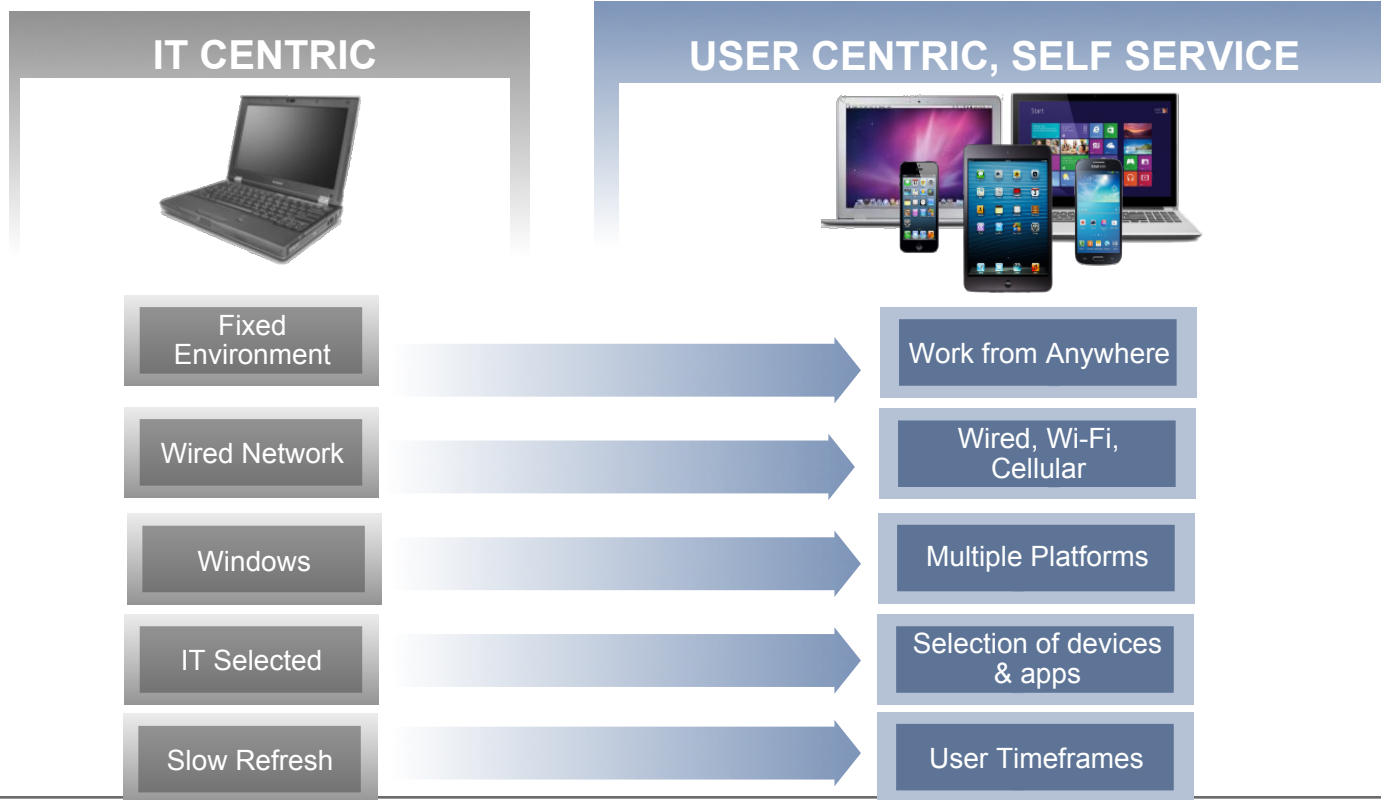


Secure Mobility Access

Aruba ClearPass



Evolving IT Landscape



Today's Mobility Challenges

VISIBILITY

What's on the Network?

WORKFLOW

No automation on unmanaged devices

POLICY

Company data on personal devices



NETWORK

NAC, Roles, Context

DEVICES

BYOD, Onboarding, MDM

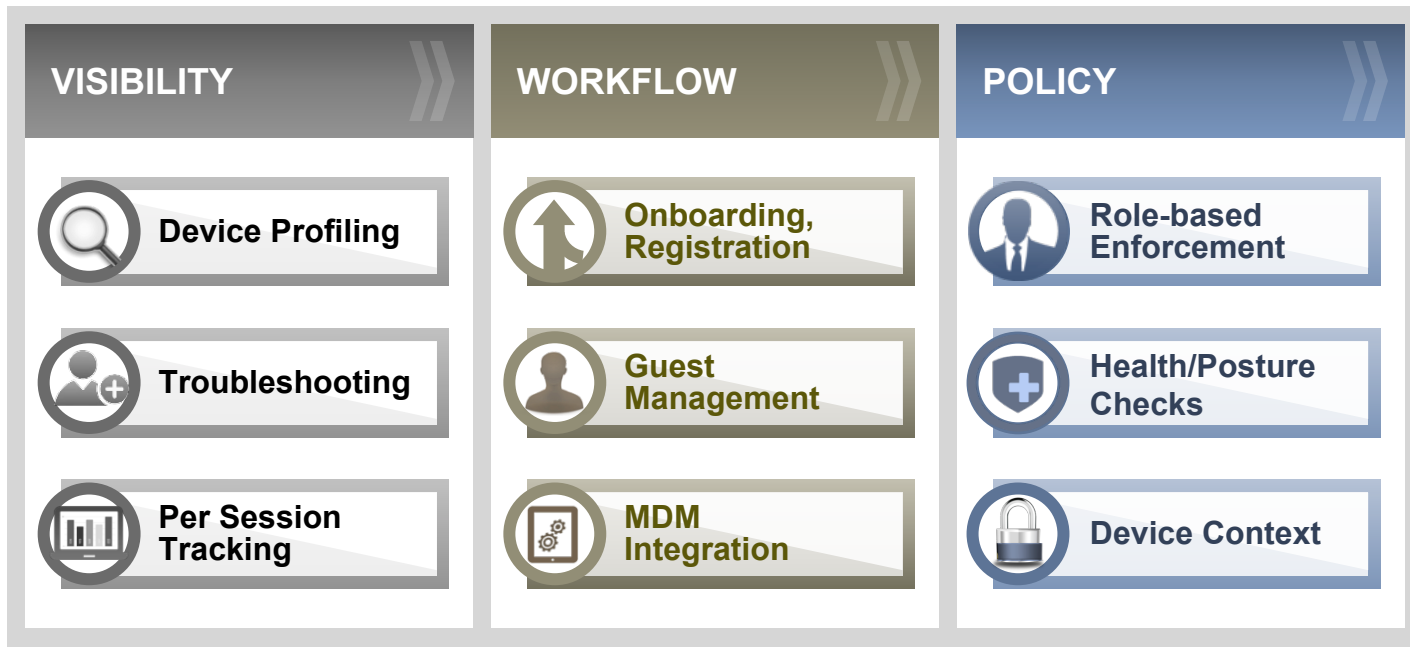
APPS

Use, Distribution, Control

Multiple solutions, increase IT touch points and errors

The ClearPass Solution

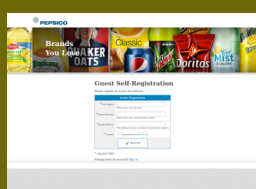
All Things Network, Device and App Management



Use Cases Customers Are Fixing

Old AAA
Solutions

AAA REPLACEMENT: Others lack integrated RADIUS & TACACS+, multivendor support, built-in profiling and ease of management!

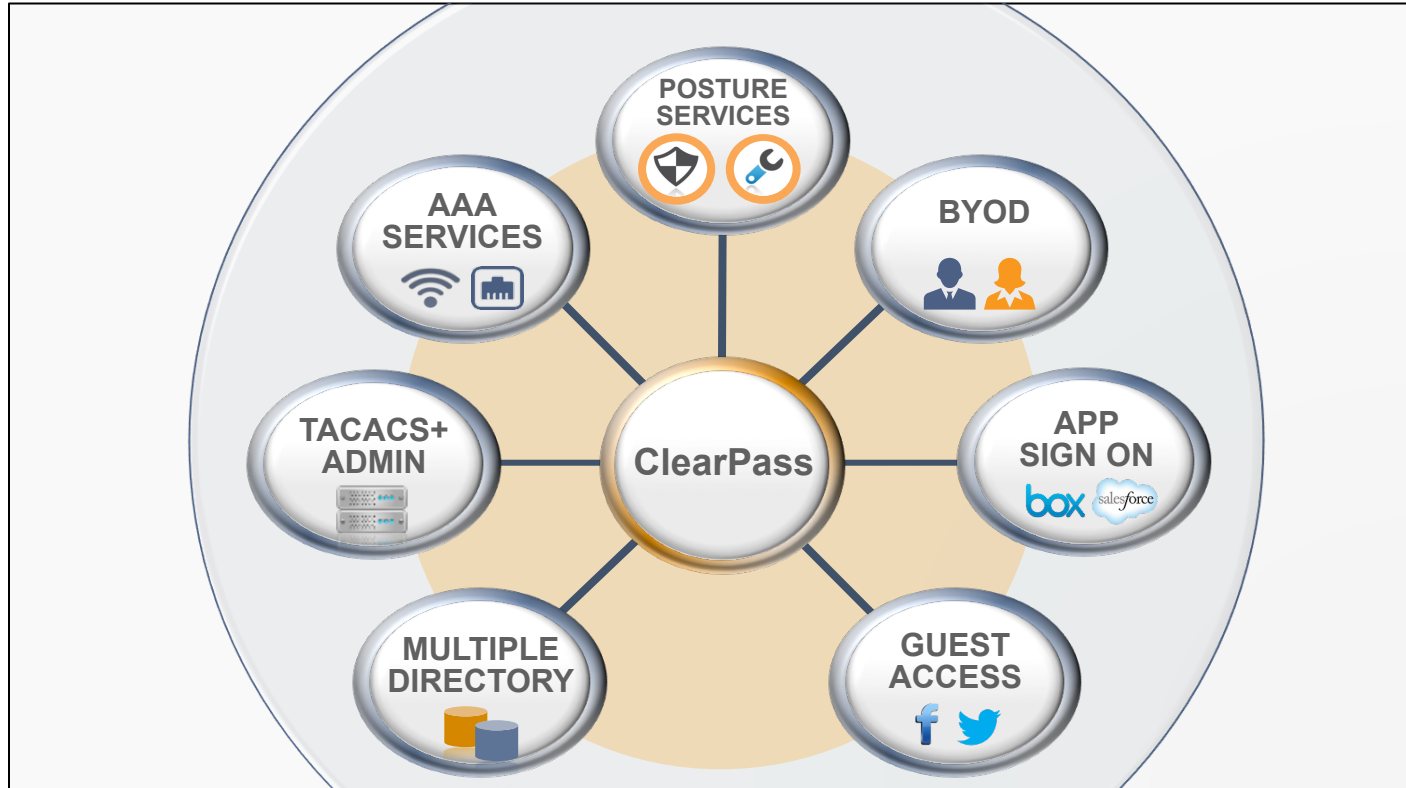


GUEST ACCESS: ClearPass works in multivendor networks, scales and makes the customer brand look good!

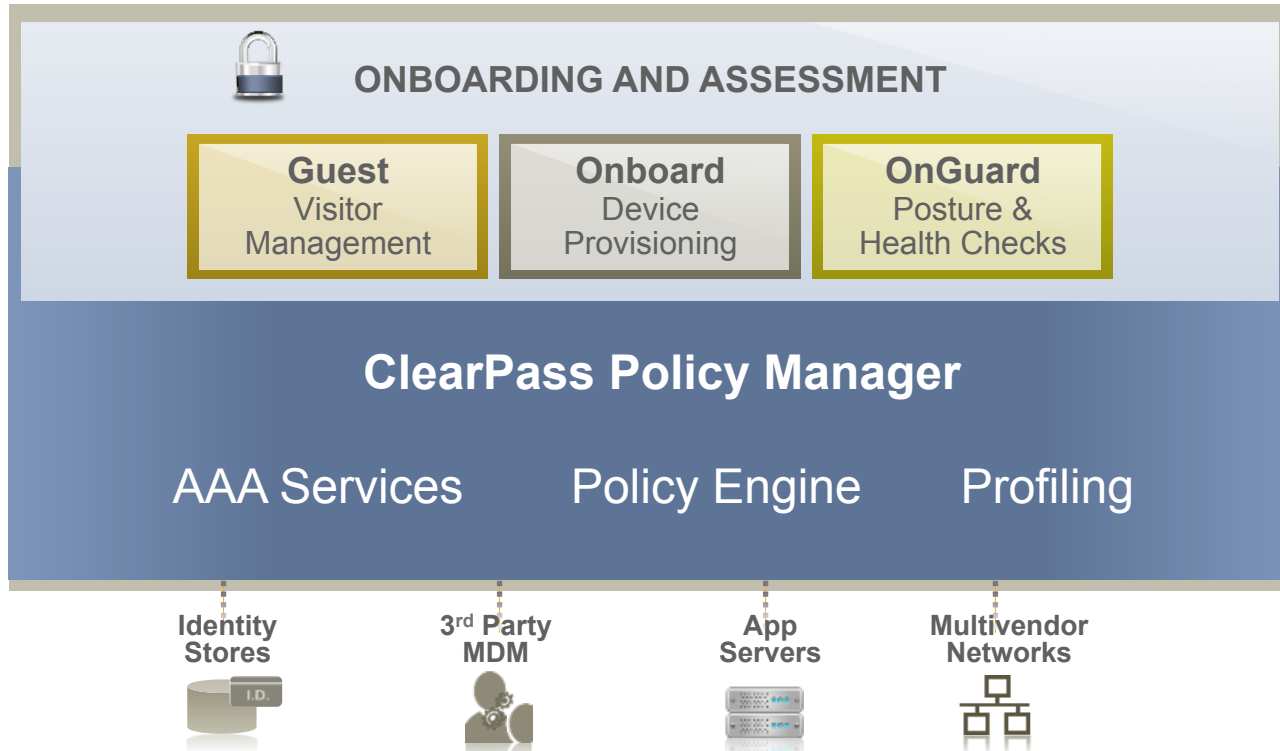


MOBILITY SERVICES: ClearPass Onboard with built-in CA, AirGroup, and IT Off-load features are making BYOD roll-outs easy!

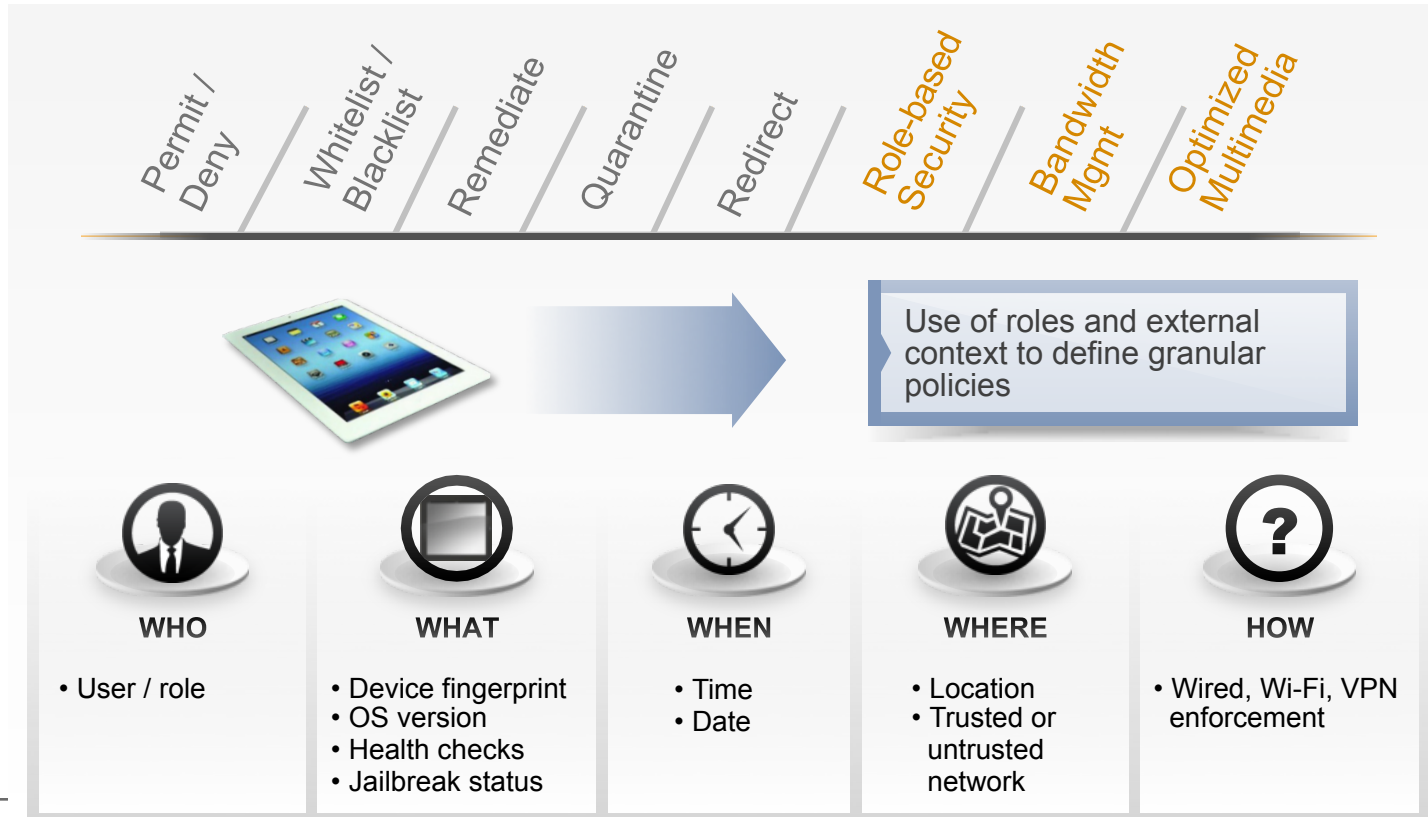
One Platform for All Authentication Needs



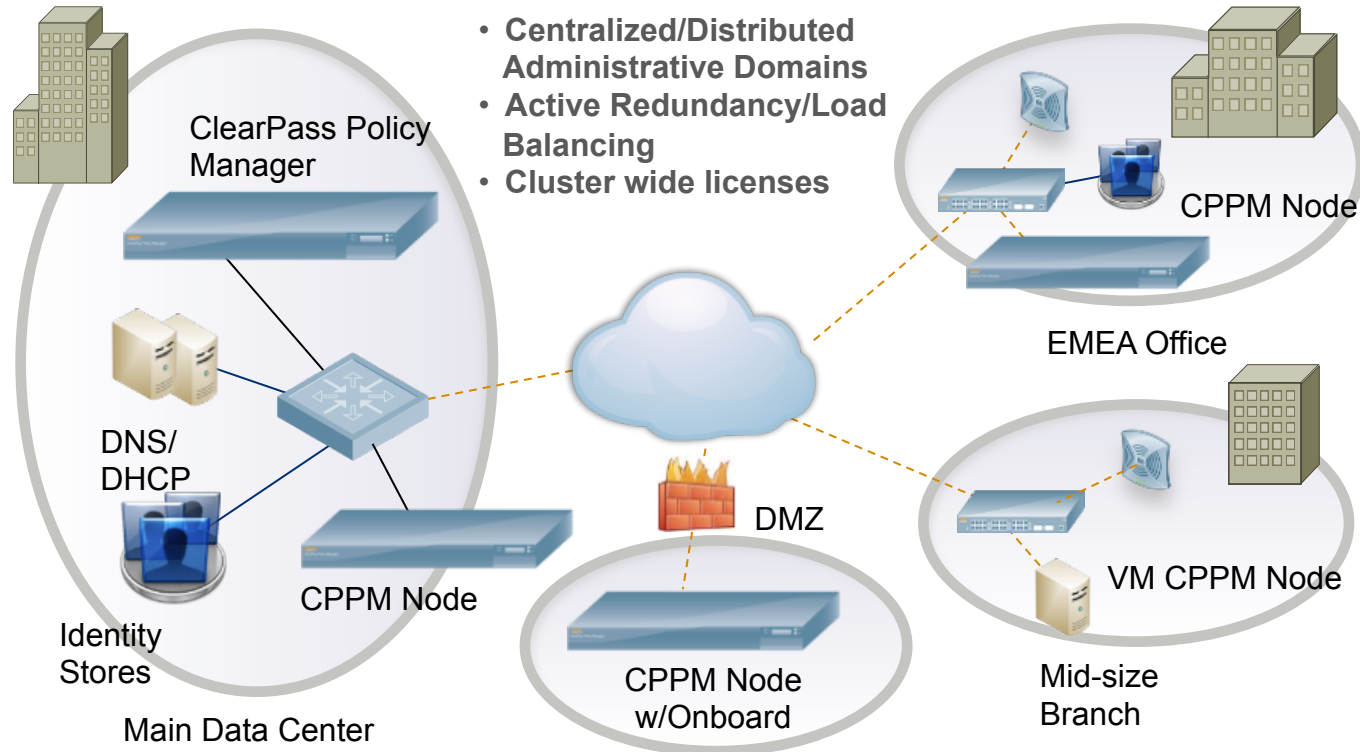
The ClearPass Access Security Platform



Extensible Multivendor Policy Enforcement



Distributed Clustering



Mobility requires a “Policy Manager”

- **Authentication**

- Check user credentials and generate WPA2 key
- RADIUS can do this, but doesn't scale well
- More apps - > SSO for Cloud Apps (RADIUS cannot do this)

- **Authorization**

- Based on WHAT, WHEN, WHERE and HOW
- This info comes from many 3rd party systems
- RADIUS cannot do this at all

- **Accounting**

- Only relevant for Guest account expiration



AirGroup Extends Media Sharing

Zero-touch install of display and print services just got better

What we Support

- UPnP and DLNA sharing
 - Android, Windows & iOS
- Apple AirPlay & AirPrint
- Works across VLANS
- Time & location-based access

ClearPass - User Control

- Self-service portal for sharing
- Context-based privileges
 - Logical groups (teachers)
 - Roles/location



AirPlay



dlna



UPnP

dlna

Aruba AirGroup

**Auditorium
Printer**
*For teacher
only*



Mary's
iPad



Mary's
Friend
Mike



Mary's
MacBook



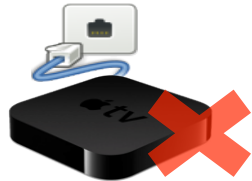
Mary's
Apple TV



Mary's
Friend Jen



**Personal
AirGroup
"Mary"**



**Classroom
Apple TV**

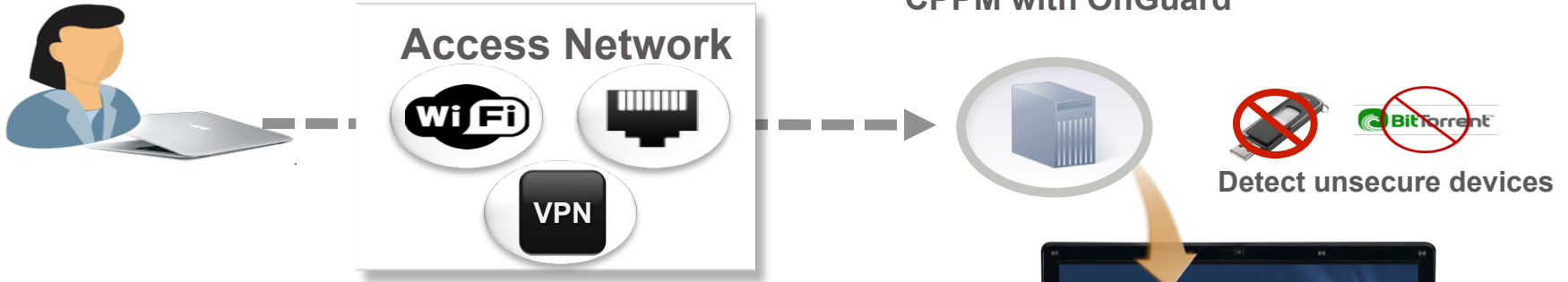
For teachers only

Posture Services

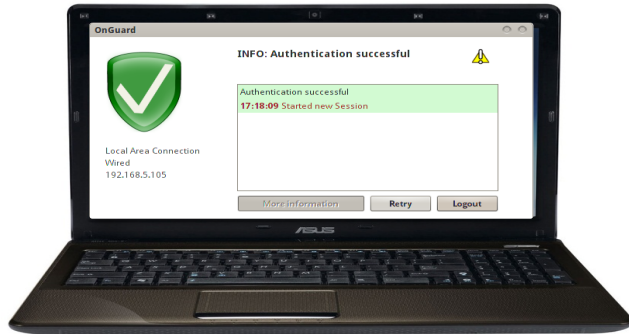


Control Compromised Devices

CPPM with OnGuard



- Minimal Risk to Network



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

AutoRemediation – Patch management

The screenshot displays the 'ClearPass Windows Universal System Health Validator' application. On the left, a sidebar lists various operating systems (Windows Server 2003, Windows XP, Windows Vista, Windows 7, Windows Server 2008, Windows 8) and system components (Services, Processes, Registry Keys, AntiVirus, AntiSpyware, Firewall, Peer To Peer, Patch Management, Windows Hotfixes, USB Devices, Virtual Machines, Network Connections, Disk Encryption, Installed Applications). The 'Windows 7' operating system and 'Patch Management' component are selected. The main panel shows configuration options for Windows 7, including a checked 'Enable checks for Windows 7' box, a checked 'Product-specific checks' box, and a 'Select Patch Management product' dropdown menu. The dropdown menu is open, showing a list of patch management products with 'Altiris Agent' selected. Below the dropdown, there are fields for 'Product Version', 'Status Check', and 'Install Level'. At the bottom of the main panel are 'Save' and 'Cancel' buttons.

ClearPass Windows Universal System Health Validator

Windows Server 2003 ☒ Enable checks for Windows 7

Windows XP

Windows Vista

Windows 7

Windows Server 2008

Windows 8

Services

Processes

Registry Keys

AntiVirus

AntiSpyware

Firewall

Peer To Peer

Patch Management

Windows Hotfixes

USB Devices

Virtual Machines

Network Connections

Disk Encryption

Installed Applications

Quarantine Message

Reset

Windows Server 2003

Windows XP

Windows Vista

Windows 7

Services

Processes

Registry Keys

AntiVirus

AntiSpyware

Firewall

Peer To Peer

Patch Management

Windows Hotfixes

USB Devices

Virtual Machines

Network Connections

Disk Encryption

Product-specific checks ☒ (Uncheck to allow any product)

Select Patch Management product **Altiris Agent**

Product Version

Status Check

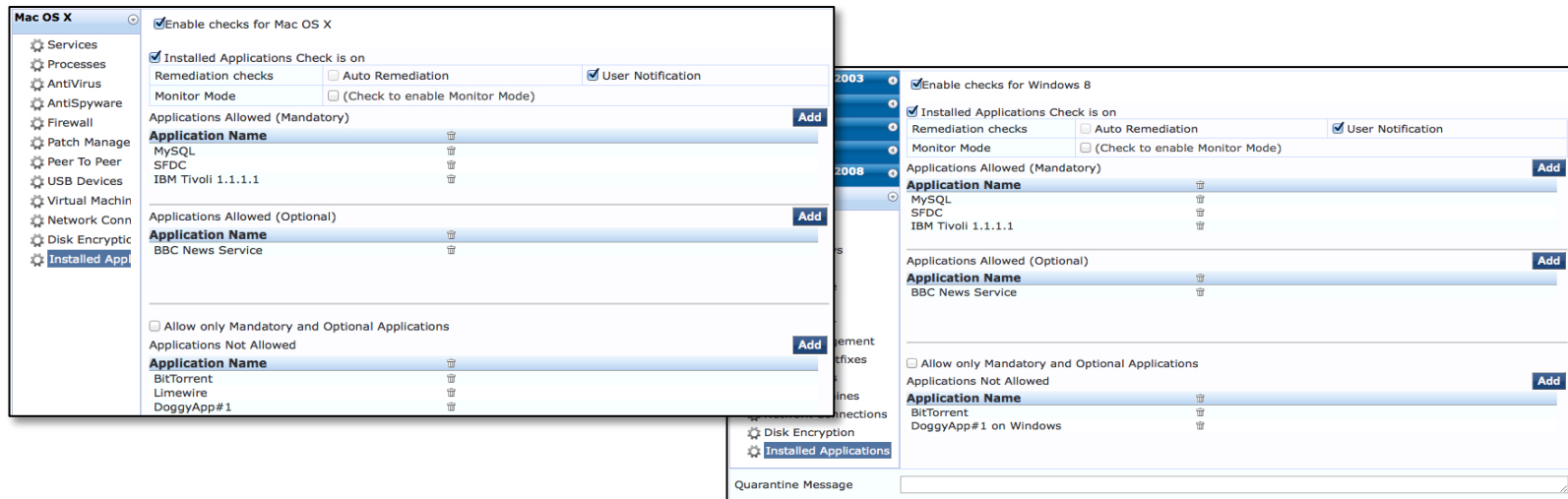
Install Level C

Save **Cancel**

BigFix Enterprise Client
BMC FootPrints Asset Core
Criston Precision
Dell KACE Agent
GFI LANguard
GFI LanGuard 2011
GFI LanGuard 2012
GFI LanGuard 2014
Lumension PatchLink
Microsoft SMS 2003 Advanced Client
Microsoft Windows AutomaticUpdate
Microsoft Windows Update Agent
Norman Patch and Remediation Agent
Secunia CSI
Secunia PSI
Security and Patch Manager
Shavlik NetChk Agent
System Center Configuration Manager
VMware vCenter Protect Agent

Health Classes

OnGuard introduced a new Installed Applications health class on Windows and OS X
An administrator can configure what applications should be present on clients.



Per-Application Posture Tokens

Enforcement Policy rules include Per-Application-Based policies.

- Based on the results of the individual Application Posture Tokens (APT) of the health classes configured in the Internal Posture Policy

Configuration » Posture » Posture Policies » Edit - student

Posture Policies - student

Summary Policy Posture Plugins Rules

Policy:

Policy Name: student

Description:

Posture Agent: Web Agent

Host Operating System: WINDOWS

Restrict by Roles:

Posture Plugins:

The list of selected plugins:

Plugin Name
1. ClearPass Windows Universal System Health Validator

Rules:

Rules Evaluation Algorithm: First applicable

Conditions

1. Passes all SHV checks - ClearPass Windows Universal System Health Validator

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement Rules Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Enforcement Policy Rules:

Conditions

1. (Posture:Applied Policy EQUALS student) AND (Posture:WindowsUniversal:Disk Encryption EQUALS HEALTHY) [RADIUS] [Allow Access Profile]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Posture	Applied Policy	EQUALS	student
2. Posture:WindowsUniversal	Disk Encryption	EQUALS	HEALTHY
3. Click to add...			

Enforcement Profiles

Profile Names:

[RADIUS] [Allow Access Profile]

Move Up Move Down Remove

--Select to Add--

Save Cancel

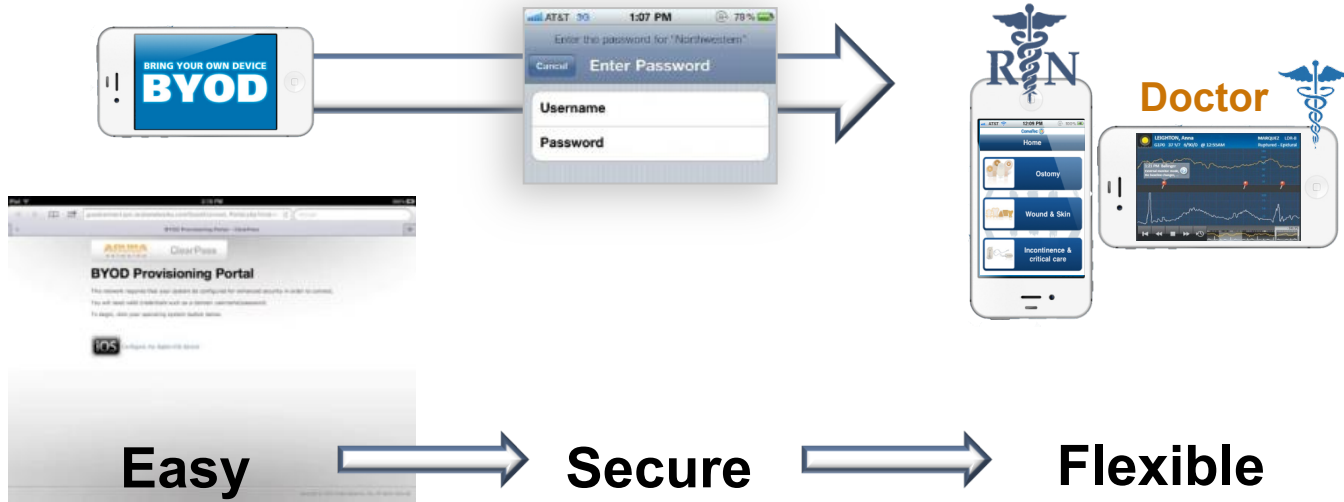
BYOD



Automated Onboarding of Personal Devices

Authentication With Unique Device Certificates

- 1 User's device detected & redirected to portal
- 2 Settings & certificate configured after credentials entered
- 3 Automatically places user on proper network segment



Built in CA for BYOD

225 employee14 230

View certificate Export certificate Revoke certificate Delete

Certificate Information

Certificate Details

Details about the certificate and its owner.

Issued To: **employee14**

Valid From: Wednesday, 08 February 2012, 05:37 PM

Valid To: Thursday, 07 February 2013, 06:07 PM

Subject:

- Country: US
- State: California
- Locality: Sunnyvale
- Organization: Aruba Networks PoC Lab
- Common Name: employee14
- mdpsDeviceType: vista
- mdpsMacAddress: 00:24:D7:AE:C6:B8

Issuer Details

Details about the certificate authority that issued the certificate.

Issued By: **POC Local Certificate Authority (Signing)**

Issuer:

- Country: US
- State: California
- Locality: Sunnyvale
- Organization: Aruba Networks
- Common Name: POC Local Certificate Authority (Signing)
- Email Address: info@poc.arubanetworks.com

Advanced

Technical information about the certificate.

Fingerprint: d4f7 b7d6 8f16 4e8b c4dc 239c f2b2 c7fa 42a3 ef11
This is the SHA-1 "fingerprint" or "thumbprint" of the certificate

Private Key: 1024-bit RSA
The type of the private key for this certificate.

Cancel

Revoke Device
Network Access

Built in CA

224 employee5 229

View certificate Export certificate Revoke certificate Delete

Certificate Information

Certificate Details

Details about the certificate and its owner.

Issued To: **employee5**

Valid From: Wednesday, 08 February 2012, 05:32 PM

Valid To: Thursday, 07 February 2013, 06:02 PM

Subject:

- Country: US
- State: California
- Locality: Sunnyvale
- Organization: Aruba Networks PoC Lab
- Common Name: employee5
- mdpsDeviceType: Android
- mdpsDeviceImei: 355182040365790
- mdpsMacAddress: 60:A1:0A:17:C1:6F
- mdpsProductName: SGH-T849

Issuer Details

Details about the certificate authority that issued the certificate.

Issued By: **POC Local Certificate Authority (Signing)**

Issuer:

- Country: US
- State: California
- Locality: Sunnyvale
- Organization: Aruba Networks
- Common Name: POC Local Certificate Authority (Signing)
- Email Address: info@poc.arubanetworks.com

Advanced

Technical information

Fingerprint: e234 e...
This is the SHA-1 "fingerprint" or "thumbprint" of the certificate

Private Key: 1024-bit RSA
The type of the private key for this certificate.

Certificate Authority Trust Chain

Imported certificate(s) for use as Onboard CA.

arubatrainning-REMOTELABSERVER-CA (self-signed)
Show certificate
ClearPass Onboard Local Certificate Authority
Aruba Networks Show certificate

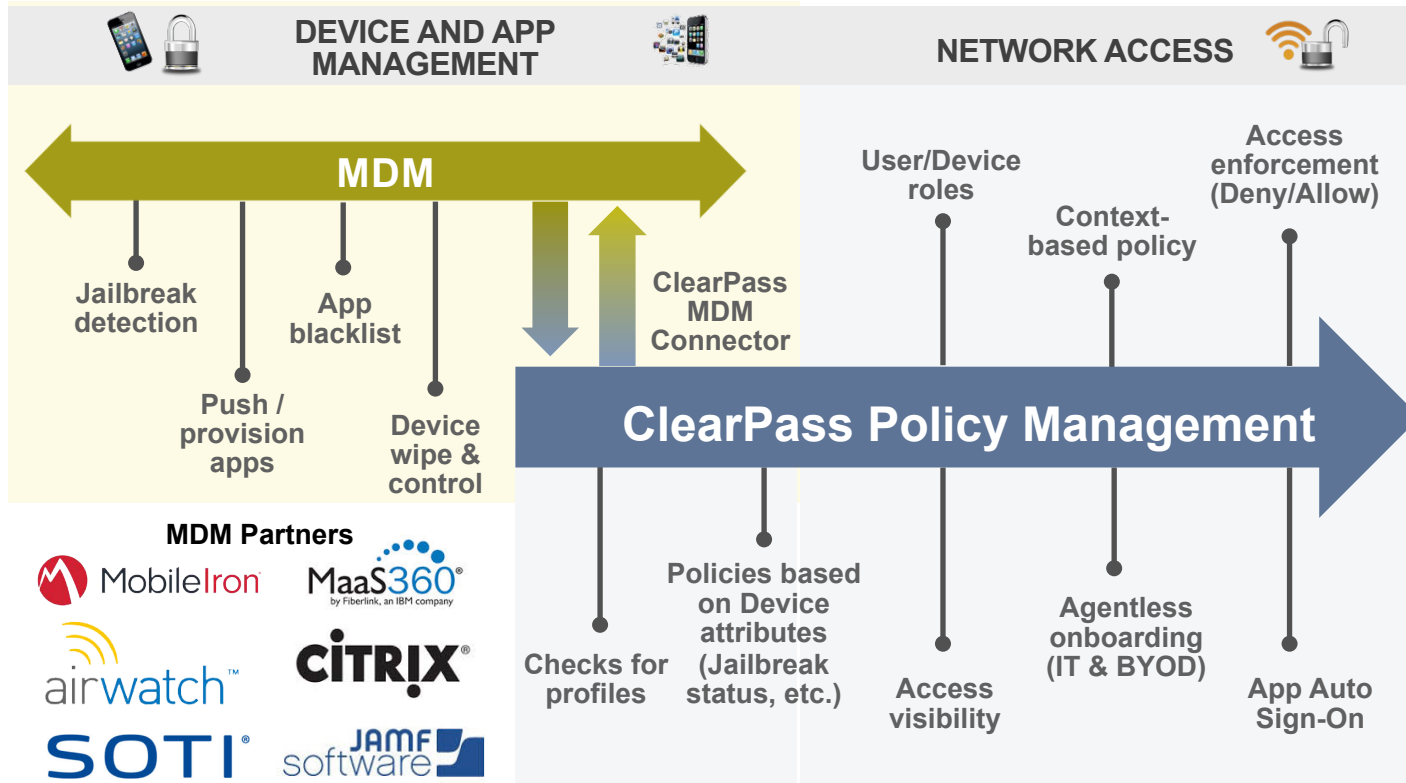
Device Inventory
Data

Filter: cggallego Clear Filter

Filtered by: Filtering Common Name, Serial Number, Type, Valid From, Valid To using 'cggallego'

Common Name	Serial Number	Type	Valid From	Valid To
cggallego	36	tls-client	2012-06-15 21:45:30+00	2013-06-15 22:15:30+00
View certificate	Export certificate	Revoke certificate	Delete certificate	
cggallego	45	tls-client	2012-06-15 22:51:25+00	2013-06-15 23:21:25+00

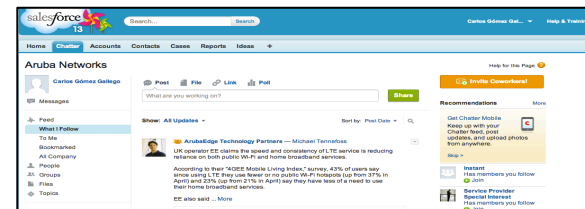
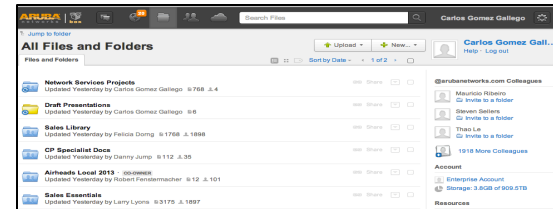
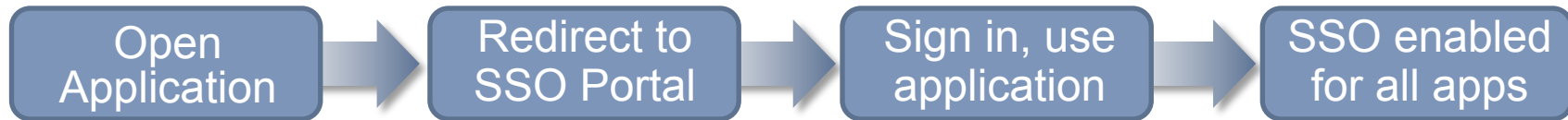
Extending MDM with Network Policy



APP SIGN ON



SSO for Cloud Applications

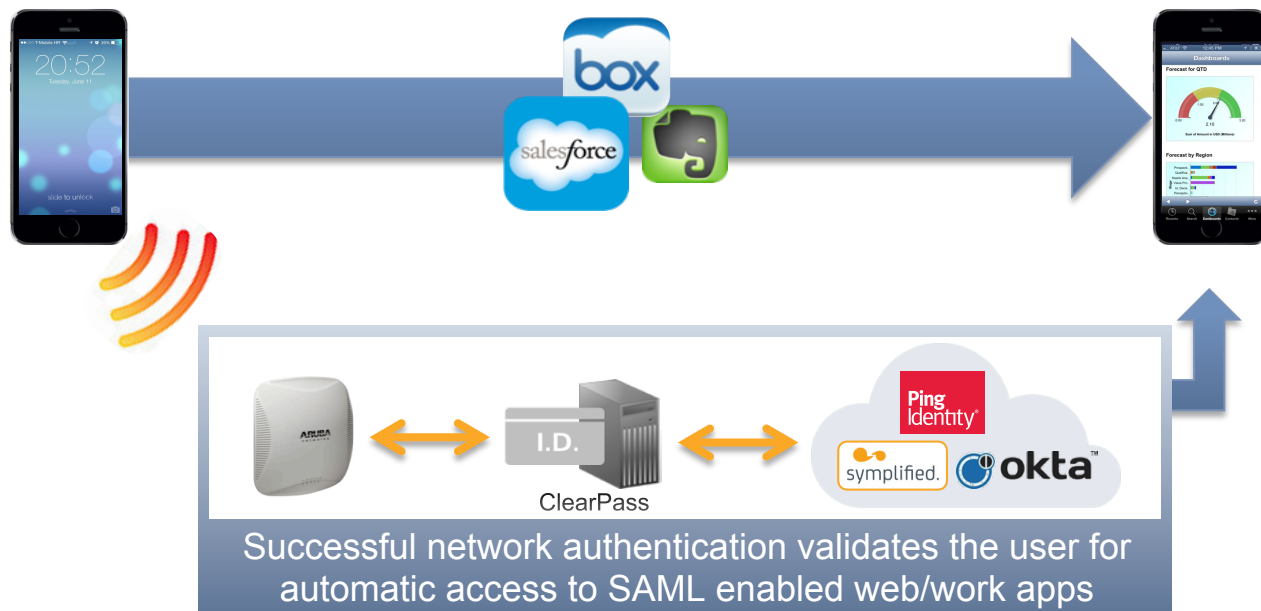


Auto Sign On to Work Apps

1. Authenticate to Wi-Fi

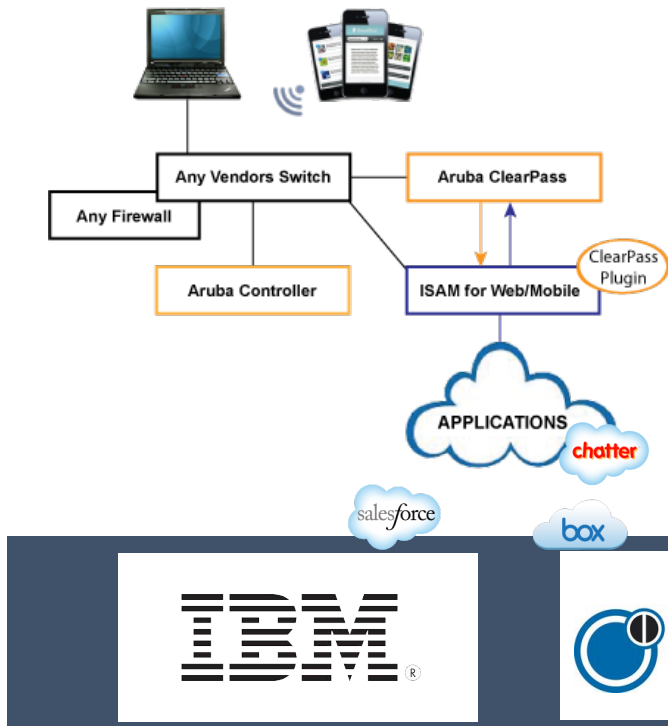
2. Open a work app

3. Start working



Auto Sign-On with Partners

Only Aruba lets you sign-in once & you're good to go



- One login for all web/mobile apps
 - Uses valid network login
- NO App logins
- IBM, Okta, Ping
- ClearPass as Provider (IdP)
 - Uses SAML, not RADIUS

Guest Access



Secure Guest Access



The image shows a digital registration form for Aruba Networks' ClearPass Guest system. The form is titled 'Welcome to Aruba Networks Visitor Self-Registration'. It includes fields for 'Sponsor's Name', 'Your Name', 'Company Name', 'Email Address', and 'Phone Number'. Below these fields is a 'Terms and Conditions' section with a checkbox and a 'REGISTER' button. The background of the form features a blurred image of two people in a professional setting.

aruba
NETWORKS

ClearPass Guest

Welcome to Aruba Networks

Visitor Self-Registration

* Sponsor's Name: Please enter the name of the person you are visiting.

* Your Name: Please enter your full name.

* Company Name: Please enter your company name.

* Email Address: Please enter your email address. This will become your username to log into the network.

Phone Number: Please enter your contact phone number. An SMS with your credentials will be sent to you.

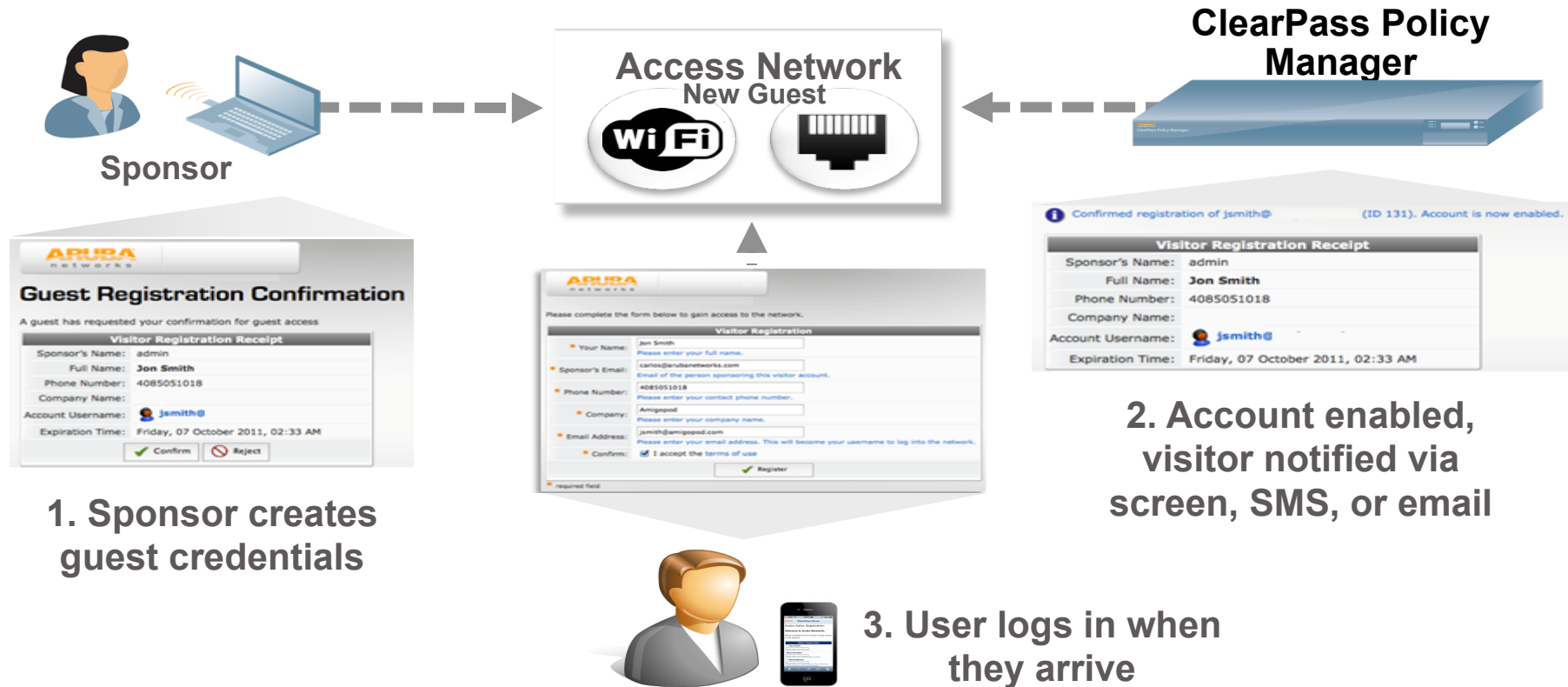
☐ Terms and Conditions

Welcome to Aruba. We expect that during your visit and in the course of your discussions with Aruba personnel you will learn some proprietary information about our company. Aruba is only willing to disclose this information to you if you agree to keep it completely confidential and that you refrain from sharing anything you learn about Aruba to anyone without Aruba's express permission. This may include, but is not limited to, information about Aruba's product development plans, details about Aruba's future prospects and any financially-related information. To confirm your understanding and acceptance of this policy please click the Register button below.

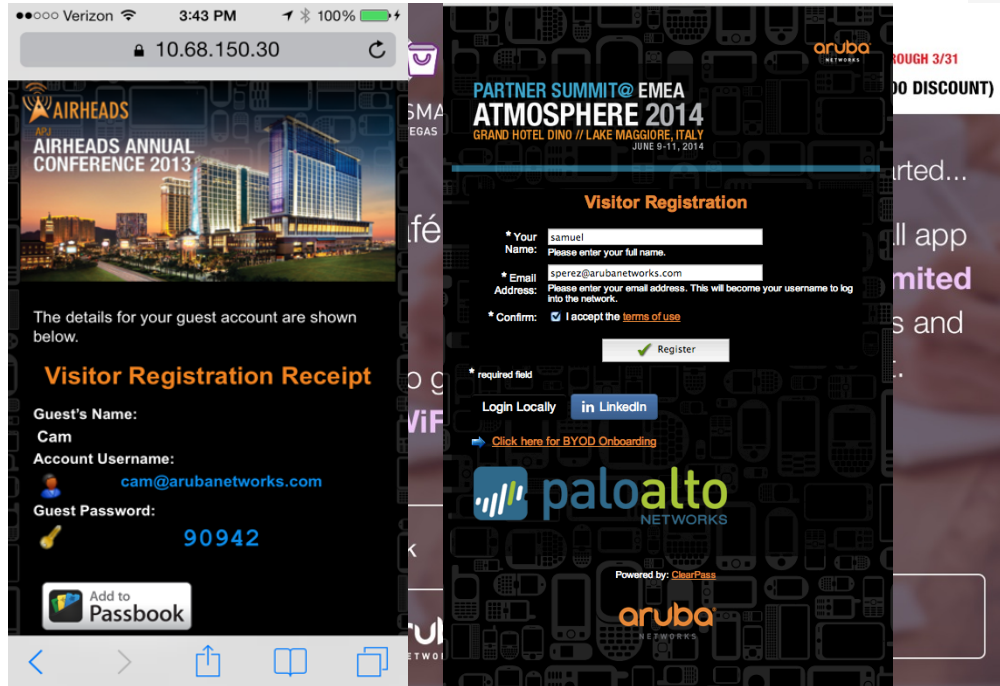
REGISTER

- **Customizable branding and data entry fields**
 - No IT involvement
 - Automated SMS/email credential delivery
 - Sponsor privileges with access verification
 - Per session controls
 - Cached login access

Automated guest Onboarding



Customer engagement



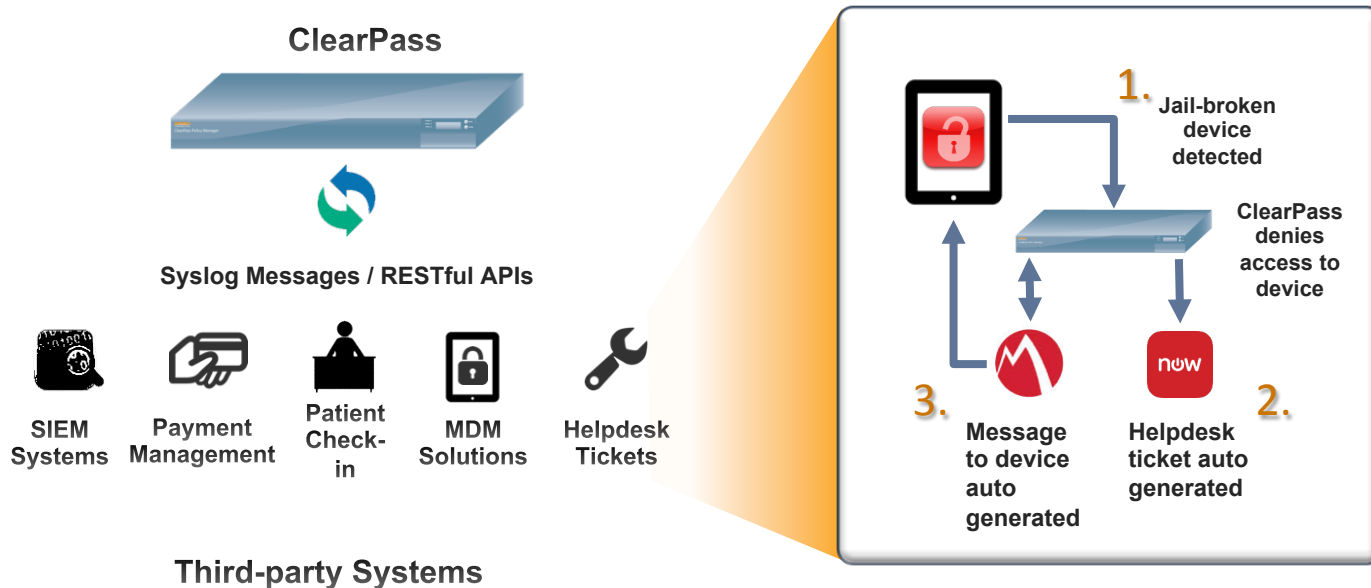
- **Passbook integration**
 - Credential, agenda delivery
- **Context driven ads**
 - Images, videos
- **Social media login**
 - “Like” for Internet Access
- **Full customer engagement**

Clearpass Exchange



ClearPass Exchange

Two-way Third-Party Integration



ClearPass and Palo Alto Networks

Aruba & ClearPass



Mobility Defined Network

Core AAA, NAC
Device Profiling
Guest + BYOD



Context:

- Exchange rich endpoint context
- Trigger real-time, intelligent network policies
- Extendable architecture

Palo Alto Networks



Next Generation Firewall

L7+ Application FW
Content Security
Threat Protection

Clearpass – Palo Alto Integration

Feed User-ID Data

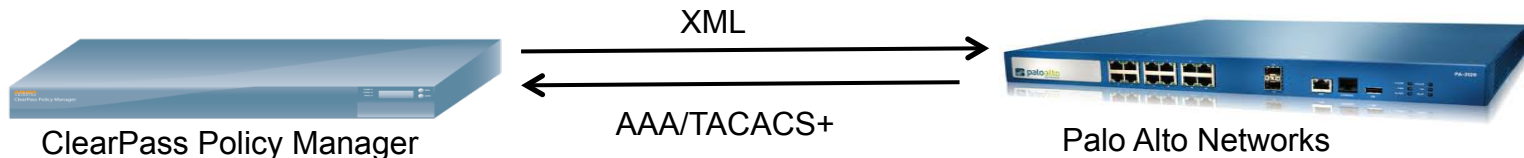
- Centralized Username to IP address mapping
- No software agents required, support multiple identity stores
- Rich visibility and reporting for compliance

Endpoint/Device Context

- Feed device context to PAN eg. iPad, Android Phone
- Enable policy enforcement based on new device context
- Extensible schema allows adding more context to endpoint data

Centralized Identity Store

- FW admin authentication using Radius, TACACS+
- Provide services for VPN authentication



AOS Palo Alto Integration



- **Upon successful authentication or COA, controller sends PAN devices**
- IP Address, User Name, Device Type
- **PAN populates their policy DB with this information**
- **Uses PAN's RESTful XML API, requires PAN OS 5.0 or later**

Configuring CPPM

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

 Add Context Server
 Import Context Servers
 Export Context Servers

Filter: contains Show records

#	<input type="checkbox"/> Server Name ▲	Server Type
1.	<input type="checkbox"/> 10.2.100.10	Palo Alto Networks Firewall

Showing 1-1 of 1

Modify Endpoint Context Server

Server Name:	<input type="text" value="10.2.100.10"/>
Server Type:	Palo Alto Networks Firewall
Server Base URL:	<input type="text" value="https://{server_ip}/api/?type=keygen&user={username}&password={password}"/>
Username:	<input type="text" value="cppmadmin"/>
Password:	<input type="password" value="....."/>
Verify Password:	<input type="password" value="....."/>
UserID Post URL	<input type="text" value="https://{server_ip}/api/?type=user-id&action=set&key={key}&cmd={cmd}"/>

- Add multiple PAN firewalls to CPPM
- Add Panorama which will send updates to all PAN firewalls

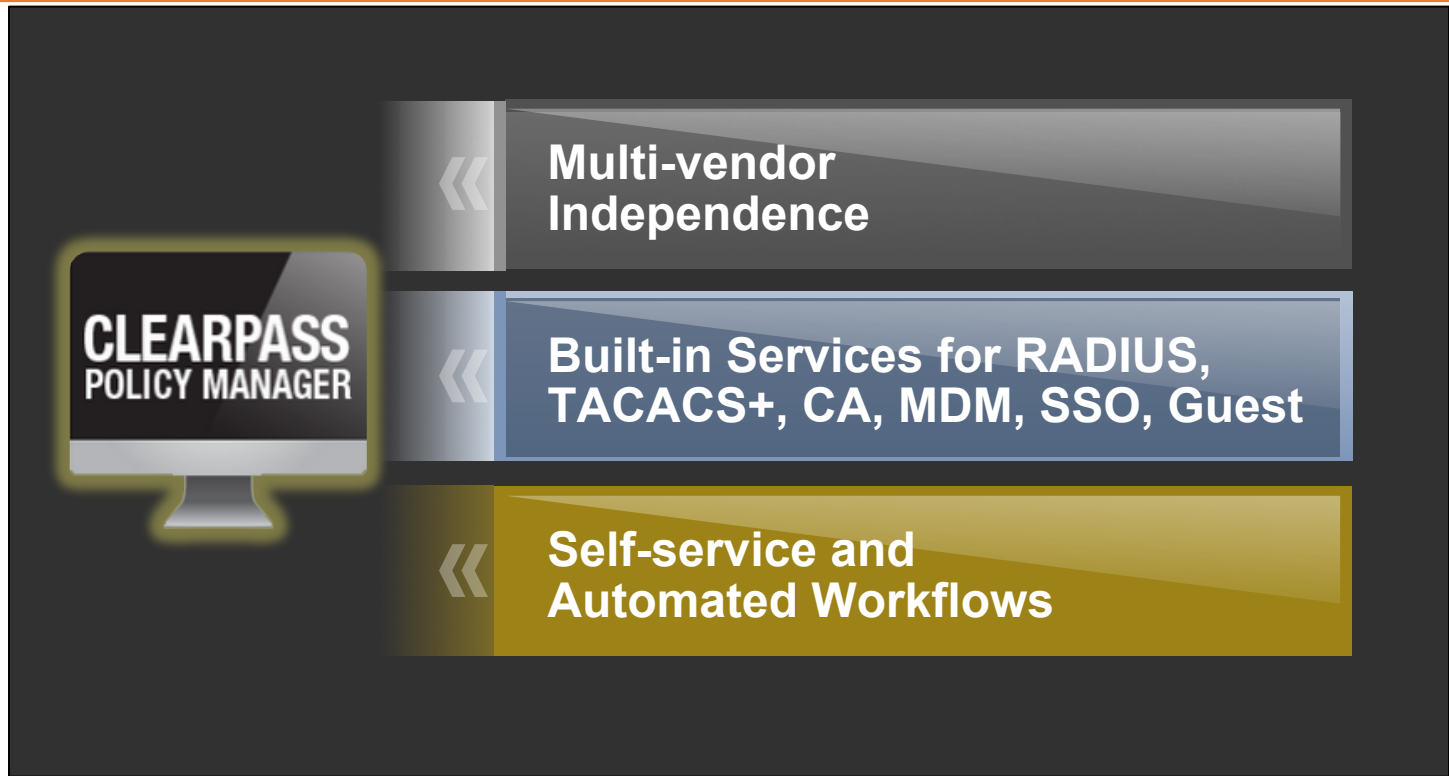
Using device type to apply policy

Manual													Help
(user.src eq marc) and (addr.src in 10.2.101.165)													
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes	
	03/12 17:57:03	end	trust	untrust	10.2.101.165	marc	216.74.41.14	80	web-browsing	allow	allow	1.2 K	
	03/12 17:56:45	end	trust	untrust	10.2.101.165	marc	216.74.41.14	80	web-browsing	allow	allow	1.5 K	
	03/12 17:54:03	end	trust	untrust	10.2.101.165	marc	54.235.161.76	443	ssl	allow	allow	24.3 K	
	03/12 17:53:36	end	trust	untrust	10.2.101.165	marc	10.1.8.200	443	incomplete	allow	Allow_FB_Android	148	
	03/12 17:53:35	end	trust	untrust	10.2.101.165	marc	10.1.8.200	443	incomplete	allow	Allow_FB_Android	148	
	03/12 17:53:35	end	trust	untrust	10.2.101.165	marc	10.1.8.200	443	incomplete	allow	Allow_FB_Android	148	
	03/12 17:53:35	end	trust	untrust	10.2.101.165	marc	10.1.8.200	443	incomplete	allow	Allow_FB_Android	148	
	03/12 17:52:33	end	trust	untrust	10.2.101.165	marc	54.235.161.76	443	ssl	allow	allow	24.3 K	

Manual													Help
(user.src eq marc) and (addr.src in 10.2.101.163)													
	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes	
	03/12 17:19:59	end	trust	untrust	10.2.101.163	marc	74.125.224.37	80	incomplete	allow	allow	432	
	03/12 17:19:59	end	trust	untrust	10.2.101.163	marc	74.125.224.59	80	incomplete	allow	allow	432	
	03/12 17:19:49	end	trust	untrust	10.2.101.163	marc	10.1.1.50	53	dns	allow	allow	244	
	03/12 17:19:49	end	trust	untrust	10.2.101.163	marc	173.223.232.153	443	incomplete	allow	allow	432	
	03/12 17:19:49	end	trust	untrust	10.2.101.163	marc	10.1.1.50	53	dns	allow	allow	228	
	03/12 17:19:09	deny	trust	untrust	10.2.101.163	marc	69.171.237.20	443	facebook-base	deny	Block_FB_Corporate	437	
	03/12 17:18:44	end	trust	untrust	10.2.101.163	marc	74.125.224.32	80	youtube-base	allow	allow	34.5 K	

- User 'marc' with BYOD device = Allow Facebook
- User 'marc' with corporate device = Deny Facebook

The ClearPass Difference



THANK YOU

Samuel Pérez – SE Aruba Iberia
sperez@arubanetworks.com