**用户手册**

# 产品介绍

## 系统功能简介

### 内网防入侵

将网络接入管控、终端与服务器设备管控、木马查杀/异常行为分析/入侵智能诱捕/威胁情报等安全技术有机整合，形成一个智能化的防内网入侵与态势感知体系，防范外来黑客侵入内部网络。

* **网络发现**

自动发现网络设备、接入设备、网络拓扑；自动发现接入设备的类型，包括：终端操作系统、受控类别、IoT设备类型；自动发现设备的接入方式及接入位置，连接的交换机及其端口或无线热点。

* **身份识别**

识别正在使用终端的用户，自动区分员工终端和其他终端。

* **态势感知**

智能感知防病毒软件安装、匿名登录、补丁设置等合规配置；智能感知设备仿冒、异常连接/流量/协议等行为；智能感知端口异常、暴力破解、渗透攻击、僵尸主机、勒索软件等攻击行为。

* **智能处置**

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，通知事件中心（SOC/SIEM），阻止威胁扩散，保护全网安全。

### 终端标准化

* **集中管控**

策略统一下发，数据统一汇总，终端统一升级，软件统一管理，桌面壁纸屏保统一设置，终端漫游管理。

* **安全管理**

支持补丁管理、安全基线管理、权限管控等功能。

* **外联管控**

支持网络访问控制、违规外联管理、移动存储管理等管控策略。

* **行为审计**

支持主机监控、上网审计、即时通讯审计、文件操作行为审计等功能。

### 软件管理

可自动对终端的软件信息进行采集，实现软件的资产管理，并支持对软件进行正版化和标准化管理，平台还提供软件分发、软件商城、工具箱等功能。

* **软件资产管理**

自动采集终端上已安装的软件信息，建立企业的软件信息库，可集中对软件信息进行统计分析。

* **软件正版化**

支持对商业软件进行订单管理，可在系统内维护商业软件的台账信息，可将其导出后，提交给国家版权局。支持对终端上安装的商业软件进行授权管理，对违规安装商业软件的行为进行检查和整改，避免企业因员工违规安装商业软件而造成的诉讼风险。

* **软件安装卸载管控**

可对终端安装软件的行为进行监控和授权，未授权的终端无法进行软件安装，配合企业软件商城，可实现只有通过软件商城才能安装软件，有效解决软件供应链安全和软件的标准化管理，降低运维成本，有效提升企业整体运营效率。

* **软件使用分析**

支持对软件的使用时长、频率、最后一次使用时间等维度进行统计分析，以帮助企业了解用户的软件使用状况，为企业的商业软件采购和员工工作效率提供数据支撑。

* **软件商城**

为企业提供软件上架、发布、授权、安装、更新、卸载的统一门户，支持大规模软件的快速分发，帮助企业建立自己的软件商城。

* **软件分发**

支持将软件进行统一分发和自动安装。

### 数据防泄露

将网络接入管控、终端与手机设备管控、DLP/沙盒/加密/水印/数据流转管控/文档追踪/行为与内容审计等数据管控技术有机整合，形成一个覆盖各种场景的数据防泄露体系，防范敏感数据被内部人员泄露或外来黑客窃取。

* **定义与发现**

支持通过数据来源、文档内容定义是否敏感，通过对文档格式的识别和文档内容的感知，实现对终端数据的智能分类、分级及可视化展现。

* **控制与保护**

通过外发通道管控、访问权限控制、安全计算环境隔离、数据安全流转、行为审计与追溯等功能与技术，打造完善的数据安全防护与信息防扩散系统。

* **协同与联动**

与安全数据摆渡系统协同，实现跨网或网内不同用户间的数据安全流转，通过与UniNAC准入控制系统协同，实现资源访问控制。

### 终端防病毒

* **病毒/木马查杀**

动态模拟检测技术，提前预判恶意行为，基于海量样本的全体系支撑，后台云计算平台提供病毒DNA解析大数据处理，支持智能打击恶意病毒。

* **主动防御**

根据样本一系列的行为特征来进行综合的风险判定，其监控和判断能力由后台的大数据训练集群支持。比传统的根据简单的单步行为规则来做监控的主防技术安全系数更高，捕获风险能力更强。

* **实时监控、智能处理**

对设备进行实时监测，出现病毒威胁时，会根据设置，自动删除病毒文件，或者锁定病毒文件禁止其运行，等待处理。

### 企业移动终端管理

* **完整的设备生命周期管理**

设备注册、设备识别、设备绑定、设备注销、设备丢失、员工离职。

* **强大的管控指令**

远程定位、解锁屏幕、单一应用限定、应用黑白名单、基于地址围栏的策略下发。

* **配置推送**

通过管理平台远程推送VPN、WiFi、Email等配置。

### 统一管控平台

通过网络准入控制、资产自动发现、安全策略强制执行等技术手段，让安全管理规定落地，实现安全合规；同时平台下子系统提供多种资产管理、远程运维、Braise脚本语言、集中管控等手段，提升IT运维效率。

* **All In One**

所有功能通过一个平台、一台设备、一个客户端实现；

* **安全流程管理**
* 遵循ISO27001等国际**先进**的管理模型，对安全事件进行主动预警、及时处置、自动修复，并定期形成安全报告；
* **资产生命周期管理**

软硬件资产自动发现，建立完整的资产清单，设备配置变更管理，软件正版化管理，资产盘点管理；

* **数据生命周期管理**

对数据在产生、存储、流转、外发等各阶段进行敏感数据的自动发现和分类分级管控；

* **分级部署与漫游管理**

支持对大型分支网络的分级管理，同时针对不同分支之间进行漫游管理；可实现管控安全策略自动同步到不同的分支，各二级分支机构的接入信息自动上传到总部的一级服务器中；

* **平台自监控管理**

可维护信息包括服务器名称、地址、当前版本、运行状态、磁盘空间、CPU负载、内存使用率；支持在控制台查看后台服务、进程运行状态，并可手工进行启动/停止等维护操作。

# 服务与支持

如在使用本产品出现任何问题，联系lijian@leagsoft.com获取技术支持。