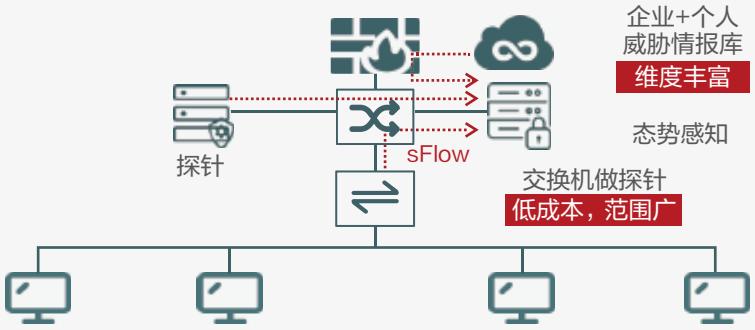
关联模型

弱口令扫描
非工作时间访问
异常登录
缓冲区溢出
SQL注入
UDP嗅探攻击
Teardrop攻击
拒绝服务攻击
端口扫描
策略变更
可疑木马端口
发现病毒事件
漏洞利用… …



设定不同关联策略，配置对应审计事件，如时间、IP地址、漏洞等，系统在关联事件中呈现给用户，用于决策。

安全计算环境：多端联动精准识别、阻断挖矿病毒，避免被通报

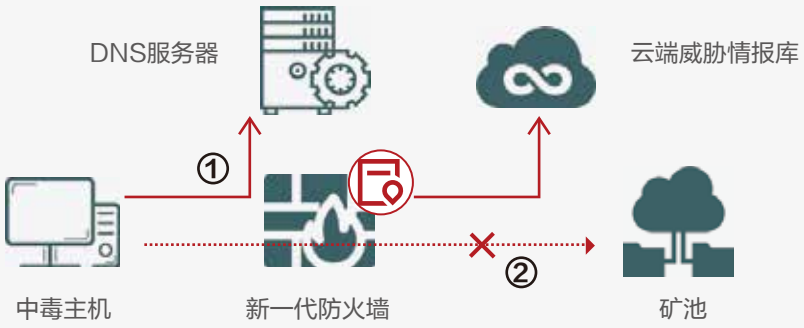


和腾讯等多家威胁情报库合作，面向**企业和个人终端的多维度情报**，结合DGA算法，**快速发现非法域名**

交换机也可以做探针，**低成本全方位识别内部传播的挖矿木马**

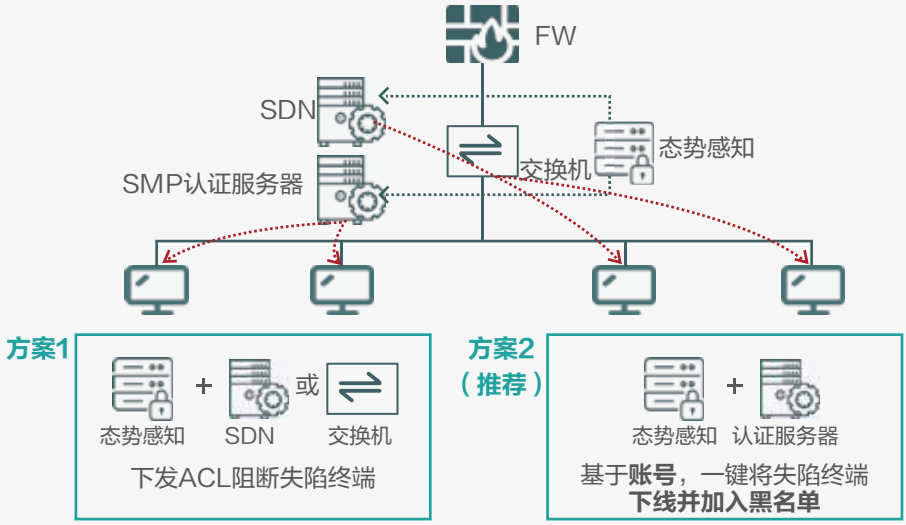
态势感知：
统一分析呈现

丰富情报+低成本交换机探针，准确识别挖矿木马



采用严格访问限制，**域名白名单**，避免被通报

2小时缩短到1秒钟，一步实名溯源



基于IP、账号的精准阻断，杜绝木马横向传播

精准识别，有效封堵

云端多情报库，变种木马及时发现
交换机变探针，及时发现内部木马
防火墙域名白名单，有效过滤木马

99%
木马识别和封堵

认证联动，实名溯源

BDS联动认证平台，一步实名

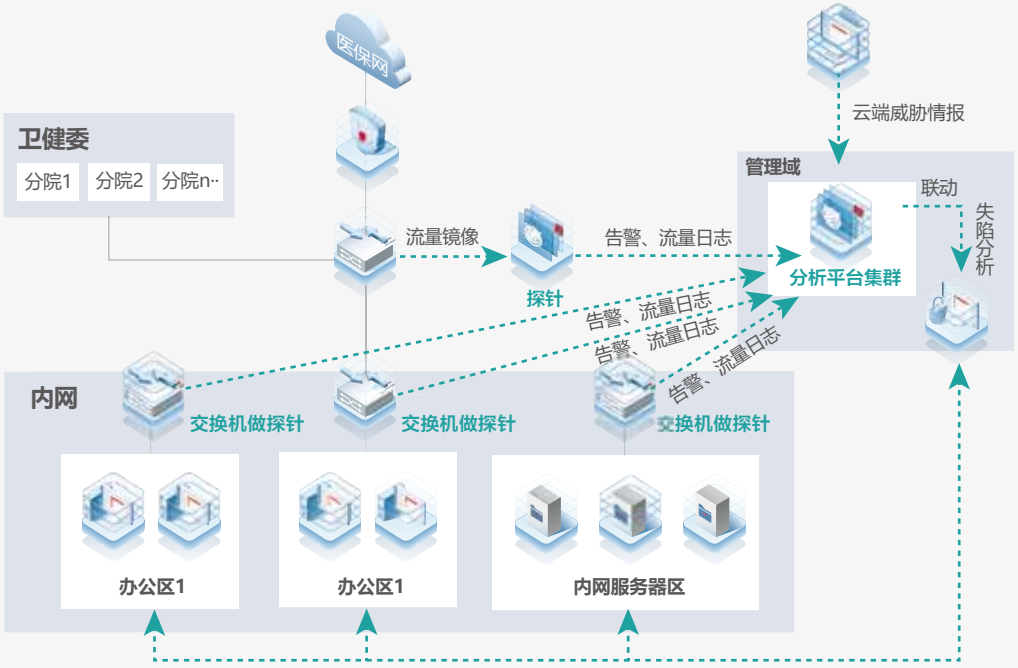
100%
效率提升

安网联动，精准阻断

BDS联合SDN、交换机，基于ACL封堵；
BDS联合认证平台，基于账号封堵；

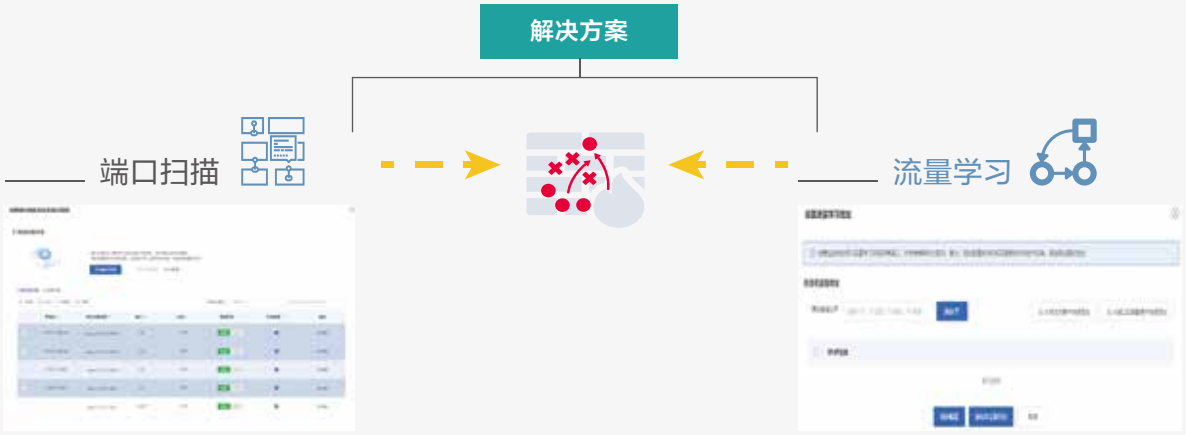
90%
横向传播降低

安全管理中心：交换机充当探针，及时发现对终端攻击的异常流量



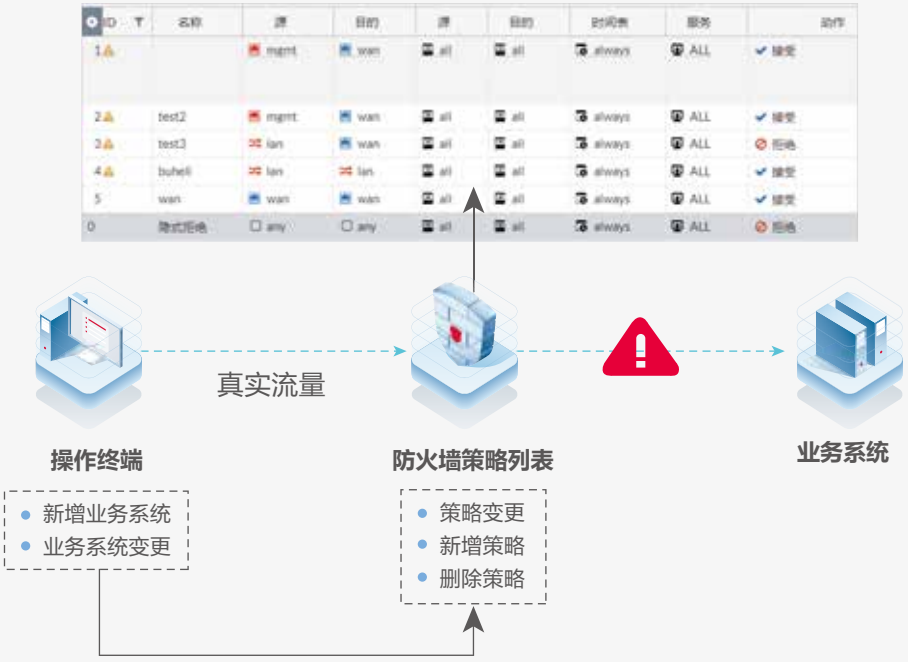
交换机做联动探针，内部异常流量无可遁形

安全区域边界：通过机器学习发现异常搭跳板行为



功能	端口扫描	流量学习
价值	2小时以上问题发现效率提升10倍以上	持续监测关键服务器的端口流量交互情况，可针对异常跳板性的流量动态配置策略。
特性	通过流量学习和端口扫描，智能推荐安全策略， 快速实现对异常流量配置安全策略。	

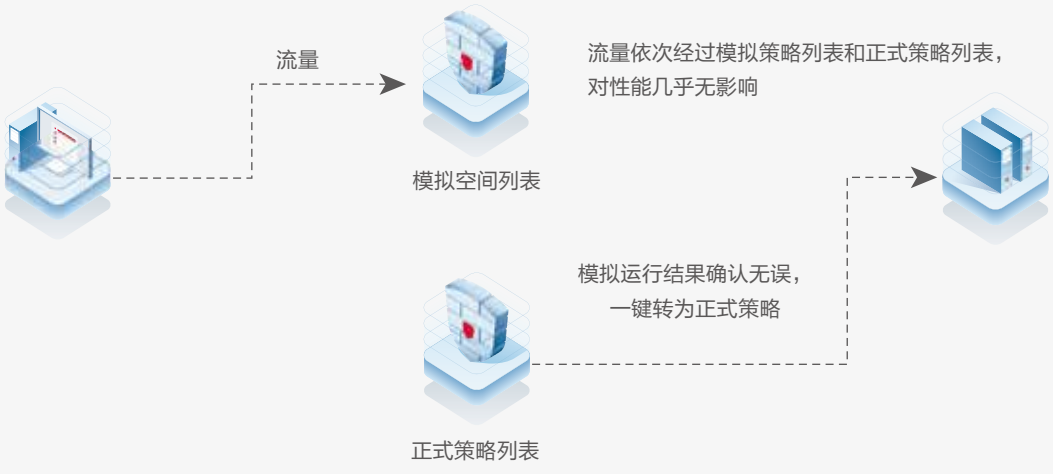
安全通信网络：策略管家，预执行策略防疏漏、错配



模拟空间

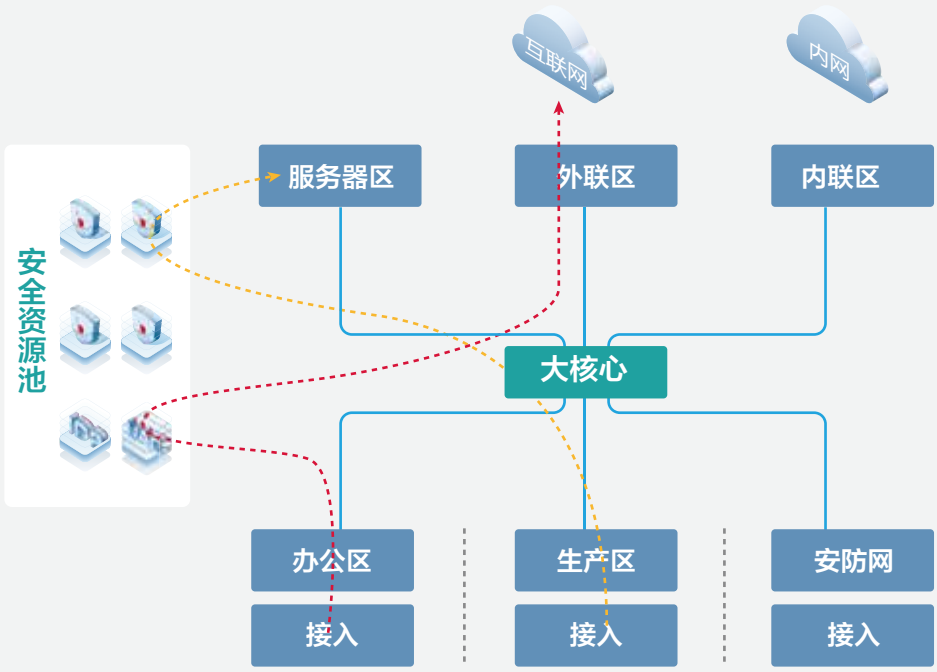
模拟运行结果

源地址	真实环境执行结果	模拟执行结果	命中次数
192.168.1.1	允许	拒绝	123
192.168.1.2	拒绝	允许	234



借助流量学习&识别，在模拟空间内执行策略，
避免因人为原因导致的断网或者攻击洼地

安全通信网络：不改变网络架构，实现流量调度安全防护



基于SDN技术
安全资源池化，流量灵活防护

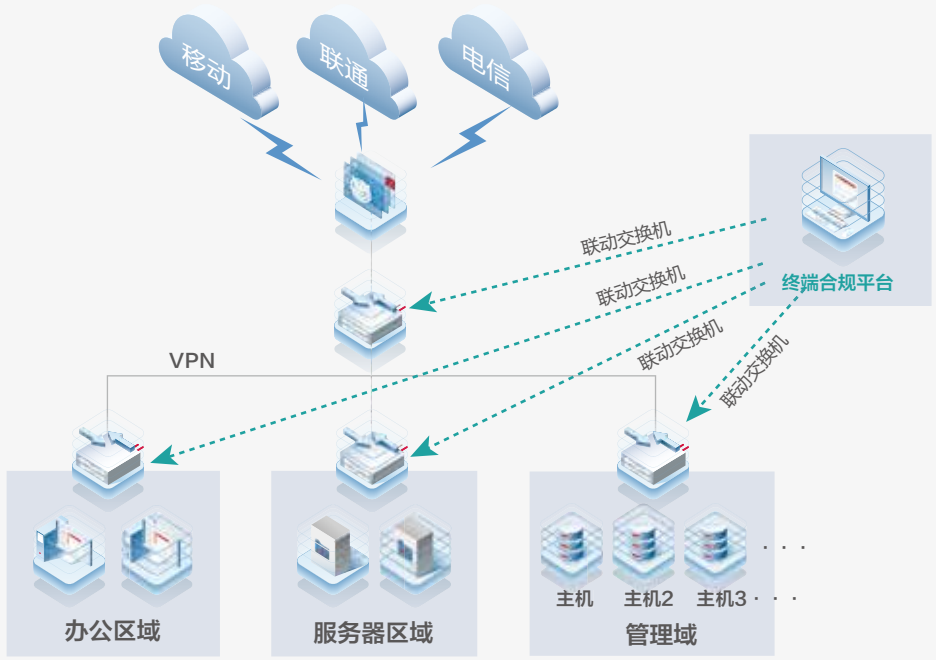
区域边界和服务区内无需直接部署物理设备，实现逻辑隔离，提高安全设备复用率

基于不同业务需求，灵活设计流量路径，分配给适当的安全设备

可进行跨厂商的安全设备冗余部署，实现负载均衡，充分满足性能需求

改变出口“糖葫芦串”式串联部署模式，使用并联方式不再存在单点故障风险

安全区域边界：免安装软件，对终端完成失陷分析



借助免客户端的终端合规平台 实现不合规的电脑自动被接入交换机阻拦强制安装插件

方案价值

产品深入融合提供精准预报

大数据安全集成漏扫，
定位高危资产

网络+安全
全面联动堵疏漏

交换机充当探针，
及时发现对终端攻击的异常流量

借助机器
学习赋能快速处置

通过机器学习，发现异常搭跳板行为
策略管家，预执行策略防疏漏、错配

创新解法
提升客户安全环境

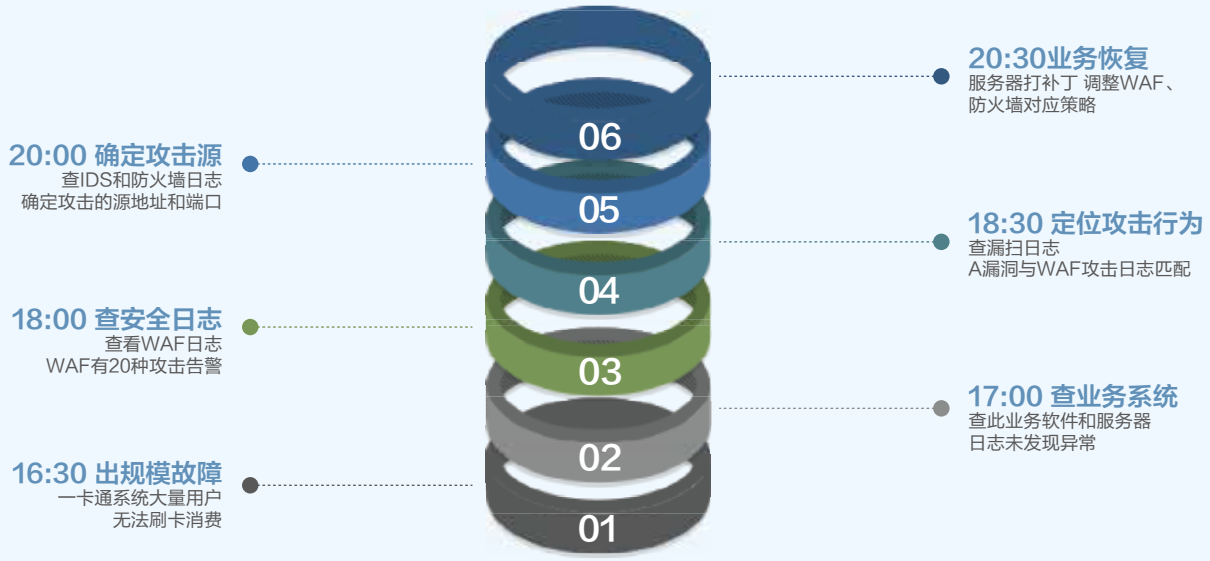
不改变网络架构，实现流量调度防护
免安装软件，对终端完成失陷分析

锐捷医疗安全方案全面防护

典型失陷案例	失陷主要原因分析	锐捷安全防护解法
软件版本旧	软件组件版本低 存在低版本容易入侵	1.大数据安全集成漏洞扫描，定位高危资产
账号弱口令	弱口令有规则性 猜解过程没能监测到	2.交换机充当探针，及时发现对终端攻击的异常流量
搭建跳板	DMZ区策略问题 搭建反向代理进内网	3.通过机器学习，发现异常搭跳板行为
人为错配置	安全策略不清晰 策略执行效果不预知	4.策略管家，预执行策略防疏漏、错配
架构不合理	网络划分不合理 存在监测不到的流量	5.不改变网络架构，实现流量调度安全防护
端口暴露	公网暴露端口多 端口漏洞没有被修复	6.免安装软件，对终端完成失陷分析

应用锐捷医院安全解决方案带来的变化

以往，常规安全事件流程耗时长



3名安全运维工程师，

百万条级的日志排查，4小时业务中断

现在，锐捷立体安全协防耗时短

1名工程师，实时问题预警和定位，
预警处理排除风险，或业务中断分钟级恢复

应用案例

客户介绍

复旦大学附属华山医院创建于1907年，是国家卫生计生委委属医院、复旦大学附属教学医院和中国红十字会冠名的医院，1992年首批通过国家三级甲等医院评审，为全国文明单位，是国内最著名、最具国际化特征的医教研中心之一，也是全国首家通过JCI认证的部属公立医院，在国内外享有很高声誉。

客户需求

- 完成等级保护建设；
- 通过医院信息安全评估。

解决方案

使用锐捷全线安全产品按照等级保护三级标准进行安全改造，取得全市三甲医院第四名的好成绩，为后续等级保护测评工作打好基础。

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818