

# **RSA**®Conference2015

Singapore | 22-24 July | Marina Bay Sands

SESSION ID: SPO-R03

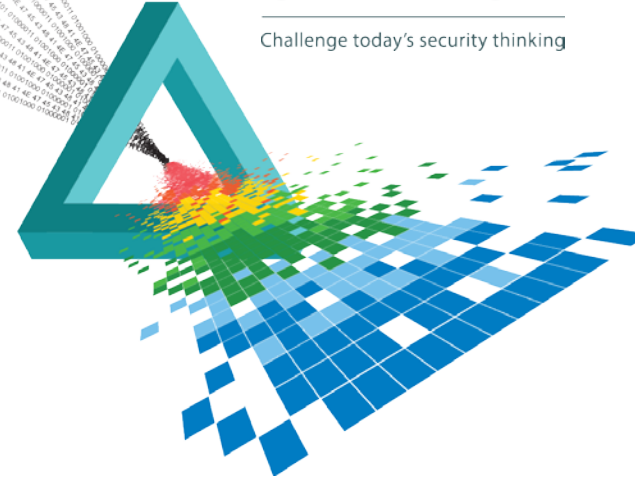
## Adaptive Trust for Secure Enterprise Mobility

**Wee Keng Tong**

SE Manager  
Aruba Networks

# CHANGE

Challenge today's security thinking



# The New Way People Work - GenMobile

ENTERPRISE



PUBLIC VENUES



HOME



OUTDOORS



# Growing Security Concerns



1. BYOD



2. Device Loss / Theft



3. Unsecured Networks

1. Personal devices connecting to enterprise resources
2. Loss of enterprise data and productivity
3. Employees using open Wi-Fi networks for work

# Running the Risk Report – High-level Findings

- ◆ Mobility security risks directly linked to user demographics, industry and geography.

(You must address all of these – not technology alone)

The behavior of #GenMobile is opening businesses to new risks

The Secure Mobility Risk Index tool – IT can benchmark relative to 11,500 users

Security must evolve to adaptive trust model – integration & context for policy enforcement



# The Threat Landscape Is Evolving

More Sophisticated Attacks

Well Resourced Groups

Risks Likely Start Within



# Unpredictable User Habits (Global)

- 31% of users lost data on mobile

- Younger users are less responsible

- 60% of users share devices



\* Aruba 2015 "Running the Risk" report

# Unpredictable User Habits (APAC)

- 30% of users lost data on mobile

- Younger users are less responsible

- 68% users share devices



1 in 3  
of workers admit to having lost data due to the misuse of a mobile device

The age bracket with the highest propensity of data and identity theft are employees between

25-34 years old



2 in 3  
share their work and personal devices with others regularly



# Industry Risk Levels Vary (Global and Singapore)

**4 in 10**

finance organisations have  
lost data through the misuse  
of a mobile device




High tech employees are nearly  
**two times**




more likely than hospitality or education  
workers to simply give up their device  
password if asked for it by IT



# A Changing Security Perimeter



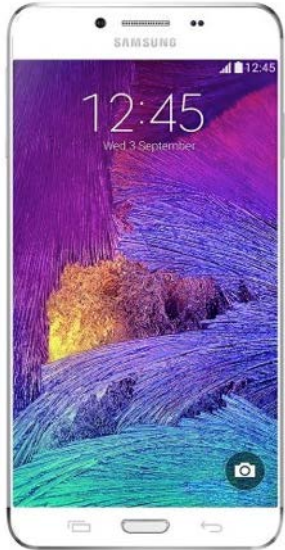
Legacy security focused  
on a fixed perimeter



GenMobile dilutes the notion  
of a fixed perimeter

# Legacy Perimeter Defense Model

## Protection Deployed in Silos



### MDM

- Cellular policies
- Device controls
- IT access required

**X** No network context

### Network Access

- User auth
- **Network controls**
- Little network policy

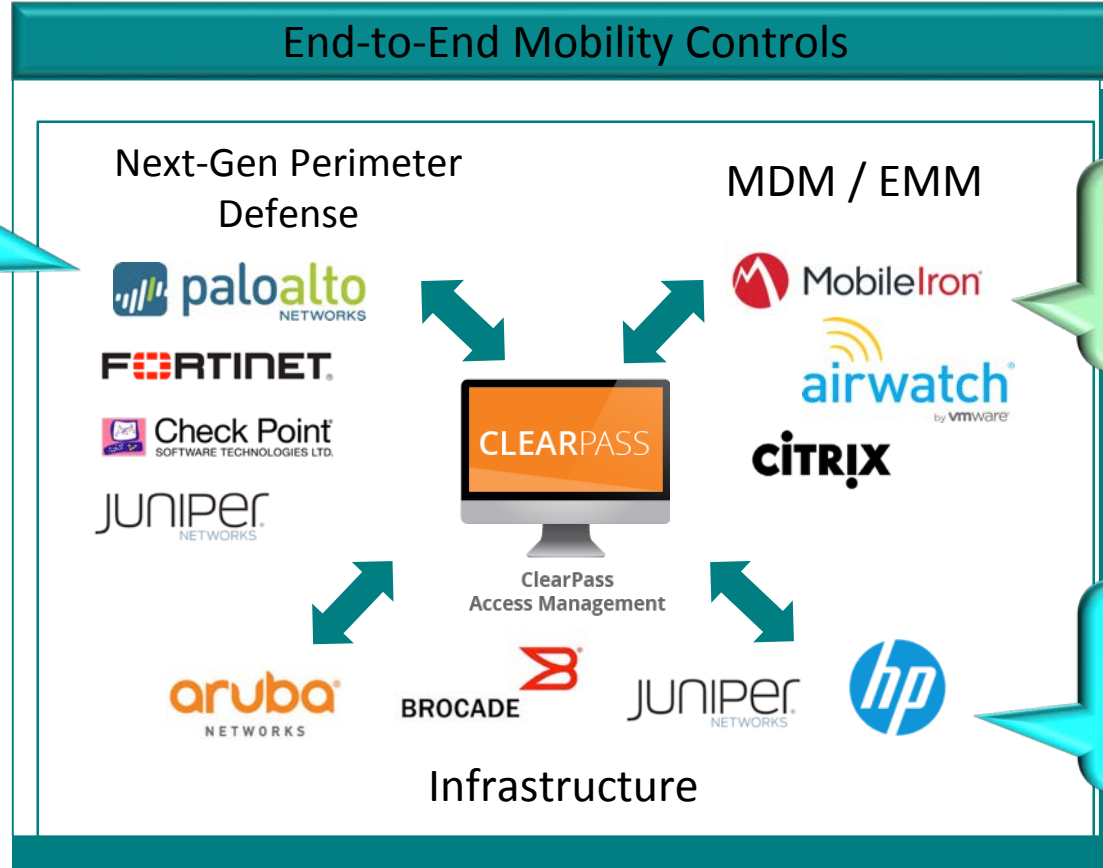
**X** No device / location context

### Perimeter Defense

- Firewalls / UTM
- **Data controls**
- External threat protection

**X** No user to device mapping

# Time for Mobile Defense – Adaptive Trust



Granular traffic control with user and device data

Network controls using real-time device data

Visibility into location and time with granular controls

- ✓ Multivendor integration
- ✓ Context sharing
- ✓ Open API

# Adaptive Trust Context Sharing - Firewalls

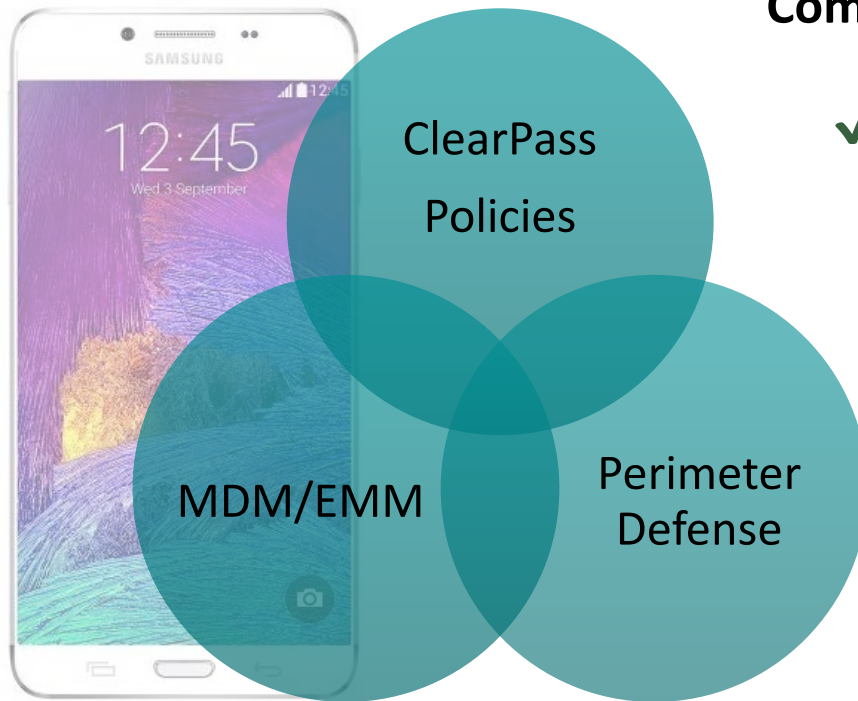
User and Device



- Works with AD, LDAP, ClearPass dB, SQL dB
- No agents/clients required



# Adaptive Trust Benefits



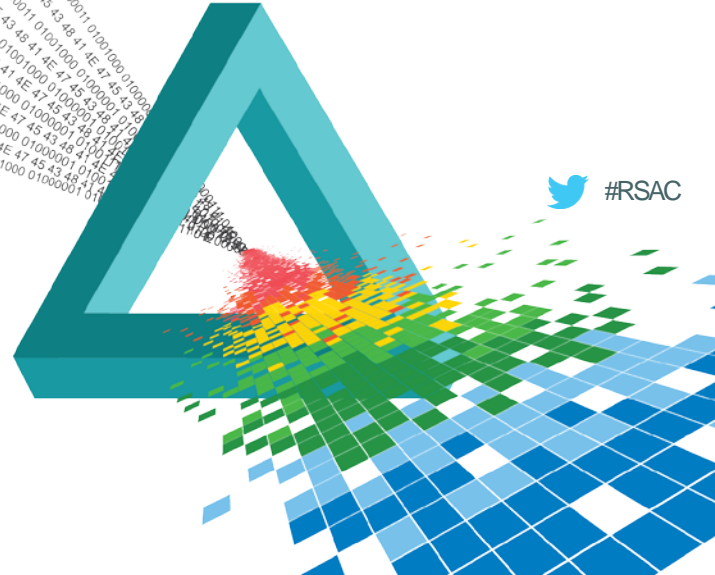
## Complete End-to-End Protection

- ✓ Wireless, wired and remote policies
- ✓ ClearPass as context store
- ✓ Accurate rules enforcement
- ✓ All security components work together
- ✓ Visibility and reporting - users and devices

# **RSA**®Conference2015

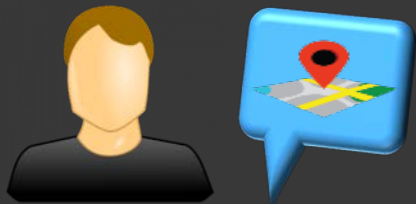
Singapore | 22-24 July | Marina Bay Sands

## **Solving Mobility Issues with Aruba ClearPass**



# Growing IT Concerns

## AAA Replacement for Access Control



Works regardless of  
role, devices, location

## Managed BYOD



Policies for  
connecting  
personal devices

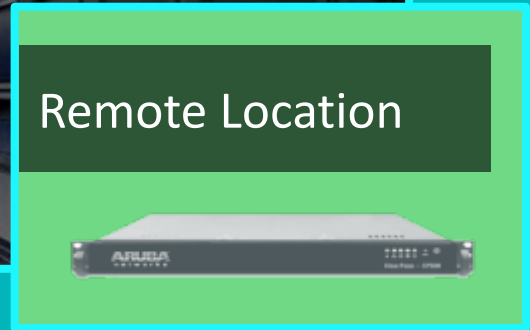
## Guest Credentials



Access does  
not require  
IT intervention

# ClearPass Platform for Policy, AAA and More

Expandable Applications



Hardware or VM Appliances  
(500, 5,000 or 25,000)



# Why AAA Replacement?

THEN

Mostly Desktops

Little Mobility

One Device per User

NOW

Mostly Mobile Devices

GenMobile

Many Devices per User

# Why ClearPass versus Legacy AAA

➤ Provides policy management with differentiated access

➤ Scales for mobility - re-authentications, locations, device types

➤ Session context captured and shared – users, devices, location...

✓ Replaces ACS, NPS and others

✓ Supports up to 1 million devices

✓ Built-in profiling and reporting

# Adaptive Policy using Device Ownership

## Enterprise Laptop

Authentication → EAP-TLS  
SSID → CORP-SECURE



**Internet and Intranet**



an HP company



## BYOD Phone

Authentication → EAP-TLS  
SSID → CORP-SECURE

**Internet Only**



# Adaptive Policy using Device Ownership

Enterprise Laptop

BYOD Phone

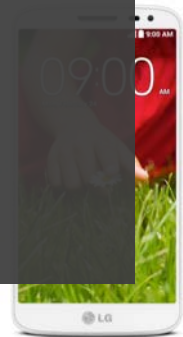
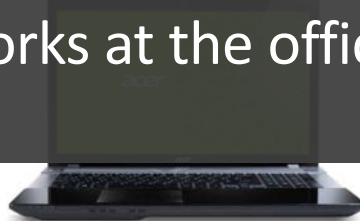
Authentication → EAP-TLS

SSID → CORP-SECURE

Authentication → EAP-TLS

SSID → CORP-SECURE

1. Uses same identity store and EAP type
2. Leverages profiling and owner data
3. No need for separate SSIDs
4. Works at the office and over VPN





# Policy Manager Customer Examples

- Replaced legacy AAA solutions and Wi-Fi for GenMobile
- Deployed AirGroup self-service to help off-load IT
- Now use policies to ensure differentiated access & security



**Automatic authentication** of devices with role-based access for all users

UNILA, 5000 students & staff, Indonesia



**Self-serve device registration** using AirGroup with auth and policy

BSJ, students (K-12), and staff, Jakarta

# Managing Personal Devices (BYOD)



User owned



Replaced often



Access from anywhere

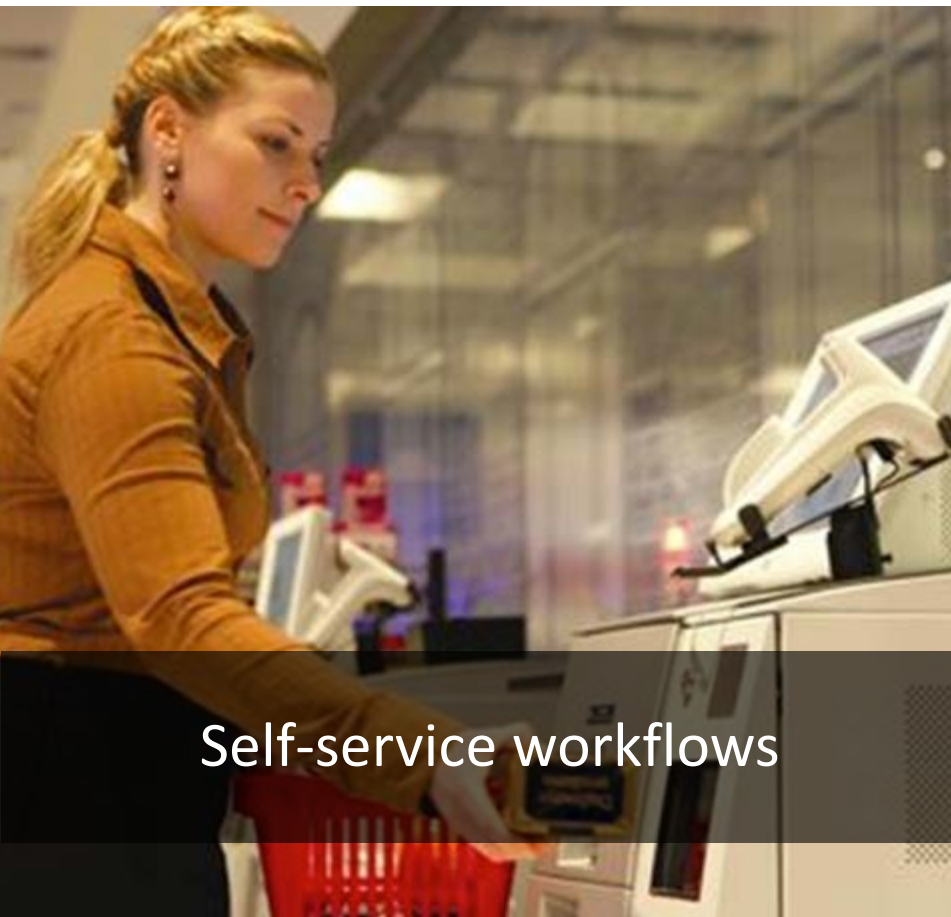


Android, iOS, Windows



Work & personal use

# Why ClearPass Onboard?



Self-service workflows

- Automated configuration: network settings and certs
- Built-in certificate authority (CA): Inc. user and device data
- Can include MDM/EMM in workflows

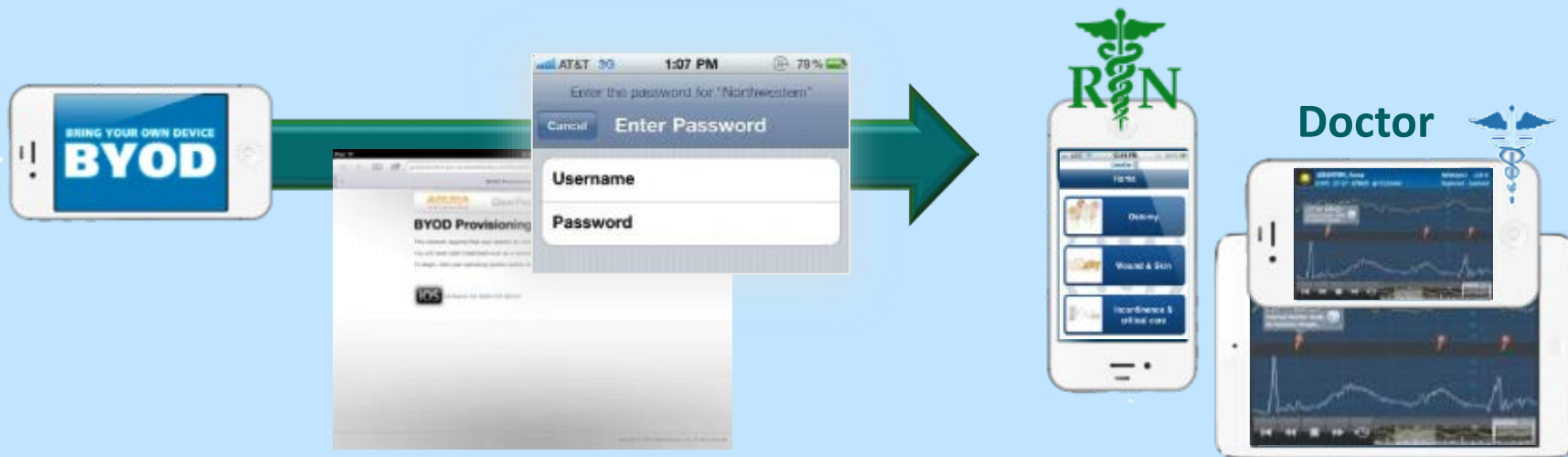
Note: Adds security, offloads IT

# Authentication using Unique Device Certificates

**1** User's device redirected to portal

**2** User enters AD credentials to start onboard

**3** Automatically places user on proper network segment



- Easy
- Secure
- No Passwords

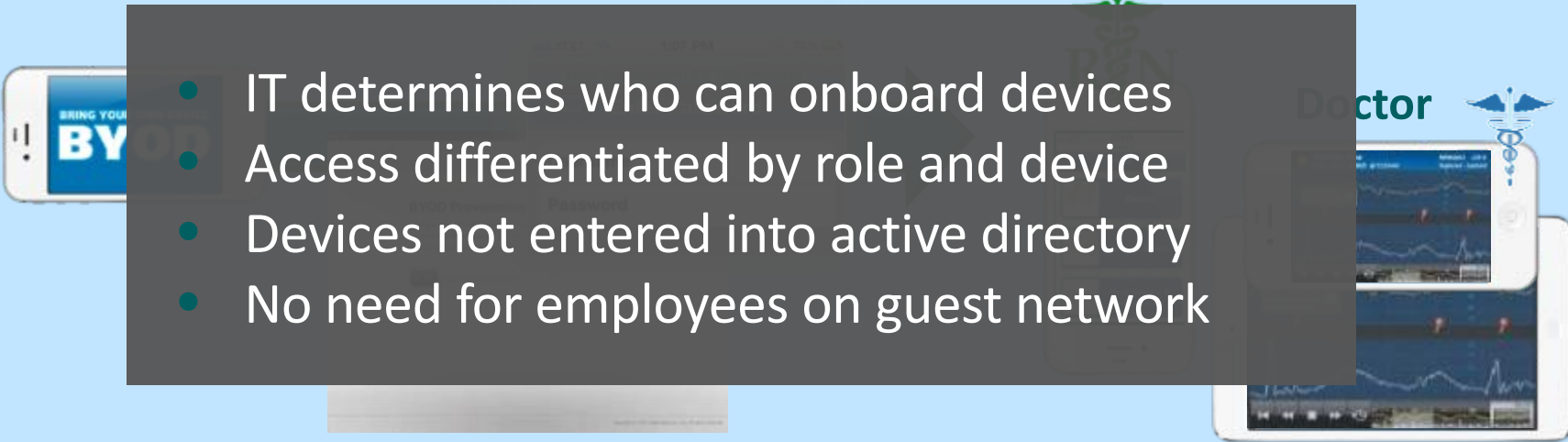


# Authentication using Unique Device Certificates

**1** User's device redirected to portal

**2** User enters AD credentials to start onboard

**3** Automatically places user on proper network segment

- 
- IT determines who can onboard devices
  - Access differentiated by role and device
  - Devices not entered into active directory
  - No need for employees on guest network

- **Easy** 
- **Secure** 
- **No Passwords**

# ClearPass Onboard Customer Examples

CLP 中電



**Automatic configuration of BYOD devices for all users**

5 Million customer accounts, Hong Kong

台灣高鐵  
TAIWAN HIGH SPEED RAIL



**Distribution and management of certs for BYO Devices**

50 year old rail system, Taiwan

➤ Self-service configuration of iOS, Android, Windows, Mac OS

➤ IT primarily involved in policy creation, not for each device

➤ No active directory management

# Challenges Delivering Guest Access



Open Network!

- ✗ Everyone expects access - even employees
- ✗ Little to No security & reporting
- ✗ Often requires staff to assist each guest

# Why ClearPass Guest?

Any industry,  
Any # of guests

Only secure guest  
app in industry

Any device, Any  
network vendor

Internet / managed  
Intranet

Self-service /  
Sponsor / Social

Portal fits phone,  
laptop, tablet

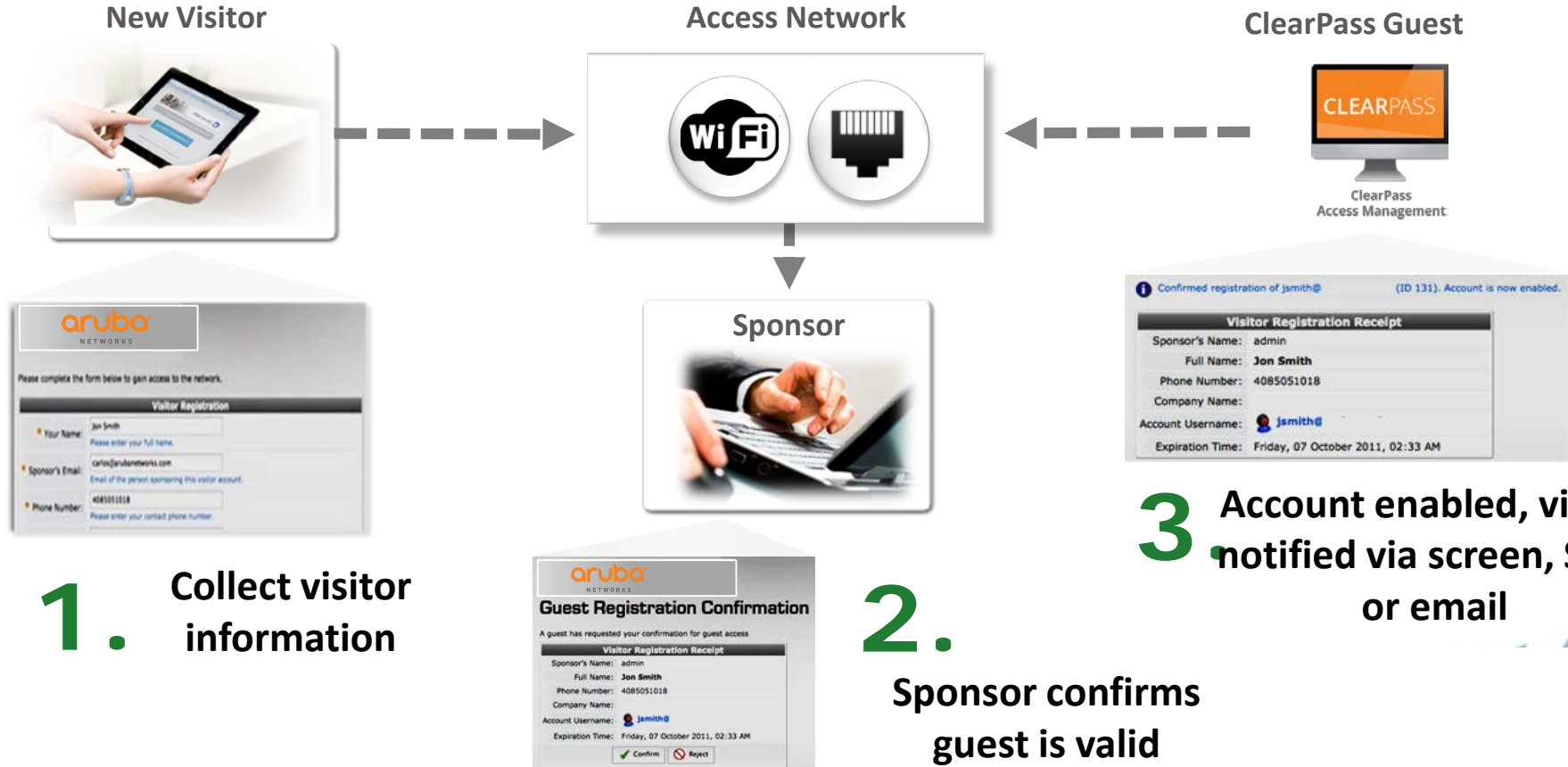
# Customizable Portal Features



- ✓ Your branding and data fields
- ✓ Advertising – mobile app, more...
- ✓ Integration with Property Mgmt – Oracle Micros, Protel, Agilysys
- ✓ Portal per department, location
- ✓ Social login, MAC cache, QoS



# Self-service with Sponsor Example



# ClearPass Guest Customer Examples

- Simple to deploy and offers excellent branding options
- Supports 1000's of users without IT intervention
- Provides same great user experience at all locations



**Custom self-service portal** for campus and events center

Over 8000 students and staff,  
Singapore



**Self-serve guest** for visitors, players and press with **differentiated policies**

Major sports venue, 700K visitors, Melbourne

# Customers Choosing Adaptive Trust



# Conclusion

- Policy is the foundation of access control and mobile security
- BYOD and guest access workflows leverage the foundation
- Organizations must adapt to #GenMobile habits and risks



Q and A

Singapore | 22-24 July | Marina Bay Sands

# Thank You

