医疗
行业解决方案

联软科技
LEAGSOFT

深圳市联软科技股份有限公司

- 企业端点安全领导者 -

覆盖云、边、端多场景的平台级网络安全解决方案

持续20年技术创新始终专注于企业级网络安全管控领域

联软ESPP企业安全检测保护平台

联软市场地位

世界500强：20+家 中国 500强：100+家	政府 近400家	银行/证券/保险 近1000家	医疗 超700家	高端制造 超600家

15,000,000+	国家主管部门认可	持续领先	合作典范
企业级安全开放市场领先 安全管控终端数量 超过 15,000,000+	中国电子政务外网 “一机两用”标准起草单位 中央网信办直属基金投资单位 与央企共创跨境数据家全并落地	金融行业市场占有率继续领先 21家全国性银行：15家 证券交易所：100% 证券行业市场率占比70%	中国排名前10医院6家选择联软 近半高科技知名品牌选择联软

医院内网终端安全一体化解决方案

需求来源

政策需求：基于《网络安全等级保护2.0》及《全国医院信息化建设标准与规范》等安全合规要求，医院信息化安全建设及运维工作中重点关注医院终端的网络边界接入控制、终端安全加固与桌面运维管理。

业务场景：在医院网络中，针对桌面终端、移动终端和哑终端的接入控制、身份管理、合规检查等要求，需要切实落地；基于医院实际运维压力，面对防止病毒扩展、应急补丁、远程管理、桌面水印等需求，必须得到拓展解决。且随着国产化服务器与终端的逐步普及，对国产化端点的管理也被提上日程。

解决方案

基于医院现有终端信息化能力，以联软主机监控与审计系统为基础的《医院内网终端安全一体化解决方案》，通过一套系统，实现医院内外网桌面终端的资产管理、安全管理、桌面管理、安全运维、外设管理、网络接入控制，在保障终端安全的基础上统一化管理及运维，减少运维工作。

方案特点

信创平滑过渡

一个平台实现信创终端与传统终端统一管理，保障信创终端稳步替换过程安全无风险；

运维效率提升

全网可视化管理、终端快速定位、软件分发、远程协助，以自动化手段提高维护效率；

便捷运维

IT资产管理、软件管理、补丁管理、实时通知、远程协助、屏幕水印、终端标准化流程等提升整院的IT管理效率；

介质安全

实现终端外设管控，防止未经授权外设或移动存储介质接入内部终端，并对移动存储介质进行注册、使用、审计、加密等控制；

支持多种接入控制技术，适应复杂网络环境

支持802.1x、Cisco EoU、WebAuth、Portal、端口镜像等多种准入技术，能够实现医院复杂网络环境下的接入控制。支持有线、无线网络接入，支持HUB、NAT、VPN接入场景；

集中管控

集中化管控平台，一套平台，一个客户端Agent实现多种功能，降低安全管理复杂度，提高管理效率，减少人力投资。针对多院区多分支医院场景，系统支持分级部署。

终端接入可信

杜绝非法接入、实现终端合规入网、权限可控，落实单位安全规范制度；

业务价值与方案优势

兼容性强、稳定性高

已完成国内主流信创操作系统（UOS、麒麟、中科方德等）、国产芯片（龙芯、兆芯、飞腾、鲲鹏、X86、ARM等）、中间件、数据库的深度适配，与办公软件、业务软件、浏览器、安全软件之间的各类兼容性强，确保在各类系统/平台上均能够稳定运行

终端一体化

通过整体规划，一个平台可以实现终端安全管理、桌面运维、准入控制、防病毒、文档加密、数据防泄密、威胁检测与响应等功能，同时现有平台可平滑过渡到信创环境，安全策略平滑沿用

支持全栈信创

系统支持在信创服务器操作系统、国产化芯片、国产化数据库、国产化中间件上进行部署，满足企业全栈信创建设需求

合规

满足卫健委行业规范和网络等级保护要求

资产管理

实时掌握院内资产动态，保障信息资产合法性、安全性、可用性

医疗文件内外网传输方案

需求来源

业务场景：近年来医院的信息化发展尤为迅速，一方面是互联网医疗业务的快速发展，另一方面是医院日常办公信息化程度的加深，且在疫情大背景下信息化业务需求大量增加。但是随着信息化程度的提高，敏感数据外泄的风险也大大增加。为了解决医院内部跨网文件交换及医院内外部医疗数据传输的需求。联软科技基于虚拟化技术开发了在网络隔离情况下的安全数据交换系统，在保证数据安全的前提下实现文件的跨网传输与分享。

解决方案

医院网络在逻辑上会划分为多张相互隔离的网络。甚至部分医院在多张网络间部署网闸设备建设物理隔离的网络。医院外网通常提供医院对外服务及网站门户服务，内网通常提供医院内部业务服务，如HIS、PACS、检验系统等。

联软科技基于UniNXG安全数据交换系统的《医疗文件内外网传输方案》，实现了网络隔离情况下的文件快捷传输。系统集成了防病毒、敏感文件检查、文件便捷分享、公共目录管理、权限控制等功能，确保病毒进不来、敏感文件出不去、内部文件仅能在许可范围内流转。

方案特点

跨网隔离

虚拟化隔离技术实现多网间 IP 协议栈隔离；

便捷交换

B/S、C/S 客户端及 H5，支持 PC 和移动端，覆盖 Windows、Linux 及信创；

文件安全

隔离交换留痕、查杀毒、审计审批、敏感识别、压缩加密、文档泄密追踪；

文件管理

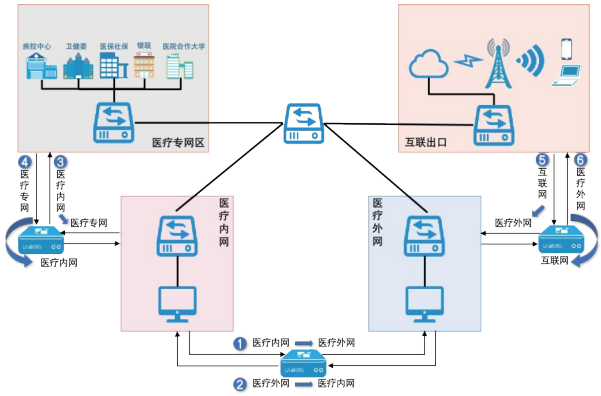
按用户、区域管理上传、下载、分享、外链、预览、编辑、备份恢复等；

敏感文件识别

流转的文件可通过关键字、正则表达式、文档 DNA 等功能识别敏感内容，触发敏感敏感内容进行阻断或审批。

高效统一

跨网共用一套认证源，统一策略管理，对接现有系统（如：组织架构、OA）；



业务价值与方案优势

全网隔离、多区交换

采用虚拟化隔离技术保障网络隔离性，同时跨网文件交换采用私有的非 TCP/IP 协议。单台设备支持 2-8 个网络同时进行文件交换，多设备级联部署可满足超过 8 个网络的文件交换

异构杀毒、内置DLP

内置杀毒引擎，同时支持第三方防病毒，多款防病毒软件实现异构杀毒。系统内置 DLP 策略，通过机器学习及敏感关键字规则对文件分级分类，可灵活配置组合规则和 DLP 策略

操作简单、统一认证

类似网盘的用户界面，支持 B/S、C/S 及 H5 方式，无需培训，易操作。统一认证源，跨网运维和系统管理简单

详尽审计、灵活审批

详细的文件上传、下载、删除、分享、外链、备份恢复等行为审计和交换文件内容审计 / 审批，审批可满足对文件多级审批和人工审批，同时可提供标准 API 接口对接 OA 审批

降本增效、相对平衡

代替传统 U 盘实现跨网文件交换，提供容错式网络与数据安全保护，便捷交换，实现安全与效率相对平衡统一，降低管理成本。系统具备等保 3 级认证，支持全栈信创，支持 IPV6

医院行业安全策略管理系统解决方案

需求来源

政策要求：国家及行业监管部门监管力度不断加强，《网络安全等级保护测评要求2.0》中提到，在“安全区域边界-访问控制”项中，要求对防火墙、路由器、交换机等边界网络设备的访问控制策略进行检查。保证访问控制策略精细化、逻辑关系合理，不允许存在宽泛、权限过大等策略。

业务场景：随着信息化的加速，应用场景不断增加，防火墙以及路由交换设备数量和种类日益增多，安全策略控制的力度日趋细化严格，导致运维效率低、出错几率大。许多用户目前对安全策略的管理缺乏有效的手段，无法检查全策略配置的正确性。在安全策略配置变更、新增时，管理员操作依据较为模糊，缺少相关的数据分析，容易造成安全策略配置上的缺陷或者错误，给运维工作带来许多困难。

解决方案

安全策略管理系统通过对全网防火墙、路由交换、负载设备的数据进行采集和解析，建立统一的设备模型和拓扑模型。实现对安全策略的智能精确梳理，发现策略中的隐藏策略、冗余策略、过期策略、空策略和可合并策略等。通过可视化视图展示路径查询结果、数据流关系、攻击面分析、跳板分析和安全域基线检查矩阵。系统内置策略自动化运维流程，可以针对不同的策略运维场景提供智能化、自动化的解决方案，辅助运维人员实现策略开通、策略批量下发、一键封堵等多项功能。

业务价值与方案优势

等保合规

协助用户满足在安全管理和基线检查方面的合规需求

策略梳理

可以定义审计项，对不合规的端口或放行过大的策略进行检查，梳理出不符合要求的策略

集中管理

集中纳管现网异构品牌防火墙、路由交换，实现全网的集中管理，可以快速全网搜索地址、服务，以及对应策略导出，提高运维效率

策略优化

防火墙存在上万条策略，平台能自动计算策略中存在的隐藏、冗余、过期策略等，生成清理脚本下发

广泛兼容

产品支持国内外 90% 厂商防火墙、路由器、交换机

业务策略迁移

不同品牌防火墙迁移后，对原有访问关系一键批量迁移，选择新增和修改策略两种方式

医疗数据防泄密解决方案

需求来源

政策要求：数据安全是数据经济产业的基石，当前数据安全的逻辑正在发生重大变化，数据资产正在脱离单独的个人甚至企业层面，开始逐渐演变成为国家的战略资源和核心资产，其战略地位和重要程度显著提升。数据安全在医疗行业也变得尤为重要，随着《数据安全法》《个人信息保护法》出台，卫生部颁布三甲医院评估细则，明确提出患者隐私保护的重要性，同时要求加强信息系统的安全保障措施。医疗行业内数据安全能力的建设与提升得尤为重要且紧迫。

解决方案

联软科技推出的《医疗行业数据防泄密解决方案》，针对办公终端的人员角色、应用场景、网络位置、环境、终端及数据类型等不同场景化要求，通过统一管理平台提供网络边界保护：

终端数据防泄密安全基线管理

部署 802.1x 和网关准入实现网络边界安全，强制终端安装客户端软件，进一步按需下发策略到客户端实现数据防泄密基础管理；

数据分类分级标签与权限管理

启用 DLP 分级分类、敏感识别，实现联合智能加解密、密级标签和用户密级关联管理；

外发数据审计

针对终端邮件、即时通讯软件、移动存储介质、打印、网络等外发通道进行审计，所有外发信息在后台留档记录，敏感数据禁止外发；

屏幕水印

打开敏感文档、业务系统 URL、自定义进程、打印时，展示对应的明文、二维码、图片、矢量、盲水印等多种水印效果，水印内容可自定义，可包含设备、用户、时间（年 / 月 / 日）及自定义等内容；

边界保护	端点保护	数据保护	威胁防御	业务平台扩展
NAC（局域网接入） SDP（互联网接入）	Windows Mac iOS Android 信创（UOS、麒麟）	内容识别 通道收敛 行为审计 安全沙箱 安全存储 安全水印 屏幕录像 文档安全	终端检测与响应 （防勒索） 网络智能防御 （防入侵）	文档发布平台 安全移动门户 邮件防泄密（网关） 网络防泄密（网关）

管理平台

一体化运维：同一管控中心、同一Agent、统一管控策略、统一账号管理、统一流程管理
统 一 架 构：传输协议、通信协议
可视化分析：大数据分析平台、全文检索系统、安全审计系统

终端数据安全运营管理

基于场景化方案，按数据生命周期对数据采集、传输、存储、使用、共享、销毁等过程进行全面数据安全管理，通过大数据处理引擎、数据分析引擎、内容识别引擎等基础组件对数据安全指标进行分类分析和集中可视化展示和管理，如：防泄密客户端安装率、安全策略执行成功率、泄密安全事件及响应情况等。

业务价值与方案优势

办公终端数据防泄密解决方案，采用成熟的先进技术，符合办公终端数据防泄密管控要求，对于企业办公终端数据安全建设具有积极的作用。

安全与效率平衡

通过规划基于业务场景化的解决方案，将数据防泄密相关安全措施融入不同业务操作中，实现数据安全和效率平衡

有效、且可交付

通过制定企业场景化的办公终端数据安全管理制度，及完善符合企业发展的数据分类分级规划。基于“一个平台 + 多个安全组件”按需求场景选择技术能力的形式，实现有效可落地

统一、持续扩展

平台及客户端支持国产化，实现跨平台统一管理，可按需提供网络准入、终端安全、防泄密、防勒索、防病毒、文档安全等能力，同时可扩展数据安全运营、防入侵、防泄密网关等

医院配发PAD管理方案

需求来源

等保合规要求：近年来医疗应用与智能终端的融合使用，在国内各大医院得到了广泛普及。最具代表性的就是医护人员通过医院配发的PAD设备进行移动查房、移动护理。医院等保3.0对医院信息系统安全性提出了严格要求。

移动设备统一管理：移动智能设备可以协助医护人员更高效和准确的查房和护理，提高了医护人员的工作效率。但移动化方案的落地也给医院带来了新的挑战及新的安全风险。

无线安全接入：医院配发PAD设备的安全接入问题，防止设备违规使用，配发设备的应用更新和推送，配发设备医疗数据的保护问题，给医院IT管理者带来了新的困扰。

解决方案

通过建设UniEMM企业移动安全管理平台为基础的《医院配发PAD管理方案》，能够很好地解决医院配发PAD设备在移动设备办公中遇到的安全问题。

资产管理

对配发设备进行软硬件资产采集，与用户或者科室进行绑定，记录设备的日常使用情况。提供远程控制、消息通知、安全事件告警等功能；

安全接入

提供安全隧道接入、802.1x 认证、NAC 认证，设备入网安全检查，强制安装移动客户端，未安装客户端禁止接入网络；

安全管理

对配发设备的外联、外设进行管控，提供 Wifi 黑白名单、蓝牙黑白名单、应用黑白名单、USB 口控制、屏幕控制、相机控制、SIM 卡控制等功能；

定制化安全桌面

强制开机进入安全桌面，自定义配置安全桌面内显示的应用，禁止下拉菜单、禁止修改设置，安全桌面禁止退出，实现专机专用。

私有应用商店

提供企业私有应用商店，对企业使用的 APP 应用、H5 轻应用等统一下发、安装、管理；

业务价值与方案优势

安全保障

禁止非法设备访问内部网络及业务系统，保障业务网络的安全性，解决医疗移动办公面临的网络设备接入、配发 PAD 设备的资产管理、医疗数据泄密等问题

规范合规

实现对配发设备的规范化管理，实现办公应用的批量管理，提高员工在工作期间的效率，同时全面满足监管要求，提高医院管理水平

效率提升

搭建医院自有的应用商店，实现内部应用的自动分发和集中管理

兼容适配

经过多年积累，联软 EMM 系统已经适配大量 Android 和 iOS 终端，支持对医院少见移动终端设备的适配，对第三方 APP 安全能力加固适配

医院全网零信任解决方案

需求来源

内外网终端、移动端统一管理难度大：随着医院各项信息化业务进入全面、快速发展阶段，接入办公网络的终端数量和终端类型日益增加，包括办公内网、办公外网、互联网三个区域的终端。为了保护各区域网络信息安全，各网络之间采取物理隔离或者逻辑隔离的方式，各区域重复性建设终端安全管理系统，无法做到统一管理，运维繁琐、效率低。

互联网远程接入设备、人员复杂，安全性低：信息管理人员紧急运维、医生随时编写电子病历、各种信息系统需要第三方厂商运维等需求，模糊了原先的网络边界。

多个平台维护难度大、成本高，需要降本增效：用户希望在内网或者互联网都能快速安全地连接到业务系统，全网零信任接入的需求愈加迫切。目前采用的传统的VPN远程接入技术不仅技术老化漏洞频发，用户网络访问权限管理较弱，并且不能对接入的终端做接入安全检查，其安全性也让医院胆战心惊。

解决方案

联软科技全网零信任解决方案融合了零信任、移动安全、准入安全、端点安全等功能。通过一套平台、一个客户端集成了接入安全、端点安全、数据安全的能力，针对不同身份、不同设备类型、不同操作系统、不同接入场景、不同的数据外发方式进行全面管控。用户可根据企业当前建设阶段及实际需求选择具体的应用场景，可基于一套平台可快速扩展，无需重复建设，满足当前及未来的安全建设需求。

方案特点

顶层设计

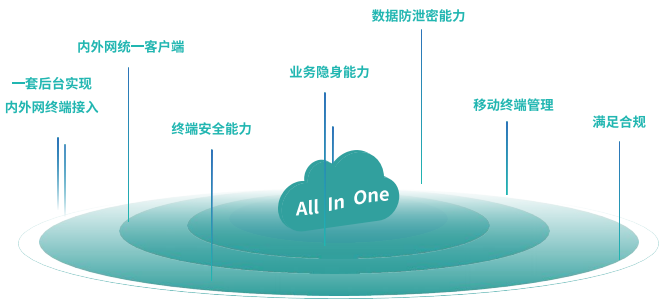
一套管理系统，一套客户端软件，同时满足办公内网、办公外网、互联网三个区域的终端安全管理，包括 PC 端和移动端；

端口隐身

医院的业务系统不用发布到互联网，零信任安全网关具备隐身，做到互联网端 “0”暴露；

统一入口

统一应用访问入口，规范用户访问行为，提升远程办公体验，提高工作效率；



持续环境感知

整合终端保护平台 EPP 功能，制定设备的安全基线，对接入企业内网的设备进行标准化设置与安全管理，包括设备的软件管理、补丁管理、外设管理等；

效率提升

规范医院内、外网终端的接入安全，应用管理安全和医护数据安全，保证业务安全的同时，也提高医护效率。

业务价值与方案优势

安全

- SPA机制隐藏服务，暴露面收敛，天然抗攻击；
- 应用级加密隧道技术，避免内网全面暴露；
- 终端数据安全沙箱，防止医院数据外泄；
- 基于属性的动态评分机制，提供持续可信访问。

高效

- 提供灵活、便捷的多因素认证方式；
- 支持SSO单点登录，无需反复认证；
- 统一门户，统一用户访问入口，规范用户访问行为；
- 部署简单、运维简单；
- 用户行为记录分析，提供丰富的决策依据。

灵活

- 微服务架构，按需灵活扩展功能模块；
- 标准API接口，轻松集成第三方系统；
- 统一后台架构，支持扩展移动平台接入；
- 控制平面与数据平面分离，天然适配混合云网络。

医疗行业防入侵(勒索)技术方案

需求来源

勒索病毒已成常态化威胁：近年来，勒索病毒已从偶发事件演变为常态化威胁，在医疗行业，时常能听到部分医院因为勒索病毒攻击而停诊，有的医院甚至多次受到此类侵害。事件造成的影响范围深远，不仅导致数据丢失，还可能使关键基础设施陷入瘫痪，进而带来巨大经济损失。

勒索攻击方式愈发狡猾：勒索病毒并非固定形态，它随着技术的不断进步而持续演变。从最初简单的文件加密到现在可能涉及整个系统的锁定、数据泄露，甚至是设备损坏，其攻击方式愈发狡猾，使得防范工作变得更为困难。

亟需构建主动预防策略：鉴于勒索病毒的高损害性和难预测性，单纯的被动防护已无法满足安全需求。企业需要构建主动的安全预防策略，结合实时监测、备份管理和应急响应，以最大程度降低被攻击的风险和潜在损失。

解决方案

随着勒索软件攻击的不断升级，保护医院的核心系统、数据资产和敏感信息已成为当务之急。为此，联软科技依托其可信数字网络架构TDNA，提出了一套立体式防御方案，能够更加有效地保护医院信息系统的安全。

方案构成

云

攻击面管理 + 勒索风险排查服务；

端

终端勒索防护 + 数据备份 + 一键隔离。

边

暴露面收敛 + 安全策略管理 + 网络隔离；

业务价值与方案优势

立体式防勒索方案开创了新的安全防护思路和方法，用户和组织可以更加全面地了解内网中的风险行为，提升了安全威胁的感知和防范能力，以下是联软科技防勒索技术方案的具体优势：

及时防护

我们采用了创新的技术，可以快速阻止网络攻击。如果有不同于以往的攻击方式出现，我们的系统会立即告警并指明具体攻击行为

快速响应

正如速效救心丸在关键时刻为心脏提供急救，快速响应模块在您遭受网络攻击时，为您提供秒级阻断保护，能够确保您的业务快速回到正常状态，保证最小的业务中断

全网调查

正如雷达在浓雾中迅速捕捉每一个目标，全网威胁调查在面临数十万终端的大环境中，提供分钟级的精准探测，仅需 1-2 分钟就能得出全面调查结果，极大减少企业风险

经济高效

相比于传统的备份方式，我们提供的方法更加节省成本，并且能够在短时间内恢复您的数据

与时俱进

持续关注网络安全最新动态，根据动态及时更新我们的保护策略和检测规则

灵活关联

检测与响应可以和防病毒模块配合工作，提供一键查找病毒来源的功能

持续扩展

我们的方案可以根据您的实际需求、业务发展进行调整，支持对于数据防泄密需求的快速扩展

医疗行业软件管理解决方案

北京协和医院　上海交通大学医学院附属瑞金医院

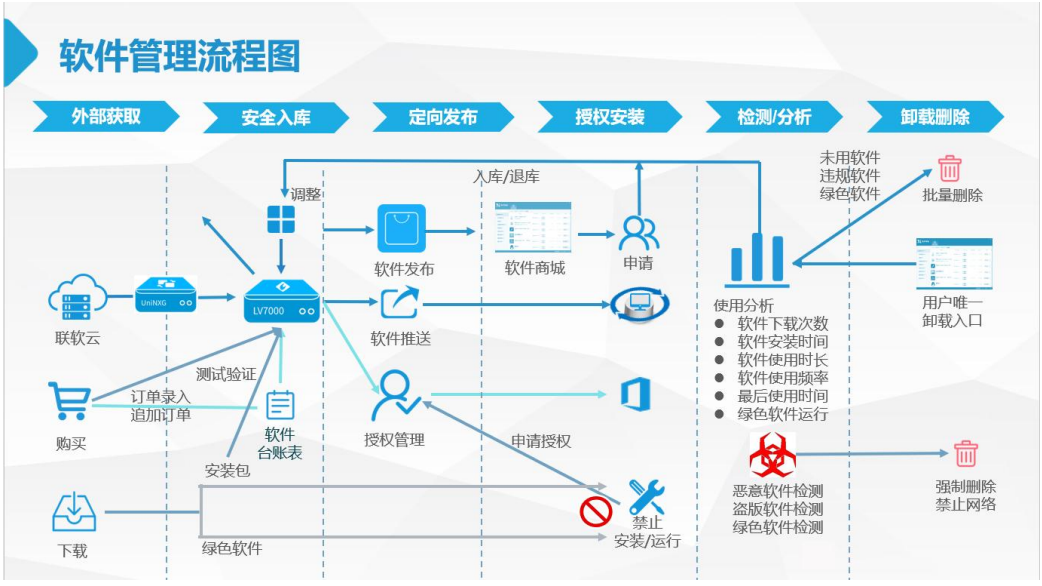
需求来源

2016年国家版权局正式颁布了《正版软件管理工作指南》，指导文件要求各级政府机关、企事业等单位落实软件正版化管理工作，规范使用正版软件行为，提高软件资源使用效率，保障信息系统安全高效运行，推进使用正版软件工作规范化标准化。

此外，各地卫健委先后提出《卫生健康行业软件正版化工作方案》，进一步推进软件正版化工作规范化、制度化、常态化和信息化。中央网信办推进互联网+健康医疗应用安全防御体系建设以及国务院推进使用正版软件工作的统一部署，将深入实施知识产权战略与网络信息安全相结合落到实处。医院员工非正规渠道下载的软件（捆绑软件）对软件管理造成诸多不便，若不做软件标准化、正版化的管理，会带来软件厂商盗版纠纷、勒索病毒感染隐患、设备系统卡顿、安全泄密事件、广告弹窗等问题。

解决方案

联软科技提供的软件管理解决方案，不但满足《正版软件管理工作指南》中关于医院软件正版化管理的要求，也能帮助医院规范软件标准化管理。



该方案包括以下内容：

- 软件采购信息、许可信息、软件介质管理信息、计量方式录入，以订单管理方式进行录入信息的管理，支持将录入信息导出报表以供台账管理；
- 软件正版化可以对终端进行软件授权管理，被授权的终端属于使用正版软件，未被授权的终端属于使用盗版软件，发布盗版软件整改通知，便于反馈整改情况；
- 实时抓取终端软件安装信息，与软件资产领用信息进行比对，筛查疑似安装盗版软件等终端，非合法途径下载的软件禁止安装和运行；

- 软件使用数量接近授权数量时及时预警，以便发起增购；
- 软件使用信息收集，包含软件安装数量、所安装的计算机信息、使用人员、使用时长等；
- 对违规软件、被报废下线软件的预警、卸载处置；
- 软件进行授权管理，用户发起软件安装申请，对终端或用户进行远程授权；
- 软件应用商城，提供企业正版软件下载通道，解决用户自主安装软件的难题；
- 提供软件分发、软件自动分类、软件黑白名单等工具来满足企业的软件管理要求；

业务价值与方案优势

该方案能全面满足合规要求，相比传统方案：

统化的台账登记与管理，提高了信息收集的效率和准确率

自动授权和自动回收机制，可以便于医院对软件正版化进行授权管理

在严格管控的同时，提供丰富的软件入口。形成了类似AppStore的环境，既满足了医院的需求，也满足了终端用户的需求

安装与使用时长信息的收集，能够获知软件的实际使用情况、终端用户对该软件的需求如何，便于医院对软件情况进行分析，提供采购计划的参考

有效地阻止了流氓软件的下载安装，提高了终端用户的工作效率和提升了终端的信息安全环境，避免一些病毒软件无法防护的黑市工具、挖矿软件、系统监控类的恶意软件降低终端的运行效率，造成企业的信息泄露、形象受损等事件

网络安全底座解决方案

需求来源

勒索事件频发：近年来，许多大中型银行、企业、医疗机构，数据中心或生产网络中勒索病毒，云上的所有虚拟主机无法启动，或者大量的终端电脑无法开机，导致业务中断，被迫缴纳赎金；

业务连续性风险：勒索病毒带来的业务连续性风险，已经成为各个单位网络安全的头号问题，问题解决不好，将导致业务中断数周甚至数月之久；

无有效现成防护方案：目前用户为应对这些问题采取了两地三中心部署、部署了大量防火墙、IPS等设施，但仍然难以有效解决勒索病毒在主中心和备中心间移动、管理服务器被入侵导致大面积入侵、黑客入侵终端后横移攻击等风险。

解决方案

联软科技网络安全底座方案针对勒索病毒导致的业务系统大面积瘫痪而专门设计，不追求“零伤亡”，做好底线风险管控，帮助企业解决最核心、最要紧、最根本的问题。在企业整个网络和信息安全的建设中，建立容错机制，采用弹性网络设计，进行分域控制，确保鸡蛋不放到同一个篮子里。在进行分域控制过程中，通过联软准入控制、零信任接入控制、数据安全摆渡、WSG/API安全网关、安全策略管理等设施，收敛域和域之间的访问关系，控制勒索病毒传播范围，实现高效防御与快速恢复，最大限度地确保业务的连续性。

全网统一访问控制（NAC/SDP/EMM）

- 采用 NAC 802.1x/SDP 等软件定义访问的方案实现终端从内、外网安全访问数据中心的效果，对内实现接入终端间的网络隔离，对外实现数据中心应用的暴露面收敛，大大减少勒索病毒在接入终端间横向扩散，以及扩散到数据中心的风险；

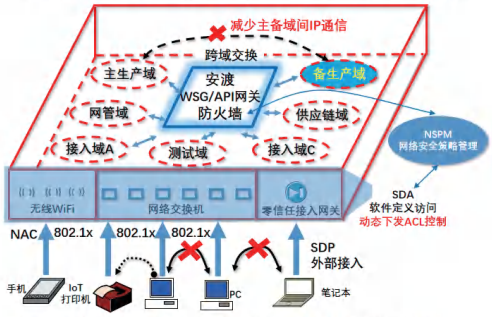
分域和跨域访问控制（防火墙/NXG/WSG/API）

- 通过将数据中心进行分域，实现各项业务的隔离和安全等级的区分，阻止勒索病毒在数据中心横向移动。通过建立单独的备份域，确保在极端情况下，生产系统可以快速恢复，保障核心业务不中断。通过防火墙 / 安渡 /WSG/API 网关来收敛和最小化跨域的网络访问关系，进一步减少勒索攻击跨域传播和扩散的可能性；

主动式网络欺骗技术（幻影）

- 在企业网管域、备生产域等重点区域，部署主动式网络欺骗等技术，加大黑客入侵难度，更早发现入侵行为；

全网统一访问控制(示意图)：内、外部接入，跨域访问



安全身份，用安全端点，以安全方式(SDP&802.1X)访问
（建议终端不要全部加入域，避免域控服务器被入侵）

网络安全策略管理（NSPM）

- 通过 NSPM 能对网络 L3/L4 层 ACL 统一管理，做到安全策略可视化管理，避免 ACL 配置错误（换岗、人为失误），预测攻击路径，真正将访问控制策略落到实处。

业务价值与方案优势

控制横向移动，实现底线风险控制

接入网络中电脑终端如果中了勒索病毒通过端口级接入控制技术，确保其难以横向移动到其它终端；数据中心的主机如果中了勒索病毒，通过 NXG/API 网关 / 防火墙等技术防止其移动到其它域。通过备生产域实现极端情况下业务快速恢复，实现底线风险管控。

做好跨域交换，收敛访问关系

提供覆盖网络、应用、数据的跨域访问控制技术，收敛访问关系，减少风险暴露面

可视化策略控制，减少人为错误

通过网络安全策略管理实现策略可视化、自动化管理，预测攻击路径，减少人为配置错误

做好重点保护，及早处置入侵

对生产域、网管域等重点域部署幻影主动式欺骗技术做增强保护，及早发现入侵，提升入侵难度

数字化安全基座解决方案

需求来源

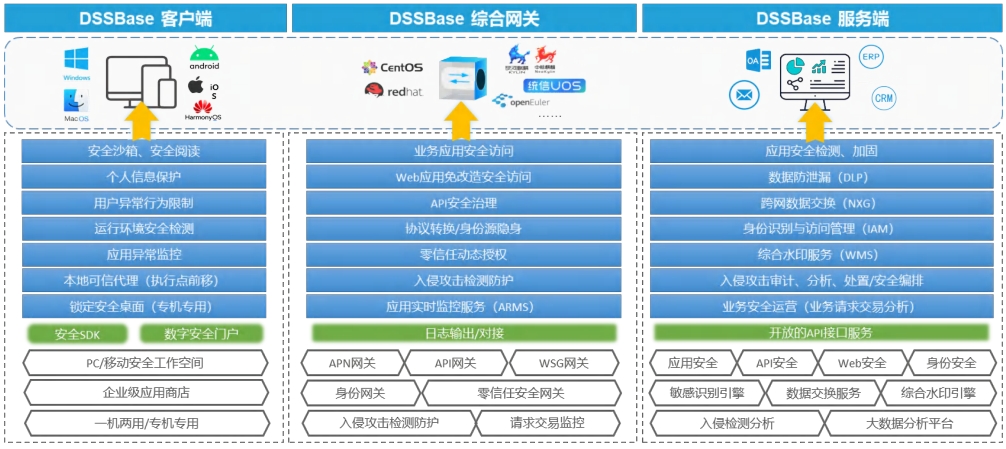
数字化应用安全要求：业务存在入侵风险、数据存在泄露风险、设备管理困难、传统VPN使用体验差、安全合规要求加强。

安全事件频发：网络攻击事件，数据泄露事件，个人隐私违规事件。

传统建设方案问题：自建业务系统安全弱、体验差、重复建设、安全无统一规范，安全过度依赖定期检测。

解决方案

联软数字化安全基座解决方案是通过提供一整套落地实践的安全架构，解决企业防入侵、防泄密、员工隐私保护等问题，达到提升安全、提升效果、减低TCO的建设效果，数字化安全基座解决方案包含云、管、端三位一体安全保护，具体内容如下：



该方案包括

DSSBase客户端

- 在终端设备本地通过可信代理、安全工作空间、员工隐私保护、专机专用等功能实现终端授权策略执行点前移，分离企业和个人数据，阻断非法越权获取个人隐私数据等效果；

DSSBase综合网关

- 具有应用安全代理、API 安全治理、Web 安全、入侵检测及身份识别管理为一体的多功能综合网关，解决业务应用访问和系统数据传输过程终端安全保护和风险管理；

DSSBase服务端

- 建设应用安全、数据安全、大数据分析和安全编排等多维度服务平台，为企业数字化转型提供安全配置、分析、监控、展现的管理基础。

业务价值与方案优势

经济收益高，以 50 个移动应用为例，可节省 875 万，数据泄露防护价值不可估量	解决传统 VPN 隧道被黑客利用及弱网环境不稳定问题，增强了员工使用体验和业务原生安全	改变安全开发模式，大幅减少安全开发工作量，开发人员专注关心企业业务实现	超越零信任，实现远超传统零信任框架的安全体系建设

联软科技
LEAGSOFT

服务热线：400-6288-116
地　址：深圳市南山区粤海街道科兴科学园A2栋9层
邮　编：518057
电　话：0755-86219298
传　真：0755-86148550
网　址：https://www.leagsoft.com

获取专家支持

知晓最新资讯