UniNID网络智能防御系统

透视每一个攻击过程，让安全更可控

随着互联网应用的深入，计算机系统安全和网络安全受到的威胁日益增加，传统基于特征的检测和防御技术已经无法应对目前新型网络攻击。

UniNID 网络智能防御系统使用世界领先的人工智能算法来检测企业内部其它防御工具检测不到的攻击。与传统基于规则和签名的方法，不同的是 UniNID 不依赖历史攻击来预测未来，它可以感知企业内部“正常”设备的行为，并且可以实时检测新出现的威胁，包括勒索病毒、APT 攻击、设备仿冒、僵尸终端、慢速攻击等未知安全威胁。

主要功能

发现与识别

发现设备属性，包括设备名、IP、MAC、设备类型、接入位置等
识别正在使用终端的用户，自动区分员工终端和其它终端
识别网络中的勒索病毒、APT 攻击、终端仿冒、僵尸终端等潜在威胁

控制与保护

根据终端类型、用户身份、接入位置分配网络访问权限
根据设备安全指数实施控制，阻止威胁扩散，保护全网安全
与联软 LeagView 平台联动，保护企业数据安全

可视化展现

展现全网风险状态
展现布控全景
展现入侵视图及过程

主要优势

自动学习

内置 AI 引擎，根据设备的变化不断优化算法模型

主动诱骗技术

通过主动诱骗技术，快速发现威胁

数据源质量高

网络和终端的一手数据采集能力

大数据分析平台

100%自主研发大数据分析平台，实现 10 亿级数据秒级查询

主要价值

安全可视化

识别资产，将用户和终端建立联系，联动 LeagView 平台，还原攻击过程

更快、更准的发现威胁

全方位多角度发现和分析未知威胁，准确即时识别风险

智能防御

随着设备安全指数降低，逐级提升风险等级，阻断通讯，防止扩散

典型应用场景

视频网准入与防仿冒

工控网反 APT

企业网反 APT 和反勒索

企业网无代理智能准入

企业网安全态势感知