prolink. solving IT

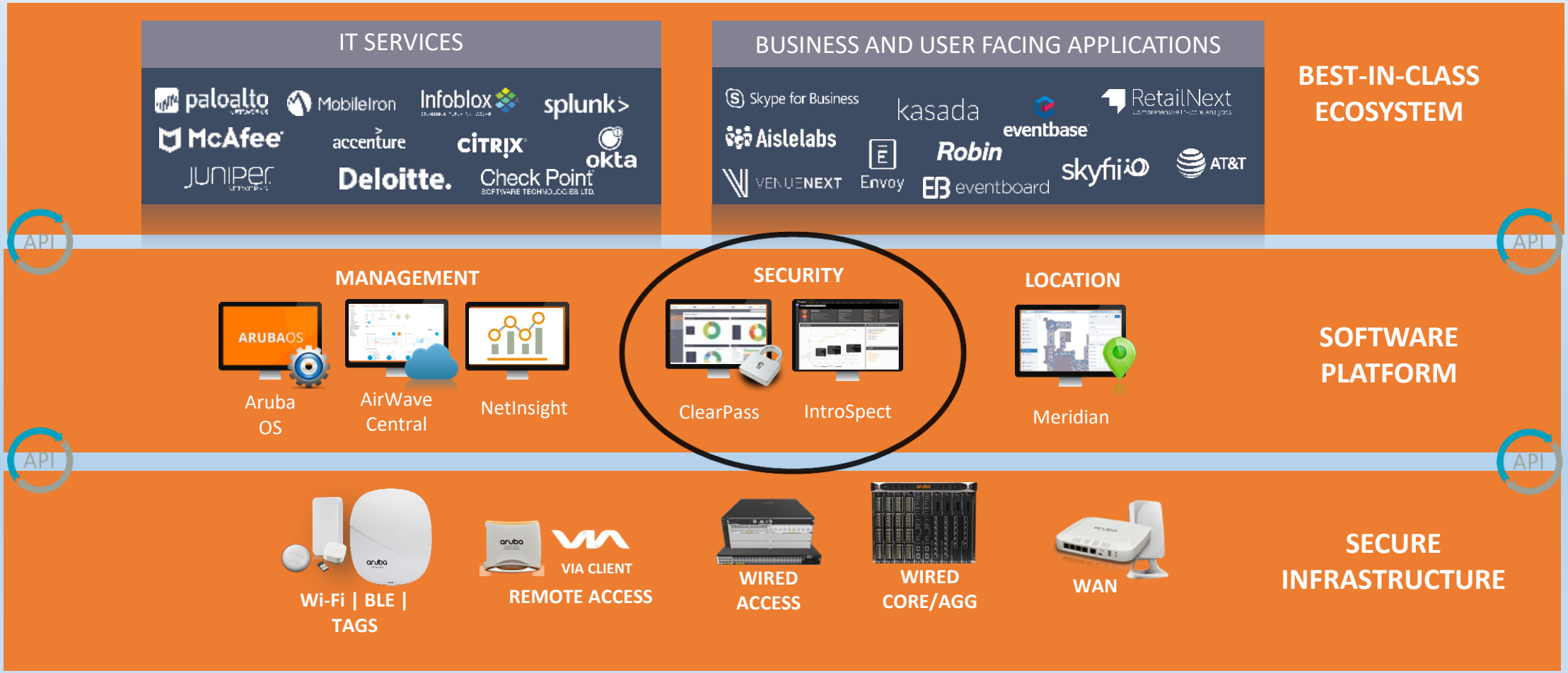
aruba a Hewlett Packard Enterprise company

ClearPass Policy Manager

Berk Bozkuş | ACDX#545 / ACCX#1018
Senior Aruba Systems Engineer

aruba a Hewlett Packard Enterprise company PARTNER AMBASSADOR 2018

Mobile First Architecture



Mobile First | Secure | Open | Insightful and Autonomous

ClearPass Continues to Grow

Granular traffic control with user and device data

Next-Gen Perimeter Defense

paloalto NETWORKS · JUNIPER NETWORKS · Check Point SOFTWARE TECHNOLOGIES LTD · FORTINET

Visibility and interactive control features

ArcSight An HP Company · splunk> · RSA SecurID · servicenow · QRadar · DUO

SIEM, Automation, MFA

Client Devices

IoT Devices

MDM / EMM

airwatch · MobileIron · Google · CITRIX · Microsoft · BlackBerry

Network controls using real-time device data

Infrastructure

Hewlett Packard Enterprise · aruba a Hewlett Packard Enterprise company · BROCADE · JUNIPER NETWORKS · CISCO

Visibility into location and time with granular controls

Multivendor Interoperability

Context Sharing

Open API & Syslogs

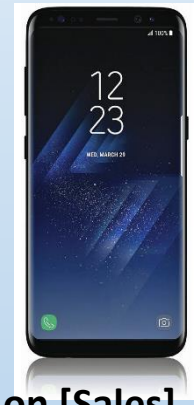
Sources of Usable Context

Device Profiling

- Samsung SM-G950U
- Android
- “Jons-Galaxy”

EMM/MDM

- Personally owned
- Registered
- OS up-to-date



- Hansen, Jon [Sales]
- MDM enabled = true
- In-compliance = true

Identity Stores

- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive office
- City – London

Microsoft Active Directory
Office 365
MySQL
okta
G Suite
Ping Identity
SAML
OAUTH 2

Enforcement Points

- Location – Bldg 10
- Floor – 3

Comprehensive Profiler Methods

- Helps ensure accurate fingerprints

- Passive Profiling
- DHCP Fingerprinting (MAC OUI & Certain Options)
  - AOS IF-MAP Interface, DHCP Relay or SPAN
- HTTP User-Agent
  - AOS IF-MAP Interface, SPAN, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Netflow/IPFIX/sFlow
  - Identifies open ports

- Active Profiling
- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP





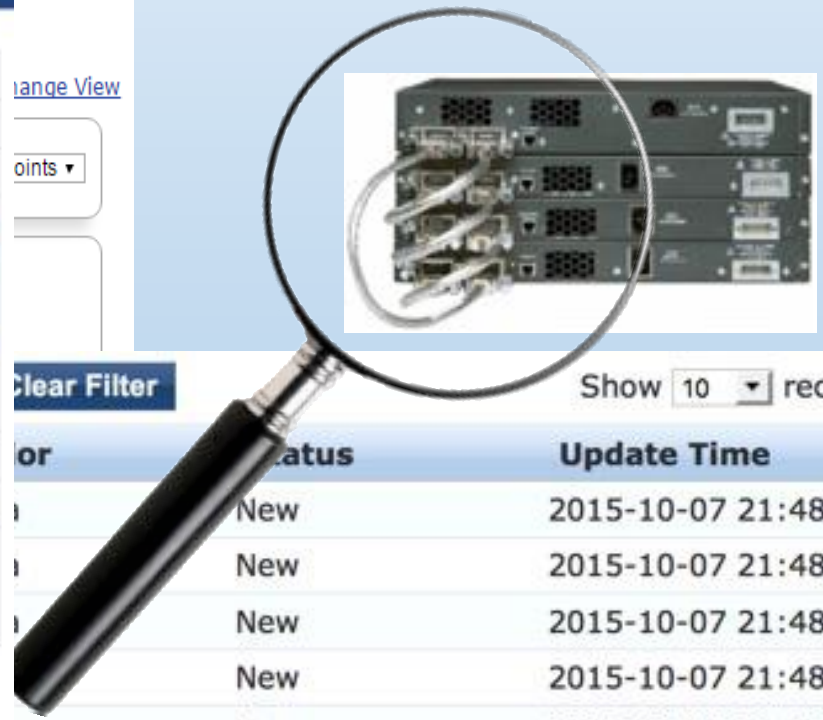
Visibility

Network Device Details

Sys Name:	Cisco-switch-51.202
Vendor:	Cisco
Sys Location:	#1344#ROW2#Rack1""
Sys Contact:	dl-cppm-qa@arubanetworks.com
Sys Description:	Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version 15.2(1)E, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2013 by Cisco Systems, Inc. Compiled Tue 27-Aug-13 11:06 by prod_rel_team
Status:	New
Update Time:	Wed Oct 07 2015 15:03:09 GMT-0700 (PDT)
IP Address:	10.2.51.202 10.2.50.202 10.2.48.193

Neighbour Device Details:-

#	IP Address	Name	Port	Device	Platform
1.	0.0.0.0	localhost.workspacedemo.com	Gi1/0/18	SWITCH	VMware ESX
2.	10.1.93.20	Cisco-Switch-48.1		SWITCH	



ange View

oints ▾

Clear Filter

Show 10 records

0019fd	9.	Cisco-Switch-51.201	10.2.50.201	Cisco	New	2015-10-07 21:48:46
58bda3	10.	Cisco-switch-51.202	10.2.51.202	Cisco	New	2015-10-07 22:03:09
e00c7f						
e0e751	Showing 1-10 of 15					

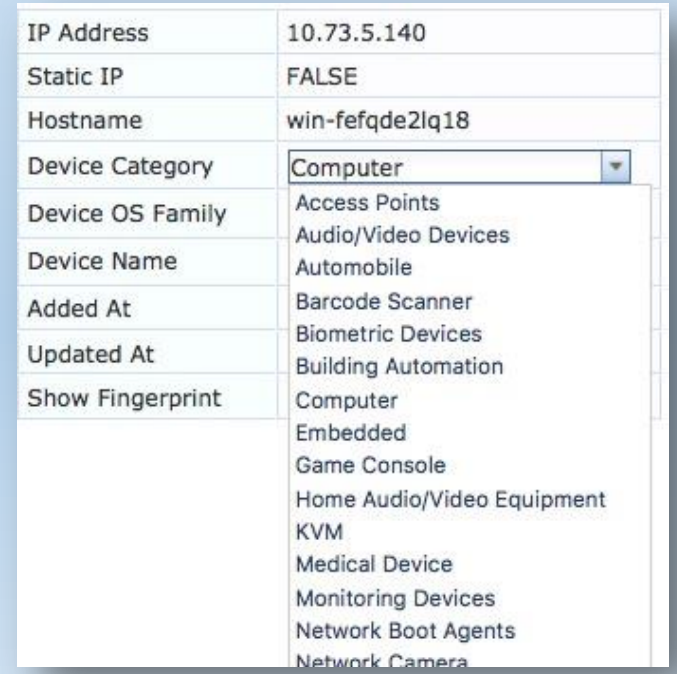
or	atus	Update Time
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 22:03:09
	New	2015-10-07 21:48:46
	New	2015-10-07 21:48:46
	New	2015-10-07 22:03:09

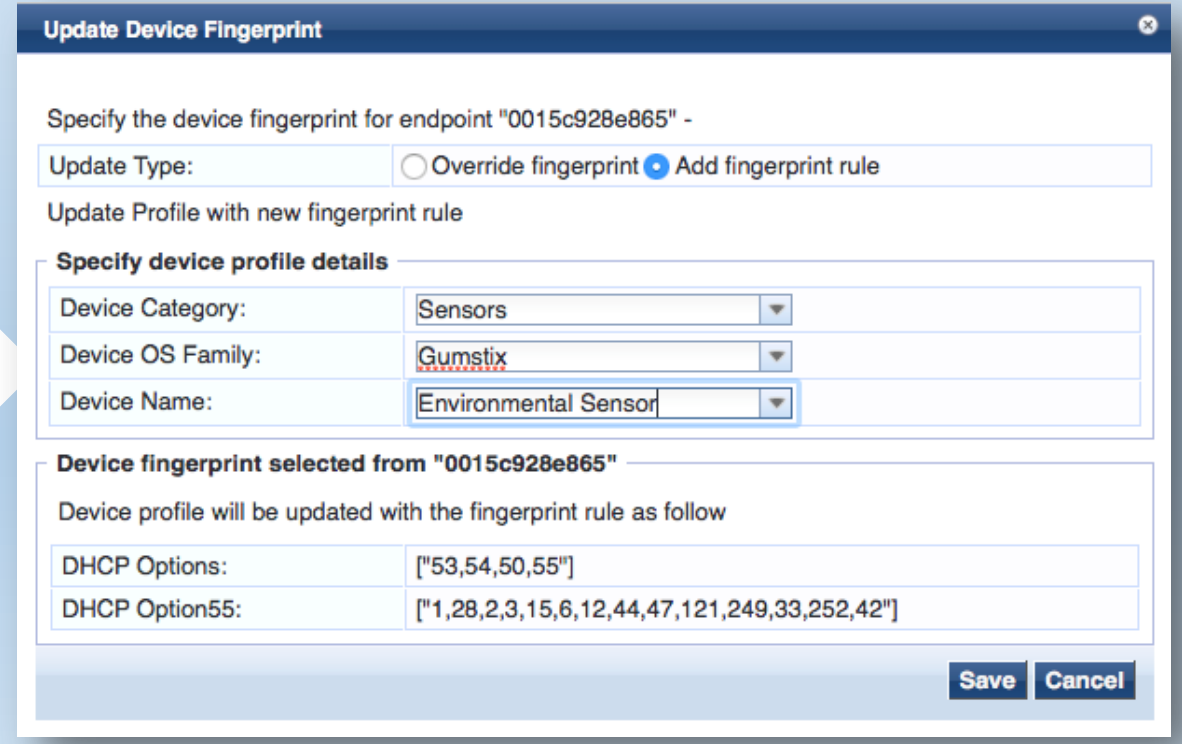
Import Ignore

Custom Fingerprinting – Solving IoT Issues

OLD WAY:

Wait for new Fingerprints to be made and/or manually override devices 1:1





NEW WAY:

Create your own Fingerprints!

Adaptive Trust Context Sharing

User and Device

Adaptive Trust Identity

WHO WHAT WHERE WHEN

Who: **Bob**
Group: **Faculty**
Device: **Personal iPad**
OS: **10.9.3**
Compliance: **Healthy**

CLEARPASS

ClearPass
Access Management

Employee Access → **Context Shared** → **FW policy adapts to need**

- **No agents/clients required**

What Context Can We Share?

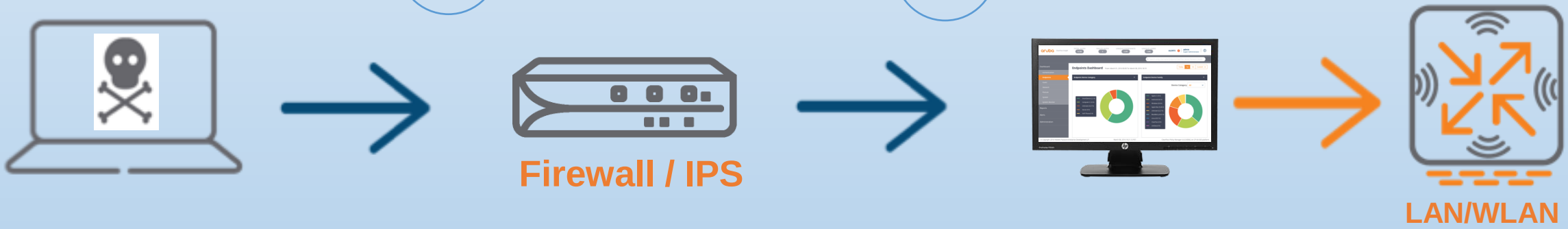
Context/Feature	paloalto NETWORKS	JUNIPER NETWORKS	Check Point SOFTWARE TECHNOLOGIES LTD.	FORTINET	SONICWALL
Source IP	↑	↑	↑	↑	↑
Username	↑	↑	↑	↑	↑
ClearPass Role	↑	↑	↑	↑	X
Domain	↑	↑	↑	X	X
Device Type	↑	↑	↑	X	X
Machine OS	↑	↑	↑	X	X
Machine Name	↑	↑	↑	X	X
Health/Posture	↑	↑	↑	X	X
Ingress Event Engine Dictionary	↑	↑	↑	↑	X

Ingress Engine Third-party Threat Protection

1 User connects and uploads/downloads threat

2 NGFW/IPS sends event to ClearPass

3 ClearPass isolates client



Adaptive Trust Defense based on real-time threat detection

- **Ingress Event Engine**
  - Ingestion of syslog messages for policy/triggers
  - Support for many popular vendors - option to import as needed

ClearPass Policy Manager - What's Built-in!

Services

- Policy Engine
- 802.1X
- MAC Auth
- Guest
- TACACS+
- Profiling/Onconnect
- Context Database
- +100 RADIUS dictionaries

IT Tools

- Policy Simulation
- Access Tracking
- Template-based policy creation
- LDAP Browser
- Per Session Logs
- Advanced Reporting (Insight)
- AirGroup

Bonjour/DLNA

Security Exchange

(3rd Party Integration)

- API's
- Syslog Feeds
- Extensions
- Ingress Events

Over 100+ Partners

paloalto NETWORKS
McAfee Together is power.
airwatch by vmware
JUNIPER NETWORKS
Pluribus NETWORKS
MobileIron
Microsoft
DUO
servicenow

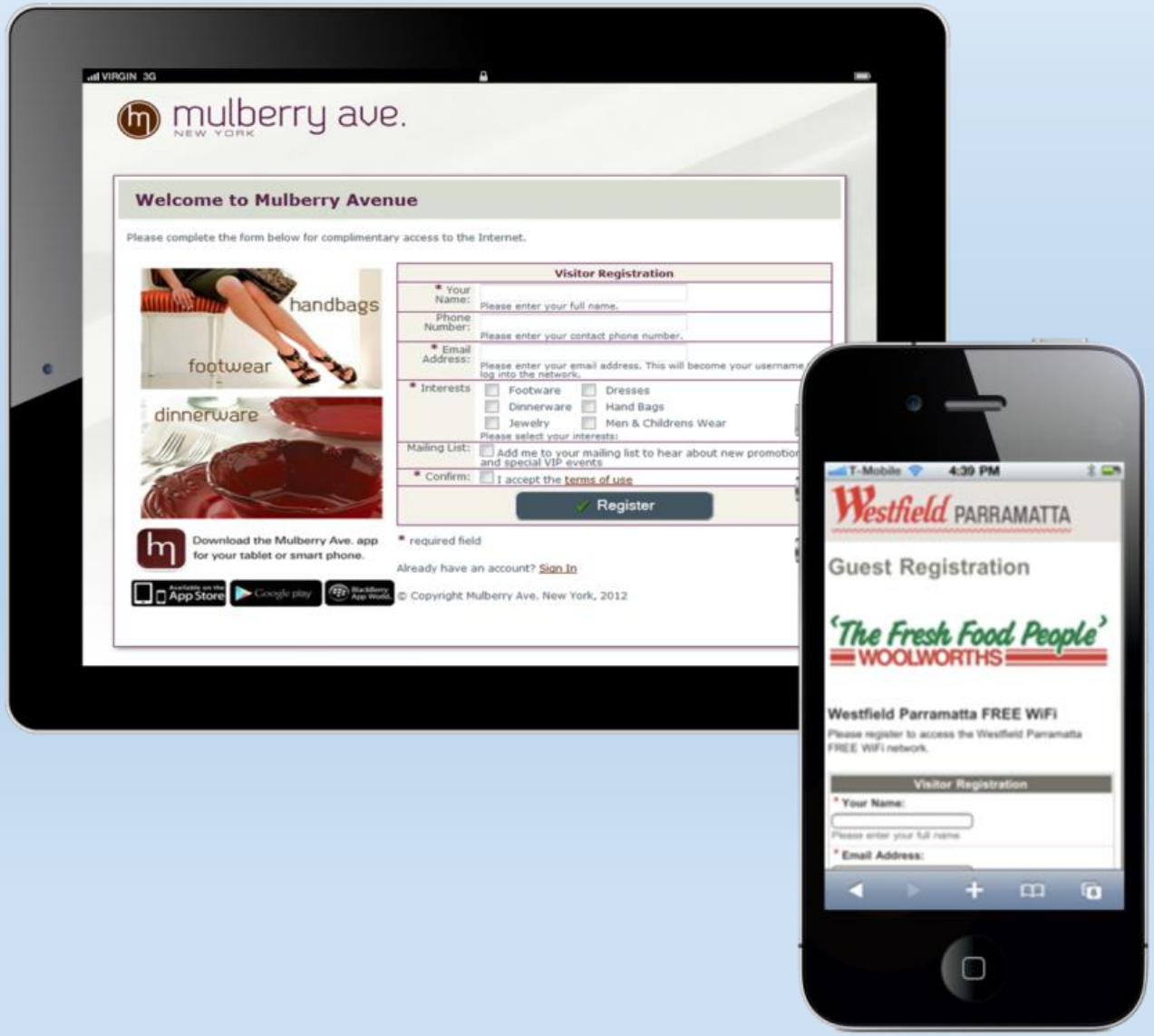
ClearPass Expandable Applications

Automated workflows

Enhanced security for BYOD and guests

Rules by user role and device types

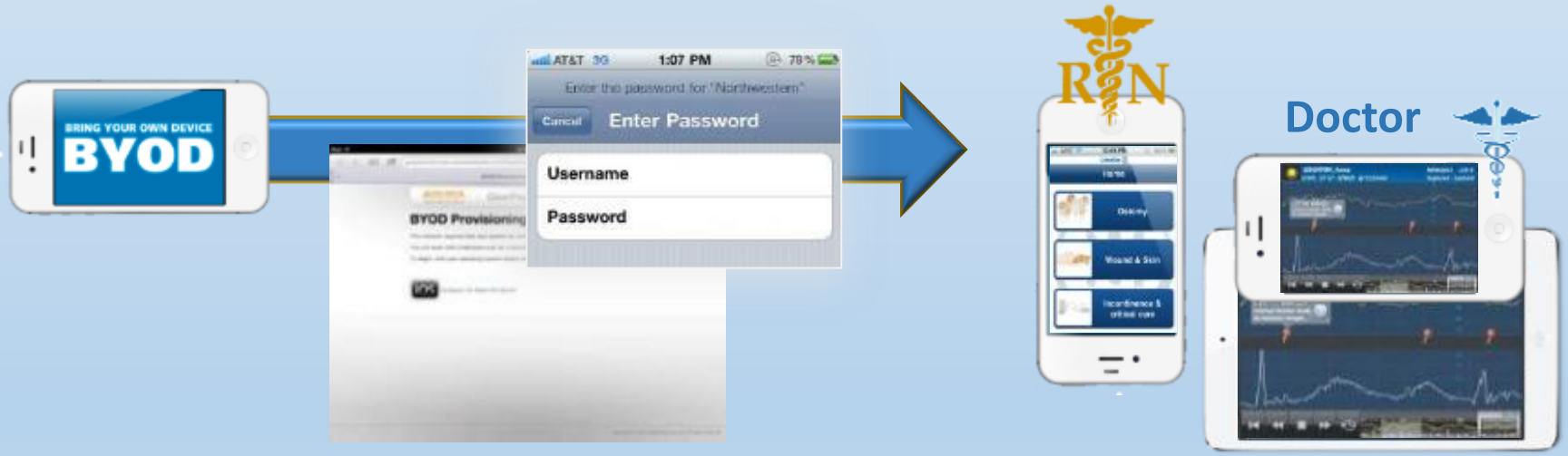
Clearpass Guest



- Sponsors, self-registration, SMS Integration
- Advertising
- Highly customizable fields to capture needed data
- Social Login (Facebook, Twitter, Linkedin, etc.)
- Bandwith Management and Quotation, MAC caching

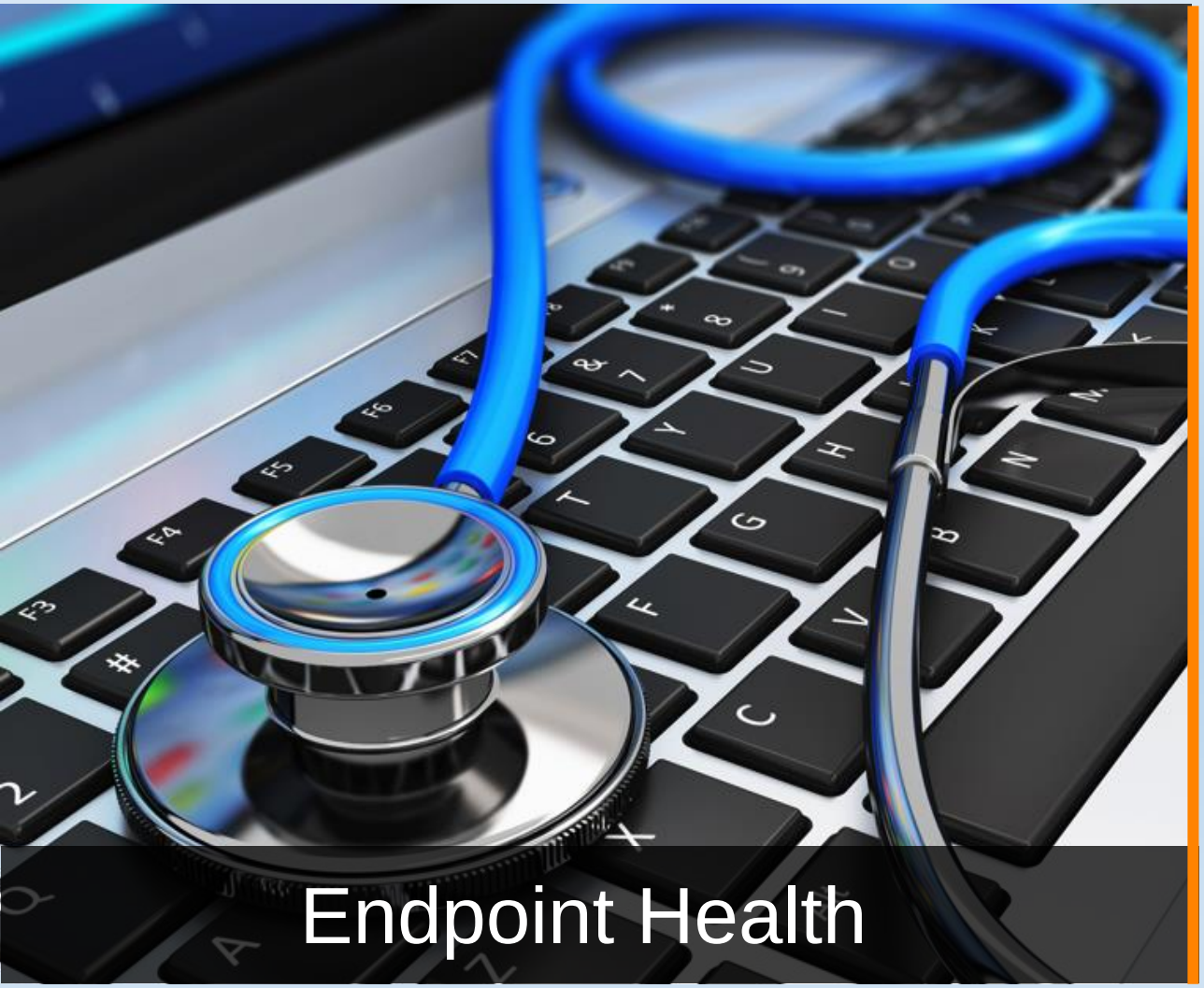
Clearpass Onboard

1. User's device redirected to portal
2. User enters AD credentials to start onboard
3. Automatically places user on proper network segment



- Automated configuration: Network settings and certs
- Built-in certificate authority (CA): Inc. user and device data

ClearPass OnGuard



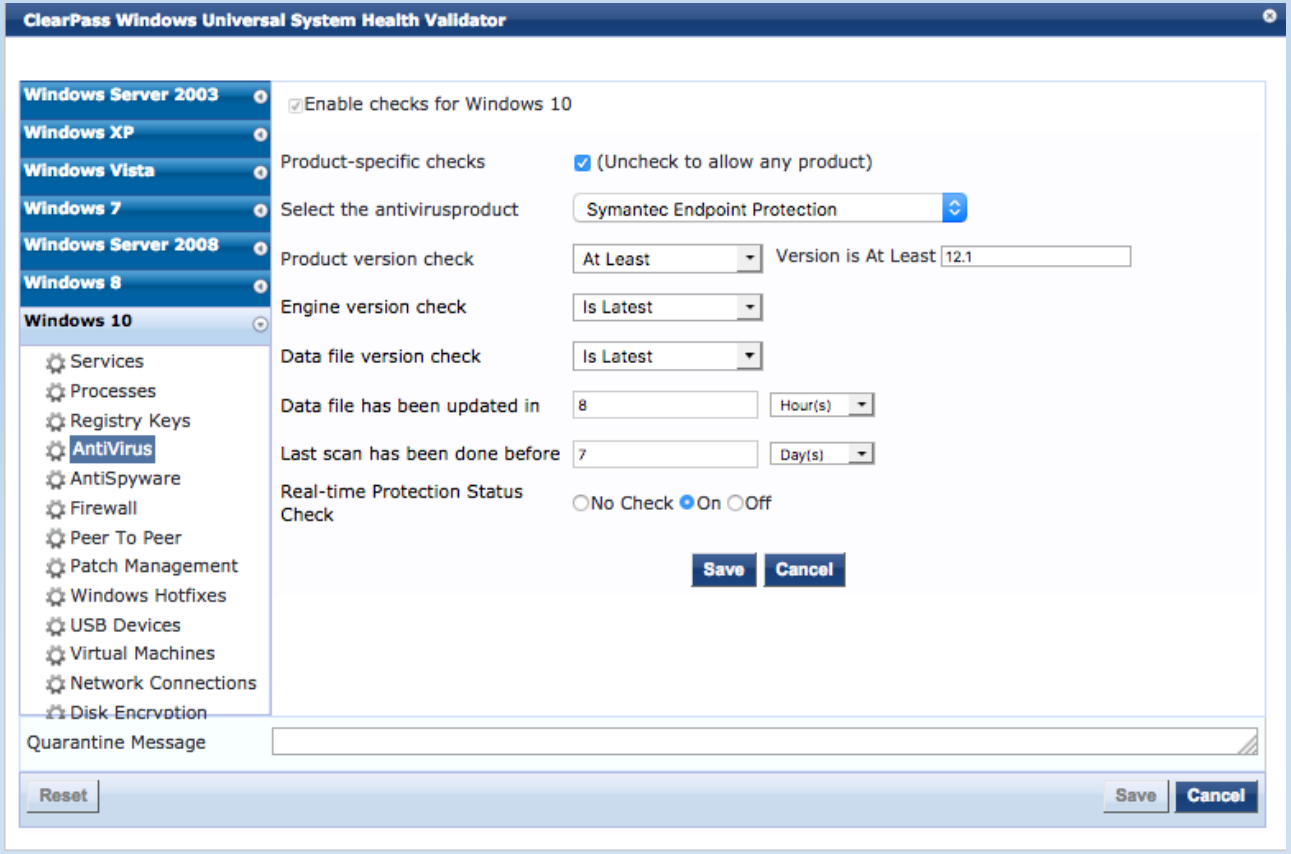
- Check health before network access
- Multiple operating systems supported
- Persistent and dissolvable agents

Automate Device Health Checking

Access Network

ClearPass OnGuard

Detect non-compliant devices



Automate Device Health Checking

Access Network

ClearPass OnGuard

Detect non-compliant devices

Block access to network resources across wired, wireless & remote

Automate Device Health Checking

Access Network

ClearPass OnGuard

Detect non-compliant devices

Block access to network resources across wired, wireless & remote

Auto-remediate the device

Minimizes risk to network

Allows user self service

Why ClearPass?

Multivendor

Clearpass Exchange

Both wireless and wired policies

Visibility (Device Profiling, Troubleshooting, Per-Session Tracking)


Thank You
Vinaka
Kiitos
Maake
Asante
Shukria
Dhanyavadagalu
감사합니다
Dank Je
Blagodaram
Ngiyabonga
Dziekuje
Juspaxar
Biyan
Dankon
Matondo
Tack
Arigato
Gracias
Grazie
Obrigado
Tingki
Gratias Tibi
Ua Tsaug Rau Koj
Bedankt
Dakujem
Grazas
Nirringrazzjak
Hvala
Welalin
Danke
Merci
Suksama
Děkuji
Matur Nuwun
Rahmat
Misaotra
Go Raibh Maith Agat
Kia Ora
Kop Khun Khap
Djiere Dieuf
Eskerrik Asko
ขอขอบคุณคุณ