

内外防护 网安联动

锐捷医疗安全一体化防护解决方案

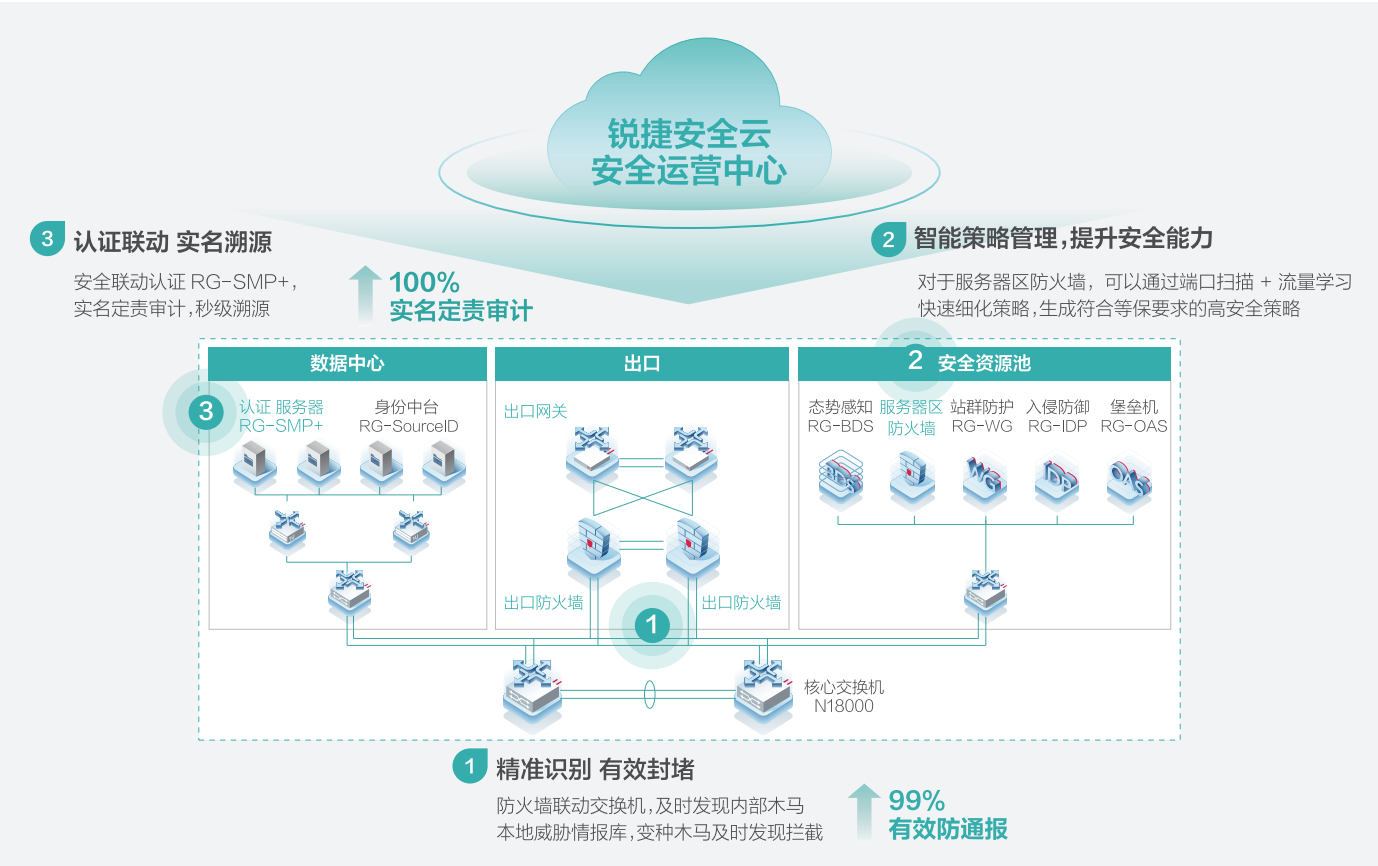


医院安全建设现状及挑战分析



锐捷医疗安全一体化防护方案设计

网络+安全联动3.0



锐捷医疗安全一体化防护方案价值

防通报

出口威胁防外溢，
有效防止被网安部门通报

快溯源

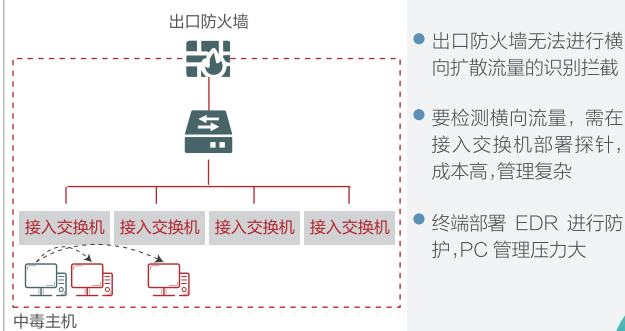
防火墙与 SMP+ 认证服务器联动，
安全事件与用户信息自动化关联，溯
源效率高

优策略

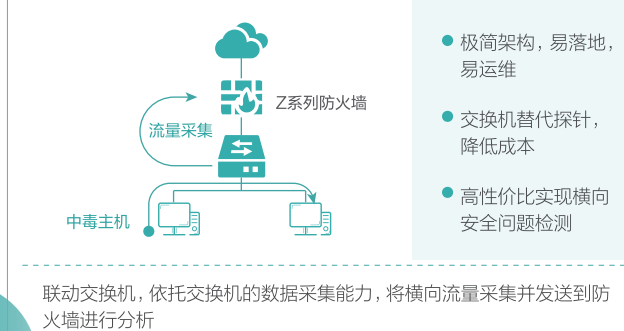
通过端口扫描+流量学习快速细化策略
生成符合等保要求的高安全策略，实实
在在提升安全能力

防通报：横、纵向威胁精准防御

传统方案缺少横向风险检测手段

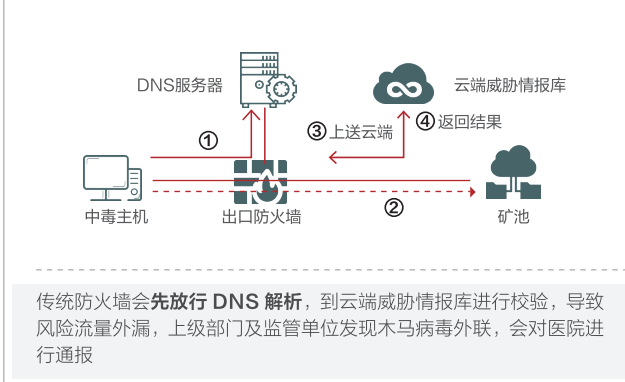


新方案：联动交换，实现横向风险检测

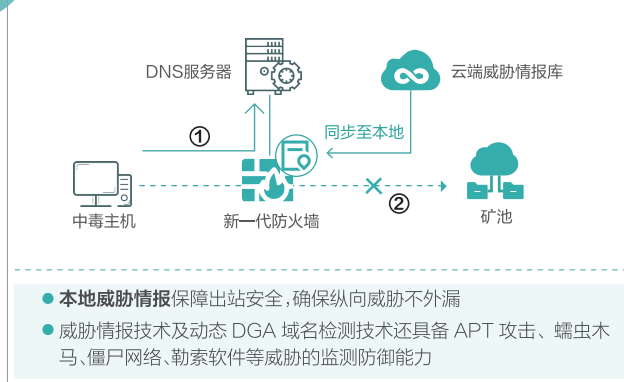


VS

传统防火墙难以避免纵向安全外溢



新方案：边缘威胁情报本保障出站安全



防通报：多源+共享情报，覆盖全、检测准、阻断快

边缘设备威胁检测代价大，恶意流量难阻断



IPS/AV 库拦截

加密流量无法监测
新型攻击无能为力
IPS 拦截相比情报效率低消耗大



矿池 DNS 变化快

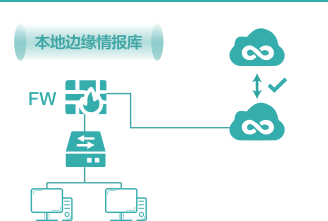
矿池 DNS 变化快，需要丰富的威胁情报库



部分木马直接使用 IP 传输

部分木马直接使用 IP 传输，传统方式难检测，内部传播难发现

新方案：多源情报



本地边缘情报库

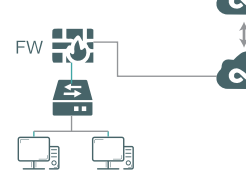
FW

安恒信息 腾讯安全

Ruijie 锐捷 更多厂商

● 安恒、腾讯、锐捷等多源情报提升拦截率，上级情报保持一致，防通报

传统方案



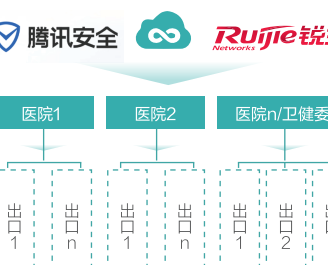
上级情报
与上级情报库不一致，易被通报

通用行业库
行业特性威胁通用情报难覆盖，如某些场景存在 10% 以上挖矿等威胁无法检测

情报难同步
组织内威胁情报难及时同步
行业客户之间情报难共享

VS

新方案：共享情报



腾讯安全 锐捷

医院1 医院2 医院n/卫健委

出口1 出口2 出口3

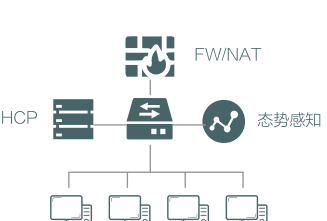
- 腾讯锐捷独家合作，针对行业特性数据生成情报，覆盖率提升 10%+
- 组织内部发现威胁，情报及时同步，全面防御
- 构建行业联盟，共享知名情报，共建网络安全生态

溯源定责到人：认证联动，自动化溯源，高效省时省力

传统方案

日常安全运营过程中

- 被通报难以及时溯源无法交代
- 发现可以威胁溯源困难，难以保障业务安全



自动化联动溯源



认证对接同步用户信息

安全事件与用户信息自动化关联



- 配合 BDS/BDS 集群支持实现海量安全告警日志依法留存与快查到人
- 与 SMP+ 对接后续版本支持

更多第三方认证系统对接

1 收到通告信息或发现可疑威胁

外网 IP 和时间点

2 查询防火墙 / 探针 / IDP 等多系统的安全日志和 NAT 日志

内网 IP 和时间点

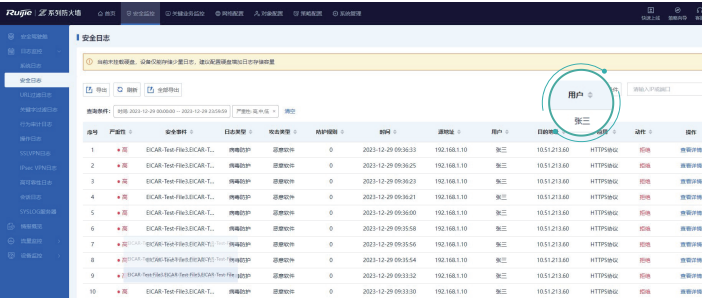
3 查询认证系统日志

4 失陷 IP 对应的实名信息

1 1 个告警 10 分钟，每天几十个告警，需要查 2 小时，费时费力

DHCP 环境下终端不断变换地址，告警信息翻倍

2 各产品日志时间不一致，造成难以查询



序号	产品	安全事件	日志类型	发生时间	持续时间	源IP	源端口	用户	目标IP	目标端口	动作	操作
1	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:23	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
2	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:25	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
3	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:27	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
4	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:29	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
5	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:30	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
6	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:35	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
7	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:36:56	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
8	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:35:54	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
9	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:33:32	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情
10	锐捷	ECAR-Test-Firewall-ECAR-T...	连接超时	2023-12-29 09:33:30	0	192.168.1.10	80	张三	10.51.213.60	HTTP/80	成功	查看详情

锐捷 Z 系列全新下一代防火墙
一键实名溯源，2 小时 缩短到 1 秒钟

多系统联动代价大，查询繁琐，费时费力

智能策略管理

只需两步生成高安全策略



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

*本资料产品图片及技术数据仅供参考，如有更新恕不另行通知，具体内容解释权归锐捷网络所有。