

YESsafe AppPortal+



企业移动应用安全管理

随着企业的移动应用日益增加，员工使用企业应用来进行日常工作的情况也更加普遍。为了让企业更有效地管理企业移动应用，YESsafe AppPortal+ 从设计之初就考虑到了企业应用安全及其监管的多方面要求，以充分保护移动应用和敏感业务信息。

用户安全特性

强认证和授权



- 利用双因素认证和生物识别技术来满足强认证需求。
- 提供场景认证功能，可动态调整认证过程。

移动单点登录平台

SSO

- 使用标准 OAuth 和 OpenID 协议实现单点登录。
- 通过模拟用户登录行为实现单点登录，即无须修改任何源代码便可实现单点登录和更改密码。

安全注册



使用一次性密码和 / 或用户的活动目录 /LDAP 凭证来认证用户。

重认证



为了增强敏感应用或高危应用的安全度，在用户进行单点登录之前，SSO 使用标准策略控制进行重认证，从而防止冒充用户进行未授权访问的行为。

应用安全特性

安全移动门户 – 移动设备应用的通用访问点



- 访问原生应用和 HTML5 应用。
- 单点登录到应用。

通过企业应用商店获取已授权的应用



- 企业应用的官方下载渠道。
- 企业应用管理和用户授权。

YESsafe AppPortal+

集成 SDK 和 APIs

YESsafe AppPortal+ 提供开放的 API 支持体系，允许开发人员使用 YESsafe AppPortal+ 的安全特性。这样可以大大减少开发人员的开发工作量，并让企业能更快启用安全移动应用。通过个性化配置应用门户、自助服务和单点登录功能，YESsafe AppPortal+ 不仅改善了用户认证过程，也提升了用户体验。

应用安全特性

沙箱保护 (适用于 Android)

SandBox

- 通过沙箱控制敏感应用安装、版本更新。
- 一旦员工离职，可以对沙箱内应用进行数据擦除、应用卸载等操作。



移动应用完整性保护

结合 AppProtect+ 产品，可以实现移动端应用的运行时保护，如：防篡改、防注入、防数据泄露、防钓鱼等攻击。

其它安全功能

快速注册和设备信息统计



- 在用户从不同的设备成功登录后，快速收集移动设备和终端信息。
- 通过仪表盘界面，可查看用户的设备信息，便于审计和安全考量。



设备指纹技术

获取设备信息用以保护用户信息的注册、交付和使用过程。此外，还可将此类信息用于数据加密处理、防止应用数据和系统克隆等多个场景。在整个认证过程中，检测移动设备状态，例如是否越狱、操作系统版本等，以决定相应的认证因素，从而实现动态扩展更高的安全认证标准。

场景认证



充分利用用户身份相关的场景数据（例如地理定位、登录时间限制和终端设备身份）来评估认证过程的可信度，从而为用户提供丰富的场景认证功能，并且能够动态调整认证过程，基于策略为不同的应用灵活适配认证手段用以验证用户身份。

Global Headquarter

Blk 750D Chai Chee Road
#08-01 Viva Business Park
Singapore 469004
☎ +65 6244 3900
✉ enquiry@i-sprint.com

For a complete list of our offices in

China, Hong Kong, Japan, Malaysia,
Thailand & United States, please visit
www.i-sprint.com/contactus

©2000-19 i-Sprint Innovations Pte Ltd. All rights reserved.

A Hierarchy Model is a patent of i-Sprint Innovations Pte Ltd. i-Sprint, i-Sprint logo, AccessMatrix, AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.