SANGFOR
深信服科技

医院零信任解决方案及案例

行业现状

随着云计算、物联网、大数据、移动互联网等技术发展，基于物理边界的防护无法满足要求，进入内网不等于安全和可信。疫情期间远程办公规模化、常态化，终端环境复杂、接入访问行为不可控，也更加让医院面临更大的威胁。如何在不安全的网络环境中构建安全的访问体系，是医院当下的主要建设目标。

建设挑战

账号存在风险，管理与用户体验差

许多用户的账号往往采用默认密码 / 弱密码，业务系统等管理台也存在缺省账号、默认密码、弱密码等情况，并且存在长期不更新密码、定期修改密码的要求难以落地的情况。

接入终端安全不可控

医院除统采固定终端外，还存在大量的 BYOD 终端（携带个人的设备办公），并且存在大量终端无法加入域控环境，院方很难集中对终端进行集中管理，导致终端软件无法统一下发安装，终端安全状况良莠不齐。当终端可以同时访问内网与互联网时，容易出现因钓鱼邮件、远控木马以终端为跳板，对业务造成危害。

访问权限难管理

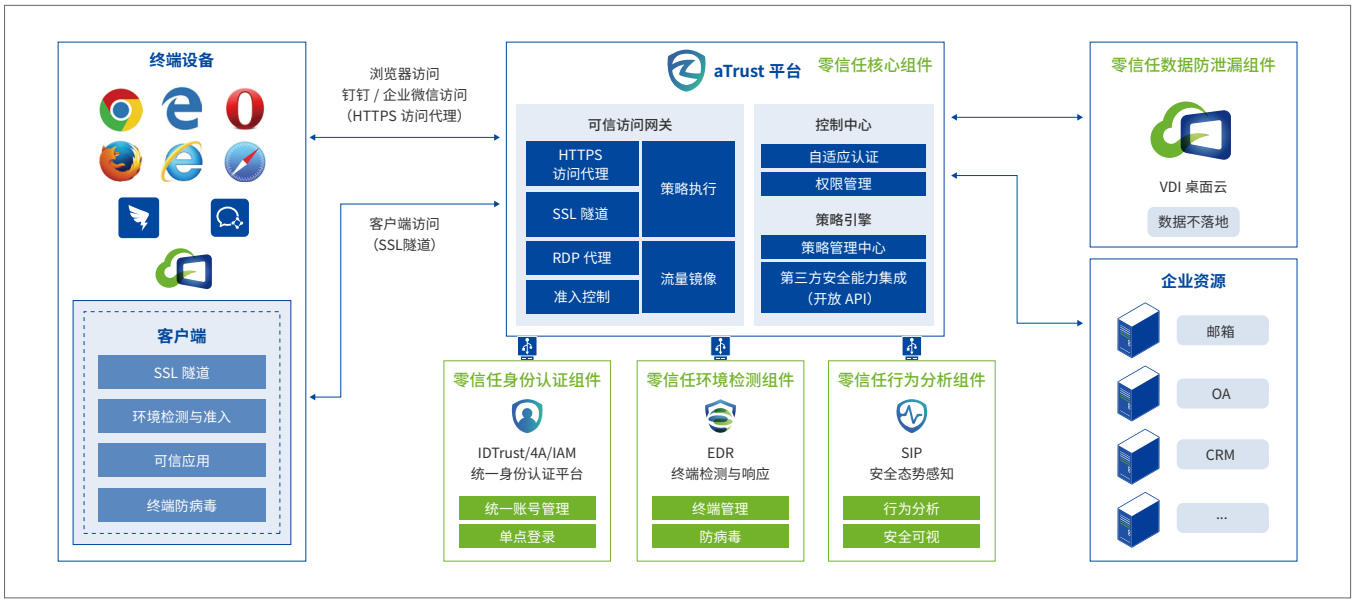
随着笔记本等移动终端的快速普及使用，传统划分网络隔离的方式或基于 IP 的访问控制权限会限制生产力，降低办公效率，很多企业往往会放松针对访问控制权限的管理。另外，网络层面的访问权限相对固化，无法结合实际情况进行调整。

访问行为不可视，可疑行为难追溯

不能及时发现接入终端的异常行为，并且不能及时做出对风险终端的处置，无法应对社工等攻击行为，风险终端的接入可能会导致内网业务遭到攻击和扫描，并且无法对这类终端进行有效处置。

SANGFOR
深信服科技

深信服建设方案



深信服零信任安全办公解决方案基于零信任理念的 SDP 架构，以 aTrust 平台为核心组件，整合终端安全监测与终端防横向、统一身份管理与认证、行为分析、数据防泄密等能力，整体实现全方位立体的业务安全访问体系。具体构成为：深信服零信任访问控制系统 aTrust 是整个系统的大脑，并与其他组件对接，由安全代理网关和控制中心两部分构成，实现控制面和数据面的分离。

- 控制中心负责认证、授权、策略管理与下发，是整体的调度与管理中心，对接入的身份、终端、环境、行为进行信任评估。基于策略引擎配置的策略结果，决定允许或拒绝会话并让可信网关进行放通或阻断。
- 内置 UEM 数据沙箱，保障接入时的终端数据安全。
- 安全代理网关支持 HTTPS 代理访问和 SSL 隧道代理访问。
- 控制中心和安全代理网关均受 SPA 单包授权技术对设备本身的服务进行隐身保护。

方案优势

建立集中式平台化管理体系，简化运维

- 基于统一平台进行账号管理，通过组织架构、用户组、角色、用户等多种方式灵活定义权限。随着用户角色发生变动，能够实现权限的相应变化，并且与当前的流程系统对接，自动完成身份与权限的匹配操作。
- 零信任通过对终端、资产进行梳理与管理，在零信任落地过程中，能够有效监测终端安全状况，实现威胁处置闭环；并且结合发现的资产逐步扩展零信任的覆盖范围。
- 当用户访问业务发生状况时，用户可自助检测原因，管理员也可以直接从后台收集日志，降低沟通成本。

显著改善医院员工体验，释放生产力

- 通过零信任安全办公方案的建设，为内外网用户提供一致性认证与接入体验，随时随地快速稳定地访问业务。
- 用户不再需要记忆复杂的账号密码并且定期修改，只需通过扫码、短信等方法认证一次（安全要求高需要进行增强认证）即可访问所有的有权限访问业务，无需重复认证。
- 医院可以放心地将业务提供给外包、供应商等上下游使用。用户无需在认证、故障报修、卡顿、权限申请等 IT 事务中花费太多时间，大幅释放办公生产力。

SANGFOR
深信服科技

精选案例——南充市中心医院（川北医学院第二临床医学院）

医院简介

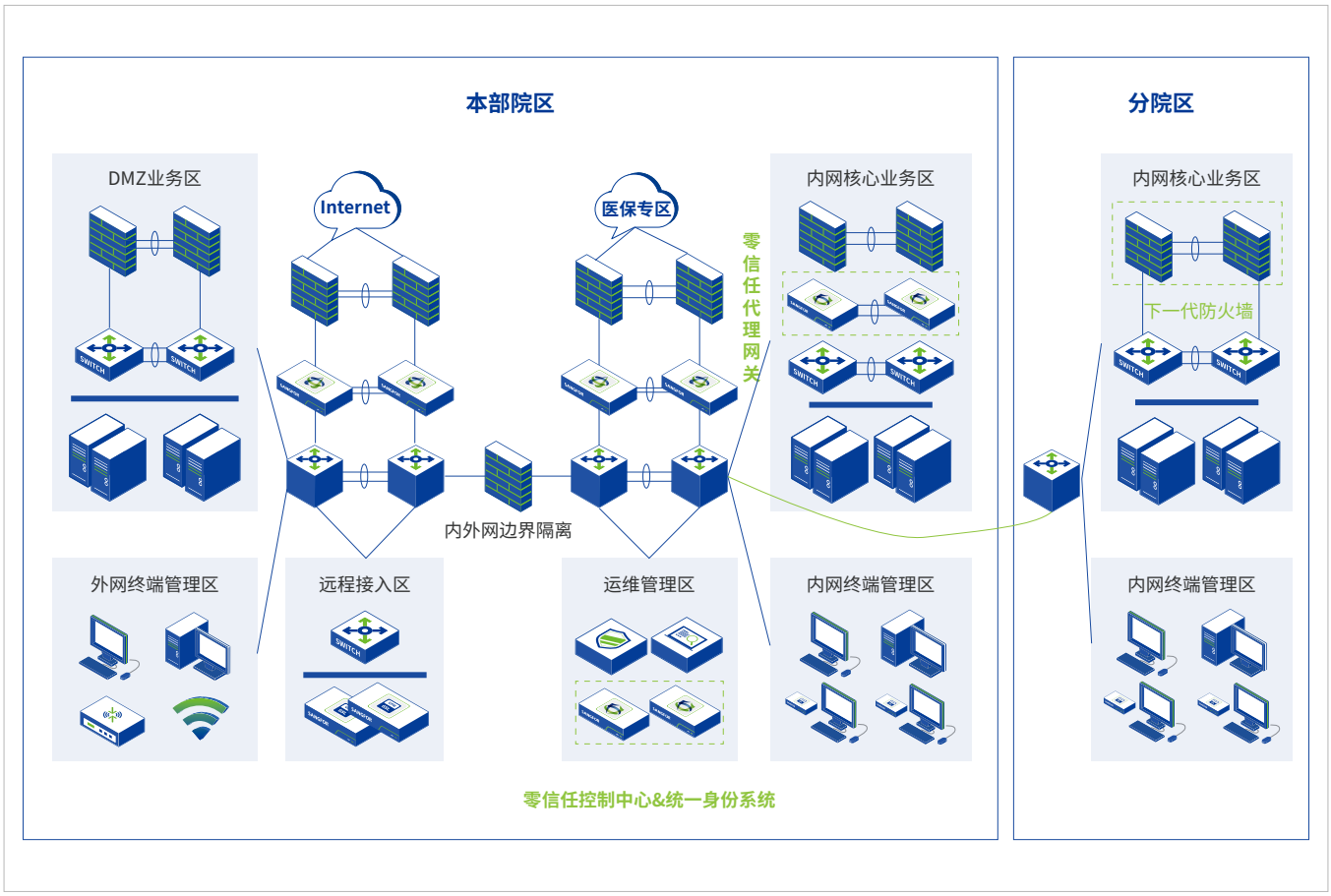
南充市中心医院由原国家副主席张澜先生于 1937 年创建，现为集医疗急救、科研教学、康复保健为一体的国家三级甲等综合医院，是川北医学院第二临床医学院，及西南医科大学等高校的临床教学医院，是国家卫健委临床药师培训基地、国际爱婴医院、中国航天员救治医院、全国脑卒中筛查基地、全国健康管理示范基地。

建设挑战

医院目前有 30 多套业务系统，100 多个子系统。出于安全考虑，要求强密码验证，但因密码较为复杂，医务人员相对比较缺乏安全意识，为方便工作，大部分都在使用弱密码，导致安全风险增加。

医院内外网之前是物理隔离，由于“互联网 + 医疗健康”的推行，医院很多业务也开始面向公众开放，患者通过移动设备无线接入即可在线挂号，与内网业务进行数据交换；驻场外包、运维人员使用第三方设备通过互联网接入医院核心系统；越来越多的自助设备也需要连入医院内网。人员复杂、设备繁多，管理不便，造成内网业务的暴露面扩大，存在严重的安全隐患。

建设方案



通过在医院 HIS/LIS 等业务前端后部署零信任网关，所有来自医务人员、患者以及第三方运维人员的访问请求都可以用零信任网关进行代理，原有多个暴露口的业务直接收敛到一个零信任的入口，业务系统的漏洞、IP、端口等信息都被隐藏起来。同时零信任的 SPA 单包授权技术还能够隐藏零信任网关自身暴露面，现在未授信的终端设备无法与零信任网关发起连接，真正做到安全可信。

用户收益

通过构建零信任体系，医院能有效规避因账号失窃、账号共享、弱密码、爆破等原因对业务造成的风险，并且从面对“灰流量”不敢阻断到“有效灰度”处置。业务被零信任收缩在内网，并且用户被分配最小业务访问权限，最小化业务的暴露面，尽可能规避因内外部威胁对业务造成的损害。针对医院用户认证与访问业务的过程进行全面安全监测，以便能及时处置，保障医院业务的正常开展。

更多案例

客户名称	级别	客户名称	级别
中国医学科学院北京协和医院	三甲医院	河北医科大学第一医院	三甲医院
四川大学华西医院	三甲医院	复旦大学附属华山医院	三甲医院
上海交通大学医学院附属瑞金医院	三甲医院	浙江大学医学院附属第一医院	三甲医院
复旦大学附属中山医院	三甲医院	.....	.....