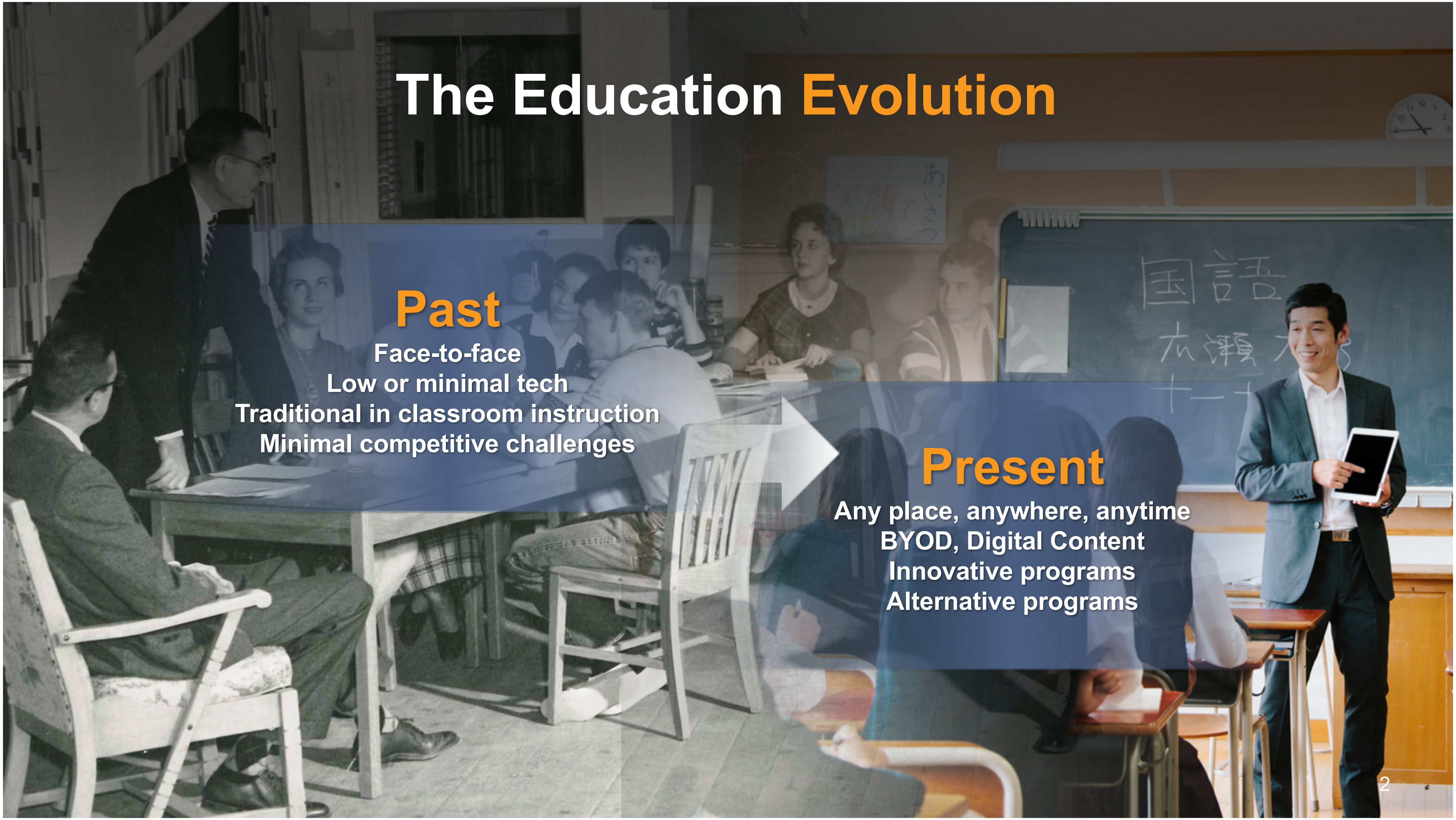
Secure & Automated Access for BYOD devices in Education

Metin SÖNMEZ
Systems Engineer
HPE Aruba

aruba
a Hewlett Packard
Enterprise company



The Education Evolution

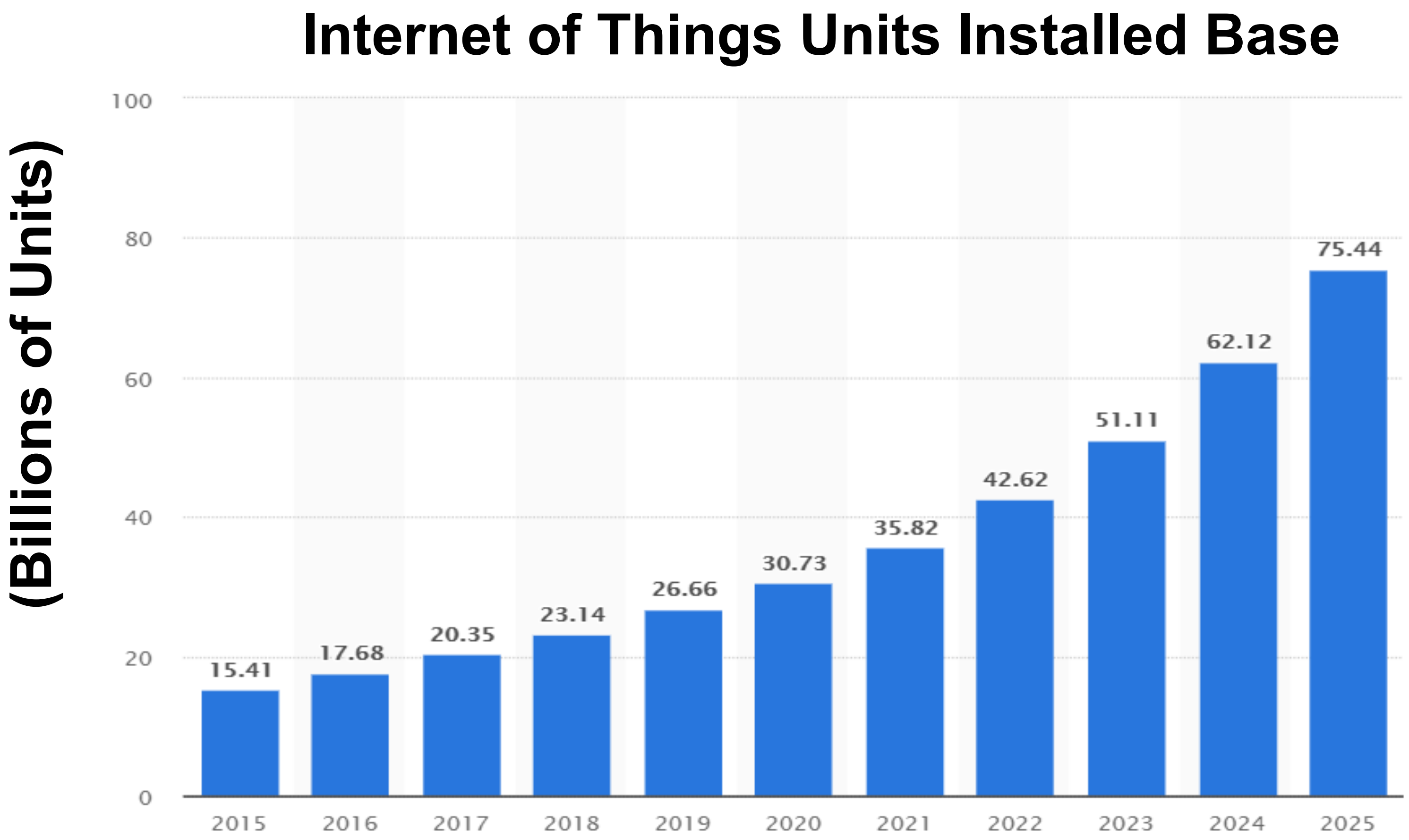
Past

Face-to-face
Low or minimal tech
Traditional in classroom instruction
Minimal competitive challenges

Present

Any place, anywhere, anytime
BYOD, Digital Content
Innovative programs
Alternative programs

Growth of Things



Source : Gartner 2016

Question of the Day – Week - Month - Year

ON

IS THE

NETWORK?

Today’s Digital Workplace Concerns

Device Visibility

Over 90% of customers do not know how many and what types are on their networks

Connection Options

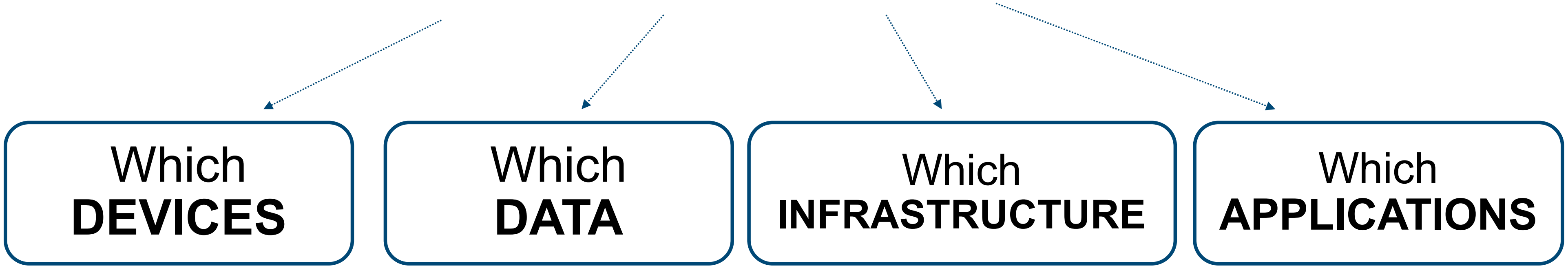
Customers lack plans for BYOD, IoT, wired, wireless and VPN policies

User Logins

Customers want help with access for employees, guests, students, doctors

What does ClearPass do ?

Defines **WHO** and **WHAT DEVICES** can connect to:



Which **DEVICES**

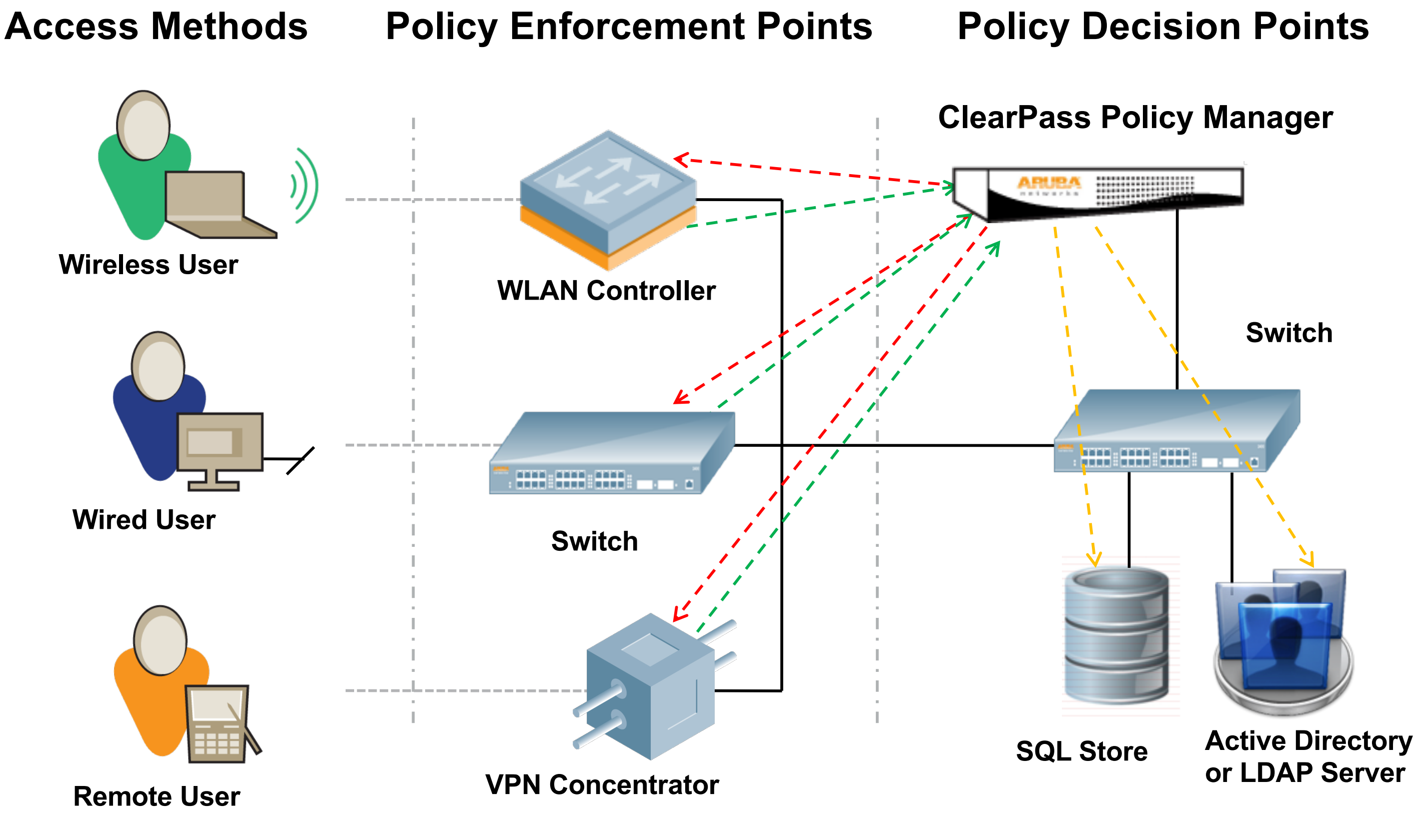
Which **DATA**

Which **INFRASTRUCTURE**

Which **APPLICATIONS**

Identify – Enforce – Protect

Where We Fit



Access Methods

Policy Enforcement Points

Policy Decision Points

ClearPass Policy Manager

Wireless User

WLAN Controller

Wired User

Switch

Remote User

VPN Concentrator

Switch

SQL Store

Active Directory or LDAP Server

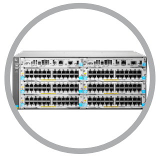
A Secure Enterprise: Identify Everything

Contractor

IoT

Headless

Employee BYOD



Infrastructure

Visitor

Administrator

Employee

ClearPass Policy Manager - What's Built-in!

Over 100+ Partners

Services

- Policy Engine
- AAA Server
- OnConnect
- RADIUS/CoA
- TACACS+
- Profiling+
- +100 RADIUS dictionaries
- Context Database

IT Tools

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

Bonjour/DLNA

ClearPass Exchange

(3rd Party Integration)

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

paloalto NETWORKS

intel Security

Pluribus NETWORKS

MobileIron

Microsoft

DUO

servicenow

Understanding Connectivity Options

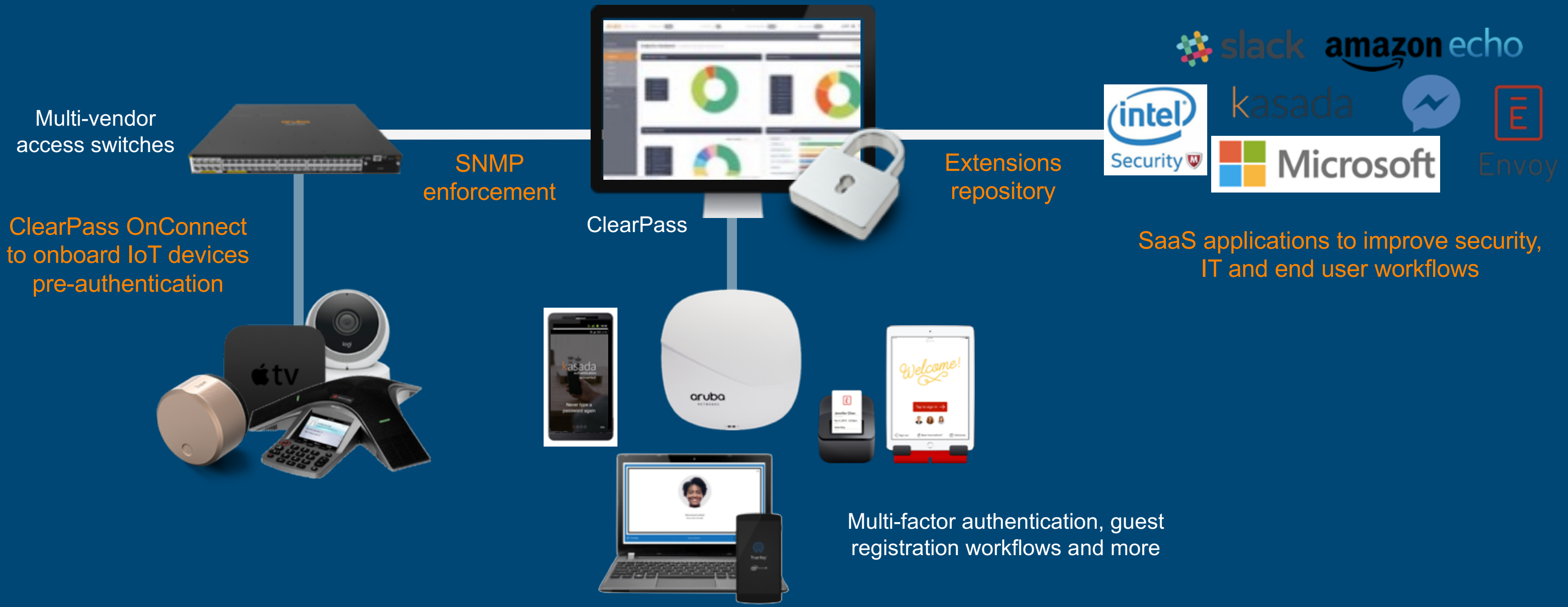
Customers want to **manage** what devices connect

Only some support .1X supplicants

50% of IoT may be wired

- ClearPass supports any customer Infrastructure and need

Extending Policies To Any Cloud App And IoT Device



Multi-vendor access switches

SNMP enforcement

ClearPass

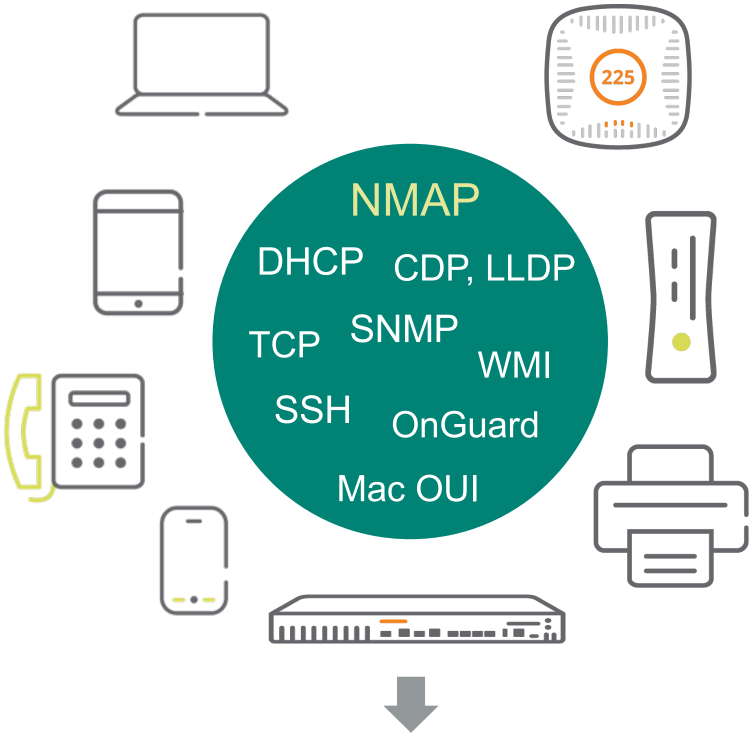
Extensions repository

ClearPass OnConnect to onboard IoT devices pre-authentication

SaaS applications to improve security, IT and end user workflows

Multi-factor authentication, guest registration workflows and more

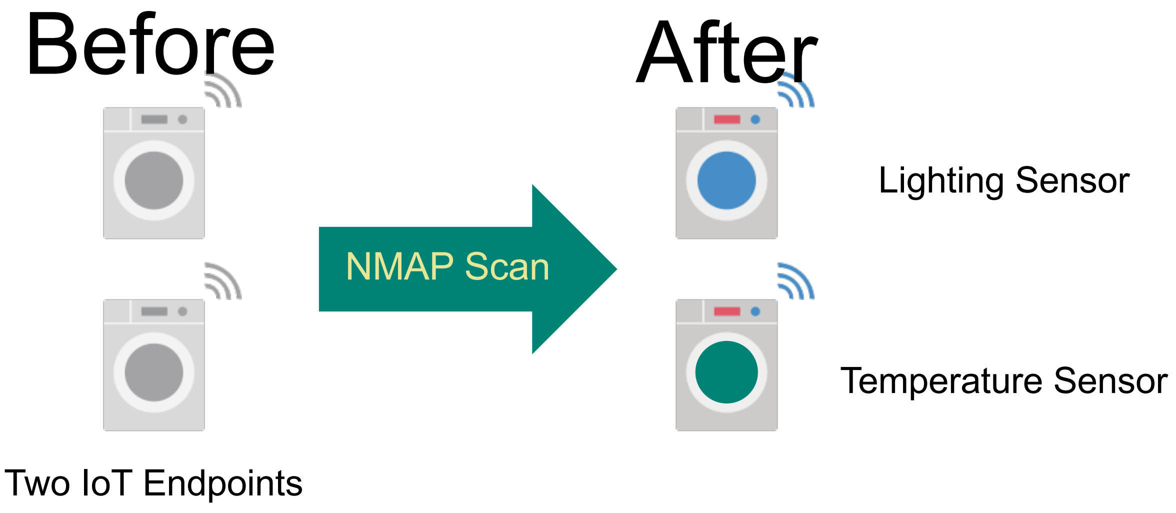
Device Visibility Enhanced



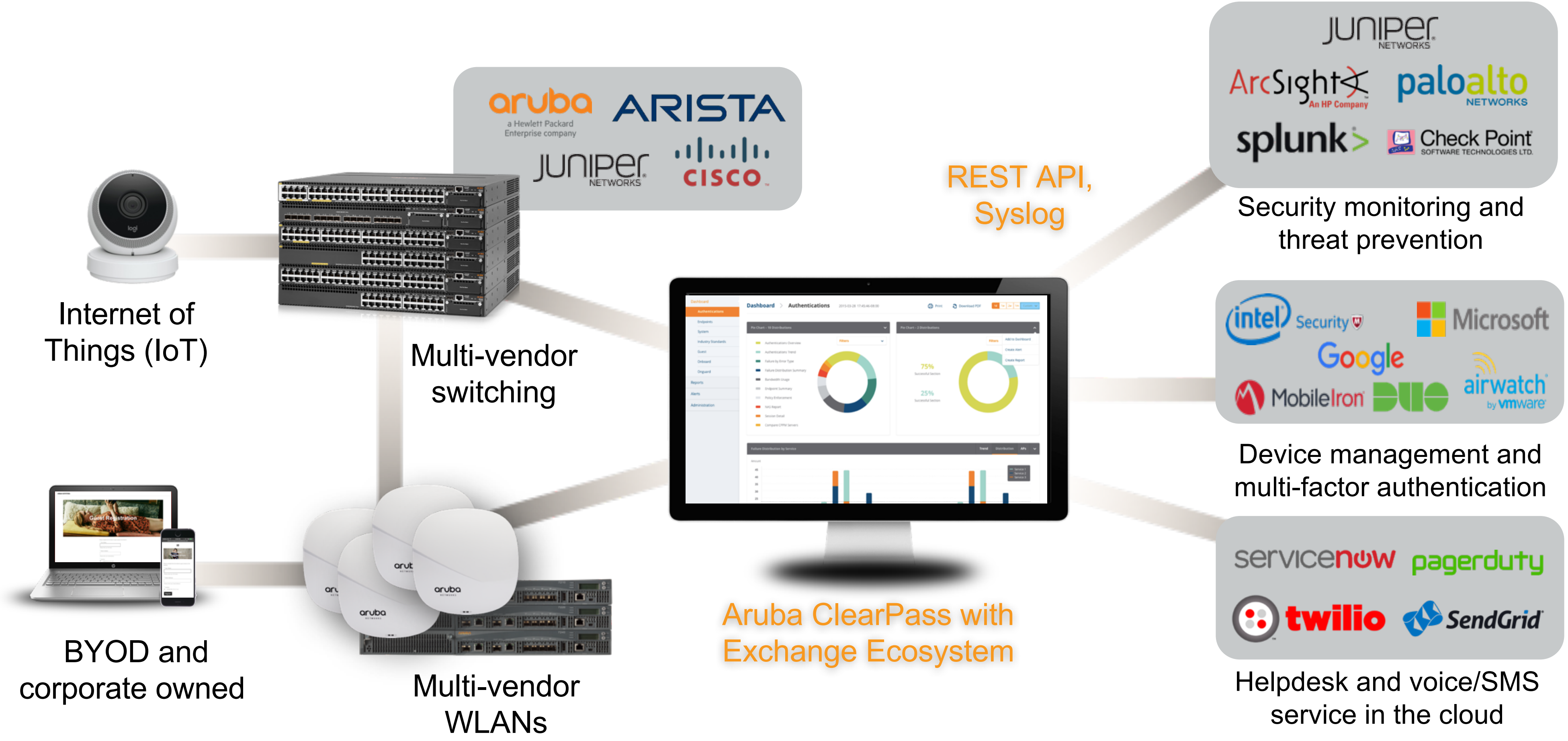
Accurate Policy Decision

NEW

- NMAP Port-based Scanner
  - On-demand or pre-scheduled scans
  - Granular visibility for like devices
- Enhances our competitive advantage



ClearPass Exchange: End to End Controls



Internet of Things (IoT)

Multi-vendor switching

BYOD and corporate owned

Multi-vendor WLANs

REST API, Syslog

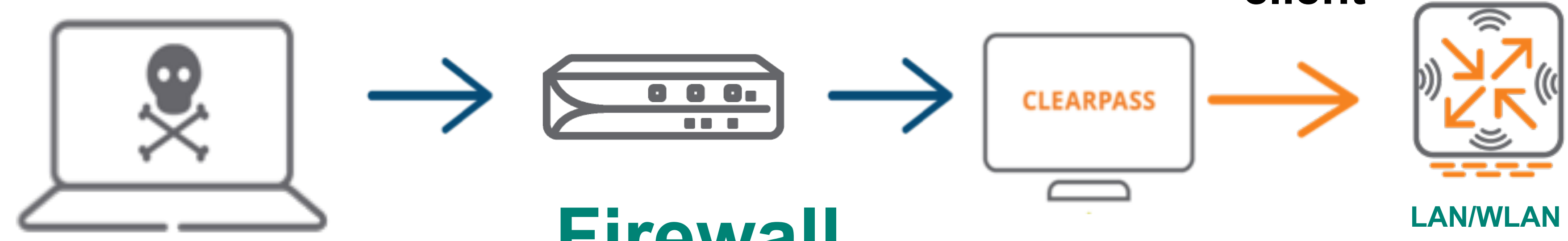
Aruba ClearPass with Exchange Ecosystem

Security monitoring and threat prevention

Device management and multi-factor authentication

Helpdesk and voice/SMS service in the cloud

Automated Defense – Nex Generation Firewall / IPS



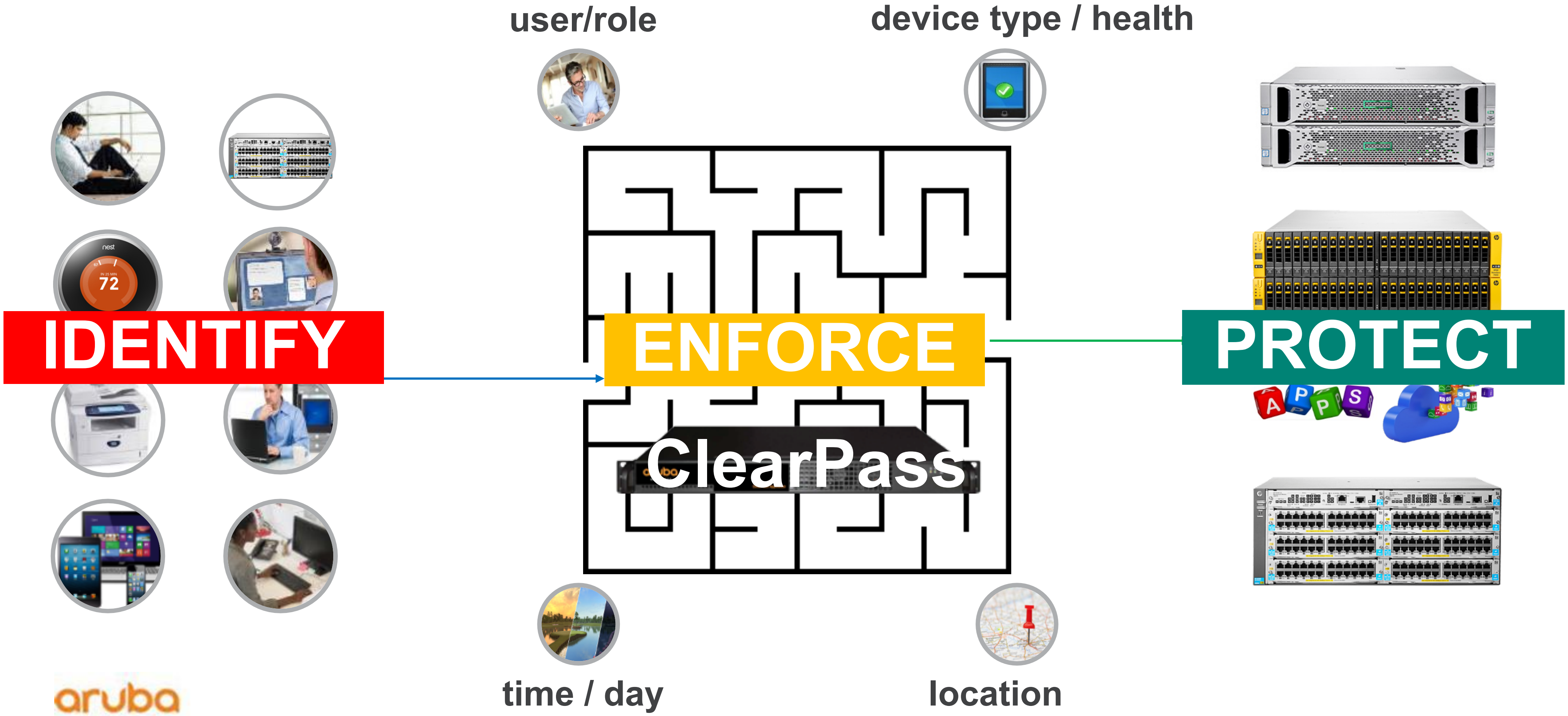
1 User connects and downloads threat

2 NGFW / IPS sends event to ClearPass

3 ClearPass isolates client

Firewall / IPS

Enforce A Per Device Policy



user/role

device type / health

IDENTIFY

ENFORCE

PROTECT

ClearPass

time / day

location

aruba
a Hewlett Packard Enterprise company

Intelligent Policy Management for Students, Staff, Guests

Aruba ClearPass

- One time user registration / no IT intervention
- Simplify and secure BYOD growth and IoT adoption
- Visibility for policy and troubleshooting
- Custom portals to promote your campus
- Social / Hot Spot 2.0 / eduroam support

Universal Profiler

Automatically identify and profile all connected devices, including controllers and switches

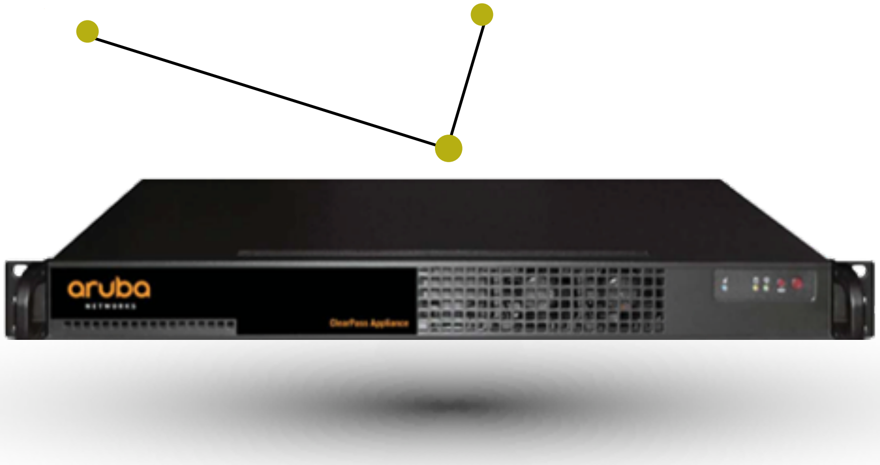
Enabling Managed Access for Wired and Wireless

Onboard

Guest

OnGuard

- Automated device fingerprinting
- Enhanced security for BYOD and guests
- Automating workflows
- Device health checks



ClearPass Guest – Access Options

- **Consistent**

  Access across verticals, locations and devices

- **No IT**

  IT should not be involved in creating secure guest access, Social Login, SMS, Sponsored Quota, Charging, Advertice

- **Other Office Access**

  Allow domain credentials on Guest to access corporate assets,

BYOD on Campus

School Issued Devices

- School-owned
- Fully managed
- Fully controlled

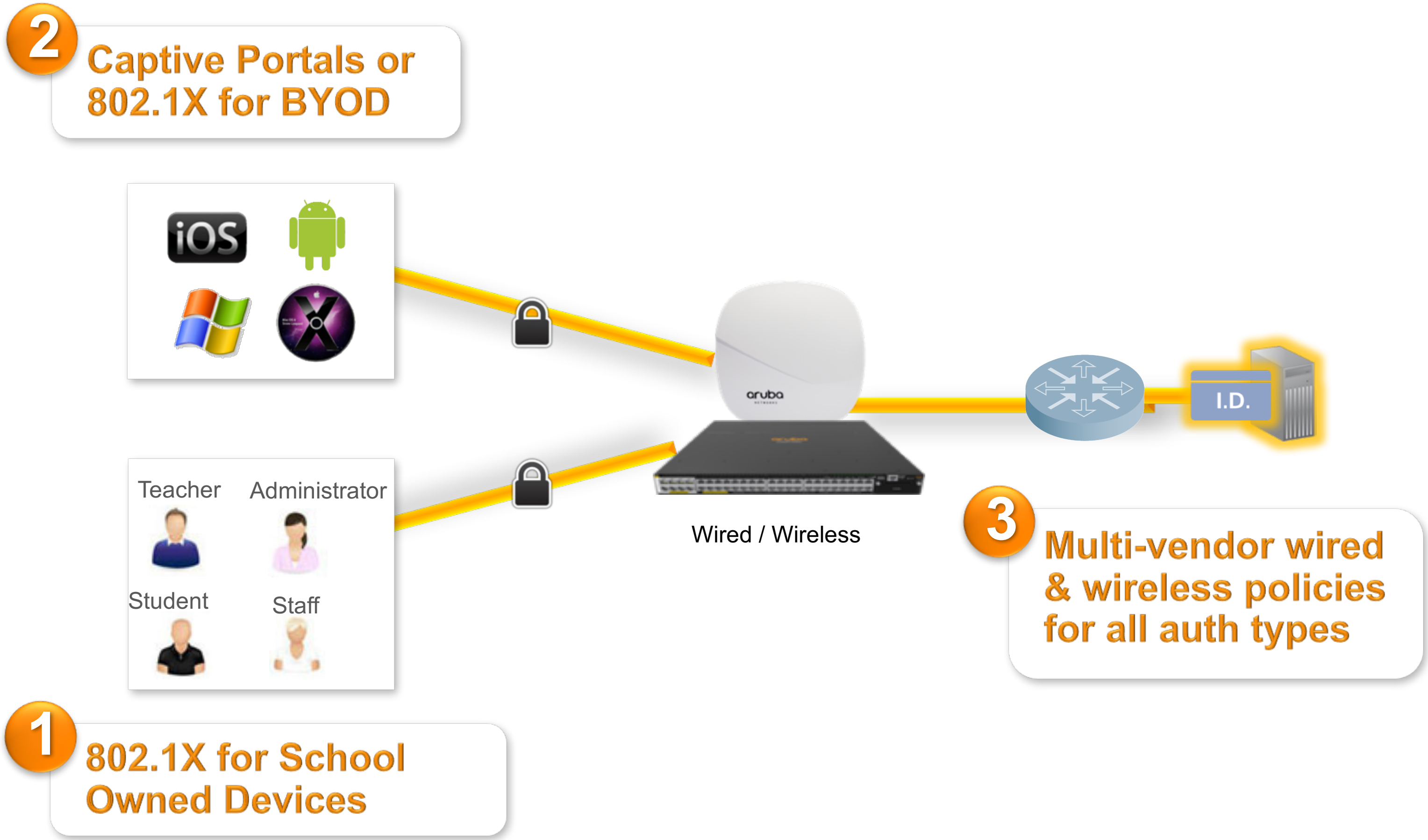
How do I:

- Maintain visibility & control?
- Deliver secure, differentiated access?
- Simplify device provisioning?

Personally Owned Devices

- School, teacher, or student owned
- Limited visibility
- Limited control

ClearPass Authentication: Easy & Secure Device Onboarding


2
Captive Portals or 802.1X for BYOD
iOS
Teacher
Administrator
Student
Staff
aruba
Wired / Wireless
I.D.
3
Multi-vendor wired & wireless policies for all auth types
1
802.1X for School Owned Devices

User and Device Access Control

School Owned Device

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet and Corporate Applications

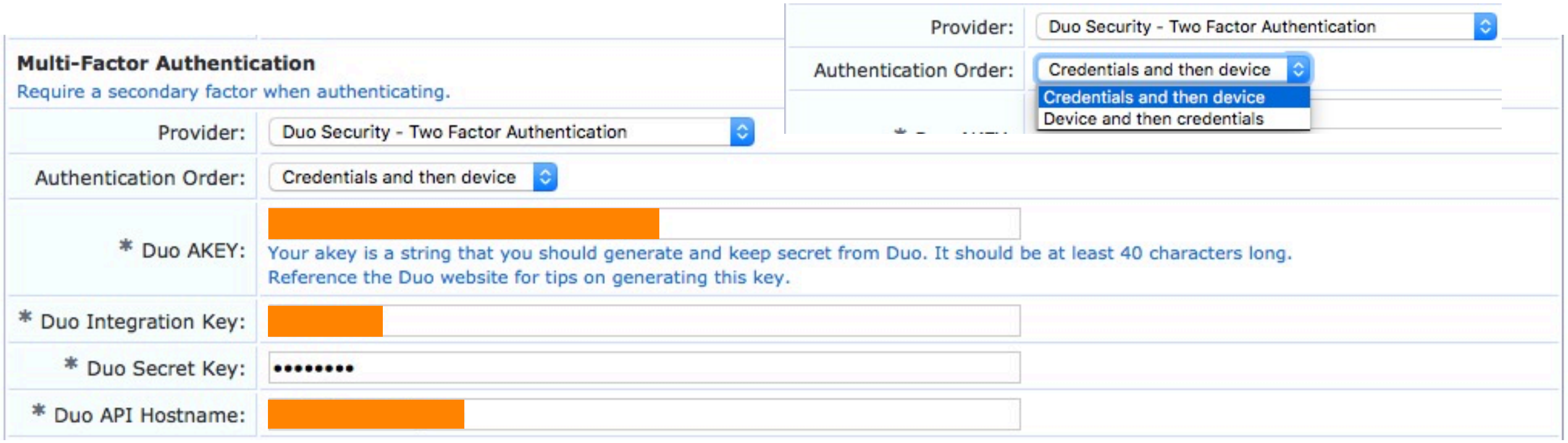
BYOD

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet

Multi-Factor Authentication



Provider: Duo Security - Two Factor Authentication

Authentication Order: Credentials and then device

Multi-Factor Authentication

Require a secondary factor when authenticating.

Provider: Duo Security - Two Factor Authentication

Authentication Order: Credentials and then device

* Duo AKEY: [redacted]

Your akey is a string that you should generate and keep secret from Duo. It should be at least 40 characters long. Reference the Duo website for tips on generating this key.

* Duo Integration Key: [redacted]

* Duo Secret Key: •••••••••

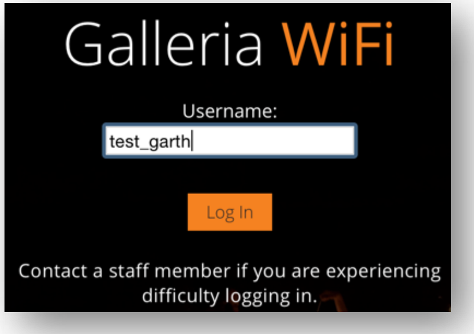
* Duo API Hostname: [redacted]

– Captive Portal Login
  – Bring MFA to captive portal logins
  – Leverage built in database or external identity stores
– Onboard Login
  – Support MFA for initial Onboarding

– Vendor Support
  – DUO
  – ZOOM
  – Imageware
  – More to come!

Multi-Factor Authentication (DUO Workflow)

Step 1 – Who are you?

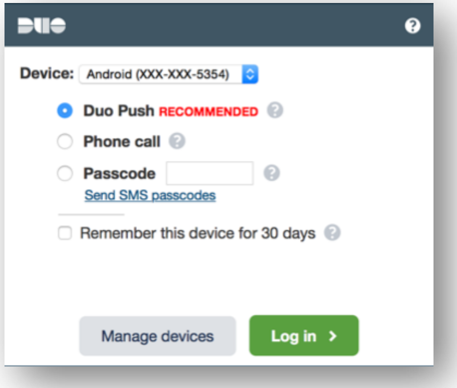


Galleria WiFi

Username: test_garth

Contact a staff member if you are experiencing difficulty logging in.

Step 2 – 1st Factor Something You Have



Device: Android (XXX-XXX-5354)

● Duo Push RECOMMENDED

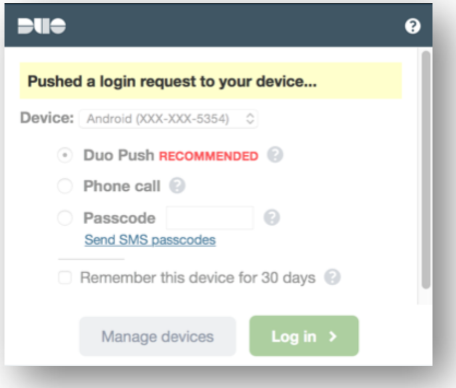
○ Phone call

○ Passcode

Send SMS passcodes

□ Remember this device for 30 days

Step 3 – Request Approval from Known Device



Pushed a login request to your device...

Device: Android (XXX-XXX-5354)

● Duo Push RECOMMENDED

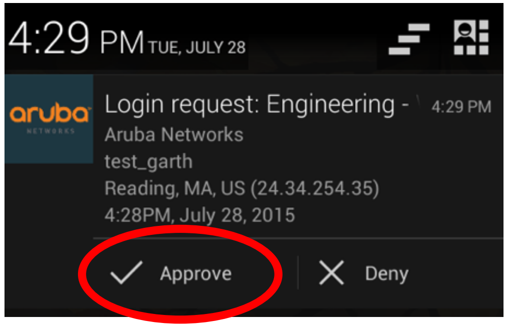
○ Phone call

○ Passcode

Send SMS passcodes

□ Remember this device for 30 days

Step 4 – Approve from Known Device



4:29 PM TUE, JULY 28

Login request: Engineering - 4:29 PM

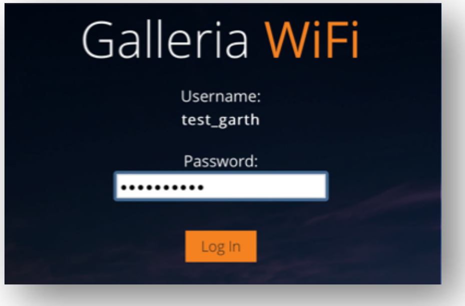
Aruba Networks

test_garth

Reading, MA, US (24.34.254.35)

4:28PM, July 28, 2015

Step 5 – 2nd Factor Something You Know

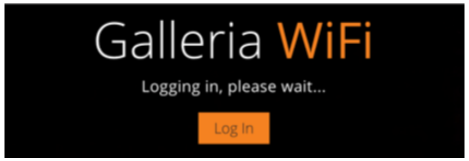


Galleria WiFi

Username: test_garth

Password: ••••••••••

Step 6 – Logging in!



Galleria WiFi

Logging in, please wait...

Why MFA?

Hackers count on people being lazy with their passwords…!!!

WiFi Passwords are shared easily

Facebook and Google do this by having users confirm authentication from their phones every time their account is accessed from an unrecognized device!!!

MFA Benefits

This requires hackers to have physical access to the accountholder's phone, which is unlikely.

Multifactor authentication is taking over as the new normal

Biggest benefits of MFA, allows organizations to use advanced security options like single sign-on, which is easier for end-users.

ClearPass OnGuard – Keeping the Enterprise Healthy

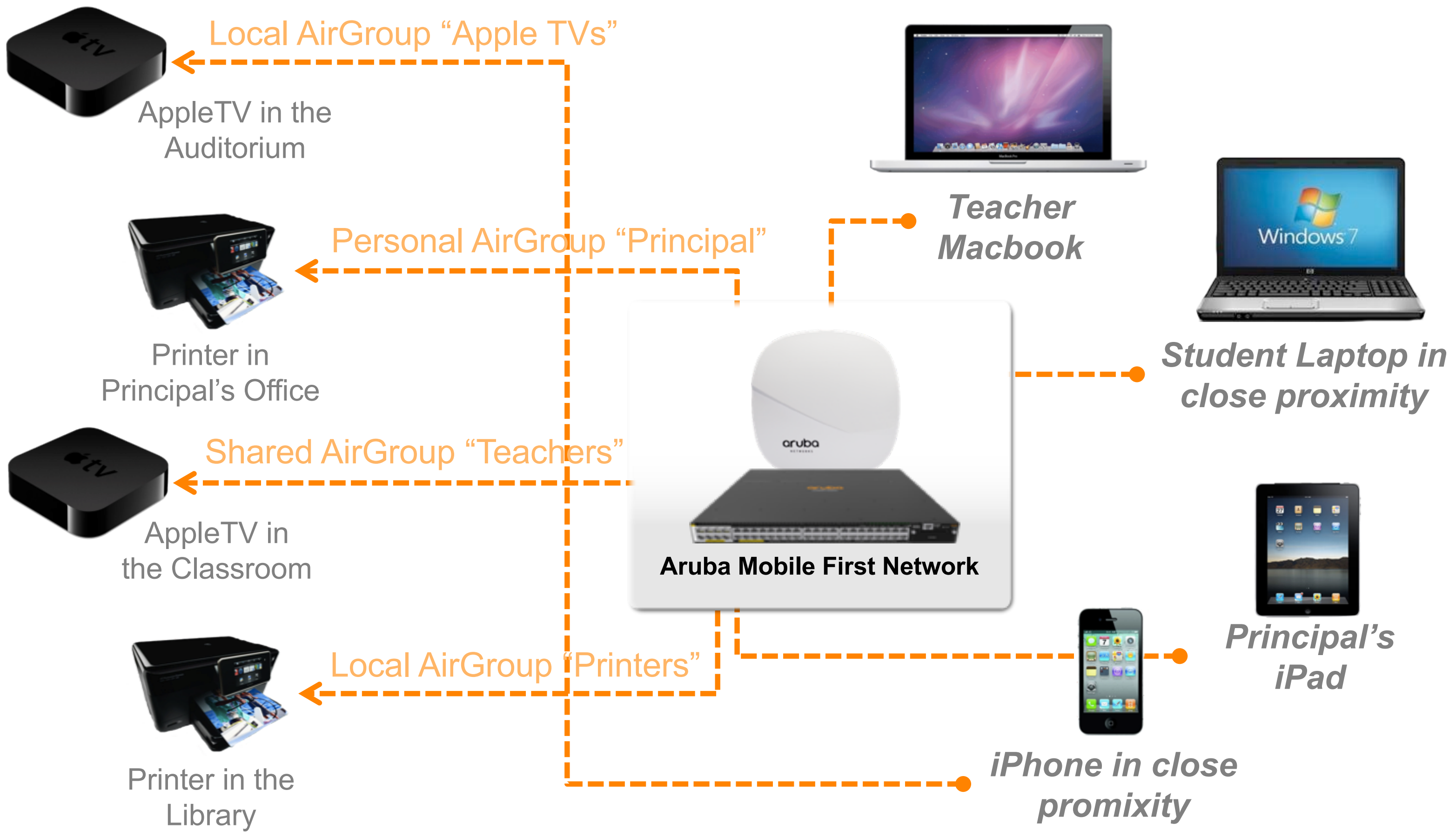
- **Automated Endpoint Compliance**
  Health checks before access. Identifies poor behavior

  Wired & Wireless Endpoints
  Ensures posture compliance for laptops/computers

- **Minimize Risk**
  Forces use of anti-virus, anti-spyware, firewalls, disk encryption

- **Remediation**
  Manual or full integration with Helpdesk solutions

Managing Bonjour With AirGroup



Local AirGroup "Apple TVs"

AppleTV in the Auditorium

Personal AirGroup "Principal"

Printer in Principal's Office

Shared AirGroup "Teachers"

AppleTV in the Classroom

Local AirGroup "Printers"

Printer in the Library

Aruba Mobile First Network

Teacher Macbook

Student Laptop in close proximity

Principal's iPad

iPhone in close promixity

Wired and Wireless
Adaptable Policy Management

Create policies that adapt to BYOD growth for staff, students, and guests

Simplify and secure IoT adoption

Customized device profiling for any uncategorized connected device

Multi-factor authentication on mobile devices for network usage

ClearPass Licensing Model

Foundation

- **HW** or **VM** appliances
- 500, 5K, 25K devices
- Appliance (AAA) capacity is measured by total, unique devices authenticated over 7 days
- **Basic Guest –** Free with Social Login
- Appliances are bundled with 25 Enterprise licenses

Clustering

- Each appliance adds capacity to the cluster but individual unit capacity cannot be exceeded
- Feature licenses are applied cluster-wide

Add Applications

- **Guest** – number of unique Guest devices PER DAY
- **Onboard** – number of unique devices onboarded or number of active certificates
- **OnGuard** – number of unique devices that will be health checked over 7 day period
- **Enterprise** – pool of licenses that can be used for any feature license; each feature used per device consumes a license; measured over 7 days

License Violation

- All counts averaged over 30 days – violation occurs when average is consistently greater than purchased amount for 4 out of 6 months
- Violation results in denied access to administrative console –**all features and functions still operate** as configured
- Subscription expiration results in stoppage of feature license functions

Special Considerations

- **High Capacity Guest** – configuration setting for Guest ONLY functionality – capacity and license measured PER DAY; appliance capacity is doubled for 5K and 25K
- **TACACS+** – counts number of unique administrative users over 7 day period

Thank You

aruba
a Hewlett Packard
Enterprise company