# Protect mobile enterprise with smarter security

# Mobility and BYOD adoptions brings new access and security challenges

## Risk of user access/transactions from the mobile device

- Unauthorized access to sensitive data and applications
- Fraudulent execution of sensitive transactions
- Weak identity assurance controls around mobile device

## Secure access from web → mobile apps and services

- SSO to mobile and cloud apps for greater user productivity
- Strong authentication to protect mobile access to apps and services
- Secure mobile app development and deployment integration

## Mobile security intelligence and compliance

- Lack of insight into user and application behavior on mobile devices
- Need context-based policy enforcement across B2E and B2C use cases

Secure
Productivity Suite

Mobile
Application
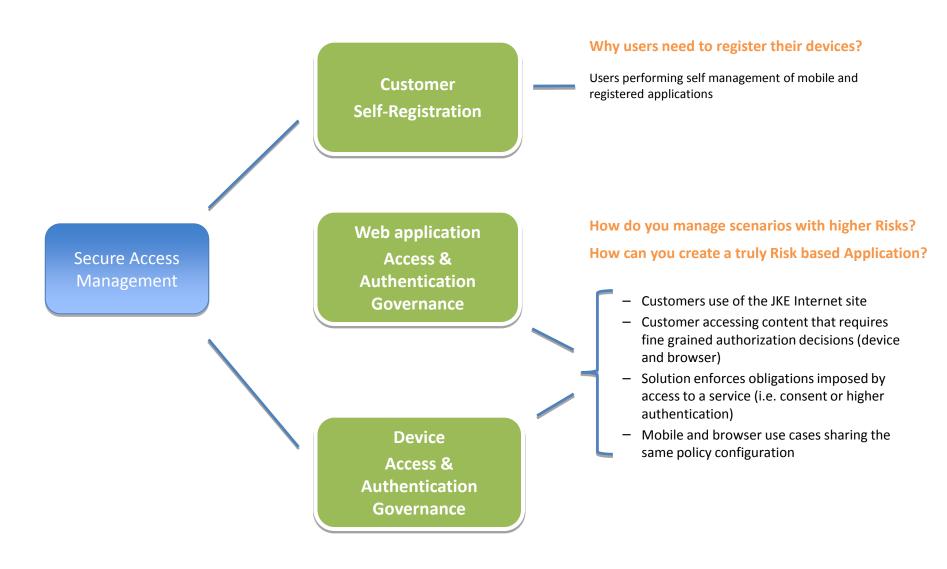Management

Secure Access
Management

## Scenario Context

- JKE Bank is a global financial institution serving clients across the world.

- JKE Bank provides a set of web-based, self-service applications, enabling its customers to access account information and other important services, minimizing the need to contact a call center or walk into a branch

- JKE Bank would like to build it's brand image by revamping the digital experience on all their channels

- JKE is embarking on a transformation program to provide exceptional digital experience to their customers

- This would involve creating great user experience on their web portal, regardless of form factor, as well as offer specific services leveraging inherent capability of mobile devices

**Customer Self-Registration**

**Why users need to register their devices?**

Users performing self management of mobile and registered applications

**Secure Access Management**

**Web application Access & Authentication Governance**

**How do you manage scenarios with higher Risks?**

**How can you create a truly Risk based Application?**

- – Customers use of the JKE Internet site
- – Customer accessing content that requires fine grained authorization decisions (device and browser)
- – Solution enforces obligations imposed by access to a service (i.e. consent or higher authentication)
- – Mobile and browser use cases sharing the same policy configuration

**Device Access & Authentication Governance**