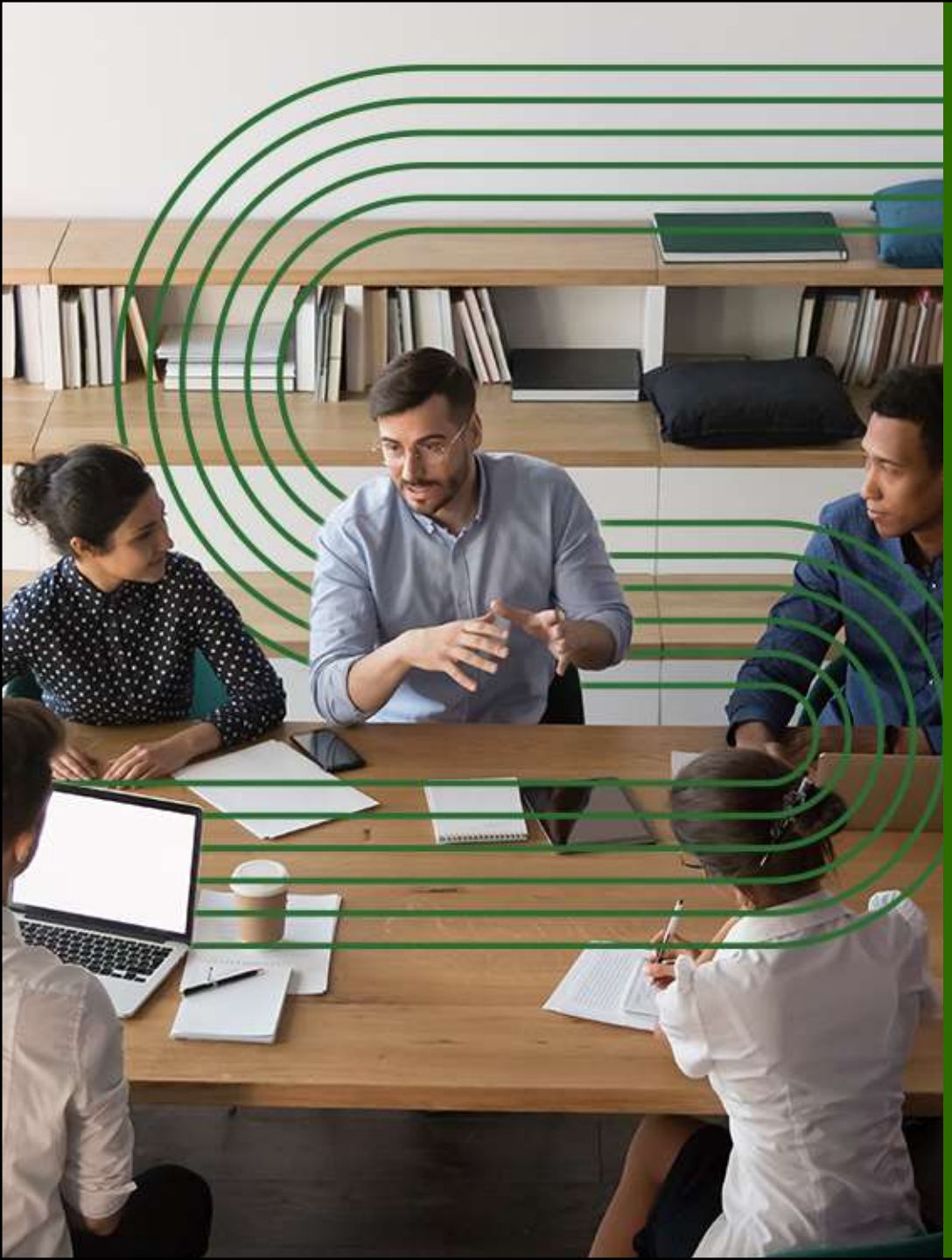
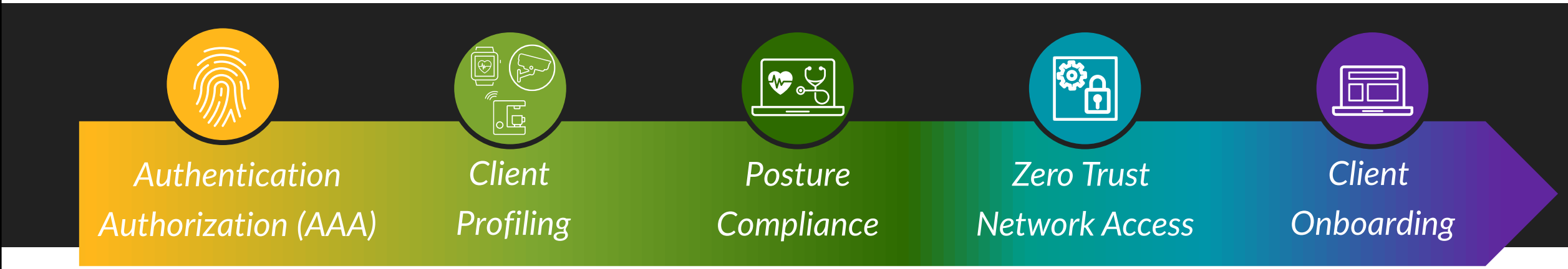


Juniper Mist Access Assurance

Vijendra Singh,Reseller at Juniper Networks

JUNIPER NETWORKS

What is Network Access Control (NAC)?
Concepts



Authentication Authorization (AAA)

- *802.1X / MAB*
- *Identify a User or a Device*
- *Determine User/Device Role*
- *Assign VLAN / Policy based on User Identity*

Client Profiling

- *Passive Fingerprinting*
- *Device Type / Manufacturer visibility*
- *OS version visibility*
- *Using device fingerprint during AAA*

Posture Compliance

- *Determine endpoint health and compliancy (antivirus, firewall, patches/updates etc)*
- *Agent-based or Agent-less*
- *Leverage Posture compliance status in AAA*

Zero Trust Network Access

- *End-Point agent tunnels user traffic to the Cloud*
- *Cloud POPs classify end-user traffic and enforce network policies*
- *Today ZTNA exists outside of traditional NAC as a standalone concept*

Client Onboarding

- *App-based on Portal based end-user device provisioning with 802.1X (certificate) or MPSK credentials*
- *Built-in PKI (cert) infrastructure*

What's Wrong with NAC Solutions Today?

Cisco ISE, Aruba Clearpass, Forescout NAC require professional services or a dedicated NAC IT expert

Solutions are complex and brittle	*Impossible to manage without breaking*
Cumbersome troubleshooting and lack insights	*No end-to-end visibility*
Lack agility and scale	*Legacy LDAP and on-prem directories*
Requires downtime	*Maintenance, feature updates & security patches*

Current NAC Customer Responsibility

1) Design for service redundancy

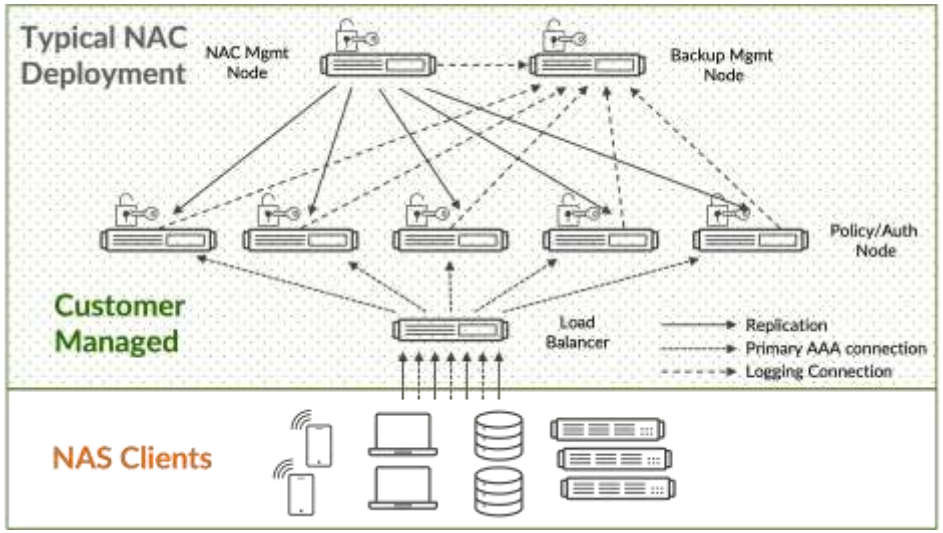
2) Design for high availability

3) Design for scale

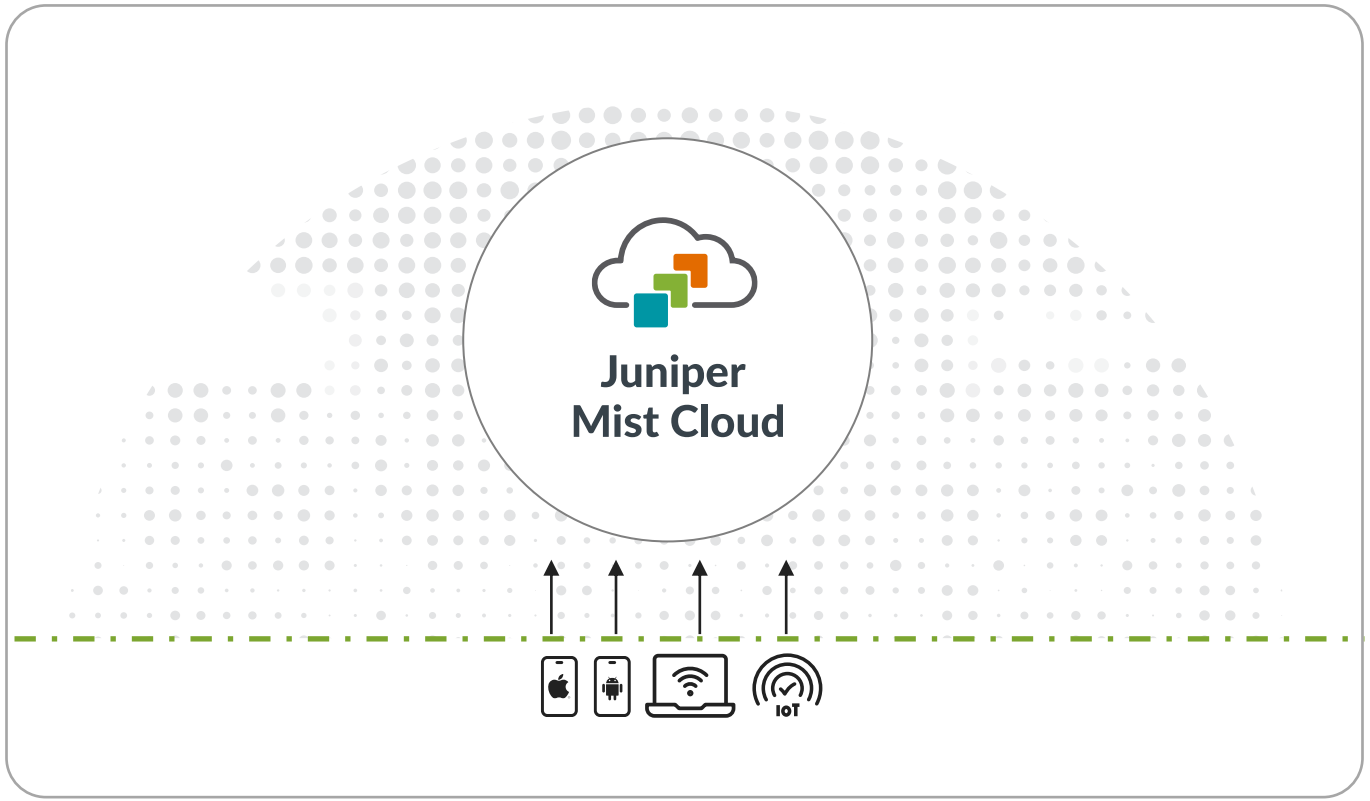
4) Manually scale up or down

5) Maintain server hardware / VM servers

6) Perform upgrades / security patches



Juniper Mist Access Assurance
Moving to the integrated cloud



- **Microservices-based** *Cloud NAC service natively integrated into network operations.*
- **IT-friendly Day 0-2 operations** *fully integrated into the network, continuously validating end-user experience.*
- **AI-driven** *network operations extended to network access control.*
- **Periodic hitless feature updates** *security patches and vulnerability fixes without downtime planning.*
- **Geo-awareness, high-availability** *Intrinsically available with the Juniper Mist Cloud.*

High availability, High Reliability & Site Survivability

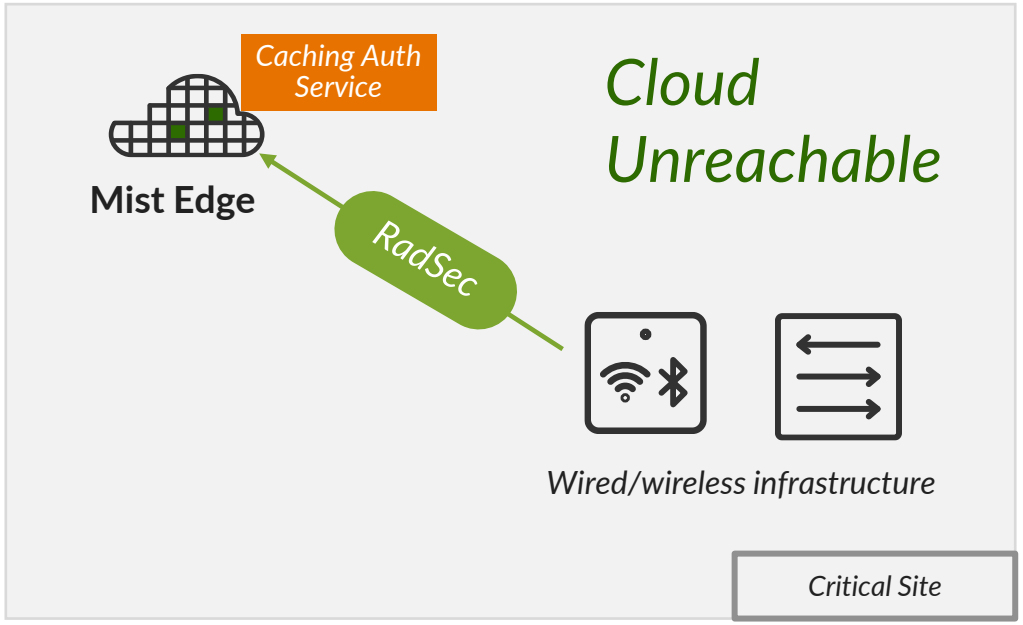
- *All previously known clients (regardless of the auth method) get authenticated and full policy gets applied (VLANs, GBP tags, Roles, etc)*
- *New clients are authenticated and applied default critical service policy*

Why does it matter?

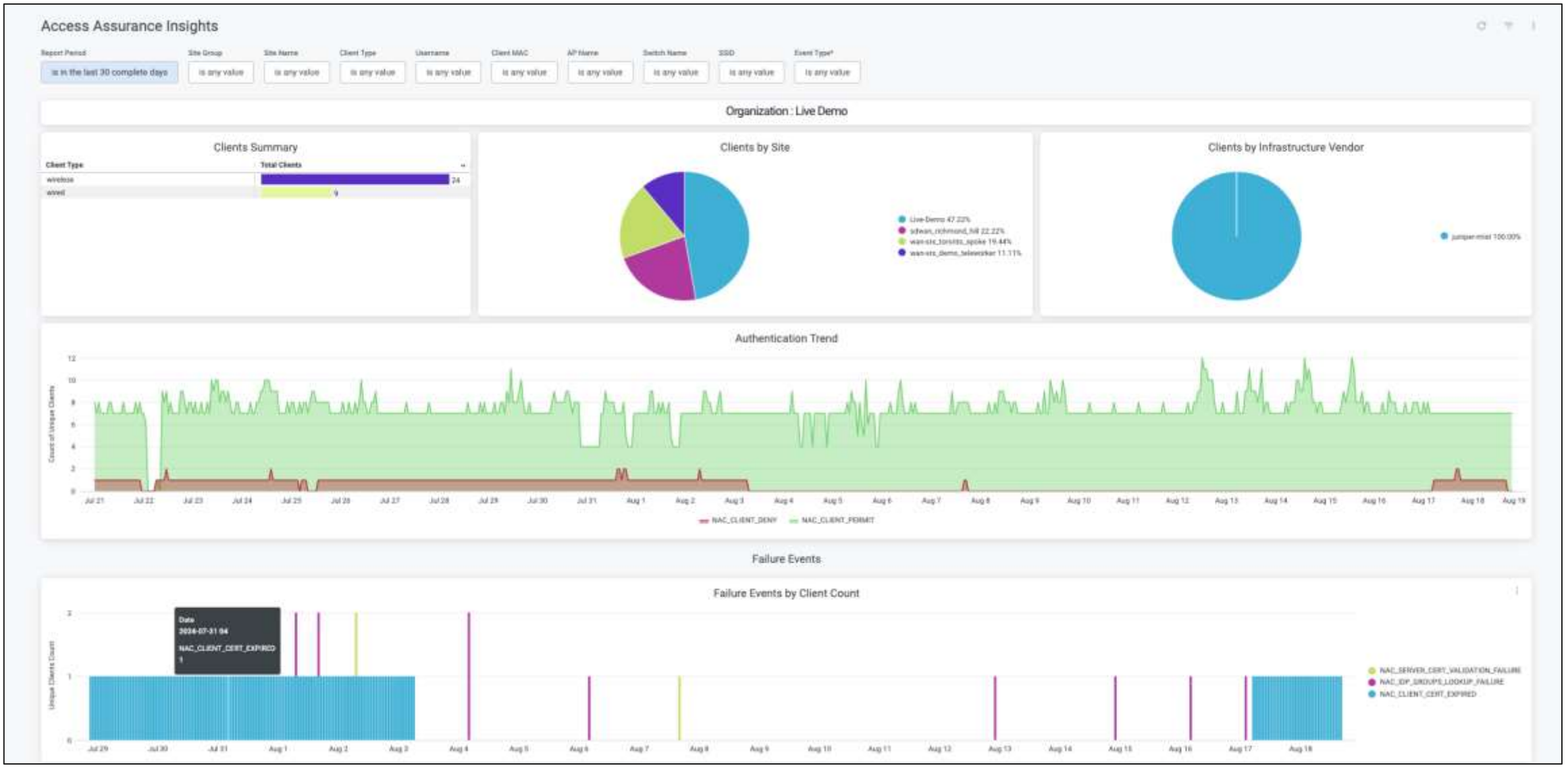
Cloud Microservices are used for the heavy lifting of authentication and authorization services.

Mist Edge provides a local on-premises point of presence for site survivability functions.

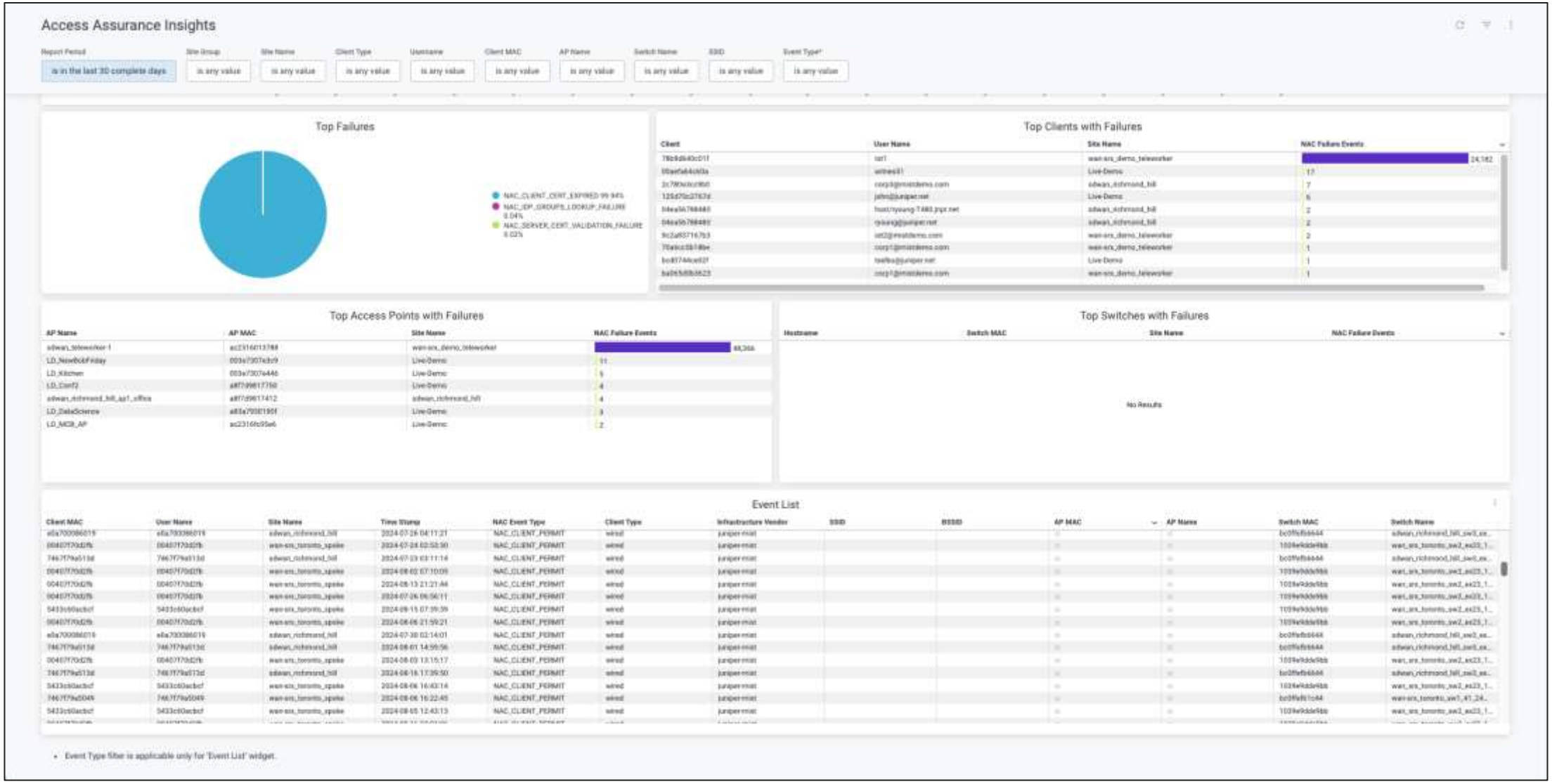
Lean operations on the Mist Edge side.

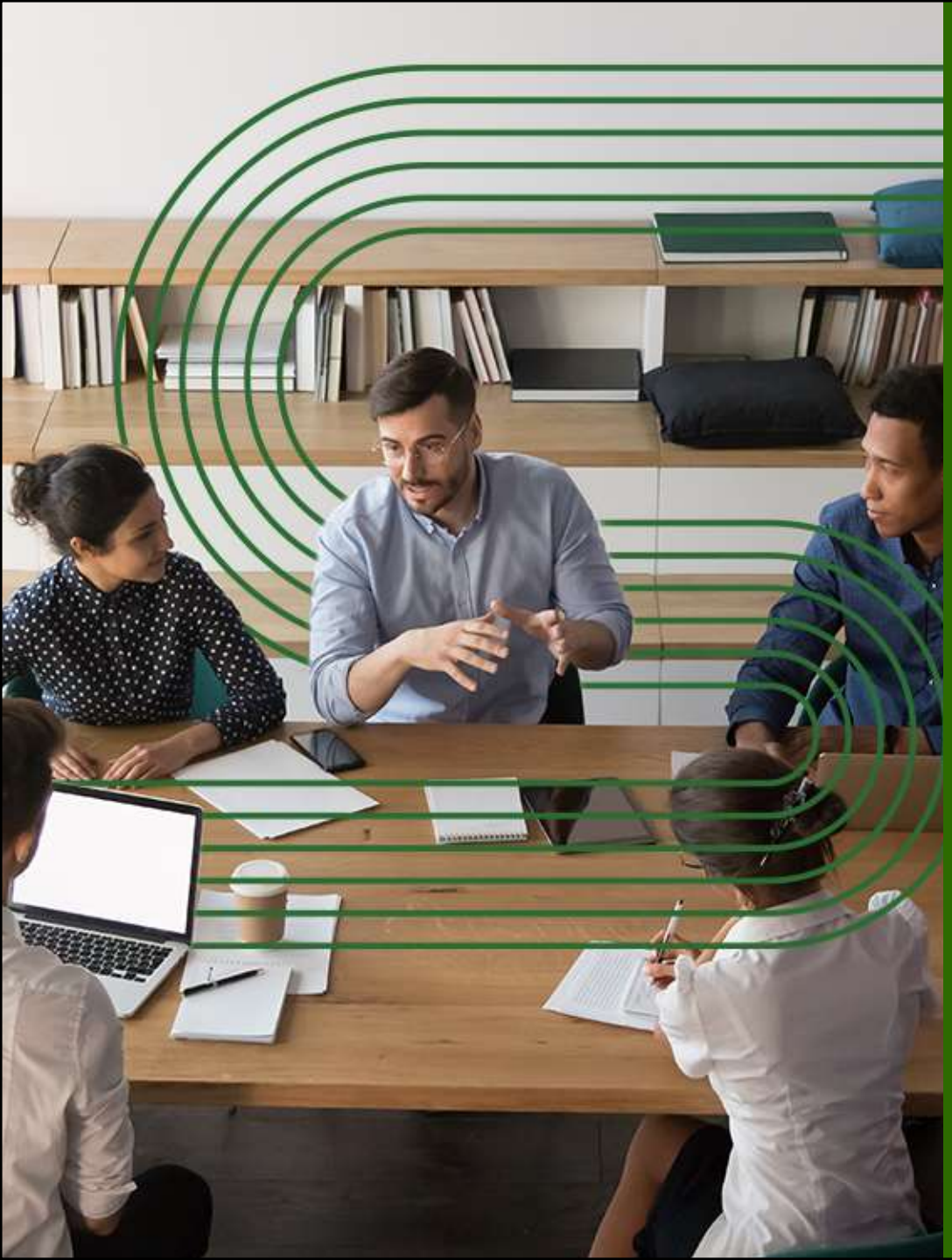


Access Assurance Insights in Premium Analytics



Access Assurance Insights in Premium Analytics





Education Use Cases for IoT Assurance

JUNIPER NETWORKS

Challenges of Today's IoT/BYOD Solutions

Lack of Central Management

Difficult to monitor and manage thousand devices

Limited Visibility

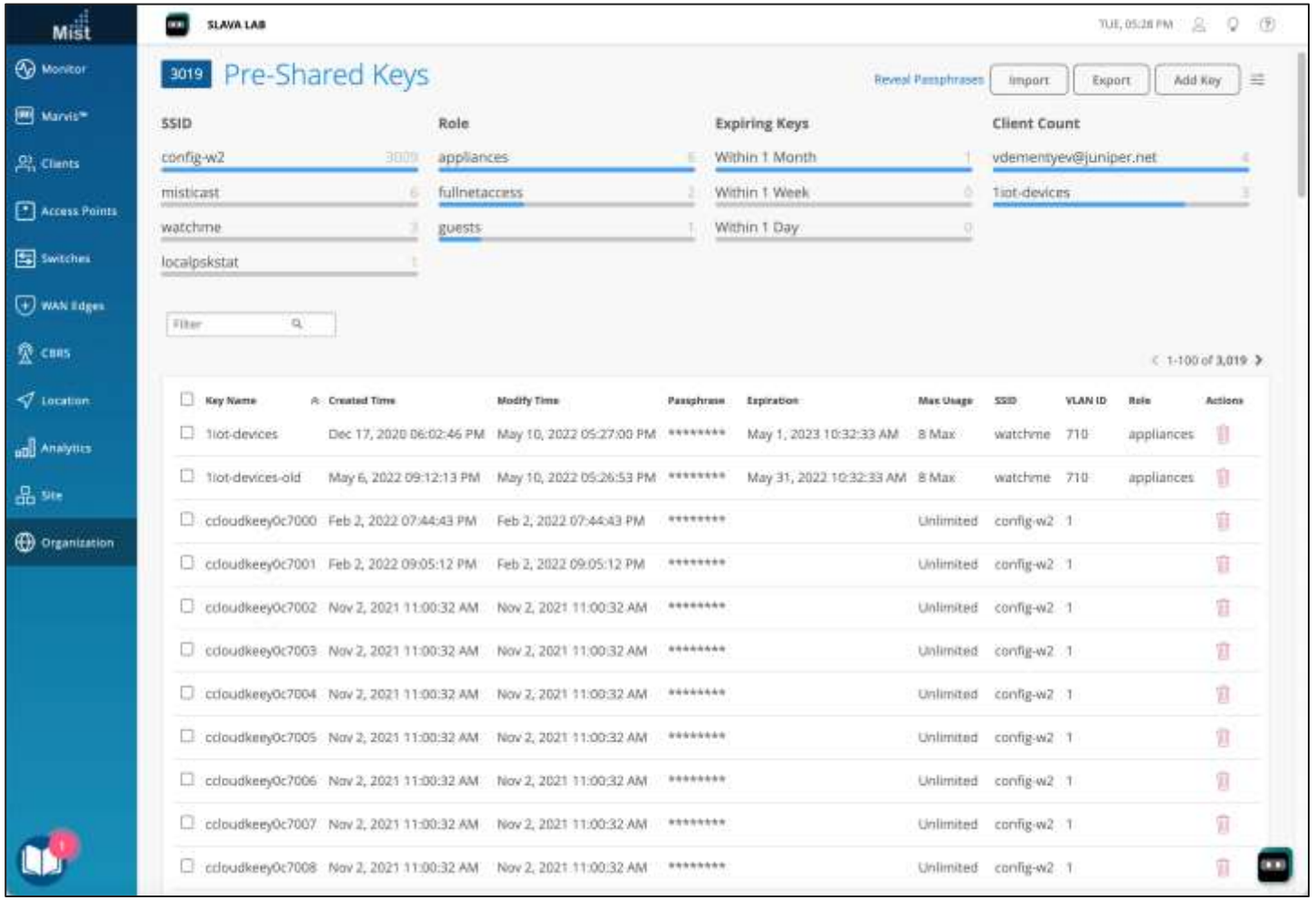
Limited visibility of user activities

Weak Password Policy

Use of easily guessable or shared passwords makes devices vulnerable to attacks

No Automation for Access Codes Generation

Manual generation of access codes need huge IT resources



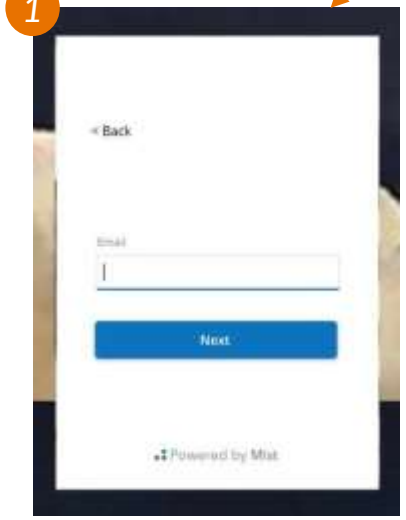
Juniper's IoT Assurance Solution

User authenticates using Corp credentials via SSO

2 User Directory

SAML

1



User navigates to SPP URL, i.e. getmypsk.company.com

PSK gets automatically generated using SSO Email as PSK Name:

3

Feature:

- *Self Provisioning MPSK Portal for BYOD*

Function:

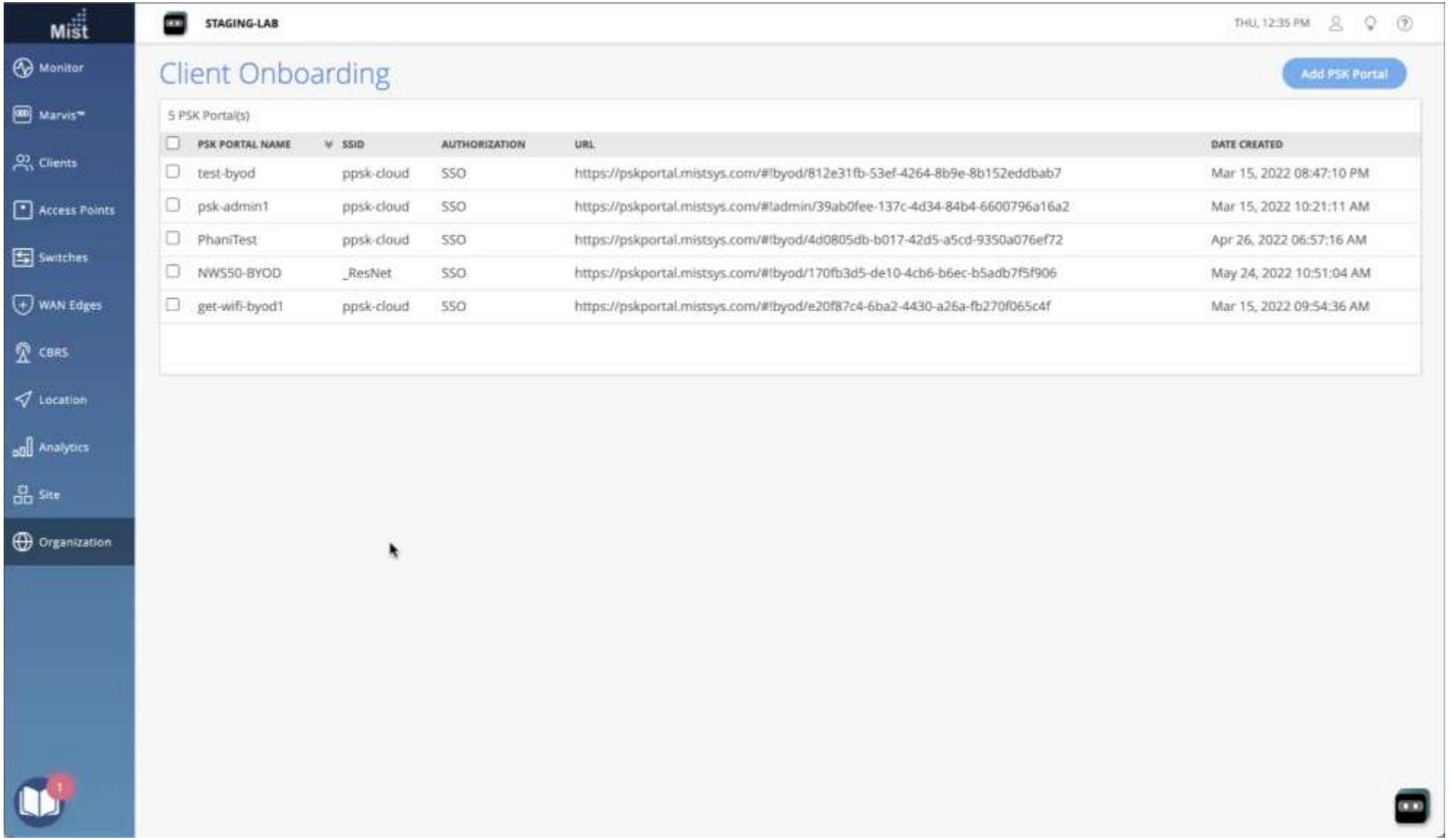
- *Self-Provisioning Portal for the end users to get Personal PSK via Single Sign-On*

Outcome:

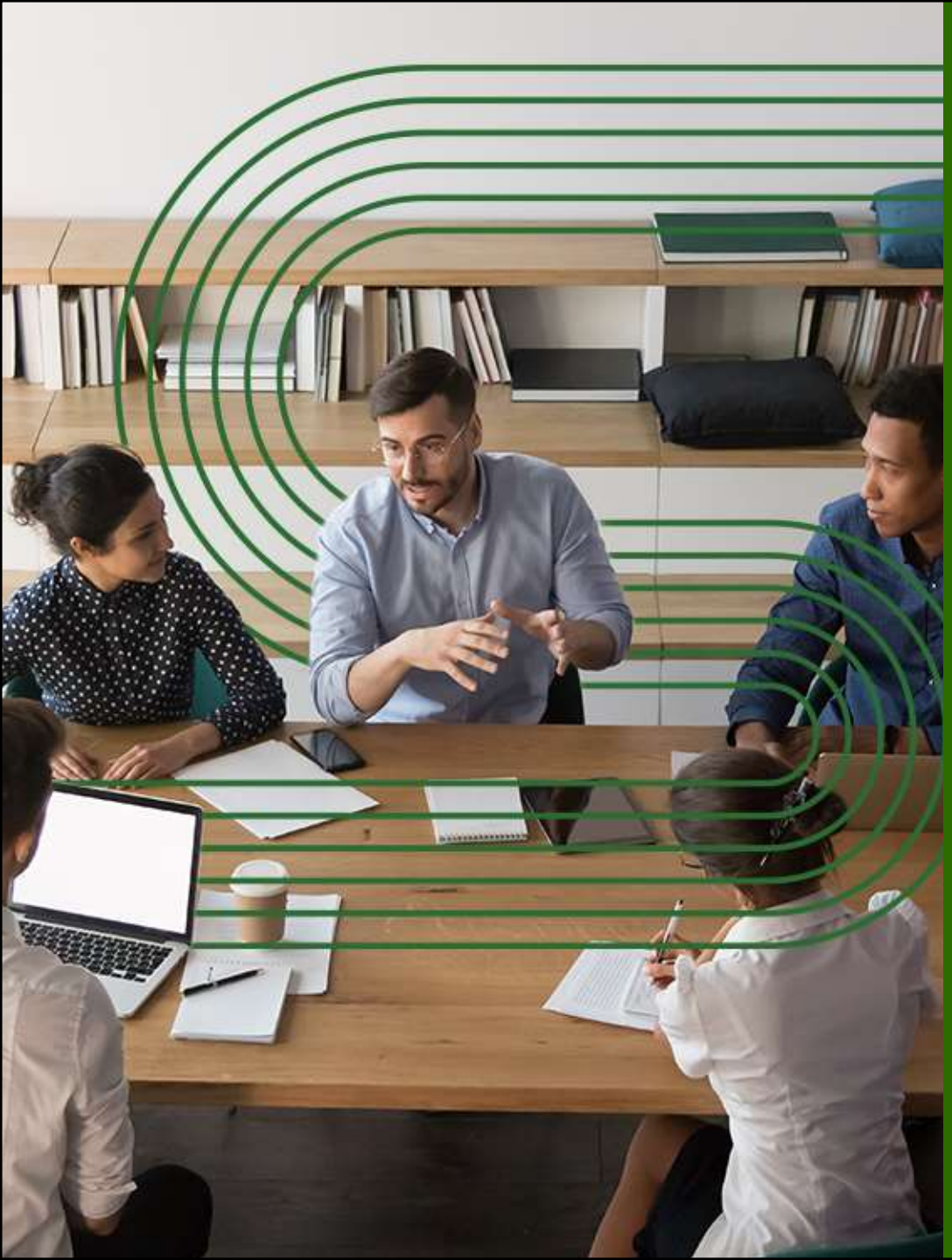
- *Complete BYOD package with seamless end user onboarding (no certificates, no 3rd party apps, zero complexity)*
- *Native Integration into any User Directory using SAML*
  - *Corporate Email = PSK Name*
- *Flexible Onboarding Workflows based on desired use-case (Employees vs Contractors vs Sponsored Guests vs Event visitors)*

JUNIPER NETWORKS

Demo 1 – IoT Assurance



JUNIPER NETWORKS

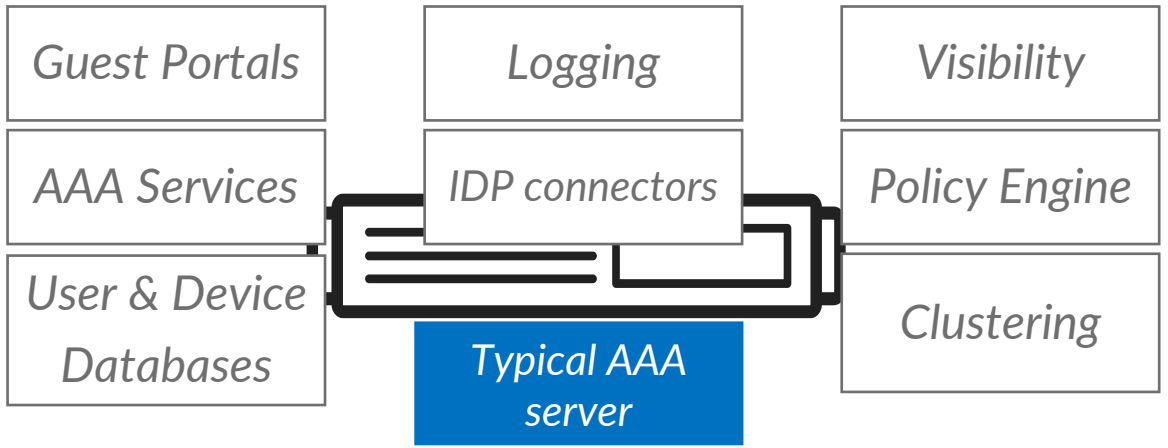


Education Use Cases for NAC Assurance

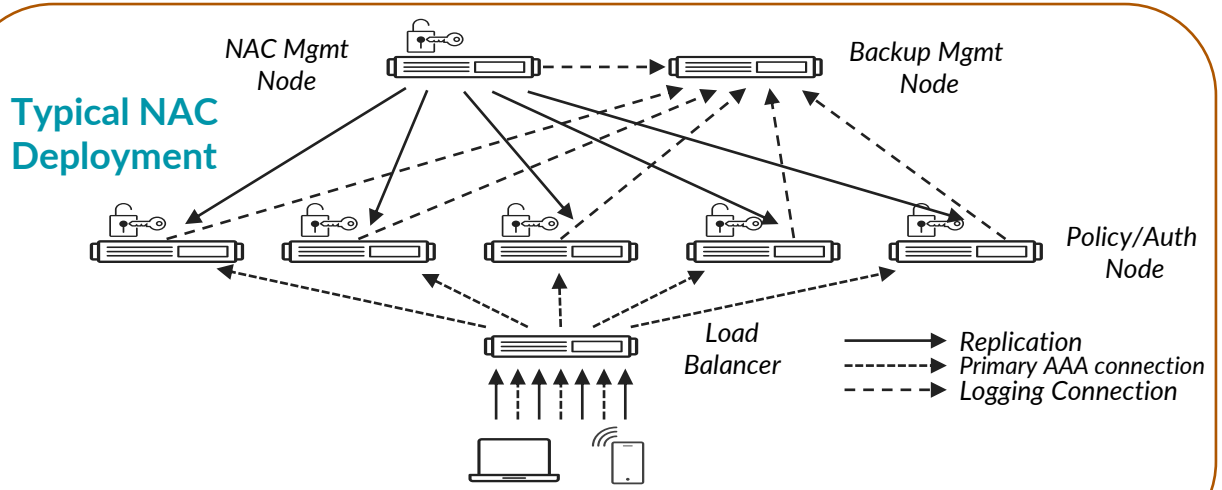
JUNIPER NETWORKS

Challenges of Today's NAC
Functional & Architectural Complexity

NAC: Logical Functions



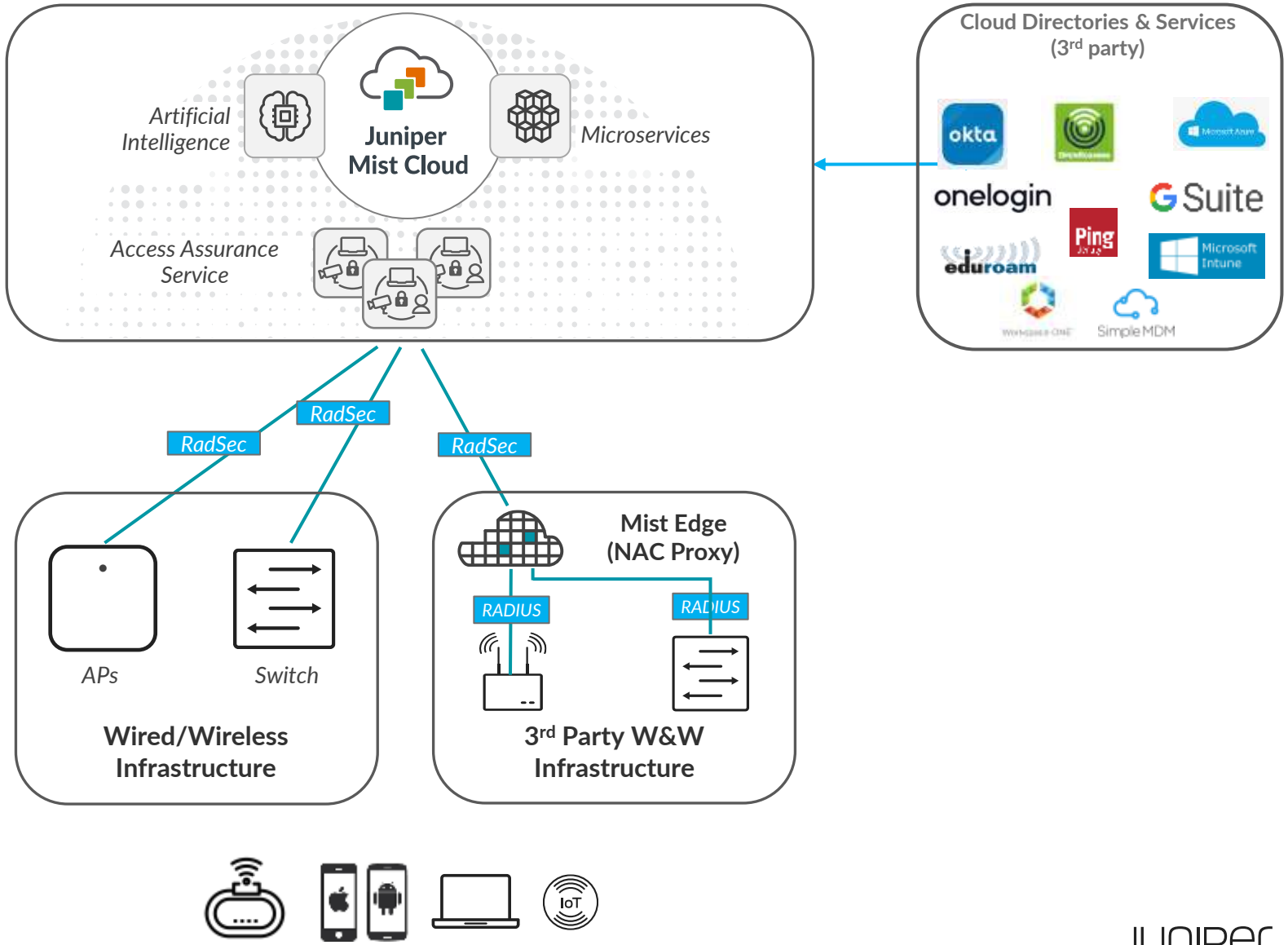
NAC: Physical Architecture



- Solutions are complex, brittle, lack scale
- Cumbersome troubleshooting and lacking insights
- Requires downtime planning

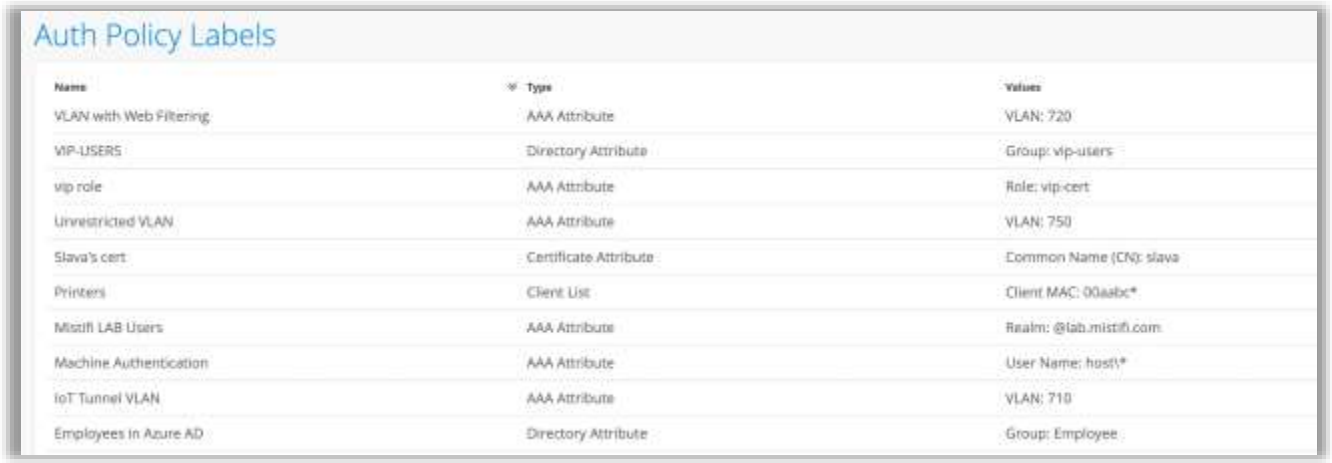
Juniper Mist Access Assurance Solution

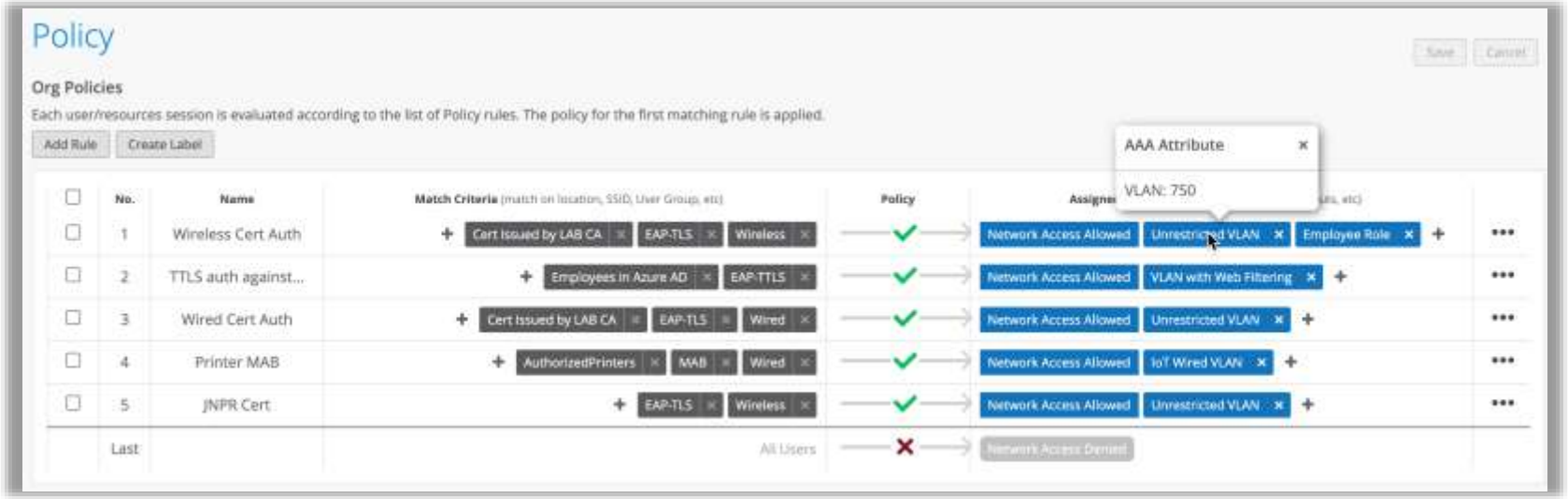
- **Micro-Services based Cloud NAC Offering**
- **Industry-first AI powered operations**
- **IT-friendly day 0-2 operations**



Mist Access Assurance = Cloud NAC Service

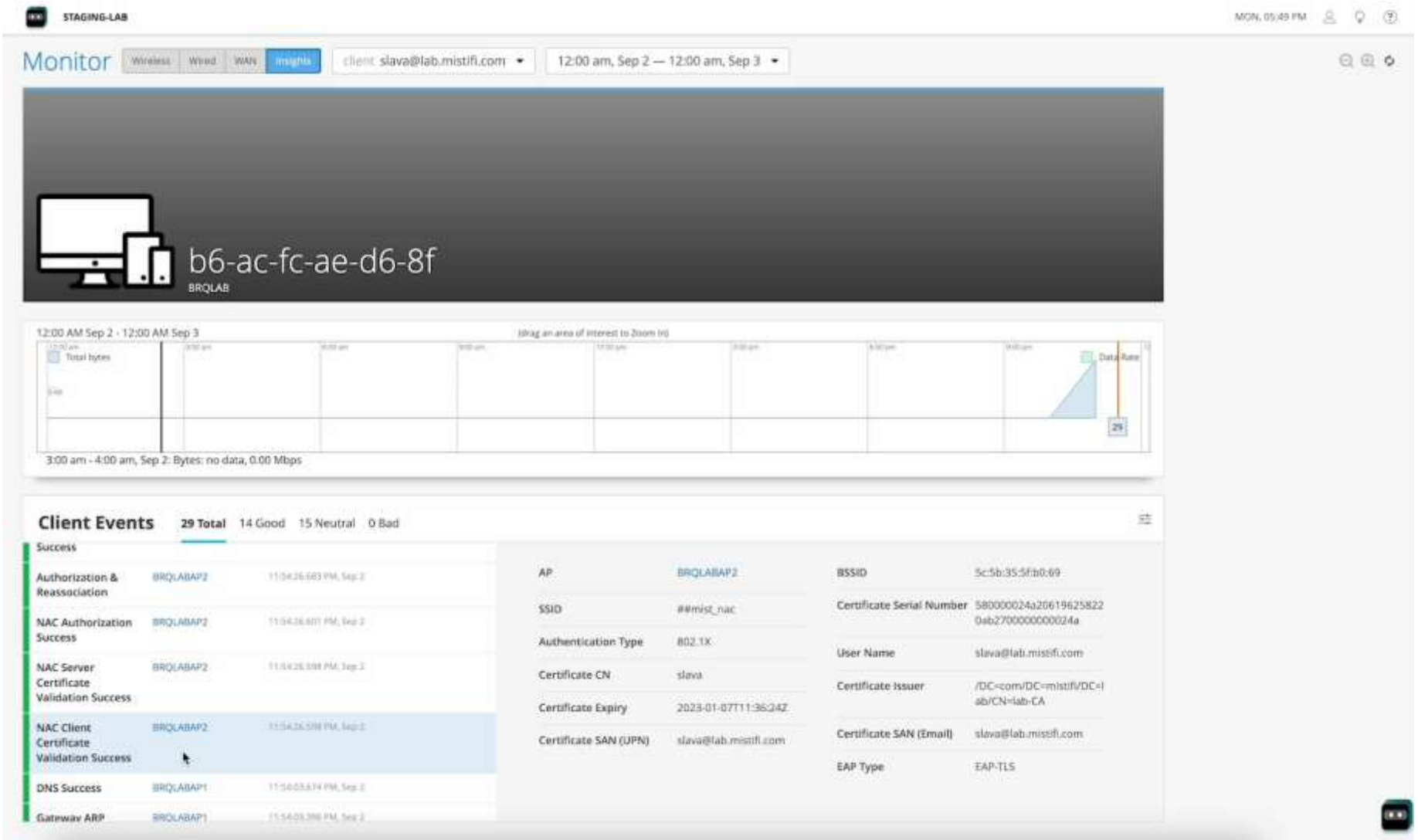
IT-friendly yet flexible Auth Policy configuration





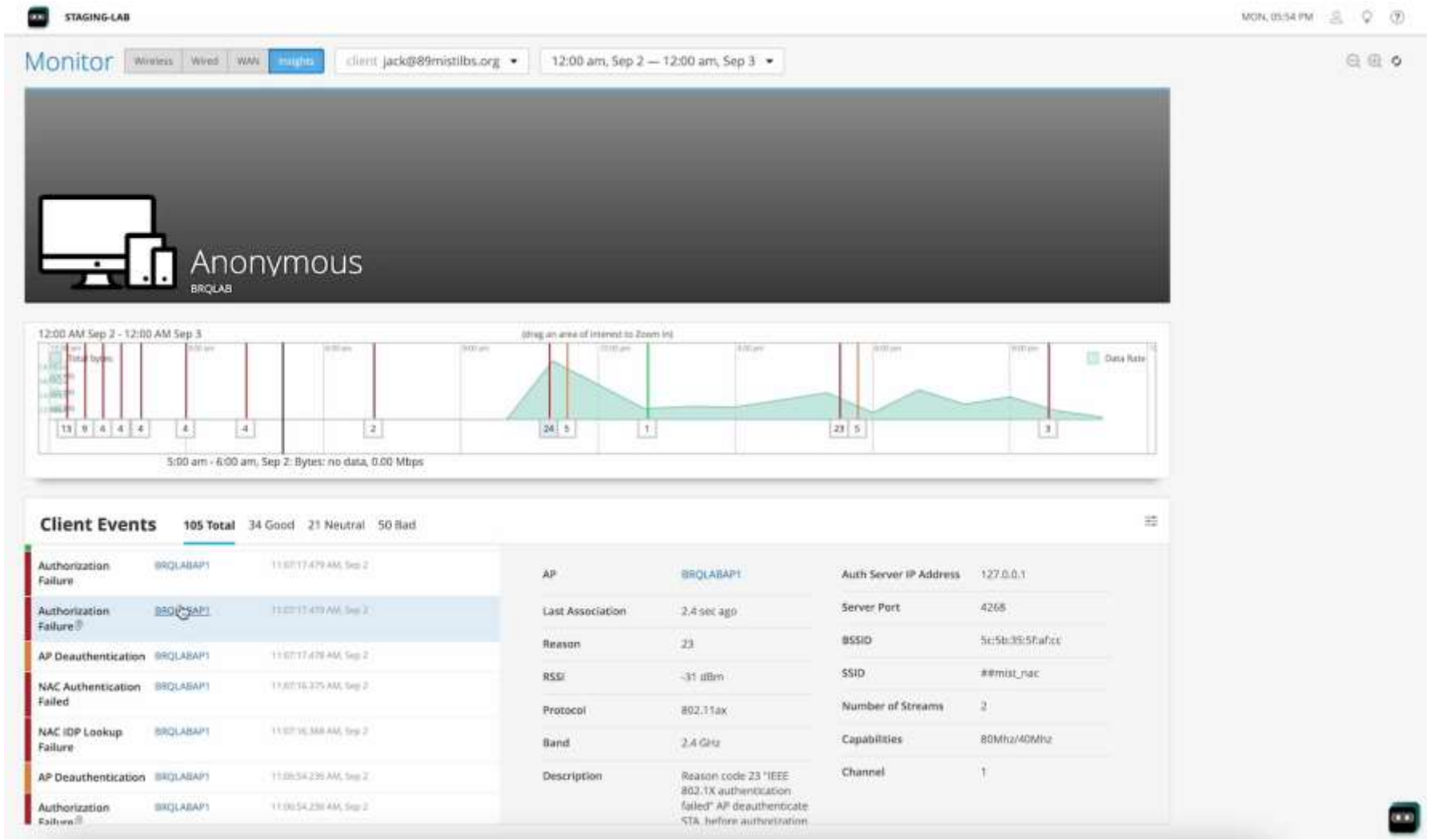
Demo 2 – NAC Assurance

Client State Machine Extended to NAC



Demo 2 – NAC Assurance

Client State Machine Extended to NAC – Failure case



Thank you

Juniper Networks | Driven by Experience™