联软科技
LEAGSOFT

制造
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

下一代企业安全综合保护解决方案

需求来源

边界模糊风险大，设备接入管理难：随着企业的应用业务逐步云化，终端接入环境也从传统单一的企业内网不断扩散。远程办公/运维终端以及有线/无线/VPN方式接入等复杂多样的设备接入，使得制造业企业传统的网络边界越来越模糊，企业内部建立的安全区域边界面临着业务访问需求的不断挑战。

运维管理压力大，终端安全管控难：越来越多的终端类型涌现在企业网络中，网络环境也在不断演变，传统单一手段或几种安全工具的简易整合式的企业信息安全建设弊端日益凸显，安全产品运营效率也无法得到保障。

数据泄密场景复杂，核心数据保护难：客户数据、财务数据、生产与配方数据等核心数据保护成为焦点。数据泄密日趋严峻，内外部人员窃取敏感数据，影响企业竞争力。防止重要数据资产、敏感信息的非法泄密，已成为制造业企业生产经营的底线与红线。

企业迫切需要从整体规划入手，在用户、设备、数据、权限、行为等方面对全网所有终端进行统一安全管理，提升综合防护能力和运营效率。

解决方案

基于联软TDNA可信数字网络安全架构下的《下一代企业安全综合保护解决方案》，融入零信任安全理念，涵盖边界、网络、终端、数据安全等信息安全领域，能够帮助企业建立一套实现企业网络边界防护、终端安全加固、防病毒、数据保护及运维管理于一体的综合保护平台。

该方案包括

全网资产可视化

对网内PC、移动终端、IoT设备进行自动发现、设备类型智能识别；

统一边界防护

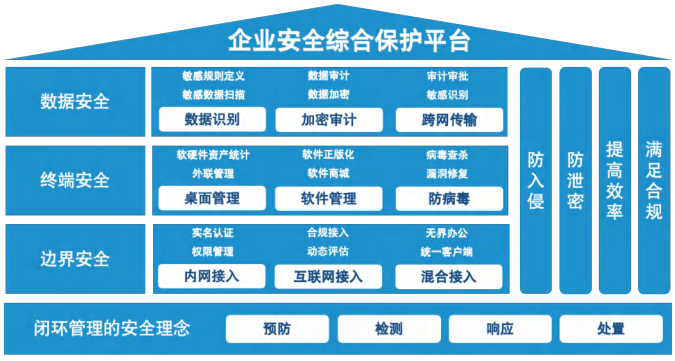
实现终端在企业网与非企业网的安全接入；

终端桌面管控

涵盖终端安全基线加固、补丁管理、软件标准化管理、非法外联管理、防病毒管理；

数据全生命周期管理

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；



立体式综合保护

一个Agent从远程接入管理、内网准入控制、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、防病毒等全场景进行统一安全保护。

业务价值与方案优势

防止入侵

全网边界统一防护，杜绝非法接入，防止越权访问，病毒实时查杀

防止泄密

基于场景化的数据防泄密保护措施，不改变操作习惯，不影响工作效率

效率提升

一个平台、一个客户端，统一安全管理，数据统一汇总，关联分析、机器学习、智慧决策

满足合规

符合《网络安全法》《数据安全法》以及国家版权局对正版软件等政策法规要求

终端安全一体化解决方案

需求来源

终端看不到找不着，资产数据无法统计：快速增长的多样性设备，使其无数专用设备、专用操作系统涌现，导致设备类型和数量越来越多，系统环境复杂，缺乏统一的设备资产管理手段。

任意终端随意接入网络，访问权限控制粗放：用户变得多样化、业务多样化、访问方式越来越复杂，终端通过有线/无线/VPN等接入方式随意接入网络，给企业内网带来了巨大的安全风险。

碎片化运维管理复杂，终端面临安全风险：日常运维工作普遍通过人工方式或单一工具对桌面终端进行管理，运维成本高，无法全面的对终端安全基线、软件标准化、系统自身安全等进行系统化管理；

无法保护敏感数据，数据泄密无法追溯：无法对终端上敏感数据进行发现与识别，客户信息、知识产权、生产与配方等核心数据外发时，无法进行识别与控制，数据泄密也无法追溯追责。

解决方案

以联软ESPP企业安全监测保护平台为基础的《制造业终端安全一体化解决方案》，基于TDNA可信数字网络安全架构进行设计，涵盖边界、网络、终端、数据等信息安全领域，能够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。

网络边界防护

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；

数据全生命周期管理

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密管控；

安全风险识别与处置

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；

全网资产可视化

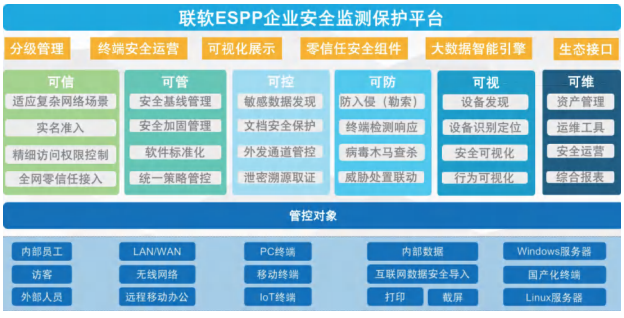
对网内PC、移动终端、IoT设备进行自动发现、设备类型识别；

统一运维管理

资产统一管理、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；全生命周期持续管理，全面掌握终端的管理状态。

方案部署后

- 实施基于强制策略的准入控制，确保接入终端**“可信”**；
- 加强终端桌面安全加固与标准化管理，确保接入终端**“可管”**；
- 采取全生命周期的数据管理控制措施，确保数据**“可控”**；
- 提升终端安全防护能力，提高免疫能力，确保终端**“可防”**；
- 强大的网络设备发现能力与敏感资产扫描能力，摸清家底，确保资产**“可视”**；
- 实现数据自动化分析、资产全生命周期管理，实现全面**“可维”**。



业务价值与方案优势

该方案实现对包括Windows、macOS、Android、iOS、Linux、国产操作系统及IoT设备在内的各操作系统和各种终端设备的集中管控，相比传统方案：

一个平台、一个客户端

整体规划，多种技术、综合解决网络与安全问题

终端安全运营

安全数据统一汇总，关联分析、机器学习、智慧决策，可视化展示

提升运维效率

终端自动化管理，大幅提升办公效率和用户体验

满足政策法规

符合等保2.0、《网络安全法》、《数据安全法》、《个人信息保护法》、等政策法规要求

数据防泄密解决方案

需求来源

政策法规驱动：随着《网络安全法》《数据安全法》《个人信息保护法》等颁布，国家对网络安全、数据安全也越来越重视，为保护国家关键数据资源安全和企业信息数据安全提供了法律依据。

数据类型多，泄密途径复杂：企业在业务不断发展和建设的趋势下，员工因业务需要，通过从业务系统下载数据、终端本地生成数据等，导致终端保存了大量不同类别敏感级别的数据，如客户资料、会议纪要、设计图纸等。数据外发途径又多而复杂，常见的途径包括移动存储、邮件、即时通信工具、网络途径（如网络共享、云盘等）、打印等，如缺乏对其外发途径进行识别、审计或阻止等手段，将面临很大的泄密风险。

解决方案

联软科技推出的《制造业数据防泄密解决方案》，从终端数据安全、跨网数据安全、业务数据安全这三个维度实施数据安全能力建设，有效地杜绝企业办公网、研发网、生产网的数据泄密风险，提升企业数据安全防护能力。

方案包括

终端数据保护

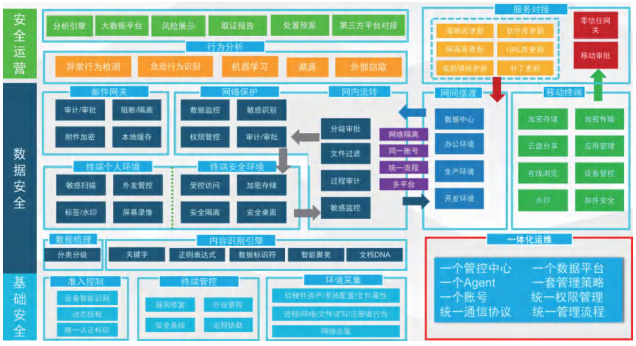
通过外发通道外发时自动进行敏感内容关联识别匹配、阻断、审计与控制；基于文档加密技术，实现对源代码、设计图纸等核心数据强管控，可支持基于敏感数据识别的密级权限与标签进行统一管理；通过对终端自动加载水印信息，实现数据泄密追溯；

业务数据保护

依托业界先进的零信任安全理念，实现远程办公场景下的业务数据安全保护。通过统一身份认证，防止身份仿冒，保障终端用户身份的合法性；保证企业内部数据落地安全性；提供业务数据水印中台，不仅可以提供水印SDK，给业务系统提供强大的在线水印，文件水印，自身也能作为文档发布平台，集成下载转发审批、权限管理等能力。

跨网数据安全交换

通过数据安全交换平台，帮助企业在不同隔离网络之间建立安全合规、高效便捷的统一跨网文件交换通道。针对所有传输文件可进行审计、留痕，同时可对文件进行病毒查杀与敏感内容识别；通过扩展组件，还可实现在线编辑、文档下载加载水印、文档预览加载水印、文件下载加密等数据安全能力；



业务价值与方案优势

立体式综合防护

一体化管理及运营、场景化的方案设计，客户端高度集成，实现企业终端数据、业务数据、跨网交换数据的数据安全管理

防止泄密

基于场景化的数据防泄密保护措施，不改变操作习惯，不影响工作效率

满足合规

符合《网络安全法》《数据安全法》《个人信息保护法》还有《工业和信息化数据安全管理办法》等政策法规要求

统一管理

主流系统及应用100%兼容，完成国产化操作系统适配，实现统一终端数据管理

全网零信任解决方案

通威太阳能 TW SOLAR | 永祥股份 YONGXIANG CO.,LTD. | 金域医学 KingMed Diagnostics | 旗滨集团 KIBING | 华人运通 HUMAN HORIZONS

需求来源

伴随着云计算、移动互联网等新技术的快速崛起，企业的应用业务逐步云化，终端接入环境也从传统单一的企业内网不断扩散。新的业务和网络环境下，企业将面临更多安全挑战：

- **业务访问安全：**公司各类员工需在不同时间不同地点均可访问业务系统进行办公，如何保证用户在企业网和非企业网业务访问的安全、确认接入终端是否符合要求、限制接入用户访问权限。
- **业务数据安全：**员工远程办公访问业务时，如何保障远程办公下的业务数据安全。
- **统一运维管理：**内、外网的终端如何实现有效的统一安全管理，持续守护企业终端和数据安全，减少运维工作成本。

解决方案

联软科技推出以“永不信任、持续验证”的零信任理念为基础的《制造业全网零信任解决方案》，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，用户只需要采购与安装、部署一套系统即可实现全网各种终端的零信任安全接入，并可对移动端和 PC 端进行统一管理，并且用户可根据企业实际需求选择方案具体的应用场景，基于一套平台、一个客户端，可快速扩展，无需重复建设，同时提高运维和管理效率。

方案部署后

可信身份

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；

可信接入

基于 UDP 的 SPA 技术实现互联网暴露面的“隐身”，提高对抗能力，降低被攻击风险；

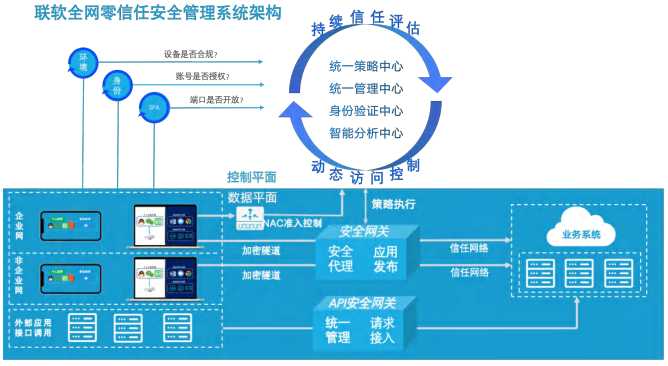
可信设备

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；

可信应用

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；

联软全网零信任安全管理系统架构



可信数据

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，确保应用及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

安全

- SPA机制隐藏服务，暴露面收敛，天然抗攻击；
- 业界领先的终端DLP防泄密技术和水印技术，防止企业数据外泄；
- 动态安全评估机制，提供持续可信访问。

高效易用

- 一个客户端实现内外网接入；
- 支持业务单点登录和手机扫码联动认证，无需反复认证；
- 统一访问入口，规范用户访问行为，无需反复切换访问环境，提高效率，提升用户体验。

可扩展

- 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；
- 统一安全架构，可集成终端EDR，杀毒等。

数据安全交换解决方案

需求来源

在制造业企业一般包含有生产网、办公外网、办公内网（禁止访问互联网）、研发网、云桌面、互联网等，各网间通过逻辑隔离或物理隔离的方式保障各网络内部数据安全，目前主要通过网络共享、FTP、U盘等传统方式，缺少审计、审批、敏感检查、杀毒等安全管理能力。如传统的双网卡存储设备网络安全风险较大，U盘可移动存储是数据泄露、病毒感染的最大风险点。因此如何在保障网络隔离、满足数据存储流转需求的情况下便捷安全的实现数据传输是制造业企业需要考虑的重点。普遍存在如下场景：

- **外部传入：**客户、供应商、合作伙伴，通过互联网将文件发送给内网员工；
- **外部分享：**内网文件给客户/供应商/合作伙伴；
- **跨网传输：**共享文件导入生产车间设备升级文件。

解决方案

该方案包括

统一通道

杜绝通过U盘等第三方外联设备进行网络间数据交换；

数据病毒查杀

在文件交换过程中，系统对文件进行防病毒扫描；

方案部署后

跨网隔离

实现多网间 IP 协议栈隔离；

安全交换

通过 B/S、C/S 客户端及移动端 H5 统一通过 UniNXG 安全通道交换文件。实现文件在跨网交换过程中，对文件进行病毒查杀、操作审计、敏感检查、审批管理、文档追踪标记及安全水印，实现文件安全防护及文件泄密追溯；

文件管理

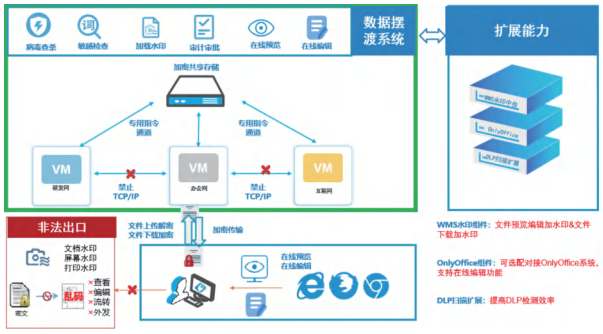
根据用户控制文件上传、下载、分享及外链等权限，实现在线预览、编辑；

审计留痕

不影响网络隔离效果的情况下，实现数据的实时交换并进行敏感字过滤审计留痕，含有关键文件必须经过审批才能进行交换，对传输文件追溯定位；

效率提升

用户在线预览、在线编辑、文件下载加载水印。



便捷办公

支持在线预览、在线编辑、极速秒传、文件共享、公共目录、生成外链。

业务价值与方案优势

安全

平台采用专有非TCP/IP协议和防病毒检测可抵御外部攻击，对跨网数据交换进行完整审计、对敏感数据进行过滤、审批管理及用户权限最小颗粒度控制

高效

平台既有网闸的安全隔离特性，又具备网盘的文件管理功能，可有效地保障员工跨网文件流转效率的同时提升安全性

灵活

平台可软硬一体化或虚拟化方式旁路部署，支持集群可灵活扩展，能够使用在企业不同应用场景及网络环境，可集成OA审批流程和第三方防病毒引擎联动

合规

系统具备等保3级认证，支持全栈信创，支持IPV6

软件管理解决方案

需求来源

终端用户在日常办公中，因业务需要，需在终端上安装系统软件、开发软件、设计软件及办公软件等。企业为有效使用及管理计算机软件资源，并确保公司计算机软件合法使用，避免人员因使用非法软件，导致触犯著作权法、知识财产权，影响公司声誉或造成计算机病毒侵害，影响业务正常运行，迫切需要对企业软件进行统一的标准化和正版化管理。同时，国家版权局《正版软件管理工作指南》等文件也要求政府机关、企事业单位等落实软件正版化，提供明确软件正版化报表。

解决方案

以联软科技UniAccess终端安全管理系统为基础的《软件管理解决方案》，能很好地满足企业对软件正版化和标准化管理要求。该方案包括以下内容：

- **软件资产管理：**实现软件资产自动统计，支持快速检索查询，让软件资产管理简单化；
- **商业软件台账：**可对采购的正版软件进行订单和授权管理，支持将采购订单导出为软件正版化台账，并能对软件进行授权安装管理；
- **企业软件商城：**将软件商城作为员工下载安装卸载软件的唯一通道，可以天然地杜绝违规软件；
- **软件标准化管控：**建立软件安装与卸载的唯一通道，实现违规软件自动卸载，必装软件自动安装；
- **软件使用时长统计：**支持对企业采购的软件使用时长进行统计，提升企业使用效率。

业务价值与方案优势

帮助企业建立基于软件生命周期的统一管理方案，相比传统方案：

保障内网安全

杜绝软件滥用风险，标准化、流程化，提高工作效率

提升运维效率

从救火队、人力解决释放出来，快速处理违规软件，提高IT管理水平

使用决策分析

梳理资产清单，为覆盖率、企业采购提供有效决策信息

满足合规要求

拥有正版化管理方案，摸清家底，抛弃纸质清单，随时提供数据支撑

文档加解密解决方案

需求来源

随着大数据、云计算技术的发展，企业迎来了数字化转型时代，伴随而来的是企业信息化办公所产生的大规模数字文档，这些文档是企业经营过程中积累的数字资产，是企业赖以发展和进步的核心竞争力。电子文档在给企业带来便利的同时，也给企业带来安全和管理隐患。电子文档内容极易被传递或被损毁，从而直接或间接造成企业内部价值的流失。

一些非结构化数据无法检测敏感，比如2D/3D图纸、图片、音频、视频和代码等数据。对这些核心竞争力文档如何进行保护，如何从源头保障文档的全生命周期安全，是企业发展中急需重视的一环。

解决方案

联软UniDES文档安全管理系统方案以透明加解密技术为核心，采用高强度加密算法实现智能透明加密，综合动态透明加密技术、文件内容识别等多种尖端技术，有效控制文档使用者对文件读取、存储、复制、截屏等权限，在有效防止企业核心信息资产外泄的同时，不影响员工工作习惯及业务效率，为企业的各类电子文件提供全生命周期的安全防护，帮助企业搭建一套完善的文档防泄密体系。

方案包括

企业内文件透明加密

对内部数据进行加密处理，使企业内部产生的涉密数据安全可控，实现数据透明加密，达到“对内透明，对外受控”的效果；

文档数据智能标密

根据文档的敏感信息进行智能标密，根据企业制定的敏感规则，自动识别敏感数据打上密级标签，实现不同保密等级文件的权限控制；

内部文件权限控制

可针对不同人员、不同部门、不同角色采用不同的加密策略管控，从而实现不同区域、不同级别、不同人员之间加密文件访问的互通和禁用；

内部文件外发管理

结合实际场景，实现文件解密审批外发、密文外发权限控制对加密文件外发进行统一管理；

企业核心业务系统集成

对各应用系统上的数据进行安全保护，实现业务数据“上传解密，下载加密”的效果。

业务价值与方案优势

一文一密

一文一密，每个文件加密时随机产生文件密钥，防止暴力破解加密文件

密级管控

支持多密钥组合和文件密级管控，实现不同部门、用户组、设备和用户间文档隔离

贴合业务

针对企业文档管理需求及不同使用场景，采取不同的加解密模式，贴合业务办公流程

灵活审批

按文件敏感级别灵活审批，不同等级的文件自动匹配审批流程，如：解密审批、修改密级和访问权限审批

安全易用

不改变习惯，不影响效率；企业安全管理员实时掌握所有加密文件位置信息和审计信息

配发设备管理解决方案

需求来源

随着移动互联网的发展，移动智能终端设备的使用越来越多，移动化业务在制造业越来越普遍，例如生产线监控平板，仓库管理手持PDA等等场景。企业基本采用企业配发设备（COPE）的方式给员工开展业务。为避免“专机私用”，保障企业业务正常运行，企业希望针对COPE设备能够进行统一安全管控。

解决方案

联软科技针对企业移动配发设备提供完整解决方案，方案内容主要包含如下：

该方案包括

配发设备全生命资产管理

包含配发设备的注册、激活、绑定、更换、回收等，提供自服务平台方便设备管理员进行辖内设备的资产管理和远程控制，包含关机、锁屏、解锁、恢复出厂恢复、截屏、推送消息、开关摄像头、开关蓝牙、数据擦除等；

安全桌面专机专用

开机即进入定制化安全桌面，安全桌面内显示的应用可以自定义配置，并且安全桌面禁止退出，实现专机专用；

应用全生命周期管理

打造企业应用商店，禁止安装非法应用，只能安装企业应用商店发布的应用；从应用登记、注册、发布、访问权限、安全传输等实现应用全生命周期管理；

数据安全保护

包含沙箱技术、安全阅读工具、安全相机/相册能力、应用级防复制/粘贴、应用级水印等多种手段保护企业数据安全；

非法外设管控

对配发设备外设进行管控，防止通过USB或蓝牙等方式将企业数据外泄，并且支持时间地理围栏策略，限制设备在指定时间地理范围内的摄像头、蓝牙、Wi-Fi等功能是否允许使用；

统一设备管控

针对配发设备进行合规检查，例如操作系统、密码强度、SIM卡变更、电量和存储空间监测等，确保设备长时间离线时能自动清除企业沙箱中的数据，实现设备统一管控要求。

方案部署后

- 配发设备专机专用，不允许私自下载软件及数据违法外发操作，提高设备使用效率；
- 实现配发设备的资产管理和安全管控；
- COPE设备可通过移动客户端完成802.1x准入连接企业Wi-Fi；
- 支持远程获取业务APP日志，提高故障定位效率。

业务价值与方案优势

提升设备使用率
专机专用，降低设备的采购投入

提高工作效率
设备专注于业务使用，提高业务办理和推广效率

提高安全性
采用零信任架构，实现身份、终端、应用程序以及业务系统之间的安全

平台扩展能力
移动安全架构一次建设多次复用，可扩展BYOD设备安全管控能力，实现移动应用管理、移动数据管理

数字水印及文档集中管理解决方案

需求来源

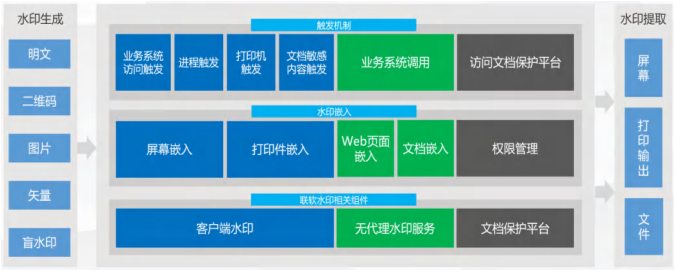
随着信息化和数字化技术的不断发展，制造企业在生产过程中，涉及到大量的设计图纸、技术资料和生产数据，传统的数据防泄露方案无法有效解决拍照、打印等媒介转换场景下的数据扩散问题，企业内部员工可能因为无意疏忽或恶意行为导致信息泄露。除了集中式的安全意识培训外，还需要通过触发式、场景化的方式进行及时提醒，以防范无意识的被动泄密。在这种场景下，数字水印技术成为了理想的选择。

解决方案

以联软科技 UniDLP 数据防泄露产品为基础的《制造业数字水印解决方案》，能很好解决企业文档在流转过程中的扩散问题，提高企业员工安全意识。

该方案包括

- 明文、二维码、图片、矢量（隐形水印）、盲水印等多种水印生成方案；
- 可以根据设备和用户信息自动生成上述不同类型的水印效果；
- 可以将上述不同类型的水印，根据业务系统、文件敏感级别触发式地加载到设备的屏幕上以及打印文件中；
- 通过将业务系统与水印平台进行对接，将上述不同类型水印嵌入到业务系统页面和从业务系统下载的文档中；



- 建立企业统一文档保护系统，将核心文档（如：会议纪要、会议材料、营销计划、战略规划等）从源头进行保护，可将文档发布在文档保护系统上面，员工可在线浏览，此时系统页面增加水印防止信息扩散，同时针对员工下载文档权限进行控制，从而防止文档系统的敏感信息泄露。

方案部署后

- 企业通过文件保护系统发布核心文档，用户在平台上仅预览，屏幕自动嵌入带有用户身份的水印信息，如需下载需要进行审批；
- 终端打开机密文档时屏幕自动嵌入带有身份信息的水印；
- 用户访问企业核心业务系统时，屏幕自动嵌入带有用户身份的水印信息，并提示用户遵守公司制度；
- 从业务系统中下载文档时，文档内自动嵌入用户水印信息；
- 文档打印时，水印内容或水印标记可以随文档一起被打印；
- 通过泄密图片、文档上的水印内容可快速定位设备和人员。

业务价值与方案优势

保护知识产权

文档保护系统能够为公司的内部文档和敏感信息添加水印，有效标识文档的版权和归属，降低重要信息被非法复制和泄露的风险

统一管理

通过文档保护系统进行文档水印的管理，可以实现公司内部多个部门和项目之间的统一标准和水印样式，提高管理效率，降低管理成本

标准化

按照统一标准为对外文档添加水印，有助于提升公司形象，体现专业性和规范性

提高效率

系统提供的文档水印服务能够实现自动化处理，员工在生成或分享文档时，可以快速应用水印，无需手动操作，从而提高工作效率

安全意识提升

对于企业核心业务系统，屏幕水印可以帮助标示系统的机密程度，提醒员工注意信息保密

防止信息泄露

水印的添加使得敏感信息即使被截图、打印，也难以去除水印，从而降低信息泄露的风险

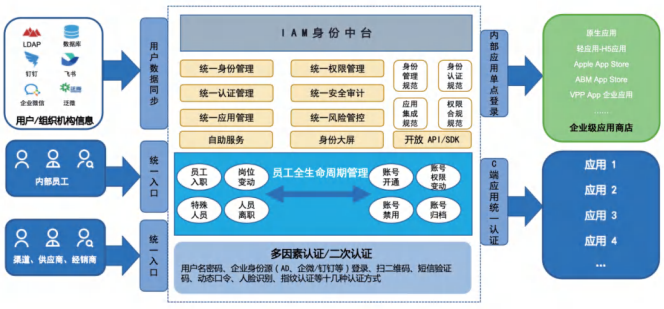
IAM解决方案

需求来源

当前企业信息化和数字化发展迅速，信息化系统规模快速增长，业务应用过于分散，用户身份数据繁杂且割裂，多系统登录切换频繁，影响工作效率。企业对用户、设备、服务多维权限管理要求日益复杂严格，需细粒度、动态灵活的权限模型，需对认证授权全过程进行风险控制，构建企业全网零信任安全体系。

解决方案

以联软科技统一身份认证管理平台为基础的《制造业 IAM 解决方案》，是集统一账号管理、认证管理、权限管理、审计管理、应用管理于一体的用户身份安全综合平台，实现统一认证门户、单点登录、多因素认证、密码安全、身份治理等能力。将身份安全态势通过身份数字大屏进行可视化呈现，使身份在企业内部可管、可控、可视，最终帮助企业形成技术标准统一、集成方式相近的企业级身份认证管理制度与应用对接标准规范。



该方案包括

统一身份管理

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，实现一站式企业身份管理。

统一权限管理

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，最大限度上控制用户或组织的访问权限，避免因权限超出、越级带来的不安全访问和数据泄露。

统一认证管理

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。

统一安全审计

全面且强大的数字身份审计能力，包括用户认证审计、管理员审计、数字身份监控大屏、业务运营态势、智能统计报表等模块支持身份分析，重复账号、僵尸账号、孤儿账号、违规账号等用户账号状态分析。

统一应用管理

企业应用全生命周期管理，包括应用商店、应用发布与审核流程、应用权限基线检测、应用安全扫描、应用安全加固等。

统一风险管控

对认证授权全程进行风险控制，构建企业全网零信任安全体系。用户业务访问过程中进行持续信任评估并动态调整权限，建立动态信任关系，确保访问安全。

业务价值与方案优势

构建数字身份体系，加速业务流转

建立数字身份体系，构建统一数字身份标准，通过“身份中台”保障身份互联、数据互通等能力，让业务流转加速，提升企业整体效率

构建数字智能生态，提升管理能力

整合企业内外部应用，构建智能化生态，提升智能化管理能力，助力企业赋能经济新模式，实现数据、身份、业务的闭环

零信任驱动安全闭环

通过零信任安全架构，打造智慧安全新生态，实现全网零信任安全，为数字化转型进程安全赋能

物联网终端安全管理解决方案

需求来源

物联网发展趋势：随着工业4.0、《中国制造2025》等概念、内容提出，数字化转型已成企业发展共识，在此过程中企业IoT的增长速度快，无数专用设备、专用操作系统涌现，类型众多，环境复杂，多样化。

安全管理需求：IT 和 OT 网络不再物理隔离，而企业网络安全产品仍然以防火墙、入侵检测、杀毒软件“老三样”为主，物联网 IoT 安全产品寥寥无几，而以物联网设备为突破口的信息安全事件逐年增加，越演越烈；因此，需从硬件、接入、操作系统、业务应用等方面着手，采取适当的安全防护措施，确保物联网终端安全乃至物联网安全。

解决方案

以联软科技网络智能防御系统为基础的《物联网终端安全管理解决方案》，能很好解决企业物联网设备安全管理的问题。

该方案包括

资产可见

- 通过系统自动发现部署在网络中的物联网终端设备，并收集设备的 IP、Mac、设备类型、接入位置等信息。

智能准入

- 可信物联网终端设备智能准入授权，非法设备禁止接入网络。

指纹防伪

- 通过设备指纹技术，对设备唯一性进行标定，杜绝仿冒设备接入。

智能幻影诱捕

- 通过智能幻影技术诱捕网内异常攻击行为，及时发现、告警异常攻击行为。

权限控制

- 已发现物联网终端设备动态控制网络权限，仅允许访问必要的网络资源。

威胁风险发现

- 对 IoT 设备流量跟踪分析，安全攻击实时监控，风险趋势预测。

业务价值与方案优势

该解决方案可以全方位地发现企业物联网当中的风险和威胁，通过自动发现技术能够快速发现企业网络中的物联网终端设备，大大减少网络管理员的管理成本。配合精准的权限控制和基于唯一特征与设备行为的分析，将风险和威胁控制到最低。

网络可视化

强大的设备发现与识别能力、灵活自定义类型识别规则，确保设备智能分类

环境兼容好

基于场景化准入方式，不改变网络环境，快速上线部署，实现精细化网络权限管控

智能防伪强

智能准入防伪技术，有效防止物联网设备被非法替换，杜绝非法接入

安全风险闭环

物联网安全风险检测、异常流量感知、快速网络隔离处置、攻击调查取证实现安全闭环

最佳实践多

拥有大量高端制造业、企事业单位成功案例与最佳实践，可为客户提供专业的专家咨询与建议

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。

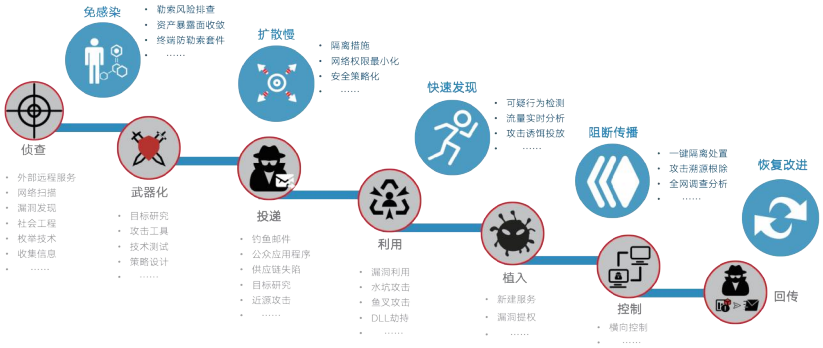
预防与响应策略：鉴于勒索病毒的高损害性和难预测性，单纯的被动防护已无法满足安全需求。企业需要构建主动的安全预防策略，结合实时监测、备份管理和应急响应，以最大程度降低被攻击的风险和潜在损失。

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；

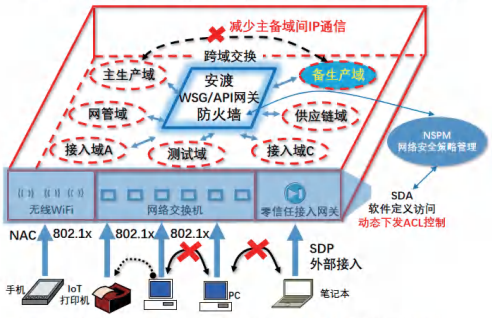
分域和跨域访问控制（防火墙/NXG/WSG/API）

- 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

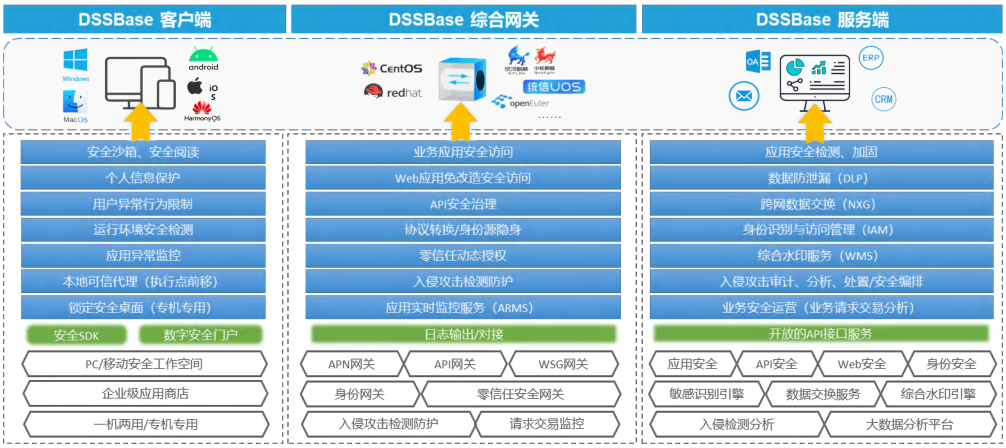
数字化应用安全要求：业务存在入侵风险、数据存在泄露风险、设备管理困难、传统VPN使用体验差、安全合规要求加强。

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