联软科技
LEAGSOFT

央国企能源
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+

企业级安全开放市场领先

安全管控终端数量
超过 15,000,000+

国家主管部门认可

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

持续领先

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%

合作典范

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

央国企行业商业秘密保护解决方案

需求来源

合规驱动：《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的颁布执行，推动央国企加强数据安全管理；

技术指引：国资委发布了《中央企业商业秘密安全保护技术指引》，明确中央企业应根据自身商业秘密数据安全管理的实际情况，建立商业秘密安全管理规范；

风险推动：构建符合当前数据安全场景与管理需求的数据安全防护体系，是保障企业商誉与商业机密的重点方向，也是规避数据安全风险的核心工作；

解决方案

联软商业秘密保护解决方案由联软 ESPP 企业安全监测保护平台为核心，基于包含《技术指引》等相关指导文件，结合文件 DNA、文件聚类等数据敏感规则梳理工具，形成商密数据定义规则，基于实际数据保护场景与规划，形成以商密非结构化数据全生命周期保护体系。

商密数据识别

结合商密数据定义与识别规则，进行整体商密数据的安全防护与运营管理，提供非结构化数据的全生命周期数据安全保护能力；

非结构化数据保护

根据用户制定的商业秘密管理规范和定密要求，结合智能规则、业务系统下载等多种数据加解密管理，提供数据落地安全防护，并可结合办公环境提供文档管理模式的切换；

商密终端安全管控

通过商密网终端安全接入管理与终端安全运营管理能力，保证商密网内信息系统安全保护，实现网络安全、终端安全、移动存储介质安全、打印刻录安全等能力，并可结合终端环境进行网络资源访问管理；

商密数据流转管理

用户在商密网内进行业务系统访问与文件操作时，针对各类文件外发通道进行审计与内容检测，并提供包括矢量、盲水印在内的多种屏幕 / 打印水印技术，针对潜在的截屏、拍照、打印等数据外泄行为进行安全意识教育与事后追溯能力。

业务价值与方案优势

以数据安全核心
方案以企业商业秘密的安全为核心目标，实现对商业秘密非结构化数据全生命周期管理与安全保护，同时能够满足个性化场景、业务流程的特殊要求

合规、有效、可操作
方案经过实际项目建设验证（为国资委示范项目），满足商业秘密建设安全要求

一个方案，两个达标
商保、等保两个安全体系充分融合，通过一次建设，商保达标、等保合规，避免重复投资，减少工期，减少投入

广泛的适用性和扩展性
方案能够满足用户个性化业务或流程需要，模块化功能扩展体系，快速满足新的安全需求

部署简单、稳定高效
方案中所使用的安全产品均为业界领先的成熟产品、经历过大规模、长期用户实践

央国企能源行业终端安全一体化解决方案

需求来源

合规要求：落实网络安全法、安全等级保护条例与关基安全保护等合规性要求，保障企业内部终端资产的安全管理；

信创推动：自主可控的建设推动下，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；

管理挑战：应对终端安全运营中面临的安全挑战，解决正版软件管理、数据安全管理及网络边界保护等客观需求；

解决方案

本方案以联软 ESPP 企业安全监测保护平台为基础，帮助企业建立一个实现企业内部终端安全保护、运维管理及数据保护的一体化管控平台，解决企业计算机入网合规性和安全管理等问题，提供包含网络准入、桌面管理、数据防泄密、文档安全、终端检测与响应、防病毒等功能。同时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。

统一管理

一个平台实现信创终端与传统终端的统一安全管理，保障信创终端稳步替换过程安全无风险；

资产“可信”

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，确保接入终端“可信”；

终端“可管”

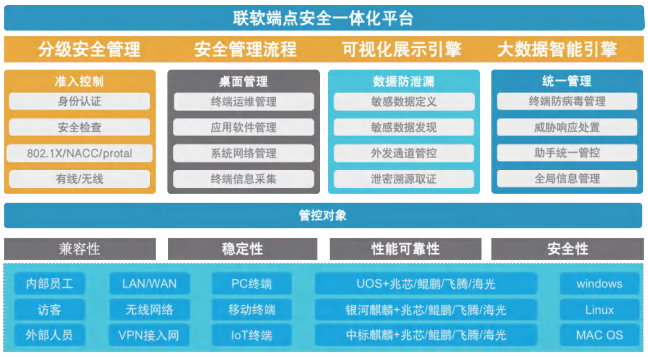
终端桌面管控，涵盖终端安全基线完善与加固、终端标准化管理、软件正版化管理、运维简化管理，确保内部终端“可管”；

一体化管理

一体化客户端与管理后台，实现从网络准入控制、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；

终端“可防”

多样的数据类型采集，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；



数据“可控”

对企业数据在创建、流转、存储、使用、外发、互联网传输等阶段进行场景化数据防泄密管控，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，确保数据“可控”。

业务价值与方案优势

满足监管要求

关键基础设施单位的信息安全建设势必会考虑国家网络信息安全监管要求。终端一体化安全管理平台系统符合国家信息安全监管要求

减轻运维压力

实现全网终端设备的集中管理，使得企业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

终端与数据安全保障

可有效地对终端进行安全加固，减少终端安全风险。基于数据安全管理，实现有效保护企业敏感信息，降低数据安全风险。对入网终端提供接入安全管理，提升网络边界安全

兼容性强，稳定性高

与国内主流信创操作系统、国产芯片、中间件、数据库等进行深度适配，与办公软件、业务软件、浏览器、安全软件之间的兼容性强，确保在各类系统 / 平台上均能构建安全管理能力

央国企能源行业数据安全交换方案

需求来源

业务驱动：便捷高效的实现跨网数据传输，满足最终用户的多种使用场景，整体易用性强，使用简单；

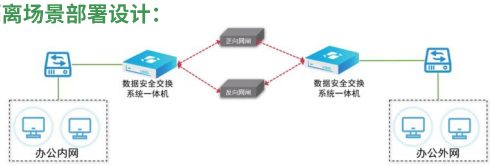
安全需求：对数据进行内容识别与安全检测，确保跨网数据传输不打破现有安全边界，避免出现病毒跨网传播风险，并可实现全流程审计与审批管理；

管理要求：建设与管理成本低，避免U盘等传统方式带来的运维压力，可提供灵活的审批方案设计，支持与现有OA类系统对接，实现统一的审批管理；

解决方案

本方案以UniNXG数据安全摆渡系统为基础，部署在办公内网与外网之间，作为内网终端与外部网络终端的文件安全交换平台，同时配套电力级安全隔离装置，在满足办公和业务对文件交换需求的同时，实现物理与逻辑隔离场景下的文件流转审批及杀毒管理，降低病毒感染和数据泄密的风险。具体如下：

物理隔离场景部署设计：



逻辑隔离场景部署设计：

全网络隔离

基于虚拟化技术实现网络隔离和协议适配，可提供一体化产品解决逻辑隔离部署要求，也可搭配电力专用正反向安全隔离装置，实现物理隔离下的网间数据安全交换；

集成防泄密

基于数据敏感性检查实现文件交换中的数据防泄密管理，结合文档跟踪能力，实现数据泄密追溯；

详尽的审计

支持详细的用户登录、行为审计和内容审计；

灵活的审批

支持对文件的多级审批和多种审批模式；

防病毒强大

支持第三方防病毒/木马引擎，支持多款防病毒软件异构杀毒；

集中化管理

支持对企业中的所有交换平台进行统一管理和配置策略集中下发；

人性化操作

用户界面类似网盘，支持B/S和C/S模式，用户无学习成本，无需培训；

便利化集成

支持与第三方邮箱/存储/办公平台整合，便于统一认证/部署/管理；

双向外链传输

支持外联分享与敏感识别进行联动，实现分享审计审批等安全管控；

兼容性全面

系统支持后台全栈信创和非全栈信创，用户可根据实际情况选择信创配件；系统客户端支持信创操作系统和非信创操作系统安装部署。

业务价值与方案优势

数据传输安全可控

数据交换的整个过程安全、受控，交换前有病毒木马查杀，交换中有完整的授权、审批及防泄密机制，交换后有详尽的审计记录和内容备份

部署便捷

软硬件一体化，无需前置机，维护简单，购置成本和运营成本（维护、电力）极低。部署简单，设备简单配置后，便能实现网络间的安全数据交换

提升效率

提供安全的文件分享、文件外链和公共目录的功能，支持协作办公，极大提高办公效率

满足合规

满足监管单位的相关合规性要求

央国企能源行业移动办公安全解决方案

中国南方电网 CHINA SOUTHERN POWER GRID 南方电网数字电网研究院有限公司 | 中国电信 CHINA TELECOM 江苏、安徽 湖南、海南 | H3C 数字化解决方案领导者 | 中国石油 陕西销售公司

需求来源

业务驱动：随着 5G、物联网时代的到来，移动与远程办公成为办公与运营的新常态，便捷迅速地实现移动办公成为业务发展的突出方向；

安全要求：实现移动办公业务的基础上，对收缩互联网暴露面，保护移动应用和数据安全，对业务流量通道加密需求；

管理需求：央国企行业互联网出入口收敛等工作的推动下，对于提供移动办公的技术平台提出更高要求，在确保业务应用的前提下符合相关指导工作的管理要求；

解决方案

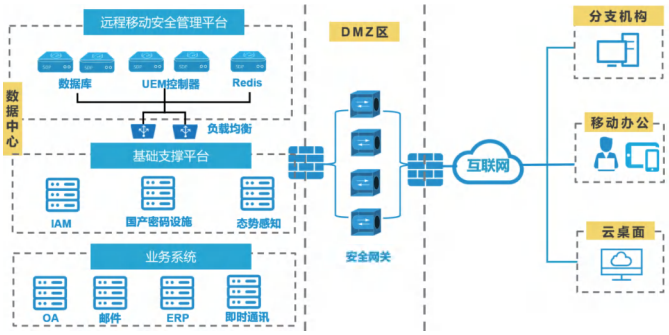
本方案以联软 UniSDP 零信任访问控制系统与 UniEMM 企业移动安全管理平台协同应用作为远程移动办公安全管理系统，境内数据中心内部署管理平台与安全网关，作为远程访问设备的统一管理平台，提供远程设备、业务应用与数据安全防护相关功能。通过覆盖 PC 与移动端的零信任安全防护体系，构建远程办公场景下使用数据过程中的设备、身份、数据、通信管理能力，整体平台部署具体如下：

远程业务访问

提供覆盖 PC（无客户端及有客户端模式）与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；

安全接入管理

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；



业务全生命周期管理

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/ 原生应用，确保基于用户身份进行业务访问的整体管理效果；

远程办公数据安全管理

以安全沙箱为基础，配合数字水印技术，确保远程办公使用数据时的数据防泄密与防扩散管理，避免工作环境不可信或设备失控情况下出现的数据泄密风险。

业务价值与方案优势

统一安全平台

基于远程移动办公场景的业务访问需要，提供覆盖境外 PC 与手机终端至企业内网业务系统的全过程安全防护体系

数据传输安全

面向跨境场景的业务访问需要，提供从终端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

保障数据信息安全

针对远程业务开展时终端与内网业务系统所使用的数据，提供安全虚拟环境，保障企业数据的信息安全性，并结合数字水印技术，实现对违规行为的事后追溯能力

终端安全加固

面向远程终端资产，提供安全评估机制与设备管理能力，避免端点安全风险影响远程移动办公业务与系统安全性

央国企行业境外数据保护解决方案

中国中原对外工程有限公司 China National Nuclear Corporation Overseas Ltd. CNNC

中国交建 CHINA COMMUNICATIONS CONSTRUCTION

需求来源

业务驱动：便捷地实现境外办公场景的业务访问与数据使用，为涉外移动业务推广提供助力，降低移动化业务的改造成本；

安全需求：确保境外接入场景下的资产安全管理，屏蔽潜在的安全风险，针对境外业务访问产生的数据安全风险实现有效管控；

管理需求：建设与运营成本可控，可持续为后续业务扩展发挥价值，投入产出比高。

解决方案

本方案以联软 UniSDP 零信任访问控制系统与 UniEMM 企业移动安全管理平台协同应用作为境外数据安全保护系统，境内数据中心内部署管理平台与跨境安全网关，作为境外访问设备的统一管理平台，提供数据安全防护相关功能，并提供可信跨境数据访问平台。通过覆盖 PC 与移动端的零信任安全防护体系，构建境外场景下使用数据过程中的设备、身份、数据、通信管理能力，整体平台部署具体如下：

境外业务访问

提供覆盖 PC 与移动设备的境外安全访问门户，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；

安全接入管理

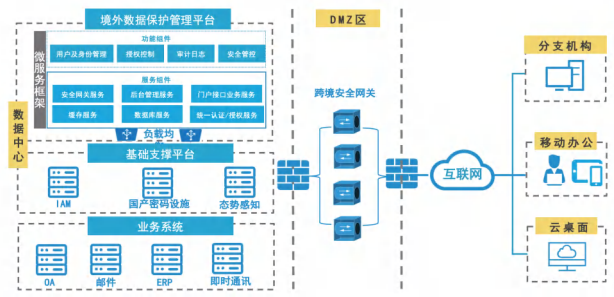
基于每个业务应用建立独立的国密安全隧道，保障境外数据访问的通信安全；

业务全生命周期管理

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/ 原生应用，确保基于用户身份进行业务访问的整体管理效果；

数据跨境防护

以隐身侠作为终端文件保险箱（双重加密空间），提供终端数据跨境防护能力；



境外数据安全管理

以安全沙箱为基础，配合数字水印技术，确保境外使用数据时的数据防泄密与防扩散管理，避免工作环境不可信或设备失控情况下出现的数据泄密风险。

业务价值与方案优势

面向跨境场景提供统一安全平台

基于跨境场景的业务访问需要，提供覆盖境外 PC 与手机终端访问国内业务系统的全过程安全防护体系，提供跨境文件保险箱

结合国产密码技术 构建跨境传输安全体系

面向跨境场景的业务访问需要，提供从终端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，保障跨境数据传输链路的安全性

构建境外办公数据安全能力

针对境外业务开展时终端与国内业务系统所使用的数据，提供安全虚拟环境与文件保险箱，保障企业数据的信息安全性，并结合数字水印技术，面向境外人员提供信息安全教育，实现对违规行为的事后追溯能力

提供境外办公终端安全管理

面向境外终端资产，提供安全评估机制与设备管理能力，避免端点安全风险影响境外业务与国内业务系统安全性

央国企能源行业全网零信任解决方案

◈ 需求来源

业务驱动：随着互联网出入口收敛工作的推动，统建业务系统与数据中心的互联网与广域网访问已成为央国企行业业务访问的新常态，保障此场景下的业务应用与落地成为当下焦点；

安全要求：实现统建业务系统与数据中心访问的基础上，保证互联网暴露面收敛，确保业务应用和数据安全，构建可信的数据传输链路是安全管理中的核心要求；

管理需求：在确保业务场景应用的前提下落实现有安全管理制度与具体要求，需通过技术应用达成管理目标；

◈ 解决方案

联软科技全网零信任解决方案融合了 SDP 软件定义边界、NAC 准入安全、NXG 数据安全交换、EMM 移动安全、EPP 端点安全、EDR 终端检测与响应、DLP 数据安全等功能，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，全面针对不同身份、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管控。

方案部署后

可信身份管理

- 构建基于人员、设备、应用的全新数字化身份，并围绕身份进行细粒度访问控制；
- 多因素的身份鉴权，支持单点登录和手机扫码联动认证，兼顾安全和效率。

可信接入管理

- 基于 SPA 技术实现互联网暴露面的“隐身”；
- 应用级的安全加密传输隧道，双向证书校验，确保数据传输过程中的安全；
- 可提供有客户端与无客户端模式，适配各类业务应用场景。

可信设备管理

- 兼容 PC 设备和移动设备，实现 PC 设备、BYOD 设备、配发手机、PAD 的统一可控管理；
- 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；
- 可提供数据采集、深度威胁识别、调查取证、威胁响应与处置修复在内的终端检测与响应能力。

可信应用管理

- 建立企业应用统一门户，简化访问流程，并对企业应用进行统一管理；
- 搭建企业级软件商城，实现应用全生命周期管理；
- 按需授权访问，杜绝违规应用运行，确保企业应用安全。

可信数据管理

- 提供多安全沙箱、终端外发通道审计、多种水印方式、数据加密等数据安全防护能力，确保数据在终端落地后的安全性，实现数据完整闭环管理。

业务价值与方案优势

更高效的管理

一套平台可对移动端、PC 端进行全端点统一管理，覆盖各类操作系统与有端无端接入场景；统一客户端基于场景智能切换，实现网络准入认证、零信任接入认证，同时可实现内外网混合办公场景下终端安全、运维和数据安全要求

暴露面收敛

基于 SPA 技术实现真正的零暴露，实现网络及资源的“真隐身”，积累了丰富的复杂场景的落地经验；应用级双向校验的安全加密传输隧道，确保数据传输过程中的安全

持续安全评估

持续检测动态授权，终端采集、检测、管控、审计能力业内领先，结合十余年端点安全技术的积累，并在零信任架构中复用，实现终端环境的全面感知

数据安全可控

集成多沙箱、终端 DLP、文档安全、通道审计管控、水印等安全能力，全面覆盖差异化场景下的数据安全保护需求，保障安全与效率的平衡

央国企能源行业信创终端安全一体化解决方案

◈ 需求来源

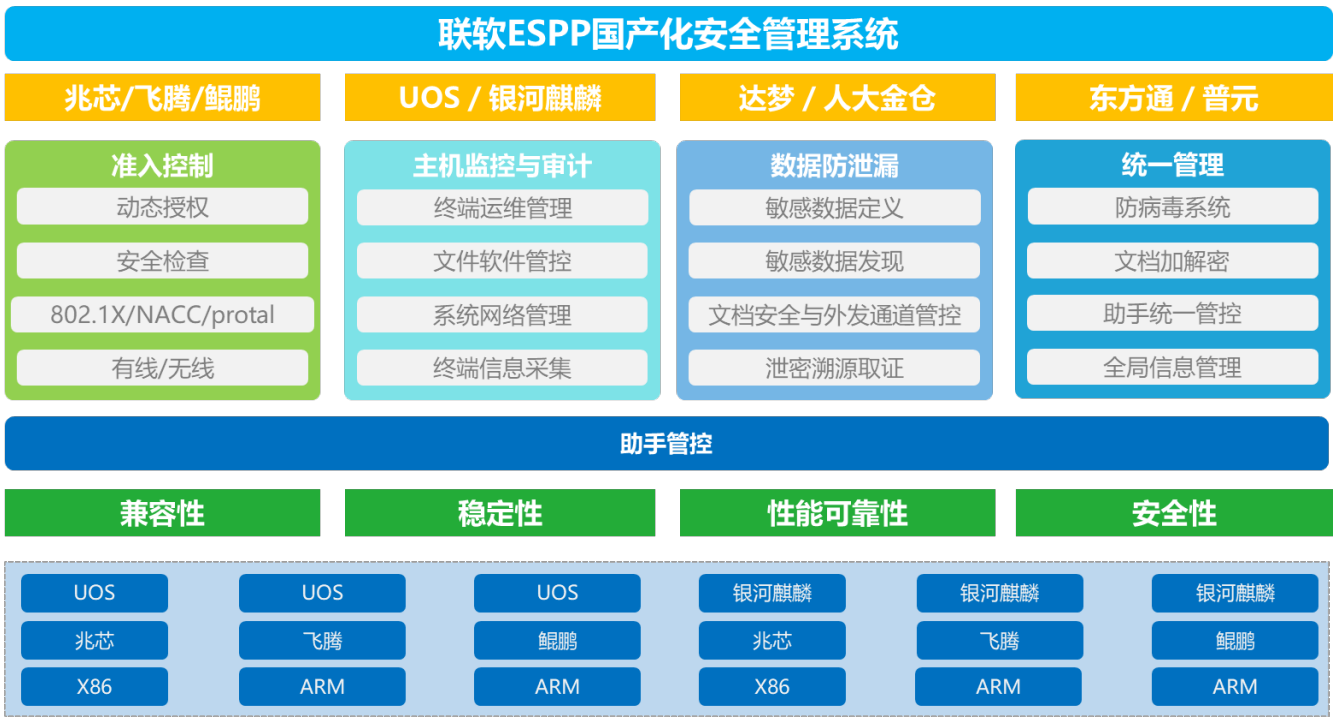
合规要求：为了解决核心技术“卡脖子”“受制于人”等问题，信息技术应用创新发展已成为当前国家战略，同时也是国家经济发展的新动力。在国家规划层面，涉及信创产业的规划包括：《国家信息化发展战略纲要》《“十三五”国家信息化规划》《软件和信息技术服务业发展规划（2016—2020年）》。

安全挑战：随着网络攻击和数据泄露的增加，建立健全的网络安全体系势在必行。同时，实现自主可控也是发展信创产业的重要动力。在国际竞争中，掌握核心技术和拥有自主知识产权对于一个国家的竞争力至关重要，央国企承担了重要“基石”作用，国有企业遍布国计民生各个重要领域，通过信创替代夯实安全可信底座，借助数字化赋能央国企的业务发展和模式创新。

信创推动：自主可控的建设推动下，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。

◈ 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，本方案以联软ESPP企业安全保护平台为基础，帮助企业建立一个实现企业内部终端安全保护、运维管理及数据保护的一体化管控平台，解决企业计算机入网合规性和安全管理等问题。



统一管理

一个平台实现信创终端与传统终端的统一安全管理，保障信创终端稳步替换过程安全无风险；

资产“可信”

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，确保接入终端“可信”；

终端“可管”

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、软件正版化管理、运维简化管理，确保内部终端“可管”；

终端“可防”

多样的数据类型采集，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；

数据“可控”

对企业数据在创建、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，确保数据“可控”；

一体化管理

一体化客户端与管理后台，实现从网络准入控制、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。

业务价值与方案优势

兼容性强，稳定性高

与国内主流信创操作系统、国产芯片、中间件、数据库等进行深度适配，与办公软件、业务软件、浏览器、安全软件之间的兼容性强，确保在各类系统/平台上均能构建安全管理能力

减轻运维压力

实现全网终端设备的集中管理，使得企业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

终端与数据安全保障

可有效地对终端进行安全加固，减少终端安全风险。基于数据安全管理，有效保护企业敏感信息，降低数据安全风险。对入网终端提供接入安全管理，提升网络边界安全

统一管理

支持全栈信创与半全栈信创平台部署，满足企业全栈信创建设需求，并可在一个管理平台和一个客户端的模式下实现整个方案全部功能，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

央国企能源行业软件管理解决方案

需求来源

合规要求：2014年国资委提出高度重视软件正版化工作，按照党中央、国务院的统一部署和安排，明确推进中央企业软件正版化工作的目标和措施，大力推进中央企业软件正版化工作。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，做好软件管理。

安全挑战：在正常的企业生产过程中，员工可能会在不知情或无意中使用未经正版授权的软件办公。一旦商业软件公司发现此类侵权行为，它们可能会向企业发出律师函，要求经济赔偿，给企业带来经济与名誉上的损失。此外，员工自行下载并安装的电脑软件如果携带恶意代码，也极有可能对企业计算机系统造成破坏，导致企业信息泄露，引发进一步的经济损失和安全风险。

运维工作量：传统软件管理方案缺乏软件云端更新能力，软件管理运维人员工作量大。

解决方案

联软科技提供的央企能源行业软件管理解决方案，不但满足《正版软件管理工作指南》中关于企业软件正版化管理的要求，也能帮助企业规范软件标准化管理。该方案包括以下内容：

终端软件资产管理

软件采购订单信息录入、软件许可信息录入、软件使用授权管理、可导出报表台账进行管理；

软件使用信息收集

软件安装数量、安装终端信息、使用人员、使用时长信息获取；

软件标准化管理

提供对已安装软件进行违规审计、预警、卸载处置；

软件运维管理

提供软件分发、软件自动分类等工具方便企业软件运维；

软件应用商城

提供用户正版软件下载通道，解决用户自主安装软件的难题；

云软件仓库

通过联软对软件专业评估、测试、杀毒后，上架到云软件仓库供企业用户免费下载使用；

云端绿色软件识别规则库

通过联软实时运维，将绿色软件规则持续发布到云端绿色软件识别规则库，持续升级绿色软件识别能力，增强软件安全管理。

业务价值与方案优势

该方案能全面满足合规要求，相比传统方案提供如下价值：

软件台账管理更便捷

系统化的台账登记与管理，提高了信息收集的效率和准确率

正版化授权管理更智能

自动授权和自动回收机制，可以便于企业对软件正版化进行授权管理

软件信息采集更全面

安装与使用时长信息收集，能够获知软件使用情况，便于企业对企业软件情况进行分析，提供采购计划参考依据

用户软件安装更方便

在严格进行软件管控同时，提供安全丰富的软件应用商城，既满足企业软件管理的需求，也满足用户办公的需求

软件管理运维更轻松

云端软件仓库和云端软件规则库，极大降低企业软件管理运维工作量，方便用户办公，提升企业软件管理安全强度

企业办公环境更安全

有效阻止流氓软件、绿色软件下载安装，提高员工工作效率，改善企业信息安全环境

央国企能源行业电力安全数据交换方案

中国华能集团有限公司 CHINA HUANENG GROUP CO.,LTD.

需求来源

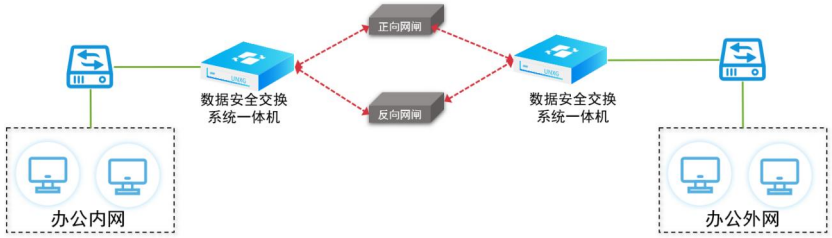
业务驱动：便捷高效地实现跨网数据传输，满足电力行业安全三四区间的数据安全交换使用场景，整体易用性强，使用简单；

安全需求：对数据进行内容识别与安全检测，确保跨网数据传输不打破现有安全边界，避免出现病毒跨网传播风险，并可实现全流程审计与审批管理；

管理要求：建设与管理成本低，可满足电力行业安全隔离要求，提供数据传输统一管理能力。

解决方案

本方案以UniNXG数据安全摆渡系统为基础，针对电力行业安全III区（办公内网）与安全IV区（办公外网）数据交换与共享方式进行创新与优化，通过部署在网间的数据安全摆渡系统，作为内网终端与外部网络终端的文件安全交换平台，同时配套电力级安全隔离装置，在满足办公和业务对文件交换需求的同时，实现物理与逻辑隔离场景下的文件流转审批及杀毒管理，降低病毒感染和数据泄密的风险。具体如下：



全网络隔离

搭配电力专用正反向安全隔离装置，实现物理隔离下的网间数据安全交换；

详尽的审计

支持详细的用户登录、行为审计和内容审计；

集成防泄密

基于数据敏感性检查实现文件交换中的数据防泄密管理，结合文档跟踪能力，实现数据泄密追溯；

兼容性全面

系统支持后台全栈信创和非全栈信创，用户可根据实际情况选择信创配件；系统客户端支持信创操作系统和非信创操作系统安装部署；

防病毒强大

支持第三方防病毒/木马引擎，支持多款防病毒软件异构杀毒；

灵活的审批

支持对文件的多级审批和多种审批模式；

人性化操作

用户界面类似网盘，支持B/S和C/S模式，用户无学习成本，无需培训；

双向外链传输

支持外联分享与敏感识别进行联动，实现分享审计审批等安全管控；

集中化管理

支持对企业中的所有交换平台进行统一管理和配置策略集中下发。

业务价值与方案优势

数据传输安全可控

数据交换的整个过程安全、受控，交换前有病毒木马查杀，交换中有完整的授权、审批及防泄密机制，交换后有详尽的审计记录和内容备份

部署便捷

软硬件一体化，无需前置机，维护简单，购置成本和运营成本（维护、电力）极低。部署简单，设备简单配置后，便能实现网络间的安全数据交换

提升效率

提供安全的文件分享、文件外链和公共目录的功能，支持协作办公，极大提高办公效率

满足合规

满足监管单位的相关合规性要求

央国企能源行业网络空间资产测绘方案

需求来源

业务驱动:聚焦围绕企业网络空间IT与数字资产风险的监测与管理;

安全需求:解决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:形成网络空间资产台账,聚焦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企业互联网资产进行发现与测绘,持续风险监控,结合多维安全情报,专家安全顾问团队支持,为客户打造托管式安全运营服务,能够帮助企业输出高价值情报,让企业在实战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”;

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，快速发现企业泄露的信息或文档，协助用户下架闭环;

组织风险完整监测

自动化分析集团型组织的股权关系，通过组织信息、搜索引擎和空间测绘引擎情报，获取和企业存在关联的疑似资产信息，并能够通过组织机构信息进行进一步搜索，帮助发现分支机构私搭乱建资产。

业务价值与方案优势

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

防入侵（勒索）技术方案

需求来源

攻击频次与影响：自Wannacry爆发以来，勒索病毒已经从偶发事件演变为常态化威胁。无论是政府、能源、交通还是医疗等关键领域，都遭受了其打击，造成的影响范围深远，不仅涉及数据丢失，还可能导致关键基础设施的瘫痪和经济损失。

威胁多样性与手段：勒索病毒并不是一个固定的形态，它随着技术的进步在不断演变。从最初的文件加密到现在可能涉及整个系统的锁定、数据泄密甚至是设备损坏，攻击方式越发狡猾和难以预防。

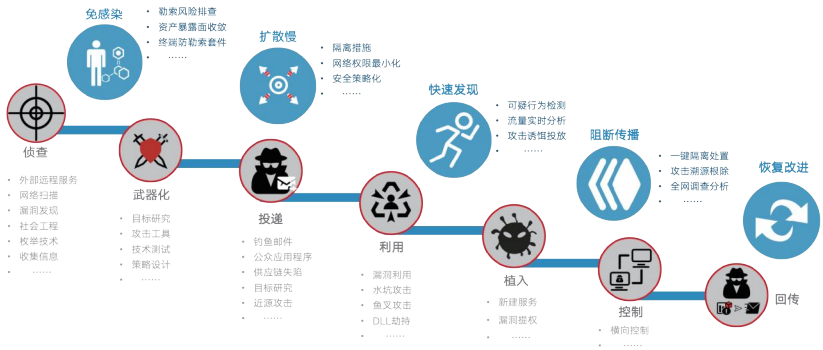
预防与响应策略：鉴于勒索病毒的高损害性和难预测性，单纯的被动防护已无法满足安全需求。企业需要构建主动的安全预防策略，结合实时监测、备份管理和应急响应，以最大程度降低被攻击的风险和潜在损失。

解决方案

勒索软件攻击的不断升级，保护企事业单位的核心系统、数据资产和敏感信息已成为重中之重。为此，联软科技基于可信数字网络架构TDNA，提出了立体式防御方案，能够更加有效地保护企事业单位的信息系统安全。

以下是联软防勒索方案的构成：

- **云：**攻击面管理 + 勒索风险排查服务
- **边：**暴露面收敛 + 安全策略管理 + 网络隔离
- **端：**终端勒索防护 + 数据备份 + 一键隔离



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 分钟就能得出全面的调查结果，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

持续关注网络安全的最新动态，并根据这些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，提供了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进行调整。不仅如此，随着业务的发展，您还可以添加更多的功能，例如数据泄密防护等

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；

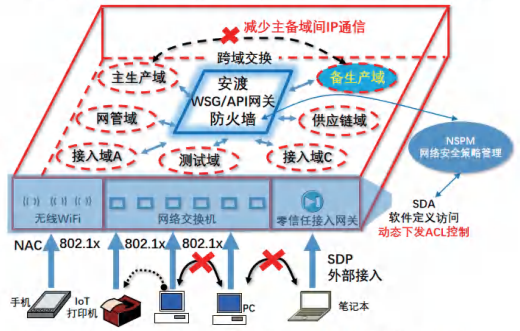
分域和跨域访问控制（防火墙/NXG/WSG/API）

- 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

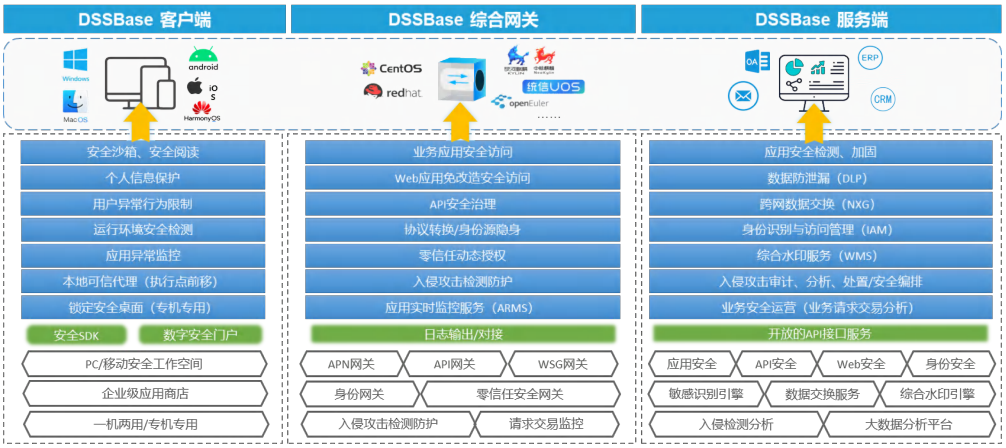
数字化应用安全要求：业务存在入侵风险、数据存在泄露风险、设备管理困难、传统VPN使用体验差，安全合规要求加强；

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、提升效率、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。

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；

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