
AIRHEADS
2013
Advanced Security:
Protecting Your Network End-to-End with Aruba Networks Personalized Security
Rich Langston
Jon Green
ARUBA networks
#airheadsconf

Agenda

- Traditional Network Security Model Is No Longer Effective
- Personalized, Context Aware Security is the Answer
- Components of Personalized Security
- Implementing Personalized Security Network-wide with Aruba Networks

Challenge of Security in the Enterprise

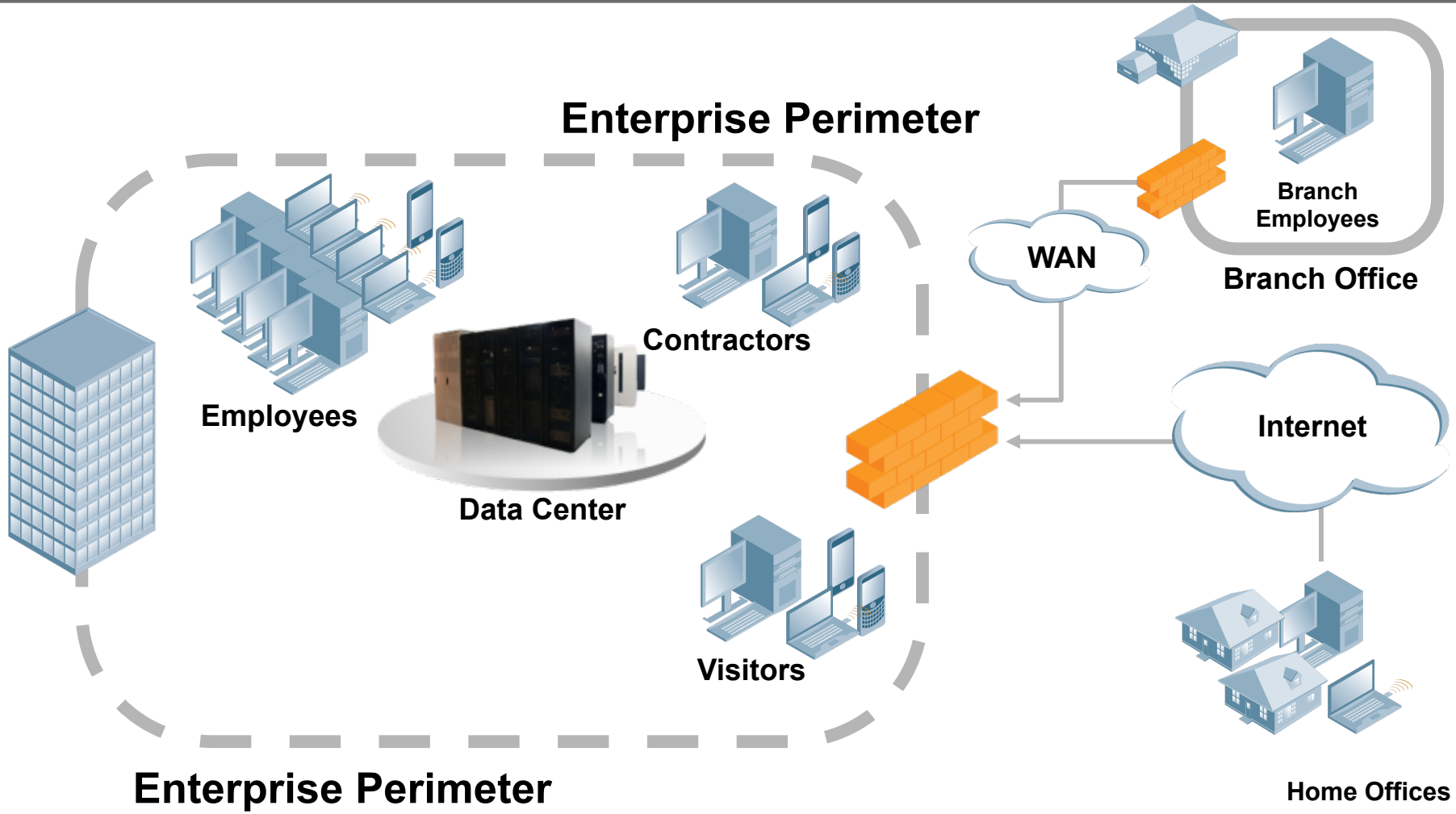
Security works toward:

- Reduce the likelihood of an information security breach
- Reduce the impact of any breach or malware outbreak
- Create an audit trail to ensure policy compliance
- Increase the reliability of your network

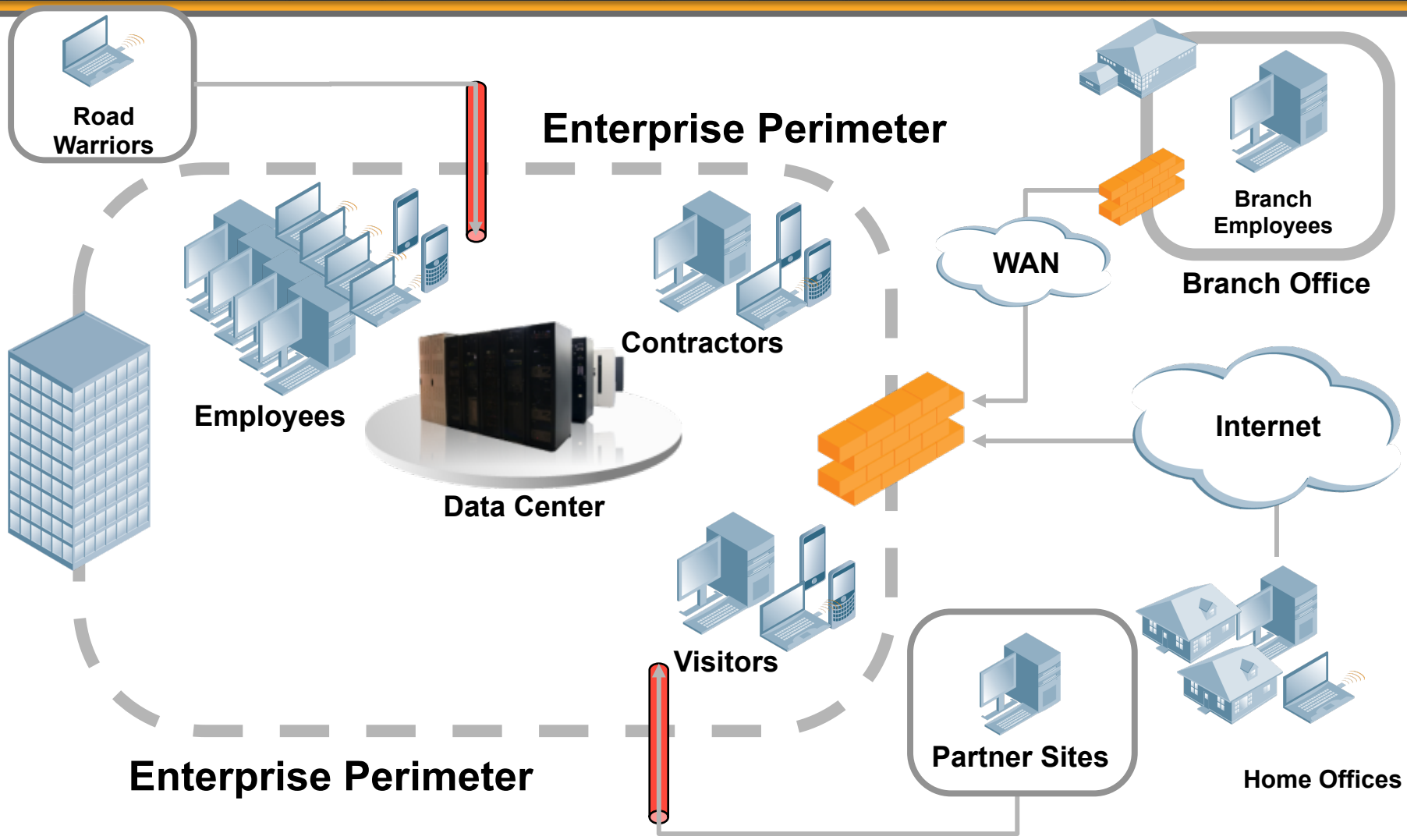
But, we also need to:

- Ensure enterprise-critical apps are always available
- Keep everyone productive
- Allow guests on our network
- Support remote workers just like they are in the office

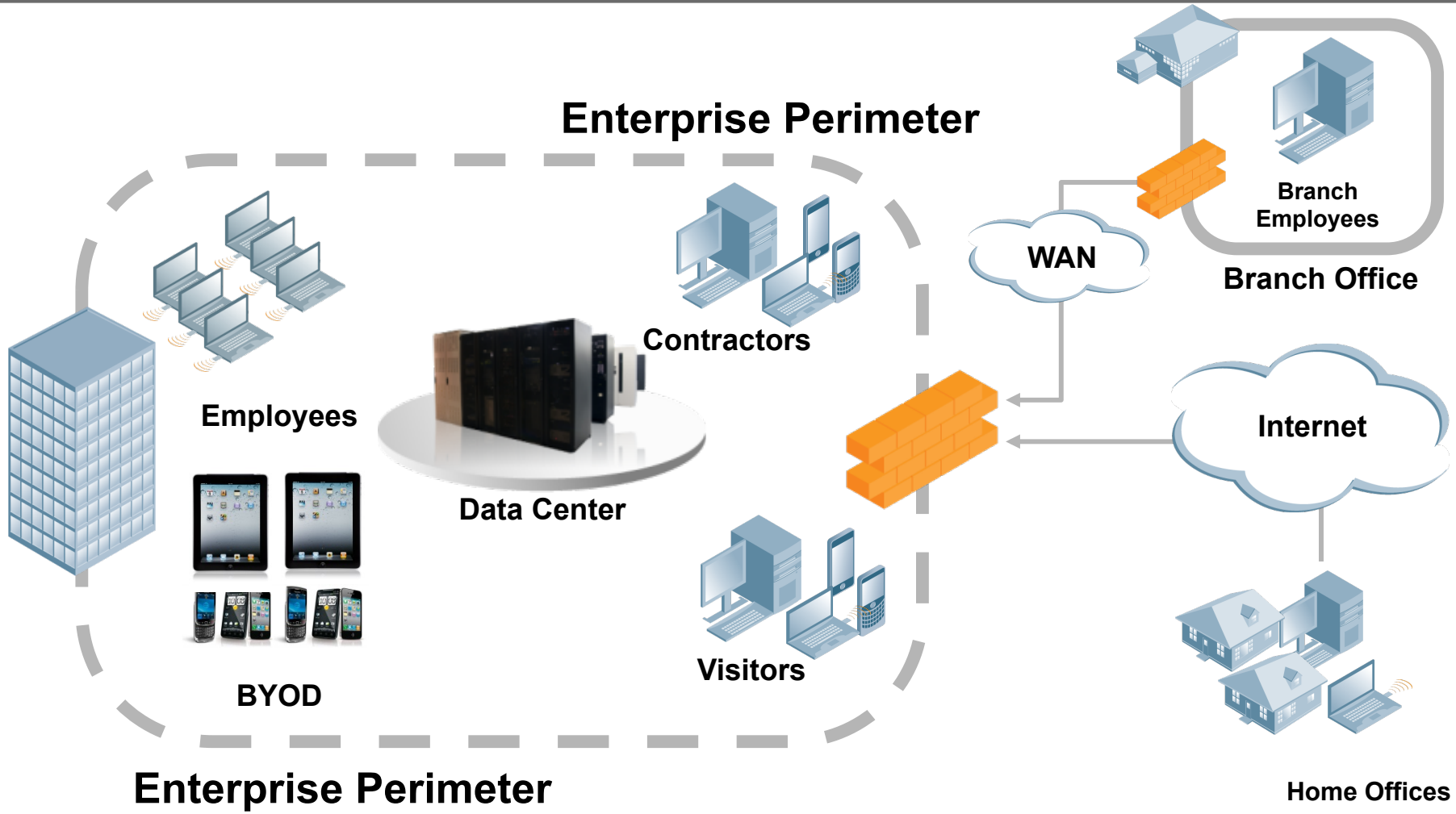
Traditional Model Barely Worked



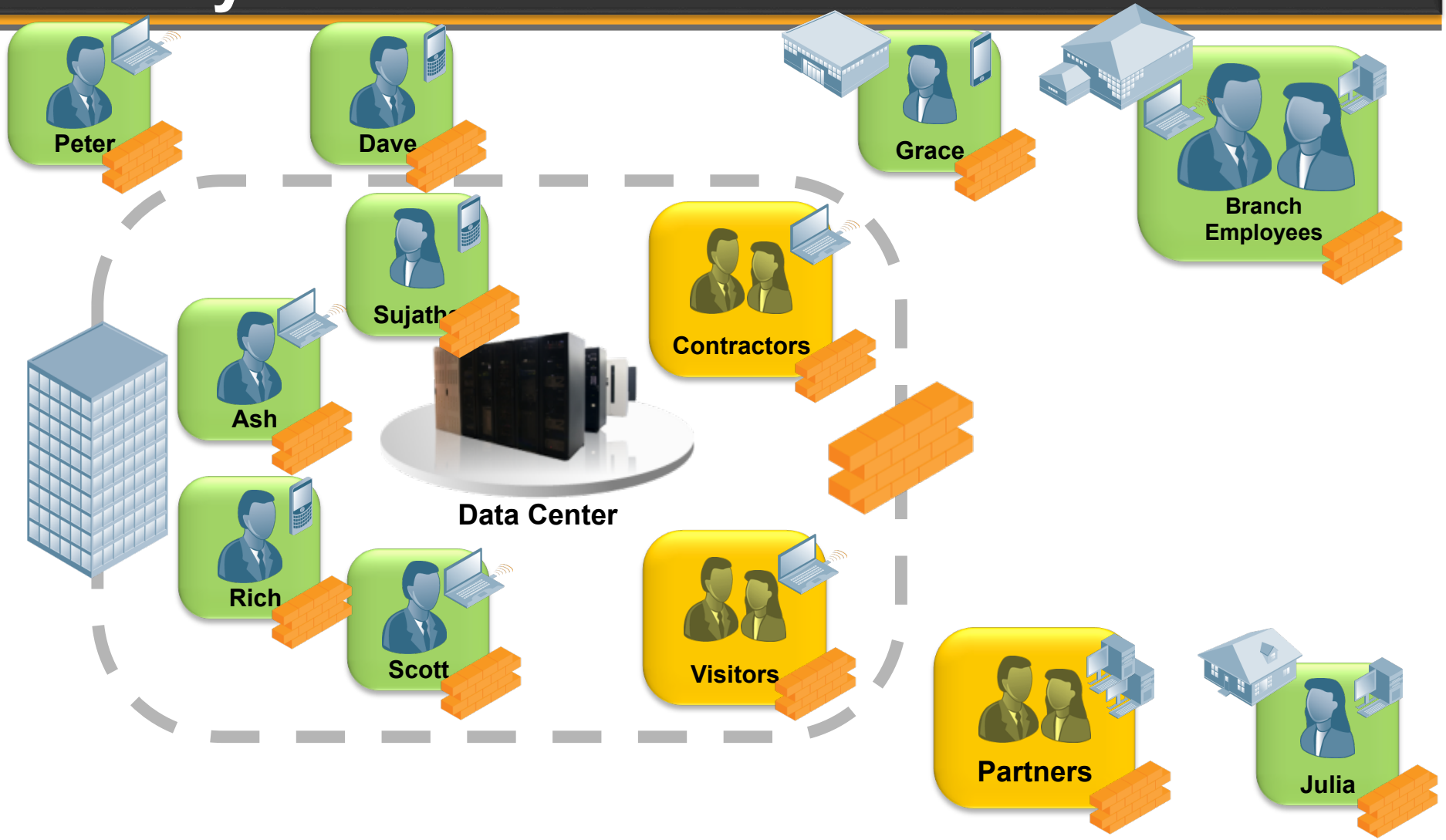
Over Time, More Holes Appeared



BYOD and Mobility Break It



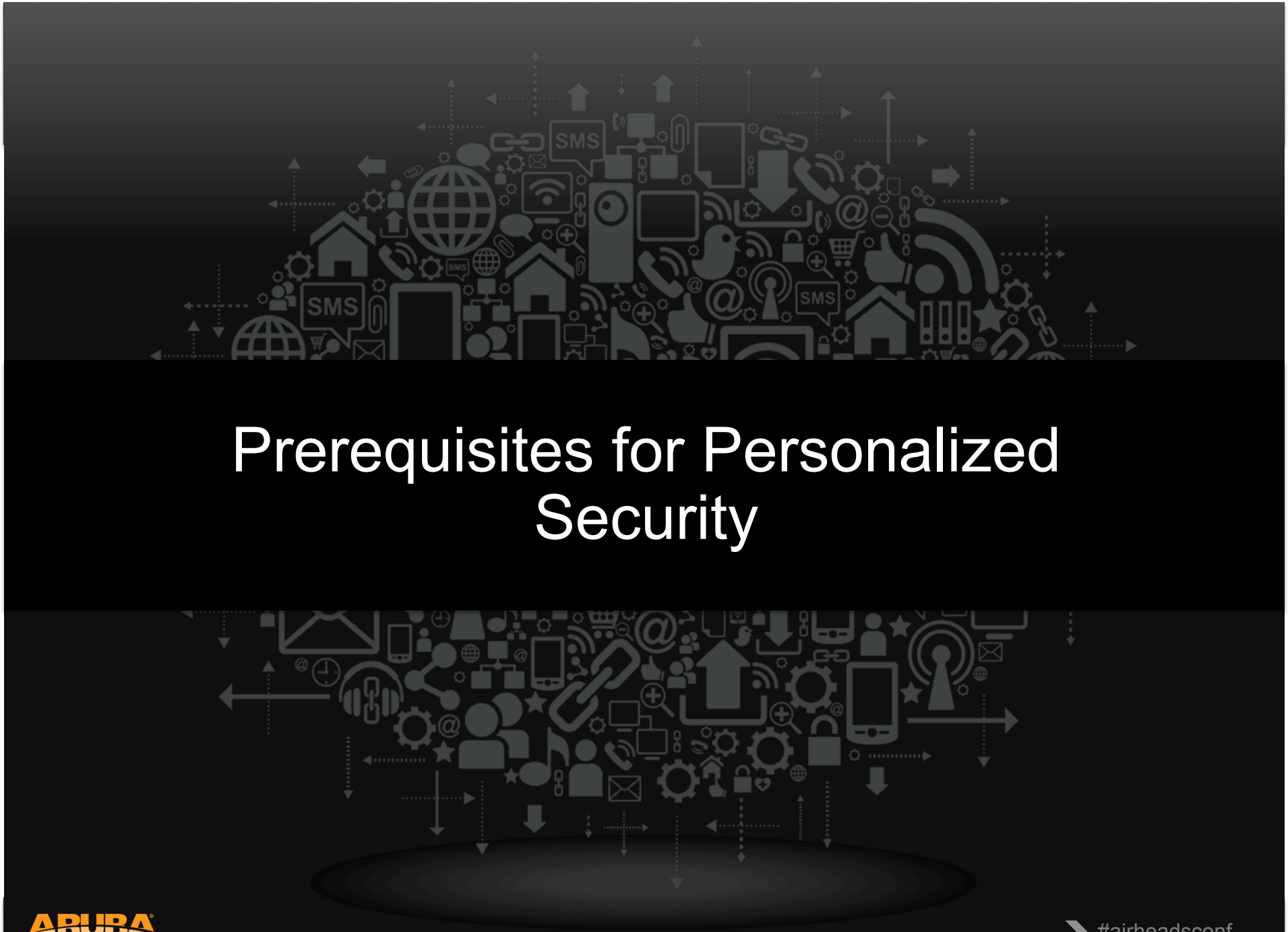
Personalized, Context Aware Security is The Answer



Personalized Security Solves Our Problems

- ✓ Reduce the likelihood of an information security breach
- ✓ Reduce the impact of any breach or malware outbreak
- ✓ Create an audit trail to ensure policy compliance
- ✓ Increase the reliability of your network

- ✓ Ensure enterprise-critical apps are always available
- ✓ Keep everyone productive
- ✓ Allow guests on our network
- ✓ Support remote workers just like they are in the office



Prerequisites for Personalized Security

Prerequisites for Personalized Security

Secure the Connection

Identify the Device and User

Classify the Traffic

Control Access

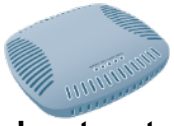
Optimize the Experience

Follow the User

VPN

Mobility Access Switch

Mobility Controller



Instant AP

Across All Access Methods

Prerequisites for Personalized Security

Secure the Connection

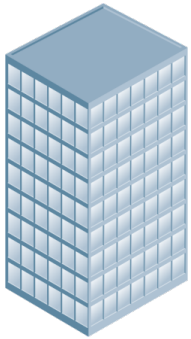
Identify the Device and User

Classify the Traffic

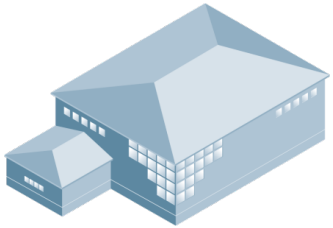
Control Access

Optimize the Experience

Follow the User



HQ



Branch

SOHO

Road Warrior

At All Locations

With a Single, Universal policy

AIRHEADS 2013

Any User

Employee

Contractor

Visitor

Shopper

Patient

Any Device

iOS

Any App

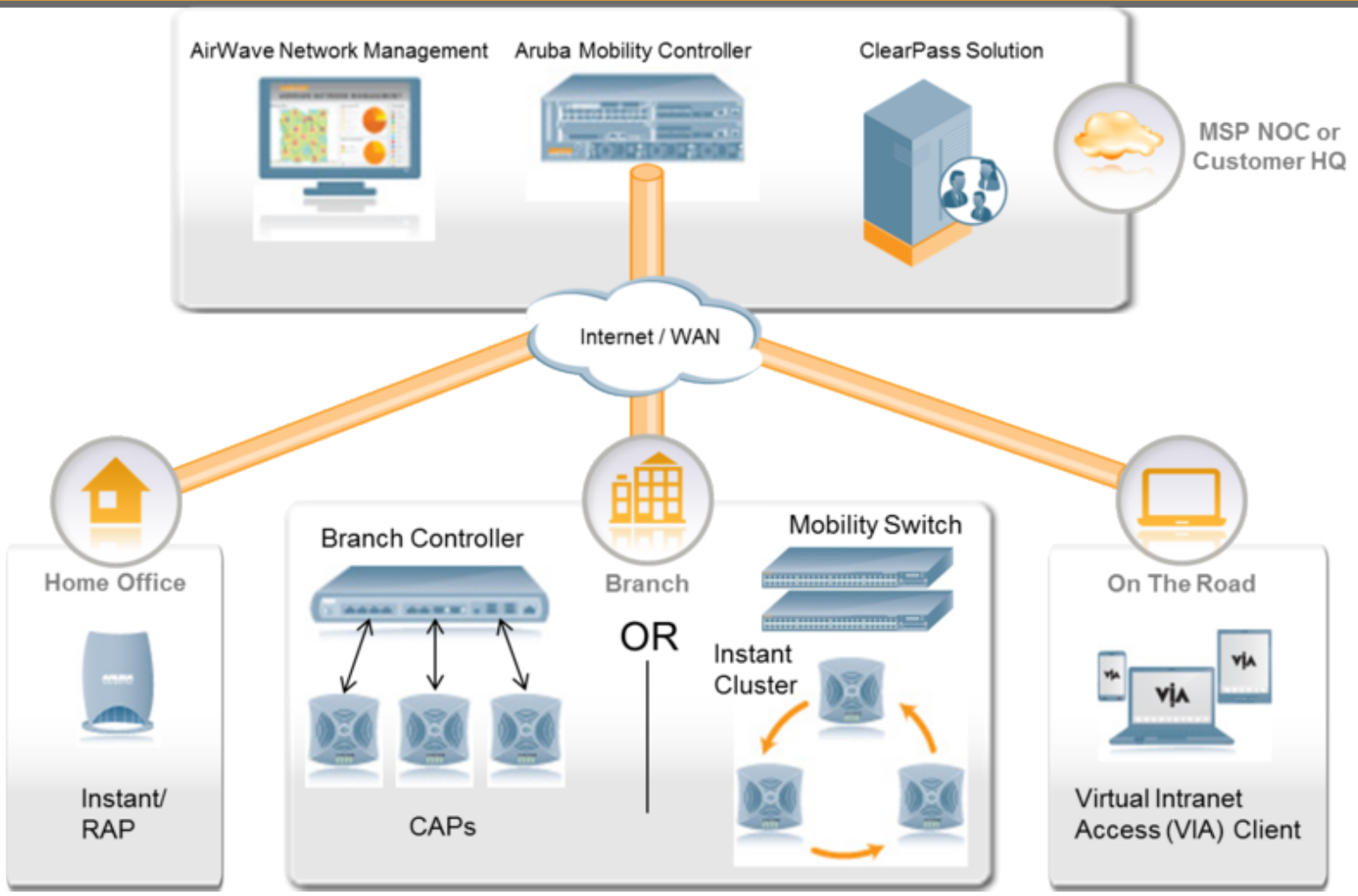
box

NETFLIX

Any Data

- ✓ Posture
- ✓ BYOD
- ✓ Corporate
- ✓ Time of Day
- ✓ External Data

Typical Aruba Network



Security Architecture Roles

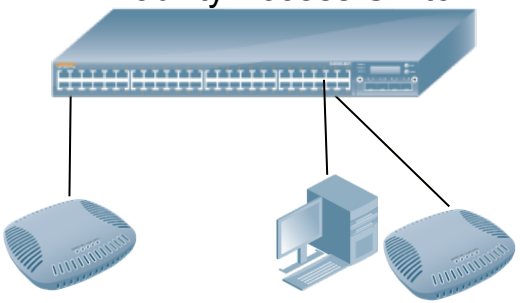
ClearPass Policy Manager

- **Policy Decision Point for wired and wireless**
- **Authentication Server**
- **Certificate Authority for BYOD**

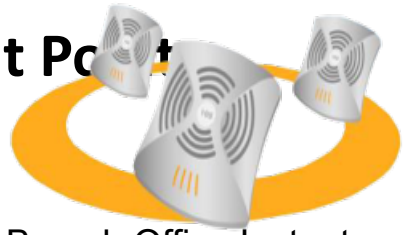
Controller

- **PDP in non-CP environments**
- **Policy Enforcement Point**

Mobility Access Switch



- **Policy Enforcement Po t**



Branch Office Instant

RAP

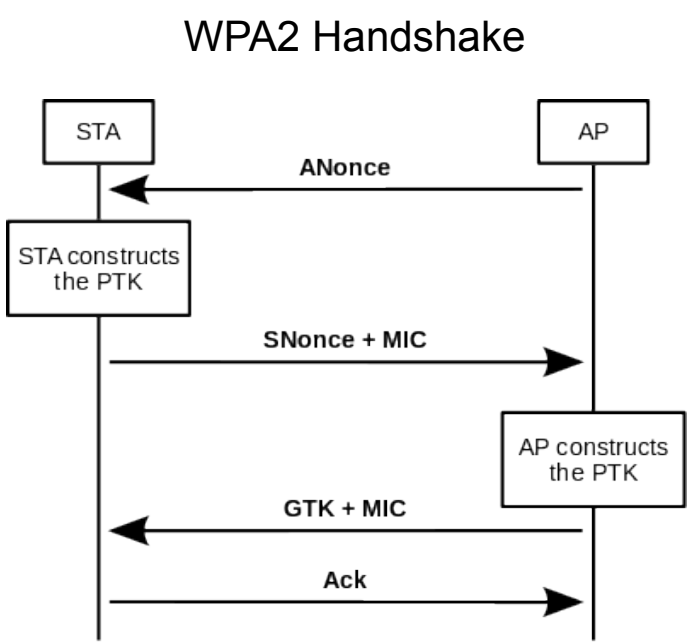
AirWave – Complete Network Insight

- **Controller sends all events to Airwave**
  - User authentications
  - Wireless Intrusion events
  - **All application data**
- **Account for network activity by user, time, date, location**
  - Who used what applications? When?
  - Which applications are taking all my bandwidth?
  - Requires AirWave 7.7 or later
- **Ensure PCI compliance with built-in reports**
- **Forensic information for network outage reports**

Personalized Security Step-By-Step

Universal Encryption

WPA2 Enterprise - Strong Over Air Encryption

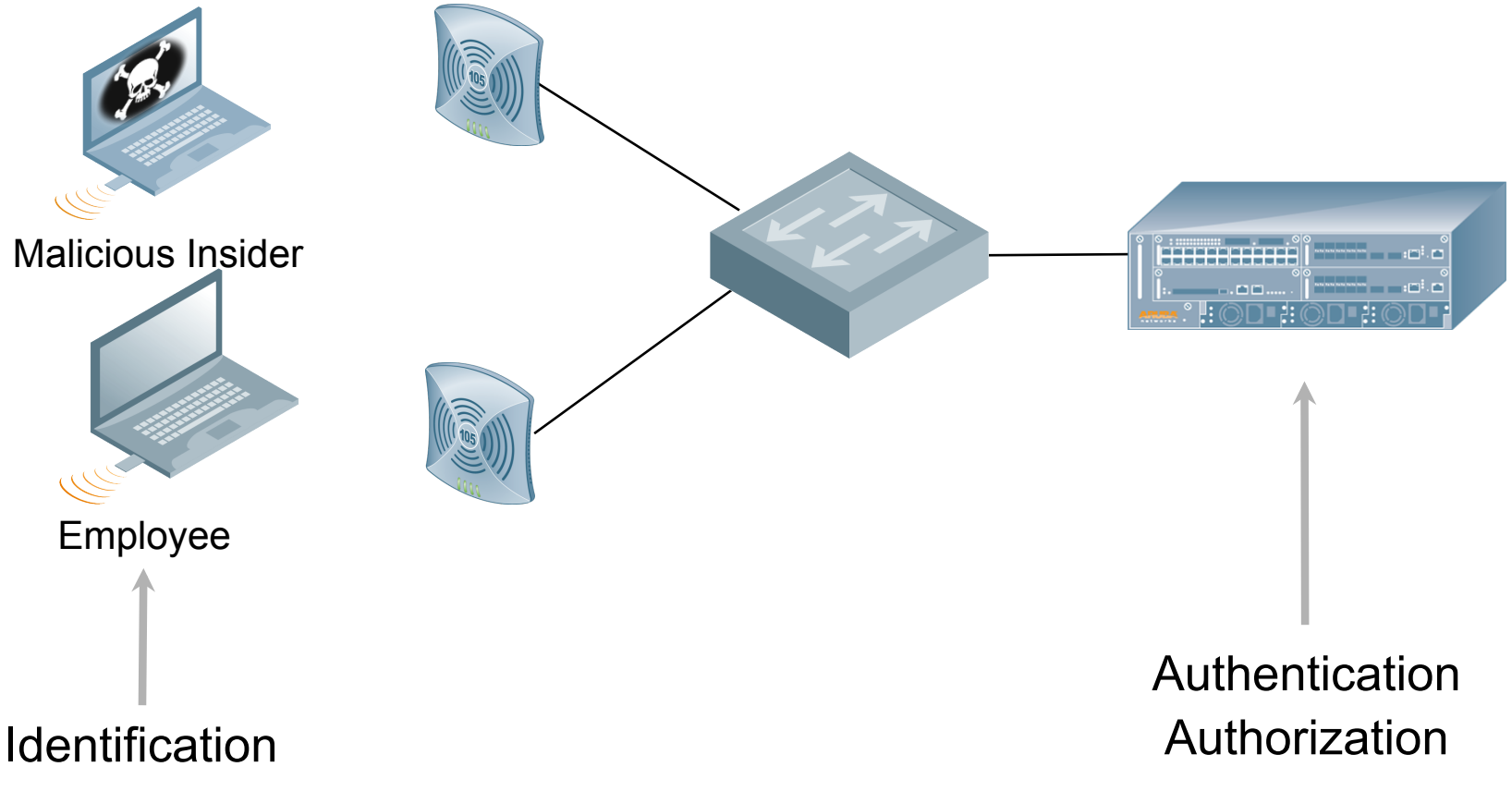


- **Combines strong encryption, including AES-CCMP, with mutual authentication**
  - Ensures users do not connect to an imposter AP
  - Protects the data to the level that the Federal Information Processing Standard requires
- **Not subject to the brute force attacks used against weak WPA2 PSK passphrases**
- **More secure than an open Ethernet port**

Isn't MSCHAPv2 broken?

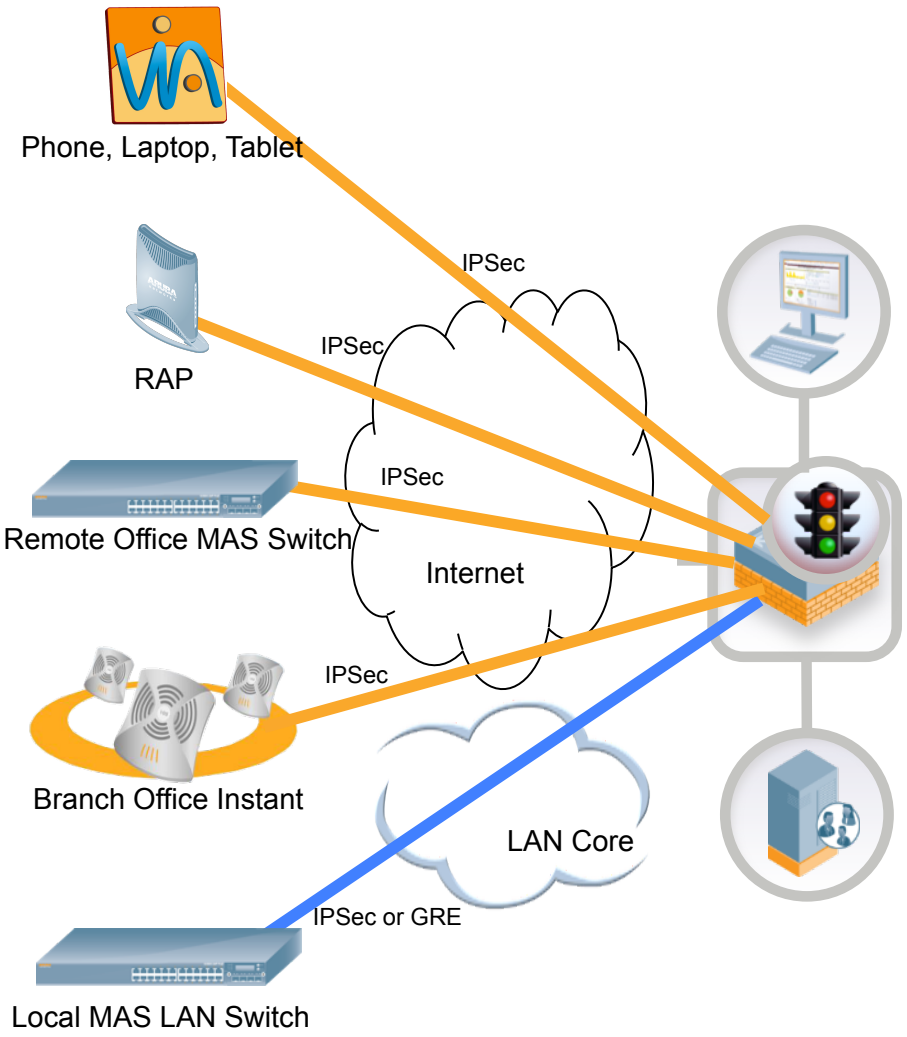
- **Short answer: Yes – because of things like rainbow tables, distributed cracking, fast GPUs, etc.**
- **This is why we use MSCHAPv2 *inside* a TLS tunnel for Wi-Fi**
- **Still using PPTP for VPN? Watch out…**

Centralized encryption increases security



Aruba Centralized Encryption

Encryption Extends Everywhere



- **IPSec encryption protects all edge traffic**
  - Full IKEv2 Support
- **Regardless of access method**
  - VIA
  - RAP
  - Remote MAS
  - Instant
  - Local MAS
- **Eliminates eavesdropping on the wire**

Aruba VIA Client

- ✓ **Mobile device policy compliance**
  - End-to-end authenticated and encrypted session to controller
  - Automatically detects trusted/untrusted network; establishes connected when needed
- ✓ **Supported devices**
  - Windows (32/64 bit)
  - Apple iOS
  - Mac OSX
  - Android 4.x
  - Linux (April 2013)
- ✓ **Seamless Mobility**
  - Firewall policies tied to user role
  - Same policy as in campus, branch
- ✓ **Best in Class Security**
  - Supports NSA-approved Suite B cryptography
  - IPsec VPN with SSL fallback

Authenticate Everything

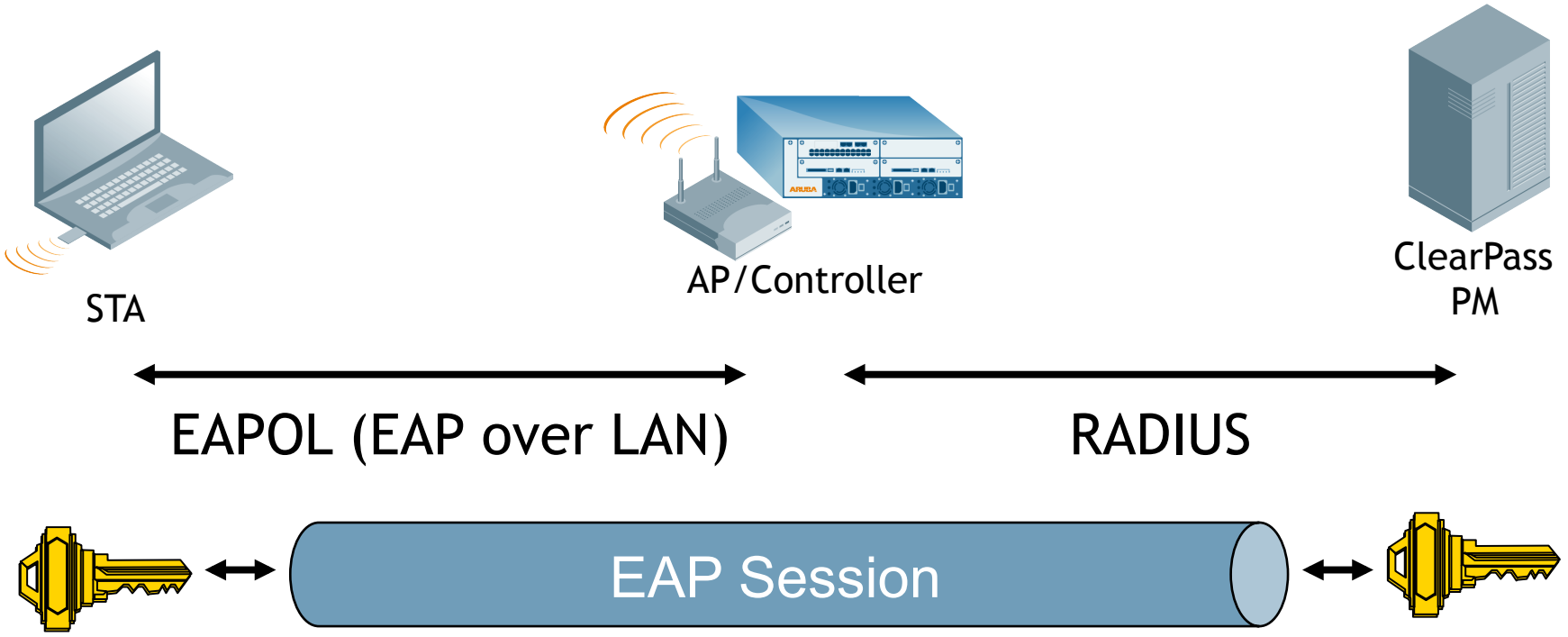
Strong Authentication of User and Device

- **Use Mutual Authentication whenever possible**
  - Network proves its identity to the client
  - Client Proves its identity to the network
- **Whenever possible, use single sign on (SSO) strategies**
  - Not only across network types, but also enterprise apps
  - Typically, link LDAP or Active Directory to all enterprise access
- **Multiple options for securing identity**
  - AD Credentials, User based certificates, machine certifications, Multifactor Authentication
  - Options for multiple identity stores

Universal Authentication for Wired, Wireless, and Remote Users

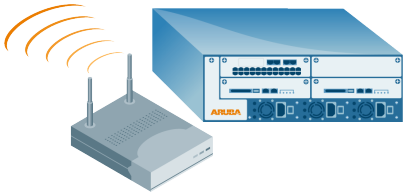
- **WPA2-Enterprise for wireless security**
  - Includes 802.1X for strong authentication
- **Multiple Methods for Wired Authentication**
  - 802.1X
  - MAC
  - User Derived Roles

EAP to RADIUS Server



Local EAP Termination

STA



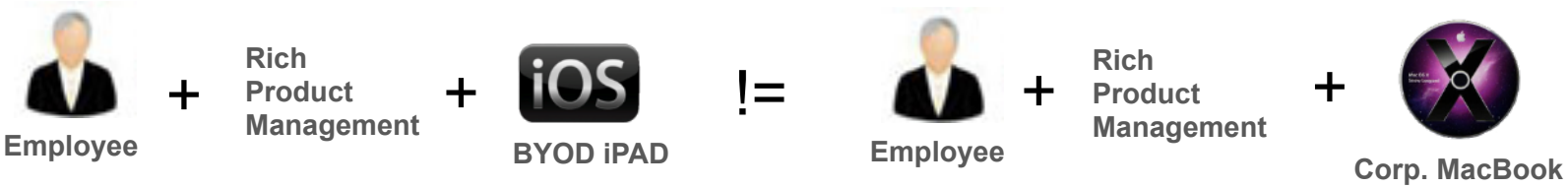
AP/Controller

Authentication Server

EAPOL (EAP over LAN)

RADIUS/LDAP (optional)

Extended Identity is Key to Personal Security



- Strong authentication of user yields their identity and their role
- Strong authentication of the device yields its risk profile
- Allows fine grain assignment of roles and a highly personalized experience

How do we assign these roles?

- **Controller**
  - Default Roles can be assigned
  - Roles can be derived using a few basic traits
- **ClearPass**
  - Roles can be assigned based on the authenticating user and device
- **ClearPass profiling**
  - ClearPass can fingerprint the device using a variety of traits
  - This can trigger an onboarding event for quicker, safer authentication next time

Role Derivation

Default Roles

- Configurable by authentication method
- SSID

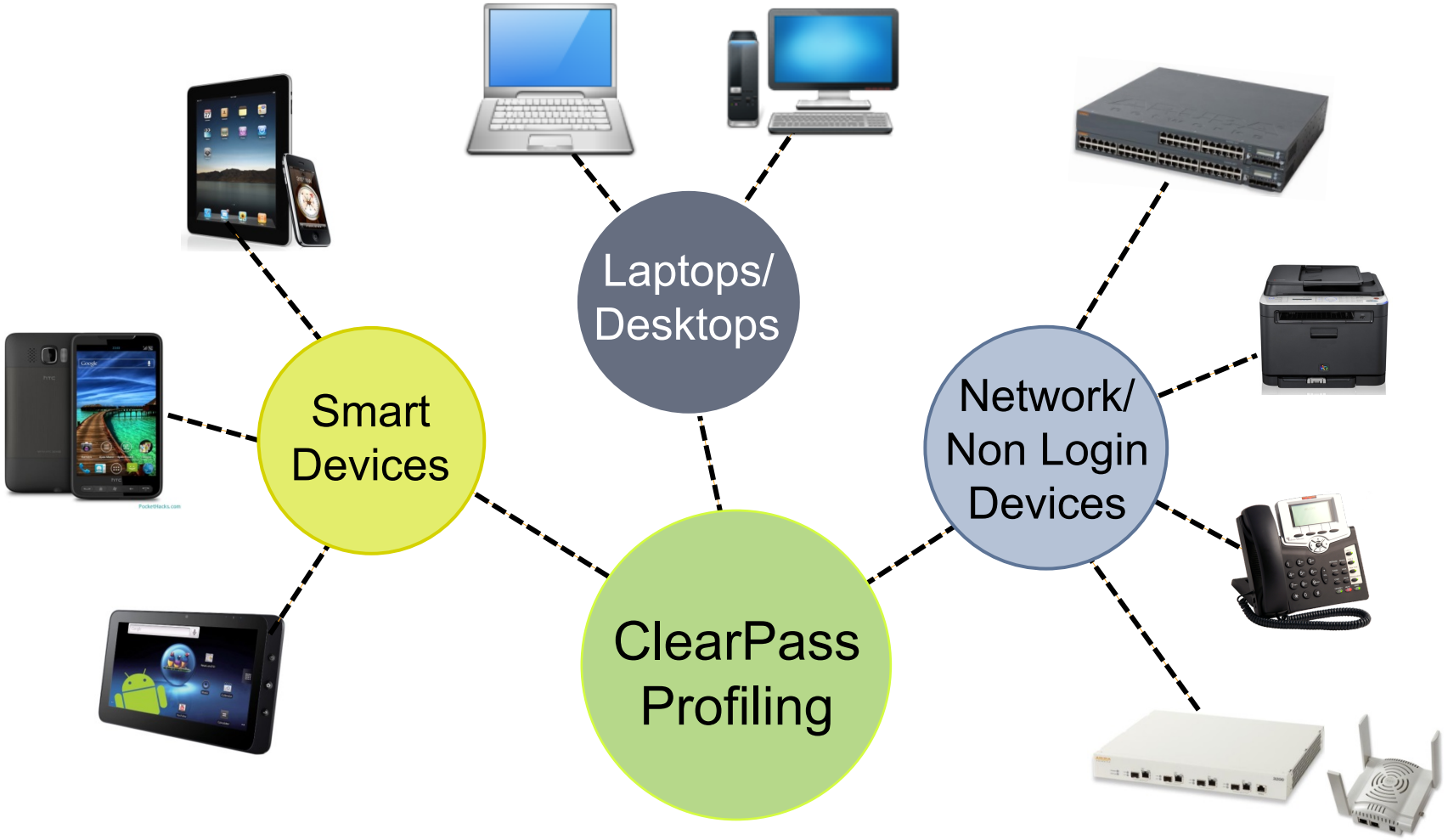
User Rules

- Device-specific attributes
- Encryption type
- AP used (by name or BSSID)

Server Derived Roles

- Role assignment based on attributes from ClearPass server
- Different access privileges based on security policy
- Can use single SSID for all users/ devices
- ClearPass advanced profiling
- Policy compliance
- Real Time event driven

What Does ClearPass Profile?

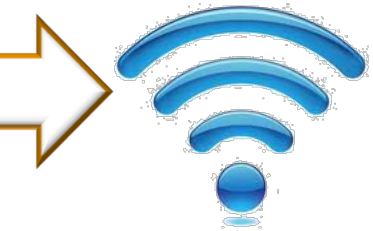


ClearPass Device Onboarding

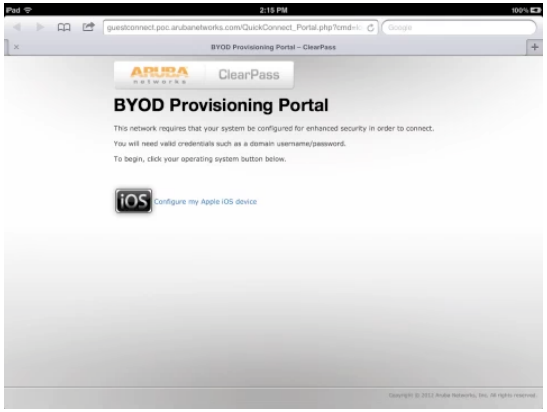
1. Device type automatically detected & redirected to portal

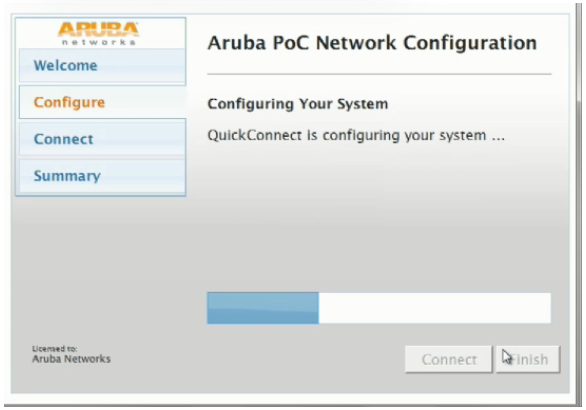
2. Settings & credentials are auto-configured after user enters domain credentials

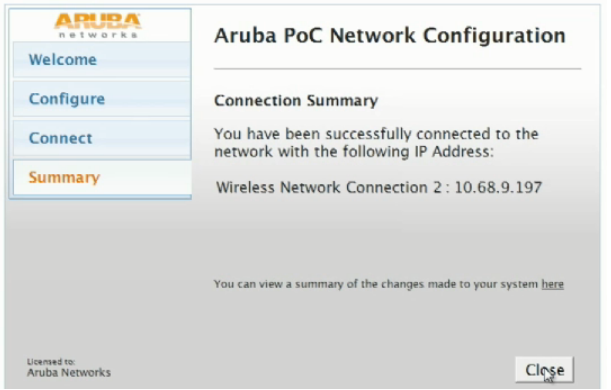
3. User automatically placed on proper SSID & network segment



SSID = EnterpriseWPA2

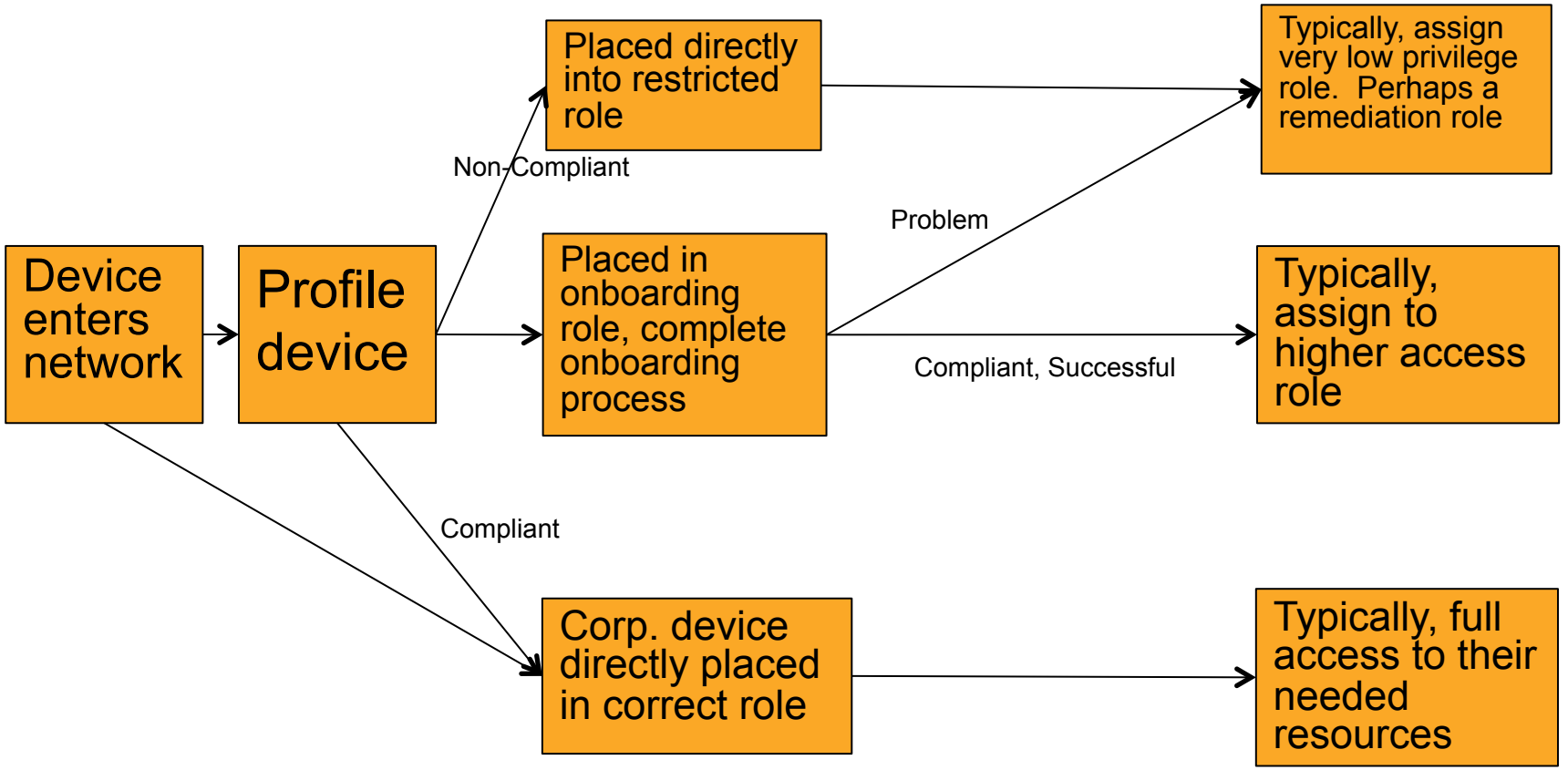






Granular BYOD Onboarding Controls

How Can I Use This Information?



How do I safely give Guests Network access

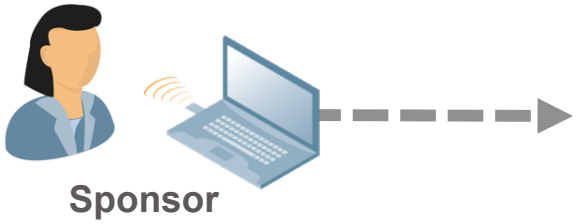
Controller-based Guest Access

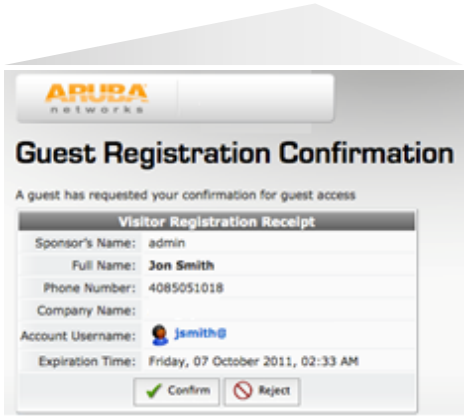
- Customizable welcome page
- Flexible authentication options

ClearPass based Guest Access

- Highly customizable
- Advertising options
- Self registration
- Sponsored registration
- Preregistration

Example: Sponsor Registration





1. Sponsor creates guest credentials

2. Account enabled, visitor notified VIA screen, SMS, or email

3. User logs in when they arrive

Control Access

Typical Roles

Guest

Contractor

Doctor

Students

Faculty

Employee

Employee – BYOD

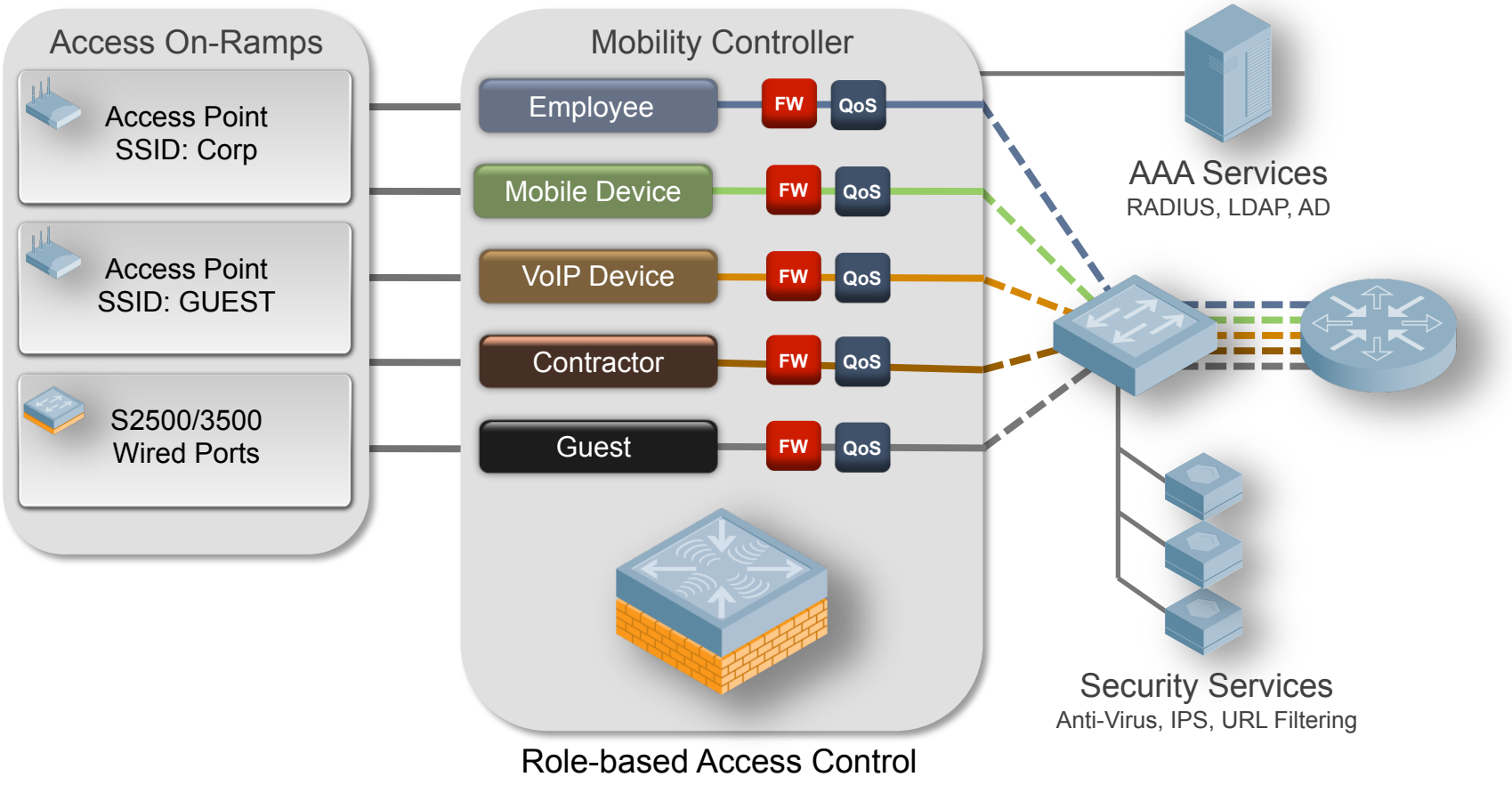
Corporate Mobile Device

Unified Communications

Infrastructure

Role-Based Security

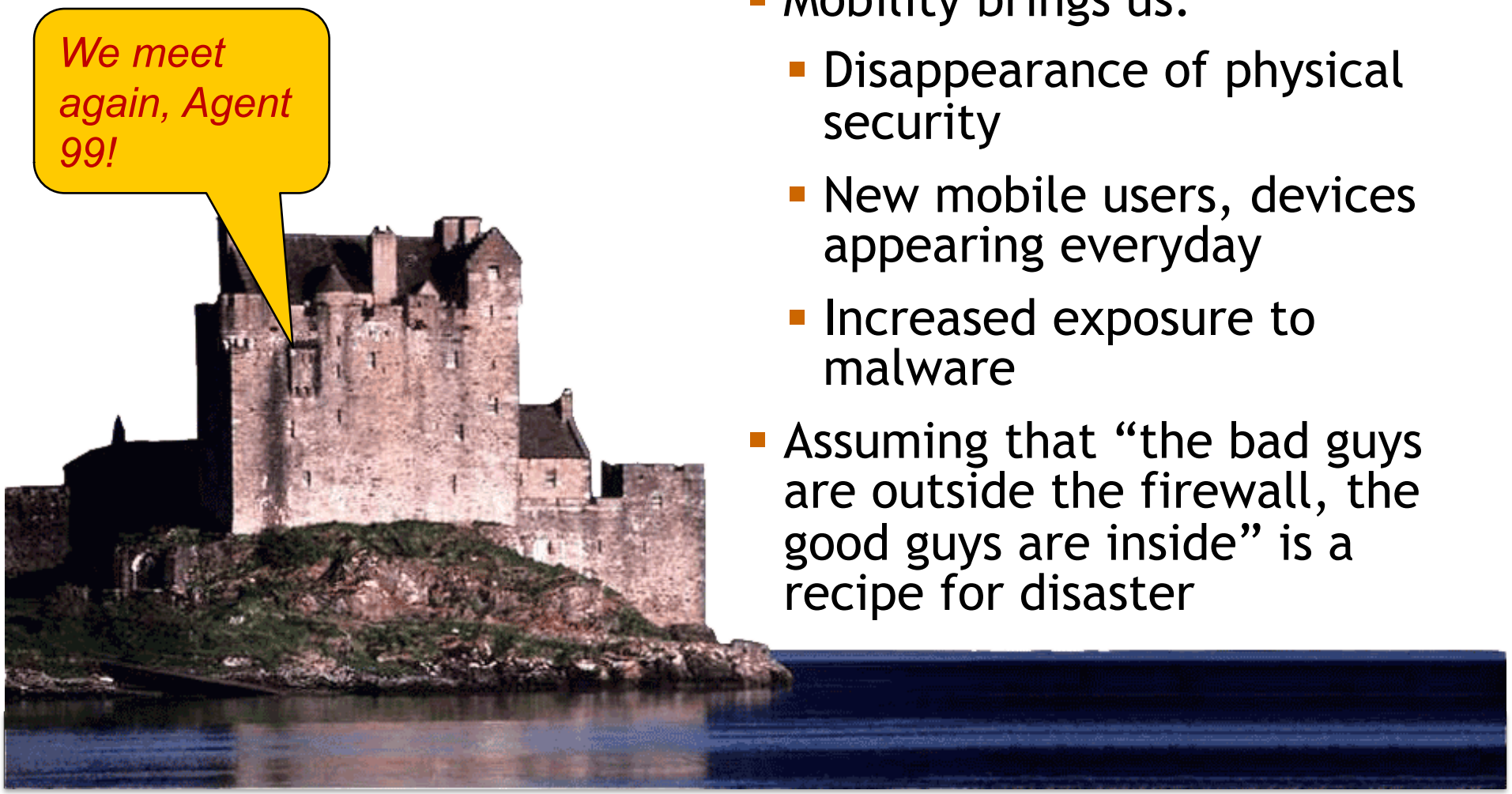
Multiple classes of users on same infrastructure easily separated



Why Worry About Authorization?

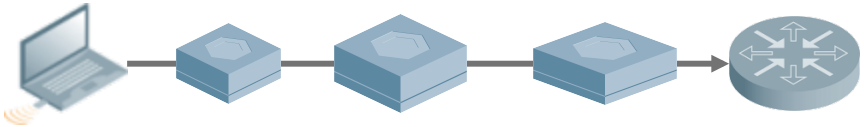
Where is the "network perimeter" today?

AIRHEADS 2013



- Mobility brings us:
  - Disappearance of physical security
  - New mobile users, devices appearing everyday
  - Increased exposure to malware
- Assuming that "the bad guys are outside the firewall, the good guys are inside" is a recipe for disaster

VLAN-Based Security Can't Scale



MAC, IP – User Mapping

User – VLAN Mapping

VLAN – Policy Mapping

- **User identity is based on MAC or IP address (weak identities – like a boarding pass)**
- **Maintaining VLAN/Role mappings across a large network is very difficult**
- **User identity can be spoofed which means ACL can be violated**

Aruba Policy Enforcement Firewall

Context Aware, Identity Based

AIRHEADS 2013

Session Processing

- Identity-based firewall policies
- MAC Address – IP Address – VLAN – User Name – User Role – Firewall Policies binding
- Traffic Management

Protocol Processing

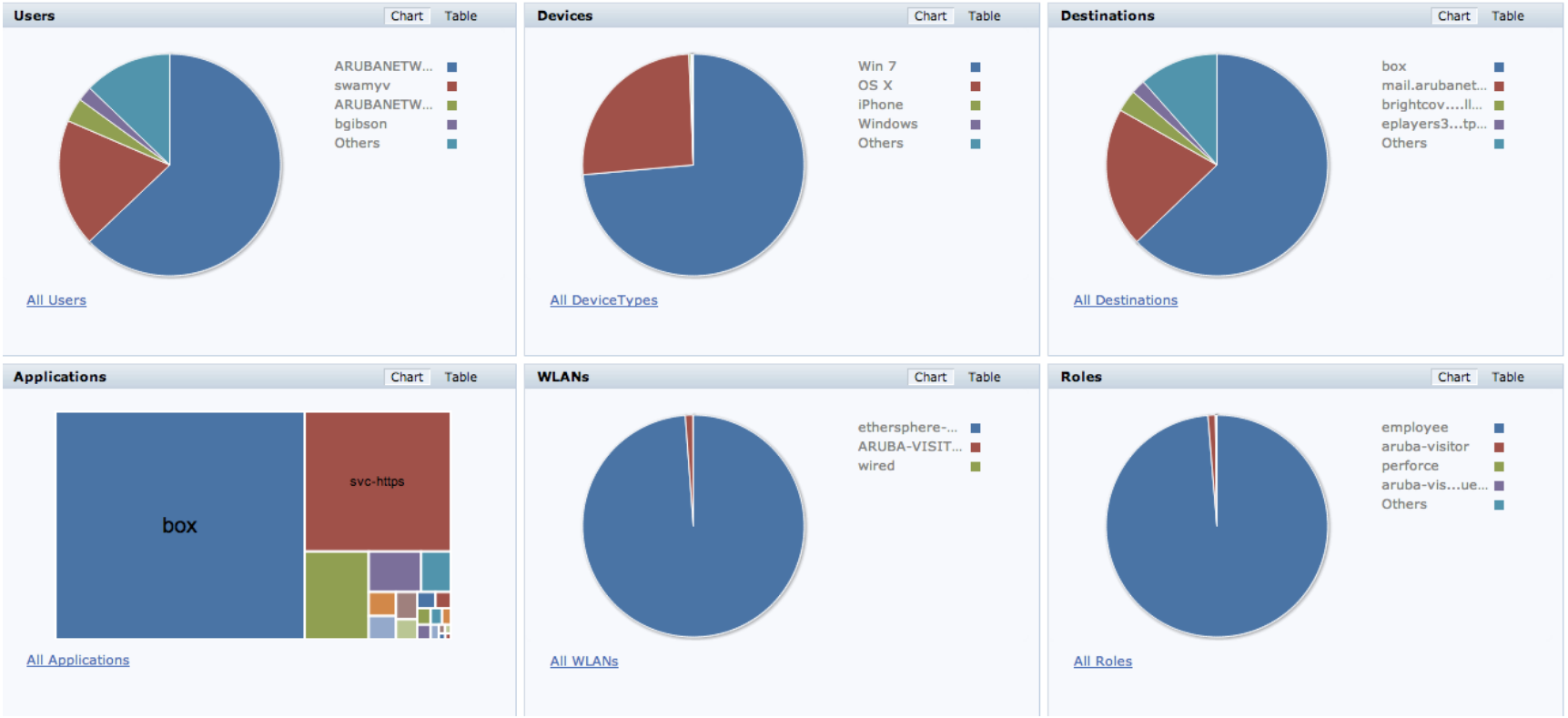
- ALG for SIP, RTSP, FTP, TFTP, SCCP, Vocera, ICMP
- Intrusion/DoS Detection and Prevention
- Detects SYN, ping, ports scan attacks
- Can prevent continued attacks (black list station)
- Enforces TCP handshakes, prevents replay attacks

Station Blacklisting

- Authentication Failure
- Firewall Rule Violation
- TCP Attacks

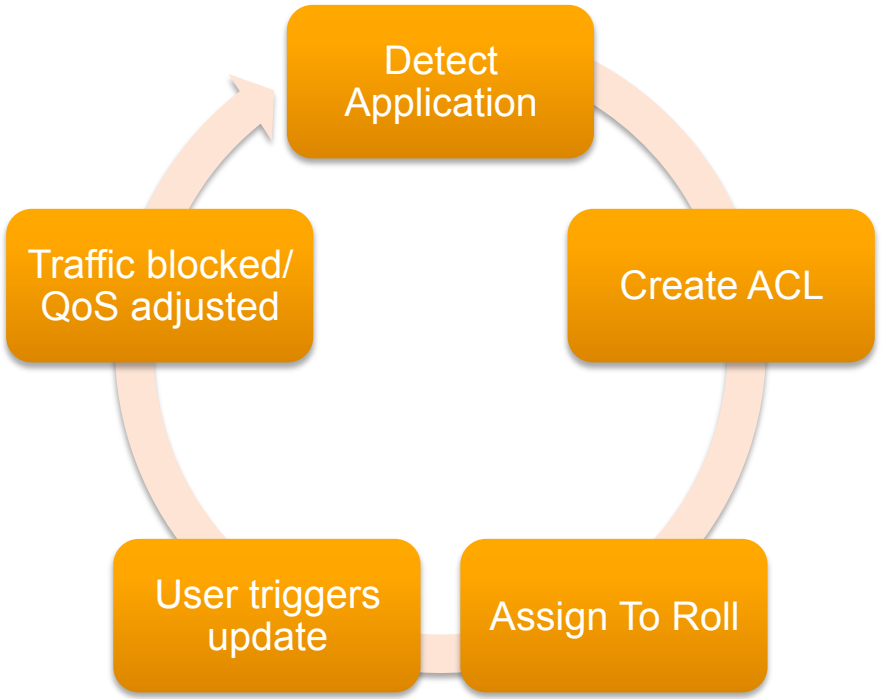
ICSA Certified

AppRF Application Monitoring and Control



- New “Firewall” Dashboard UI
- Includes summary views of activity by Users, Devices, Destinations, Applications, WLANs, Roles
- Allows drilling down into details of each

Real-Time Application Control



- Dynamic web-application prioritization
- Use roles to limit or QoS applications
- Real Time ACLs updated whenever user tries to use app
- ACLs can block, QoS, log, mirror traffic, pause scanning
- No impact on throughput

Soon:

- Config stubs for common web-based applications

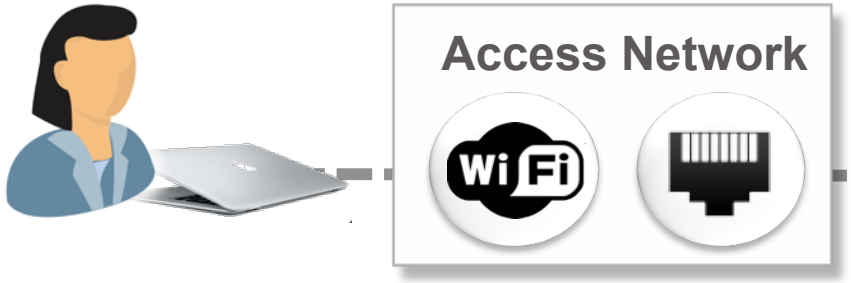
Built in CA for BYOD Device Access Revocation

What about compromised devices?

In order to maintain the reliability of your network, it's important to maintain the security health of your clients

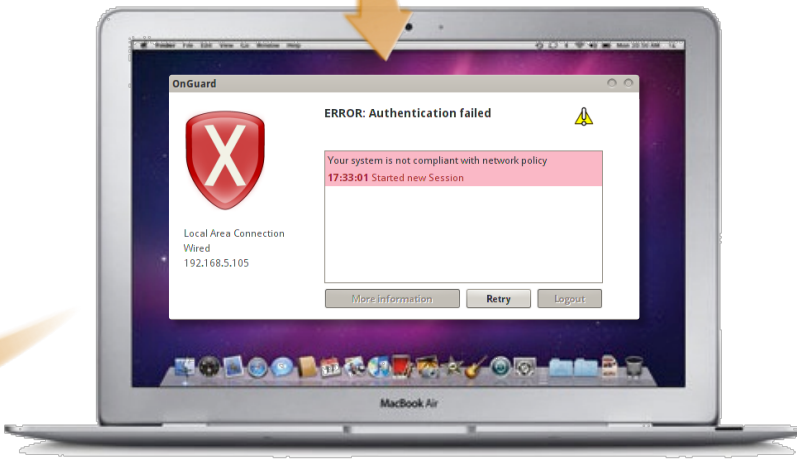
- Software updates
- Security patches
- Active and current antivirus

OnGuard - Control Compromised Devices

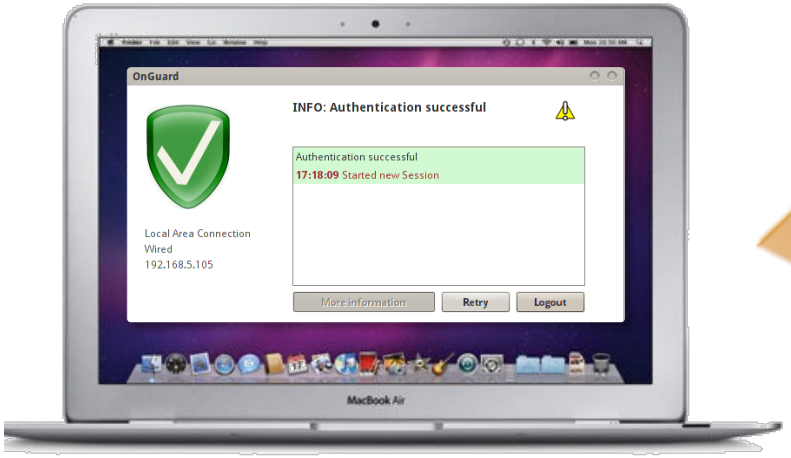


ClearPass Policy Manager with OnGuard

Detect unsecure devices



Minimizes Risk to Network



Block access to network resources across wired, wireless & remote
Auto-Remediate the device

Supported Endpoint Computers

- **Persistent and Dissolvable Agents for laptops/desktops**

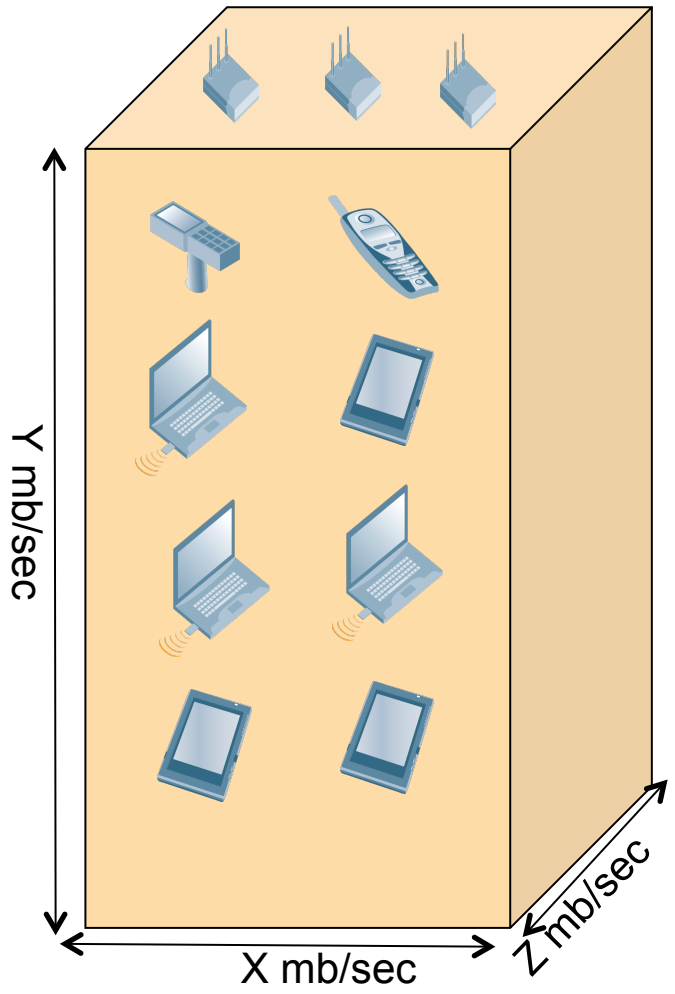
- All Windows Versions
- A/V, A/S, FW, registry keys, services, patch Mgmt, processes, peer-to-peer apps, USB storage devices, Hot Fixes, Hotspots & VMs

- Red Hat, CentOS, Fedora, SUSE
- Status of services, anti-virus and firewall

- Mac OS X
- Status of anti-virus, anti-spyware and firewall

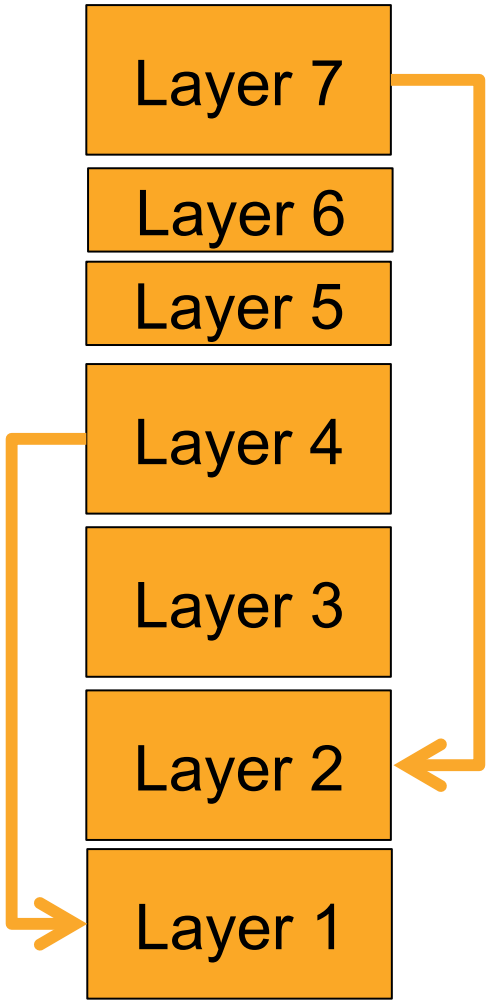
Optimize the Experience

Personalization and Control Required for Optimal Network Experience



- **Even as WLAN gets faster, there are new demands on networks**
  - Higher Device Density
  - Higher Bandwidth Apps
  - Complete reliance on wireless networks
- **Therefore, the air is a commodity that must be policed to ensure productivity**

Deep Network Awareness is Essential



- **Application awareness allows optimization of networking stack**
  - Use higher level information to add value at lower levels
- **Blocking inappropriate applications from wasting the air**
- **Layer 1 adjustments**
  - Pause radio scanning for critical apps
- **Layer 2 adjustments**
  - Fine grain QoS marking by User and APP to prioritize use of the air
- **Multicast and Broadcast Control**

Policy Must Follow User

Remember Universal Policy?

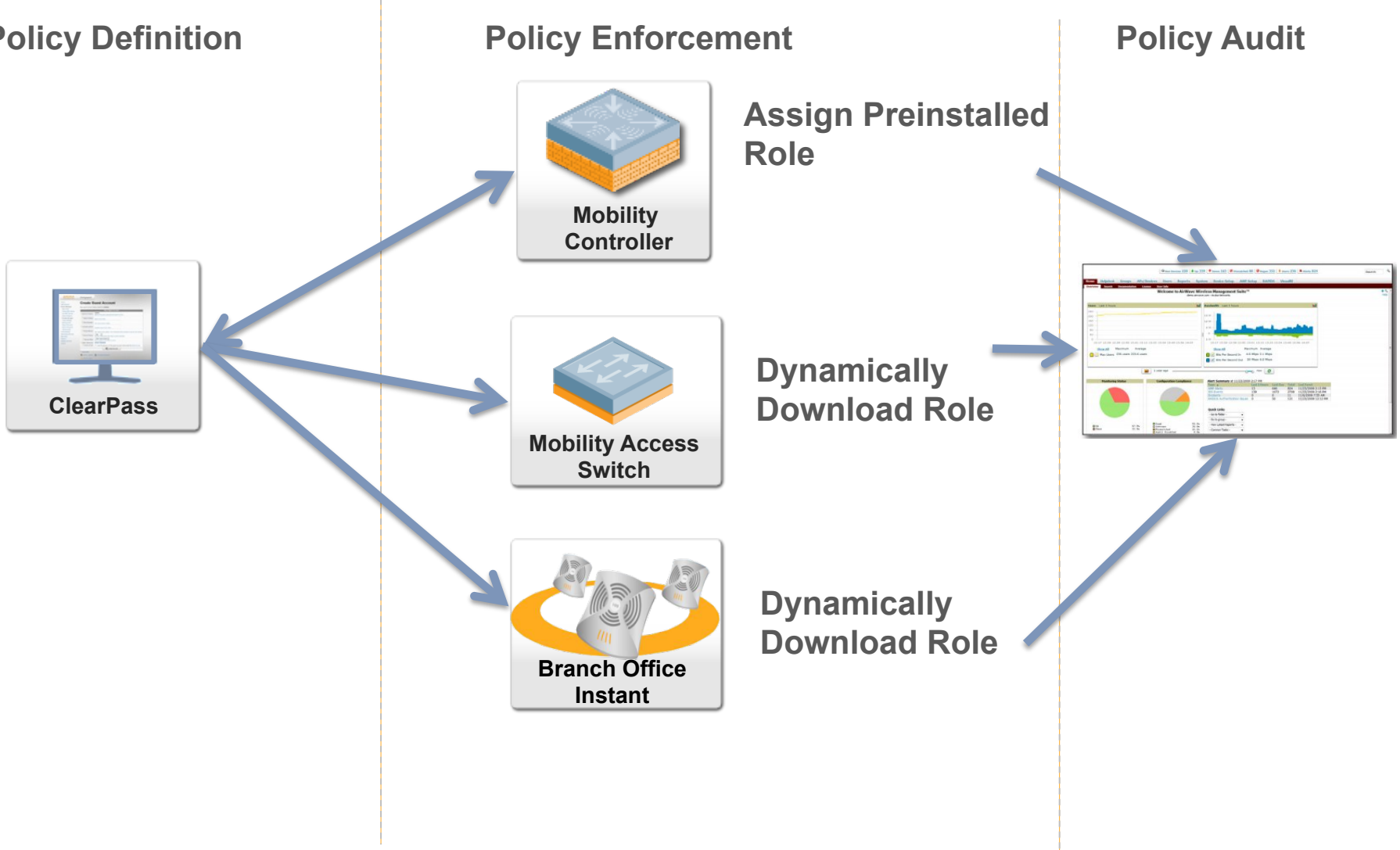
AIRHEADS 2013

ClearPass Policy Manager

ClearPass Context Sources

- Identity Stores – LDAP, Active Directory
- Controller – mDNS, HTTP Agent Strings, DHCP requests
- Active Profiling – SNMP, Nessus
- Passive Profiling
- Agent information – Microsoft NAP, OnGuard
- Time of Day
- Location
- Mobile Device Management Systems

ClearPass Policy Manager
Orchestrates Policies for all Users and Devices

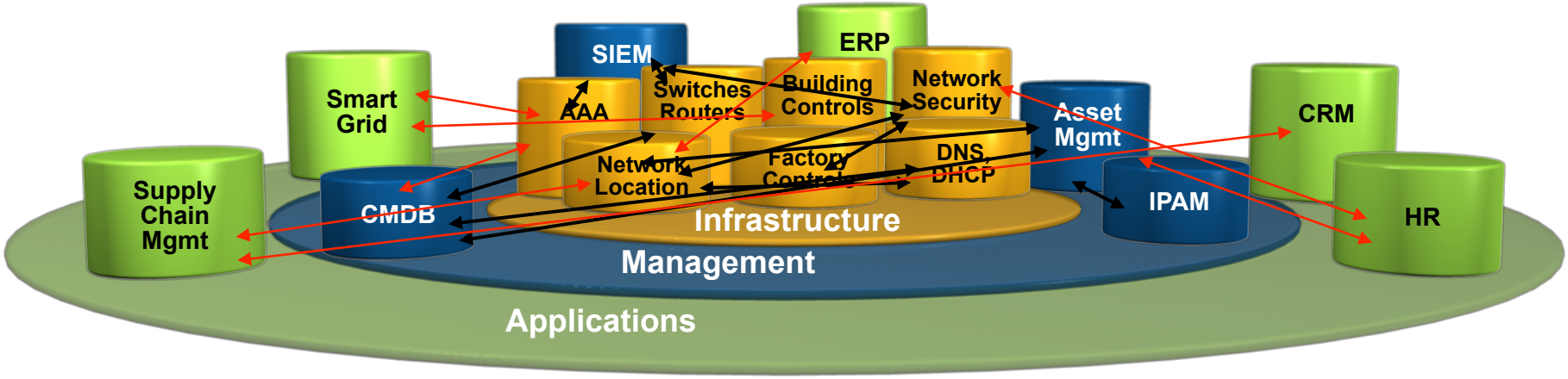


*New in AOS 7.2

Application and Data Control Features

	Controller	AirWave	ClearPass
Basic Device ID	✔		
Role based app enforcement	✔		
Real Time visualization	✔		
Guest Portal	✔		
Historical visualization and trending		✔	
Fault Identification		✔	
Network Wide Policy Enforcement			✔
Advanced Device ID			✔
Dynamic Role Provisioning			✔
Endpoint Policy Enforcement			✔
Advanced Guest Portal			✔
BYOD Device Onboarding			✔

Current Information Sharing Approaches

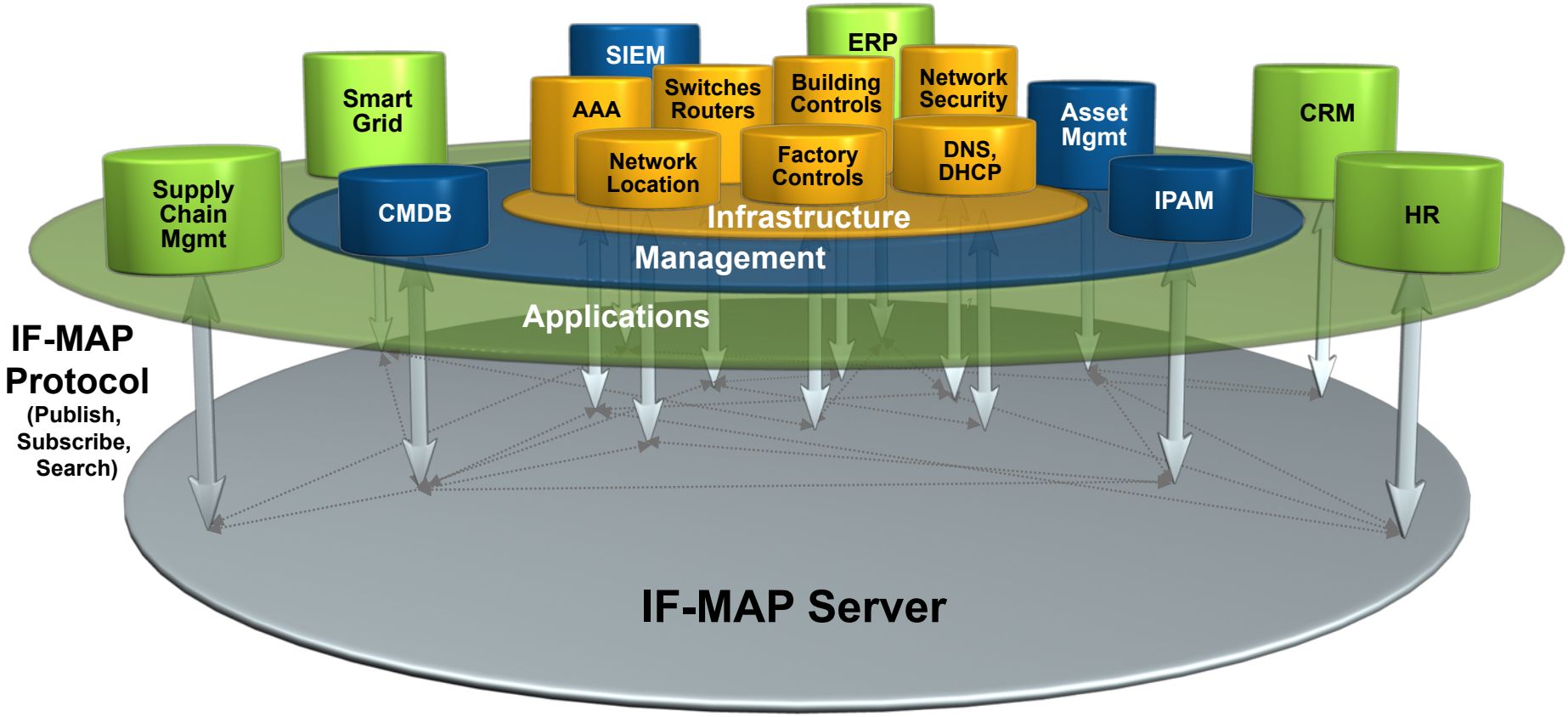


SNMP, Syslog, Netflow

Custom Integration – API's, Scripts

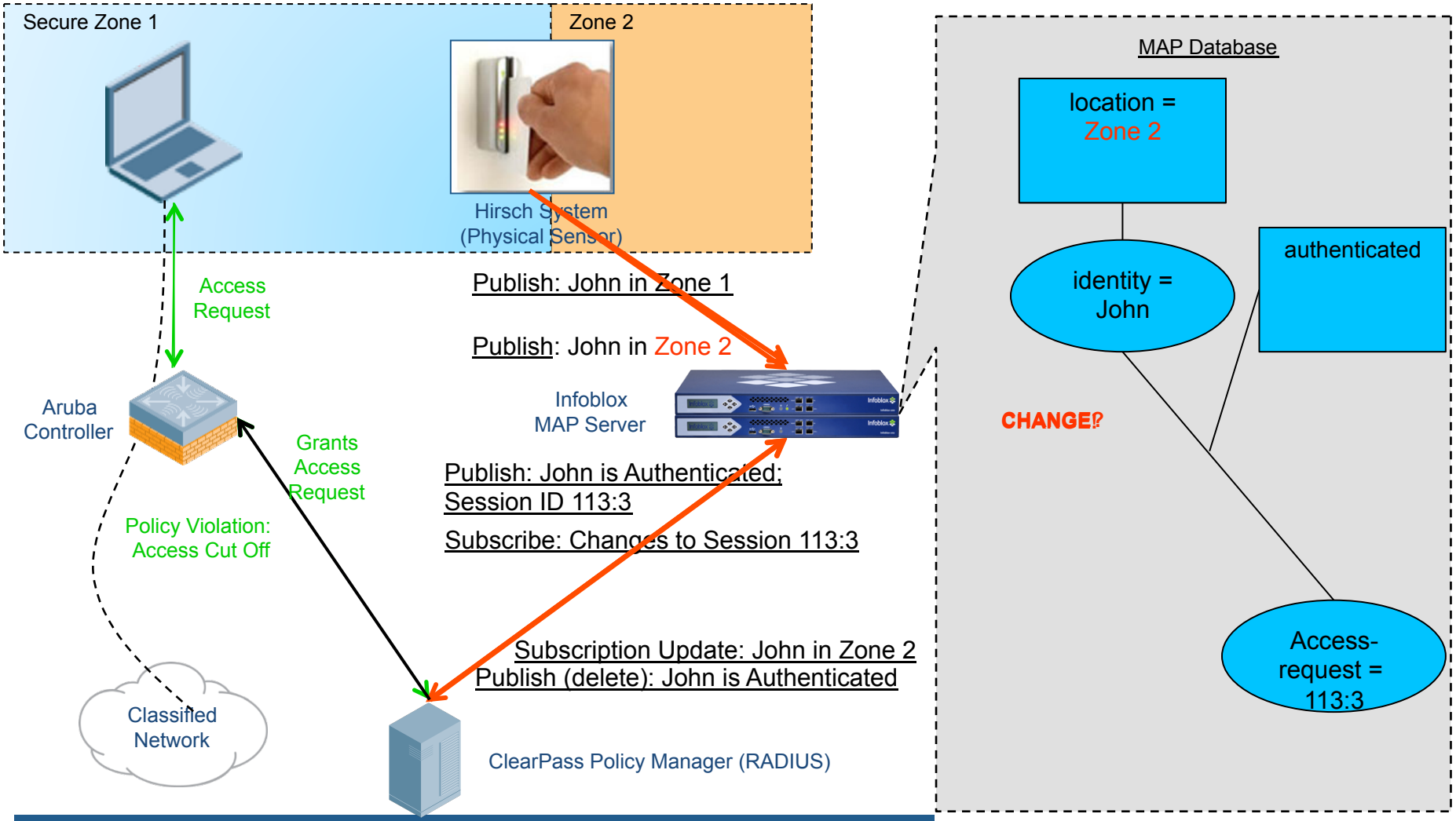
- Complex
- Costly
- Brittle
- High Maintenance

IF-MAP: Future of Information Sharing and Real-Time Policy



Automatically aggregates, correlates, and distributes data to and from different systems, in real time

Use Case – Integrated Network / Physical Security Solution



10- MAP updates PDP about the location change

Summary

- Personalized security and user experience is essential to meeting today's information security challenges
- These personalized policies must be enforced at every network touch point in a consistent manner to be effective
- Using an Aruba Networks infrastructure, the process of implementing personalized security is dramatically simplified
- Aruba's vision for the future of networking extends this vision even further

Thank You - Questions?


AIRHEADS
LAS VEGAS 2013
JOIN: community.arubanetworks.com
FOLLOW: @arubanetworks
DISCUSS: #airheadsconf