UniEMM企业移动安全支撑平台

将安全融入业务，为移动展业、移动办公保驾护航

UniEMM 企业移动安全支撑平台秉承联软科技“构建可控互联世界”的战略思想，采用先进的“零信任”安全架构设计理念，把安全隐藏在业务背后，为企业应用提供安全、快捷的部署环境，通过多平台多终端接入、业务 APP 统一的认证中心、统一的门户管理、应用级安全隧道，实现全业务开放，提供企业业务移动化的安全保障，实现差异化竞争优势。UniEMM 平台是目前证券行业实施规模最大、集成应用最多的移动安全支撑平台。

主要功能

移动应用管理（MAM）

- 完整的应用生命周期管理：登记、注册、发布、权限配置、升级、静默安装、卸载；
- 管理员可自定义应用发布类型、应用归属、应用图标、应用使用范围；
- 统一安全门户内置应用商店，应用安全检查，应用单点登录等功能。

移动内容管理（MCM）

- 云端：支持公有云或私有云部署，采用业界领先微服务技术架构，平台里每一个服务都可根据用户业务能力进行横向扩展，所有微服务在云端集中管控；
- 管道：安全网关提供应用级安全隧道；
- 移动端：应用安全沙箱、文档安全阅读、安全浏览器、安全邮件、安全 SDK、行为安全管控、数据远程擦除、公私分离。

移动设备管理（MDM）

- 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。

移动用户管理（MUM）

- 支持与企业 AD、LDAP、Email 等多种类型服务器进行联动认证；
- 支持与联软 UniRadius 认证服务器进行联动认证；
- 内置强大的用户组织架构，可实现用户与策略的灵活关联。

扫毒杀毒

- 病毒扫描：支持本地、云查、本地+云查三类扫描方式；
- 病毒清除：针对扫描结果，用户可以手动卸载和删除应用。

主要优势

功能

- 统一门户：同时支持原生应用和 HTML5 应用，支持数据安全存储、安全阅读，支持业务系统应用自定义水印，实现“门户+应用”的安全生态环境；
- 安全网关：基于应用的安全加密隧道，手机上的个人应用是无法通过安全隧道访问公司内部系统的，同时还可以基于应用、用户、设备关闭安全隧道，它细化了安全访问控制的颗粒度；
- 认证中心：内置 SSO 认证中心、PC 端 H5 应用门户，支持在移动安全门户获取动态口令用于 PC 端登录业务系统提供双因素认证的认证因子之一、支持业务系统通过注册调用认证中心接口生成二维码扫码登录、支持客户端动态生成身份码，在授权的情况下通过身份码到认证中心获取用户信息。

性能与扩展

- 网关单台系统最大并发用户为 64000+，最大吞吐率 2000TPS。支持线性扩展；
- 提供第三方功能扩展开发接口，可深度定制客户端、后台、管理页面。

可靠性与可用性

- 可靠性设计领先：产品采用业界领先的零信任安全架构，服务端采用微服务技术架构设计，根据现场实际应用场景每个服务可以横向扩展，提供业界最好的可靠性措施；
- 系统维护简单：管理台集中管理所有微服务，监控服务 CPU、硬盘、内存、进程等占用及运行状态，可设置预警阀值，有异常状况自动预警。

主要价值

- 减少企业配发设备采购成本，利用员工自带设备实现的安全的移动办公、移动展业；
- 国内最完整的移动化安全解决方案，不需要额外采购第三方 VPN 等设备，降低 TCO 和落地风险；
- 企业数据加密存储在沙箱中有效防止泄露，移动设备被窃或遗失后可远程擦除企业数据；
- 为企业应用提供统一的安全防护，降低开发门槛，提高开发效率，为企业业务快速创新保驾护航。

典型应用场景

金融行业

银行、证券、保险等金融行业员工通过员工自有设备及统一配发智能终端实现移动展业、移动办公，如信用卡办理，移动开卡，保险业务办理、移动 OA、移动邮箱等。

企事业单位

企业员工在智能终端上移动办公，实现工作区与个人区隔离，保障企业应用数据安全可控。

医疗

对医生查房、护士护理 PAD 或 PDA 专用设备进行强管控，防止病人隐私信息泄露。

政府执法单位

公安警员通过移动终端实现对公安内部网警务信息的访问来完成警务执法工作。法院、检察院执法人员通过智能终端完成移动执法、移动法务、移动检务等办公流程，实现整个流程相关移动数据安全防护。