

UniAccess 终端安全管理系统

业界功能最强大的终端安全管控系统

UniAccess 终端安全管理系统帮助企业搭建集中管控平台，提供资产管理、补丁管理、企业软件管理、用户操作权限管控、安全状态评估、主机监控审计、上网行为管控、移动存储介质管理、桌面运维管理等主要功能模块，解决终端的各种安全管理问题和满足各种合规需求，是业界最为强大的终端安全管理软件。

主要功能

集中管控

- 资产管理：终端入网自动发现，自动收集终端软硬件资产信息，设备快速定位；
- 分级部署：支持多级部署架构，策略统一下发，数据统一汇总，终端统一升级，桌面壁纸屏保统一设置，终端漫游管理；
- 远程协助：本地免开端口，NAT 远程独家支持，支持 MAC OS；
- 软件管理：软件统一推送、统一卸载、企业软件商店、工具箱、正版软件授权管理、软件标准化管控，软件自动分类，软件使用时长管控。

安全管理

- 补丁管理：支持 Win10，智能中继，支持与 WSUS 联动，内网自动安全导入补丁，秒级漏洞检查；
- 安全基线：支持密码、屏保口令、AD 域、共享目录、计算机名、注册表、文件、系统、进程、服务、杀毒软件等检查；
- 权限管控：组策略、注册表、网络、服务等设置，软件卸载权限、进程黑白名单管理、IP-MAC 地址绑定。

外联管控

- 网络访问控制：内置终端个人防火墙，自定义访问控制列表，自定义触发场景，网络流量统计及网络异常检测；
- 违规外联管理：可禁用和审计自检 WiFi 热点、智能设备、双网卡、无线网卡、串并行接口、蓝牙、红外、光驱等行为；
- 移动存储管理：支持 U 盘、移动硬盘、移动智能设备等进行注册、授权管理及拷贝审计，支持加密 U 盘。

行为审计

- 主机监控：对主机的软硬件配置变更，系统账号、设置变更，事件日志采集，屏幕录像；

- 上网审计：对上网、发帖、网盘上传、BT 下载等进行审计与控制；
- 即时通讯：对 QQ、微信、钉钉等数十款即时通讯工具进行审计，对聊天内容、收发文件、图片进行场景化还原，可对敏感内容进行告警；
- 文件操作：对 U 盘、共享文件夹、FTP 拷贝，打印、光驱刻录、导入导出等行为进行敏感审计和阻断。

主要优势

功能丰富

- 十多年数千家客户的经验与智慧，持续迭代优化，满足企业客户终端安全管理的绝大多数功能需要；
- 自带高性能文件审计服务器 LVFS，自带高性能海量数据处理引擎，内置 Braise 脚本语言，与防泄密、NAC 功能高度集成。

性能突出

- 容量大：单服务器支持 15 万+设备管控，支持集群部署，集群部署案例超过 60 万+设备；
- 资源小：一个 Agent 实现各种功能，对比同类产品，同等功能下 CPU、内存、磁盘空间等资源占用最少；
- 效率高：策略实时下发，管控实时生效，信息实时上传，文件快速分发，在亿级以上大数据量下查询速度快。

补丁管理

- 检查速度快，结果准确；
- 补丁安装速度快，智能安装与重试机制，成功率高；
- 支持补丁回退与蓝屏自动回退修复；大数据量情况下，报表与查询速度稳定；
- 支持隔离网络环境下的补丁自动下载安装；
- 支持与 WSUS 集成，支持 Win10。

稳定性与兼容性好

- 在稳定性方面，UniAccess 采用了网络与主机资源占用最小化设计，通过智能算法自动避开系统、网络资源使用高峰期，降低软件、补丁的分发对带宽的占用产生的影响；
- 在兼容性方面，Agent 经过微软数字签名认证、WHQL 认证，同时与多家安全软件厂商在产品上深入合作，确保 UniAccess 的良好兼容性。

主要价值

满足法律法规要求，防止内部信息泄密

避免网络、终端瘫痪，保障运营安全

集中管控，批量处理，简单有效，提升效率

典型应用场景

信息系统等级保护、上网行为与即时通讯审计、系统补丁管理、终端外联及 U 盘管控、桌面标准化管理、终端安全基线检查、企业软件管理、资产管理、终端流量管控、终端运维支持

