联软科技
LEAGSOFT

政府
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

政务终端一体化安全解决方案

中国环境检测总站	湖北省公安厅	河北省财政厅	中国城市规划设计院
潮州市政务服务数据管理局	湖南省监狱管理局	江苏省税务局	深圳市交通局

需求来源

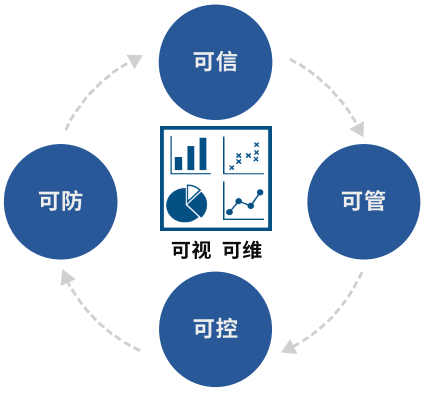
合规驱动：2022年7月1日，国家电子政务外网管理中心印发《政务外网终端一机两用安全管控技术指南》（GW0015—2022），明确了政务外网终端安全防护技术要求，指出局域网终端安全防护应当在遵守等保等安全规范要求基础上，执行实施终端安全“十项”安全能力，原则上应对终端进行恶意代码防范、终端入侵防护、非法外联控制、安全基线检查、漏洞检测修复、数据安全防护、终端软件管理、终端补丁管理、终端资产管理及终端精准阻断。

事件驱动：随着各级政府电子政务信息化的深入发展，信息网络已经成为国家各级政府单位运行的基础。近些年政府部门开展的信息安全大检查中，发生了多起重大信息安全事件，主要是由于计算机终端引起。

需求驱动：随着信息安全的建设，各政府部门对终端进行网络准入控制、补丁管理、桌面管理、安全加固、U盘管理、网络行为审计、敏感数据管理、数据防泄漏管理、病毒防护、终端检测与响应、加密等措施，导致一个终端安装多个管理客户端，严重影响终端运行速度和用户体验。另一方面，从2016年提出安全可控体系以来，国家提出了“2+8+N”体系， 逐步实现国产化替代，“2”是指党、政。随着国产化建设的不断深入发展，国产终端安全也面临着日益严峻的考验。

解决方案

以联软ESPP企业安全监测保护平台为基础的《政府终端一体化平台解决方案》，通过一个平台、统一框架、数据集中，实现更强更智能的安全保护，涉及网络准入控制、网络智能防御、桌面安全管理、数据防泄露、病毒防护、检测与响应、终端安全运营等方面，为用户提供一体化、全方位的政务外网网络与信息安全解决方案。



可信
全网零信任方案，构建企业网络安全边界，确保接入终端“可信”

可管
加强端点安全防护能力，提高免疫能力，确保终端“可管”

可控
面向企业可落地、有效果、安全和效率统一的方案，确保数据“可控”

可防
结合终端主动防御、EDR+杀毒，实现立体式防入侵（勒索），实现终端“可防”

可视
基于强大的网络可视化能力,自动发现并识别全网设备,确保资产“可视”

可维
提供简化桌面运维，增效降本的运维管理工具，实现终端“可维”

该方案包括

统一客户端

- 一个客户端 Agent 从网络准入控制、桌面运维管理、终端安全管理、到补丁加固、外设管控、终端行为审计、数据防泄密、文档安全、终端检测及响应等全场景端点安全功能覆盖；

全网资产可视化

- 对网内 PC、移动终端、IOT 设备进行自动发现、设备类型识别，确保资产“可视”；

统一权限

- 统一管控用户的网络资源访问权限、终端操作权限、数据外发权限，实现以人为中心的统一安全管理；

终端数据防泄密

- 对政务外网数据在创建、流转、存储、使用、外发、互联网传输等阶段进行场景化的数据防泄露，通过敏感检测、水印、文档加密、文档追踪等技术进行泄露数据的快速追溯定位，自动发现、自动收集、智能分类、统一管控、风险分析、流转追溯；

终端检测与响应

- 多维的终端行为数据类型采集，快速分析海量数据，快速识别告警安全风险，深度发现威胁事件，并快速调查取证，威胁响应，处置修复。

终端桌面管控

- 涵盖终端安全基线完善与加固、终端标准化管理、运维简化管理、软件正版化和标准化管理；

终端防病毒

- 除了防范常见木马、病毒，还提供文件防勒索、钓鱼行为检测等能力避免终端文件遭受勒索病毒的入侵；

业务价值与方案优势

该方案实现对包括Windows、macOS、Linux、统信UOS、银河麒麟、中科方德、IoT设备在内的各种操作系统和各种终端设备的集中管控，相比传统方案：

满足监管要求

深入贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度，确保政务信息安全工作落到实处，满足法律法规与技术规范监管要求

减轻运维压力

统一平台化管理，简化维护人员工作，实现全网终端设备的集中管理，使得政务业务终端安全做到实时的可管、可控、可信、可视，并且管理员随时能够掌握终端资产的配置及变动情况

一体化的网络安全防御体系

N合1的解决方案，减少客户重复投资，实现网络准入控制、防泄露、桌面管理等系统的集成与联动，具有网络访问控制、主机安全检测加固、网络异常检测、非授权外连、网络行为审计等功能，平台功能全面

响应国家信创政策

已完成与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。一个平台支持windows、Linux、macOS及国产操作系统的统一管理，保障信创终端稳步替换过程安全无风险

政务外网终端一机两用安全管控解决方案

国家信息中心 | 安徽省大数据中心 | 黑龙江省政务大数据中心 | 中山市政务服务数据管理局 | 中华人民共和国全国人民代表大会

韶关市政务服务数据管理局 | 清远市政务服务数据管理局 | 吴川市政务服务数据管理局 | 黄冈市政务服务和大数据管理局

需求来源

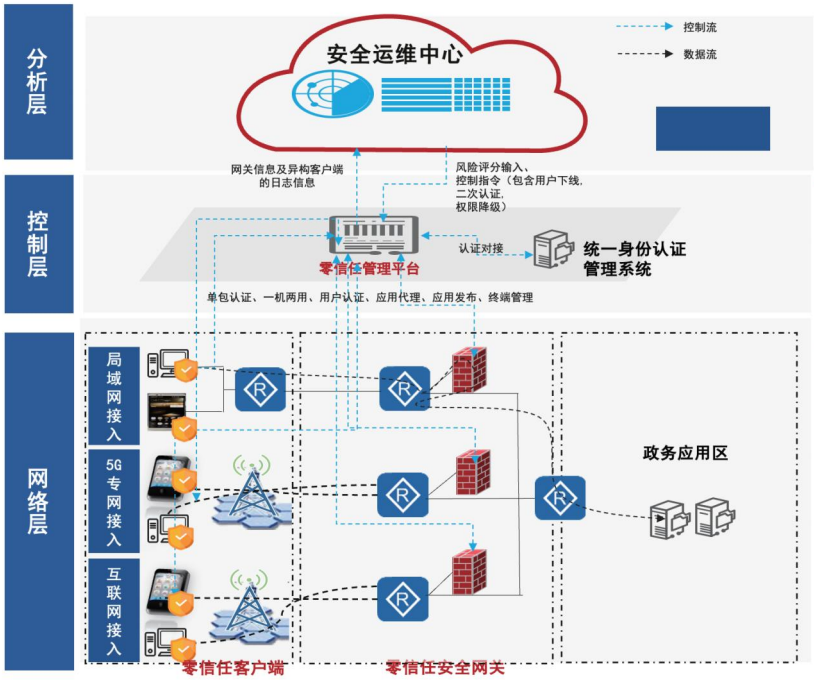
业务需求:政务外网终端同时连接政务外网和互联网，存在着“一机两用”场景；

安全需求:政务外网终端极易成为网络攻击的跳板，将互联网安全风险引入到政务外网中，极易带来跨网攻击、数据泄露等安全隐患，严重影响政务外网安全；

政策合规:2022年7月，国家电子政务外网管理中心发布《GW0015-2022政务外网终端一机两用安全管控技术指南》建议实施基于零信任理念的一机两用方案，应实现网络隔离、会议隔离和数据隔离。

解决方案

以联软科技UniSDP零信任访问控制系统为基础的《一机两用解决方案》，以“永不信任、持续验证”的零信任理念为核心，通过接入认证、网络隔离、数据隔离、应用代理、统一管控等手段，解决局域网、5G专网、互联网接入三个场景零信任安全接入，提供更全面的安全、更极致的体验、更高效的管理。



入网可信认证，防止非法用户接入

- 通过零信任技术，使政务应用系统“隐身”，仅合法终端能访问；
- 采用应用代理模式，隐藏访问政务应用的真实地址，缩小攻击面。

网络隔离，防范跳板攻击

- 通过单网通策略，同一台终端无法访问两张网络，防止互联网攻击以终端为跳板，攻击电子政务外网。

数据隔离，防数据泄露

- 采用数据沙箱技术，防政务数据被非法导出、打印泄露；
- 采用数字水印技术，对数据泄漏行为进行溯源。

二次鉴权，保障5G专网接入安全

- 通过零信任技术，实现对5G专网接入设备二次鉴权，终端需要通过认证后才能访问政务外网网络与应用；

该方案包括

零信任终端

- 此处所说的用户终端主要是指“一机两用”终端，用户终端上需部署零信任客户端，实现接入认证及入网安全检查、网络隔离和异常行为检测；

零信任管理平台

- 实现应用申请及发布管理、零信任客户端运维管理、评分动态授权等功能，以及终端安全策略集中管理和下发；

安全运维中心

- 零信任管理平台与现网中的安全运维中心进行信息同步，包括但不限于网关信息及异构客户端信息的同步；零信任管理平台提供 restful 接口供安全运维平台等系统调用，提供风险评分输入、控制指令，指令包含用户下线、二次认证、权限降级等。

零信任安全网关

- 主要实现接入鉴别、访问控制和网络隐身等，通过将业务隐藏在零信任安全网关之后，可以有效收敛各级政务部门业务暴露面，减少被入侵的风险；

统一身份认证

- 各级政务部门需建立自身的统一身份认证系统，用于用户的准入认证，零信任体系与本部门已有统一身份认证体系进行对接；

方案部署后

更全面的安全

- 对接入终端进行认证，确保接入人员身份合法，终端禁止同时访问电子政务网络和互联网，阻断跨网攻击，数据安全沙箱加密隔离存放；

更高效的管理

- 通过一套管理后台，实现终端安全防护一体化管理，降低管理复杂度。

更极致的体验

- 终端一次接入认证，可一键切换网络，提高用户体验，高性能零信任安全网关支持分布式集群部署，保证用户接入速率；

业务价值与方案优势

方案节省投资
一套管理后台打造多种安全能力，一台网关实现多网业务代理转发，一台终端多网访问，降低系统建设费用，一套系统实现合规、安全、高效

保护重点业务
隐藏真实地址与端口，缩小暴露面，重要应用基于角色的发布管理

保障业务安全
确保网络安全、终端安全、数据安全，支持安卓、鸿蒙、UOS、麒麟等主流国产或非国产操作系统

威胁精准溯源
基于终端 DeviceID 重塑威胁识别体系，将设备信息、用户信息在网络中“流转”，实现端点侧威胁的精准溯源

提升业务效率
终端一次接入认证，操作便捷，一键切换网络

高可用高扩展
云部署、集群等高可用部署，可扩展移动终端安全管理、终端安全管理等功能模块

政务移动安全接入解决方案

国家信息中心	中山市政务服务数据管理局	深圳市大数据局资源管理中心
黄埔政法委	东营公安	安徽省大数据中心

需求来源

政策驱动：国家“十四五”规划提出要推进政务信息化发展；各级政务外网管理单位也发布相关标准要求，包含《信息安全技术电子政务移动办公系统安全技术规范》以及《政务外网终端一机两用安全管控技术指南》，明确了接入政务外网终端、移动设备的安全防护技术要求。

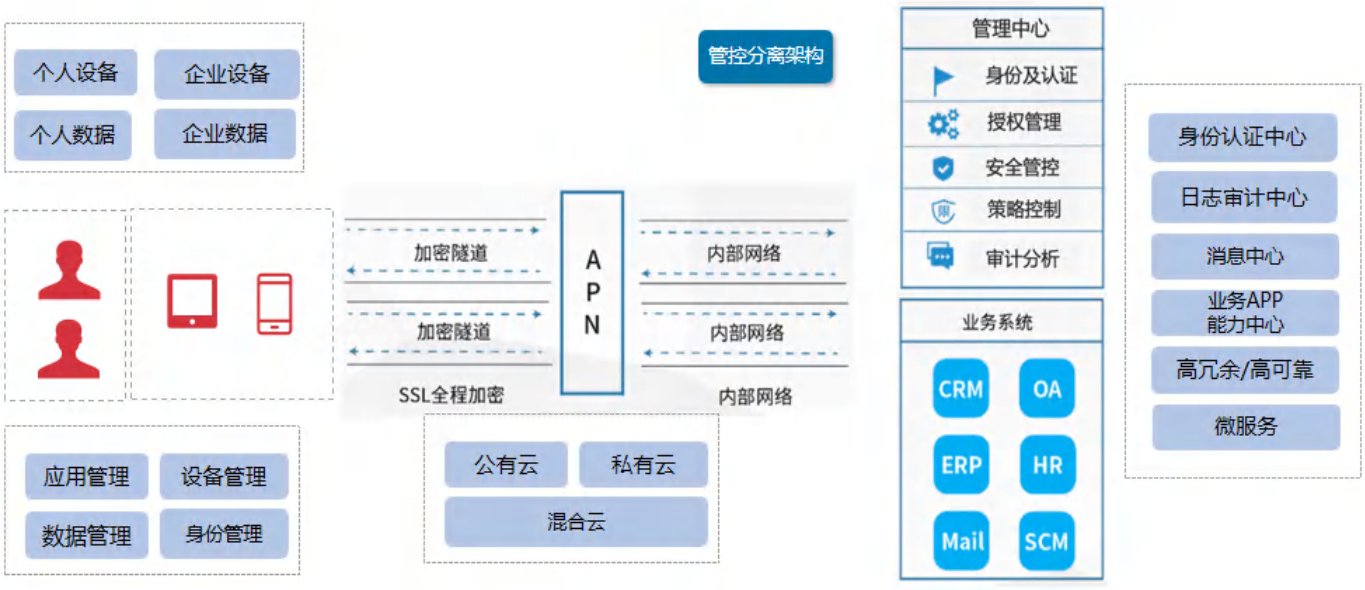
业务场景：移动设备安全接入到政务外网，囊括政务外网的四个安全维度，移动接入安全、移动设备安全、移动应用安全、移动数据安全，通过对四个维度的管控来规范移动设备通过互联网接入政务外网访问业务。

一机两用：移动安全接入也是一机两用的场景之一，接入政务外网的移动设备与接入政务外网的办公终端要形成联防联动，形成政务业务应用运营平台，规范在政务外网发布上线的应用建设。

隐私保护：针对政务人员手机办公场景，提供个人信息安全保护，防止越权导致的个人信息泄露。

解决方案

本方案以联软UniEMM企业移动安全管理平台为主，作为《政务外网移动安全接入解决方案》，可与政务外网一机两用解决方案形成联防联动，通过在政务外网数据中心部署管理后台，互联网接入区部署安全网关，主要管控移动接入设备。



该方案包括

移动统一门户

- 提供移动设备的远程办公安全访问门户，并结合用户现有认证系统与本系统自身多因素认证体系（动态码、生物特征等）构建境外数据安全访问方式，实现用户通过门户进行统一登陆后，访问政务外网办公业务；

政务业务管理

- 以管理平台自身的业务全生命周期管理能力，灵活管理 CS/BS/H5/ 等政务业务应用，定义业务发布上线规则，确保每个业务系统在政务外网上规范化管理，确保基于用户身份进行业务访问的整体管理效果；

移动数据安全

- 对政务外网业务应用产生的数据通过安全沙箱、水印等手段进行防护，用户基于业务系统下载的业务数据，保存在移动安全沙箱，与本地数据隔离，可通过安全浏览器或安全阅读器进行查阅，同时附加屏幕水印防护，预防拍照；禁止截屏，保护数据安全。

国密安全隧道

- 基于每个业务应用建立独立的国密安全隧道，保障远程数据访问的通信安全；

移动设备管理

- 对于网格员、消防公安体系、税务大厅等场景的配发设备进行统一规范管理，对设备可实现行动轨迹审计，软件下载控制、流量监测、上网行为管理等，必要时能够擦除设备数据，锁定设备等，防止设备盗用或恶意使用；

业务价值与方案优势

移动政务安全接入

基于互联网远程移动办公接入场景的业务访问需要，提供覆盖市面主流国产手机品牌系统的政务业务访问全过程安全防护体系

政务人员隐私保护

通过移动安全接入平台上架的应用，能够进行安全检测及 app 权限管理，禁止获取电话、短信、通讯录、wifi 等，阻止越权行为

政务数据国密传输

依据国家政务场景业务访问需要，提供从设备至业务系统间的数据链路安全保障，建立基于国密算法的安全加密隧道，保障数据传输链路的安全性

工作数据安全保护

针对移动政务业务产生的业务数据，提供安全虚拟环境，实现与个人数据有效隔离，内置安全阅读器，杜绝第三方软件调用带来的风险，保障工作数据的信息安全性

工作应用办公防护

结合数字水印技术，面向移动政务办公人员提供信息安全教育，震慑使用第三方工具拍照行为，实现对违规行为的事后追溯能力

设备统一安全管理

针对特殊业务部门的配发设备使用，提供严格管控措施，杜绝设备私用、链接非法无线、设备丢失等安全问题，实现统一管理，统一防护，严格执行的管理能力

一机两用联防联控

与政务外网一机两用解决方案形成联防联控，统一管理

政府行业IAM解决方案

国家信息中心	中央广播电视总台	安徽省大数据局	中山市政务服务数据管理局
深圳消防	四川司法厅	大连市公安局	肇庆高新区政府

需求来源

业务需求：由于政务应用规模的快速增长，且用户类型也呈现多样化，用户身份的维护以及权限的治理日益棘手，造成在流程效率、信息安全、管理方面的诸多风险。

安全需求：缺乏集中统一权限分配、有些账号多人共用容易造成安全漏洞；用户在使用系统过程中，经常需要在各系统之间切换，用户体验不佳。

管理需求：同统一的身份认证平台可以减少开发成本，缩短开发周期，降低系统的维护成本，有效防止安全事件的发生，提高管理效率。将应用的认证流程以及权限访问控制集中在一起，方便管理。同时为了兼容性，需要有能对接多种应用场景，复杂应用架构的能力，提供标准的认证集成方案流程。

解决方案

以联软科技零信任身份管理IAM系统为基础的《政府行业IAM解决方案》，以“用户管理、应用管理、权限管理、认证管理、审计分析、应用门户”六大功能组件，提供统一认证管理、统一组织架构、统一授权管理、统一审计管理、统一账号管理、单点登录等安全能力，实现以用户为中心实现账号的生命周期管理。

该方案包括

用户管理

- 包含数据源管理、组织用户管理、用户标签管理、用户自注册；数据源可以支持 LDAP 同步、API 同步、数据库同步、FTP 同步、Excel 导入等多种方式；组织用户管理，包含用户试图、用户管理等；

应用管理

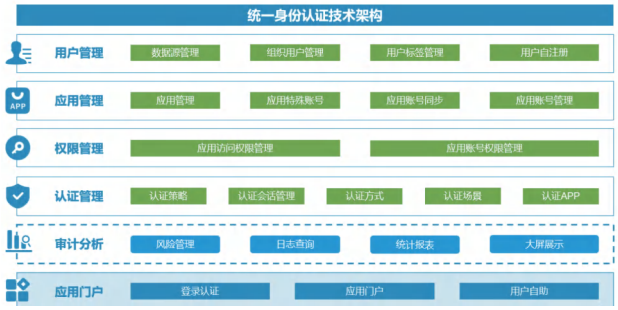
- 支持应用认证接入模板管理，提供应用增删改查、应用接入控制；应用账号管理：支持 IAM 主账号与应用从账户两种策略，用户主账号映射并关联应用账号，支持应用账号新增、导入、删除、绑定、解绑管理；应用账号同步，平台推送组织与账号到应用系统 LDAP、AD 目录、数据库、API 等，提供应用公共账号管理、授权绑定到个人用户，个人用户真实身份登录使用公共账号；应用特殊账号，支持应用多账户管理，支持应用账号委托，按用户（组）维度对应用授权，用于特殊用户授权；

认证管理

- 支持多种身份认证，多因素认证、分级认证，账密、短信，动态验证码认证、微信、钉钉、扫码、指纹等多种认证方式，支持单点登录，提升员工使用体验；

权限管理

- 通过配置授权级别、授权范围、授权功能与权限实现最小颗粒度授权，联软零信任身份管理 IAM 系统的动态授权是通过将 ABAC 和 RBAC 策略进行组合下发，达到灵活的访问控制基线的目的；



审计分析

- 支持身份分析，重复账号、僵尸账号、孤儿账号、违规账号，用户账号状态分析；行为分析，连续多次登录失败，短时间频繁登录，异地登录，非工作时间登录，同一 IP 多次不同账户登录，修改密码次数等。

业务价值与方案优势

业务价值

身份基础设施统一监控，统一认证身份设施割裂，内部多个身份源无法统一观察与监控；同时也能对这些身份基础设施进行加固；**内部风险控制**，对通用业务账号的多种数据维度自动建立基线持续调优助力业务风控安全

运营价值

解决当前运管存在相关痛点，身份凭据滥用，账号管理松散，密钥管理混乱极易引发安全问题规避；**检测滥用的权限**，确定用户任务所需的适当权限级别，监测高级权限使用，防止权限滥用

攻防价值

黑客入侵防护，从身份角度入手的安全检测能够从登陆验证的角度发现安全问题，以此为检测核心可极大的提高安全检测能力；协助护网演习，护网演习中身份权限常成为红队攻击的主要目标，如果身份基础设施遭到攻陷，会造成防守方的大量失分，ITDR 不仅能对身份进行监控还能对身份凭据进行安全防护，防止凭据落入攻击者手中

政务网数据安全交换解决方案

上海海事局	宁波海事局	信阳人力资源和社会保障局	明光市自然资源与规划局
中国民用航空管理局	河北省税务局	广东省税务局	江苏省税务局

需求来源

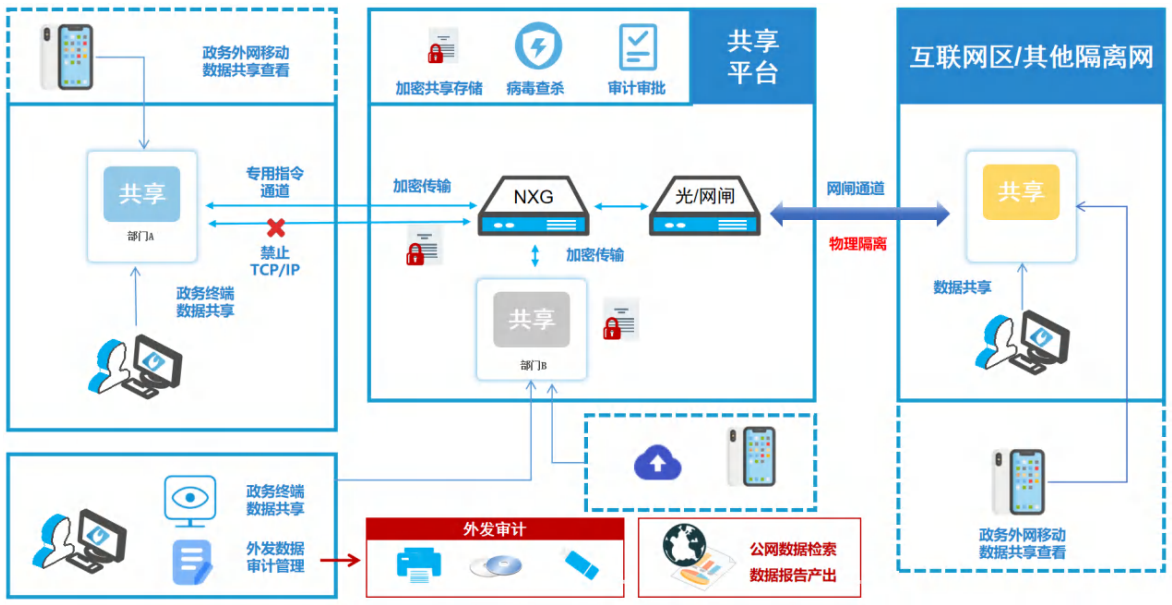
政策驱动:国家“十四五”规划提出推进政务信息化发展，同时针对网络隔离提出技术要求，包含《信息安全等级保护管理办法》以及《国家电子政务外网网络与信息安全管理暂行办法》，其明确提出不同网络间的隔离要求，要安全隔离且高效的信息交换，需实现各区域之间逻辑隔离和安全有效控制。

业务驱动:由于政务场景下存在互联网区、网管区、政务网区等其他分区分域情况，其产生大量政务敏感数据需要安全地进行跨域传输，故需构建一个安全的数据交换平台，实现电子政务外网业务在本地网络及跨网络间的数据安全传输效果。

场景驱动:在政务外网中，因一机两用建设禁止政务数据外发，但用户依然存在内部数据共享的场景，包括针对移动端建设也存在PC与移动数据共享查阅的场景。

解决方案

本方案以联软UniNXG+光/网闸组合为主，作为《政务跨网数据安全交换平台解决方案》，能够与《政务外网一机两用解决方案》形成联动方案，同时也能解决政务外网中多个隔离网之间的非结构化数据安全传输需求，可通过在多个逻辑隔离网之间部署UniNXG实现。



结构化数据

数据库数据交换

- 支持全库、全表、行列同步，单向和双向同步，主动同步异构数据库、字段同步、同步时间设置，内容过滤、病毒过滤；

流媒体数据交换

- 支持 TCP、UDP、RTSP、RTP、SIP、HTTP 等协议，HTTP 协议身份认证、双向或单向视频传输、实时数据传输、私有协议过滤、请求内容过滤、响应数据过滤；

非结构化数据

跨网隔离

- 虚拟化隔离技术实现多网间 IP 协议栈隔离，与网闸搭配符合物理隔离要求；

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）；

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；

在线操作

- 可实现用户在线编辑，在线预览，文件水印；

跨端共享

- 提供沙箱场景的终端和移动设备的文档共享平台，双端同步，实时查看。

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。单设备支持 2—8 个网络同时进行文件交换，多设备级联可满足超过 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

易用性强，贴合政务行业使用习惯，支持 B/S、C/S 及 H5 多种场景及访问方式，无需培训，易操作。可与现网统一认证对接，跨网运维和管理简单

集中管理、高效交换

可集群部署、集中管理，多个 UniNXG 安全数据交换设备或系统，可进行统一管理和策略集中配置下发。跨网文件交换速率接近网络带宽

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

政府行业跨网数据安全交换解决方案

中华人民共和国上海海事局	中华人民共和国宁波海事局	信阳市人力资源和社会保障局	明光市自然资源和规划局
中国民用航空管理局	河北省税务局	广东省税务局	江苏省税务局

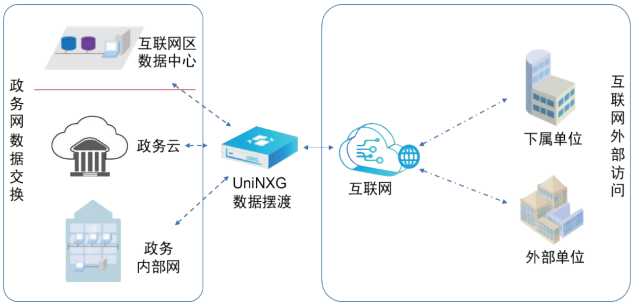
需求来源

政策驱动：国家“十四五”规划提出推进政务信息化发展，同时针对网络隔离提出技术要求，包含《信息安全等级保护管理办法》以及《国家电子政务外网网络与信息安全管理暂行办法》，其明确提出不同网络间的隔离要求，要安全隔离且高效的信息交换，需实现各区域之间逻辑隔离和安全有效控制。

业务驱动：政务行业内部存在内部业务与外部单位进行数据交换场景，但是由于没有较好的管控方式，数据的交换经常会带来病毒的感染，管理不严等问题，故需对内部的文件交换需建立更安全的能力建设，弥补当前业务场景下的安全风险。

解决方案

本方案以联软 UniNXG 数据安全摆渡平台为主，能够为各级政务部门内部多张逻辑隔离网间的数据交换提供安全的解决方案，部署简单，可通过一台设备实现多网交换效果。



业务交换

- 在业务大厅内部署UniNXG系统，业务需求者办理业务时通过外部的终端使用UniNXG往内部导入文件，政务人员通过UniNXG导出文件给业务需求者，如税务；

跨网隔离

- 虚拟化隔离技术实现多网间IP协议栈隔离，采用私有协议传输；

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）；

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。

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

易用性强，贴合政务行业使用习惯，支持B/S、C/S及H5多种场景及访问方式，无需培训，易操作。可与现网统一认证对接，跨网运维和管理简单

集中管理、高效交换

可集群部署、集中管理，多个UniNXG安全数据交换设备或系统，可进行统一管理和策略集中配置下发。跨网文件交换速率接近网络带宽

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

税务大厅场景覆盖

由于税务系统内部将终端U口全部封闭，从业务和安全考虑使用UniNXG既可以保证业务的便利性，也可以保证文件传输的安全性

政府行业消防配发移动设备管理解决方案

深圳市公安消防支队　　大连市公安局

需求来源

合规驱动：2019年11月12日，应急管理部下发《国家综合性消防救援队伍内务条令（试行）》第一百八十六条："第一百八十六条：基层单位人员在由个人支配的时间，可以使用移动电话。具体使用时机和管理办法，由支队以上单位结合实际制定"。

事件驱动：智能手机为消防队员日常工作训练提高带来便利，提升休闲生活质量，消防指战员使用手机和移动互联网连接的同时，也存在着访问非法网站、下载非法 APP 和涉赌、涉黄、涉黑、涉密、涉非法借贷等安全风险，手机安全管理问题制约着消防队伍的发展。

需求驱动：在原公安消防局发布《关于全面推进"智慧消防"建设的指导意见》、国务院安全生产委员会《"十四五"国家消防工作规划》等政策发文引导下，综合运用物联网、云计算、大数据、移动互联网等新兴信息技术，加快推进"智慧消防"建设。充分应用移动互联网手段加强执法监督、远程办公和指挥决策能力移动执法、移动办公、移动指挥信息化建设。消防系统安全性是重中之重，网络安全、应用安全、设备安全均需进行缜密设计，在广大消防员管理和工作中，免除安全方面的后顾之忧。

解决方案

本方案采用联软自主研发的UniEMM平台，为提供统一的移动端管理平台，在"云、管、端"三点构筑核心能力，为移动化管理提供端对端的整体运营解决方案。联软UniEMM系统采用成熟、可靠、安全和灵活的分层组件化技术架构，确保系统使用的稳定性、安全性及后续升级和扩展。

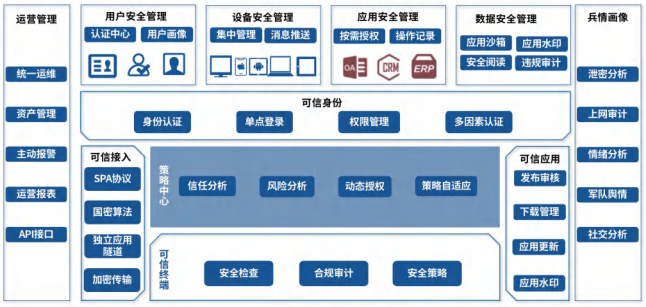
该方案包括

移动统一门户

- 提供移动设备的远程办公安全访问门户，并结合用户现有认证系统与本系统自身多因素认证体系（动态码、生物特征等）构建数据安全访问方式，实现用户通过门户进行统一登录后，访问消防移动办公业务；

零信任安全接入

- 消防移动办公业务系统部署于零信任安全网关后，通过零信任安全网关代理发布，不直接对外开放，隐藏在内网，实现业务服务及端口的隐藏，另外基于每个消防移动应用建立独立的安全隧道，保障远程数据访问的通信安全；



统一消防移动应用商店

- 以管理平台自身的业务全生命周期管理能力，灵活管理CS/BS/H5等消防移动业务应用，定义业务发布上线规则，确保每个业务系统在政务外网上规范化管理，确保基于用户身份进行业务访问的整体管理效果；

移动设备管理

- 提供MDM移动设备管理能力，支持移动设备生命周期管理，对移动设备提供设备级管理能力，可以对设备本身的硬件、软件功能进行限制，提供基于时间、位置以及扫码等构建的围栏策略，提供执勤工作模式，在消防员执勤工作时锁定在安全工作区；

移动数据安全

- 对消防移动业务应用产生的数据通过安全沙箱、水印等手段进行防护，用户基于业务系统下载的业务数据，保存在移动安全沙箱，与本地数据隔离，可通过安全浏览器或安全阅读器进行查阅，同时附加屏幕水印防护，预防拍照；禁止截屏，保护数据安全；

消防员态势感知

- 提供可视化态势综合分析能力，通过大数据建模，可智能分析、展示全体消防员总体思想态势，包含思想倾向、上网偏好、心理特征等以及有无红包赌博、交友情况等红色预警，管理者可及时掌控全局态势，及时遏制消防员违规倾向，实现新的互联网条件下消防员整体管理的技术支撑与手段。

业务价值与方案优势

融合零信任安全架构

采用零信任安全架构体系来保障业务安全，将政务外网服务器隐藏在安全网关之后，消防业务系统无需向互联网开放任何端口，保障应用安全，降低安全维护成本

移动业务数据安全保护

针对消防业务移动应用产生的业务数据，提供安全虚拟环境，实现与个人数据有效隔离，保障消防业务数据的信息安全性，并结合数字水印技术，面向消防队员提供信息安全教育，实现对违规行为的事后追溯能力

配发设备强管控、严管控

针对配发设备使用，提供严格管控措施，强制管控措施，实现统一管理，统一防护，严格执行的管理能力，有效规范消防队员使用行为，防止过度沉迷

统一可视化管理

统一可视化管理所有移动终端，掌握消防员配发手机使用情况，通过大数据分析平台对广大官兵的手机使用情况进行实时智能分析，为军队开展政工教育提供数据支撑和线索

政府行业5G专网零信任二次鉴权解决方案

国家信息中心	中山市政务服务数据管理局	安徽省大数据中心	深圳市大数据局资源管理中心	澳门博彩监察协调局

需求来源

业务需求：国家电子政务外网作为我国电子政务重要公共基础设施，是服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。5G技术具有高带宽、低时延、海量终端通信三大基本特征，正赋能促进政务信息化、数字化、智能化转型。5G基础设施布局、以5G专网为代表的创新技术发展基本成熟，足以支撑政务行业赋能，各地政府单位已开展5G智慧应用建设，如移动办公、移动执法、疫情防控、安防监控等场景，5G新技术的政务应用处于快速发展阶段。

政策合规：在政策推动方面，《“十四五”国家信息化规划》代表着由中央从顶层规划5G发展数字蓝图。国家大力支持出台包括《5G应用“扬帆”行动计划(2021-2023年）》在内的政策文件，其中各省市重点扶持5G政策文件574个，全国各地掀起了5G应用“扬帆”发展的热潮，各地政府纷纷结合当地实际需求和产业特色推出5G发展行动计划。同时，也对5G专网提出了很高的安全要求，例如十四五“国家信息化规划”中提出要强化5G网络安全保障体系；《广东省电子政务外网5G无线接入服务建设规范》中要求：5G无线网络应提供网络侧的二次认证能力，并应对接政务外网认证服务器，当5G无线网络核心网收到移动终端的业务请求时，触发用户二次鉴权。国家信息中心也于2022年7月1日颁布《政务外网终端一机两用安全管控技术指南》，5G专网作为政务外网组成的一部分也应该参考该标准要求，利用零信任技术，确保只有合法合规的终端才能接入到5G专网访问相应权限范围内的应用。

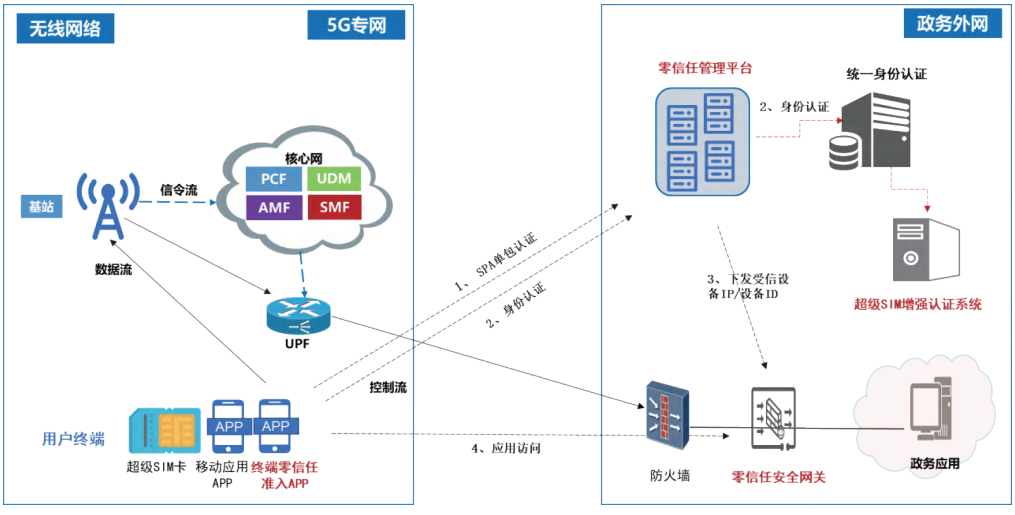
安全需求：5G专网带来高速、便捷的政务业务访问，同时也伴随着安全风险，这些风险来源于：

1）5G 专网二次认证安全风险：终端接入到 5G 网络时通过 5G 核心网 UDM 进行的鉴权认证成功后，获得 5G 专网网络资源，在访问电子政务网时不需要进行认证，存在安全风险。

2）5G 专网热点共享安全风险：终端接入到 5G 专网存在热点共享非授权访问风险，即 5G 专网手机开启 WIFI 热点，非授权终端能够通过该热点访问 5G 专网。

解决方案

以联软UniEMM企业移动安全管理平台为基础的《政府行业5G专网零信任鉴权解决方案》，采用零信任技术实现5G专网终端二次鉴权认证、移动数据安全等安全能力，也能够与政务外网一机两用解决方案形成联防联动，解决5G专网接入、局域网接入、互联网接入三大场景零信任安全接入，提供更全面的安全、更极致的体验、更高效的管理。



该方案包括

终端零信任准入APP/SDK

- 支持移动终端(Android、鸿蒙、ios),提供 SPA 认证;

零信任管理平台

- 提供控制平面的统一控制及管理能力。具备身份认证、终端管理、数据安全防护、动态权限控制、持续信任评估等能力;

零信任安全接入

- 终端接入 5G 专网访问政务外网办公业务时需要经过零信任安全接入认证,基于每个业务应用建立独立的国密安全隧道,保障远程数据访问的通信安全;

移动数据安全

- 对政务外网业务应用产生的数据通过安全沙箱、水印等手段进行防护,用户基于业务系统下载的业务数据,保存在移动安全沙箱,与本地数据隔离,可通过安全浏览器或安全阅读器进行查阅,同时附加屏幕水印防护,预防拍照;禁止截屏,保护数据安全。

零信任安全网关

- 为访问政务专网业务系统提供了统一的对外访问入口,终端访问内网应用必须经过零信任安全网关,并且与零信任安全网关之间通过安全隧道进行连接。所有的内网业务均隐藏在安全网关后面,通过零信任安全网关统一对外发布,实现远程接入场景下,业务系统的隐藏,同时通过 SPA 预认证技术,实现安全网关本身对外的端口隐藏,有效防止被扫描攻击;

统一认证

- 系统支持与省统一身份认证平台对接,实现普通用户账密认证、短信认证、粤政易扫码认证。也支持与运营商超级 SIM 认证系统对接,实现手机 SIM 认证;

政务业务管理

- 以管理平台自身的业务全生命周期管理能力,灵活管理 CS/BS/H5/ 等政务业务应用,定义业务发布上线规则,确保每个业务系统在政务外网上规范化管理,确保基于用户身份进行业务访问的整体管理效果;

业务价值与方案优势

固移一体化

一套系统管理 PC 终端、移动终端,节省投资、简化运维

有效隐身

基于 SPA,解决业务扫描带来的安全风险,实现 5G 专网网络及资源的“真”隐身

数据安全

集数据沙箱、水印、应用行为管控(复制 / 截屏 / 分享等)于一体的数据保护能力,实现多场景下的数据安全保护

统一兼容

覆盖各类操作系统:Android、iOS、鸿蒙、Windows、macOS、Linux、UOS、银河麒麟,实现统一管理

落地经验

具备国家信息中心、安徽省大数据局、深圳市政数局、中山市政数局、澳门博彩监察协调局等政府客户丰富落地经验

安全策略管理解决方案

上海市嘉定区行政服务中心	三一集团有限公司	中国银行股份有限公司江苏省分行	广州农村商业银行股份有限公司
齐鲁银行股份有限公司	广州农村商业银行股份有限公司	安徽环新集团股份有限公司	复旦大学附属中山医院老年中心

需求来源

随着电子政务网络规模的扩大，政务应用场景不断增加，网络环境更加复杂。为了保障电子政务外网安全性，采用更先进的安全技术和设备，如防火墙等安全设备，来保护网络免受攻击和威胁。电子政务外网的安全性得到了增强，安全运维压力也相应加大，由于防火墙以及路由交换设备日益增多，形成跨多个区域、多个机房、多层级的复杂局面，安全策略控制的粒度日趋细化严格，导致运维效率低、出错几率大。

许多政府单位目前对安全策略的管理缺乏有效的手段，使得安全策略处于“不可见”的状态，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，给系统安全与稳定性带来隐忧。

解决方案

通过联软至赛 UniNSPM 安全策略管理平台的部署与建设，协助政府用户对防火墙的安全策略进行梳理，分析，下发验证以及可视化运维，将大大提高工作人员运维效率，且满足国家法规规定的防火墙网络设备管理要求。

UniNSPM 的管理对象主要为政府单位运维组如：防火墙管理运维组，网络运维组，安全运维组，以及存有涉及所有网络变更需求的人员。管理网络设备范畴涵盖三层交换机，路由器，防火墙等三层级的网络设备。主要涉及的内容为对所有的三层级网络设备防火墙进行管控，提供策略集中管理，策略梳理，策略可视，策略运维的能力。

方案效益

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；

自动计算

- 对于开通工单，平台可以自动计算路径判断是否已有策略放通，没有放通的定位设备给出规划建议和脚本；

跟踪配置变化

- 记录设备的变更情况，对不同配置版本进行比较跟踪管理，帮助管理员及时了解配置变化详情；

集中管理

- 纳管现网所有防火墙、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，通过人为清理无效策略很难落地，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；

黑名单监控

- 根据业务定义不同的逻辑安全域，计算域间的放通情况，对不允许的定义黑名单，不断进行监控。

政府行业网络空间资产测绘方案

中山市政务服务和数据管理局 | 深圳市信息安全测评中心 | 湖南省电子信息产业研究院 | 坪山区人民政府

深圳市综合交通设计研究院 | 中国信息安全测评中心广东测评中心 | 南方科技大学

需求来源

政策驱动：习总书记2016年4月19日在国家网信工作座谈会上发表的重要讲话中指出，要加强关键信息基础设施保护，感知网络安全态势是最基本最基础的工作。要全面加强网络安全监测，摸清家底，认清风险，找出漏洞，通报结果，督促整改。

安全需求：解决各单位网络攻击面安全管理中关键的资产种类复杂、资产变动感知滞后、数字资产监控缺失、安全事件响应难等核心问题的有效解决；

管理要求：形成政务网络空间资产台账，聚焦政务资产风险相关痛点场景的治理、构建指标化安全运营的技术与服务基础。

解决方案

本方案以 EASM 外部攻击面管理系统与 CAASM 网络资产攻击面管理系统为基础，以攻击者视角自动化对各政务部门的互联网及内网资产进行发现与测绘，持续风险监控，结合安全情报，安全服务团队支持，形成综合性安全运营，能够帮助各政务部门提供基础安全数据支撑，在网络攻防中能够真正化被动为主动。

影子资产精准监控

- 通过平台化的风险监测与搜索引擎，基于文字线索、图形线索等组合方式，为用户自动搜索整个互联网空间，输出高价值疑似、仿冒资产数据，实现影子资产监测的常态化、自动化，大幅降低未知资产或未知风险被通报的风险；

数字资产全面可见/统一纳管

- 根据主域，利用机器学习算法、分布式扫描自动发现暴露在互联网上的全部数字资产，包括域名、Web 网站、证书、中间件、公众号、小程序等，帮助用户清楚地了解在互联网的全部数字足迹，实现“新型资产，统一纳管”；

内网资产安全管理

- 通过部署内网探针，采用“主动探测”+“被动流量发现”+“资产适配器”等多种技术手段实现摸清家底，大大缓解碎片化问题；采用图数据库引擎呈现实时的脆弱资产关联，进行攻击路径推演，实现真正的挂图作战！

漏洞深度检测与响应

- 具备强大的 POC 插件检测能力，支持 0day/1day/Nday 漏洞的精准、无害化扫描与验证，针对性漏洞排查全网可在 2 小时内完成，提供单个 / 多个漏洞一键复验；

敏感数据全网监控

- 基于用户提供的关键字或关键字组合，通过自研监控引擎及第三方数据集成，智能生成监控字典，对开源社区、网盘文库、暗网交易平台进行全面监控，快速发现泄露的信息或文档，协助用户下架闭环；

资产全景视图

- 针对采集的资产信息，进行可视化展示，从“IP 资产”、“Web 资产”、“Poc 漏洞”等多个唯独进行基础数据展示，针对资产变化趋势进行时间唯独显示，实现资产信息展示、关联信息展示、风险状态展示。

IT与数字资产台账监控

资产暴露面详情，创建平台化资产台账，自动持续监控，平台化用户自助服务，实现资产、风险和变化一目了然

监控敏感信息泄露，避免合规与入侵风险

安全类数字化资产风险监控，搜索开源社区、网盘、互联网文库上泄露的敏感信息，以及暗网渠道非法交易信息，配合运营团队协助用户处置敏感信息泄露，规避风险

持续漏洞发现及风险预警

持续扫描互联网暴露面安全风险，覆盖安全漏洞、弱口令、风险端口等，专业运营团队验证并基于优先级预警通告

漏洞情报驱动精准预警

基于资产台账，提供最新高危漏洞的精准预警，以及漏洞应急响应的技术支持

政府行业信息安全等级保护适配解决方案

中央环境监测总队	湖北省公安厅	河北省财政厅	潮州市政数局
湖南省监狱管理局	江苏省税务局	中国城市规划设计院	深圳市交通局

需求来源

政策背景：自1994年第“147号令”，我国开始实施信息系统等级保护。十几年来，在政府、金融、能源、电信、医疗卫生等多个行业都已深耕落地，但是随着云计算、大数据、物联网、移动互联以及人工智能等新技术的发展，等级保护1.0已无法有效的应对新技术带来的信息安全风险，为了满足新的技术挑战，有效防范和管理各种信息技术风险，提升国家层面的安全水平，等级保护2.0应时而生。《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

解决方案

为落实“分等级保护、突出重点、积极防御、综合防护”的总体要求，联软科技提出了基于可信数字网络架构的等保适配解决方案，可协助政府机关建立一体化的网络安全综合防御体系，积极防御，同时满足云计算、移动互联、工控系统、物联网提出安全扩展要求。

一、安全区域边界

网络接入控制

- 通过 UniNAC 不但能够对非授权设备私自联到内网的行为进行检查或限制，还能适应有线、无线、VPN 等复杂网络环境，并对提供多重高可用设计，可大幅提升系统可靠性；

非授权外联

- 通过 UniAccess 非授权外联功能可对内部用户非授权连接到外部网络的行为进行检查、预警和阻断，如 WIFI 热点等；

移动接入控制

- 针对移动终端，通过 UniEMM 不但对接入终端和服务节点采用双向认证，并可保证跨界的访问仅可通过安全网关受控接口进行通信，并采用密码技术保证通信过程中数据的完整性和保密性；

资源访问控制

- 可联动所有主流网络设备动态下发访问控制策略（包括源地址、目的地址、源端口、目的端口、协议等），仅允许受控端口通信拒绝其他所有；也可通过边界网关支持动态访问控制策略，仅允许受控接口通信，拒绝其他所有通信；

访问控制列表最小化

- 通过数据安全摆渡设备实现数据安全交换，实现防火墙 / 网闸访问控制列表最小化；同时管理后台集中管理访问控制策略，可在后台删除多余 / 无效的访问控制列表，确保访问控制列表排序合理；

外部网络攻击行为

- 可在关键网络节点处通过网络智能防御设备及时发现网络扫描、挖矿、漏洞利用等网络攻击行为，可向管理员预警，也可联动防火墙阻断恶意 IP 或域名；

内部网络攻击行为

- 可在网络关键节点部署网络智能防御设备，及时发现设备仿冒、IP/MAC 伪装连接、异常访问、异常接入位置等异常行为，并可向管理员预警或联动准入阻断失陷主机的横向攻击行为，避免风险扩散；

新型网络攻击行为

- 通过智能欺骗技术，高仿真内网真实设备或服务，可捕获新型网络攻击行为，并分析预警或联动准入、防火墙等设施阻断风险，避免扩散；

恶意代码防范

- 通过数据安全摆渡设备可防止外网感染恶意代码的文件导入内网，另外可确保格力情况先，失陷恶意代码库在线或离线更新；

安全审计

- 可对本地或远程每个接入的用户进行安全接入审计，也可对仿冒接入、非法外联、DDOS 攻击等安全事件进行审计，审计记录包括日期事件、用户、事件类型、事件是否成功等信息，可留存备份。

二、安全计算环境

1、PC终端安全

安全检查

- 通过 UniAccess 对账户身份身份进行验证，可发现系统中是否存在默认账户，并可禁止或删除默认账户，同时通过安全检查可对终端上的恶意软件进行检查，对恶意代码库是否及时更新进行检查；

安全审计

- 通过 UniAccess 可对终端邮件、打印等各种外发通道实现管控、审计和阻拦，同时通过 UniDLP 更可发现外发通道中传输的敏感信息，针对敏感信息留存审计记录；

入侵防范

- 通过 UniAccess 标准化管理功能科对终端软件进行卸载或安装，服务、端口、共享禁用，可管理终端 IP 地址，防止用户或黑客程序修改 IP 或 MAC 等

可信验证

- 通过 UniAccess 可对可信区域模板机提取程序、程序目录下所有文件、程序安装过程中产生文件的 MD5 值，并存储在管理服务器上，终端计算机仅能运行 MD5 库中经过验证的程序。

个人信息保护

- 通过 UniDLP 可禁止未授权访问和非法使用用户个人信息。不因失窃等泄露个人信息和机密信息。控制各种客户信息、业务敏感数据等多种泄露途径，从而防止数据外泄。

2、移动终端安全

边界防护

- 边界部署接入网关，对通过无线接入的终端进行双向接入认证，并实现动态资源访问控制。

入侵防范

- 能够发现非授权移动终端的接入行为，并能够阻断非授权移动终端接入；另外，能够检测无线接入设备 SSID 广播、WPS 等搞风险功能的开启状态，并可关闭这些存在的高风险功能。

移动终端管控

- 可检查并强制移动终端安装、注册并运行移动终端客户端软件，并可对移动终端进行远程控制及设备全生命周期管理，如远程锁定、远程数据擦除等

移动应用管控

- 通过应用商店可选择用户需要的应用安装并运行；可在移动终端只允许指定证书签名的应用软件安装和运行；提供软件白名单功能，通过白名单功能控制应用软件安装和运行。

安全建设管理

- 通过后台发布软件，确保软件来自可靠分发渠道；可确保软件由指定的开发者开发；可对应用软件开发者进行资格审查，审查通过后软件签名发布，管理平台可确保签名证书合法性；

安全运维管理

- 可建立无线接入设备和合法移动设备配置库，并通过配置库识别非法设备。

3、资产探测及漏洞检测

访问控制

- 可针对互联网资产和内网资产，执行弱口令检测扫描，识别出操作系统、网络设备、安全设备、数据库、中间件等系统存在的默认口令（弱口令账户），及时整改。

入侵检测

- 可针对互联网资产和内网资产，执行资产探测、端口服务识别，发现目标系统开放的不需要的系统服务、默认共享和高危端口。通过漏洞扫描功能，发现可能存在的已知漏洞，并提供漏洞结果的 POC 验证信息，协助安全人员确认漏洞的真实性，为整改提供帮助。

审核和检查

- 通过可执行周期性扫描检测任务，及时发现互联网或内网存在的漏洞，并可导出数据、生成风险扫描报告，留存以备等级保护测评检查。

上线前安全测试

- 在上线前，利用系统扫描功能、集成扫描能力，统一调度上线前安全性测试的扫描任务，进行上线前的系统层和 Web 应用层漏洞扫描，并出具安全测试报告。

漏洞和风险管理

- 通过建立周期性的扫描任务，完善最新全量资产库。执行常规漏洞检测可识别已知安全漏洞，并推动修补整改。在高危漏洞爆发 / 重大安全威胁时，可根据漏洞 / 安全情报，执行快速排查和 POC 扫描检测，完成精准识别，协助修改。另外，管理员可以通过持续扫描，跟踪漏洞修复进度、更新状态，实现闭环管理。

业务价值与方案优势

安全区域边界

确保只允许合法、合规用户接入，同时实现访问控制列表最小化，并可有效检查或控制非授权内联、非授权外联等行为，最大限度满足等保 2.0 测评要求

安全计算环境

可实现 PC 终端、移动终端等多种计算机环境的安全，满足身份鉴别、账号管理、入侵防范等合规需要，并可通过标准化管理、安全检查等功能，确保主机安全可控，程序可信

资产识别管理

统一识别和管理服务器、终端、网络等设备基线和漏洞，保护核心资产，提高管理员运维效率

异常行为可管

不依赖黑白名单，实现外部攻击行为、内部异常行为，新型网络攻击行为可管可控

数据安全可控

提供敏感内容识别、屏幕与打印水印、数据内部安全流转、数据授权外发、泄密追踪溯源等数据保护技术，确保个人隐私数据可控

智慧洞察安全

基于 AI 的深度分析和全景安全展示，真正做到用户可见、行为可控、风险可视、响应及时

软件正版化管理解决方案

需求来源

合规及正版化管理要求：国务院办公厅印发的《政府机关使用正版软件管理办法》和《2016年全国打击侵犯知识产权和制售假冒伪劣商品工作要点》，以及国家版权局办公厅印发的《正版软件管理工作指南》，为指导各级机关和单位开展正版软件管理工作提出了建议和要求。

企业软件安全使用管理要求：企业用户终端私自安装未授权软件会面临被软件厂商起诉的风险，从互联网上下载的软件可能携带“全家桶”，导致机器卡顿，破解软件带有病毒或者自身带有恶意代码，无法从源头上保障安全。

解决方案

以联软科技主机监控与审计系统为基础的《软件正版化管理解决方案》，能很好地满足企业自身的软件正版化和标准化要求。

该方案包括

终端软件资产台账管理

- 资产自动统计，快速检索查询；

软件安装、卸载权限管控、行为审计

- 记录相关情况，管理用户私自在计算机上安装或卸载软件；

终端标准化管理

- 支持对终端已安装软件进行违规审计、提醒、卸载；

软件使用时长统计

- 作为采购或运营支撑；

方案兼容性强

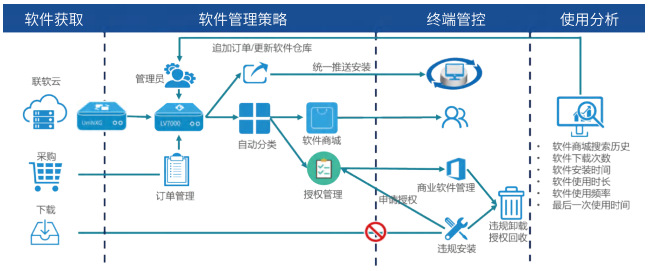
- 同时支持对信创终端的软件正版化、标准化管理。

企业软件采购订单管理

- 录入相关信息，支持导出台账，软件使用授权管理；

企业软件仓库

- 作为企业软件获取安全受控唯一通道，支持手动维护，支持云端软件仓库自动或手动同步更新获取服务；



业务价值与方案优势

该方案能全面满足正版化管理要求，相比传统方案：

AppStore应用商城体验安全、高效

在严格管控终端软件安装权限的同时，提供安全、便捷获取软件的入口，避免互联网不安全软件的下载安装使用，也提升终端用户办公效率

保障软件供应链安全

从源头上解决终端软件的安全问题，阻止流氓软件等的安装

软件使用分析

提供软件安装列表、软件使用时长审计等采集信息，能够帮助企业获取终端用户软件使用的实际情况，为运营、采购等提供数据支撑

信创终端安全一体化解决方案

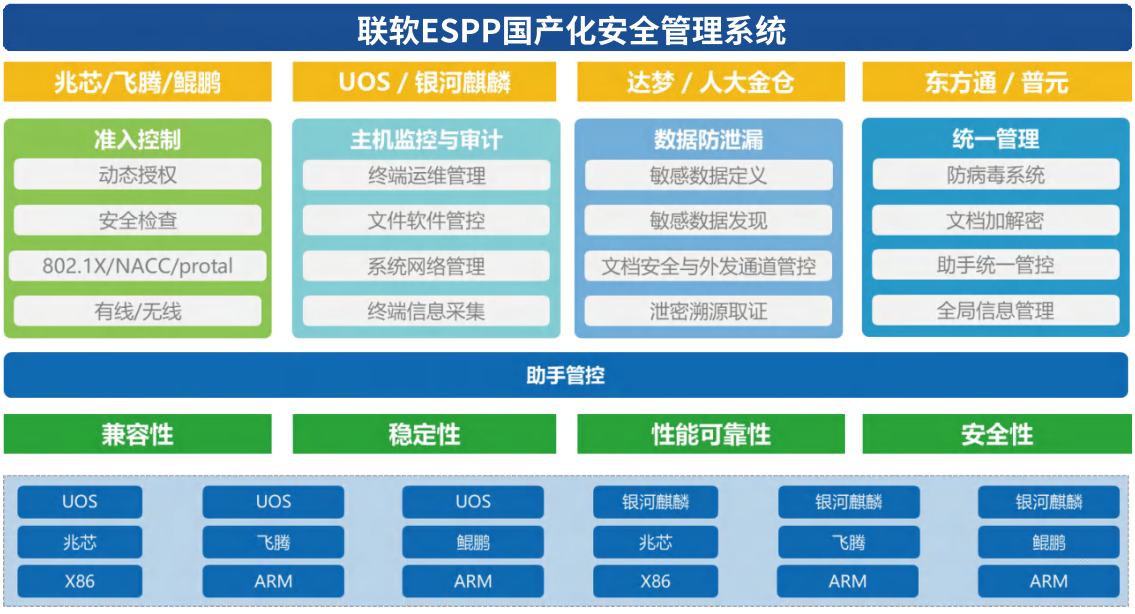
需求来源

信创产业发展：信息系统国产化的浪潮中，国产操作系统新的安全框架与传统的安全管控工具不匹配，成为单位整体安全防护体系的漏洞，信创终端安全面临考验。

信创终端一体化，安全建设规划需求：信创与非信创终端下面临病毒、恶意软件、内网用户私自访问外网、违规终端私接内部网络、终端敏感数据外发等风险，需要构建信创终端安全一体化管控平台，提升整体安全防护能力和运营效率。

解决方案

联软科技已经完成与 UOS、麒麟等信创操作系统，龙芯、兆芯、飞腾、鲲鹏、X86 等各类国产芯片，国产化数据库与中间件的适配，并拥有大量成功应用案例。以联软 ESPP 国产化安全管理系统为基础的《信创终端安全一体化解决方案》，能够帮助单位建立信创终端安全一体化管控平台。



该方案包括

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。

终端接入可信

- 杜绝非法接入、实现信创终端合规入网、权限可控，落实单位安全规范制度。

终端安全加固

- 提升信创终端自身防护能力，完善终端安全基线配置，加强桌面安全加固与标准化管理。

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。

数据防泄密

- 敏感文件识别与外发控制、行为审计溯源管理、文档安全、屏幕水印防扩散，有效避免数据泄密。

终端一体化

- 一个平台、一个 Agent，实现网络接入控制、终端安全管理、数据安全防护、终端运维支撑等多样化安全能力。

业务价值与方案优势

统一终端管理

一个管理平台和一个客户端便可实现整个方案的所有功能，整合多种防护技术，从顶层入手进行体系化建设，避免重复投资，实现信创终端与传统终端统一管理

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

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

方案完整，功能性强

从准入控制到终端管控，从内容识别到数据保护，从行为分析到泄密预警，从已知风险管控到未知威胁发现，平台整体功能性强

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；

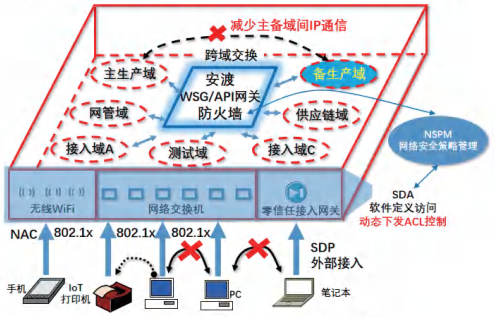
分域和跨域访问控制（防火墙/NXG/WSG/API）

- 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

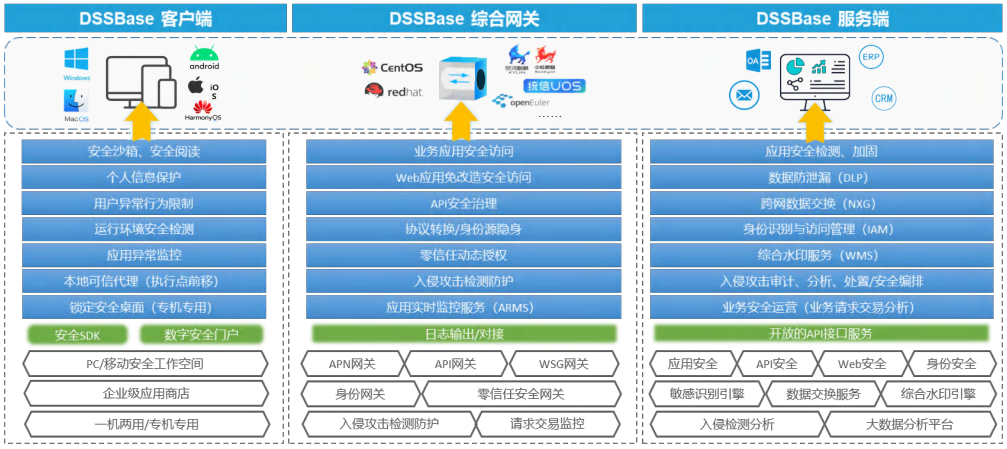
数字化应用安全要求：业务存在入侵风险、数据存在泄露风险、设备管理困难、传统VPN使用体验差、安全合规要求加强。

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