联软科技
LEAGSOFT

防勒索技术方案

立体式防护　安全无担忧

LEAGSOFT

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

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；

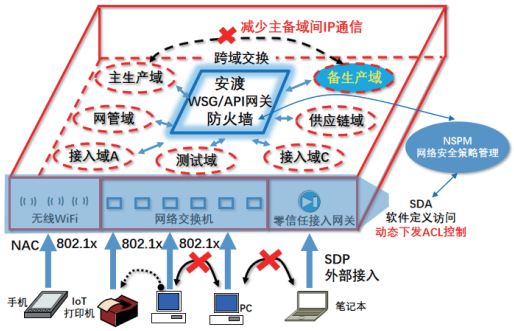
分域和跨域访问控制（防火墙/NXG/WSG/API）

- 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

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。

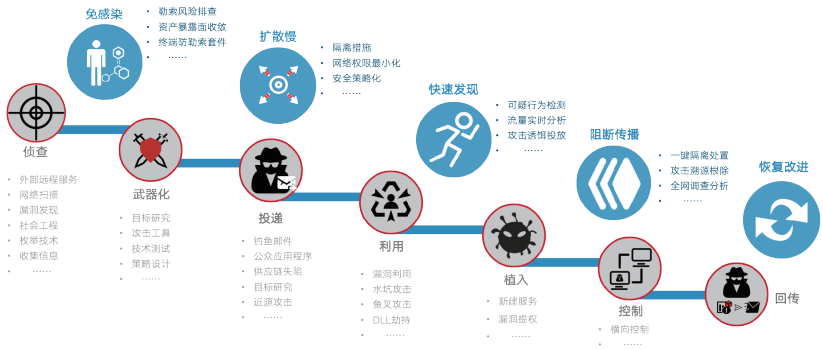
预防与响应策略：鉴于勒索病毒的高损害性和难预测性，单纯的被动防护已无法满足安全需求。企业需要构建主动的安全预防策略，结合实时监测、备份管理和应急响应，以最大程度降低被攻击的风险和潜在损失。

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

终端防钓鱼技术方案

需求来源

渠道变化：网络钓鱼已经从简单的虚假电子邮件逐渐演变为多元化的攻击手段。现在除了传统的电子邮件形式外，攻击者更倾向于利用IM工具和社交媒体来传播虚假信息。这种多途径的攻击方式增加了网络钓鱼的覆盖范围和欺骗性。

攻击手法：网络钓鱼的核心目的是获取企业或个人的敏感信息，或进一步破坏内部系统。随着IT技术的发展，攻击的手法也在不断进化，针对性更强，更难以识别。网络钓鱼的内容、设计和投递方式都更具迷惑性和欺骗性。

防护困难：现代网络钓鱼更主要采用社会工程学的方式，如通过模仿真实的交流情境或使用诱导性的语言，使受害者更容易上当。这种针对人的弱点的攻击方式使得单纯依赖技术手段进行防护变得更加困难。

解决方案

网络钓鱼已成为一种高级持续的网络威胁。针对这一挑战，联软科技精心设计了全方位的防护措施，构筑了多维度的防钓鱼技术体系。这套体系能更加高效地保护政府机构、企业单位的信息系统安全，以下是联软防御网络钓鱼的主要步骤：

静态特征分析

- 通过病毒检测引擎对电子邮件附件进行初步筛查，识别已知的病毒和恶意文件；

威胁情报分析

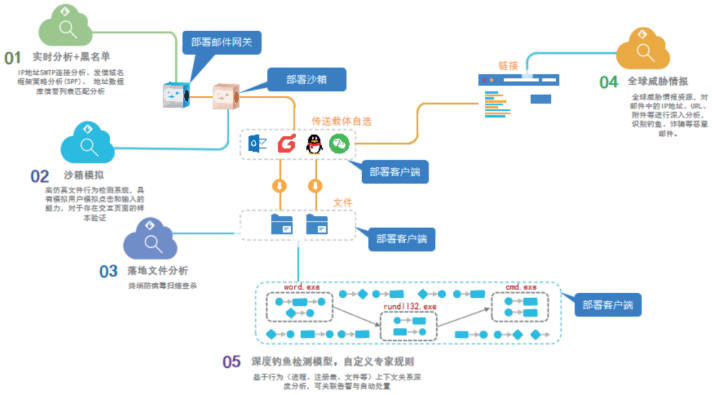
- 利用最新的全球威胁情报资源，对电子邮件中的 IP 地址、URL、附件等进行深入分析，识别钓鱼、诈骗等恶意邮件；

动态沙箱分析

- 在高仿真环境下执行电子邮件附件，通过监控其行为来识别未知的恶意软件和 APT 攻击；

邮件附件监控

- 网络钓鱼的另一种形式是在正常的文件中隐藏恶意的附件。防病毒客户端可以持续监控附件执行后续行为和动作，及时发现并隔离可疑文件；



深度终端网络钓鱼模型检测

- 基于各种网络钓鱼深度检测模型，发现各个进程、注册表、文件等上下关联关系，发现异常行为可及时告警或自动处置，也可基于实际场景进行自定义规则策略实现更高级别的安全防护。

业务价值与方案优势

多层防护效果好

从不同维度全方位识别和拦截恶意邮件，结合情报、邮件网关、沙箱、AV 及 EDR 深度检测分析，可以显著提高发现网络钓鱼的行为，相比单品防护效果显著

灵活性高

可基于网络钓鱼场景随意设置检测渠道，如微信、QQ、钉钉、飞书等，也可设置专属规则进行安全检测

减少损失

网络钓鱼往往会导致企业严重的经济损失和声誉损失。采用上述方案可以及时发现并阻止攻击，避免或减少发生这些损失

降低运营成本

通过集中化管理、自动化运维等方式，能够减少企业的运营成本，同时提高安全防御水平，实现安全与效率的平衡

支持拓展

方案扩展性强，后续可满足企业终端一体化管控、数据安全的需求

EDR终端检测与响应方案

需求来源

攻击特点：APT（高级持续性威胁）是高度组织化并专为特定目标进行的计算机网络攻击。这种攻击特点是精准和长期，攻击者通常专注于某一特定行业或组织。他们深入研究和了解目标，这样的定向性使得每次攻击都更为精确和难以察觉。对于APT攻击者来说，PC终端由于其在企业网络中的广泛应用和包含的关键信息，成为首选的攻击对象。

持续时间：APT攻击者不仅拥有高超的技术能力，而且他们的进攻策略也经常是长线作战。随着技能的不断提升，他们进行的攻击活动持续时间也在延长。这意味着一个目标可能在数月乃至数年的时间里不断遭受威胁。

预警和发现能力：有效的安全策略必须具备前瞻性和应急响应能力。考虑到APT的持续和隐蔽特点，安全团队需要有能力在早期阶段就对威胁进行识别，并迅速采取措施进行应对。此外，针对潜在的或已知的威胁，实时预警机制是必不可少的。

解决方案

传统终端保护方案以防御为核心，易被定制化的恶意软件和针对性攻击绕过。为了解决这一问题，联软科技推出了基于GartnerEDR概念的终端检测与响应系统，用于解决终端高级威胁攻击。该系统可通过联软EPP管控平台扩展，提供多维度数据采集技术、威胁行为检测、深入调查和终端威胁处置。

多维度数据采集技术

- 联软 EDR 采集数据涵盖 18 大项 336+ 子项内容，可自定义采集方式，丰富的数据采集是威胁检测的基础；

威胁深入调查

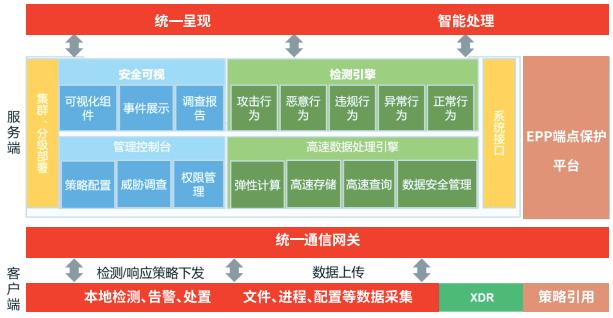
- 支持通过域名、MD5 等信息进行关联查询和证据留存，更好地了解端点上发生的攻击；

终端威胁处置

- 能对恶意文件 / 进程进行全网追溯和全方位处置，通过自定义全局搜索或者通过 YARA、高级语言语法、高级威胁检测规则等对终端进行全面的数据调查，快速定位全网感染终端，并针对发现的威胁定义对应的处置策略。

威胁行为检测

- 通过深度学习、大数据关联分析、高级威胁引擎实现实时入侵检测，并提供毫秒级报警并处置；



业务价值与方案优势

防护从被动到主动

联软的安全自适应架构实时监测端点安全状态，第一时间发现和溯源威胁，完善体系建设防止未来攻击

检测从粗略到精准

实时端点监控结合大数据分析精确识别未知风险，实现无间断入侵监测，快速响应，提供毫秒级报警

响应从缓慢到快速

EDR的检测响应能力与专业安全响应流程相结合，助力安全人员快速确定威胁范围和影响，及时止损，提高响应效率

独创技术

支持多种语法方式，实现不同维度的自定义，满足复杂规则定义和开源规则使用，可复用已积累的专家规划库

协同从单点到整体

联软UniEDR天然与EPP平台无缝集成，可实现统一平台统一客户端的一体化管控，减少终端资源占用和员工抵触心理。平台自带Syslog、WebServer、Web API等多种数据传输接口可以与企业内部威胁检测响应框架集成

UniAV终端防病毒系统方案

需求背景

在当今数字化的时代，计算机病毒的形态和传播机制正日益多样化与复杂化。为应对这一挑战，终端防病毒的措施不能再局限于单一维度的检测和清除。

技术维度：随着病毒技术的进步，它们的侵入性、隐匿性和破坏性都在加强。我们需要一种能够不断迭代、适应新型威胁的防病毒机制，既要能够对付传统的病毒，也要对抗日益先进的恶意软件和零日攻击。

策略维度：除了技术，有效的病毒防护还需基于深入的风险评估和策略规划。这要求我们构建一个多层次、立体的防护体系，从物理层到应用层，从入侵检测到数据恢复，为企业IT资产提供全方位的保护。

解决方案

UniAV 防病毒系统是联软面向企业客户的端点综合安全防护软件，其内置下一代威胁检测引擎，为各类端点场景提供多层次、全周期的动态防护能力。

资产与设备全方位安全

- 资产注册登记：全景视角的资产可见性，确保每一个 IT 资产都在守护之中；
- 软硬件管理：不仅仅是管理，更是为了确保软硬件合规性，减少潜在的安全隐患；
- 安全 U 盘管理：移动存储，也能安全无忧；
- 外设管控：对于连接系统的每一项外设都给予足够的关注，确保没有安全死角。

实时监测与响应

- 防病毒引擎：高效、智能，我们的引擎始终在您的前线抵御恶意软件；
- 广告拦截：使电脑不被恶意广告打扰，提供安全的办公环境；
- 高危端口监控：帮企业紧锁每一个可能的入侵之门；
- 勒索诱捕：主动出击，设下陷阱，确保勒索软件无处遁形；
- 日志报表：透明且详细的日志，对企业的安全状况了如指掌。

数据保护

- 数据备份：即使遇到紧急状况，也确保企业数据能够迅速恢复，让业务不受打扰；

网络与应用防护

- 浏览器保护：网络首页锁定，防止恶意篡改；
- 黑白软件名单：完全掌控哪些软件可以在系统上运行，确保应用的安全；
- 禁止非可信可执行程序落地：不给未经验证的程序留下落脚之地。

业务价值与方案优势

全方面安全保护

- 资产保护：不止于病毒防护，它提供了360 度的资产和设备安全视角，确保从软硬件到移动存储设备都得到全面保护；
- 多维度防护：不仅可以查杀常见的病毒、木马、蠕虫等，还具备勒索病毒的专项防护能力；
- 主动反击策略：采用勒索诱捕技术，实现对勒索软件的主动识别与阻断。

提高工作效率

- 广告弹窗拦截：更清爽的办公体验，减少干扰，大幅减少恶意广告带来的风险；
- 智能自动备份：自动备份核心文件，减少因恶意攻击造成的数据损失风险。

成本效益

- 一体化解决方案：整合常规的防病毒功能与多项高级威胁防护，减少了多个产品和服务的维护成本；
- 良好的扩展性：可满足客户对于终端一体化、数据防泄密等需求。

外部攻击面管理解决方案

需求背景

资产泛化导致企业攻击面扩增：大量新技术应用于业务场景，引发了企业受攻击面的蝴蝶效应，组织运行的边界正在不断被打破，资产数字化成为不可逆的大趋势，原来相对封闭的组织攻击面迅速扩大，除了传统的互联网IP、域名、端口、漏洞等有形资产外，影子资产、App、公众号、小程序、SaaS应用、API，还有复杂的软件供应链和关联机构都可能成为攻击利用点，暗网、论坛、文库、网盘、开源社区、社交媒体等平台也可能泄露企业敏感信息，带来数据泄露和入侵的风险。

攻防极度不对称，防守人员亟需获得攻击者视角：在网络安全“体系化、实战化、常态化”的指导思想引领下，组织的网络安全建设需要从安全合规导向演进到能力导向和实战对抗，目前防守方能力往往滞后于攻击者，企业构建的防御体系更多聚焦在已知信息系统的漏洞发现与修复上，并不能保护“看不见的资产”，亟需获得攻击者视角。

攻击面管理缺乏顶层设计及优良实践参考：当前大部分组织仍然采用渗透测试、安全服务、资产测绘等人工服务或半自动化的方式进行，缺乏主动化、持续化的技术手段，更缺乏可参考的精细化运营策略，帮助攻击面管理构想落地。

解决方案

联软科技魔方安全外部攻击面管理系统 EASM(SaaS) 以攻击者视角自动化、智能化对企业数字化资产进行持续发现、分析和风险监控，结合多维安全情报，SaaS 专家顾问团队 1 对 1 支持，为客户及时输出高价值情报与服务，共同构建企业互联网攻击面管理“全景视图”。

影子资产精准监控

- 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，输出企业已知台账外的未知资产，即影子资产。大幅降低影子资产存在风险，减少被监管单位通报的风险。帮助用户自动发现、研判、纳管，让“不可见”无所遁形，让“不可控”尽在掌握；

漏洞深度检测与响应

- 平台具备强大的 PoC 插件检测能力，内置 4000+PoC，支持 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，并支持单个 / 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，通过自研的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，实现主动监测。运营团队将协助用户对信息泄露的对象进行下架处置，及时阻断数据泄漏。

数字资产全面可见/统一纳管

- 用户只需要提供主域名，系统会根据主域，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”；

组织风险完整监测

- 通过单位名称自动化分析集团型组织的股权关系，辅以自动化、智能化的资产盘点和风险监测，可获得组织当前完整的暴露面台账为组织视角的攻击面管理，提供强有力的技术支撑；

业务价值与方案优势

互联网资产“一本账”

IT 信息资产 + 新型的数字化 = 资产一本账，持续监测“影子资产”

风险持续监测与快速收敛

结合魔方持续更新的漏洞情报库，HW/ 高危漏洞事件爆发，第一时间知晓影响面

敏感信息泄露有抓手，能下架

先于监管和攻击者发现开源社区、网盘、文库等渠道的敏感信息，协助下架处理

对齐行业头部最佳实践

基于持续沉淀的行业最佳实践，通过持续迭代的产品能力 + 优质运营服务，对齐行业头部

全方位的管家式服务

技术 + 情报 + 运营能力持续交付，暴露面治理专家经验

幻影系统解决方案

中煤集团山西有限公司

需求背景

企业攻防视角需要转换：当前，主流的网络安全观点是：进攻容易，防御不对等，这与《战争论》里认为防御方有优势的观点相悖。实际上防御方有战略纵深的优势，如：系统数量多、地域分布广、网络复杂等，而攻方的劣势有：对网络架构不熟悉、全面入侵需要时间、挖掘关键系统的漏洞成本极高、高技能的人时间资源不足等，企业在做安全规划时视角需要转换。

低成本加强防御优势：利用欺骗的技术，通过低成本的方式，将战略纵深优势发挥到极致，通过大量生成的仿真设备，对网络中的入侵攻击行为进行诱捕；攻击欺骗（Deception）是Gartner从2015年起连续四年列为最具有潜力安全技术的新兴安全技术手段。

网管域、备份域等核心区域安全亟待提升：针对企业的核心区域如备份域、网管域本身网络流量相对较少的特点，通过幻影欺骗技术的部署，提升黑客攻击难度、及时准确发现入侵。

解决方案

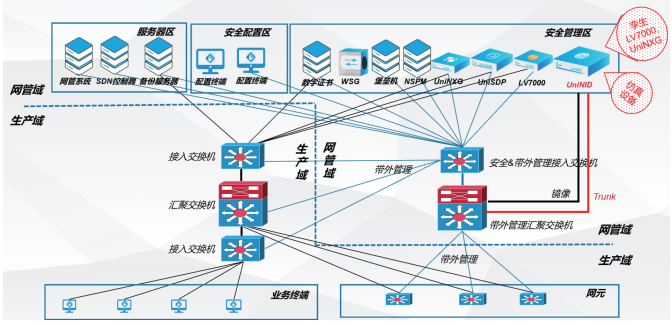
参照《战争论》的思路，利用网络空间里的地形特征，让防御方有优势。联软科技精心设计了利用欺骗技术的幻影系统，通过网络欺骗，让整个网络中布满了虚假目标，提升监控的效率，一旦访问伪冒的系统服务，就会被记录并提前预警，为企业安全管理员争取足够的处置时间。用低成本的方式，极大地增强了防御纵深，并且提高了发现入侵的准确性。以下是联软幻影系统的主要步骤：

设备资产发现与识别

- 通过网络流量或者主动探测技术发现和识别现网中的设备，设备发现和识别是智能幻影的基础；

智能幻影

- 根据用户网络中的设备的类型和数量智能生成大批量的仿真设备，并通过主动诱捕技术将攻击行为引诱到仿真设备上，主动捕捉异常或恶意行为；



系统联动

- 告警信息可以短信、电子邮件发给管理员；syslog 日志发给 SIEM、SoC、态势感知等系统，进行统一分析；幻影支持跟第三方蜜罐联动，可对攻击行为做进一步分析；

流量分析

- 通过流量分析提升威胁检测精准度。

业务价值与方案优势

发现快

只要有人访问了假目标，可快速被判断入侵（大概率），让安全管理员更早、更快地发现攻击行为

发现准

在企业核心区域如网管域和备生产域部署，通过幻影欺骗 + 流量深度检测，可以更精准地识别攻击行为

提高攻击成本

可以仿真出数十倍的 IP、端口，让黑客在迷宫中打转转，消耗其时间

攻击武器缴获

配合仿真的业务系统，可缴获黑客的攻击武器

终端安全一体化解决方案

需求来源

终端管理越来越复杂：随着5G、物联网技术的发展，企业上云、终端移动化对企业网络边界安全、数据安全、应用安全带来新挑战，越来越多的终端类型涌现在企业网络中。

整体规划，更高 ROI：传统查漏补缺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，企业需要从整体规划考虑，在用户、设备、数据、权限、行为等方面对网内所有终端进行统一安全管理，提升整体防护能力和运营效率。

解决方案

以联软 ESPP 企业安全监测保护平台为基础的《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，帮助企业建立涵盖终端准入控制、桌面运维管理、数据防泄密、文档安全、终端检测与响应、防病毒等子系统于一体的统一管控平台，具体功能如下：

用户设备接入可信

- 统一管控用户设备的网络访问权限，以人为中心的统一安全管理。

终端桌面运维可管

- 涵盖终端安全基线加固、终端标准化管理、运维支撑。

终端数据流转可控

- 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密保护，通过敏感检测、水印、文档加密、文档追踪等技术进行泄密数据的快速发现、收集、智能分类、流转追溯、风险管控。

终端威胁风险可防

- 丰富数据采集能力，海量数据快速查询能力，识别安全风险，发现威胁事件，调查取证，威胁响应，处置修复。

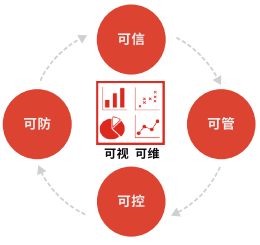
全网终端资产可视

- 对网内 PC、移动终端、IoT 设备进行自动发现、设备类型识别。

终端统一管理可维

- 一个 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、行为审计、数据防泄密、文档安全、终端检测及响应等端点安全管理全场景覆盖，高效运维，更高 ROI。

方案部署后



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”

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设备类型终端的集中管控，相比传统方案：

整体规划
一个平台、多种技术、综合解决网络与安全问题

管理统一
安全数据统一汇总，关联分析、机器学习、智慧决策

效率提高
大幅提升管理效率和用户体验

经验积淀
持续 20 年端点安全开发与投入，为 3000 多家高端行业客户提供服务

办事大厅终端安全管控解决方案

国家开发银行 CHINA DEVELOPMENT BANK　浙江农信　中国电信 CHINA TELECOM 江苏

需求来源

办事大厅业务需要：如银行、运营商等，为方便业务开展，放置在办事大厅的客户体验专用设备（平板电脑、智能手机、PC一体机等）数量逐渐增加。

统一安全管控需求：办事大厅专用设备接入互联网时，无法对它们进行集中、统一的管控，安全管理面临较大风险。

解决方案

以联软 ESPP 企业安全监测保护平台为基础的《办事大厅终端安全管控解决方案》，可以解决智能化网点建设带来的多种问题。

该方案包括

集中管控

- 通过建立 EPP 集中管控中心，对智能化网点客户体验终端，包括平板电脑、智能手机、PC 一体机等，进行设备的统一管理。

远程控制

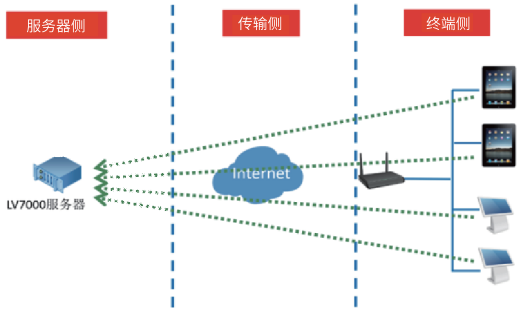
- 在终端上安装管控客户端（Agent）对终端进行远程控制，禁止客户修改体验终端的系统密码、系统参数和下载无关 APP 应用，统一软件分发，建立应用商城，以及全面审计。

网络接入认证

- 要求终端接入各网点无线 WiFi 时进行认证和合规检查，未安装客户端的设备将不能进行认证，无法接入网络；未通过安全策略检查的设备将进入隔离区，修复后重新发起认证及检查流程，防止外来设备违规接入。

客户免费WiFi服务接入认证

- 为客户在等待业务办理期间提供免费 WiFi 接入管理。



业务价值与方案优势

该方案实现对包括 Windows、macOS、iOS、Android 在内的各种操作系统智能终端的集中管控，在同一个系统中实现网络接入认证管理和客户免费 WiFi 服务接入认证管理，大幅度提高设备运行效率，提高对设备的统一管理能力，同时也降低后期设备维护成本，总体提升系统的部署效率和运行保障能力。

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

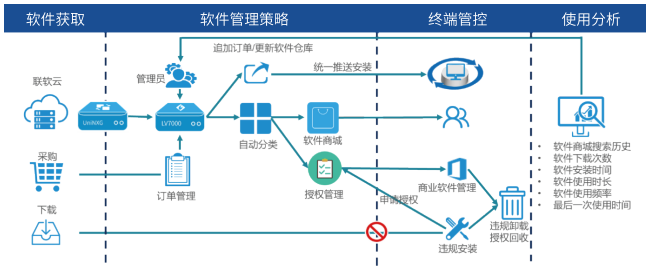
- 同时支持对信创终端的软件正版化、标准化管理。

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

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

信创终端安全一体化解决方案

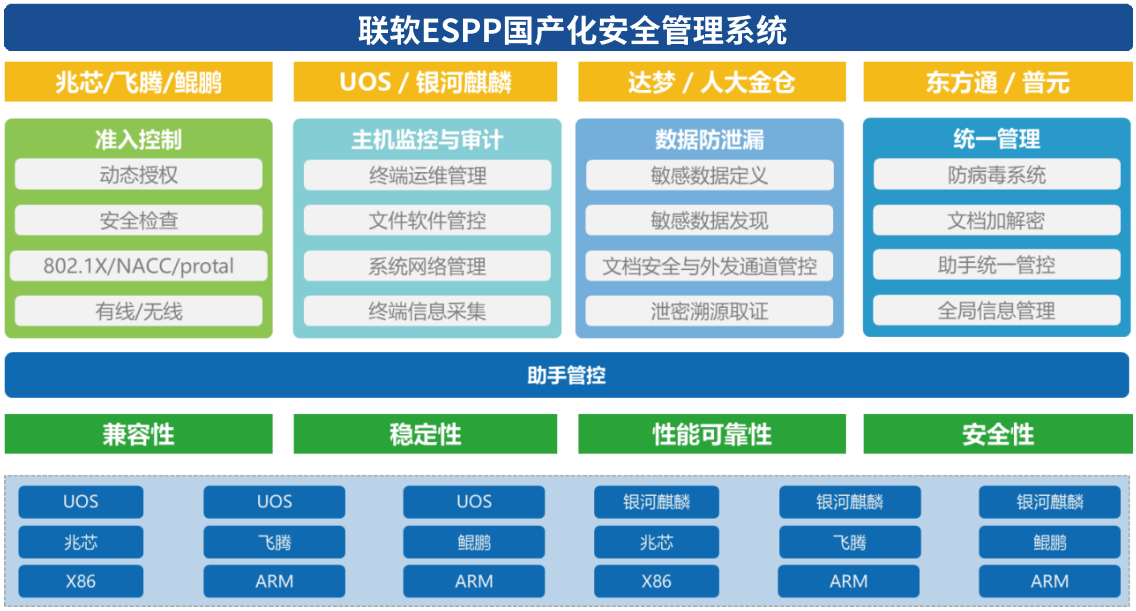
需求来源

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

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