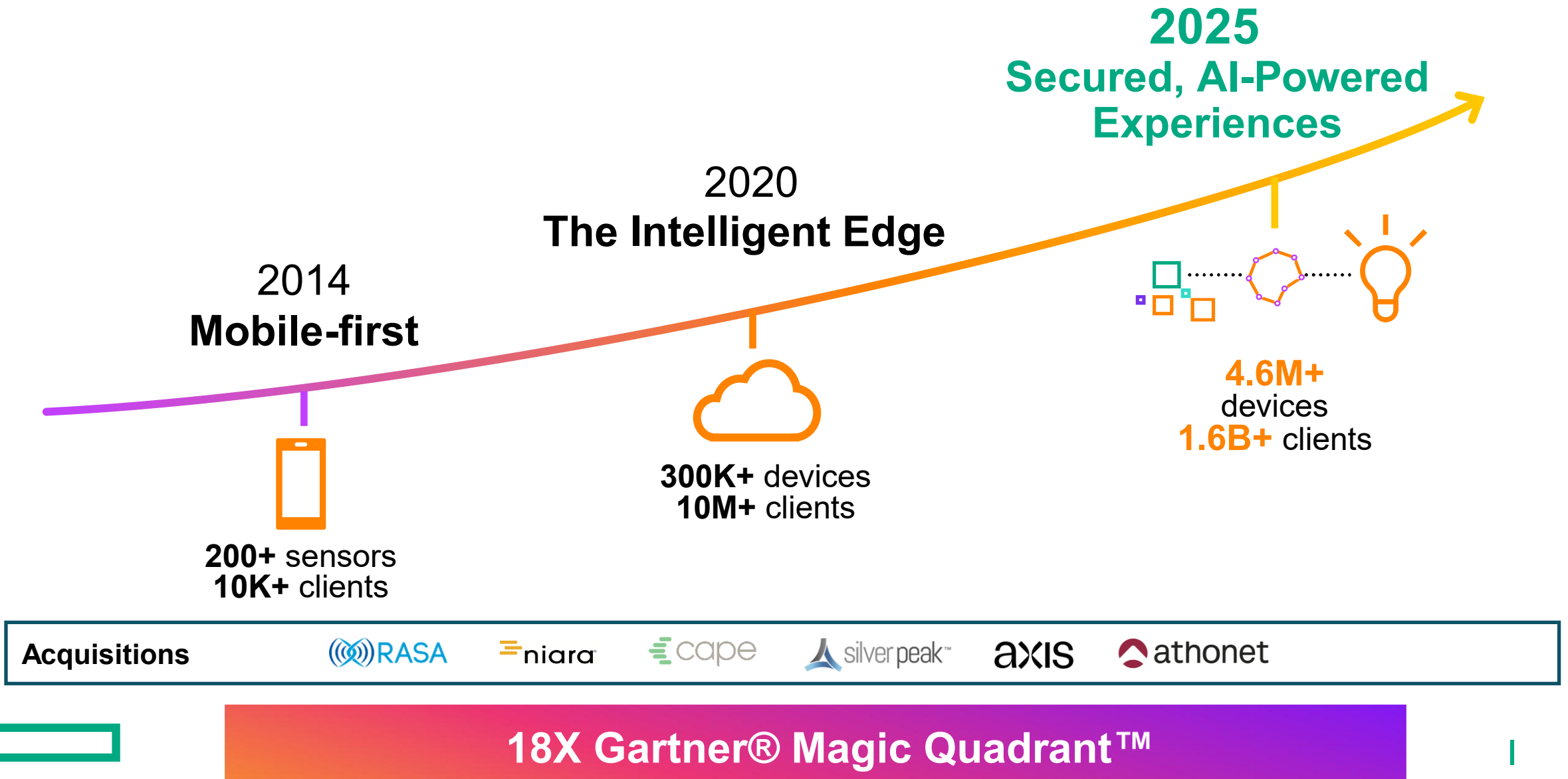




New Central Hands-on-Lab

Wendell Williams – Channel SE NYC, NJ & Eastern PA

Evolution of Central

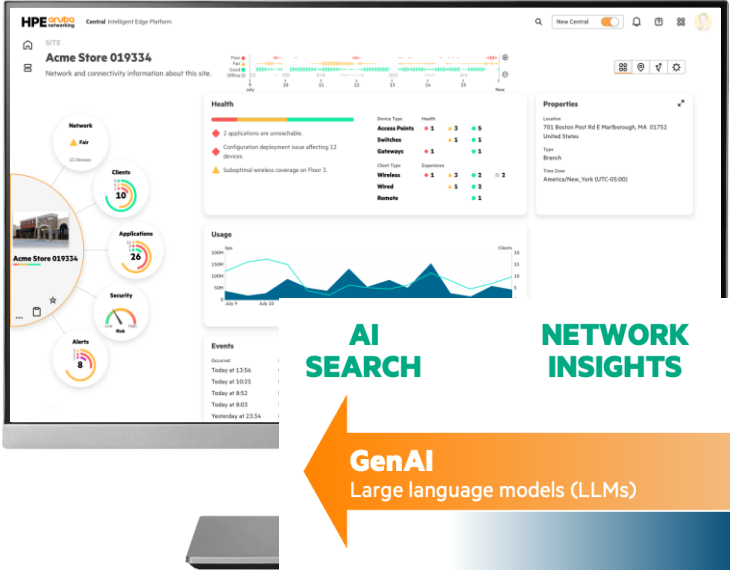


New Central: Learns from the Industry's Largest Data Lake

5M+
Devices

2B+
Clients

30+
Industry Verticals



AI
SEARCH

NETWORK
INSIGHTS

AI
ASSIST

CLIENT
INSIGHTS

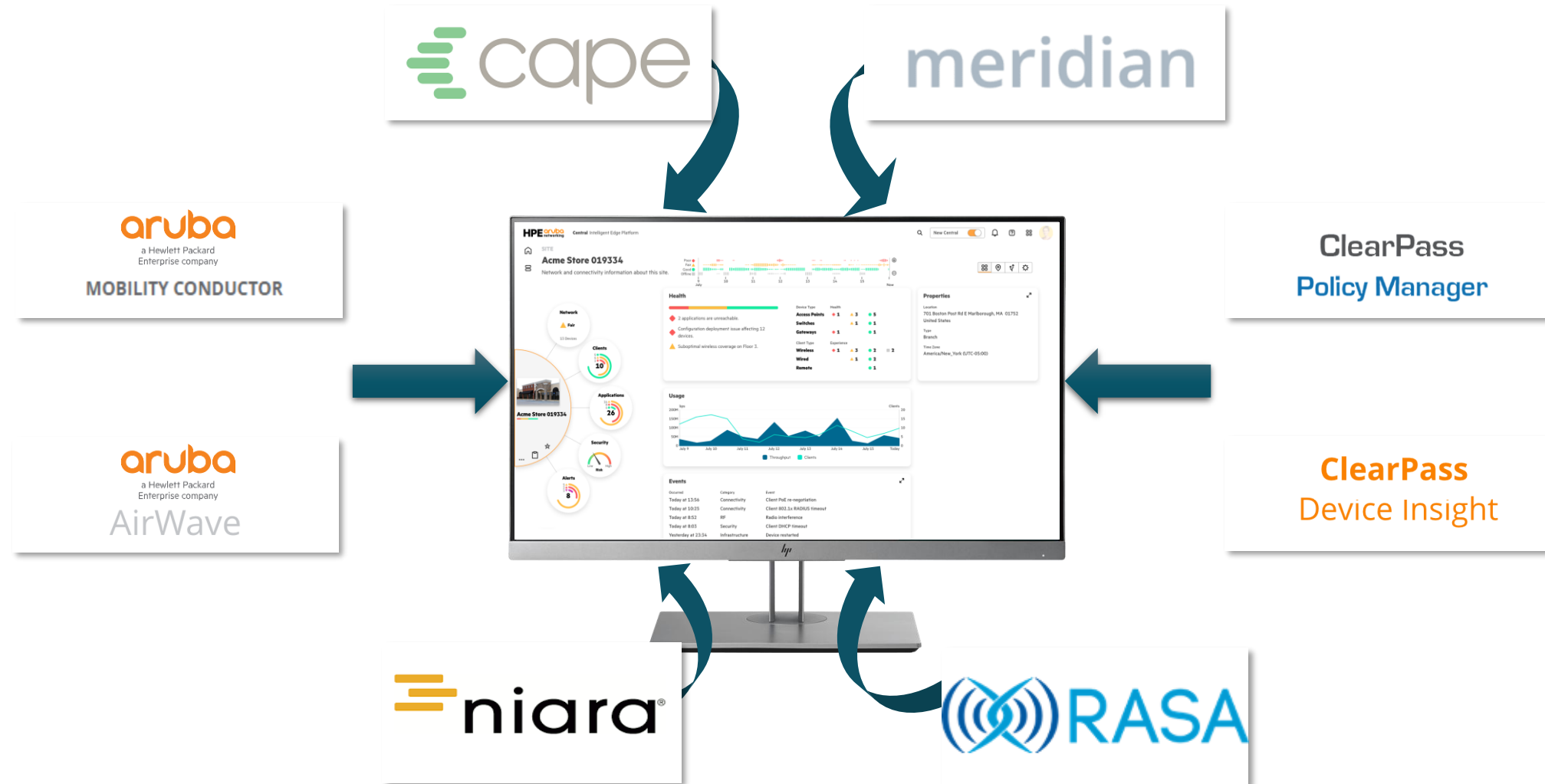
INCIDENT
DETECTION

GenAI
Large language models (LLMs)

Classification AI
Clustering, correlation, regressions...

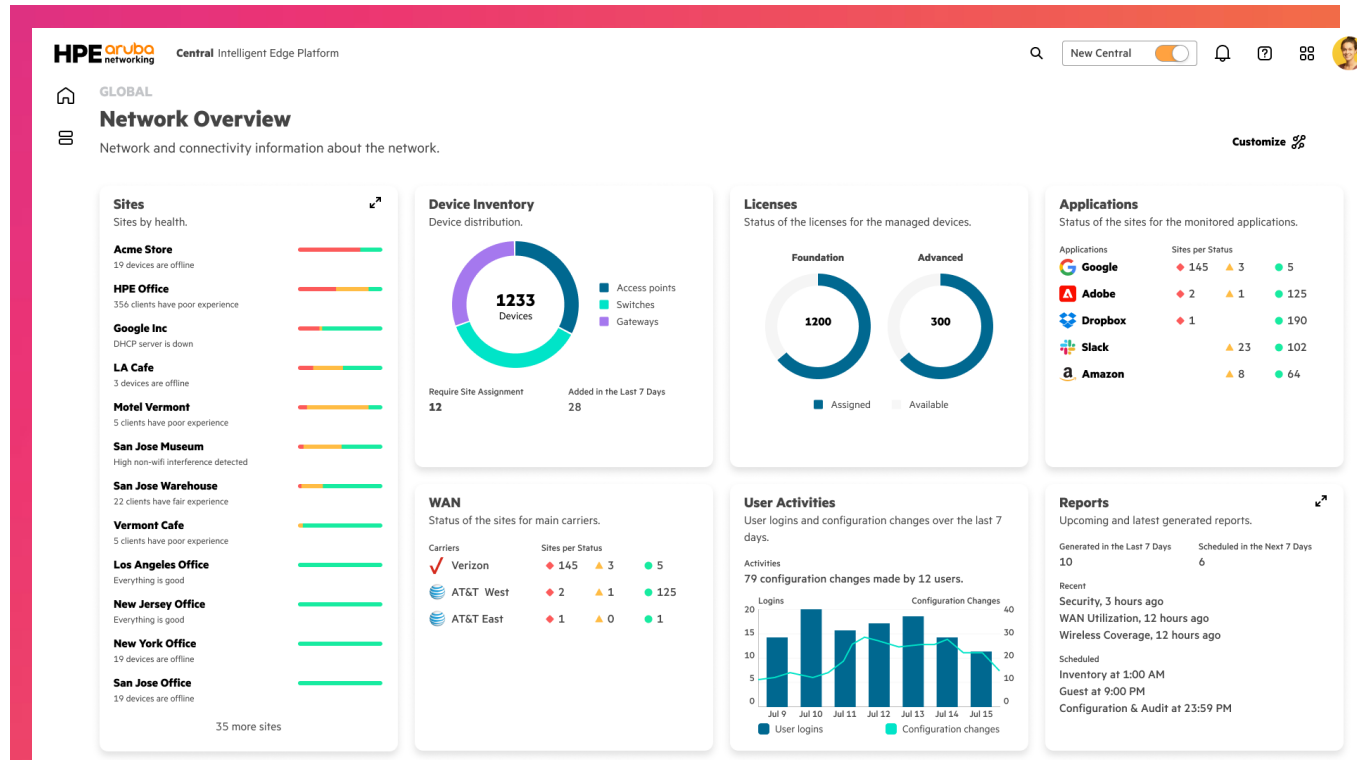


New Central: The Best From the Past and the Future



Network operations Center dashboard

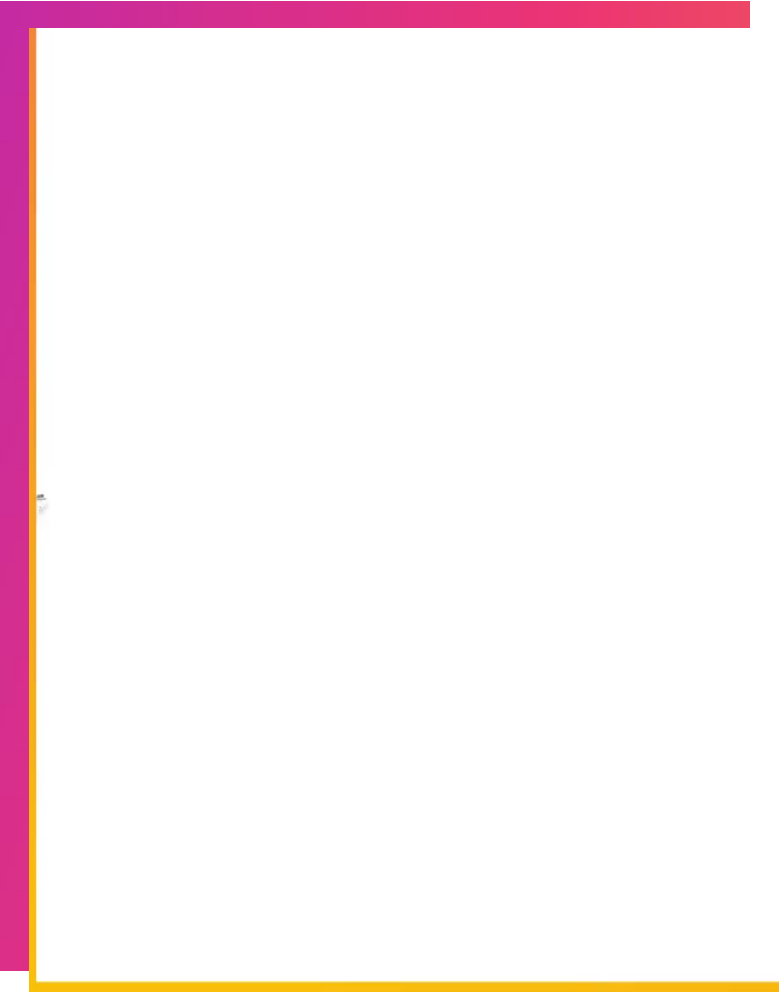
Powerful *command center* view to direct operator attention



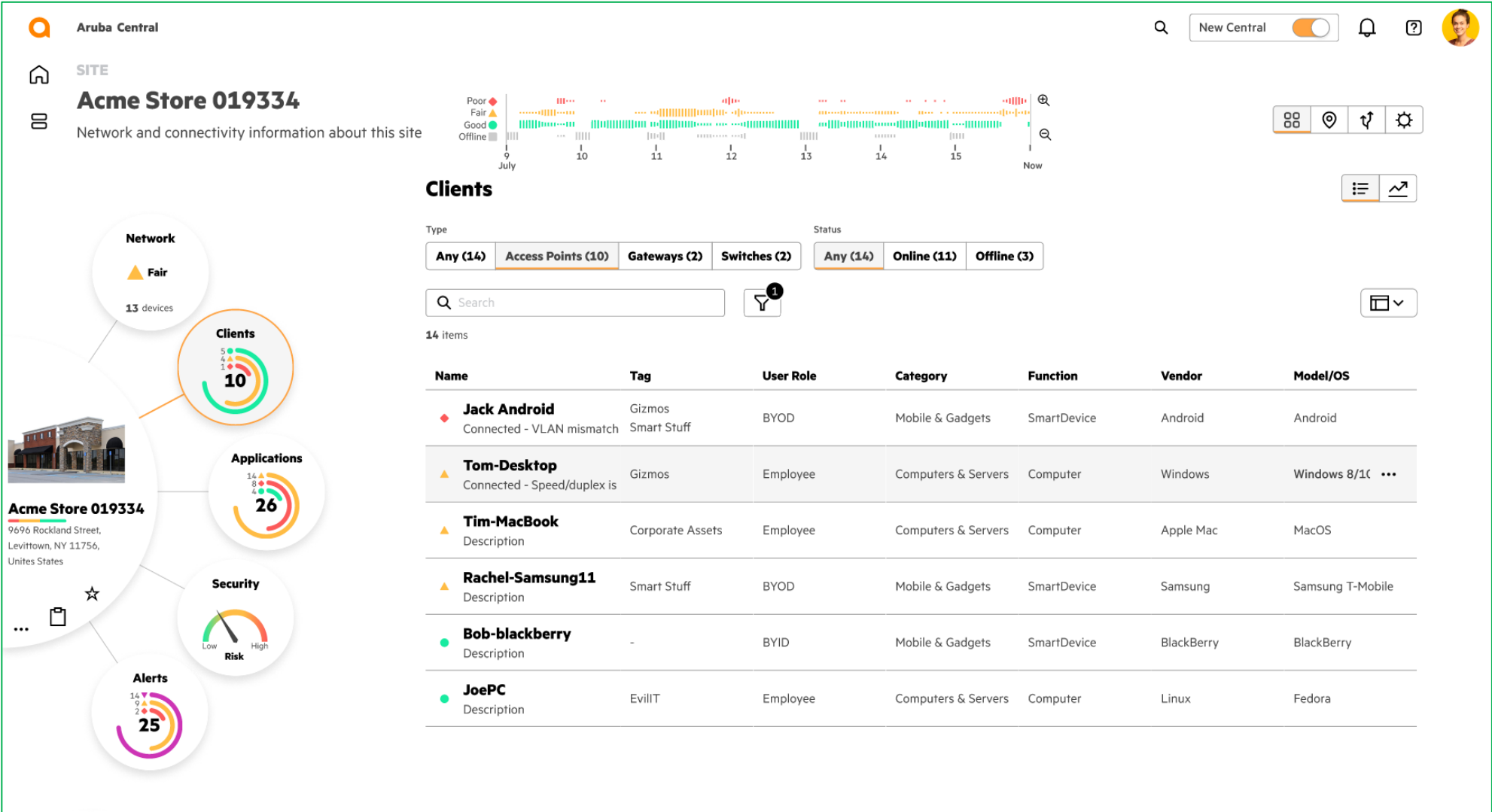
- Unified view of the network for quick assessment of site health, application experience, device inventory, and more
- Optimizing the ***to-do*** list of a network operator
- Blended indicators highlight issues requiring **immediate attention**

Entity-centric *Solar System* view

Reduce navigation clicks and minimize manual correlation

- 
- Promotes **quicker discovery** without navigating across several screens and tables
 - **Proactive summarization** with *blended* indicators
 - Seamless switching between site, network devices, clients, applications, etc.
 - Access to unified network device and client lists

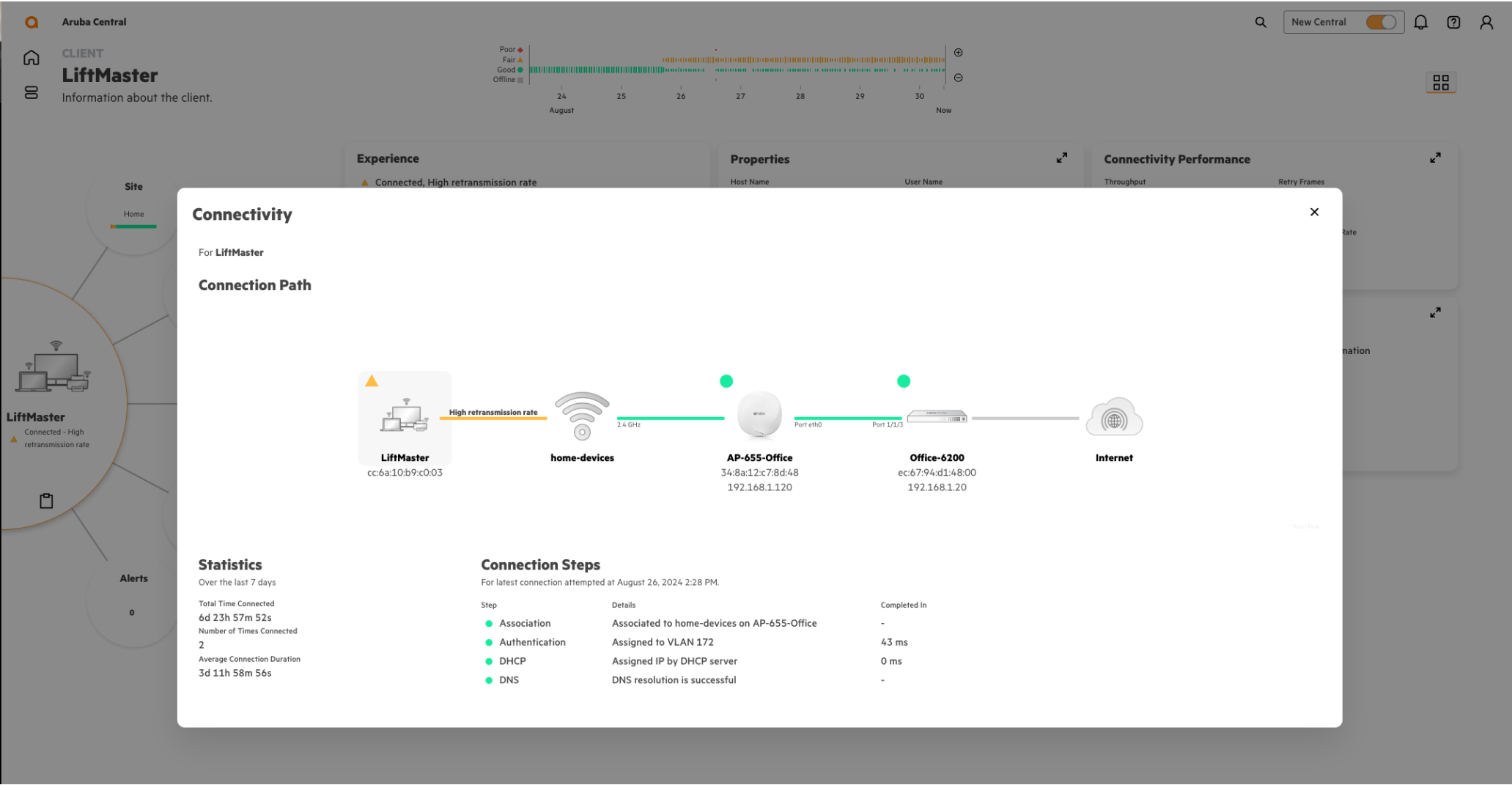
Easy to See Endpoint Client Status



Page 10

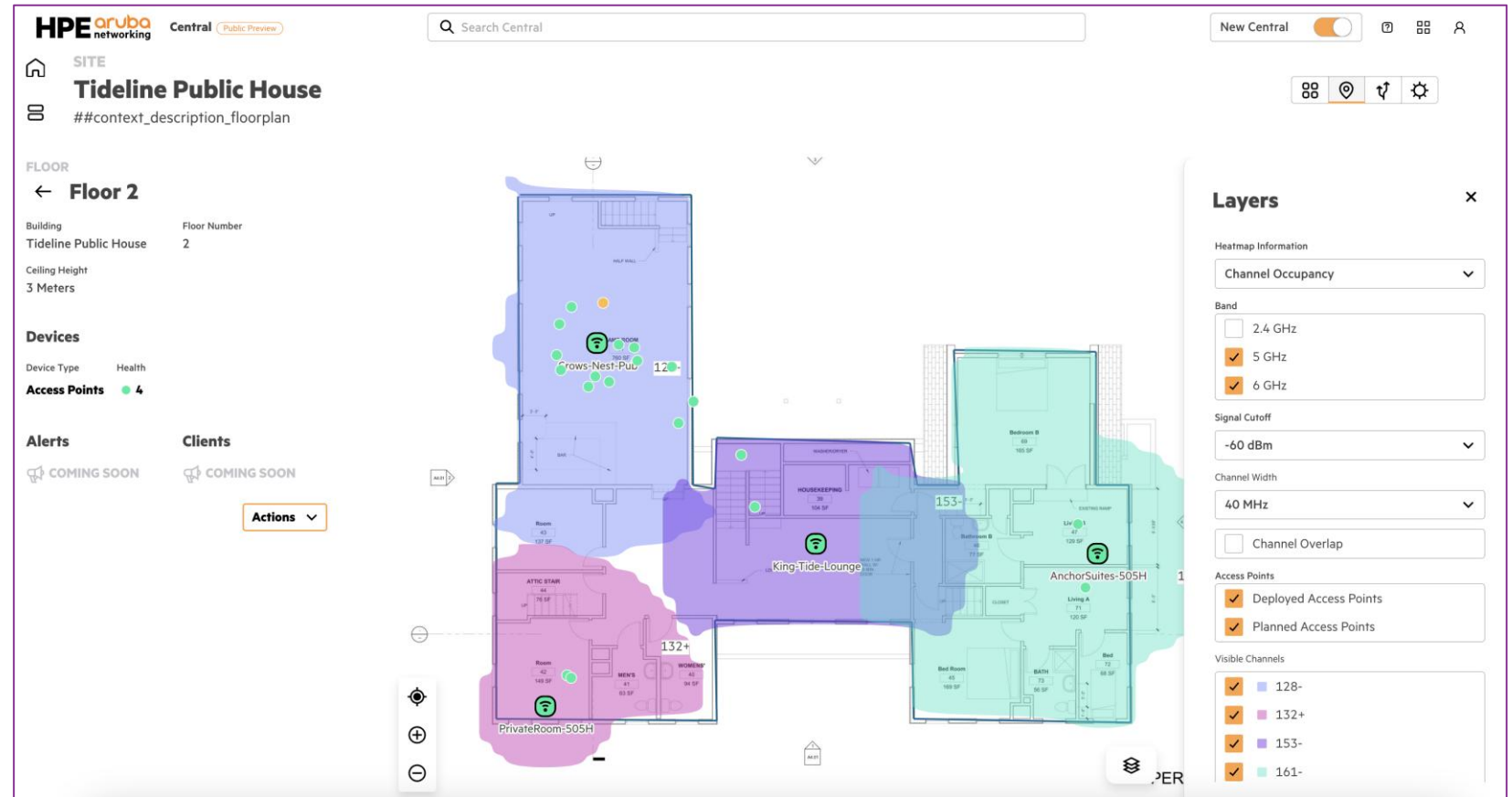
8

One-Stop Experience Views – deeper details



Enhanced Floorplan Manager

- **Auto Placement of APs**
- **Multiple Layers** – RF, Channel Occupancy, Overlap
- **Migrate from Classic Central**
- **Import** from Airwave, Ekahau, Hamina



Asset Tag Inventory and Location

- **Aruba and 3rd Party** asset tags
- **Create** custom names and labels
- **View location on floorplans**
- **Last known location and battery levels**

GLOBAL

Asset Tag Inventory

Manage wireless tags used for physical asset tracking.

ASSET TAG

Office Closet



MAC Address
cc:78:ab:9d:4c:96

Custom ID
-

Type
ArubaAssetTag

First Seen
03/19/2025, 2:28 PM

Labels
Office Tags

Battery Level
87%

Last Seen
Today at 8:35 AM

Location



1 of 4 items selected

Name	MAC Address	Classes	Labels	Battery Level	Last Known Location
Office Closet	cc:78:ab:9d:4c:96	ArubaAssetTag	Office Tags	87%	Home / Home: 1 - I
Office Desk	cc:78:ab:c6:c9:5e	ArubaAssetTag	Office Tags	97%	Home / Home: 1 - I
cc:78:ab:c6:ca:13	cc:78:ab:c6:ca:13	ArubaAssetTag	-	65%	Home / Home: 1 - I
cc:78:ab:c6:cb:0b	cc:78:ab:c6:cb:0b	ArubaAssetTag	-	79%	Home / Home: 1 - I

Troubleshooting Tools

Framework

- Tests
- Sequence
- Remote console
- Commands
- History

Troubleshoot

For Acme Store.

Tests

Sequence

Remote Console

History

Q Search

Y

59 items

ID

Initial Context

Start Time

End Time

Username

Type

Test Results

45

AP-Aruba 123

2023-12-17, 14:30:09

-

tim@hpe.com

Tests

7

2

44

San Francisco

2023-12-17, 10:45:15

2023-12-17, 11:20:06

tim@hpe.com

Tests, Sequence

18

3

43

SW-6300 Frontdesk

2023-12-16, 16:02:20

2023-12-16, 16:03:33

john@hpe.com

Sequence

4

4

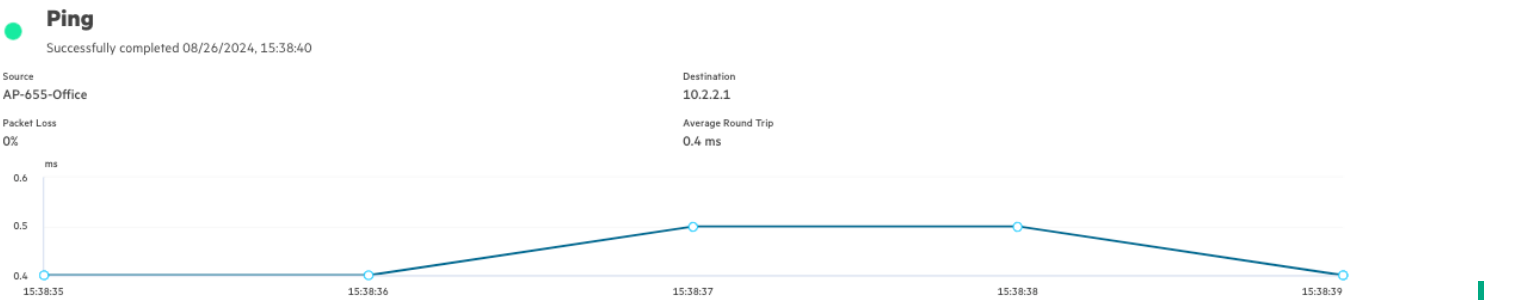
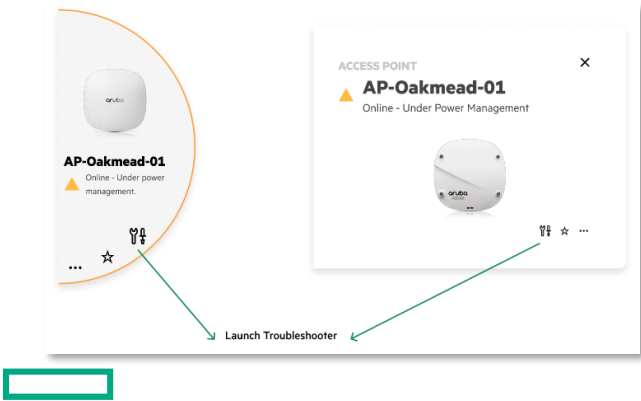
Tests

Remote Console

Visual and CLI options for test results



Multiple Entry points into the workflow



Third Party Observability with OpsRamp

Currently supported third-party switches:

- Arista
- Cisco
- Extreme
- Juniper

Customer Environment

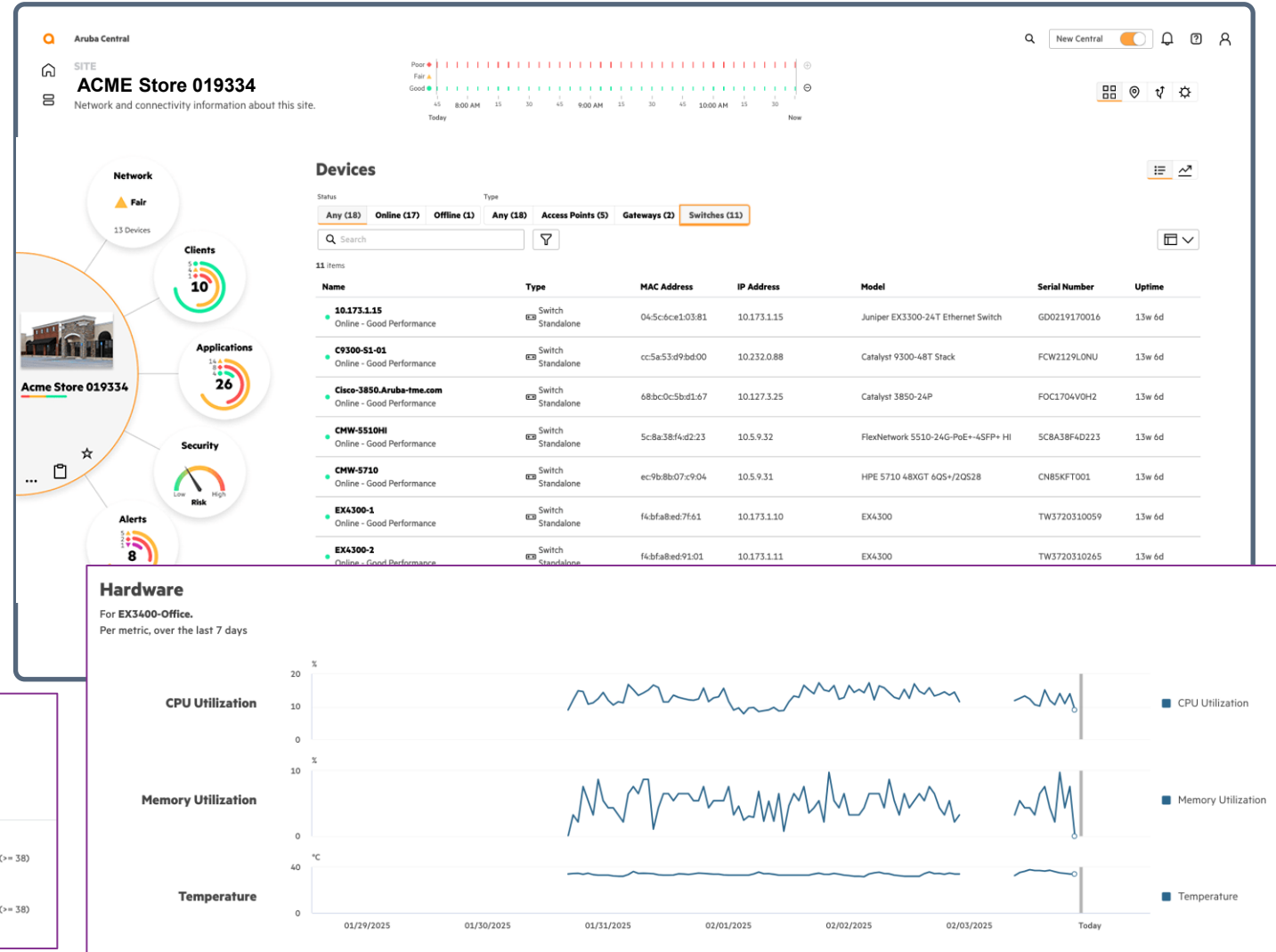
Network Infra

Storage

Servers

Collector
(VM)

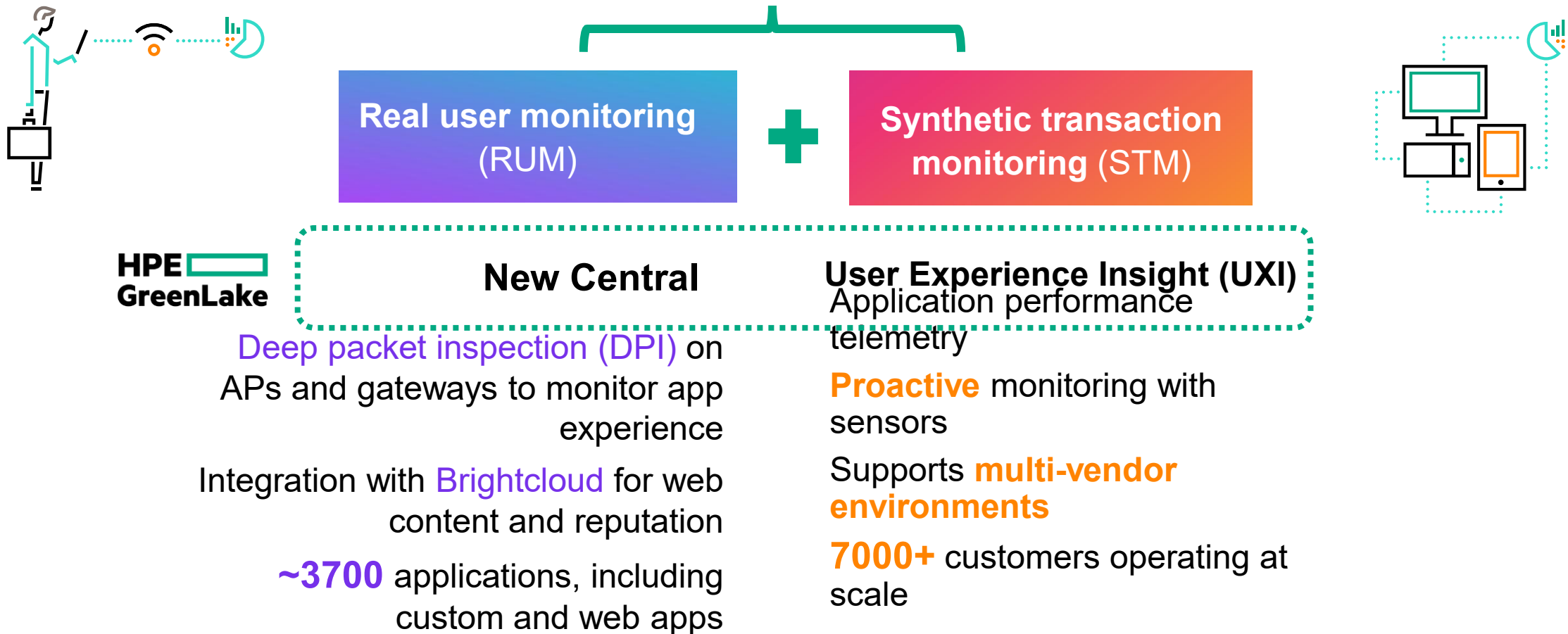
TLS



Bringing together Central and UXI

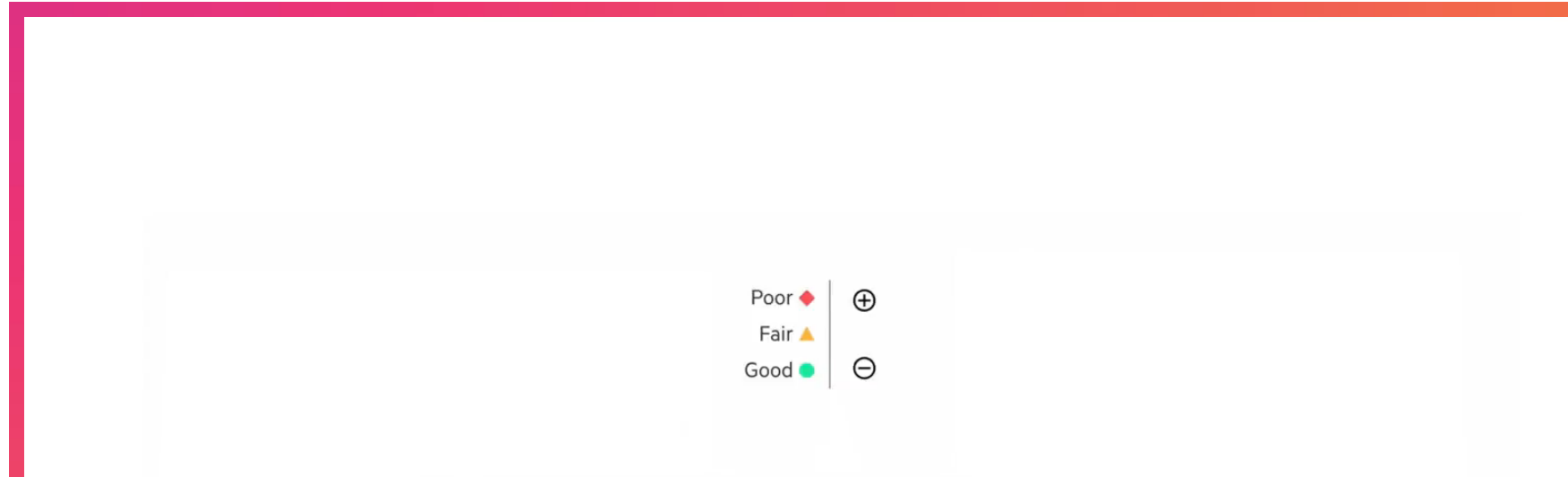
Enhanced application observability for end-to-end experience monitoring

Digital experience monitoring



Industry-first network *Time Travel*

Helping IT teams answer *What changed? When? Why?*



- Holistic **point in time** network snapshot to troubleshoot difficult issues
- Deep correlation that goes beyond manual analysis of event logs and packet captures
- Move back in time for up to **seven days**, with granularity of **one minute**
- On selecting a timestamp, all dashboard views reflect what the network looked like at that point

Gen AI powered search

Enhanced with enterprise-grade LLMs for improved operator experience

The screenshot shows the Aruba Central interface. At the top, a search bar contains the query 'How do I create a Port Profile on AOS-CX using Aruba Central?'. Below this, a 'Summary' section provides an overview of Port Profiles. A list of steps for 'Creating a Port Profile' is visible. In the foreground, a 'Search Results' window is open, showing a search for 'Catania'. The search scope is set to 'Devices'. The results table lists two items: 'GW-Catania-02-MB' (Gateway Cluster) and 'AP-Catania-01-LR' (Access Point Standalone). A blue box highlights the search bar in the search results window.

How do I create a Port Profile on AOS-CX using Aruba Central?

Summary:

Configuring Port Profiles on AOS-CX using Aruba Central

Port Profiles enable group level configuration of interface-specific commands on AOS-CX devices. Aruba Central's **Port Profiles** page allows you to manage these profiles - create, apply, clone, modify, and delete. They can be configured on interface ranges, list of interfaces, wild cards, MCLAG, split, sub-interface, and management interfaces. Please note, the configuration should be complete when applying a profile to an interface. The new profile will overwrite the existing configuration.

Creating a Port Profile

1. Launch the **Aruba Central** app, and set the filter to a group that contains at least one switch.
2. Navigate to **Devices > Switches** under the **Manage** section.
3. Click on the **Config** icon to access the switch configuration dashboard.
4. Navigate to **Interfaces > Port Profiles**. Here you'll see a list of existing port profiles.
5. Click on the + sign in the Port Profiles table to create a new profile.
6. Provide a **Name** and a **Description** for your profile.
7. Configure in
8. Click **Save** to

Important Considerations

- The parent group
- Overlapping
- When creating
- Before applying
- Post application

Show more

Aruba Central

Q devices running 10.4

Search Results

Search Scope

Catania

Devices Documentation

2 Items

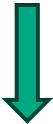
Name	Type	MAC address	IP Address	Model	Serial Number
GW-Catania-02-MB ONLINE	Gateway Cluster	20:4c:03:d3:11:f8	9.9.9.1	A9004	CNMHKL8032
AP-Catania-01-LR ONLINE - Last seen -	Access Point Standalone	90:4c:81:c0:53:14	10.1.50.3	AP-345	CNFKY510L2

- Trained and tuned on **multiple proprietary LLMs**, purpose-built for networking
- Pre-conditioned with 3 million network questions for improved performance and accuracy
- **Sub-second summarization** of latest 30k pages of VRDs and tech pub documents
- **Uncompromised security** with no external API interfaces, and no PII/CII shared beyond customer instance

Agentic AI Enhances Search

Show me how to map a VLAN between AP and the Gateway

Summarize new features in AOS-10 release



Show me how to @map a VLAN between AP and the Gateway

Thought for 11 seconds

New Features in AOS-10.7.2.0

AOS-10.7.2.0 introduces several new features and enhancements to improve network performance and management capabilities. Here's a summary of what's new in this release:

New Features

- **Split Image Firmware Upgrade**
 - Introduced for select AP models
 - Consists of a base image and an extension image
 - For more information, refer to Managing Firmware Upgrades documentation

Enhancements

- **DHCP Reservation Limit**
 - Increased from 64 to 256 for devices running AOS-10.7.2.0 or higher
 - Note: Devices running lower AOS-10 versions might experience issues with the increased reservation value
- **Enhanced show tech-support CLI Command**
 - Now includes AP information and associated configuration details
 - Added multiple debug commands for better troubleshooting including:
 - Zigbee radio and client tables
 - IoT USB device information

Thought for 11 seconds

Mapping VLANs Between Aruba APs and Gateways

When configuring Aruba networks, properly mapping VLANs between Access Points (APs) and Gateways is essential for ensuring proper traffic flow and network segmentation. Here's how to establish this mapping:

AP VLAN Configuration

1. **Create AP Groups**
 - First, create an AP group to support wireless service in your branches
 - AP groups allow you to apply consistent VLAN configurations across multiple APs
2. **Configure VLAN Trunk Settings**
 - For APs that will tunnel traffic to gateways, configure the port-access role to allow specific VLANs:

```
port-access role ARUBA-AP auth-mode device-mode
vlan trunk native 100
vlan trunk allowed 100,101,104-107
```
 - This example shows a configuration where VLAN 100 is the native VLAN, and VLANs 100, 101, and 104-107 are allowed on the trunk

Gateway VLAN Configuration

1. **Create VLANs on the Gateway**
 - Navigate to the Gateway configuration interface
 - Select the LAN tab and then VLANs
 - Create the necessary VLANs that will be mapped to the AP traffic

Enter a prompt here



Agentic AI: Create a custom workflow

What are the specific commands to upgrade APs using the 'ap convert' command?

How should I upgrade from AOS8 to AOS10

Migrating from AOS 8 to AOS 10 requires careful planning and execution due to significant architectural changes. This guide outlines the key considerations and steps for a successful migration.

Prerequisites

Before beginning the migration process, ensure the following prerequisites are met:

- **Controller Requirements:**
 - Associated gateway must be running AOS 8.10.0.12, 8.12.0.1, or later release
 - If using AOS 8.10 prior to 8.10.0.5, avoid using SCP for image transfer as it will result in incorrect permissions
 - If using AOS 8.10 prior to 8.10.0.11 with CPSec enabled, be aware that pre-validation operations may fail
- **Knowledge Requirements:**
 - Familiarity with AOS 10 architecture is essential for successful migration
 - Review recommended resources including:
 - HPE Aruba Networking Central Help
 - Architectural Overview of AOS 10
 - Validated Solution Guides for Campus WLAN architecture and deployment

Planning Considerations

Architectural Changes

- **Management Platform Change:** AOS 10 requires HPE Aruba Networking Central for operation and management of APs and Gateways
- **Configuration Recreation:** The entire AOS 8 configuration must be recreated in Central before upgrading devices to AOS 10

Testing Recommendation

- Test the migration process in a lab or controlled environment before implementing in production
- Ensure all steps are understood and work properly in a test environment

Migration Process

Step 1: Plan Your Configuration

- Create a detailed plan for AOS 10 configuration in Central before upgrading any devices
- Review each layer of your network against migration guidelines

Step 2: Upgrade Test AP First

1. Select a test AP for initial migration
2. Upgrade using the appropriate `ap convert` command
3. Verify successful conversion by checking LLDP neighbor information from the switch:
 - AOS 8 APs appear as "CAP"
 - AOS 10 APs display as "IAP"
4. Perform standard client testing procedures to ensure functionality

Step 3: Upgrade Remaining APs

After successful testing, proceed with upgrading the remaining APs using the same process with other `ap convert` command options (e.g., `all-aps`, `ap-group`)

Post-Migration Considerations

Authentication Updates

- Update NAD/RADIUS client IP lists on all RADIUS servers to ensure uninterrupted 802.1X WLAN client authentications
- Prepare for changes if using Internal Authentication Server or EAP-Offload

Troubleshooting



AOS8 to AOS10 AP Convert Command Syntax

The `ap convert` command is used to migrate controller-managed APs from AOS 8 to AOS 10. This command facilitates the conversion process and allows for management through Aruba Central.

Basic Command Structure

```
ap convert
  active {all-aps|specific-aps}
  add {ap-group|ap-name}
  cancel
  clear-all
  delete {ap-group|ap-name}
  pre-validate {all-aps|specific-aps}
```

Command Parameters

Parameter	Description
active {all-aps specific-aps}	Convert active Campus AP or Remote AP to Instant APs managed by Aruba Central
add {ap-group ap-name}	Add AP group or AP name to the list for AP conversion
cancel	Cancel conversion (APs currently downloading will continue)
clear-all	Remove all AP groups and AP names from the conversion list
delete {ap-group ap-name}	Delete AP group or AP name from the conversion list
pre-validate {all-aps specific-aps}	Pre-validate the Campus AP or Remote AP connection to Aruba Activate or Central

Command Examples

Adding APs to Conversion List

```
(host) [mynode] #ap convert add ap-group
```

Or for individual APs:

```
(host) [mynode] #ap convert add ap-name
```

Pre-validating APs

```
(host) [mynode] #ap convert pre-validate specific-aps
```

Checking Conversion Status

```
(host) [mynode] #show ap convert-status
```

Converting APs Using Different Methods

Using HTTP server:

```
(host) [mynode] #ap convert active specific-aps server http common.cloud.hpe.com path ccssvc/ccs-system-firmware-registry/IAP <img>
```

Using SCP server:

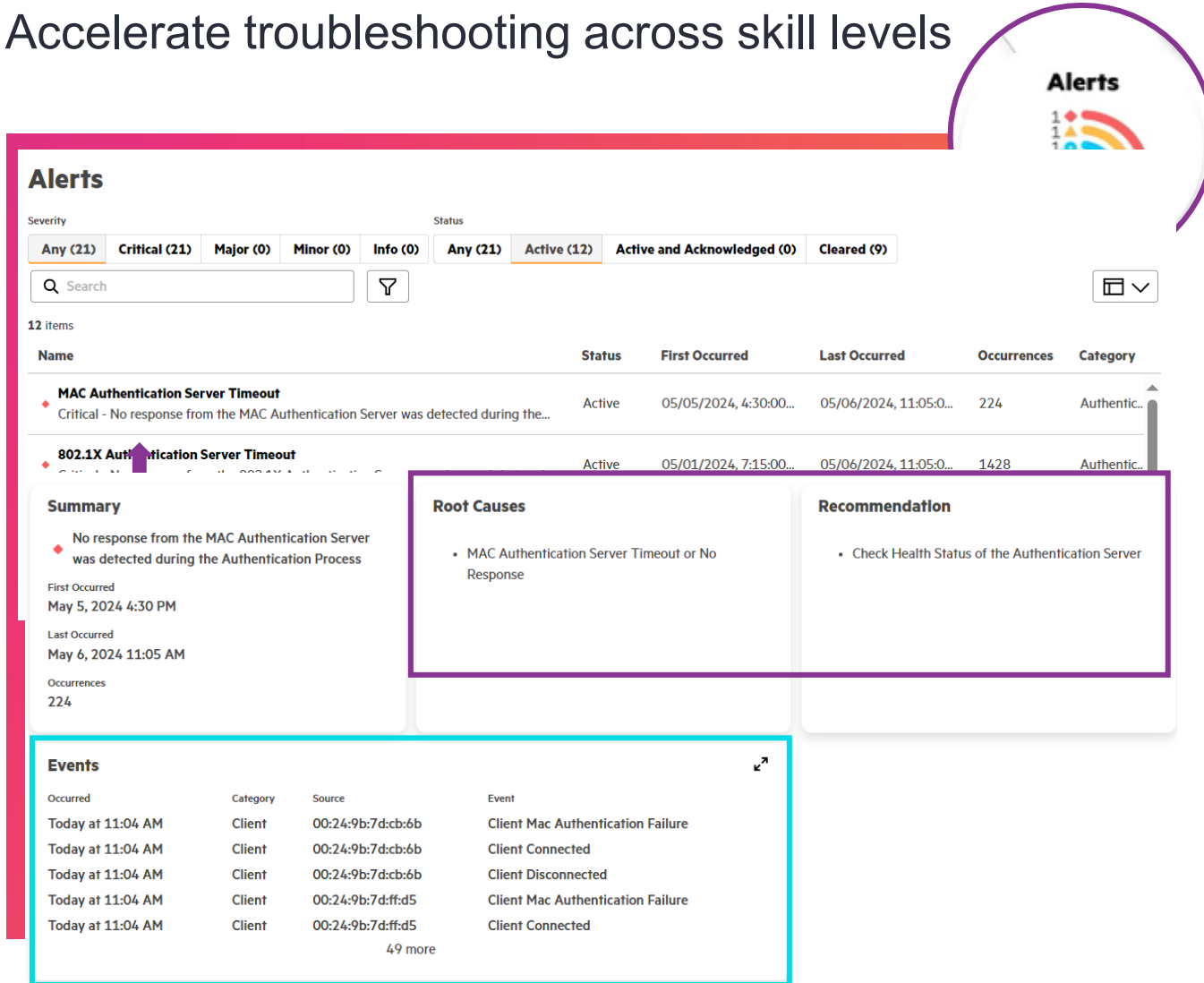
```
(host) [mynode] #ap convert active specific-aps server scp username <img>
```

Using local flash:

```
(host) [mynode] #ap convert active specific-aps local-flash ImageFile.tar
```

AI-driven assurance and alerts

Accelerate troubleshooting across skill levels



The screenshot shows an 'Alerts' dashboard. At the top, there's a search bar and filters for Severity (Any, Critical, Major, Minor, Info) and Status (Any, Active, Active and Acknowledged, Cleared). Below this is a table of 12 items. The first item is 'MAC Authentication Server Timeout' (Critical, Active, 224 occurrences). The second item is '802.1X Authentication Server Timeout' (Active, 1428 occurrences). A purple box highlights the details for the second item, showing a 'Summary' (No response from the MAC Authentication Server was detected during the Authentication Process), 'Root Causes' (MAC Authentication Server Timeout or No Response), and 'Recommendation' (Check Health Status of the Authentication Server). A cyan box highlights the 'Events' section below, showing a list of events with columns for Occurred, Category, Source, and Event. The events include 'Client Mac Authentication Failure', 'Client Connected', and 'Client Disconnected'.

Alerts

Severity: Any (21) Critical (21) Major (0) Minor (0) Info (0) Status: Any (21) Active (12) Active and Acknowledged (0) Cleared (9)

Search: [Search] [Filter]

12 items

Name	Status	First Occurred	Last Occurred	Occurrences	Category
MAC Authentication Server Timeout Critical - No response from the MAC Authentication Server was detected during the...	Active	05/05/2024, 4:30:00...	05/06/2024, 11:05:00...	224	Authentic...
802.1X Authentication Server Timeout No response from the MAC Authentication Server was detected during the Authentication Process	Active	05/01/2024, 7:15:00...	05/06/2024, 11:05:00...	1428	Authentic...

Summary

No response from the MAC Authentication Server was detected during the Authentication Process

First Occurred
May 5, 2024 4:30 PM

Last Occurred
May 6, 2024 11:05 AM

Occurrences
224

Root Causes

- MAC Authentication Server Timeout or No Response

Recommendation

- Check Health Status of the Authentication Server

Events

Occurred	Category	Source	Event
Today at 11:04 AM	Client	00:24:9b:7d:cb:6b	Client Mac Authentication Failure
Today at 11:04 AM	Client	00:24:9b:7d:cb:6b	Client Connected
Today at 11:04 AM	Client	00:24:9b:7d:cb:6b	Client Disconnected
Today at 11:04 AM	Client	00:24:9b:7d:ff:d5	Client Mac Authentication Failure
Today at 11:04 AM	Client	00:24:9b:7d:ff:d5	Client Connected

49 more

- **Event-to-insight in <5 minutes** with near real-time alerts, speeding up MTTR
- **Full-stack correlation** with precise root-cause, recommendation and impact
- Reduced alert fatigue with consolidated list of triggered events
- Assurance indicators for device health and client experience for quick diagnosis

New Central Alerts Overview

Alerts

Severity

Critical (195) Major (1) Minor (5) Info (0) Active (19) Deferred (0) Cleared (182)

19 Items

Name	Priority	Status	First Occurred	Last Occurred	Occurrences	Category
WPA Passphrase is Incorrect	Medium	Active	09/28/2024, 1:45:00 AM	10/21/2024, 5:35:00 PM	6711	Authentication
DHCP Discover Timeout	Medium	Active	10/19/2024, 5:05:00 AM	10/21/2024, 5:30:00 PM	688	DHCP
Loop Detected	Critical	Active	Critical - A loop was detected between switches.			
Switch Interface Tx Rate	Critical	Active	Critical - Switch BO-MIAI-EGSW03's transmit rate for interface 1/1/16 was above 90% for 30 minutes			

Summary

Client did not receive a response to its DHCP Discovery broadcast packet.

First Occurred

October 19, 2024 5:05 AM

Last Occurred

October 21, 2024 5:30 PM

Occurrences

688

Priority

Medium

Impact

Clients 2% (1/68)

Switches No impact

Access Points 13% (1/8)

Gateways No impact

Action

Root Cause

Response to DHCP Discover message is not received from the server

Affected VLAN(s): 101

Affected SSID(s): AnyCorpInc-MIA-1x

Affected Server(s): 10.129.192.1

Action

Currently additional troubleshooting information is unavailable. SSID is configured as an overlay network with tunnels from the Access Point to the Gateway

Troubleshooting

Steps

1 VLAN Configuration Check

2 Traceroute

3 Other IP Allocations Successful in Same VLAN

4 Ping Check

Result

190+ alert types and more coming!

Automated troubleshooting steps

5-minutes to generate

Custom alerts on any KPI

Root cause recommended action*

20

New Central Alerts - enables faster troubleshooting

Site

Miami (MIA) - Branch

Network

Good

BO-MIA-AP01

Applications

0

Security

Alerts

1

Summary

802.1X authentication server 10.127.195.1 on WLAN MIA-1X did not respond within 5 seconds.

First Occurred

May 2, 2025 3:40 AM

Last Occurred

May 2, 2025 4:20 AM

Occurrences

9

Duration

45m

Priority

Very High

Impact

Clients

5% (11/220)

Switches

No impact

Access Points

50% (3/6)

Gateways

No impact

Actions

Root Cause

Potential connectivity issues from APs to the gateway affect the entire deployment

Affected server: 10.127.195.1

Affected SSID: MIA-1X

Actions

1. Verify VLAN configs on APs and upstream switches

2. Check firewall rules between APs and gateway

3. Ensure routing between APs and gateway has no issues

4. Investigate potential link or route flap issues between APs and gateway

Root Cause

Potential connectivity issues from the gateway to the 802.1X server affect the entire deployment

Affected server: 10.127.195.1

Affected SSID: MIA-1X

Actions

1. Verify VLAN configs on gateway and upstream switches

2. Check firewall rules between gateway and 802.1X server

3. Ensure routing between gateway and 802.1X server has no issues

4. Investigate potential link or route flap issues affecting connectivity

Troubleshooting

Tests

Ping Server Check 10.127.195.1

Overall Impacted Clients for the Customer

6

4

2

0

20:00

0:00 Today

Alerts

Severity

Critical (33)

Major (8)

Minor (10)

Info (0)

Active (1)

Deferred (0)

Cleared (50)

Search

1 item

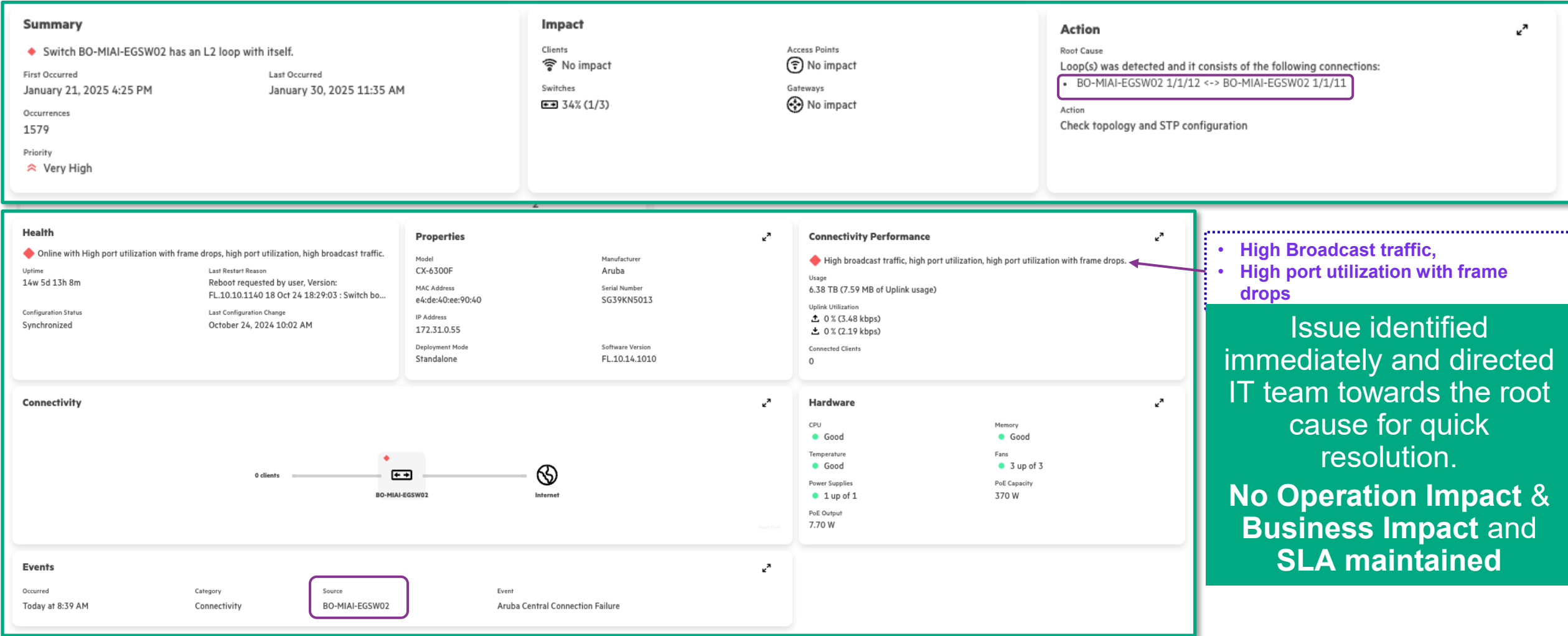
Name	Status	First Occurred	Last Occurred	Occurrences	Duration	Category	Device
802.1X Server Timed Out	Active	05/02/2025, 3:40:00 AM	05/02/2025, 4:15:00 AM	8	40m	Client	Access Point

Granular Root Cause & LLM generated Action

Automated Troubleshooting Steps*

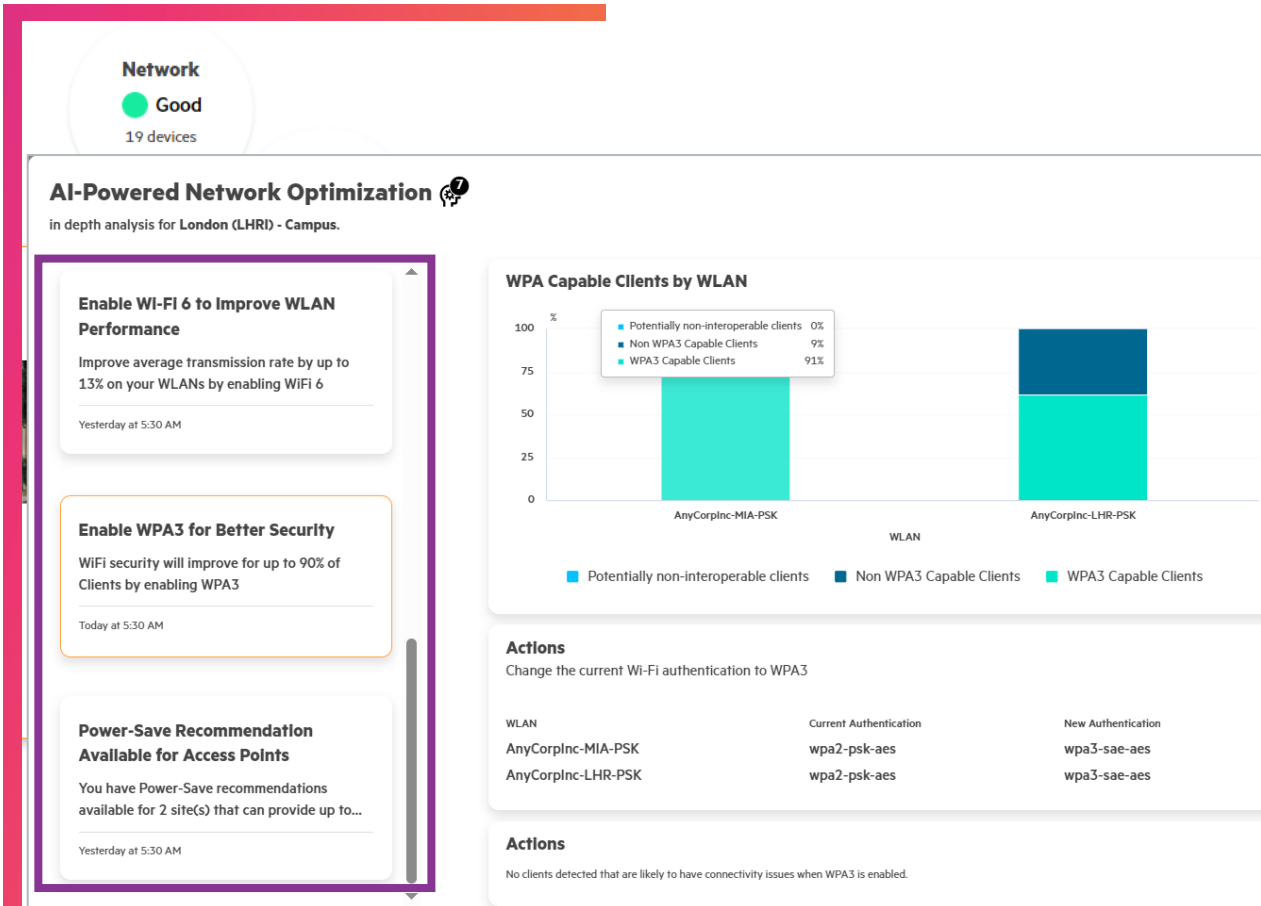
21

New Central Alerts – Loop Detection



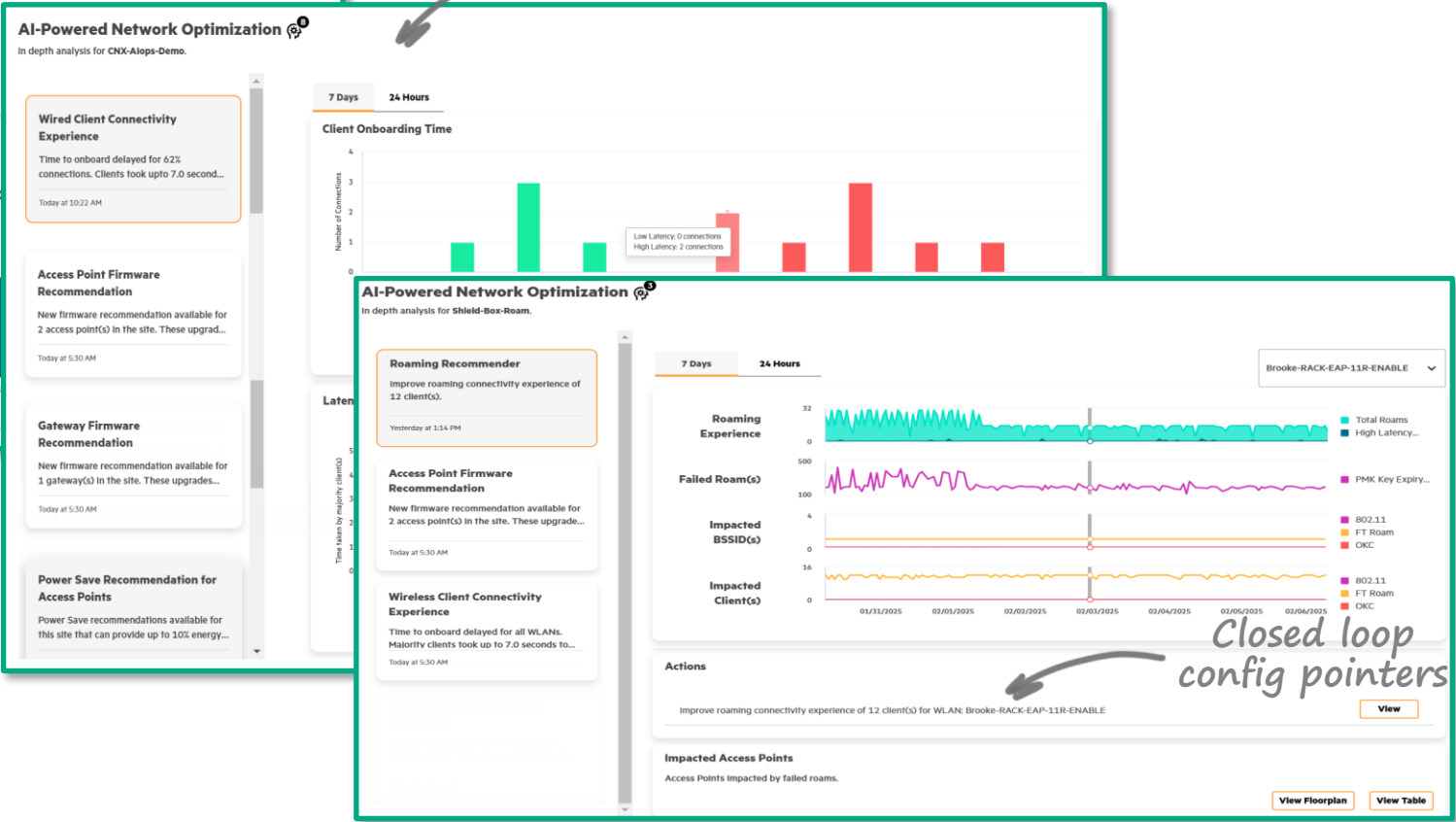
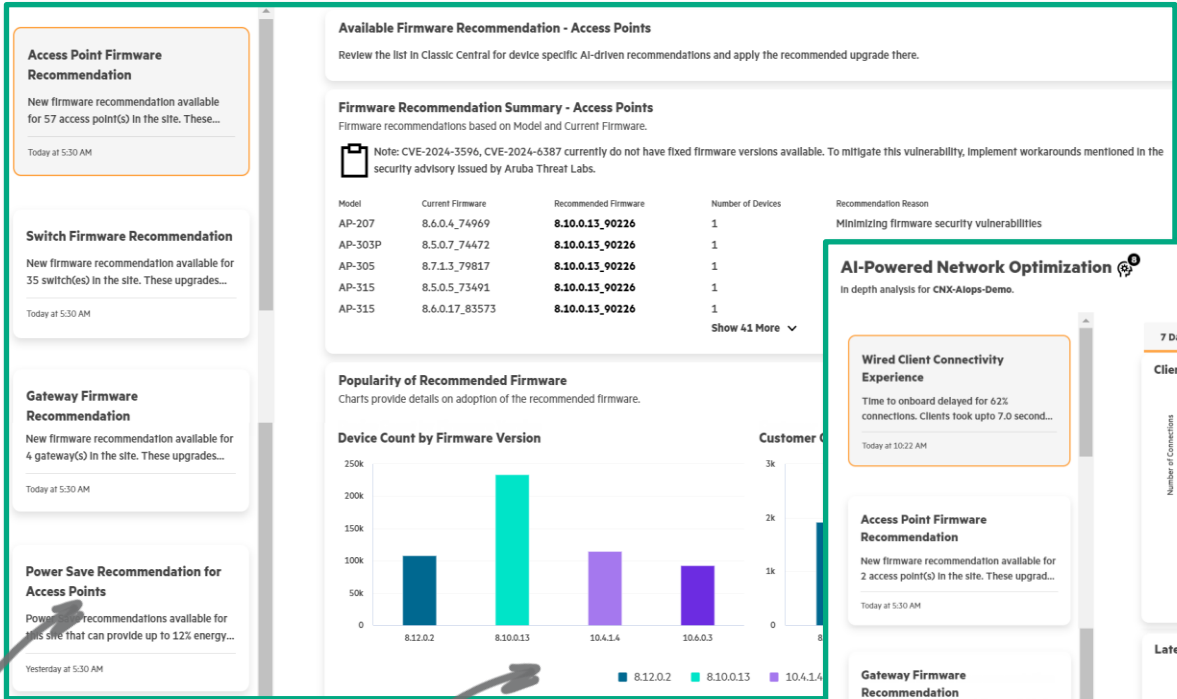
AI-powered recommendations

Free up valuable IT cycles and reduce risk with proactive optimization insights



- **Custom, actionable recommendations** at a global/per-site basis
- AI/ML models trained and re-trained **weekly** on **data from anonymized peer groups** with similar environments
- **Examples**
 - Firmware Recommendations
 - Enable Wi-Fi 6 to Improve Wi-Fi Experience
 - Enable WPA3 for Better Security
 - IoT Policy Optimization
 - Coverage Hole Detection
 - DFS
 - Roaming
 - Abnormal Data Upload/Download
 - Client Connection Times – wired and wireless
 - Save Power Using Green AP
 - Improve Wi-Fi Performance using 6GHz
 - Probe Threshold Recommendation
 - Application Performance

AI Insights at a Glance



LLM-powered search

Closed loop config pointers

23+ use cases solved

Peer baselining



New Central HOL

<https://console.greenlake.hpe.com>

Use SSO for login; onecon2025@arubademo.net/OneCon2025@

Lab guide link: https://www.dropbox.com/scl/fi/bq4lzx86hixep4a28yepg/New-Central-Troubleshooting-via-DXP-LabGuide-v1.4-CUSTOMER_.pdf?rlkey=o8iel5uecierezhd416wwi07&st=6a2i7ghs&dl=0

Lab guide QR code

HPE

Connecting to Hewlett Packard Enterprise

Sign-in with your HPE account to access HPE GreenLake edge-to-cloud Platform

Sign In

Username

☐ Remember me

Next

OR

1 **Sign in with SSO**

[Need help signing in?](#)

New to HPE? [Create account](#)

Sign In with Single Sign-On

Sign in and access HPE's cloud services.

2 **Append @arubademo.net**

Email*

3 **Next**

Signing In is your acknowledgement of the [HPE Terms of Use](#).

4 **HPE DXP SSO**

Please login to the network using your ondemand credentials (including @arubademo.net).

Username:

Password:

5 **LOG IN**

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

