YESsafe AppPortal+

A comprehensive Enterprise Mobile App Security Management Solution that creates a unified security platform to help enterprises to deploy, secure and run their mobile apps and authenticate their users.

With the proliferation of mobile apps in many organizations, their employees depend heavily on companies' mobile apps to perform daily business activities. In order to provide a more efficient approach for companies to manage their mobile applications, YESsafe AppPortal+ has been designed to deliver a number of critical security functions and features to protect mobile Apps and sensitive business information:

Enterprise Information Security Features

Strong Authentication and Authorization

- Leverage 2FA, biometrics for strong authentication requirements
- Provides contextual adaptive authentication feature based on the login location, time, network to dynamically adjust the authentication process

Mobile Single Sign On Platform

SSO

- SSO using standard OAuth, OpenID Connect protocol and auto-fill technology
- Auto-fill technology supports native mobile app (iOS and Android) and web app without the need for source code modifications

Extensibility

Supports integration with enterprise internal LDAP system, certification system, enterprise content management system and network security portal.

Re-Authentication Capabilities

SSO using standard Policy control for re-authentication before single sign-on to enhance security for sensitive or high risk apps and to avoid unauthorized access by impersonate users.

Application Security Features

Secure Mobile Portal – Common Access Point for Apps on Mobile devices

- Access to native apps and HTML5 apps
- Single Sign-On to apps

Enterpise App Store To Access Authorized Applications

- Official download channel for enterprise apps
- Enterprise app management and user entitlements

Mobile App Integrity Protection

For mobile apps (iOS and Android), AppPortal+ provides RASP (Runtime Application Self-Protection) service to protect app from attack.

Sand Box Implementation (applicable for Android)

SandBox

- Additional level of app data protection, data will be encrypted when installed in Sandbox
- Remote removal of apps installed in Sandbox for system manager

YESsafe AppPortal+

Integration SDK & APIs

YESsafe AppPortal+ provides open APIs, to enable developers to leverage the security features of YESsafe AppPortal+. This can greatly reduce their development efforts and enable enterprises to quickly launch secure mobile applications at a faster speed. It not only enhances the user authentication process, it also improves user experience by personalizing configurable application portal, and providing self-service and SSO capabilities.

System & Apps Security Features

Environmental Security Scan

Scan the operation system and installed apps to detect any risks on mobile devices.

Policy Control Based on Scanning Results

Based on the scanning results, company can determine the action for launching and limiting the functions of integrated apps.

Mobile Apps Protection

Both iOS and Android apps are protected from repackaging, code injection, overlay attack and data theft even when apps are running in a vulnerable environment.

Additional Security Features

Fast Enrolment and Device Insight

Quickly collect mobile devices and endpoints information individually after the user has successfully enrolled from different devices. View a complete inventory of users' devices via a dashboard, useful for auditing and security oversight.

Data Encryption Protection

Provides a secured environment for enterprises during data transmission:

- Supports International standard encryption Algorithms and China SM standards
- Supports E2EE
- Supports message authentication to ensure data integrity during transmission

Device Fingerprint Technology

Captures information about the mobile device for identification purpose during user enrolment process, leveraging on such information for data encryption and prevention of device and application cloning. It detects the state of the mobile device, e.g. Jail-broken, OS version etc. to determine the appropriate authentication factors.

Contextual Authentication

Provides contextual authentication feature to leverage a wide range of identity-related contextual data (e.g. geographic location, time-of-day and endpoint identity) to elevate the trust of the authentication process and dynamically change the authentication process to verify user identity by various factors gathered from the user during the authentication process.

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

Scan for more information