Secure Mobility Access

Aruba ClearPass

Evolving IT Landscape

IT CENTRIC		USER CENTRIC, SELF SERVICE
		
Fixed Environment	→	Work from Anywhere
Wired Network	→	Wired, Wi-Fi, Cellular
Windows	→	Multiple Platforms
IT Selected	→	Selection of devices & apps
Slow Refresh	→	User Timeframes

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

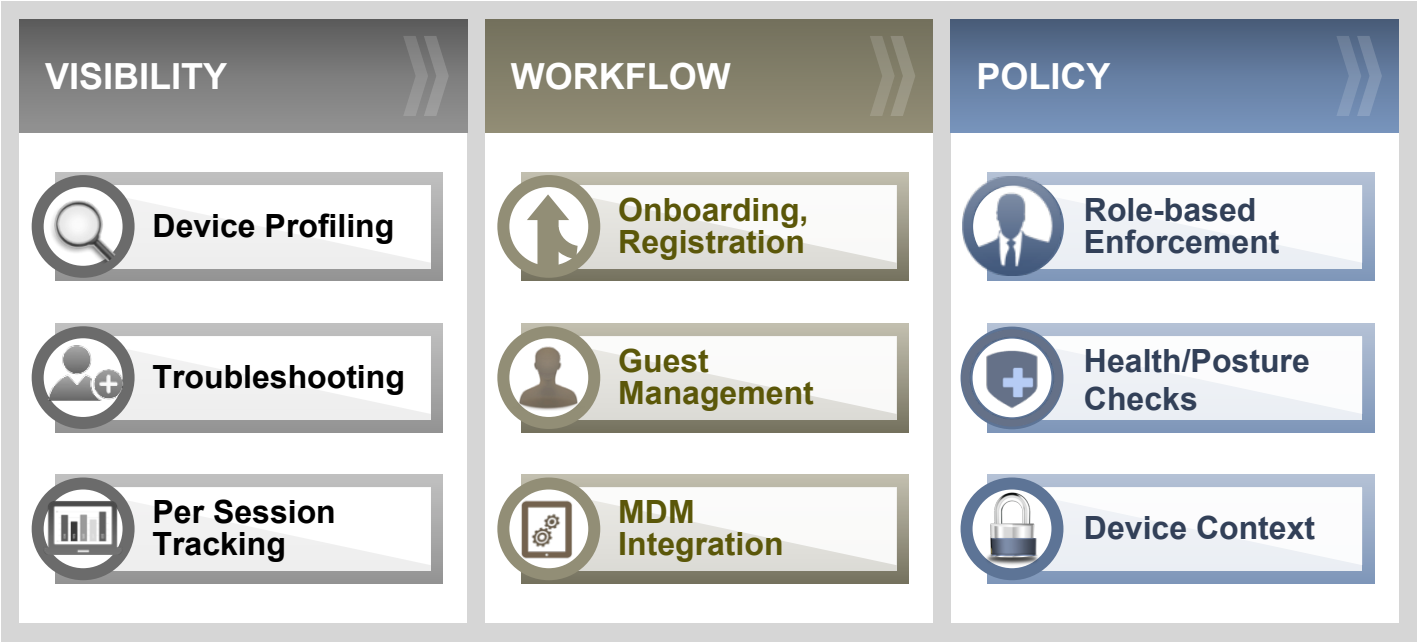
DEVICES
BYOD, Onboarding, MDM

APPs
Use, Distribution, Control

Multiple solutions, increase IT touch points and errors

The ClearPass Solution

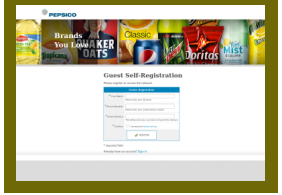
All Things Network, Device and App Management



Use Cases Customers Are Fixing

Old AAA Solutions

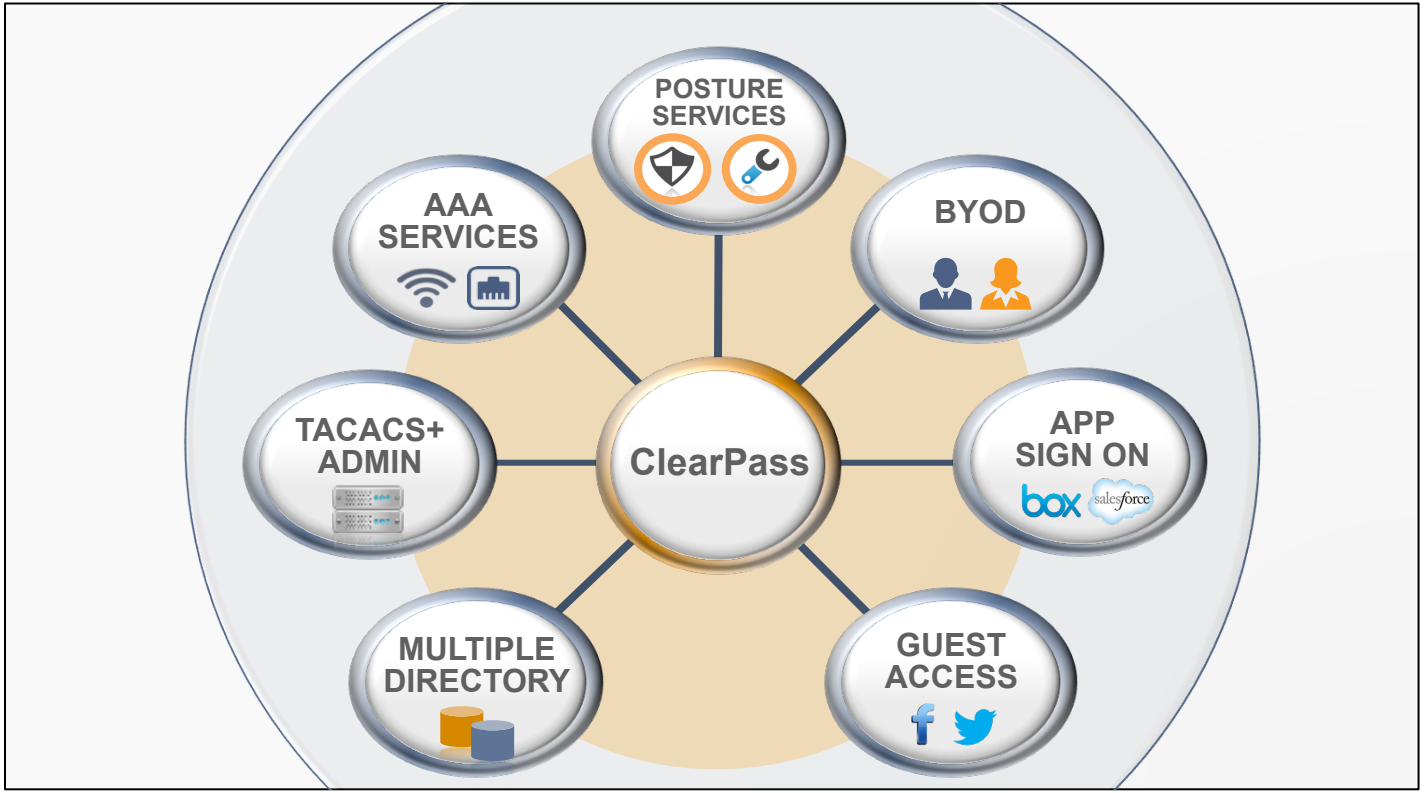
AAA REPLACEMENT: Others lack integrated RADIUS & TACACS+, multivendor support, built-in profiling and ease of management!



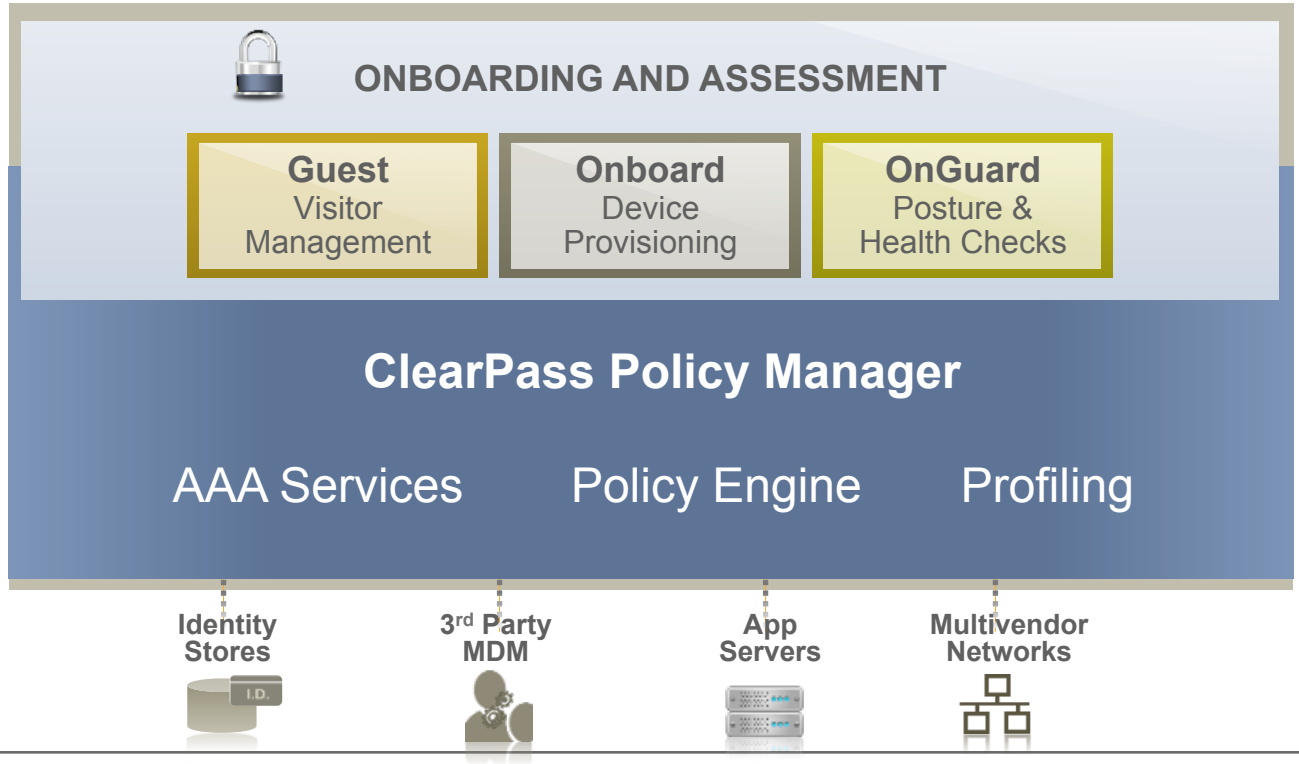
GUEST ACCESS: ClearPass works in multivendor networks, scales and makes the customer brand look good!

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

Permit / Deny

Whitelist / Blacklist

Remediate

Quarantine

Redirect

Role-based Security

Bandwidth Mgmt

Optimized Multimedia

Use of roles and external context to define granular policies

WHO

- User / role

WHAT

- Device fingerprint
- OS version
- Health checks
- Jailbreak status

WHEN

- Time
- Date

WHERE

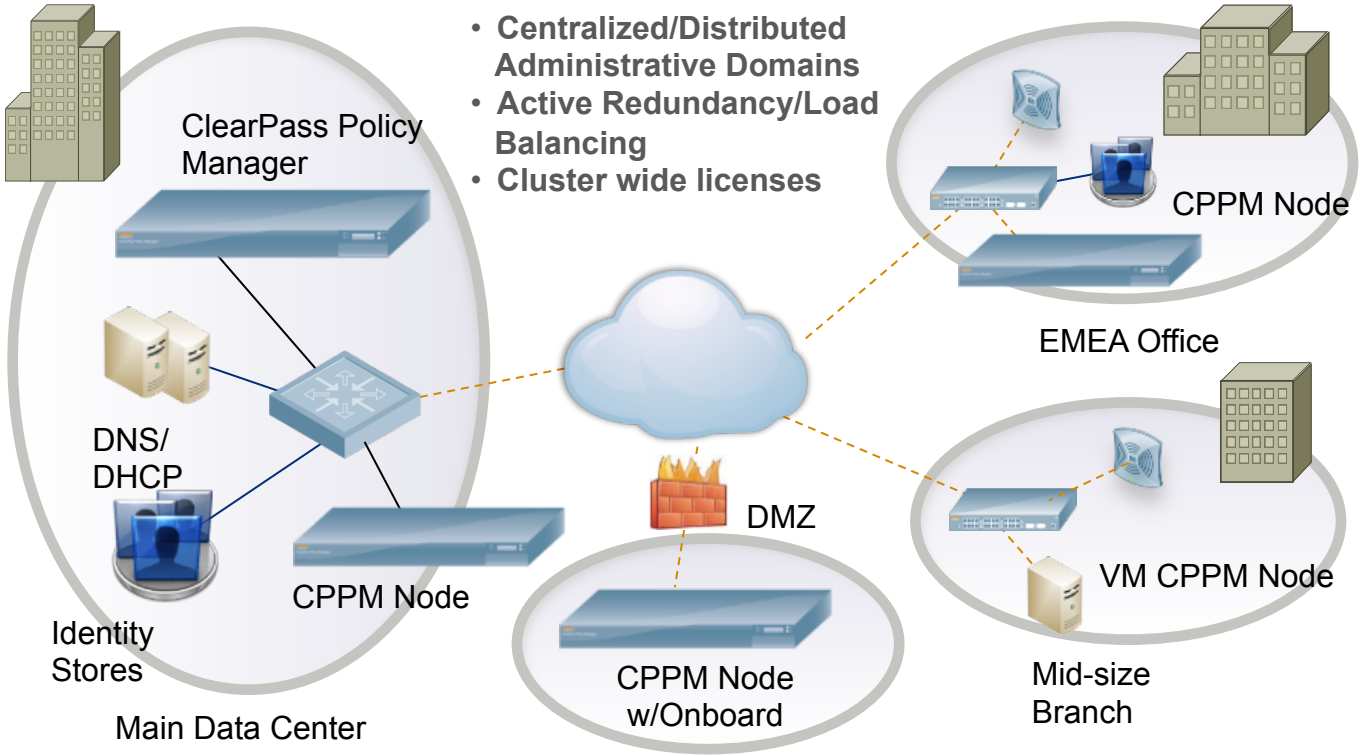
- Location
- Trusted or untrusted network

HOW

- Wired, Wi-Fi, VPN enforcement

aruba NETWORKS

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

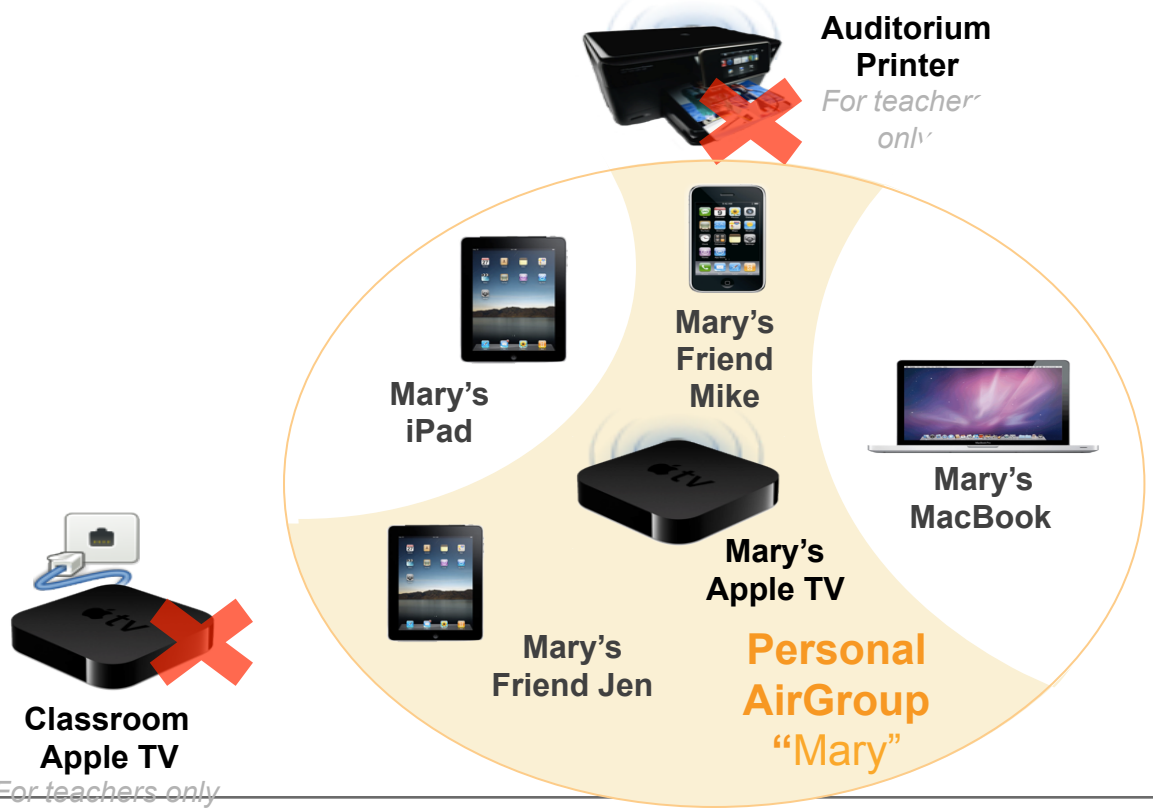
ClearPass - User Control

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

AirPlay AirPrint UPnP dlna

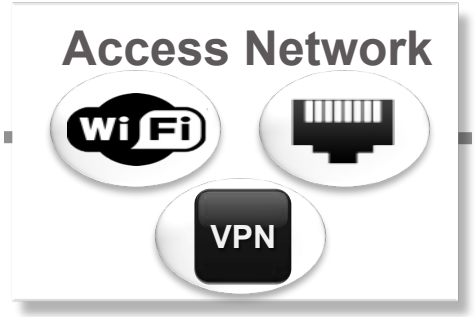
aruba NETWORKS

Aruba AirGroup



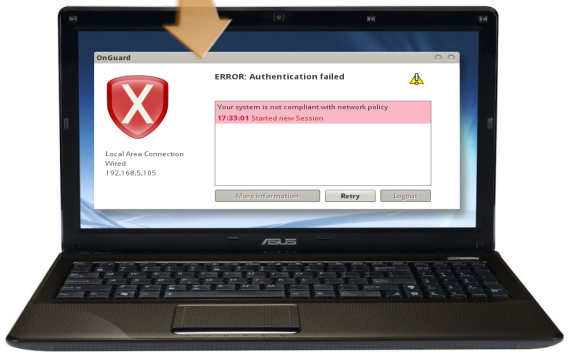
Posture Services

Control Compromised Devices

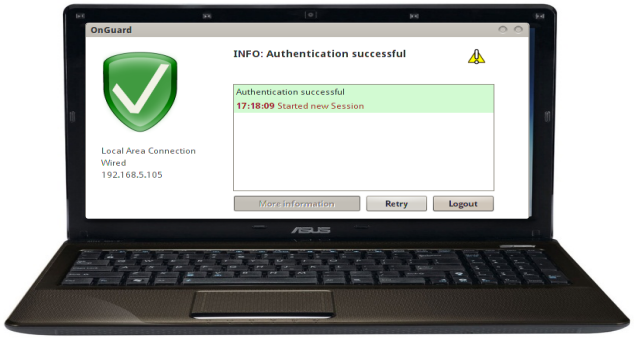


CPPM with OnGuard

Detect unsecure devices

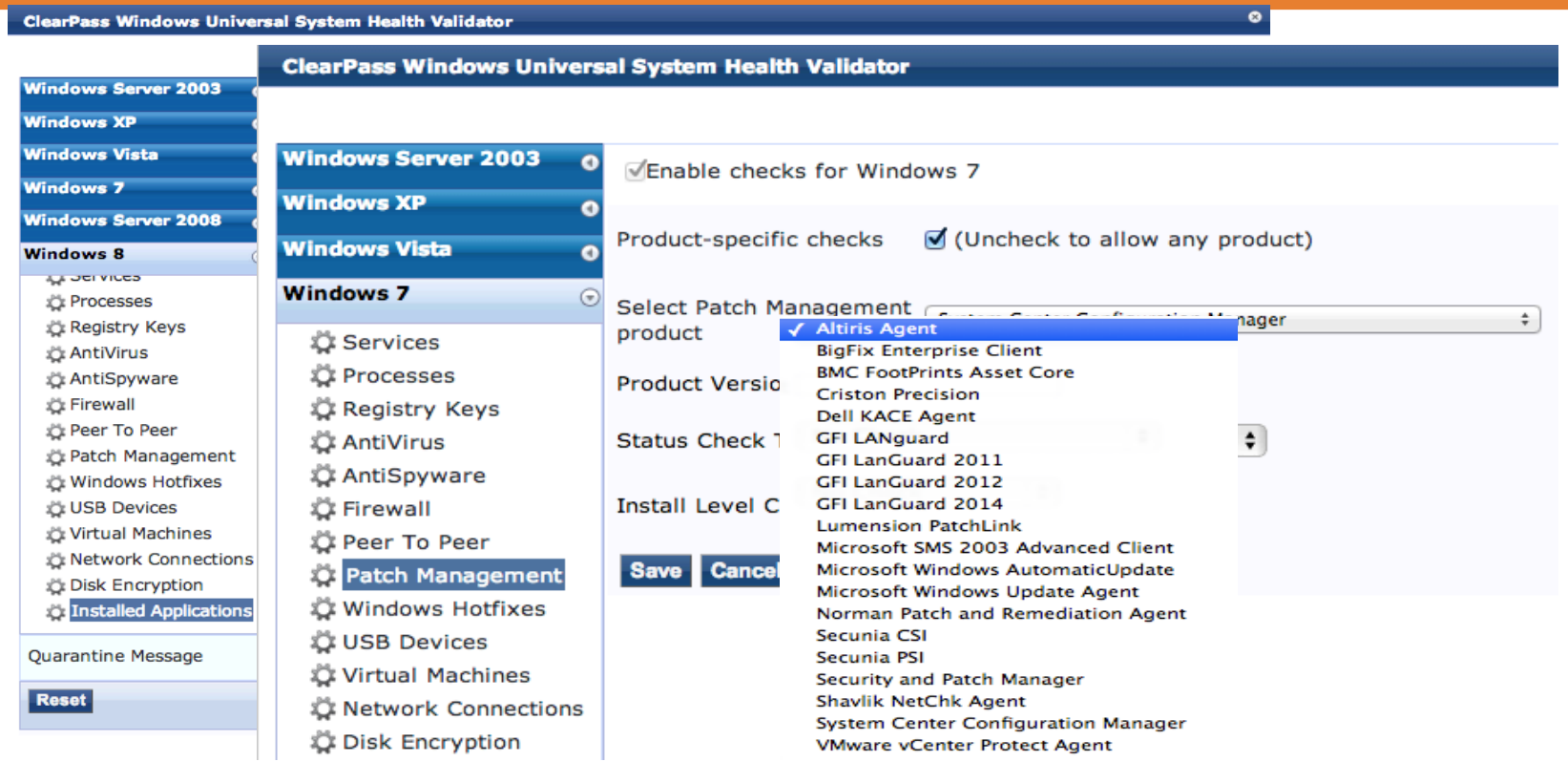


- Minimal Risk to Network



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

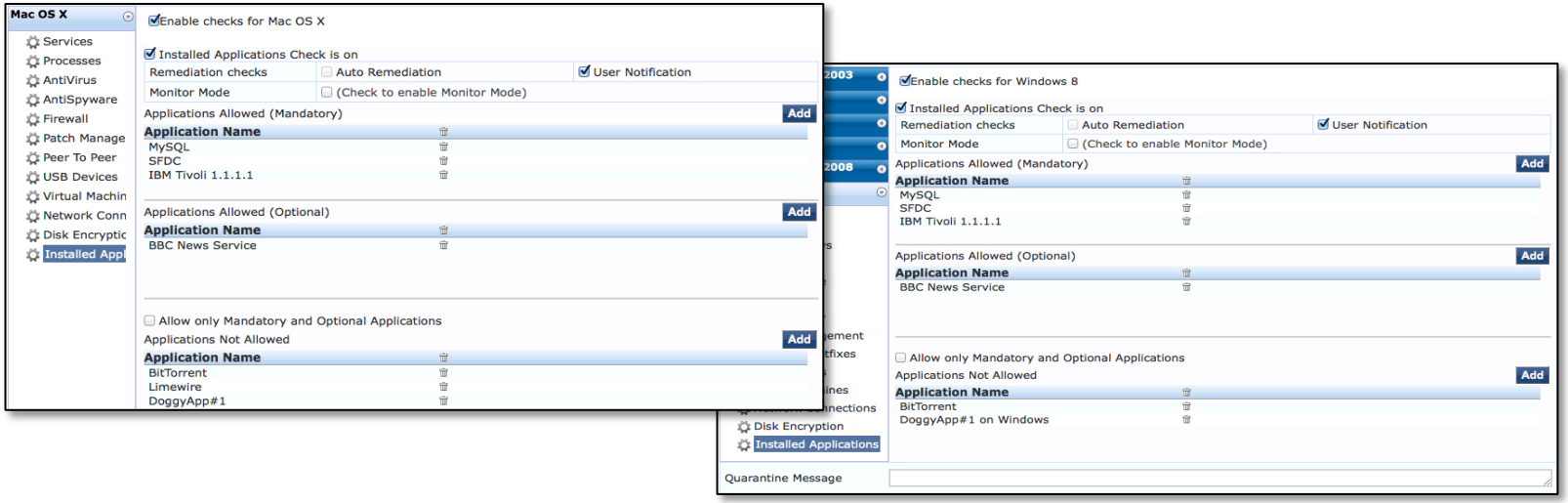
AutoRemediation – Patch management



Health Classes

OnGuard introduced a new Installed Applications health class on Windows and OS X

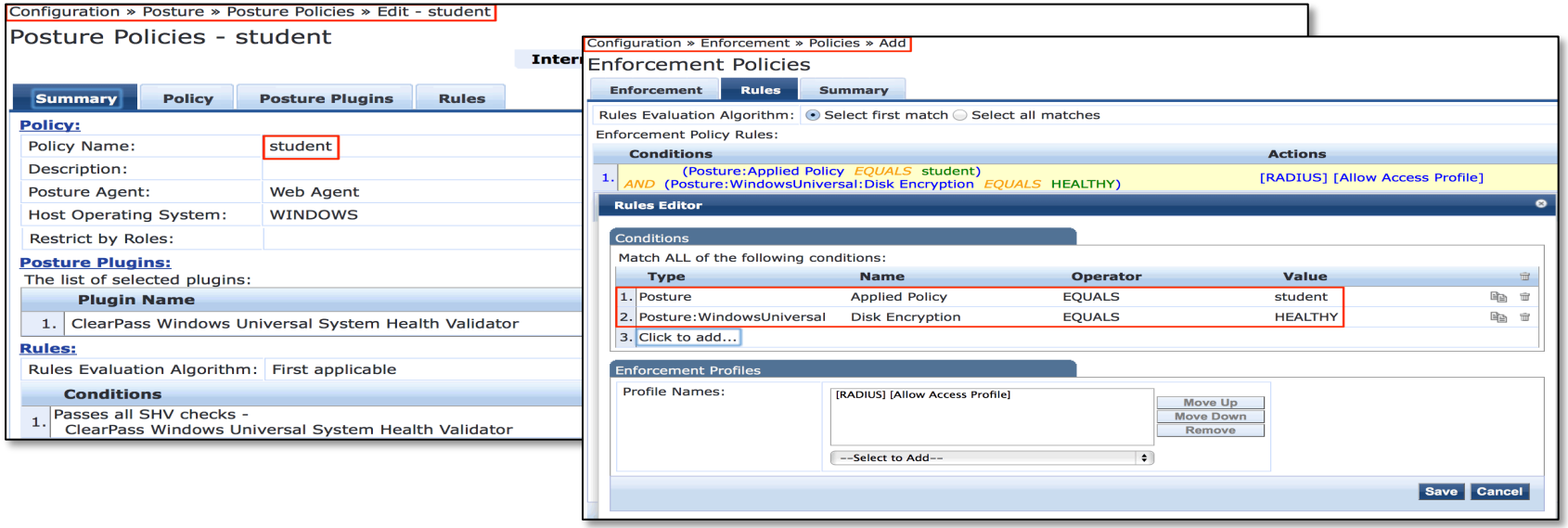
An administrator can configure what applications should be present on clients.



Per-Application Posture Tokens

Enforcement Policy rules include Per-Application-Based policies.

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



BYOD

Automated Onboarding of Personal Devices

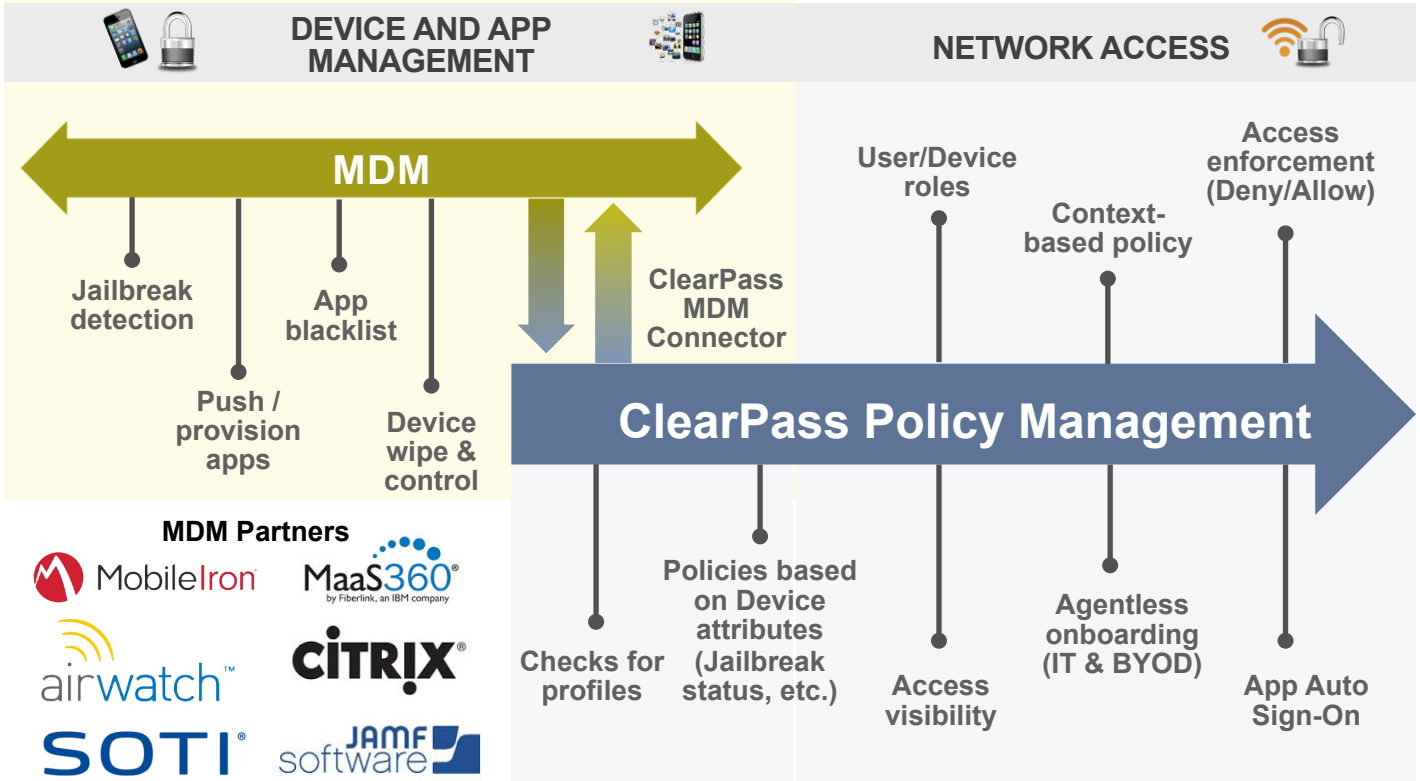
Authentication With Unique Device Certificates

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

Easy → **Secure** → **Flexible**

Built in CA for BYOD

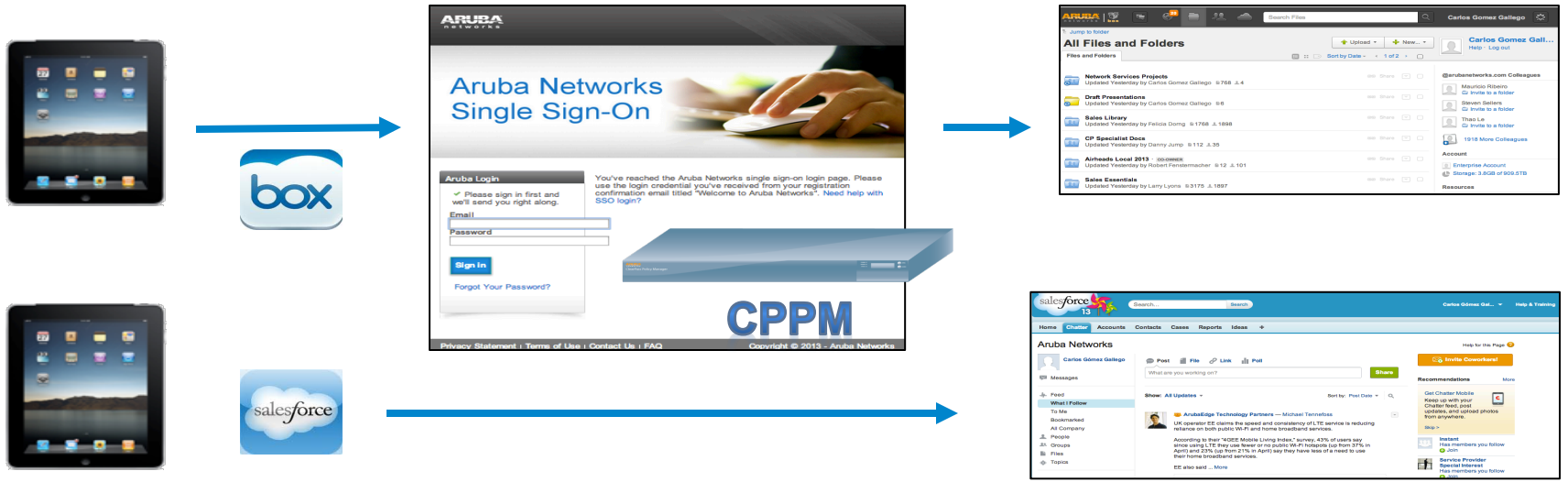
Extending MDM with Network Policy



APP SIGN ON

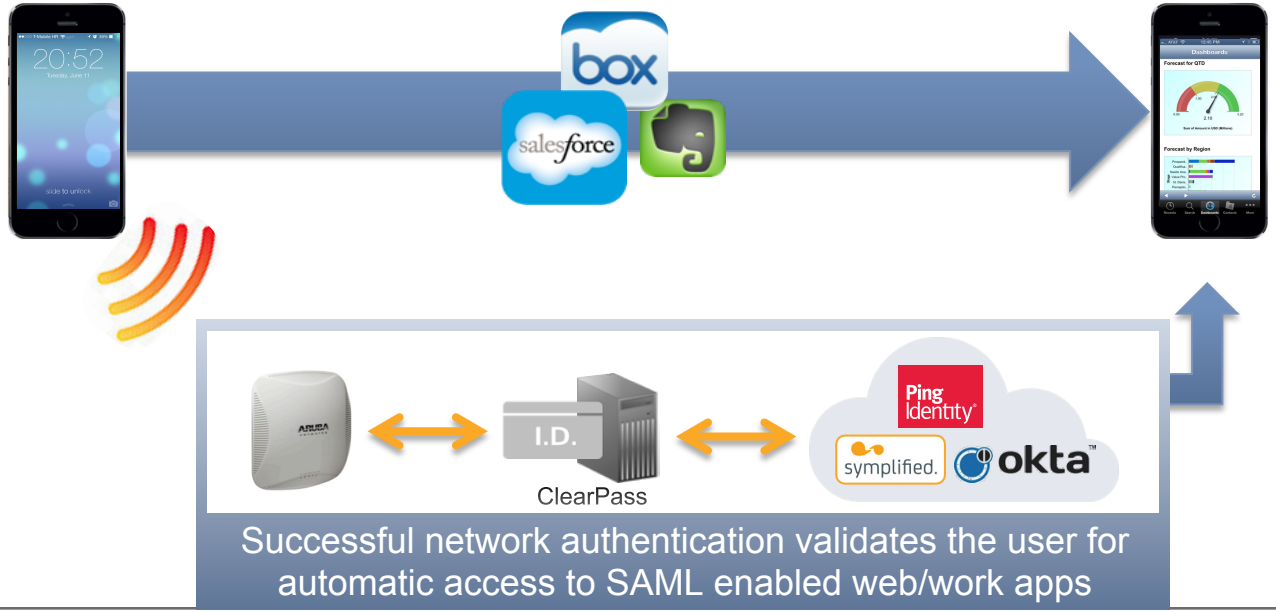
SSO for Cloud Applications

Open Application → Redirect to SSO Portal → Sign in, use application → SSO enabled for all apps



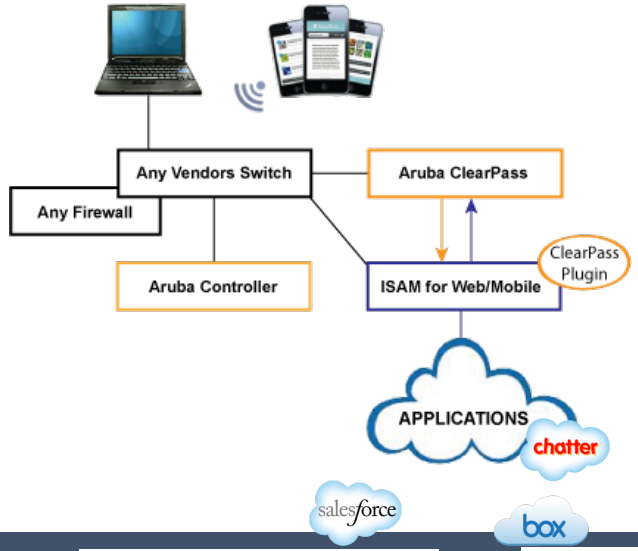
Auto Sign On to Work Apps

1. Authenticate to Wi-Fi
2. Open a work app
3. Start working



Auto Sign-On with Partners

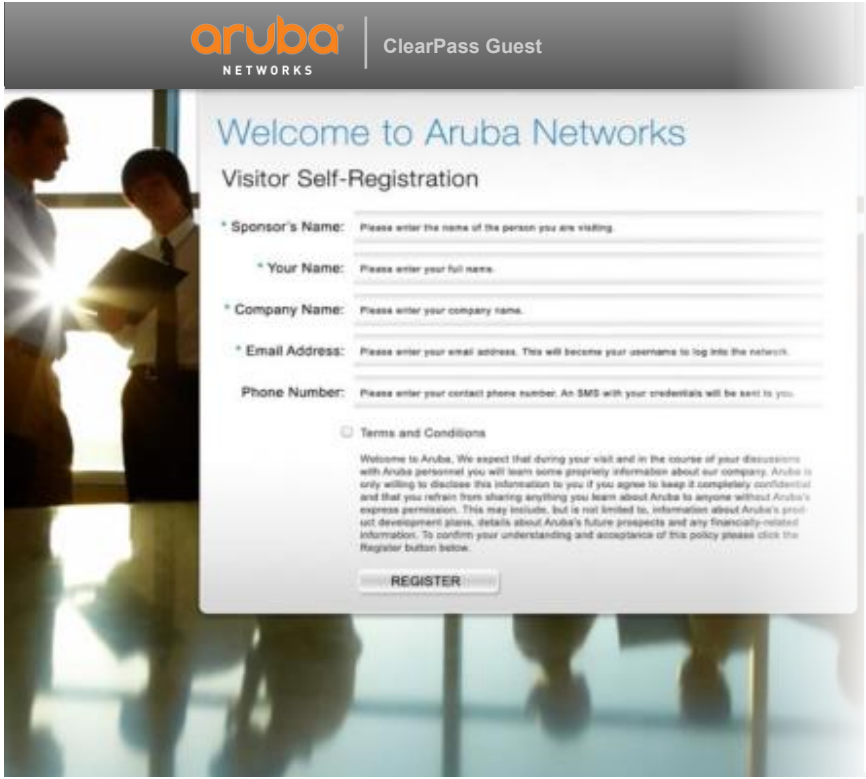
Only Aruba lets you sign-in once & you're good to go



- 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

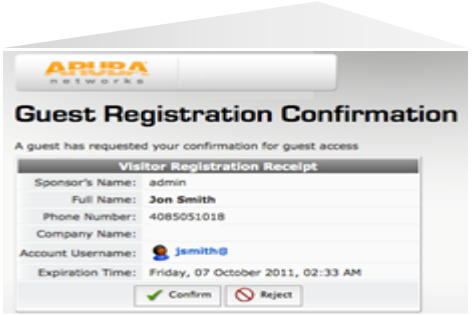


- **Customizable branding and data entry fields**
  - No IT involvement
  - Automated SMS/email credential delivery
  - Sponsor privileges with access verification
  - Per session controls
  - Cached login access

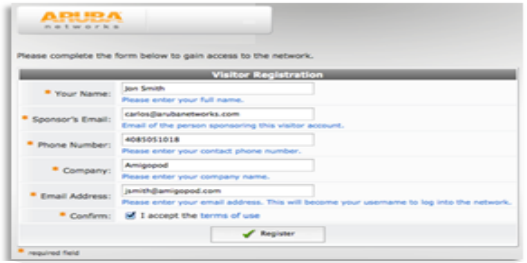
Automated guest Onboarding

Sponsor

ClearPass Policy Manager



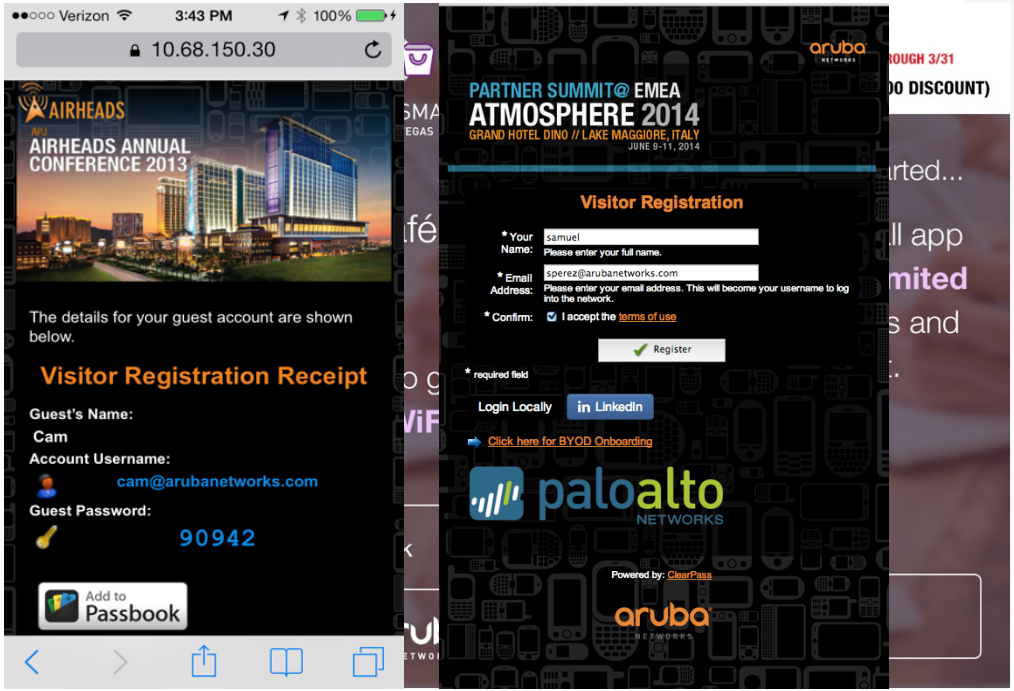
1. Sponsor creates guest credentials



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

3. User logs in when they arrive

Customer engagement

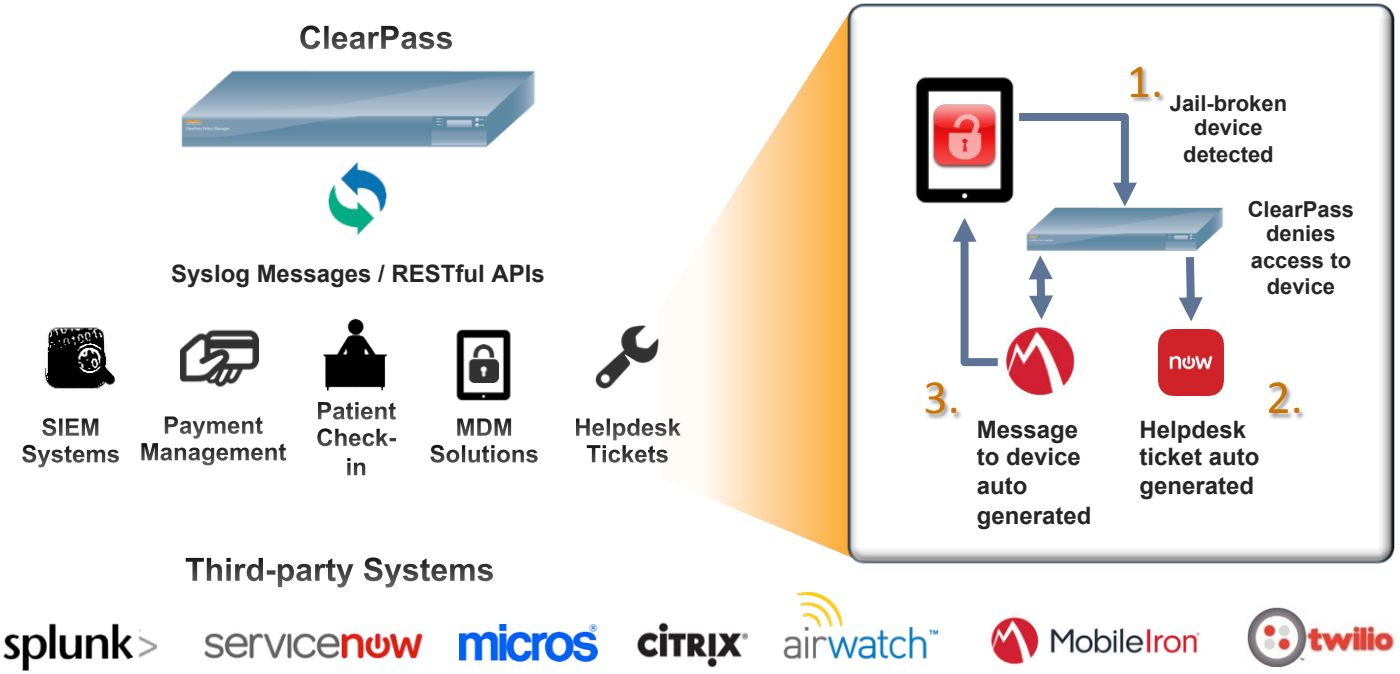


- **Passbook integration**
  - Credential, agenda delivery
- **Context driven ads**
  - Images, videos
- **Social media login**
  - "Like" for Internet Access
- **Full customer engagement**

Clearpass Exchange

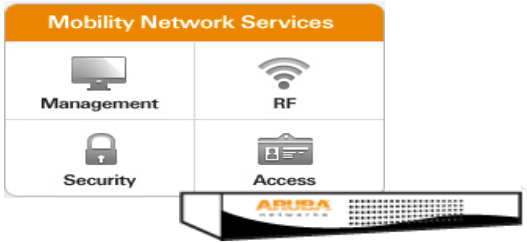
ClearPass Exchange

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

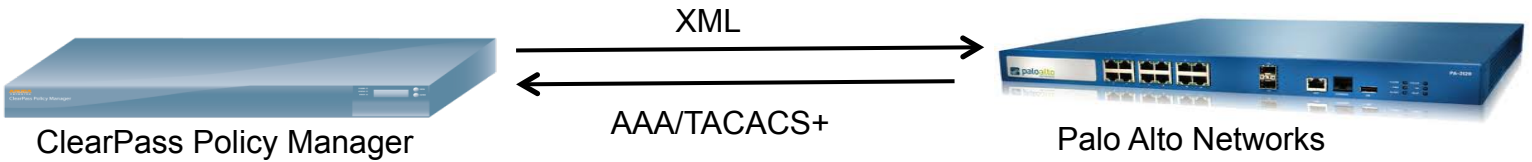
- Centralized Username to IP address mapping
- No software agents required, support multiple identity stores
- Rich visibility and reporting for compliance

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

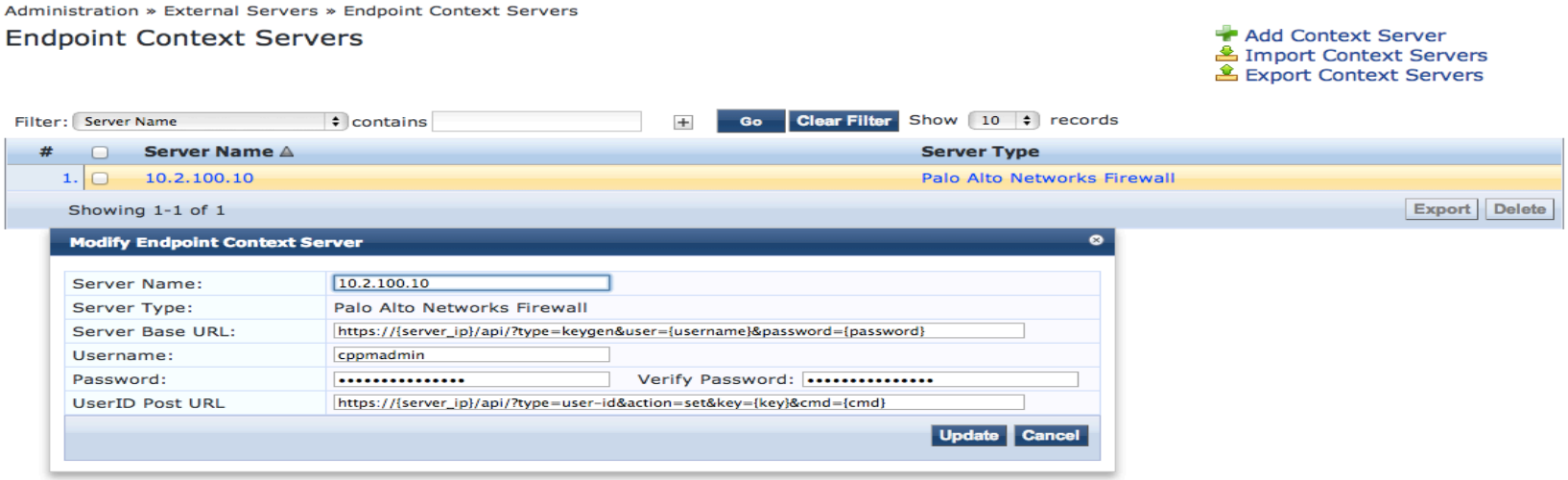
- FW admin authentication using Radius, TACACS+
- Provide services for VPN authentication



AOS Palo Alto Integration

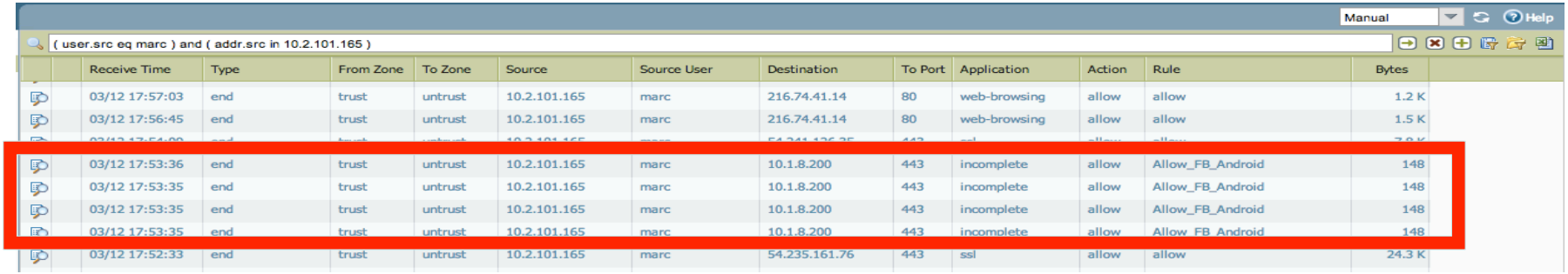
- **Upon successful authentication or COA, controller sends PAN devices**
  - IP Address, User Name, Device Type
- **PAN populates their policy DB with this information**
- **Uses PAN's RESTful XML API, requires PAN OS 5.0 or later**

Configuring CPPM

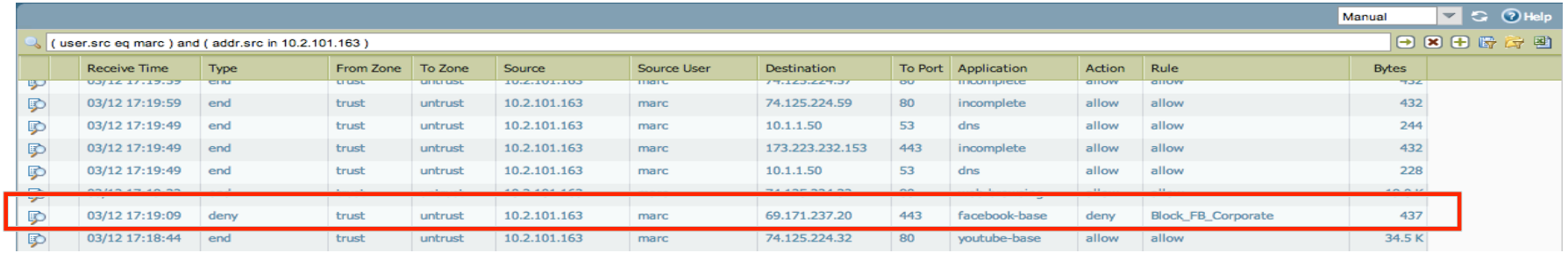


- Add multiple PAN firewalls to CPPM
- Add Panorama which will send updates to all PAN firewalls

Using device type to apply policy



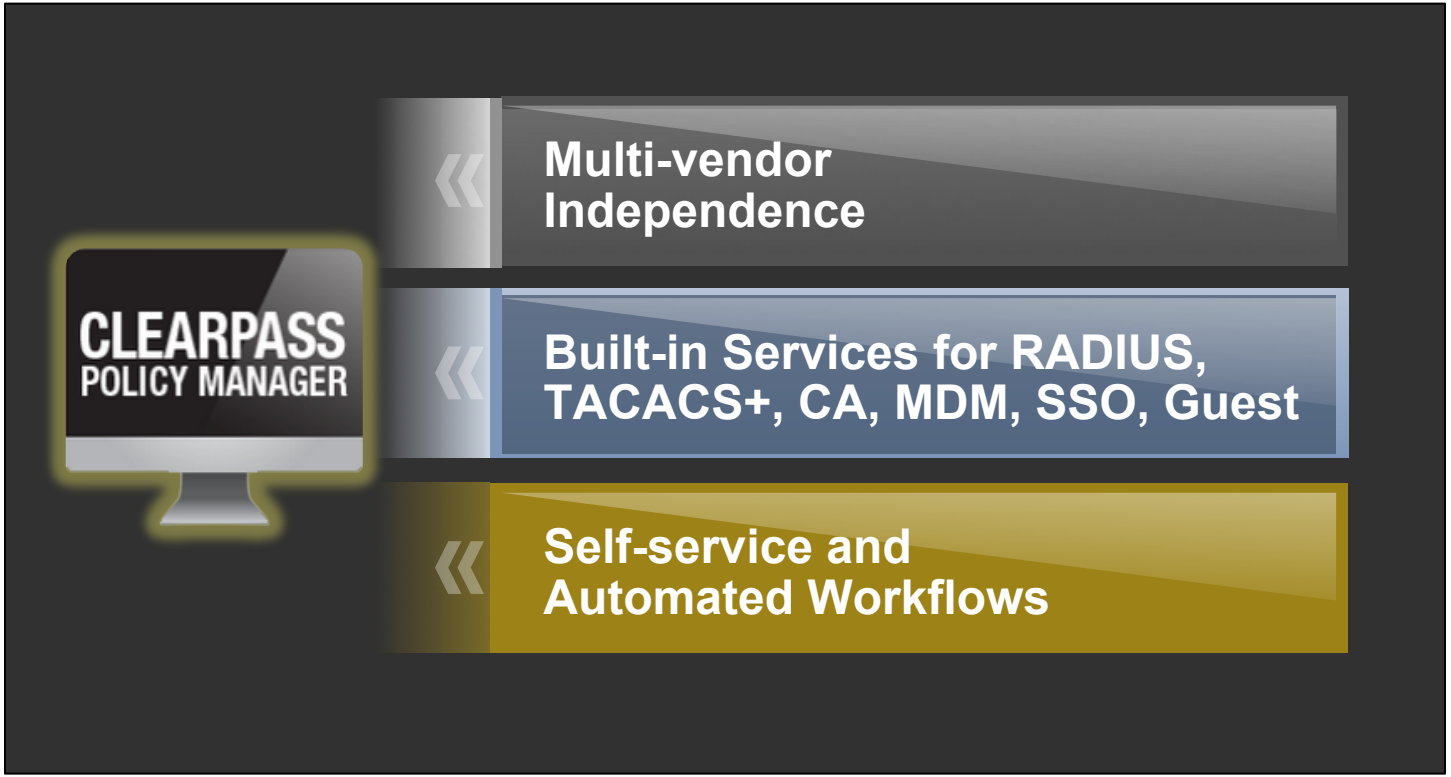
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
03/12 17:57:03	end	trust	untrust	10.2.101.165	marc	216.74.41.14	80	web-browsing	allow	allow	1.2 K
03/12 17:56:45	end	trust	untrust	10.2.101.165	marc	216.74.41.14	80	web-browsing	allow	allow	1.5 K
03/12 17:53:36	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



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	74.125.224.59	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