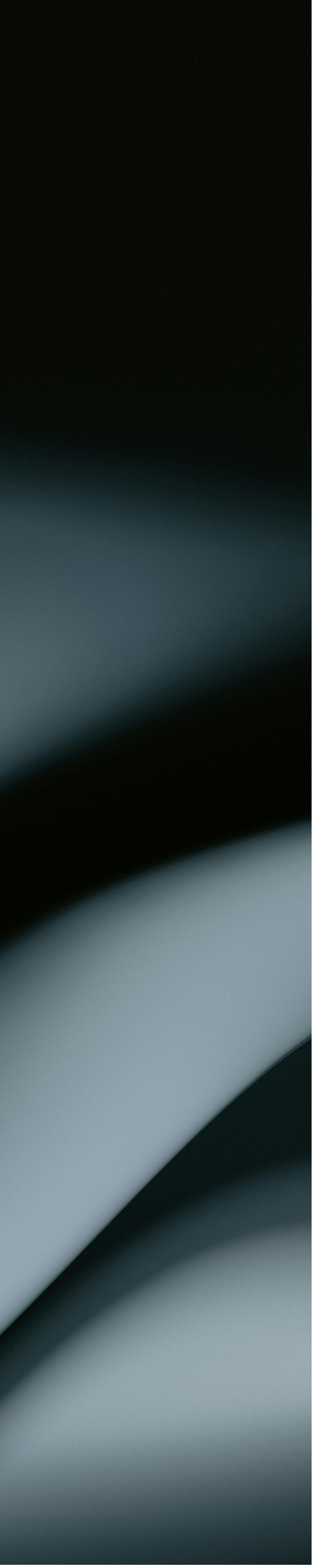
NSecsoft
安在软件

医疗行业

企业数据防泄漏&终端安全管理解决方案



目录

01

项目背景

医疗行业经过十几年的信息化发展，积累了大量的数字信息，这些信息不仅记录着大量的医疗案例记录着大量的患者隐私信息，以及内部重要财务、采购等重要数据。健康医疗数据一旦发生外泄不仅涉及到个人层面，也涉及到公共利益，甚至是国家安全。经相关数据分析，医疗行业是所有行业中唯一一个内部威胁大于外部威胁的行业。

此外，医疗机构面临终端数量大，分布广，终端运维困难，软硬件资产信息统计困难等问题。网络安全法、等保2.0、医院信息化建设标准下医疗数据安全合规问题促使医疗机构应建立完善的终端数据安全管控体系，确保终端系统安全及内部数据安全。
医疗行业等保的要求：

2011年，根据国家卫健委《指导意见》，三级医院重要业务系统必须达到等保三级，二级医院必须通过等保二级测评。

2016年，国家卫健委规定，重要业务系统必须达到等保三级标准才满足三级医院评审标准中对于网络安全的要求。

2018年，国家卫健委规定健康医疗大数据的平台必须通过等级保护，一般引入大数据技术的医院都是三级甲等医院，基本以三级等保为主。

2018年，国家卫健委《互联网医院管理办法（试行）》规定，承载互联网医院的平台必须通过等保三级测评。

02

面临问题

医疗信息外泄

- 病人信息、用药信息被随意打印及外泄
- 内部机密信息通过U盘或其他外部设备被带离医院
- 内部机密信息通过E-mail、聊天工具等方式外泄
- 非授权人员通过合法账号登录HIS窃取机密数据

系统运维繁琐

- 软硬件资产庞大统计困难
- 软、硬件资产变化更是全然不知
- 软件和补丁无法统一部署、安装
- 管理员东奔西跑处理终端故障

工作效率低下

- 无节制的非法网站访问，增加安全威胁
- 工作时炒股、聊天、游戏等，因分散注意力导致医疗纠纷
- P2P下载等应用堵塞网络，影响HIS等业务系统的运行

03

需求分析

面对几近失控的终端安全管理现状，针对医院的终端安全管理我们需要对以下几方面进行思考。

- 如何达到等保的要求?
- 如何确保医疗信息的数据安全?
- 如何实现医院终端的人性化管理?
- 如何规范职工的桌面行为，提高工作效率?

鉴于上述各医院终端系统安全管理难点，医院需要建立一套完善的终端安全防护系统，保护企业正常业务的运行、以及对核心资产的防护。

- 规范员工办公行为，对员工上网行为、文件操作等建立严格的管控措施。
- 细粒度管控外接设备的使用，记录设备插拔，文档拷贝。
- 划分U盘等移动存储设备使用权限，保证U盘使用安全，提高工作效率。
- 需监控终端资产使用情况，实时获取变更信息，保证系统资产安全。
- 软件需统一分发部署，禁止违规软件下载安装及使用。
- 系统关键配置管控与实时告警。
- 终端故障需求快速响应，远程协助。

04

解决方案

4.1方案概述

- Ping32终端安全管理系统软件（以下简称“Ping32”）基于企业内网信息安全建设管理需求，通过多模块一体化管理方案，通过上网行为管理、文档安全管控、外接设备管控、软件管理、系统安全、远程运维等功能模块，提供细粒度的管控策略。通过对医院网络环境的了解，医院一般分为医疗内网、办公网络等网络环境，因此解决方案将从两种办公环境进行针对性解决。

4.2 医疗内网终端管理

外接设备管控

移动存储等外接设备在为日常办公带来便利的同时，也引入了很多安全问题，如：传播病毒木马，增加泄密风险等。

- 未知U盘可以随意接入终端，存在病毒感染风险。
- 智能手机、蓝牙、USB接口无法有效管控，设备随意接入。

移动存储管控

- Ping32对员工U盘授权管理，确保只有经过认证的U盘才能接入终端，区分授权与未授权U盘的使用权限。设置未授权U盘只读或禁止使用。

U盘授权

移动存储加密

- 文Ping32将内部U盘制作成加密盘，实现U盘仅限于内部使用，在未客户端电脑无法识别，防止U盘丢失、外带泄密。 通过密钥管理，将加密盘密钥下发到不同终端，加密盘只能在特定客户端打开实现内部专盘专用。

移动存储审计

- 审计终端普通U盘、授权U盘、加密盘的插拔；记录文档的拷入拷出，以及U盘内部文件的操作记录。

设备管理

针对不同外接设备做细粒度的权限划分，规范设备使用，杜绝非法设备接入。

- 严格管控智能手机、光驱等存储设备的接入，防止企业内部数据流出。
- 管理通讯设备、便携WIFI、外接网卡等设备，防止非法外联带来的数据安全风险
- 禁用除键盘鼠标之外的所有USB设备，保证正常办公的同时，确保终端安全。防止未知设备带来的安全风险。

打印安全

- 为了防止医疗信息电子文档以纸质形式输出导致的泄密事件，我们需要对医院的打印设备进行安全管控。

打印审计

- 详细记录终端打印信息，包括打印标题、时间、页数、内容等信息，同时支持打印内容快照对打印的内容查看。

打印管控

- 根据员工所在的部门不同通过设置敏感词限重要文件的打印或者是禁止员工的打印权限。打印出的文件自动置入对应该终端的水印。

系统访问监控

- 通过屏幕监控对用户访问业务系统的行为进行追溯。
- 访问业务系统时（HIS等），对行为进行屏幕录像，确保事后可追溯。
- 通过实时屏幕实时监控用户操作。

4.3医院办公网终端管理

上网行为管理

- Ping32的上网行为管理可以帮助用户控制和管理对互联网的使用，确保互联网的使用安全合规。包含：即时通讯监管、网页访问过滤、电子邮件监管、用户行为分析等功能。此外，Ping32率先支持HTTPS/SSL加密协议的上网行为管理。

网站访问管控

- 审计终端网站访问行为，对Chrome、IE全系列浏览器的网站访问行为进行监控、拦截，通过网站访问白名单控制只允许员工访问特定网址。

- 网站访问黑名单、访问敏感词拦截，阻断违规网站的访问权限，一旦访问违规网站支持自动跳转至指定网址。

邮件安全

- Ping32可以审计邮件正文、收发件人、附件等内容的，并且是业内唯一一家支持HTTPS加密协议的邮件审计厂商。同时，Ping32还可以提供收发邮件的白名单功能，防止邮件的超范围发送；分析邮件内容，发现“身份证账号、手机号”等敏感信息时自动拦截邮件的发送，保护数据的安全。

终端准入

- 对接入医院网络终端的合法性检测是等保中要求必须实现的一点，通过Ping32准入控制可实现非法终端禁止访问公司内外网资源，并且可对终端进行杀毒软件、补丁、服务、应用程序的安全状态检测，对于不合规终端自动进入隔离区，待其达到合规监测后再放行，确保所有终端安全可控。

软件合规管理

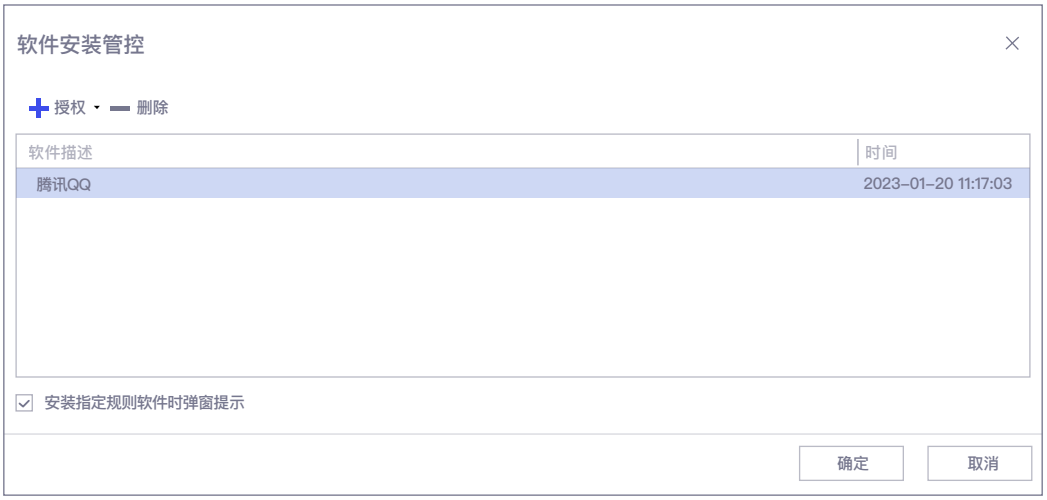
- 由于医院办公网具备互联网访问权限，因此相关人员可随意从互联网下载各类软件，从而引起软件合规问题。
- Ping32可以加强计算机软件的使用管理，规范使用具有版权和知识产权的计算机软件，保护企业软件和信息的完整性，应用软件统一管理，使终端计算机最大限度满足企业办公场景需求，提升工作效率，预防病毒与各种恶意软件的入侵。
- 软件合规管理遵循从软件安装源、软件安装权限、软件运行管理、软件统计、软件卸载等方面进行全方位合理的管控，保证企业终端的软件完全合规。

软件商店

- 终端用户可通过软件商店安装、升级应用程序，确保软件来源安全可靠、符合企业软件标准化管理需求

软件安装管控

- 完全阻断终端安装、卸载软件的权限，预设软件安装白名单，只有经过管理员允许的软件才可以进行安装，对已安装的软件可以远程卸载，从根源上杜绝违规软件的使用。

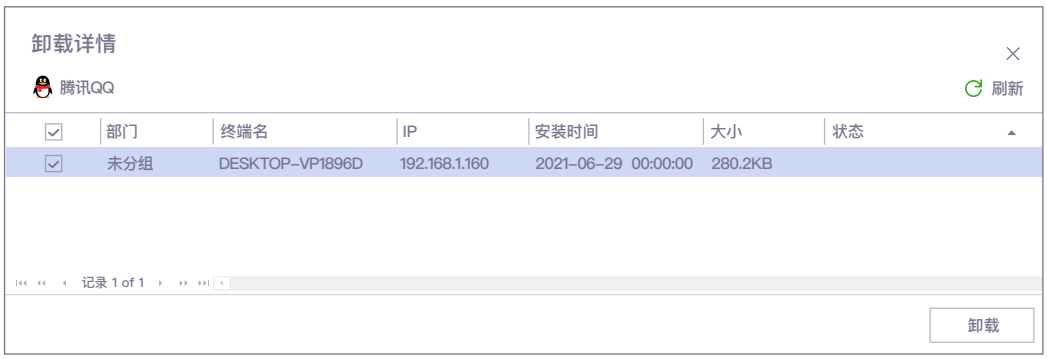


软件安装管控

软件使用管控

- 管理员可一键禁止非法软件的运行，并且软件黑名单支持多种特征匹配方式，比如进程名、窗口名以及哈希值等。

- 同时可以对已安装的软件可以远程卸载，从根源上杜绝违规软件的使用。



软件违规卸载

4.4全网管控

由于医院终端数量庞大，难以对IT软硬件资产有一个很清楚的了解。并且对医院IT部门来说每天有大量的时间用在终端运维工作中，导致工作效率相对低下，这时我们需要专业的运维工具来降低运维压力，提高运维效率。

资产管理

- Ping32的资产统计管理可以帮您更加快速、便捷地梳理企业内部的资产分布。显著提高企业资产统计、管理效率，简化IT运维工作，防范资产流失风险。

- 实时检测软件安装卸载行为、硬件插拔变更行为，资产变更告警可以第一时间帮您发现违规资产以及避免资产流失的风险。

高效运维

- Ping32提供了众多高效的运维工具协助医院IT管理人员进行运维工作。

高效运维

05

方案优势

- 通过方案实施实现医院终端和规划管理。
- 完全私有的部署模式，无须借助任何第三方服务，确保你的数据安全可控。
- 细粒度权限设置，精细化员工对核心数据的使用权限，在不影响工作效率前提下，提高终端系统安全。
- 统一规范桌面行为，确保终端安全运行。
- 统一终端运维管理，提高IT人员工作效率。
- 规范终端上网行为，实现随时溯源。

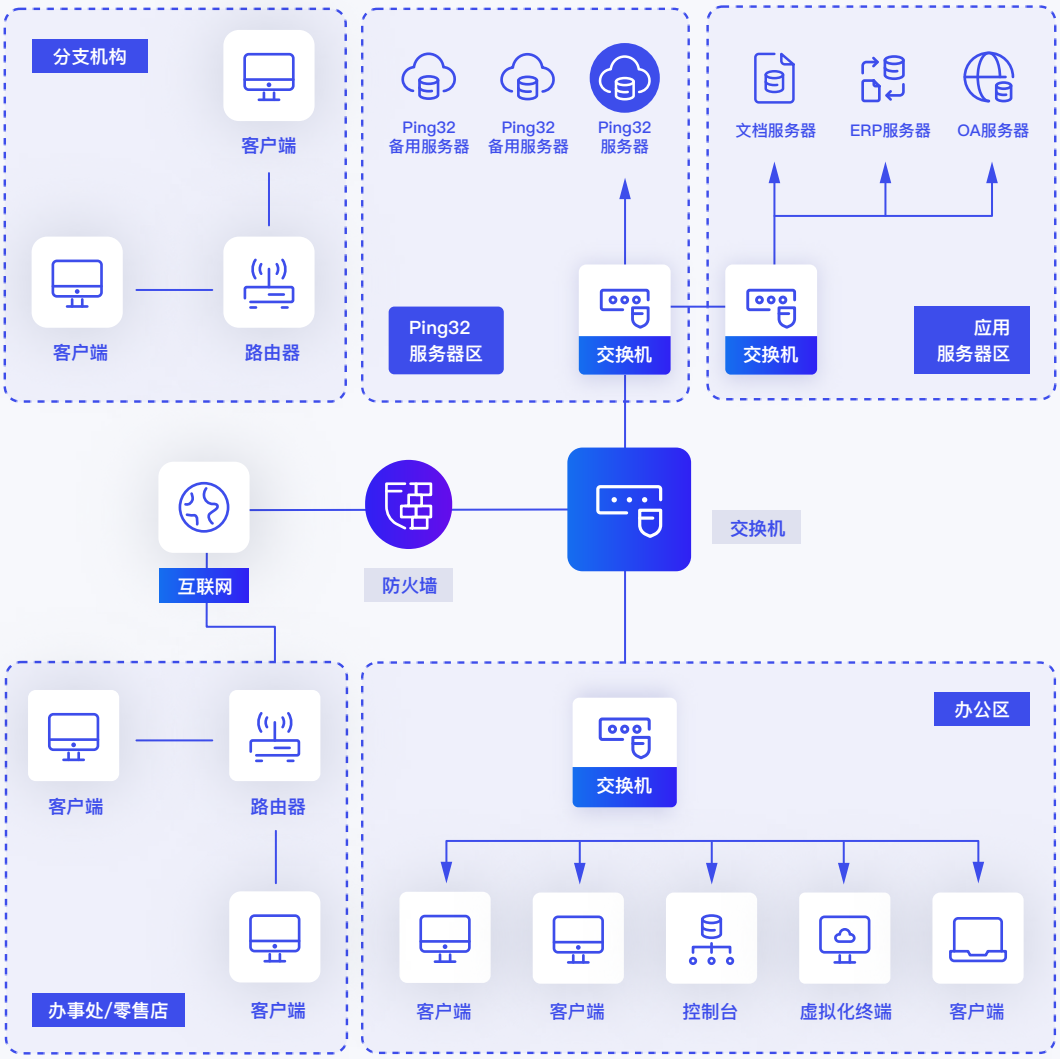
06

系统架构

Ping32是基于C/S架构设计，系统主要由三个模块组成，客户端模块、服务器模块和控制台模块。

- **客户端：**安装在被管控的计算机上，执行管理者设定的管控策略，采集计算机运行的各项数据并上传给服务器。
- **控制台：**供网络管理员、企业负责人用来管理终端计算机，审计操作使用。管理者通过控制台设置管理策略，查看日志和各项统计信息。控制台操作界面简洁易用，支持多个管理员登录。
- **服务器：**安装在系统内的一部高性能计算机上。存储系统的管理策略和客户端上报的数据，向客户端计算机下发管理策略。

系统架构图



公司简介

山东安在信息技术股份有限公司成立于2014年，是一家以研发信息安全类产品及提供相关服务为主营业务的技术驱动型公司。是中国领先的、拥有完全自主知识产权的信息安全产品和服务解决方案专业提供商。

安在软件自主研发的Ping32终端安全管理系统，构建了全生命周期的一站式信息安全产品与整体解决方案平台，包括文档透明加密、办公行为审计、操作管控、敏感内容识别、终端系统安全、运维管理等功能，有效防护由于不正当的办公行为造成的数据泄漏。

Ping32凭借优异的信息安全管理方案以及良好的用户体验受到广泛好评。被广泛应用于政府、金融、军工、运行商、制造、能源、教育、医疗等行业的大型知名单位和机构，涵盖衣食住行各行各业，为国内10000多家用户，超过200万台终端提供安全保障。

400-098-7607
nsecsoft.com

济南
高新区经十路7000号汉峪金谷
互联网大厦12层

support@nsecsoft.com

NSecsoft 安在软件