YESsafe AppProtect+

移动应用实时保护

保护移动应用免遭破解 · 防止运行时外部入侵 · 提供回调API客制化开发

YESsafe AppProtect+ 是一种为应用提供实时保护的安全技术，它可主动保护应用，令应用即使在不安全的设备上运行时，也可免受恶意应用程序的攻击。AppProtect+ 提供回调 API，用户可以调用回调API以实现所需功能，例如：收集相关风险数据并报告后台。

AppProtect+ 与传统杀毒软件相比，它不需要更新病毒数据库或者联网，便可实现应用自我保护；与传统的应用加固产品相比，它可防止被动攻击（例如反编译、二次打包、修改源代码），也可主动侦测应用在运行时受到的实时攻击并作出即时反应，为应用提供全面且实时的保护，即使在传统加固产品保护较薄弱的 iOS 端 AppProtect+ 也能完美支持。

四大核心功能

防逆向、防篡改

防止 apktool、dex2jar、JEB 等破解工具对 APK 进行逆向工程、动态调试及内存攻击。唯一性验证技术可确保若 APK 内部任何信息被篡改，则 APK 包无法运行。

防调试

使用白盒加密技术防止恶意代码注入，彻底屏蔽游戏外挂、HOOK 攻击和利用系统辅助功能攻击，避免钓鱼攻击、交易劫持、数据修改等恶意行为。

防窃取

支持加密存储数据，提供可信键盘检测、阻断截屏事件、内存数据保护等，有效防止捕获、劫持和篡改应用的动态数据和静态数据。

服务器管理客户端

用户可调用服务端接口将移动端收集的数据传给服务端，服务端管理员可以根据基于这些数据制定的策略管控用户账号、设备使用权。

主要抵御的风险

- 模拟器调试移动应用
- 调试器攻击移动应用
- 恶意屏幕阅读器
- 恶意屏幕截图
- 运行时恶意代码注入
- 恶意键盘记录
- 设备越狱/ Root
- 二次打包
- Hook 框架攻击
- 代码逻辑泄露

安讯奔
安全认证 超越云端

功能清单

源代码保护
- Dex 文件混淆
- SO 文件混淆

移动环境监测
检查越狱/ Root，终止 App 运行，并可以通过回调函数通知服务端

App完整性保护
- 代码、资源文件、配置文件校验
- 校验异常，终止 App 运行，并可以通过回调函数通知服务端

防欺诈
- 防钓鱼欺诈
- 防恶意代码注入
- 防 Overlay 攻击
- 证书保护
- 防进程注入攻击

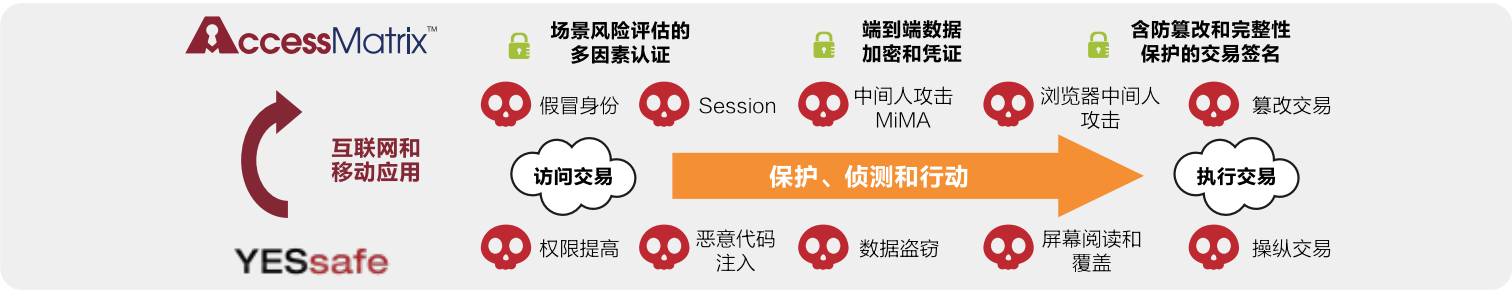
防逻辑泄露
- 防模拟器调试
- 防调试器调试
- 防 HOOK 攻击
- 防 dump 调试分析
- 防静态分析

数据保护
- 内存数据保护
- 防系统发起的截屏
- 防用户发起的截屏
- 防止投屏
- 防键盘记录
- 使用白盒加密技术保护数据

防篡改保护
- 防二次打包
- 防交易支付攻击
- 防账号密码泄露
- AndroidManifest.xml 修改检测
- 防止反编译
- 资源文件保护

核心优势

AppProtect+ 基于客户端发生的风险事件做出响应，结合 AccessMatrix 产品实现保护，侦测，响应的全过程，在保护应用过程的生命周期中不漏掉一个环节。



保护
防止恶意入侵

- ✔ 代码混淆
- ✔ 应用绑定
- ✔ 应用隔离
- ✔ 通讯数据保护
  - TLS 证书绑定
  - 基于设备与应用的强认证
- ✔ 本地数据存储保护
- ✔ 加密数据绑定设备
- ✔ 白盒加密
- ✔ 应用管理解决方案
  - 将可信的用户，应用，设备相互绑定
  - 无需外部安全令牌标注可信应用
  - 在注册/激活时安全的将应用/设备与用户进行匹配

侦测
侦测运行时攻击

- ✔ App进程监控
- ✔ 二次打包侦测
- ✔ App 运行环境侦测
  - 调试器侦测
  - 越狱或 Root 侦测
  - 模拟器侦测
- ✔ 运行时恶意攻击侦测
  - 截屏事件侦测
  - 键盘读取侦测
  - 屏幕覆盖侦测
  - 投屏事件侦测

行动
反制攻击

- ✔ 通过可配置的方式可实现
  - 强制退出应用
  - 调用服务器后台接口，传递参数
- ✔ 通过 SDK 集成方式可实现
  - 设备信息收集
  - 实施风险监控
  - 基于终端风险的场景认证

RASP 实时应用自我保护

· AppProtect+ 将应用与设备环境隔离，即使移动设备已 ROOT/ JailBreak 或感染了恶意软件，AppProtect+ 也会检测并阻止这些恶意攻击，例如安卓设备上的屏幕阅读器或不信任键盘窃取用户的输入（例如登录凭据），以实现对应用的实时保护。

· AppProtect+ 基于风险事件侦测，异于传统病毒数据库匹配方法，避免病毒信息不同步而发生的风险，无需依赖外界协助。

核心价值

打击
有针对性的攻击

提供
可信赖的应用

保护
多个业务应用

实现
移动安全策略

保护
软件密钥

快速部署

符合
严格的合规要求

用户
体验无变化

部署

· 在有应用源代码的情况下，可以将 AppProtect+ 里的 SDK 文件放到项目中作为开发类库，既可以轻松集成上述安全功能到某个现有应用，又可以实现SDK里的回调函数以请求服务端接口的功能。

· 在没有应用源代码情况下，因为无法取得应用源代码所以无法使用 SDK 回调函数，只能通过 wrapping 的方式将 AppProtect+ 功能添加到现有应用中。

适用设备

适用于安卓和 iOS 平台

安讯奔简介

北京安讯奔科技有限责任公司（安讯奔，i-Sprint）隶属于安讯奔集团，是世界领先的身份管理和认证专家，专注于为全球金融机构、政府部门和高安全敏感环境提供身份管理和应用安全解决方案，集自主研发、生产、销售、服务为一体，专业从事数字身份认证、身份和访问管理、凭证管理、关键数据的端到端加密、云端强认证和物品身份认证等信息安全产品的应用开发及行业推广。提供专业的身份保护、移动保护、数据保护、云保护和防伪溯源解决方案，包括统一生物认证、统一身份管理、通用凭证管理、安全单点登录、电子渠道整合、移动应用安全和安甄品防伪溯源等，全方位保护企事业单位的隐私和机密信息，保障产品充分满足国内安全市场的业务需求，保障厂商和消费者的切身利益，以及信息安全等级保护、银监会等行业监管要求。

核心优势

自有知识产权

迄今，安讯奔已经成功地申请到了各种知识产权证书和资质证书，包括专利8件、计算机软件产品著作权证书 26件、计算机信息系统安全专用产品销售许可证4件、商用密码产品销售许可证、商用密码产品定点生产单位、国家高新技术企业、中关村高新技术企业证书等。

各行各业的成功实践

解决方案已长期稳定地成功部署在超过 50家世界领先金融机构和超过 200家银行及企业，并广泛应用于各行各业知名企业的信息化建设，包括政府、医疗、制造、电信、能源、航空运输、IT、媒体等，助力企业加强对内对外的信息安全建设，提高信息化水平，实现高效运营，塑造良好的企业形象。

权威 IT 评价机构的充分认可

荣获中国软件行业协会企业信用等级评价 AAA 级“中国年度优秀软件产品奖；获得由中国计算机行业协会、中国计算机产业推进联盟和中国计算机报联合颁发的“中国信息安全领域最佳解决方案奖”；并获得由人民银行旗下《金融电子化》杂志颁发的“优秀技术创新奖”等诸多荣誉。

实力雄厚的国内外合作伙伴

与知名生物识别厂商 SenseTime、Face++、BOOMHOPE（博宏）等，建立了良好的合作关系，在建设统一生物认证平台方面展开了深度合作。

北京安讯奔科技有限责任公司
北京市海淀区西直门北大街 60号
首钢国际大厦 909室
咨询热线：0756-6322666
www.axbsec.com

安讯奔分公司和办事处
北京 | 上海 | 广州 | 深圳 | 成都 | 珠海