No Passwords!
Secure Mobile Architecture for Enterprise Mobility and BYOD

Ben Ayed, CEO, Secure Access Technologies

Dr. Scott Jenkins, CEO, m-Health Technologies

In-Depth Seminars – D13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

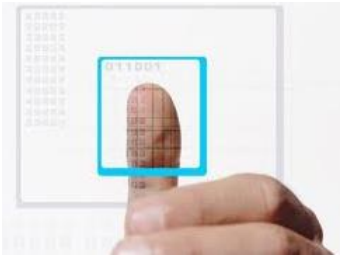
THE MOBILITY TSUNAMI

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

The Mobility Tsunami

- Why iPads are a threat to enterprise?

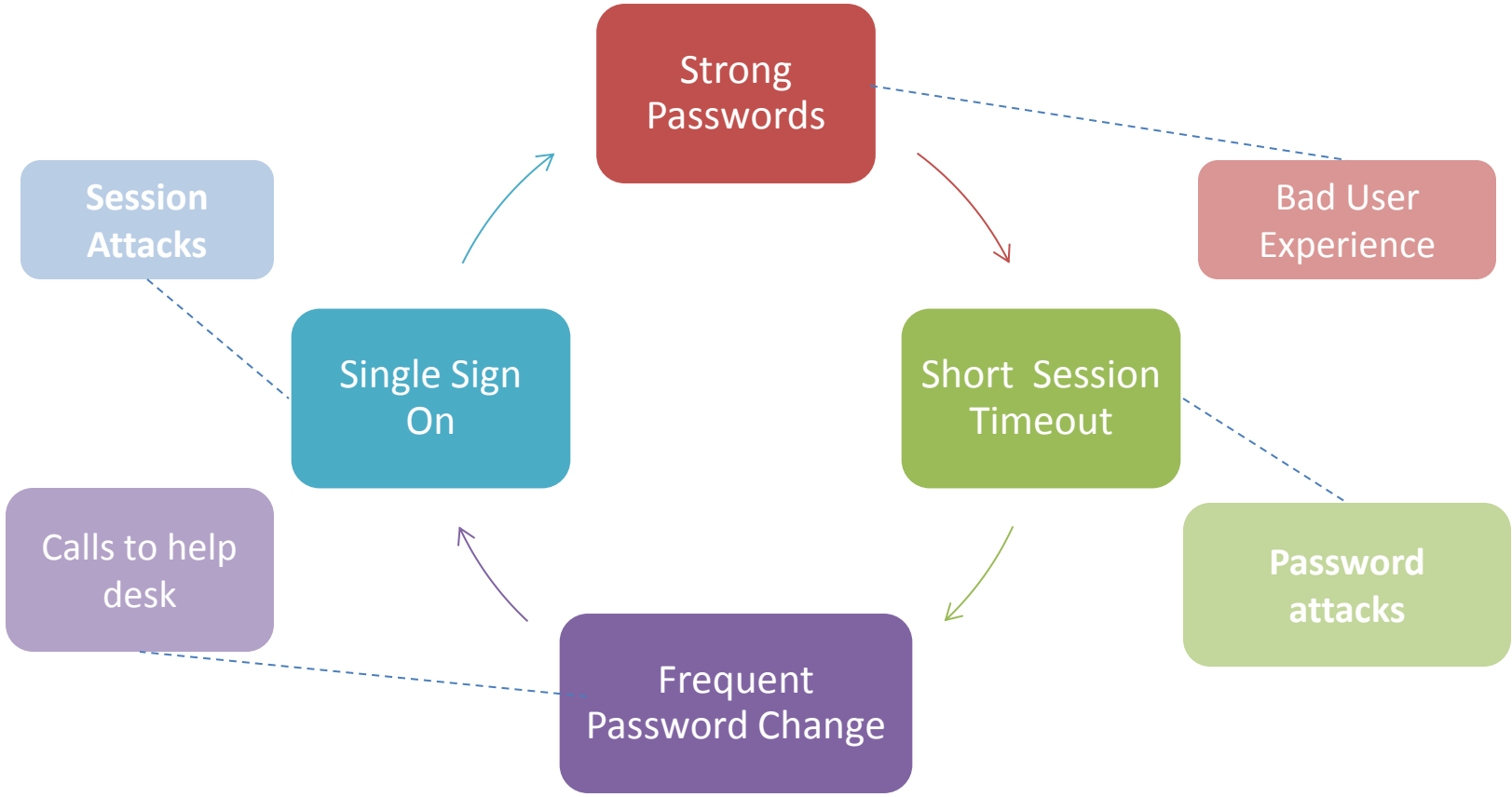
- Does legacy security work with mobile devices?



Security Vulnerability Assessment

- Data Leakage
- Password Attack
- Device Attack

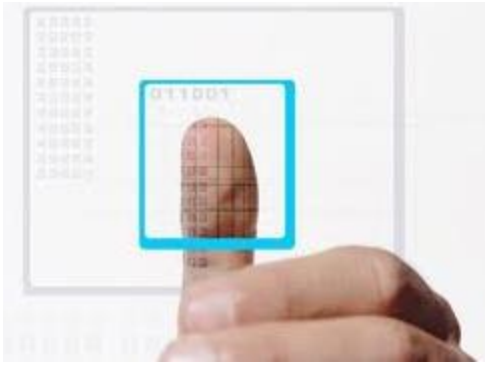
The Security Conundrum



Passwords & SSO are risky for enterprise. CISOs need to focus more on user authentication instead only focusing on intrusion detection and monitoring

Security Solutions

- Do fingerprints solve mobile security problems?



Security Solutions

- Do MDM / MAM solve mobile security problems?
- Does Virtualization solve the problem?

Mobile Security Solutions

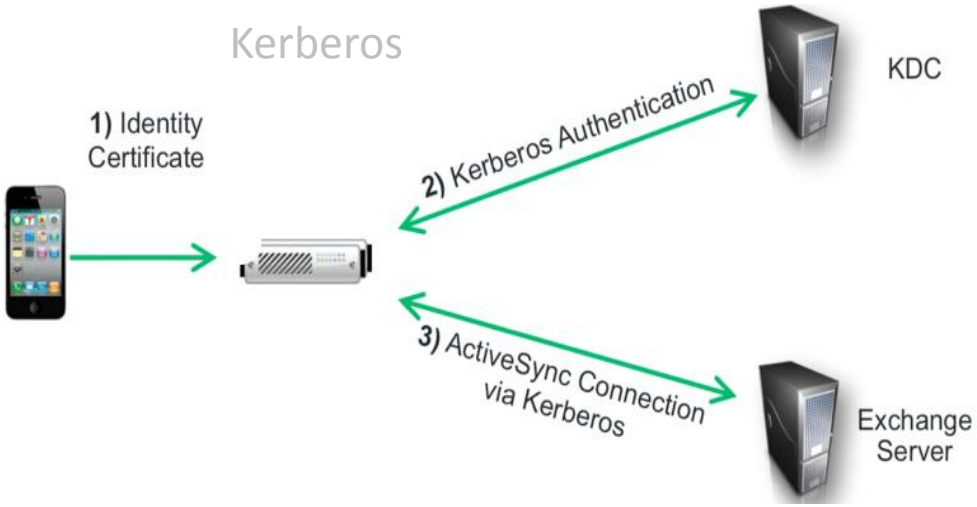
Other Solution:

- Location based authentication
- Presence monitoring:
  - Bluetooth proximity or motion detection
- No passwords
- Application self-defense

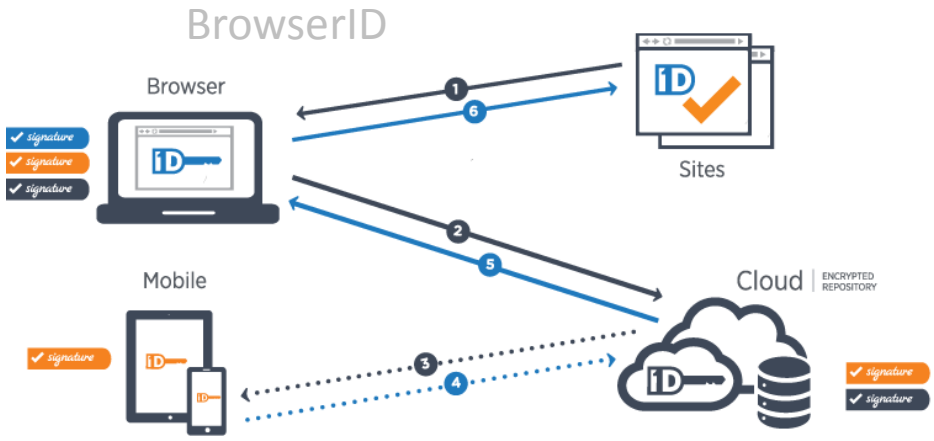
SECURE MOBILE ARCHITECTURE

Mobile Architecture Security Challenges

- Compliance gaps
- Single Point of Failure
- Requires connectivity

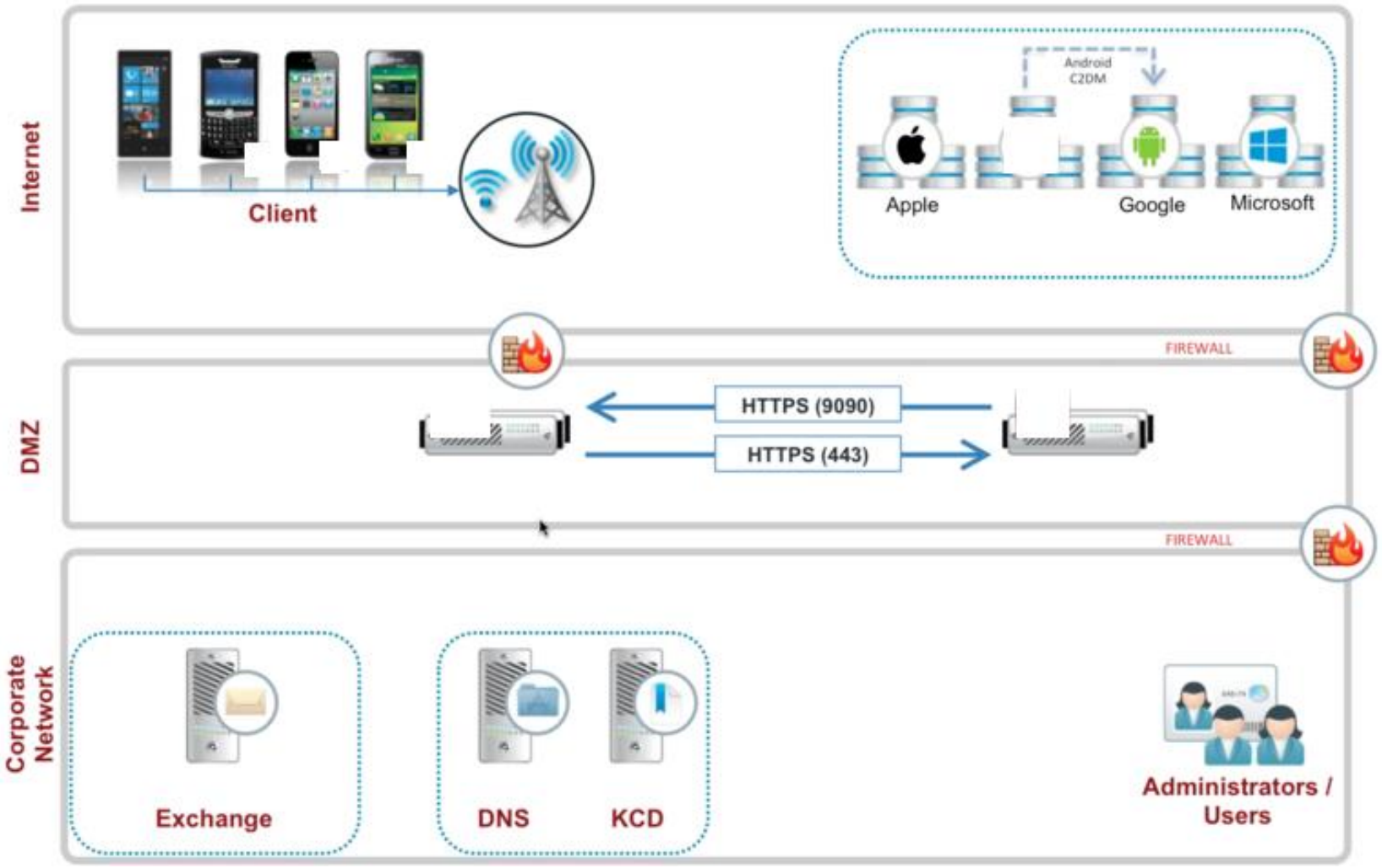


- Kerberos & BrowserID type solutions amplify those vulnerabilities on mobile devices… An attacker that gains access to one application on the authorized device can access all applications



Not So Secure Mobile Architecture

Can Compromise Network Security

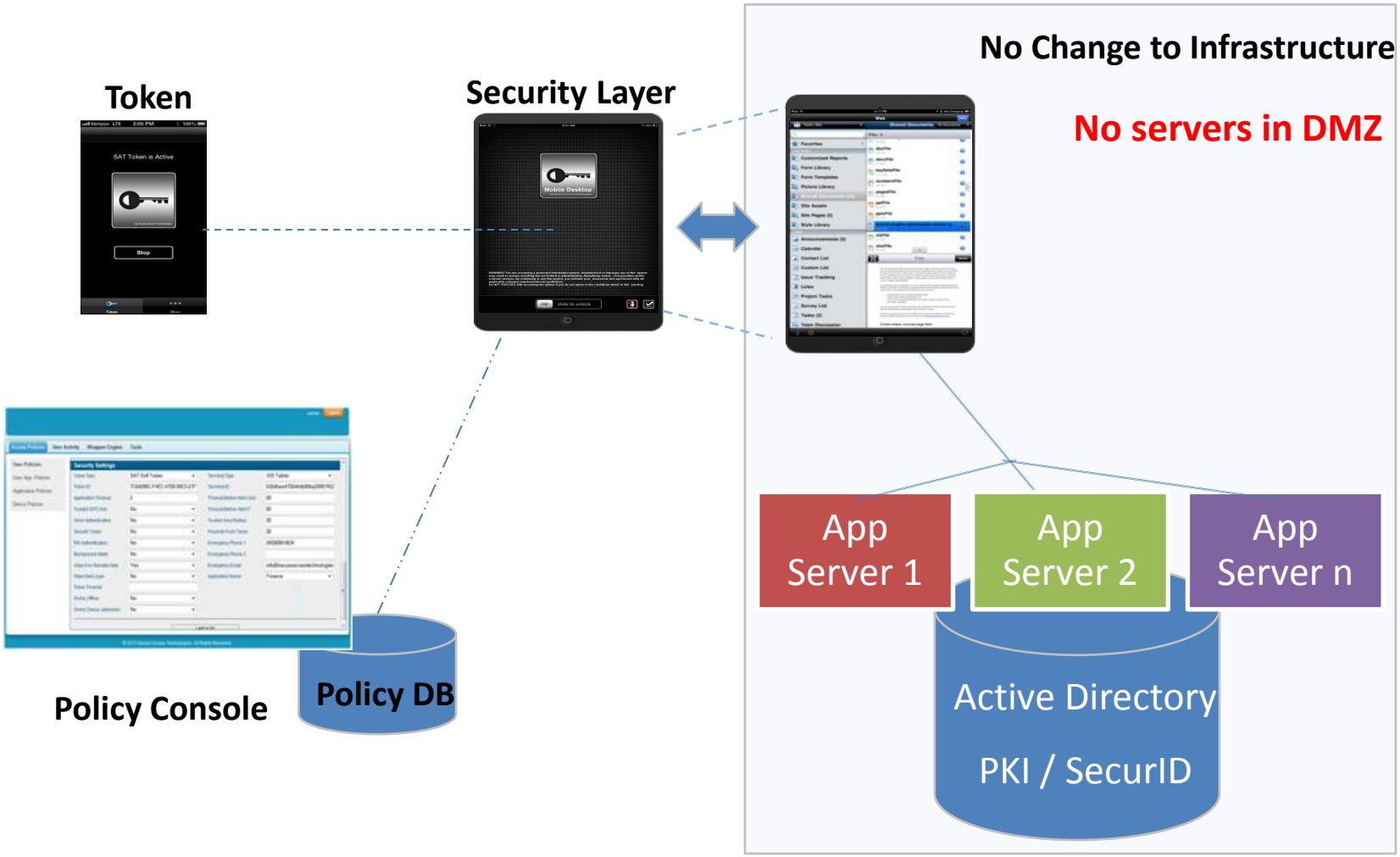


More Secure Mobile Architecture

No servers in DMZ

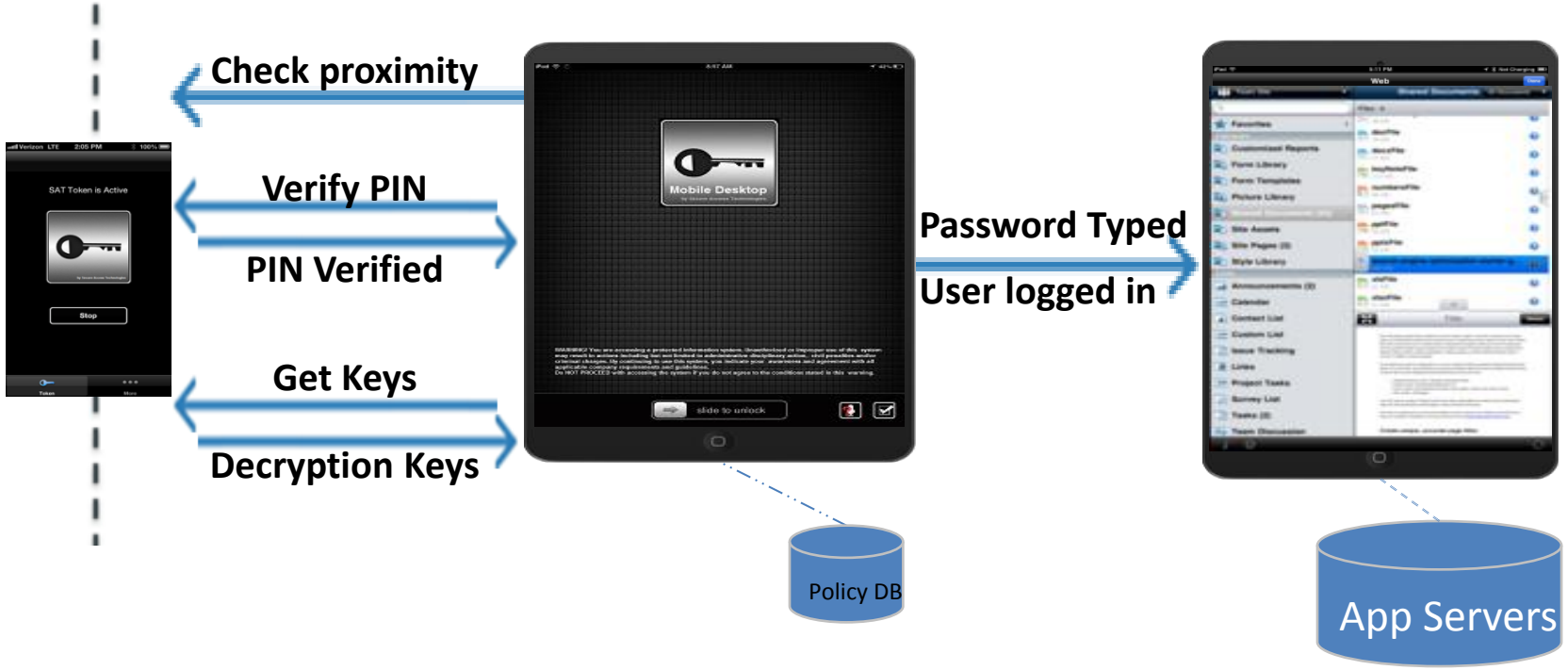
Secure Mobile Architecture

No tradeoff between security and usability



Secure Mobile SSO

SSO with No Single Point of Failure



Comparison with SSO / Kerberos / SAML:
-Works out-of-network
-No single point-of-failure
-Works with any application
-Easy installation

-Biometrics authentication enables authentication without token
- Can be installed/removed on small number of devices without impacting others

Secure Mobility Requirements

Requirement	Benefits
FFIEC Multi-factor Requirements	Compliant
Real-time presence monitoring & Application self-defense	Security / Compliance
Adaptive Authentication based on location, transaction risk and policy	Security / User experience
Off-line access	Flexibility
Works on any device	Scalability
Policy driven	Manageability
Easy integration	Affordability
No password	Minimize helpdesk calls

Market Solutions

Solution Type	Description	Advantage	Disadvantage (Limitations/Concerns)
MDM:	Enforce device level passwords, Wifi access Provide remote wipe when lost device is still connected to the network e.g.: Airwatch, MobileIron, Fiberlink	Cloud infrastructure	Require connectivity Password attack Session attack
MAM:	Encrypt email, calendar and browser Force traffic through their servers e.g.: Good Email, Fixmo Safezone	Data resident security Data in transit security	Require connectivity Password attack Session attack
VDI:	Convert data to screens on a server and transfer them to the mobile device for viewing e.g.: Citrix, Armor5	Secure Browser	Require connectivity Password attack Session attack
Application Wrapping:	Inject object code in iOS and Android applications e.g. Mocana, Apperian	Mobile only Data resident security Data in transit security	Require connectivity Password attack Session attack

Closing Mobile Security Gaps

Type of Limitation/Concern	Mitigation	Example Solutions
Require connectivity	Off-line multi-factor authentication: -Application scans the user through Bluetooth to detect that the user phone is in proximity - Application asks the user some questions and request voice response	Secure Access Technologies (SAT) provides off-line multi-factor user authentication
Password attack	Authenticate the user with adaptive multi-factor authentication depending on location, application and policies Request a token or biometrics	Secure Access Technologies (SAT) provides real-time proximity monitoring
Session attack	monitor the user proximity to the application or motion in real-time. If the user moves away, lock	Secure Access Technologies (SAT) integrated with Good Email, Fixmo Safezone and Citrix Worx

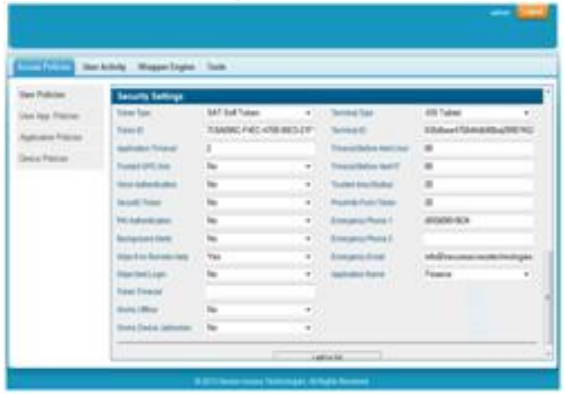
SAT Architecture

Wrapper Engine Upgrades Legacy Applications in Minutes

Soft or hard token:
- 3-factors of authentication including biometrics
- 4-factors of authorization

Wrapper Engine: Takes legacy apps, injects security layer object code

The policy dashboard defines:
- Rules for Adaptive authentication
- Rules for application self-defense



Smart Phone Token or Bluetooth Token: PKI Key

1- Check: **token proximity, location, device integrity, PIN, CAC or biometrics …**
2- Login: **No-password login** to any app
3- Real-time monitoring
4- Breach: **Application self-defense**

Policy Console sets access and sets wipe policies for all applications

LIVE DEMO:
USE CASE: NO PASSWORDS
ONE-CLICK LOGIN TO ANY ACCOUNT

Thank You

Ben Ayed & Scott Jenkins

Secure Access Technologies Inc.

1370 Willow Rd. #2, Menlo Park, CA 94025
Tel: 650 209 6670

Email: bena@SecureAccessTechnologies.com
Web: www.SecureAccessTechnologies.com

10+ patents issued:
Proximity token / proximity security, Security layer, application self-defense, wrapper engine, SSO, mobile biometrics…

iPhone

iPad