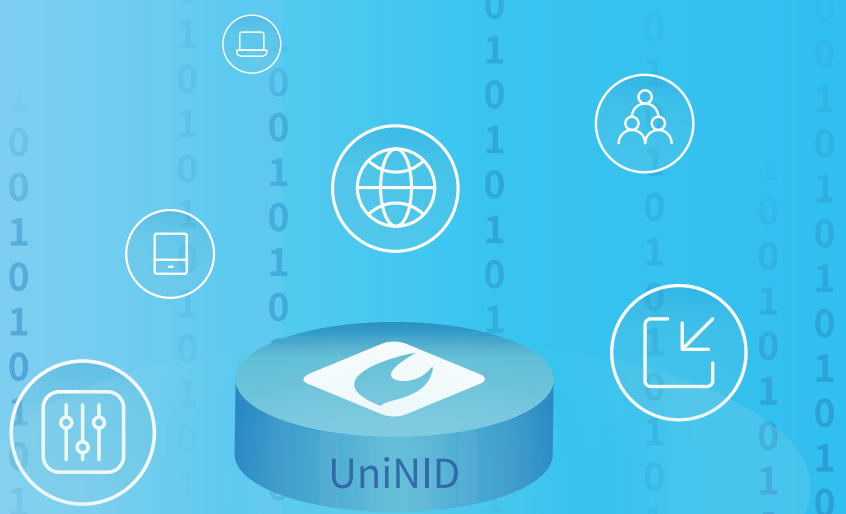
联软科技
LEAGSOFT

UniNID网络智能防御系统

准确发现未知类型攻击的新一代智能化网络安全基础设施



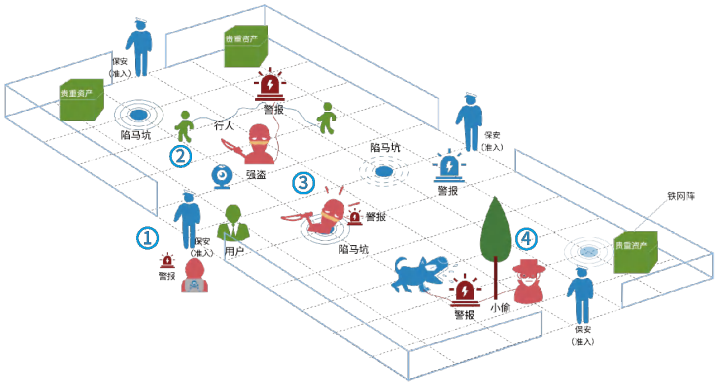
深圳市联软科技股份有限公司

UniNID网络智能防御系统

产品概述 Product overview

联软网络智能防御系统（简称：UniNID）是一款软硬件一体、无感知旁路部署的企业网络安全防护产品，创造性地把网络智能准入、网络威胁与异常行为发现、智能诱捕及处置等技术结合起来，成为新一代的智能化网络安全基础设施。

UniNID基于联软自主研发的数据处理引擎，通过高质量的数据来源与机器学习，帮助企业识别内网安全风险，通过基于伪装欺骗技术的动态“陷马坑”精准及时发现已知与未知威胁。通过在边界布控智能准入的“铁网阵”准确定位和处置风险。UniNID是企业防范勒索软件、僵尸主机等APT攻击，发现威胁、识别风险、合规遵从的最佳选择。UniNID不仅可以独立部署，还可以与联软UniEDR等产品联合部署，实现更完整全面的安全保护。



UniNID网络智能防御布控图

产品型号 Models

UNACC-5021

- 内置200点无代理准入管理控制中心许可；
- 单电源，4个千兆网口，保修12个月；
- 最大认证并发数100个/秒；最大支持200台幻影设备（支持瘦终端、IoT设备、ICS设备），2个幻影网段。

UNACC-5051

- 内置500点无代理准入管理控制中心许可；
- 冗余电源，6个千兆网口，可扩展2个万兆光口（需单独配置万兆模块），保修12个月；
- 最大认证并发数250个/秒；最大支持500个幻影设备（支持瘦终端、IoT设备、ICS设备），4个幻影网段。

UNACC-5101

- 内置1000点无代理准入管理控制中心许可；
- 冗余电源，6个千兆网口，可扩展2个万兆光口（需单独配置万兆模块），保修12个月；
- 最大认证并发数500个/秒;最大支持1000个幻影设备（支持瘦终端、IoT设备、ICS设备），8个幻影网段。

UNACC-5201

- 内置2000点无代理准入管理控制中心许可；
- 冗余电源，6个千兆网口，可扩展2个万兆光口（需单独配置万兆模块），保修12个月；
- 最大认证并发数1000个/秒，最大支持2000个幻影设备（支持瘦终端、IoT设备、ICS设备），16个幻影网段。

UNACC-5501

- 内置5000点无代理准入管理控制中心许可；
- 冗余电源，6个千兆网口，可扩展2个万兆光口（需单独配置万兆模块），保修12个月；
- 最大认证并发数2000个/秒;最大支持5000个幻影设备（支持瘦终端、IoT设备、ICS设备），32个幻影网段。

UNACC-5901

- 内置20000点无代理准入管理控制中心许可；
- 冗余电源，6个千兆网口，2个万兆光口，可扩展2个万兆光口（需单独配置万兆模块），保修12个月；
- 最大认证并发数2000个/秒；最大支持20000个幻影设备（支持瘦终端、IoT设备、ICS设备），64个幻影网段。

NACC-5050H

- 两个千兆网口；
- 支持集群部署；
- 支持设备发现和设备信息采集；
- 支持仿冒处置；
- 支持设备在线、离线状态检测；
- 支持有线、无线方式接入网络，支持自动升级；
- 支持对接UniNID单机、双机热备以及分布式管理中心，单台NID设备最大支持20台硬件探针；
- 支持并发处理200个ARP包。

产品方案 Solutions

产品适用场景 Application scenarios

全网资产管理

- 集成了多项设备发现检测技术，新接入设备能够实现秒级发现，支持用户自定义设备分类规则，支持自定义设备分组，具有极高的设备识别精度。

保护网络安全底座安全

- UniNID是网络安全底座解决方案四大功能组件之一，部署在网管域、备生产域，可以极大提升黑客的攻击难度，大幅缩短发现入侵的时间周期，缴获入侵者的武器，有效提升网络安全底座的安全性。

无代理智能准入

- 企业终端设备无需任何Agent，就可实现终端的准入。企业网中的PC设备、移动终端、哑终端（打印机、摄像头）等设备可以使用“设备指纹”完成免检准入。

IoT设备准入与仿冒检测

- 可实现物联网（比如金融系统、医疗系统，政府的雪亮工程、平安城市、智慧城市等）IP设备准入控制和仿冒检测。

产品功能 Functions

网络布控

- 自动发现：自动发现网络上所有在线资产，而且能自动区分资产；
- 边界布控：提供强制认证与智能认证两种方式，既可按设备指纹进行认证，又可结合设备使用者账号进行鉴别与认证；认证未通过的设备自动阻断或隔离其网络访问；
- 资源访问控制：自动按照设备的类型、安全状态、指纹特征、使用者身份等信息，自动下发ACL到网络接入控制点，控制其所能访问的网络资源；
- 动态“陷马坑”：根据用户网络在线的设备动态生成大批量的幻影设备，并通过主动诱捕技术将攻击行为引诱到幻影设备上。

合规检查

- 安全设置：自动发现不合规的文件共享、匿名登录、补丁服务器、DNS服务器、代理服务器等设置；
- 软件安装：自动识别是否安装防病毒软件等必要的合规软件；
- 弱口令检测：支持检测Web/SSH/TELNET/FTP等应用的弱口令，支持用户导入自主的账号和密码字典；支持摄像头弱口令检测，内置原厂默认账号和密码；
- 漏洞检测：与魔方CSM联动，可以发现终端、服务器等的脆弱性；
- 补丁安装情况检测：与联软LeagView平台联动，可以发现终端、服务器等的补丁修复情况。

风险感知取证

- 危险行为感知：智能感知针对高价值资产的异常访问与攻击；自动检测已知的危险行为；智能发现未知危险行为；
- 异常行为感知：智能感知设备仿冒、慢速攻击、异常连接、异常流量、异常协议、异常域名与IP访问、异常时段访问、异常访问位置等异常行为。

风险处置

- 控制：跳转修复，设备下线，重认证；
- 取证：全景视图、风险趋势、攻击路径、取证报告；
- 告警：通知事件中心（SIEM/SOC）、态势感知平台、XDR平台、管理员、使用者。

产品特点 Features

- 准确及时发现入侵，保护高价值资产，防止数据破坏与泄露；
- 提高效率，自动化智能化让安全合规、安全管理工作更简单；
- 高投资回报，与NAC系统融合，一套系统解决多方面问题。

方案优势 Advantages

安全可视化

- 资产可视化：集成了多项设备发现检测技术，自动发现网络资产，识别高价值资产（如数据库、源代码服务器、域控服务器、ERP服务器等），可视化展现资产的状态、类型、位置、使用者等信息；
- 行为可视化：自动识别设备与用户行为，可视化展现访问关系和使用习惯；
- 攻击可视化：识别网络攻击，可视化展现攻击入侵路径、横向移动过程、攻击方式等。

风险精准识别

- 通过自主与第三方威胁情报进行黑名单识别；
- 通过高质量的大数据与AI算法实现精准识别，高质量表现为数据自行从源头直接采集、加工，避免数据失真；另外高质量还表现为数据维度多，包括设备的类型、安全状态、使用者、接入位置、接入时间、网络行为、访问对象、使用习惯等信息；
- 区别于传统的准入一次性合规检查，从脆弱性、异常行为、威胁行为多维度对设备进行安全评分，有效发现未知威胁，精准发现内部失陷终端。

部署简单、兼容性强、扩展性强

- 设备采用旁路部署的方式，无需修改现有的网络拓扑，配置简单，开箱即用；
- 适应各种网络接入场景：支持多种准入控制技术，适用于LAN、WLAN、NAT、分支机构接入等各类复杂环境，且技术成熟稳定，通过多重冗余保障技术实现网络准入的高可用性；
- 多种部署模式：支持轻代理/无代理终端部署模式，兼容各厂商网络设备；
- 支持分布式部署和集中部署，管理中心支持线性扩展（集群）。

风险监控告警处置

- 实时监控：NID安全态势大屏持续监控；
- 告警通知：可进行页面告警，并支持通过短信/邮件/SYSLOG主动通知管理员；
- 响应处置：网络隔离（关闭交换机端口、802.1x强制下线、VFW过滤）；联动联软UniEDR，进行溯源取证。

发现未知类型攻击

- 动态“陷马坑”：通过幻影技术并联动蜜罐，以诱捕的方式发现攻击，无需知道攻击类型亦可捕获攻击行为；
- 通过大数据和机器学习算法发现未知类型攻击，包括画像式发现、关联分析、可疑域名分析等。

部分典型客户 Some Typical Customers

金融行业

华西证券 HUAXI SECURITIES | 中金财富 CICC Wealth Management | 南方基金 CHINA SOUTHERN FUND | 华泰期货 HUATAI FUTURES | 国信证券 GUOSEN SECURITIES | 中国进出口银行 THE EXPORT-IMPORT BANK OF CHINA
中国民生银行 CHINA MINSHENG BANK | 华夏基金 | 光大证券 EVERBRIGHT SECURITIES | 中国建设银行 China Construction Bank | 中信证券 CITIC SECURITIES

能源行业

ENN新奥 | 贵州电力设计研究院有限公司 | 中核能源科技有限公司 CHINERGY CO., LTD. | 深圳能源 SHENZHEN ENEAGY | 国家电投 SPIC | 中国电力工程顾问集团中南电力设计院有限公司
中国南方电网 深圳供电局有限公司 | 中国南方电网 广东电网广州供电局 | 中国南方电网 贵州电网有限责任公司 | 广东电网公司 | 中国华能集团公司（香港） CHINA HUANENG GROUP | 国家电网 STATE GRID 国网北京市电力公司

运营商

山东移动 | 中国电信（海南） CHINA TELECOM | 产业互联网专家 | 中国移动通信（四川） CHINA MOBILE | China unicom 中国联通（重庆） | 中国移动通信（河南） CHINA MOBILE

政府行业

厦门市政 | 中华人民共和国海关总署 | 国家电网 STATE GRID 江苏省电力公司 | 四川省人民政府国防动员办公室 四川省人民防空办公室 | 中国核动力研究设计院 | 中华人民共和国南京海关
福建档案信息网 WWW.FJ-ARCHIVES.ORG.CN | 北京市统计局 | 海南省人民政府 | 国家税务总局河北省税务局 | 国家信息中心 国家电子政务外网管理中心 | 中华人民共和国上海海事局

医疗行业

长海医院 CHANGHAI HOSPITAL | 中山医院 ZHONGSHAN HOSPITAL | 广东省人民医院 | 山西省人民医院

公安

日照市公安局 | 奉贤公安 | 静安公安 | 茂名市公安局 | 泰都区人民政府 | 五河县人民政府

制造业

mindray迈瑞 | CSPC 石药集团 | ZOWEE 卓翼科技 | liby立白 健康幸福每一家 | uniview 宇视科技 | YUTONG
西部超导 | 郑州日产 | RHEGEN | 中国机械设备工程股份有限公司 China Machinery Engineering Corporation | HBIS 河钢 | TOPBAND 拓邦 深圳拓邦股份有限公司

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