



Shared IT Services for Higher Education & Research

Conference 2018

# Implementing Aruba ClearPass at BCIT

Use Cases and Experience

# Agenda

- Presenter Introductions
- Introduction to Aruba and Clear Pass Policy Manager
- BCIT adoption of CPPM – Use Cases and Experience
- Other Higher Education CPPM use cases



# Presenter Introductions

- Joubin Moshrefzadeh - BCIT
- Jason Fernyc - Aruba
- Marko Majkic - Aruba

# About Aruba

aruba

a Hewlett Packard  
Enterprise company

**Intelligent Edge Division**  
Intelligent Edge Networking for  
the Mobile, Cloud, and IoT Era

**“Customer First,  
Customer Last”**  
Dedicated Sales  
and Support

**Innovation Pioneers**  
Leader in Wired and  
Wireless Networking

**Innovation Hubs**  
Santa Clara, CA -HQ,  
Portland, Roseville, Canada,  
China, Costa Rica, India





# Products Overview

## MOBILE FIRST ARCHITECTURE



Mobile First | Secure | Open | Insightful and Autonomous

# What Is Clear Pass Policy Manager (CPPM)



# CPPM Secure NAC Solution



## VISIBILITY

- Know what's connected, connecting in your wired & wireless multivendor environment



## CONTROL

- Reduce risk and workload through Automation – All devices Authenticated or Authorized – NO UNKNOWN DEVICES



## RESPONSE

- Adaptive response brokering best of breed security solutions



# CPPM Exchange: End to End Control



# BCIT Implementation of CPPM

- Main drivers for ClearPass
- Initial Implementation
- Additional services integrated
- Benefits gained (and challenges)

# Main Drivers for ClearPass

- Wireless guest self-registration
- Easier guest account management
- Decoupling guest accounts from institute directory
- Standard approach to varying authentication sources
- Reducing complexity



# Initial Implementation

## Before ClearPass

---

### BCIT

- Open Captive Portal-based network for guests and non-802.1x clients
- LDAP via Active Directory

### BCIT\_Secure

- 802.1x network for staff and students
- Radius via AD-joined NPS server

### eduroam

- 802.1x network for staff, students, and visitors
- Radius via Radiator on Windows Server

## After ClearPass

---

### BCIT\_Connect

- Guest self-registration and access
- Client auto-configuration for our secure networks (via QuickConnect)
- Radius with MAC caching via ClearPass (guest DB)

### BCIT\_Secure

- Radius via ClearPass (AD joined + LDAP)

### eduroam

- Radius via ClearPass (AD joined + LDAP)

# Additional Services Integrated

## **Residence PPPoE Service**

- Radius auth against ClearPass (SQL lookup in Banner)

## **BCIT\_IOTNet Network**

- WPA2-PSK network with MAC auth (static host lists)

## **Juniper User Access and Authentication**

- Radius auth against ClearPass (local DB)



# Benefits Gained

## Easier troubleshooting

- One system to troubleshoot
- Easy to access logging and tracking information

## Stronger policy enforcement

- Re-use same policies/profiles across multiple services

## Single authentication frontend to varied backend repositories

- AD, SQL, local DB, local static host lists

ClearPass Policy Manager

[Support](#) | [Help](#) | [Logout](#)  
(Super Administrator)

Dashboard
Monitoring
Live Monitoring
Access Tracker
Accounting
OnGuard Activity
Analysis & Trending
Endpoint Profiler
System Monitor
Audit Viewer
Event Viewer
Data Filters
Blacklisted Users

Monitoring » Live Monitoring » Access Tracker

### Access Tracker

Apr 09, 2018 11:00:57 PDT

Auto Refresh

[All Requests]
default (2 servers)
Last 4 days before Today
Edit

Filter: Request ID contains Go Clear Filter
Show 20 records

#	Service	Source	NAS IP Address	Username	Login Status	Request Timestamp	Enforcement Profiles
1.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Student_Profile
2.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Student_Profile
3.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Student_Profile
4.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Student_Profile
5.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Employee_Profile
6.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Employee_Profile
7.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Employee_Profile
8.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:55	BCIT_Secure_Student_Profile
9.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
10.	BCIT_Eduroam VISITING USERS	RADIUS		@langara.ca	ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Guest_Profile
11.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
12.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
13.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Employee_Profile
14.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
15.	BCIT_Secure_Service	RADIUS			REJECT	2018/04/09 11:00:54	BCIT_Secure_Default_Profile
16.	BCIT_Eduroam HOME USERS	RADIUS		@bcit.ca	ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Employee_Profile
17.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
18.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:54	BCIT_Secure_Student_Profile
19.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:53	BCIT_Secure_Student_Profile
20.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:00:53	BCIT_Secure_Student_Profile

Showing 1-20 of more than 20 records

- Accounting
- OnGuard Activity
- Analysis & Trending
- Endpoint Profiler
- System Monitor
- Audit Viewer
- Event Viewer
- Data Filters
- Blacklisted Users

Filter: ☒ Request ID  
☐ Source  
☐ Username  
☐ NAS IP Address  
☐ NAS Port  
☐ Service  
☐ Login Status  
☐ Error Code  
☒ Host MAC Address  
☐ Alerts  
☐ Monitor Mode  
☐ Auth Type  
☐ Roles  
☐ Enforcement Profiles  
☐ System Posture Token  
☐ Audit Posture Token

contains

#	S	NAS IP Address	Username	Login Status
1.	B			ACCEPT
2.	B			ACCEPT
3.	B			ACCEPT
4.	B			ACCEPT
5.	B			ACCEPT
6.	B			ACCEPT
7.	B			ACCEPT
8.	B			ACCEPT
9.	BCIT_Secure_Service RADIUS			ACCEPT
10.	BCIT_Secure_Service RADIUS			ACCEPT
11.	BCIT_Secure_Service RADIUS			ACCEPT
12.	BCIT_Secure_Service RADIUS			ACCEPT
13.	BCIT_Secure_Service RADIUS			ACCEPT
14.	BCIT_Secure_Service RADIUS			ACCEPT
15.	BCIT_Secure_Service RADIUS			ACCEPT

Filter: Host MAC Address contains 3d:c4 Go Clear Filter Show 20 records

#	Service	Source	NAS IP Address	Username	Login Status	Request Timestamp ▾	Enforcement Profiles
1.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:03:17	BCIT_Secure_Employee_Profile
2.	BCIT_Secure_Service	RADIUS			REJECT	2018/04/09 11:02:43	BCIT_Secure_Default_Profile
3.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 11:02:33	BCIT_Secure_Employee_Profile
4.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 09:53:52	BCIT_Secure_Employee_Profile
5.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 09:53:46	BCIT_Secure_Employee_Profile
6.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 09:44:14	BCIT_Secure_Employee_Profile
7.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 09:43:43	BCIT_Secure_Employee_Profile
8.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 09:31:22	BCIT_Secure_Employee_Profile
9.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 07:55:11	BCIT_Secure_Employee_Profile
10.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 07:54:49	BCIT_Secure_Employee_Profile
11.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/09 07:54:17	BCIT_Secure_Employee_Profile
12.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/06 15:58:58	BCIT_Secure_Employee_Profile
13.	BCIT_Secure_Service	RADIUS			TIMEOUT	2018/04/06 15:54:47	BCIT_Secure_Default_Profile
14.	BCIT_Secure_Service	RADIUS			REJECT	2018/04/06 15:54:18	BCIT_Secure_Default_Profile
15.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/06 15:52:35	BCIT_Secure_Employee_Profile
16.	BCIT_Secure_Service	RADIUS			ACCEPT	2018/04/06 14:49:37	BCIT_Secure_Employee_Profile



Filter: Host MAC Address contains 3d:c4 Go Clear Filter Show 2

#	Service	Source	NAS IP Address	Username	Login Status	Request Timestamp	Enforcement Pr
1.	BCIT_Secure_Service RADIUS				ACCEPT	2018/04/09 11:03:17	BCIT_Secure_Emp
2.	BCIT_Secure_Service RADIUS				REJECT	2018/04/09 11:02:43	BCIT_Secure_Defi
3.	BCIT_Sec						Secure_Emp
4.	BCIT_Sec						Secure_Emp
5.	BCIT_Sec						Secure_Emp
6.	BCIT_Sec						Secure_Emp
7.	BCIT_Sec						Secure_Emp
8.	BCIT_Sec						Secure_Emp
9.	BCIT_Sec						Secure_Emp
10.	BCIT_Sec						Secure_Emp
11.	BCIT_Sec						Secure_Emp
12.	BCIT_Sec						Secure_Emp
13.	BCIT_Sec						Secure_Defi
14.	BCIT_Sec						Secure_Defi
15.	BCIT_Sec						Secure_Emp
16.	BCIT_Sec						Secure_Emp
17.	BCIT_Sec						Secure_Emp
18.	BCIT_Sec						Secure_Emp
19.	BCIT_Sec						Secure_Emp
20.	BCIT_Sec						Secure_Emp

**Request Details**

Summary Input Output Alerts

Login Status: **REJECT**

Session Identifier: R00b5bedb-05-5acbaac3

Date and Time: Apr 09, 2018 11:02:43 PDT

End-Host Identifier: 3DC4 (Computer / Windows / Windows 8/10)

Username:

Access Device IP/Port: (ArubaM3-bby-Local\_2)

System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: BCIT\_Secure\_Service

Authentication Method: EAP-PEAP,EAP-MSCHAPv2

Authentication Source:

Authorization Source: -

Roles: -

Enforcement Profiles: BCIT\_Secure\_Default\_Profile

Service Monitor Mode: Disabled

Online Status: Online

Showing 2 of 1-20 records

Show Configuration Export Show Logs Close

**Request Details**

SummaryInputOutputAlerts

Username:

End-Host Identifier:

Access Device IP/Port:

3DC4

(Computer / Windows / Windows 8/10)

(ArubaM3-bby-Local\_2\_)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	SW1_GROUP
Radius:Aruba:Aruba-Device-Type	Win 10
Radius:Aruba:Aruba-Essid-Name	BCIT_Secure
Radius:Aruba:Aruba-Location-Id	BBY_SW01_FL02_RM2301_AP02
Radius:IETF:Called-Station-Id	001A1E03ED00
Radius:IETF:Calling-Station-Id	3DC4
Radius:IETF:Framed-MTU	768
Radius:IETF:NAS-Identifier	802.1x_ClearPass
Radius:IETF:NAS-IP-Address	
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	10

Showing 2 of 1-20 records

Show ConfigurationExportShow LogsClose

Request Details

Summary

Input

Output

Alerts

Enforcement Profiles:	BCIT_Secure_Default_Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role

logon\_role

Showing 2 of 1-20 records

Show Configuration

Export

Show Logs

Close

Request Details

Summary

Input

Output

Alerts

Error Code:216

Error Category:Authentication failure

Error Message:User authentication failed

Alerts for this Request

RADIUS

MSCHAP: AD status:Logon failure (0xc000006d)  
MSCHAP: Authentication failed  
EAP-MSCHAPv2: User authentication failure

Showing 2 of 1-20 records

Show Configuration

Export

Show Logs

Close

# Benefits Gained

## Easier troubleshooting

- One system to troubleshoot
- Easy to access logging and tracking information

## Stronger policy enforcement

- Re-use same policies/profiles across multiple services

## Single authentication frontend to varied backend repositories

- AD, SQL, local DB, local static host lists

- Dashboard
- Monitoring
- Configuration
  - Start Here
  - Services
  - Authentication
    - Methods
    - Sources
  - Identity
    - Single Sign-On (SSO)
    - Local Users
    - Endpoints
    - Static Host Lists
    - Roles
    - Role Mappings
  - Posture
    - Posture Policies
    - Posture Servers
    - Audit Servers
  - Enforcement
    - Policies
    - Profiles
  - Network
    - Devices
    - Device Groups

Configuration » Enforcement » Profiles

## Enforcement Profiles

Filter:  contains

#	<input type="checkbox"/>	Name ▾	Type	Description
1.	<input type="checkbox"/>	BCIT_Secure_Student_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "student"
2.	<input type="checkbox"/>	BCIT_Secure_Resident_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "student"
3.	<input type="checkbox"/>	BCIT_Secure_NoWireless_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "banned"
4.	<input type="checkbox"/>	BCIT_Secure_Instructor_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "employee"
5.	<input type="checkbox"/>	BCIT_Secure_Guest_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "bcitguest"
6.	<input type="checkbox"/>	BCIT_Secure_FAC_Wireless_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "facwireless"
7.	<input type="checkbox"/>	BCIT_Secure_Employee_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "employee"
8.	<input type="checkbox"/>	BCIT_Secure_Default_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "logon_role"
9.	<input type="checkbox"/>	BCIT_Secure_CIT_Wireless_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "citwireless"
10.	<input type="checkbox"/>	BCIT_Secure_CAE_Wireless_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "caewireless"
11.	<input type="checkbox"/>	BCIT_Secure_AV_Wireless_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "avwireless"
12.	<input type="checkbox"/>	BCIT_PPPE_Wired_Profile	RADIUS	On Radius Accept it pushes Ingress/Egress Unisphere Policy's
13.	<input type="checkbox"/>	BCIT_Junos_SU_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "raduser-su"
14.	<input type="checkbox"/>	BCIT_Junos_RO_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "raduser-ro"
15.	<input type="checkbox"/>	BCIT_Junos_OP_Profile	RADIUS	On Radius Accept it pushes Aruba-Role: "raduser-op"
16.	<input type="checkbox"/>	BCIT_IOTNet_kinomo_profile	RADIUS	On success, pushes Aruba-role: "kinomo-role"
17.	<input type="checkbox"/>	BCIT_IOTNet_alexa_profile	RADIUS	On success, pushes Aruba-role: "amazon-role"



Dashboard

Monitoring

Live Monitoring

Access Tracker

Accounting

OnGuard Activity

Analysis & Trending

Endpoint Profiler

System Monitor

Audit Viewer

Event Viewer

Data Filters

Blacklisted Users

Monitoring » Live Monitoring » Access Tracker

Access Tracker

Apr 09, 2018 14:02:16 PDT

Auto Refresh

[All Requests]

default (2 servers)

Last 4 days before Today

Edit

Filter: Service

contains

Eduroam

Go

Clear Filter

Show 20 records

#	Service	Source	NAS IP Address	Username	Login Status	Request Timestamp	Enforcement Profiles
1.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:14	BCIT_Secure_Employee_Profile
2.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:13	BCIT_Secure_Employee_Profile
3.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:13	BCIT_Secure_Employee_Profile
4.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:12	BCIT_Secure_Employee_Profile
5.	BCIT_Eduroam VISITING USERS	RADIUS			ACCEPT	2018/04/09 14:02:10	BCIT_Secure_Guest_Profile
6.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:08	BCIT_Secure_Student_Profile
7.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:08	BCIT_Secure_Student_Profile
8.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:07	BCIT_Secure_Student_Profile
9.	BCIT_Eduroam HOME USERS	RADIUS			ACCEPT	2018/04/09 14:02:07	BCIT_Secure_Student_Profile

# Benefits Gained

## Easier troubleshooting

- One system to troubleshoot
- Easy to access logging and tracking information

## Stronger policy enforcement

- Re-use same policies/profiles across multiple services

## Single authentication frontend to varied backend repositories

- AD, SQL, local DB, local static host lists

Configuration » Authentication » Sources

## Authentication Sources

[Add](#)  
[Import](#)  
[Export All](#)

Authentication source Banner\_Connector updated

☐ Select ALL matches 
 ☒ Select ANY match

Filter: Name contains Banner  
 Filter: Name contains IOTNet  
 Filter: Name contains DC1  
 Filter: Name contains DC2

Go Clear Filter

Show 100 records

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	Banner_Connector	Generic SQL DB	Residence authentication via Banner SQL
2.	<input type="checkbox"/>	BCIT_AD - DC1	Active Directory	BCIT Active Directory
3.	<input type="checkbox"/>	BCIT_AD - DC2	Active Directory	BCIT Active Directory
4.	<input type="checkbox"/>	BCIT_IOTNet-alexa-auth-source	Static Host List	BCIT_IOTNet auth for Amazon Alexa devices only
5.	<input type="checkbox"/>	BCIT_IOTNet-kinomo-auth-source	Static Host List	BCIT_IOTNet Auth source for Kino-mo devices only

Showing 1-5 of 5

[Copy](#)
[Export](#)
[Delete](#)

# Challenges

## Steep learning curve

- Four products (Policy Manager, Guest, Insight, Onboard)
- There are a lot of features and options

## Redundancy can be complex

- Opted for geographically split HA cluster with Virtual IP



# ENABLING COLLABORATION

## Challenge #1

**Collaboration/AV Systems are Expensive to deploy, configure & maintain across the Campus.**

## Challenge #2

**Collaboration/AV Systems are difficult for Faculty, Staff & Student End-Users to understand & leverage.**

## Challenge #3

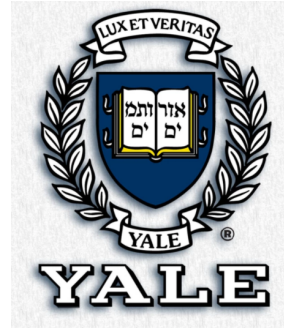
**Collaboration/AV Systems are difficult to Secure and Control.**

# ENABLING COLLABORATION





# ARUBA ENABLING COLLABORATION



WHO

- User / role



WHAT

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



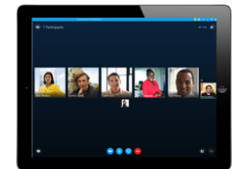
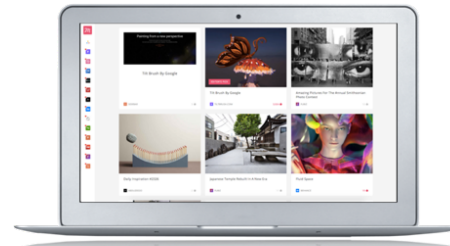
WHEN

- Time
- Date



WHERE

- Location
- Trusted or untrusted network



# CONTROL OF WIRED & IOT NETWORKS

## Challenge #1

Legacy networks aren't designed to easily support critical building, dormitory, classroom, and IoT systems. Non-Traditional devices (beyond laptops, tablets and smartphones) will soon outnumber traditional devices by a significant margin.

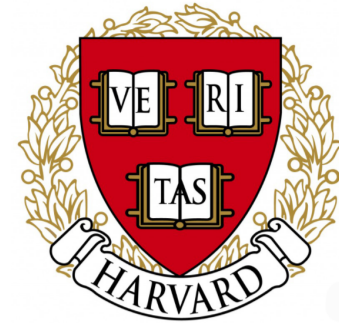
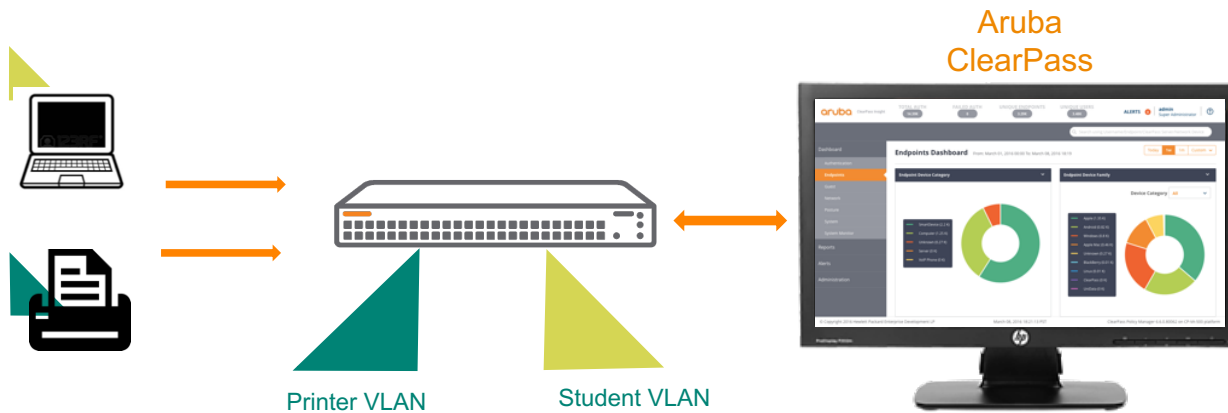
## Challenge #2

Most fixed Wired Devices are not in traditional data stores (e.g. Active Directory), nor are they managed via the same mechanisms (e.g. Group Policy)

## Challenge #3

IoT systems – both open and closed - have vulnerable attack surfaces that can expose systems, users, and facilities to security and privacy breaches

# ARUBA CENTRALIZED POLICY CONTROL





# POSTURE CONTROL OF CLIENTS

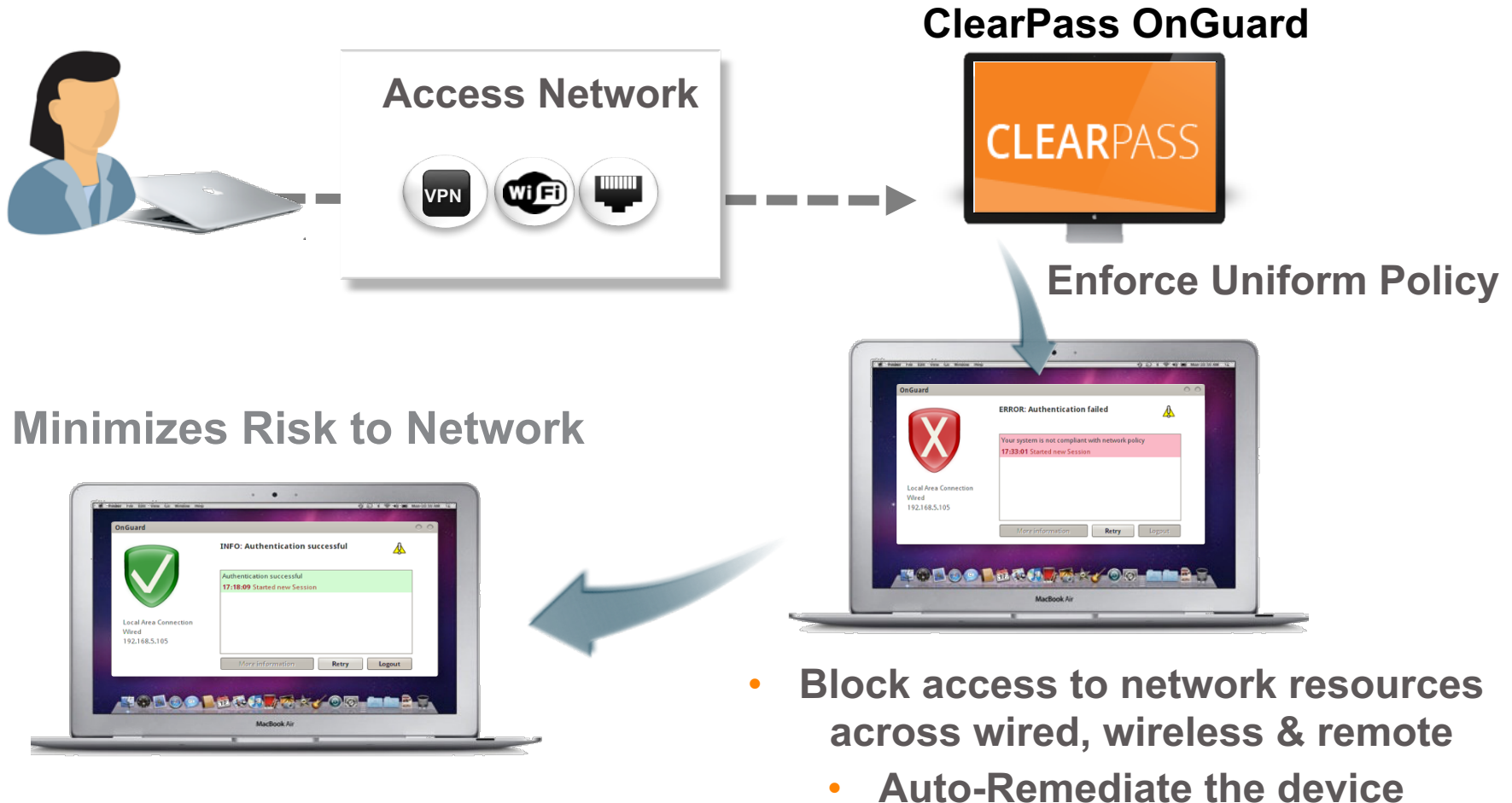
## Challenge #1

Clients of all kinds can easily be infected by Malware, Spyware, Virus and/or Ransomware.

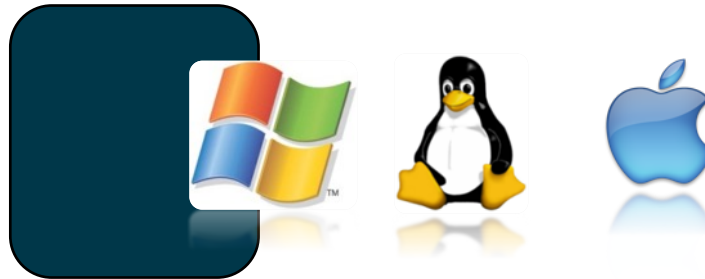
## Challenge #2

How to be enforce a uniform set of security requirements across client base, including organization owned and personally owned devices.

# ARUBA POSTURE CONTROL OF CLIENTS



# ARUBA POSTURE CONTROL OF CLIENTS



**Persistent and dissolvable** agents for laptops and desktops.

	Windows	Mac OS X	Linux
Installed Applications	X	X	
AntiVirus	X	X	X
AntiSpyware	X	X	
Firewall	X	X	
Disk Encryption	X	X	
Network Connections	X	X	
Processes	X	X	
Patch Management	X	X	
Peer to Peer	X	X	
Services	X	X	X
Virtual Machines	X	X	
Windows Hotfixes	X		
USB Devices	X	X	
File Check	X	X	



# OPTIMIZING IT OPERATIONS

## Challenge #1

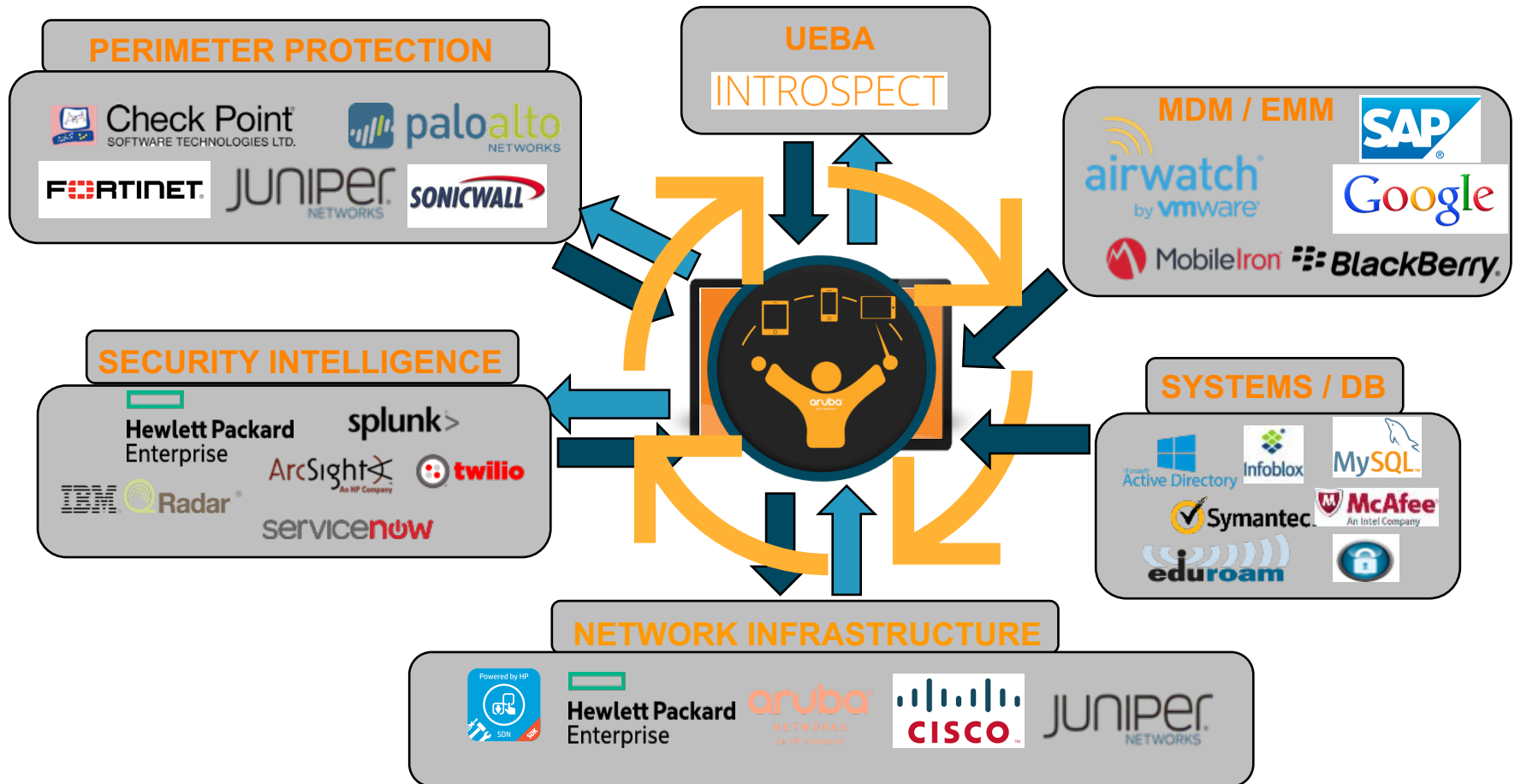
IT Personnel & Resources are stretched to keep up with current network requirements incorporating laptops, tablets, and smartphones as devices per user, and BYOD trends continue to ramp.

## Challenge #2

IoT deployments will further stretch existing resources and budgets due to exponential and unprecedented “non-traditional” device types with limited user interfaces.



# ARUBA IT OPERATIONS AUTOMATION







Shared IT Services for Higher Education & Research

Conference 2018

Thank You!