14 May 2020
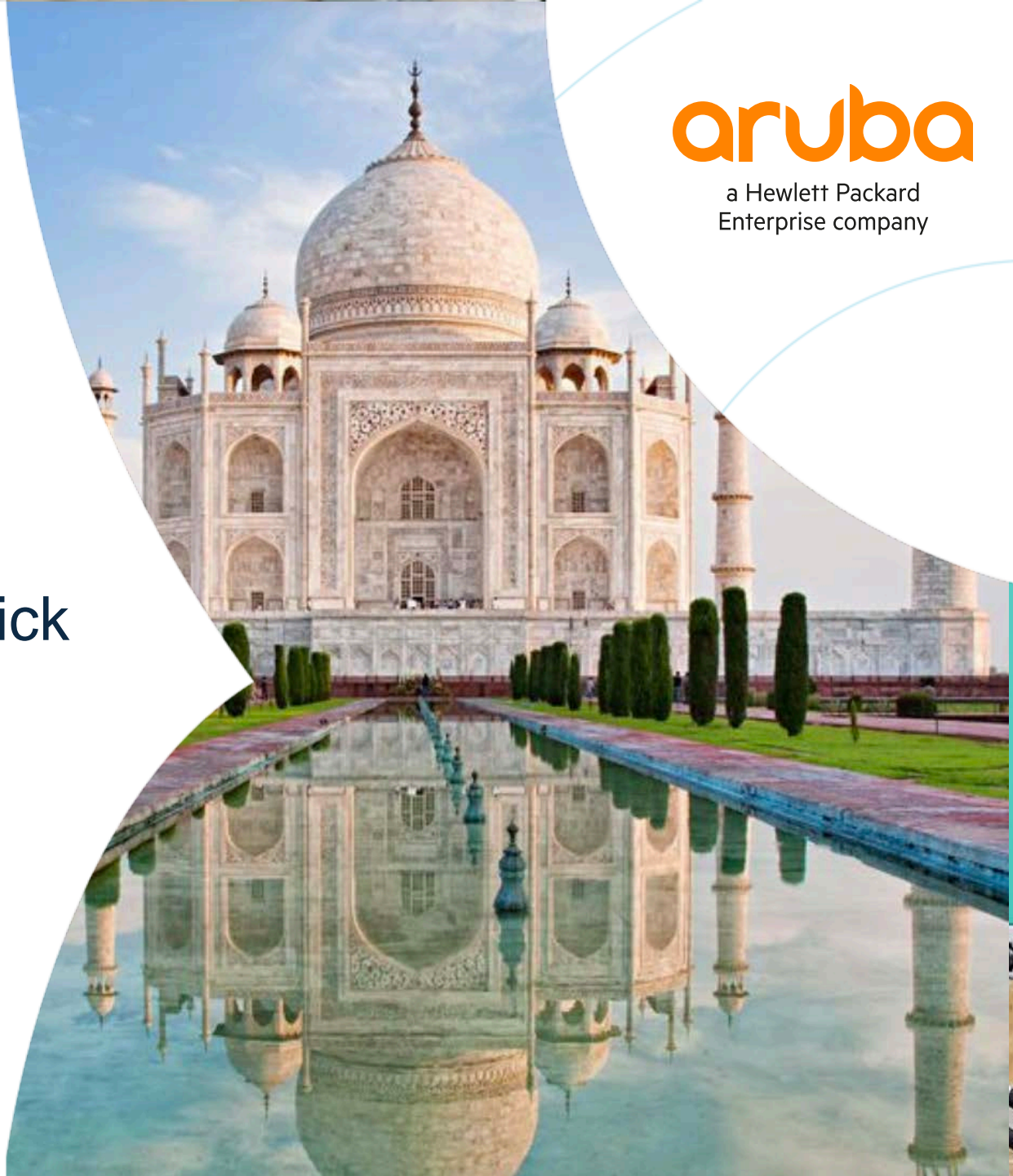
Aruba
SD-Branch

Jenalyn Zapanta & Elissa McCormick

Category Manager, APJ
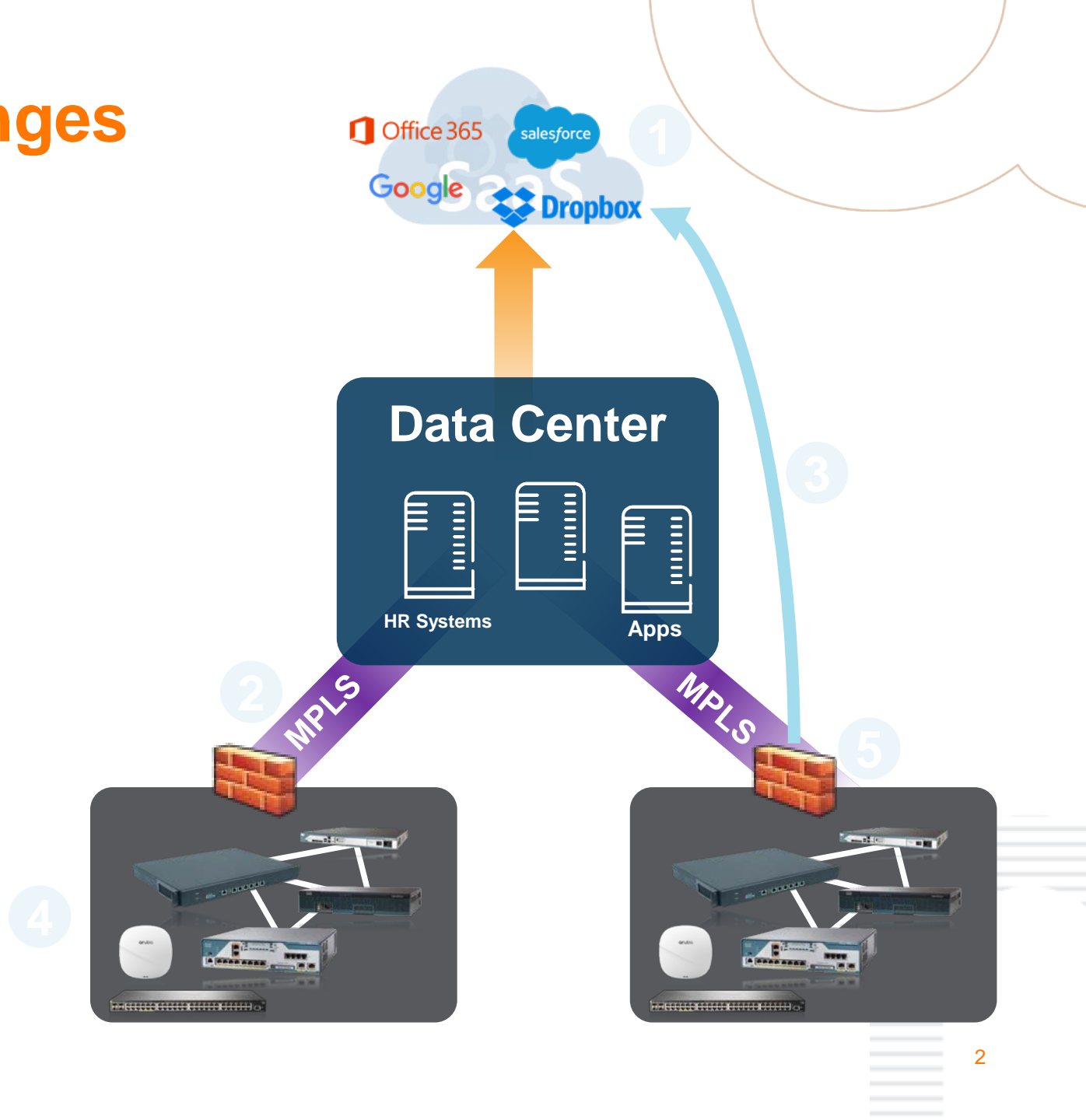
aruba

a Hewlett Packard
Enterprise company
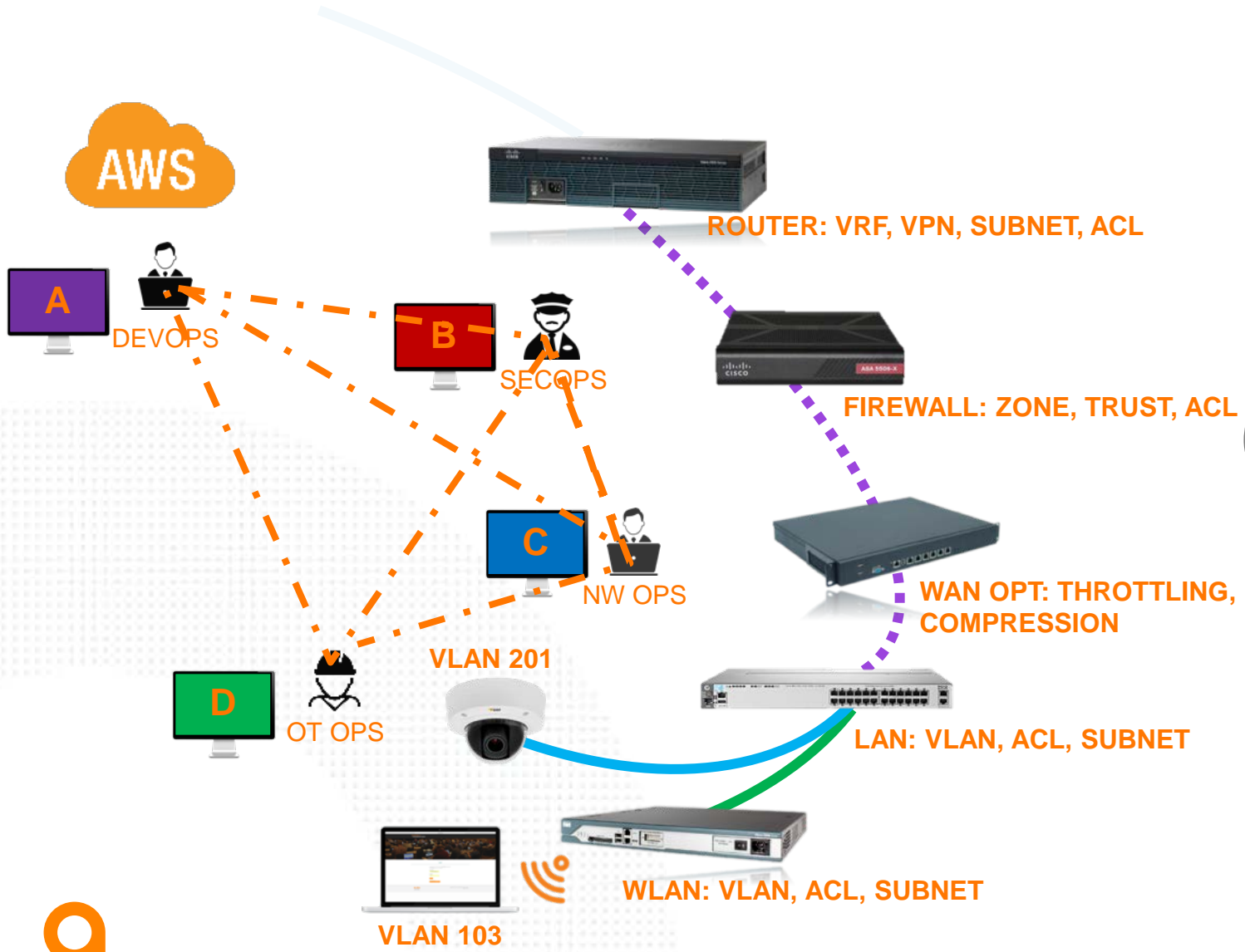
WAN Architecture Challenges

1. SaaS Applications from DC
2. Expensive BW on private WAN
3. Performance and reliability tradeoffs
4. Complex branch infrastructure and ops
5. Security challenges due to IoT, Mobility, etc

Office 365 salesforce
Google SaaS Dropbox

1

Data Center

HR Systems   Apps

3

2 MPLS   MPLS 5

4

End-to-End Branch Operations Today

ROUTER: VRF, VPN, SUBNET, ACL

FIREWALL: ZONE, TRUST, ACL

COMPLEXITY

AWS

A
DEVOPS

B
SECOPS

C
NW OPS

D
OT OPS

WAN OPT: THROTTLING, COMPRESSION

VLAN 201

LAN: VLAN, ACL, SUBNET

WLAN: VLAN, ACL, SUBNET

VLAN 103

3

SD-Branch = SD-WAN + SD-LAN

Security

Private WAN is complex and expensive

SaaS applications are backhauled to the data center

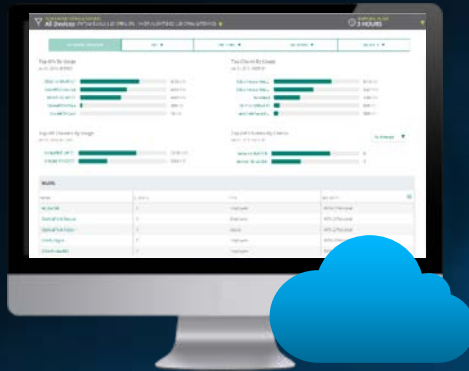← WAN Challenges

Increased security risk from the rise in IoT

Device sprawl and static configurations

← BRANCH Challenges

Aruba Central Management at Scale

Experience-First Management

LAN / WAN / WLAN

Aruba-OS Switches

Security Gateways

Instant Access Points

Value Added Services

Guest Wi-Fi

Presence Analytics

Connectivity Health

SD-WAN

Security

Extensibility via REST APIs

(Configuration, Monitoring, Alerts and Secure Access)

Streamlined Provisioning & Workflow-drive usage models

Comprehensive management & intelligent automated insights

Platform integrated mobile & IoT Advanced Profiling

Built-in APIs for Integration with 3rd Party Solutions

SD-Branch Architecture

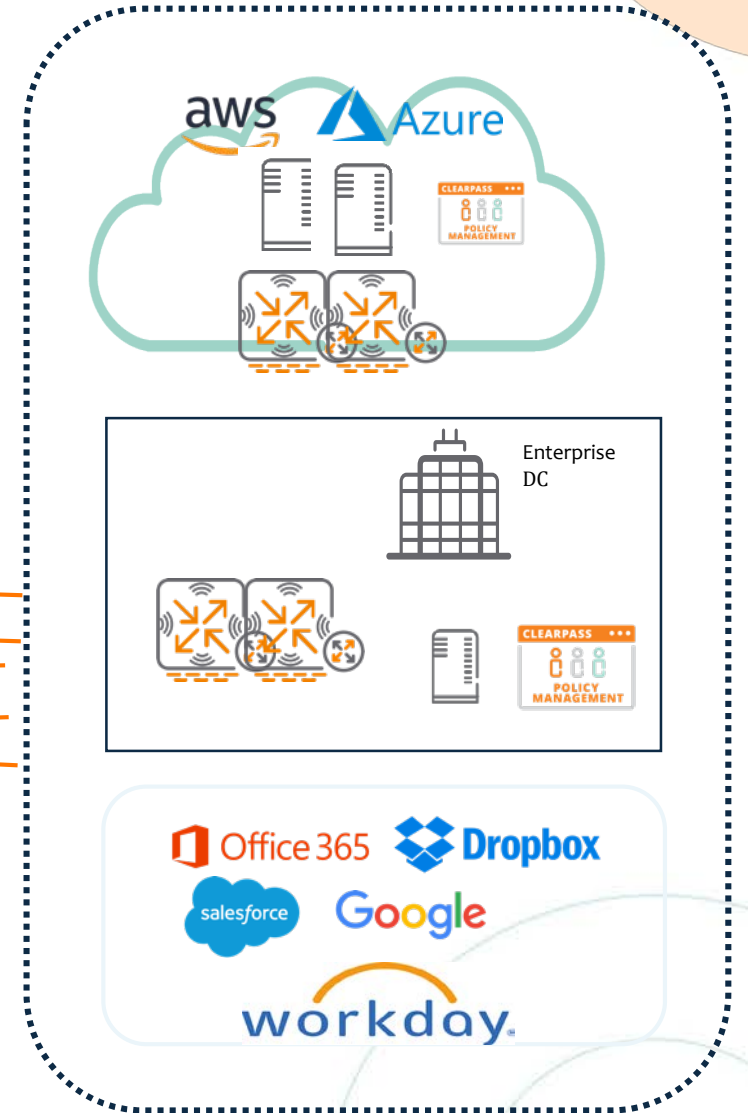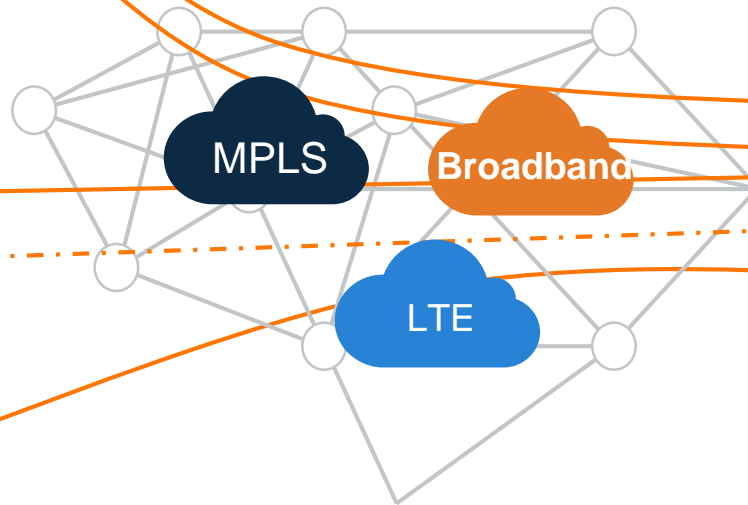One solution fits all!!

TOP REASONS WHY
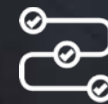# ARUBA SD-BRANCH

SEAMLESS ORCHESTRATION

MANAGE EXPERIENCE

END-TO-END SECURITY

SIMPLIFIED OPERATIONS
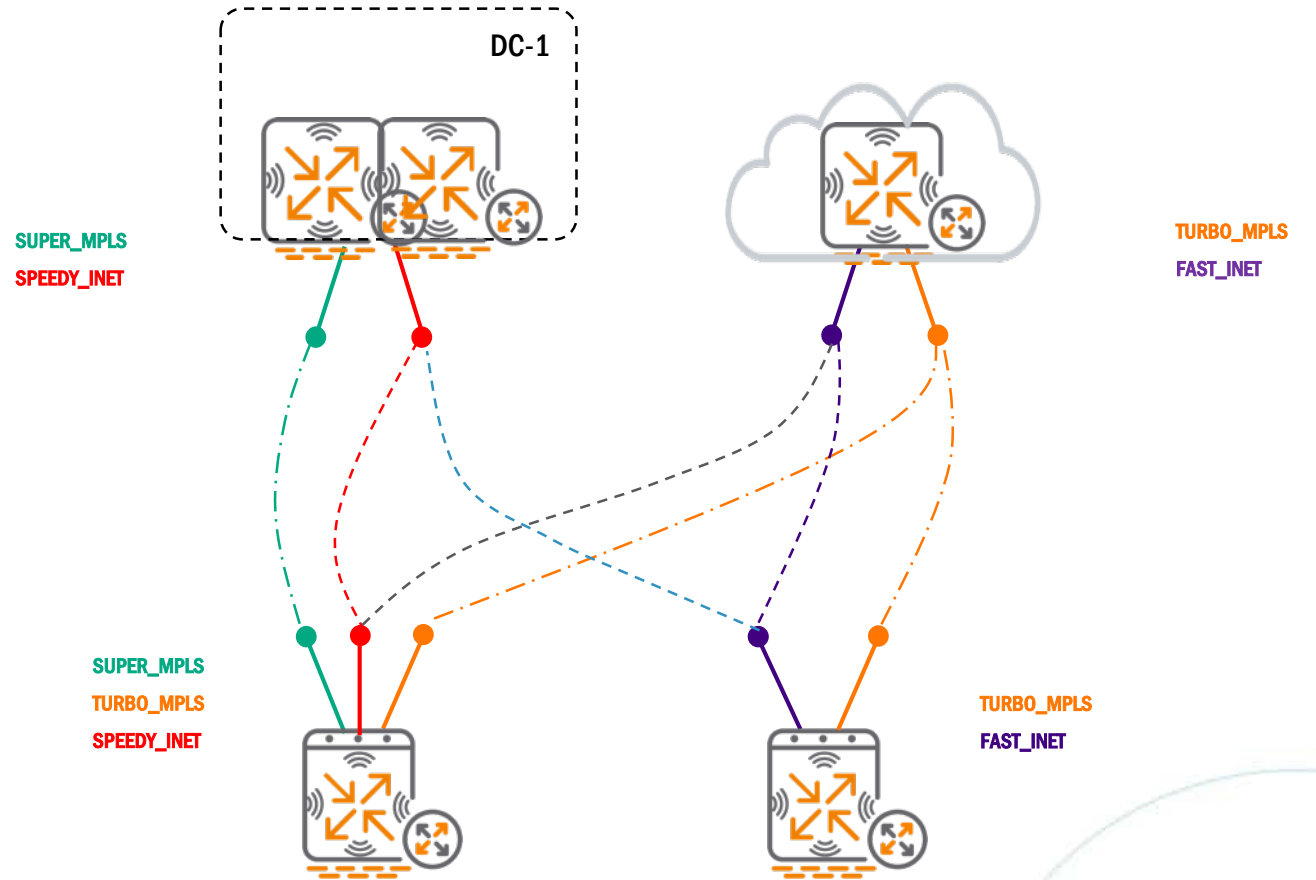
Seamless Orchestration

SD-WAN Orchestrator

Tunnel Orchestration

SD-WAN Orchestrator

SRC	DST	TYPE	Tag	Cost
BG-1	DC-1-VPNC-1	MPLS	SUPER	10
BG-1	DC-1-VPNC-2	MPLS	SUPER	20
BG-1	DC1-VPNC-1	INET	SPEEDY	10
BG-1	DC-1-VPNC-2	INET	SPEEDY	20
BG-1	DC-2-VPNC-1	MPLS	TURBO	30
…	…	…	…	…

DC-1

SUPER_MPLS
SPEEDY_INET

TURBO_MPLS
FAST_INET

SUPER_MPLS
TURBO_MPLS
SPEEDY_INET

TURBO_MPLS
FAST_INET

Orchestrated Overlay

Route Orchestration

SD-WAN Orchestrator

Regional DC

DC

OSPF

BGP

Direct Routing

Routing

OSPF

Subnet A

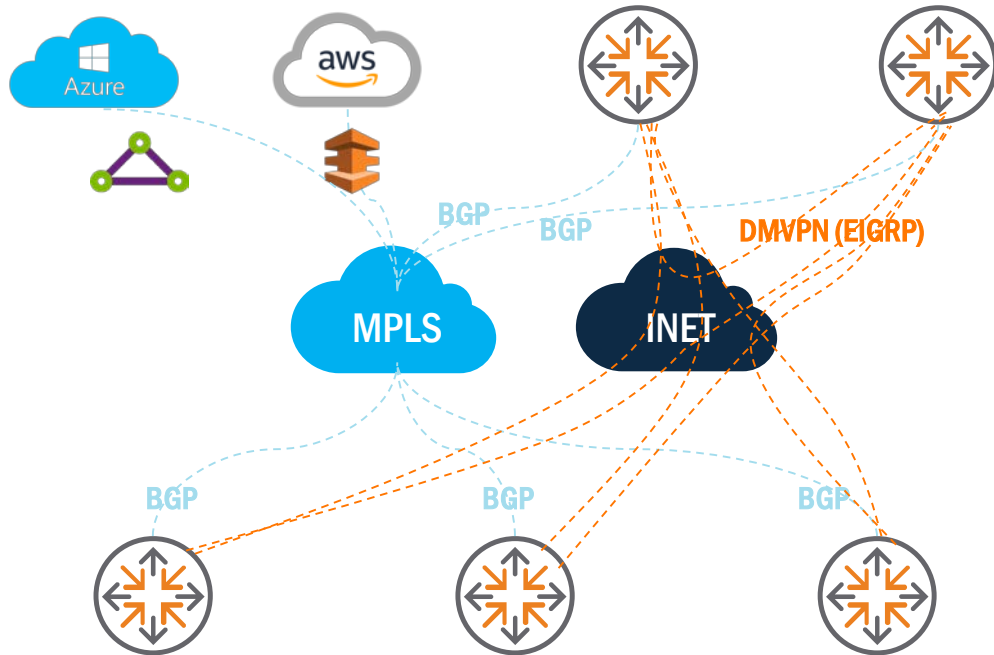Subnet B

GW	Network	NextHop
BGW-01	10.96.0.0/16 (branches)	R-DC
BGW-01	10.0.0.0/8 172.16.0.0/12 (summary-global)	Main-DC
BGW-01	10.127.0.0/16 (AWS-VPC)	Cloud
…	…	…
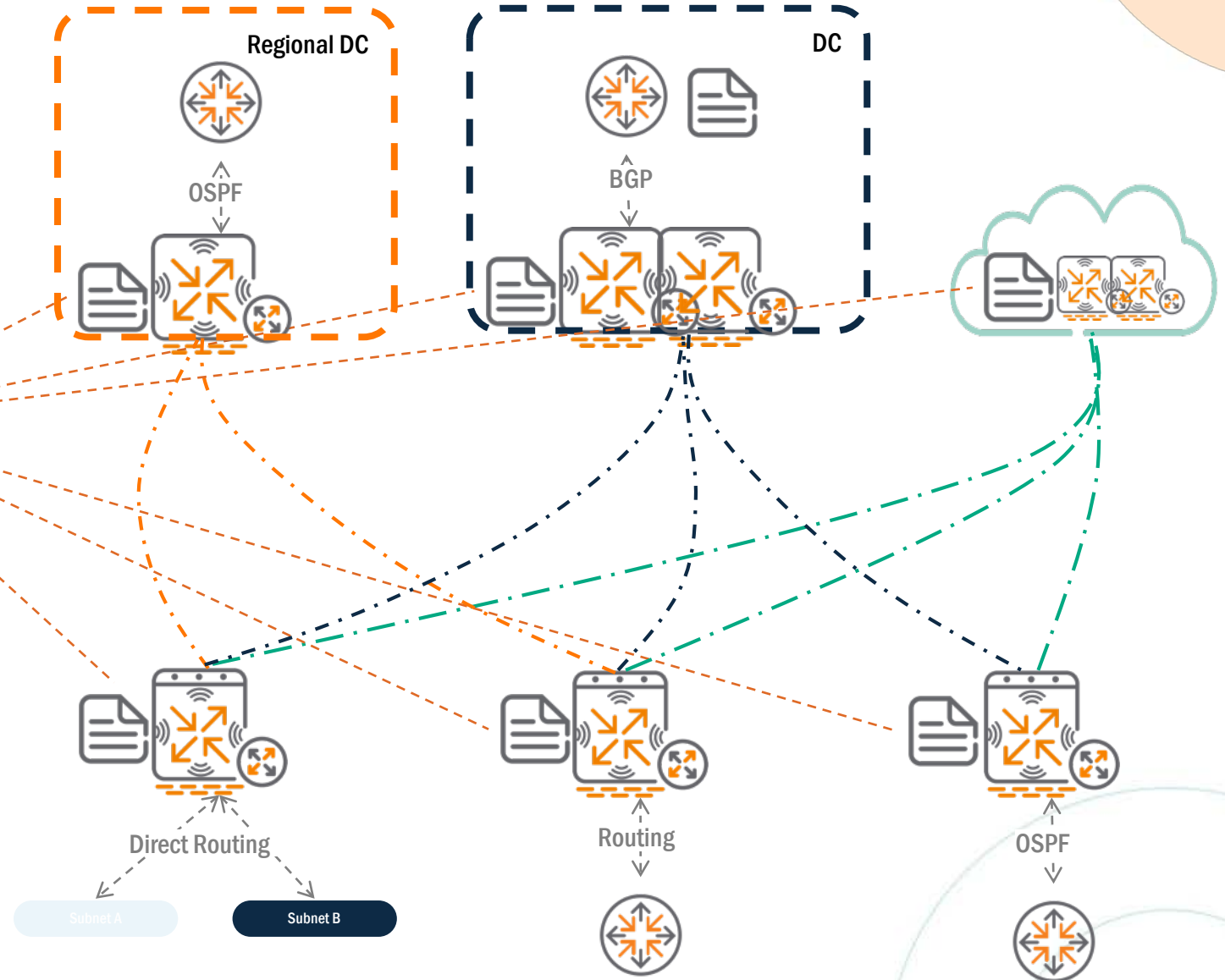
SD-WAN Orchestration

Why is it important??

How did we connect things before?

Orchestrated SD-WAN

Cloud-Native SD-WAN Orchestrator

Boss: *We're launching a new app. We need to make XYZ changes.*
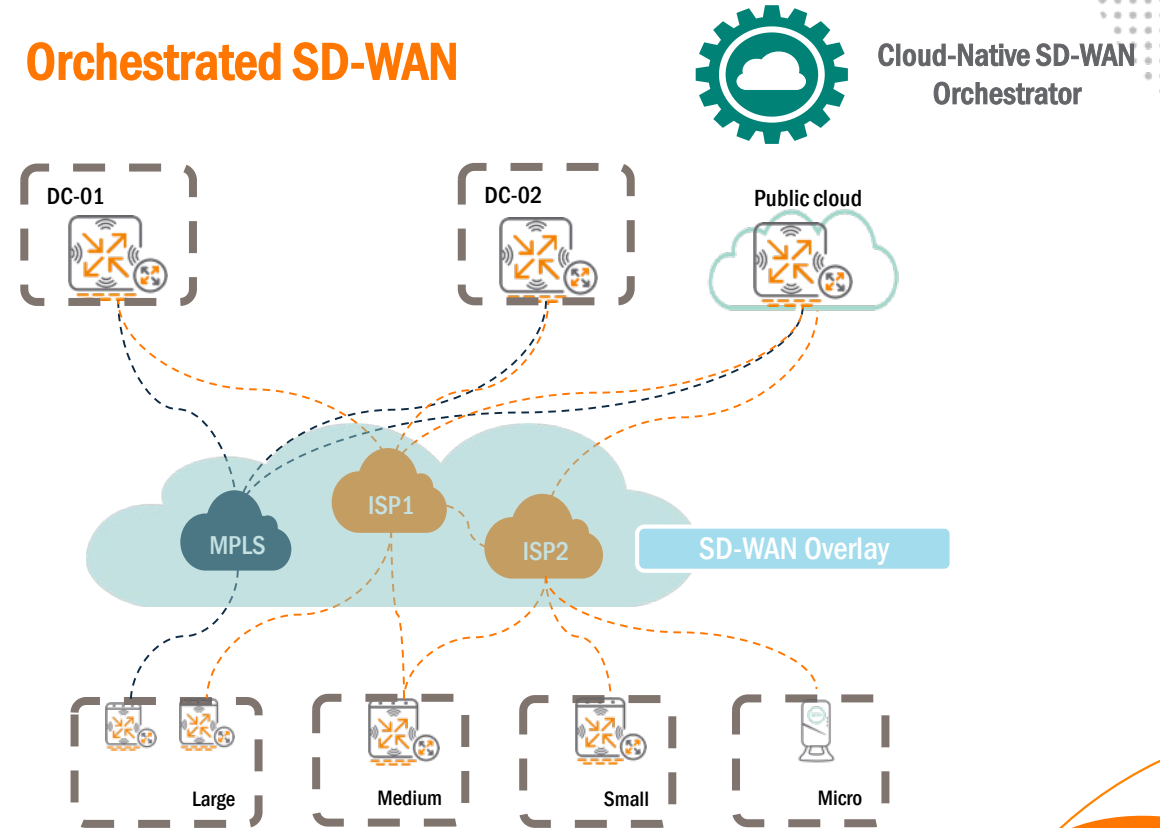
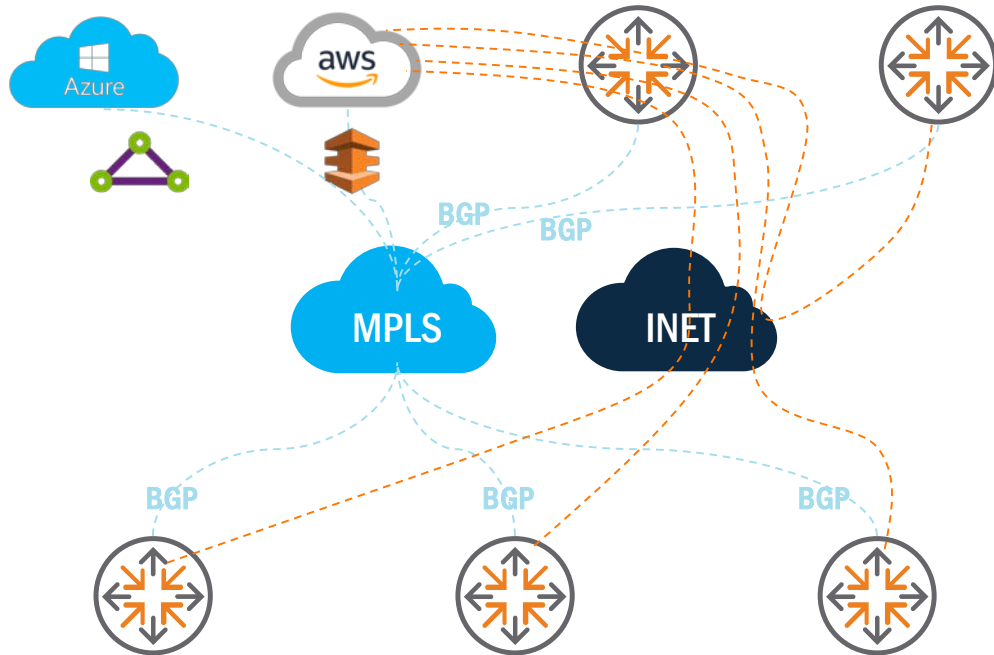**Boss:** *We're launching a new app. We need to make XYZ changes.*

Done!

Demo

Public Cloud Integration

Azure   awsmarketplace

Why is it important?

How did we connect to IaaS before?

Orchestrated Virtual Gateway

Azure   aws

BGP   BGP

MPLS   INET

BGP   BGP   BGP
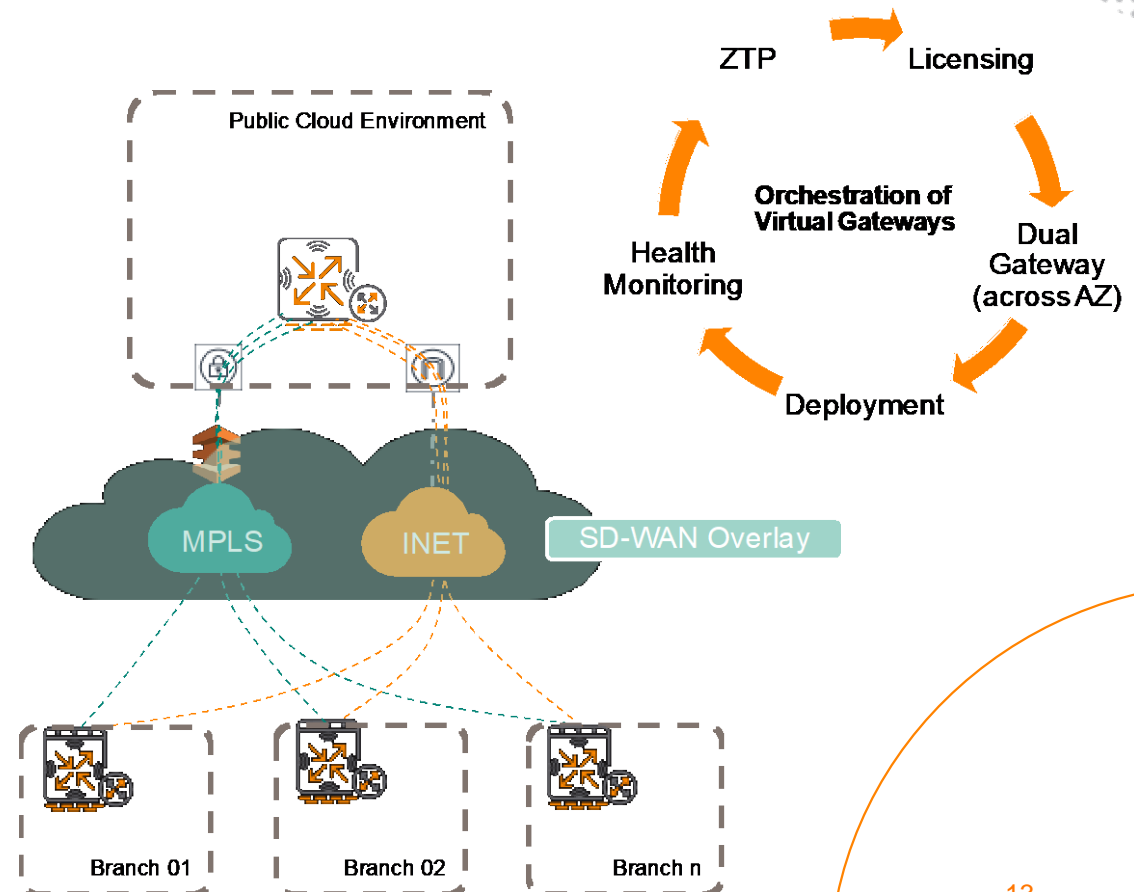
Boss: *We're starting to deploy apps in us-east-1 (aws) and west-us (azure)*

ZTP   Licensing

Orchestration of Virtual Gateways

Health Monitoring   Dual Gateway (across AZ)

Deployment

Public Cloud Environment

MPLS   INET   SD-WAN Overlay

Branch 01   Branch 02   Branch n

13

Aruba vGW in Public Cloud Marketplace

Customer

1 Purchases subscription from Aruba

2 Search for product in Marketplace --> Subscribe!

3 Generate 3rd party token for Central

4 Orchestrate vGW from Aruba Central!

Aruba Cloud

1 Load vGW Subscription in Aruba Central

2 Search for Aruba vGW in the marketplace and subscribe.

3 Request 3rd party token

4 Bring up Aruba vGW and orchestrate connectivity

5 Customer pays AWS/Azure for IaaS

aws marketplace

Microsoft Azure Marketplace

Manage Experience
Ensuring Quality

Quality of Experience

Definitely Important!

How did we ensure quality before?
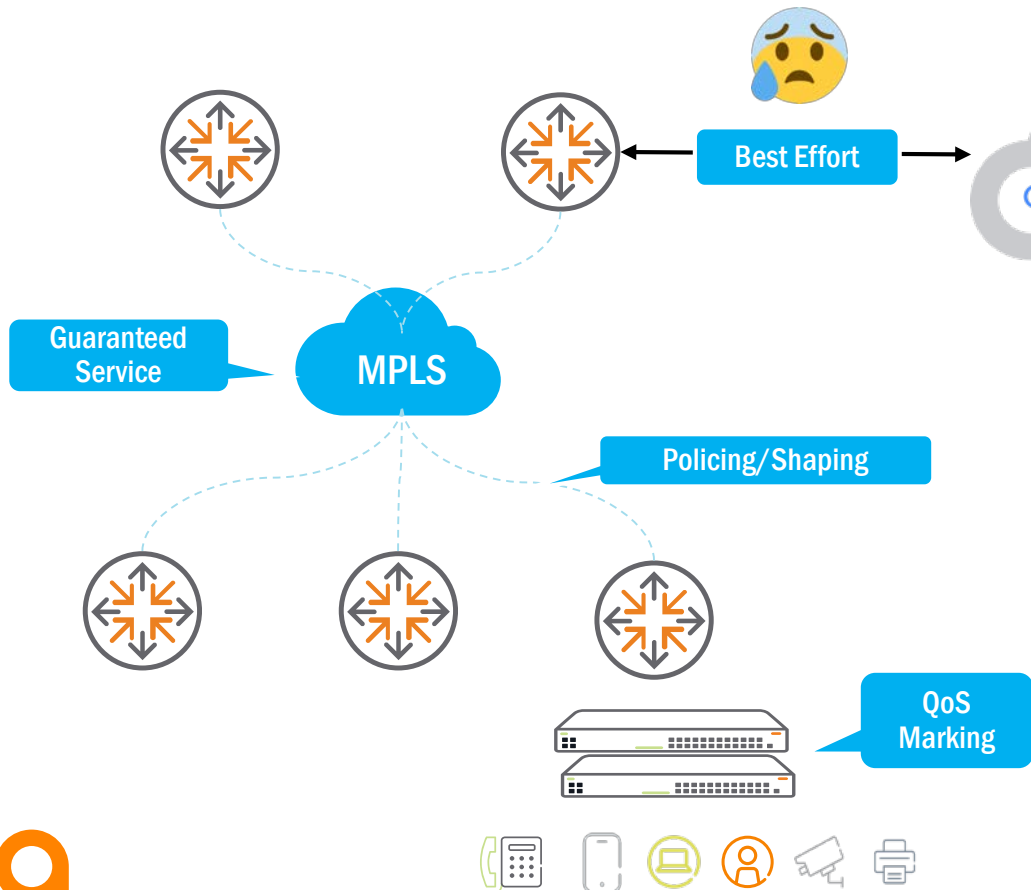
How is QoE achieved with SD-WAN?

Best Effort

Office 365
Google Dropbox

Guaranteed Service

MPLS

Policing/Shaping

QoS Marking

Data Center

Aruba PQM Service (ACP)

3 Headend Gateways

4 SaaS Applications

2 Aruba Cloud

ISP1

ISP2

1 Default Gateways

Branch gateway monitors SLA (latency, jitter, loss, utilization)

Branch
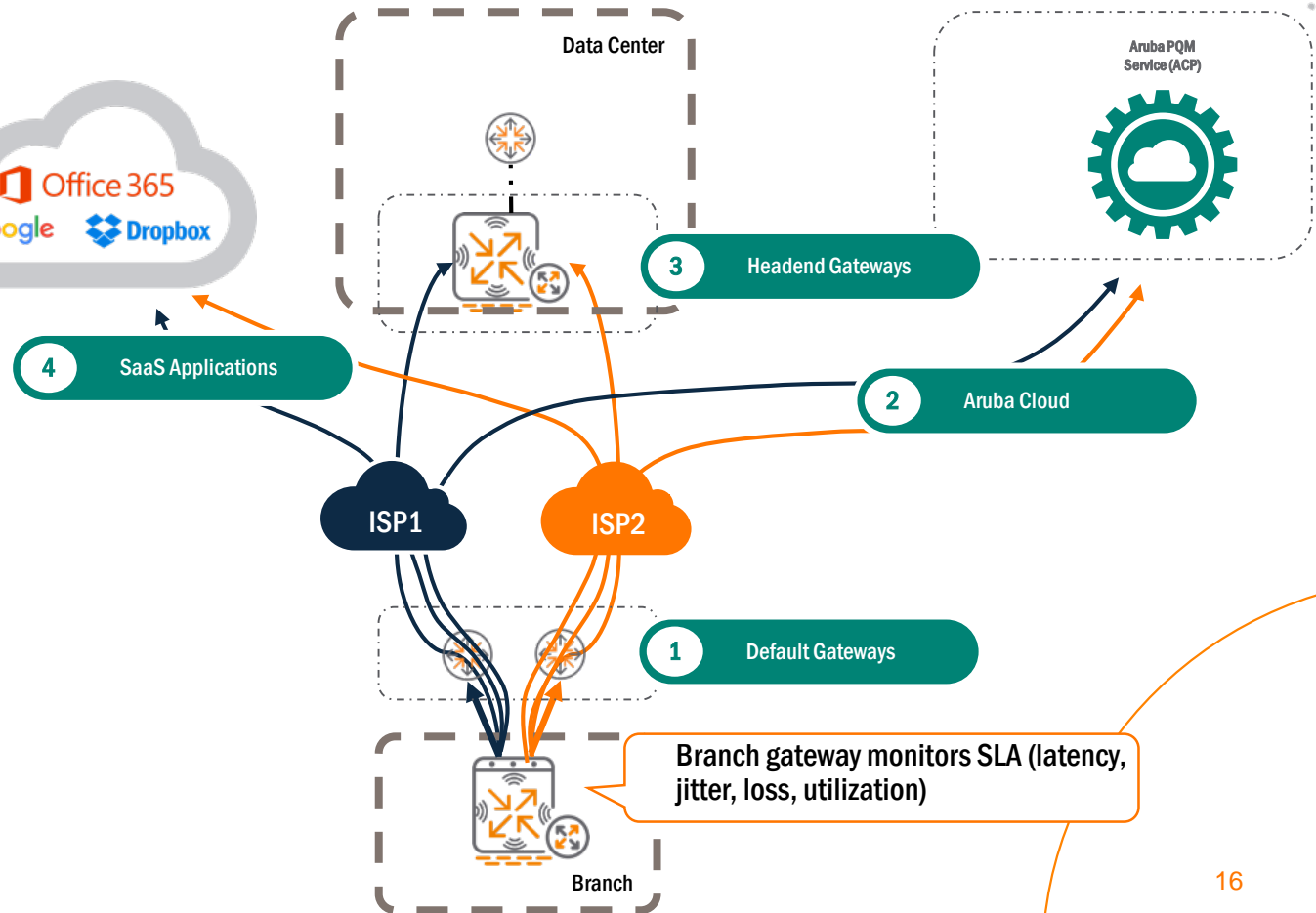
Dynamic Path Steering

How does it help me?

— **What was the challenge?**

- — VoIP Services are critical, making low-latency and low-jitter MPLS very desirable.

- — At the same time, MPLS couldn't cope with BW demands of new applications

— **How did we address it?**

- — Aruba SD-WAN monitors state of all WAN circuits for latency, loss, jitter and utilization.
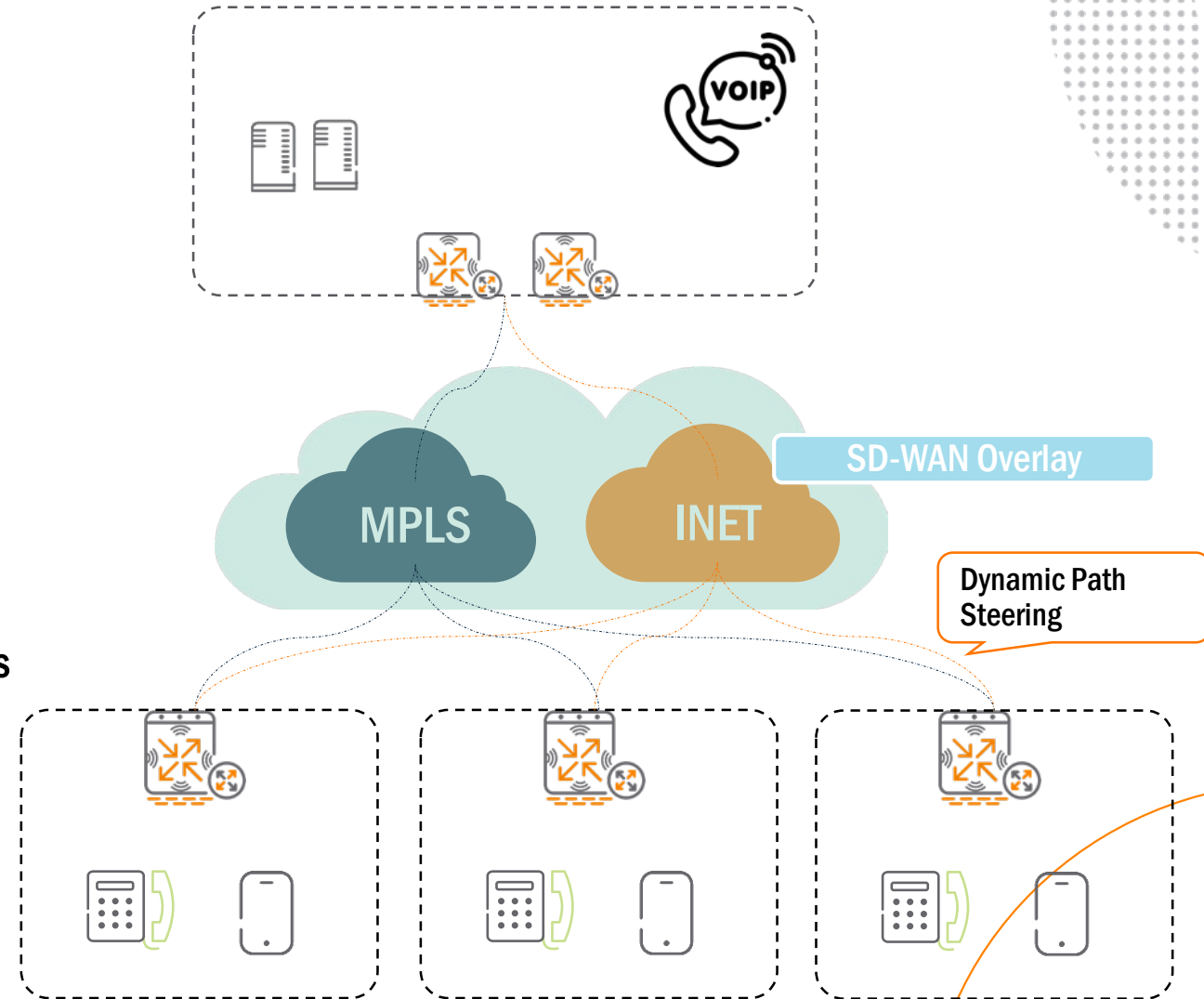
- — Aruba SD-WAN applies **double QoS tagging for MPLS links**, and **App-based QoS scheduling for Internet circuits**

- — Dynamic Path Steering selectively places traffic on the ideal circuit:
  - — MPLS for latency/jitter sensitive traffic
  - — INET for BW-Hungry applications
  - — Traffic is steered in real-time if SLA isn't met

VOIP

SD-WAN Overlay

MPLS   INET

Dynamic Path Steering

Dynamic Path Selection/Steering

1 Role + Application

Per user role, classify important applications for e.g. Employee Business Critical, Voice, Best-Effort, Guest

2 SLA

Delay

Jitter

Loss

Configure SLA parameters per user & application category

3 Path Preference

MPLS

Internet

4G/LTE

Configure path preference and fall back options per application category
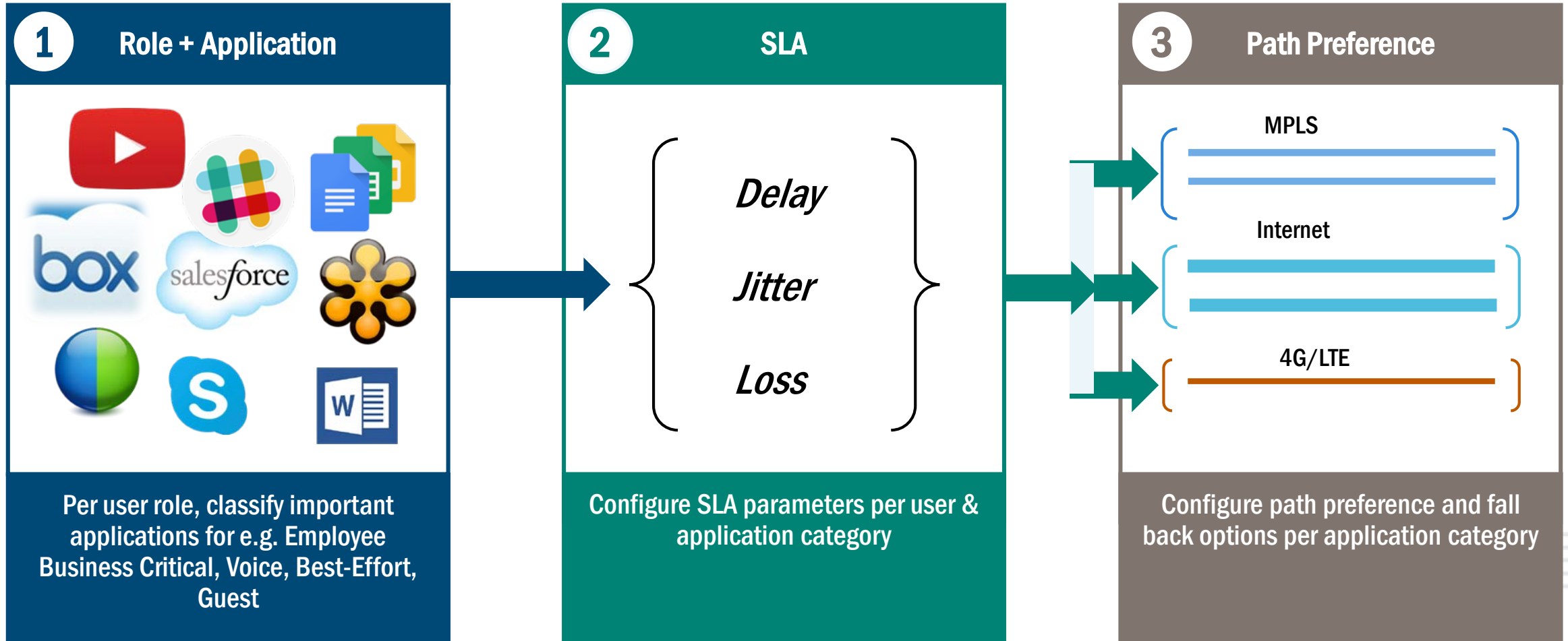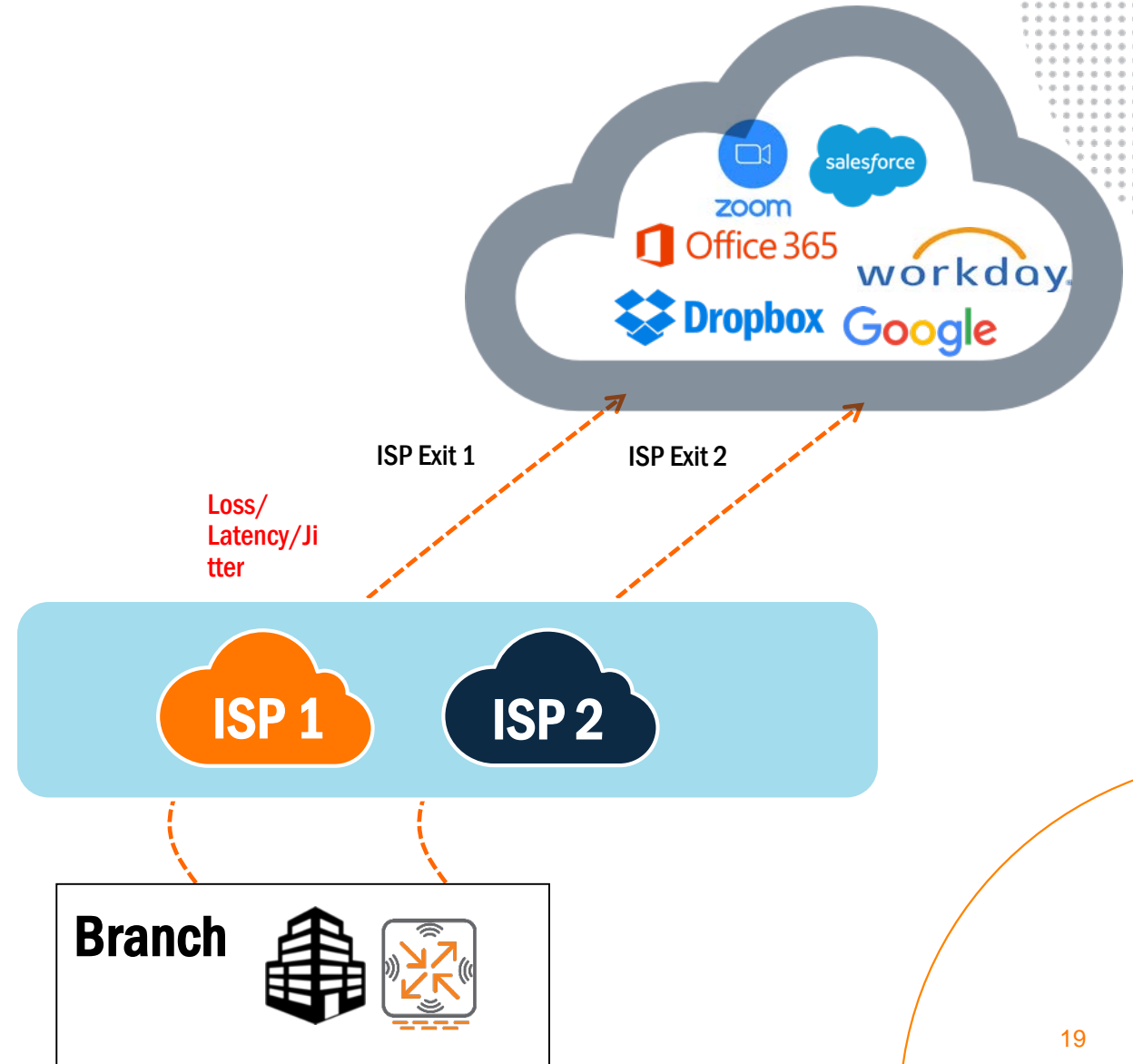
SaaS Optimization

How does it work?

— Dynamically identify optimal routes for high-priority SaaS solutions, such as Office 365

- HTTP probes to SaaS to measure end-to-end Quality of Experience from each branch

- Redirect DNS request through selected ISP
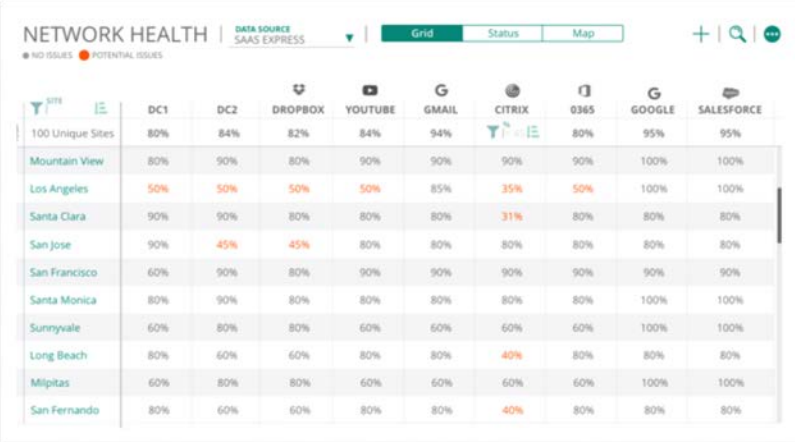
- First Packet Classification

SaaS Optimization

## How does it help me?

- **What was the challenge?**
  - Nation-Wide deployment, heavy dependence on SaaS Services deployed nation-wide
  - Devices in Corporate network use corporate DNS, which is inevitably hosted in the corporate DC
  - Failover can take up to 30s with default timers (we could go as low as 2-3s, but that would be overkill).

- **How did we deliver this?**
  - SaaS Express
    - HTTP probes to SaaS to measure end-to-end Quality of Experience from each branch
    - Redirect DNS request through selected ISP
    - First Packet Classification

NETWORK HEALTH	DATA SOURCE SAAS EXPRESS								
	SITE	DC1	DC2	DROPBOX	YOUTUBE	GMAIL	CITRIX	O365	GOOGLE	SALESFORCE
100 Unique Sites	80%	84%	82%	84%	94%		80%	95%	95%
Mountain View	80%	90%	80%	90%	90%	90%	90%	100%	100%
Los Angeles	50%	50%	50%	50%	85%	35%	50%	100%	100%
Santa Clara	90%	90%	80%	80%	80%	31%	80%	80%	80%
San Jose	90%	45%	45%	80%	80%	80%	80%	80%	80%
San Francisco	60%	90%	80%	90%	90%	90%	90%	90%	90%
Santa Monica	80%	90%	80%	80%	80%	80%	80%	100%	100%
Sunnyvale	60%	80%	80%	60%	60%	60%	60%	100%	100%
Long Beach	80%	60%	60%	80%	80%	40%	80%	80%	80%
Milpitas	60%	80%	80%	80%	80%	60%	60%	100%	100%
San Fernando	80%	60%	60%	80%	80%	40%	80%	80%	80%

SaaS Nodes

Branch

DC
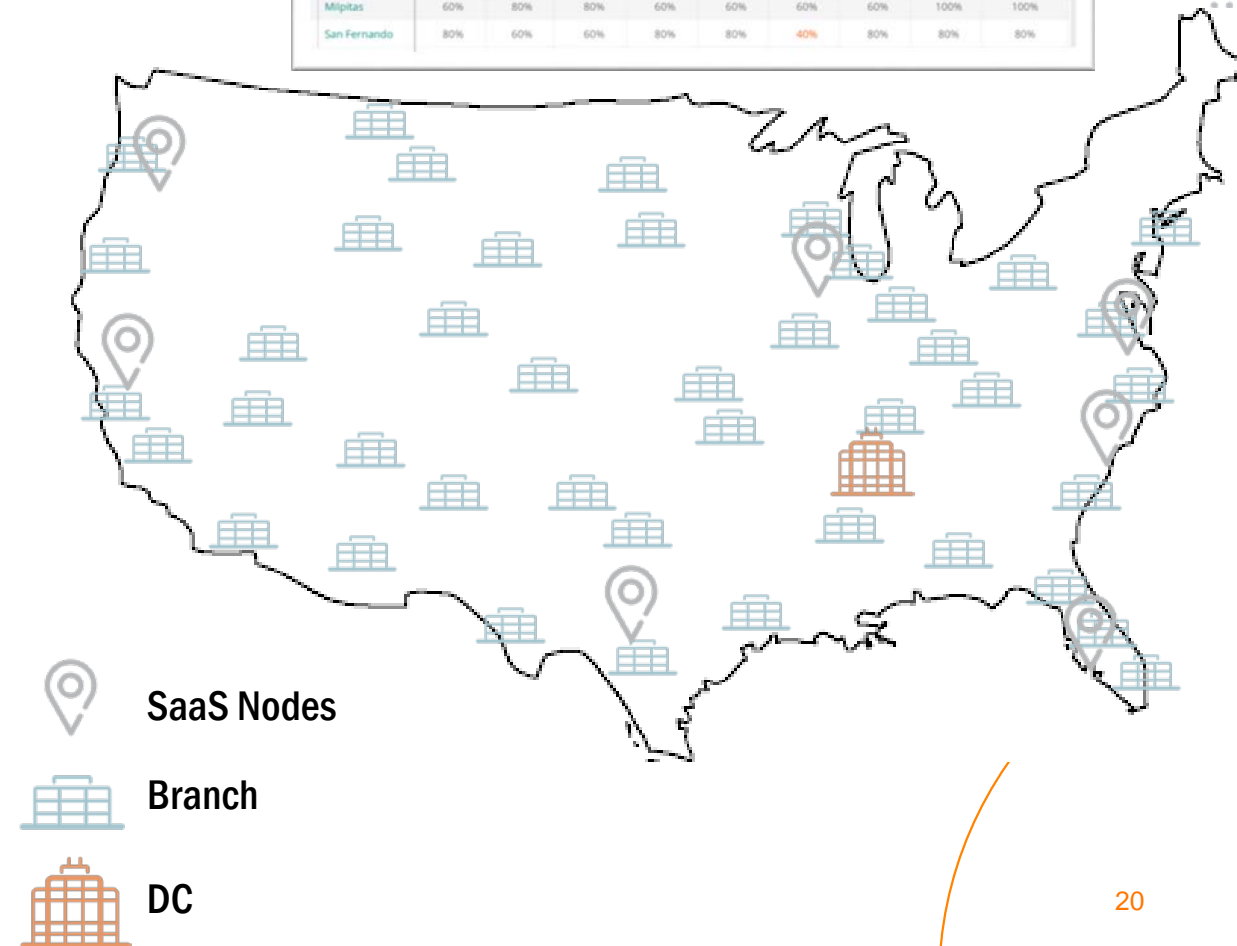
End to End Security

Zero Trust Security in the Branch

Roles are "Dynamic"

"Segmentation" even within the same VLAN

Users and Devices

Applications, Destinations and Users

ClearPass

Corp

BYOD

IOT

Guest

Role-based Branch Firewall!!

Office 365

Network Camera

n0tma1ware.biz

AirGroup

Unified Branch Defense in Depth

Cyber Kill Chain

Zero Trust Architecture
First-Line of Defense
ClearPass Policies
Policy Enforcement Firewall

User/Device Finger-printing/Auth
Role-Based Access Cont
Dynamic Segmentation

Stateful, L7 Firewall, DF
Web Content, 3100+ App Class
IP/Domain Reputation & URL

IDPS Rule Sets, CVE
Signature & Pattern base

Emerging Methods for possible APTs
New precedents/policies to minimize risk
Integration to 3rd Party CASB, Cloud FW

Emerging Threat
Intelligence Feeds/Score
40+ Threat Categories
3rd Party Integration

3rd Party
Actionable
events to SOC or
CPPM

Require analysis for SOC to detect potential
Zero-day, Insider Threat, Breach

1 Reconnaissance
2 Weaponization
3 Delivery
4 Exploitation
5 Installation
6 Command & control
7 Action on Objectives

Threat Intelligence Categories

- Malware Command and Control Server
- Known Infected Bot
- Known Spam Source
- Drop site for logs or stolen credentials
- Spyware Reporting Server
- Questionable Gaming Site
- Drive by Source
- POLICY Chat Server
- POLICY Tor Node
- Known compromised or Hostile
- P2P Node
- Proxy Host
- IP Check Services
- Known Good Public Utility
- Target of a DDoS
- Host Performing Scanning
- SSH or other brute forcer

- Fake AV and AS Products
- Domain or IP Related to a Dynamic
- DNS Entry or Request Undesirable but not illegal
- Abused or free TLD Related
- Self Signed SSL or other suspicious encryption
- Blackhole or Sinkhole systems
- GoToMyPC and similar remote access services
- Distributed CnC Nodes
- Domain or SEO Parked
- VPN Server
- Observed serving executables
- Known CnC for Mobile specific Family
- Spyware CnC specific to mobile devices
- Observed Skype Bootstrap or Super node
- Bitcoin Mining and related
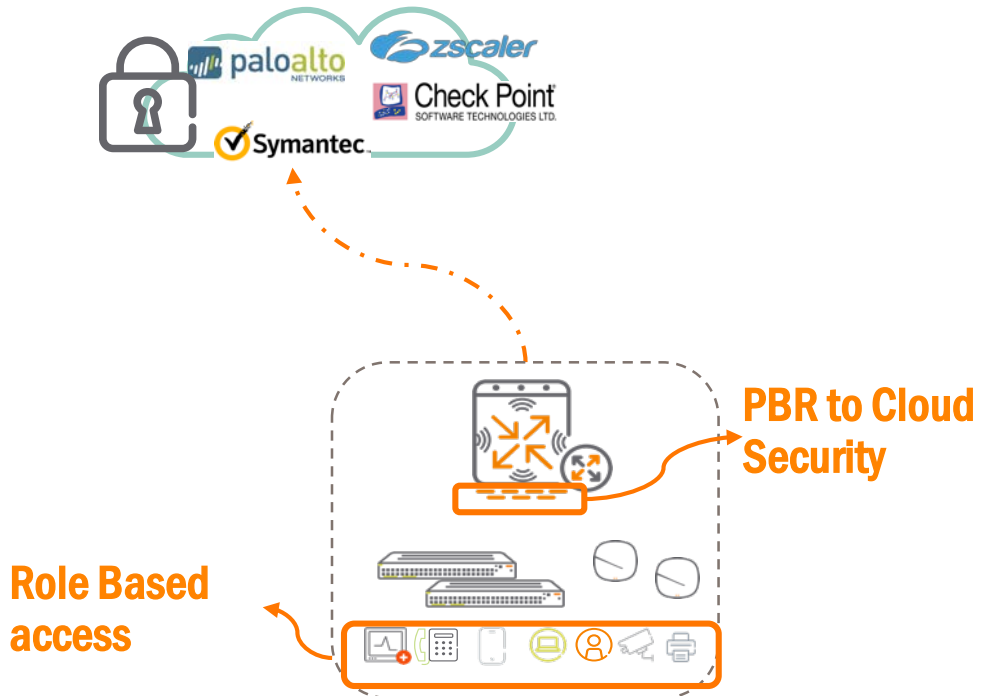- DDoS Source

Security Dashboard

- **Threats Over Time**
  - User/App Launch & Network Traffic vs Threat
  - Threat Trends
- **Threat Metrics**
  - By category, type and severity
  - Threat prevalence
  - Impacted users / device
  - Source and level of impact
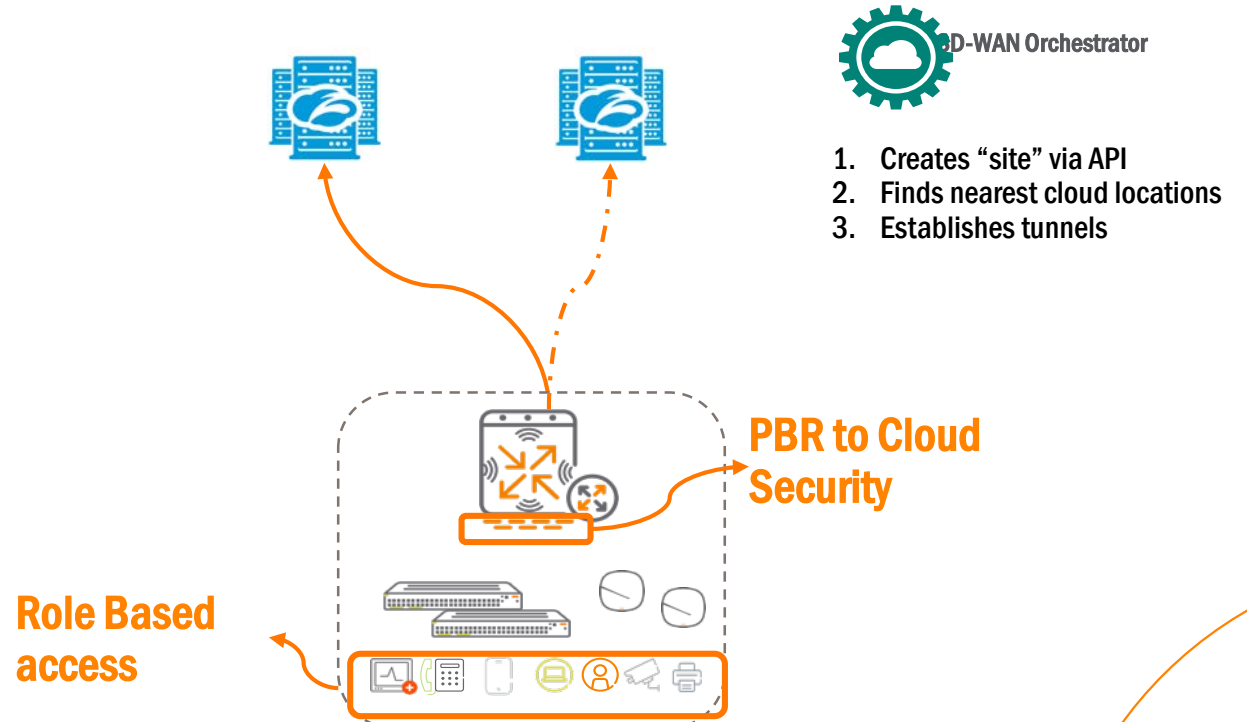- **Drilldowns**
- **SIEM integration (Splunk)**
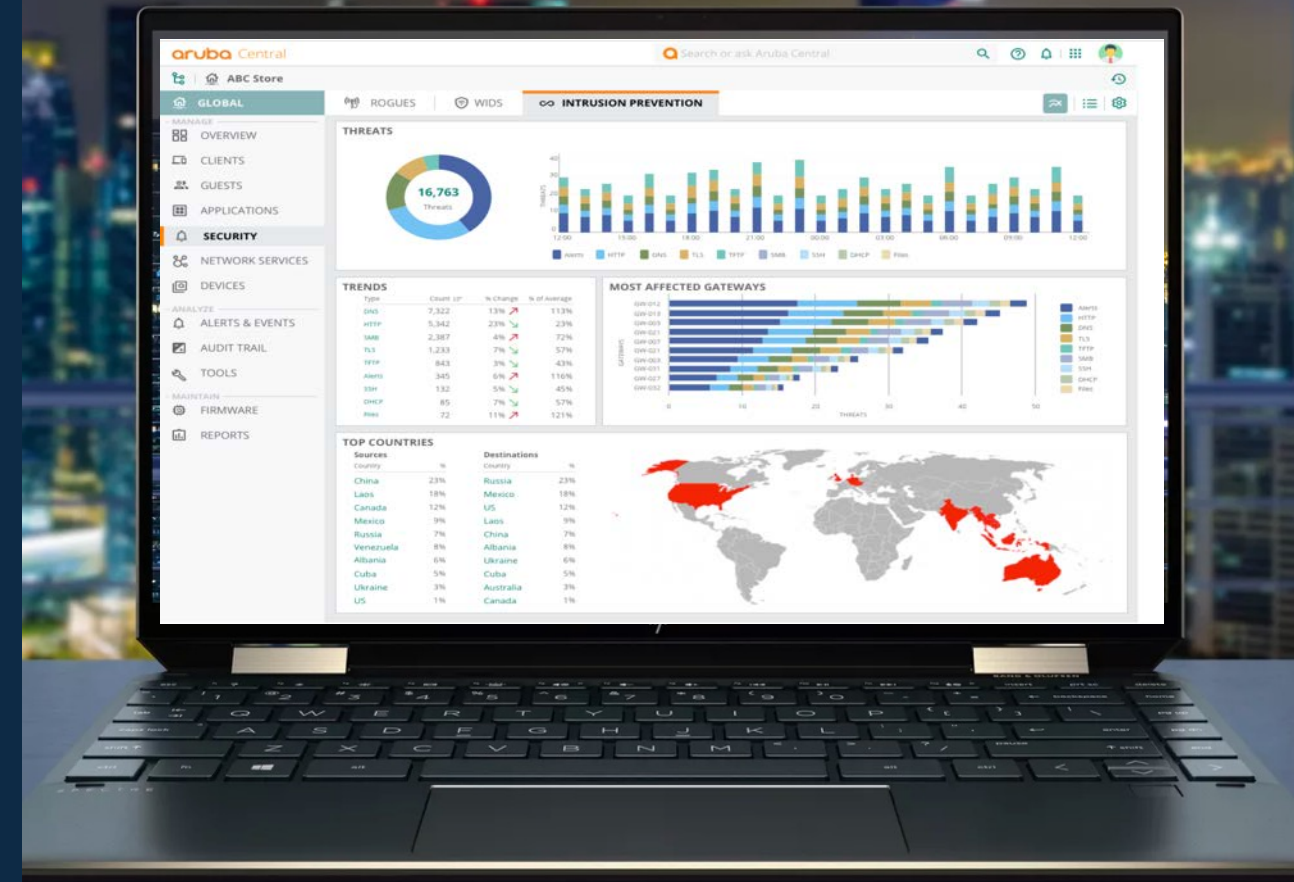
Cloud Security Integrations

Where does advanced security make most sense for branches?

Manual Integration

Orchestrated Integration

SD-WAN Orchestrator

1. Creates "site" via API
2. Finds nearest cloud locations
3. Establishes tunnels

PBR to Cloud Security

Role Based access

PBR to Cloud Security

Role Based access

SD-Branch Security & Zero Trust

How does it help me?

- **What was the challenge?**
  - IoT leading to VLAN explosion (20+)
  - Individually configured colored ports are hard to manage at scale.
  - Large-scale NAC project (100s of clinics/hospitals). is difficult to handle with VLAN derivation. Not every device reacts well to CoA Port-Bounce

- **How did we deliver this?**
  - Underlay VLAN for infrastructure mgmt.
  - Overlay VLANs for branch services (as low as 1 VLAN).
  - Role-based security policies.

CLEARPASS • • •

POLICY MANAGEMENT

Profiles devices and place them in their right role

Role-based security policies.

Underlay VLAN

Internal traffic forced through branch gateway (firewall)

Services VLAN
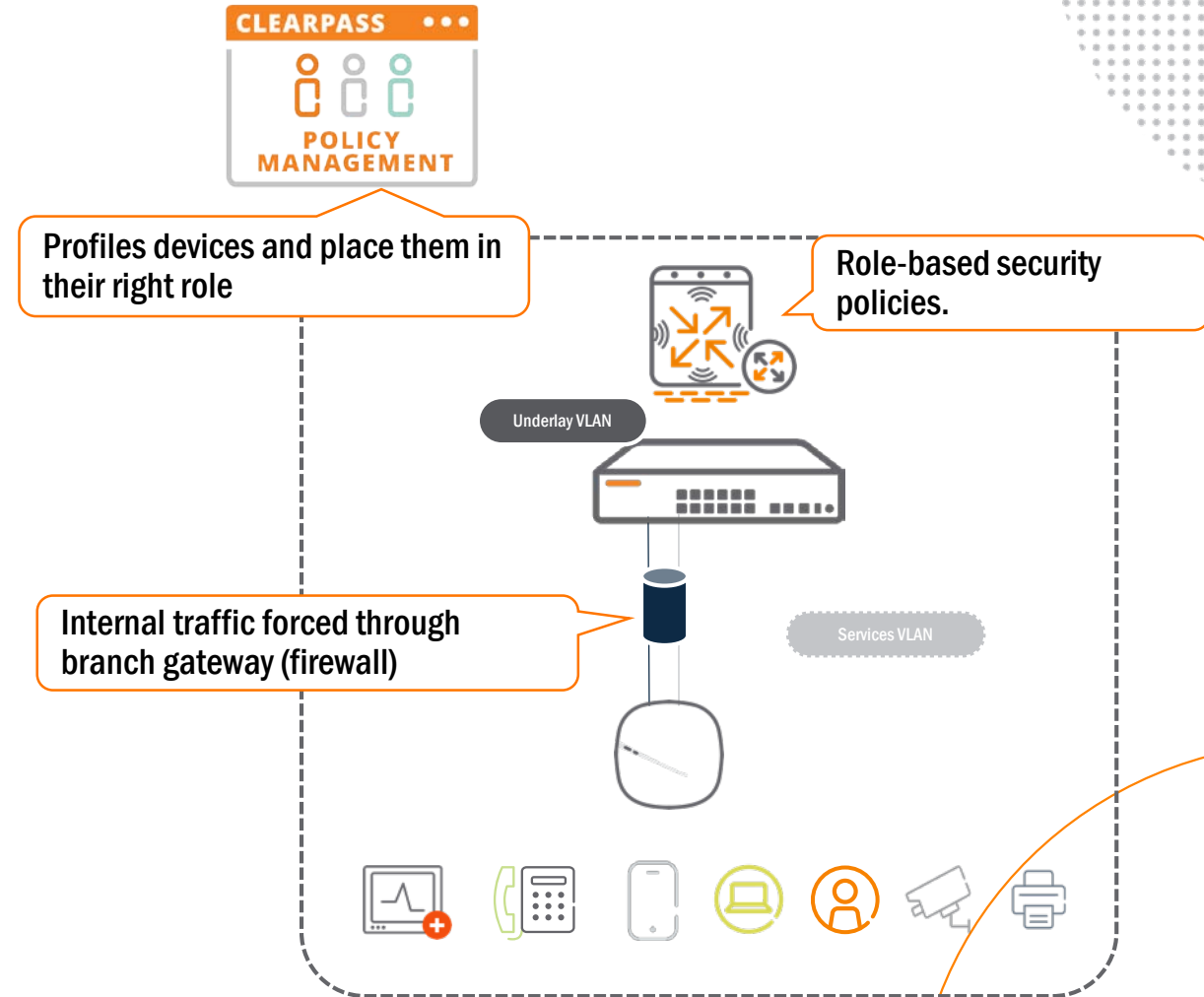
Simplified Operations
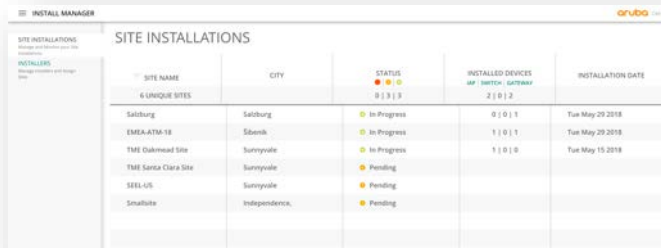
For the new normal

Streamlined Operations

This is great. How do I get here?

2 Installer scans devices
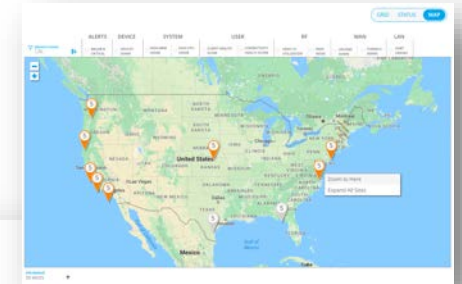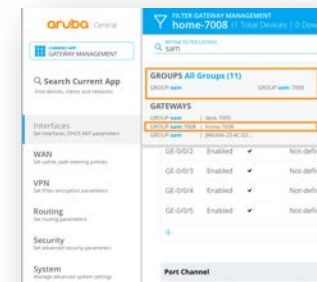
1 Create job
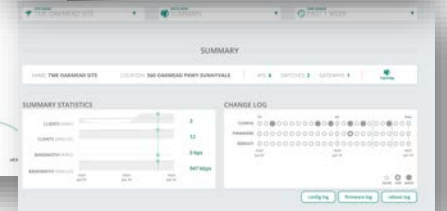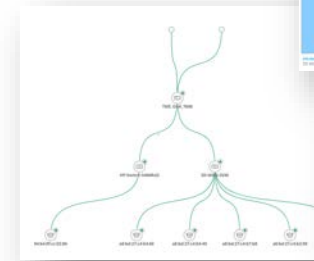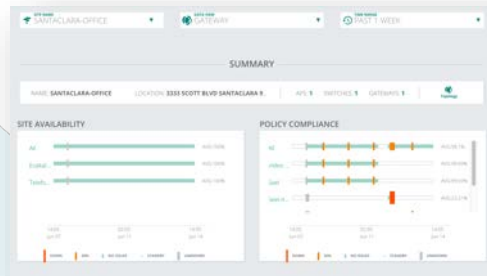
3 Devices geotagged Branch view created

4 Auto SW upgrade Hierarchical config pushed
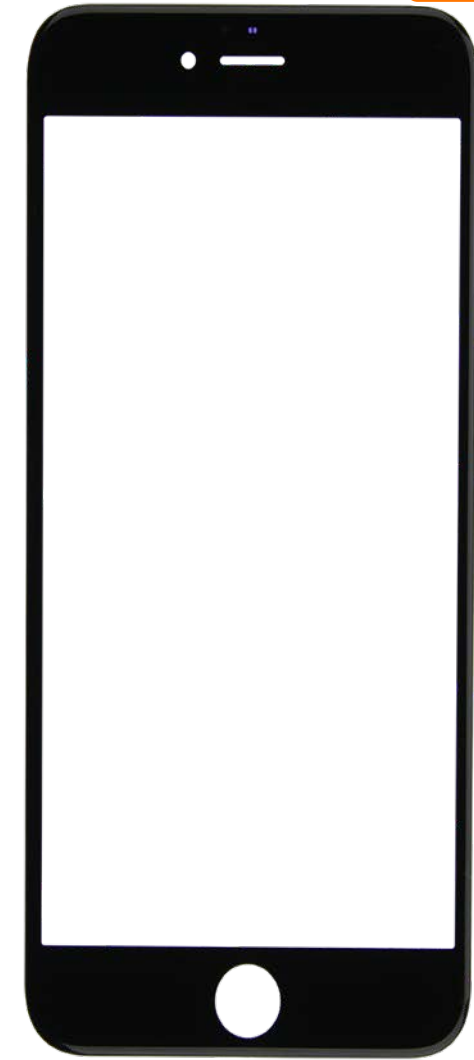
5 Proactive alerting/reporting on a site/group basis
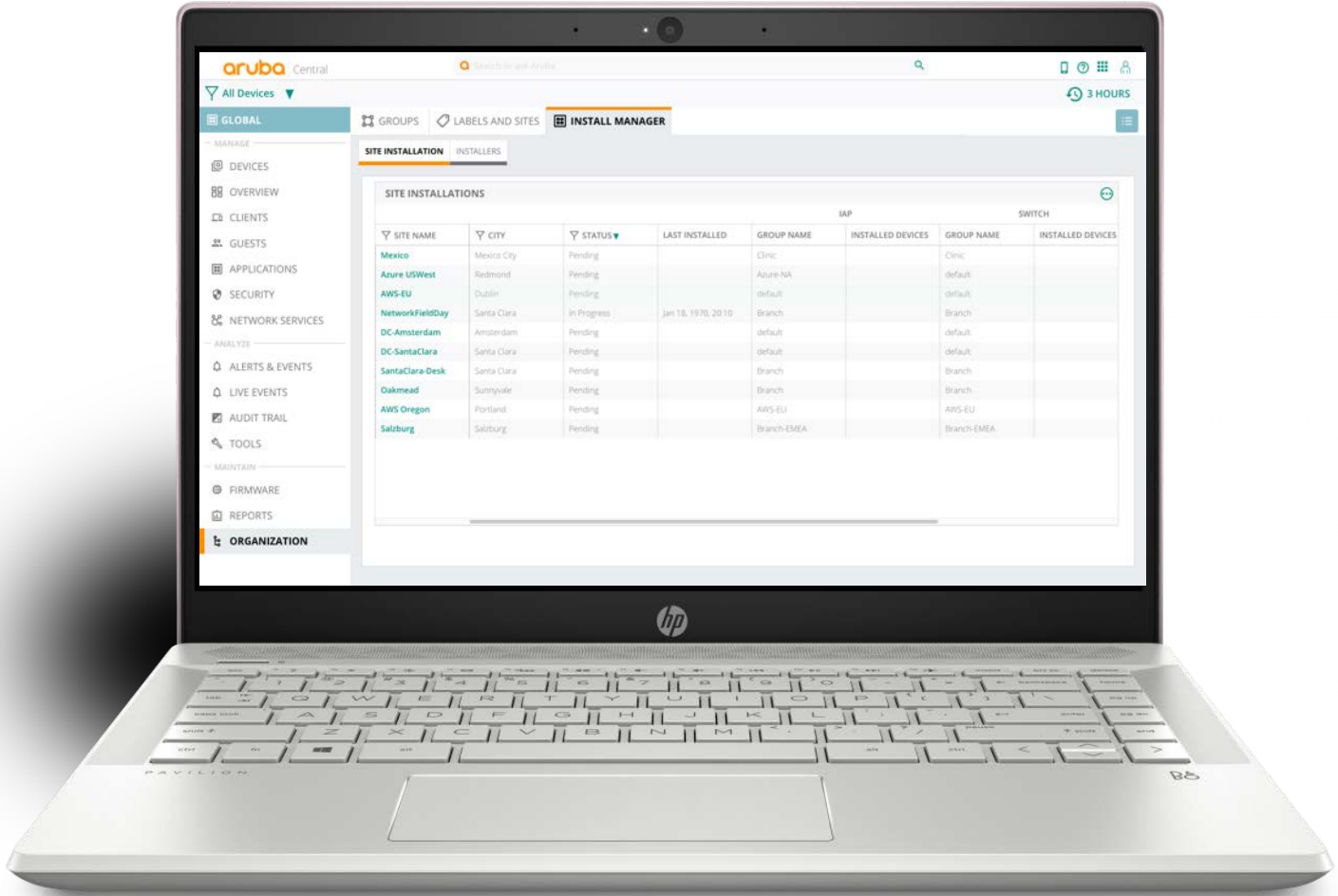
Report

API

Streamlined Operations

More than just monitoring...

Reports

Remote Console

Software Management

{REST}
API

API for all platform interactions

NETWORK MANAGEMENT

Troubleshooting

slack

now™

splunk>

...

Alerting

31
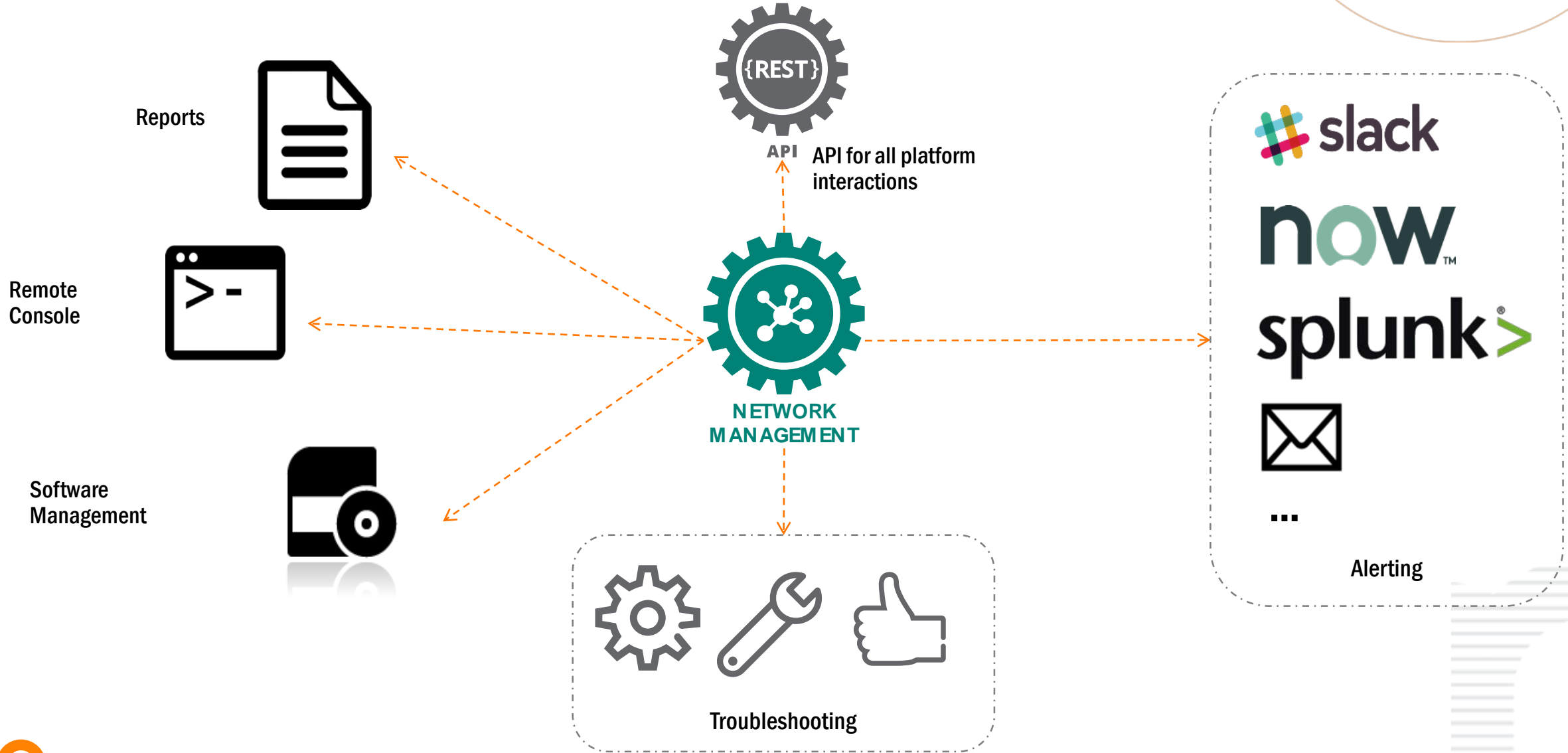
AI/ML POWERED TROUBLESHOOTING

AI Insights

Analytics Engine

Machine Learning

Network Expertise

Data Extraction
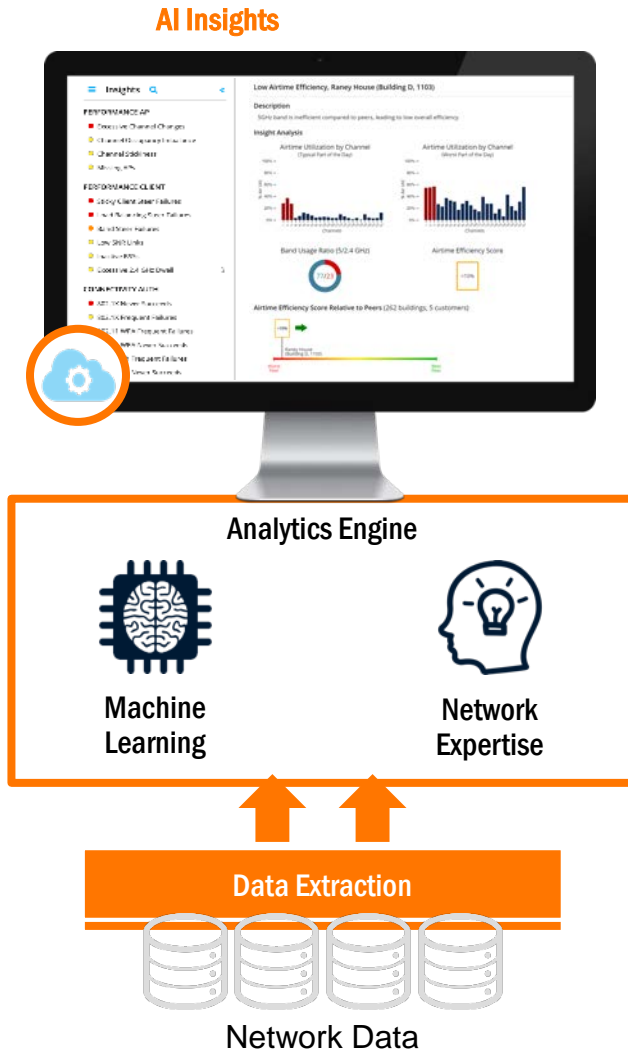
Network Data

Insights for improving network performance & user experience

Leveraging Machine Learning, Aruba network expertise & latest Cloud technologies to transform existing network data into advanced network analytics

SD-Branch = SD-WAN + SD-LAN

Security

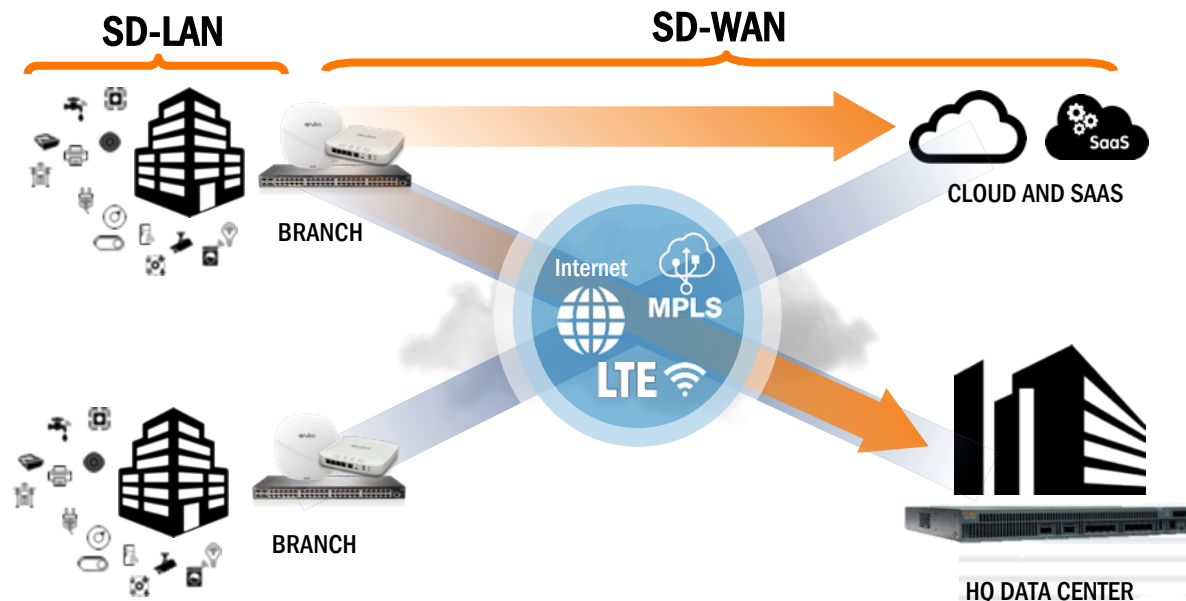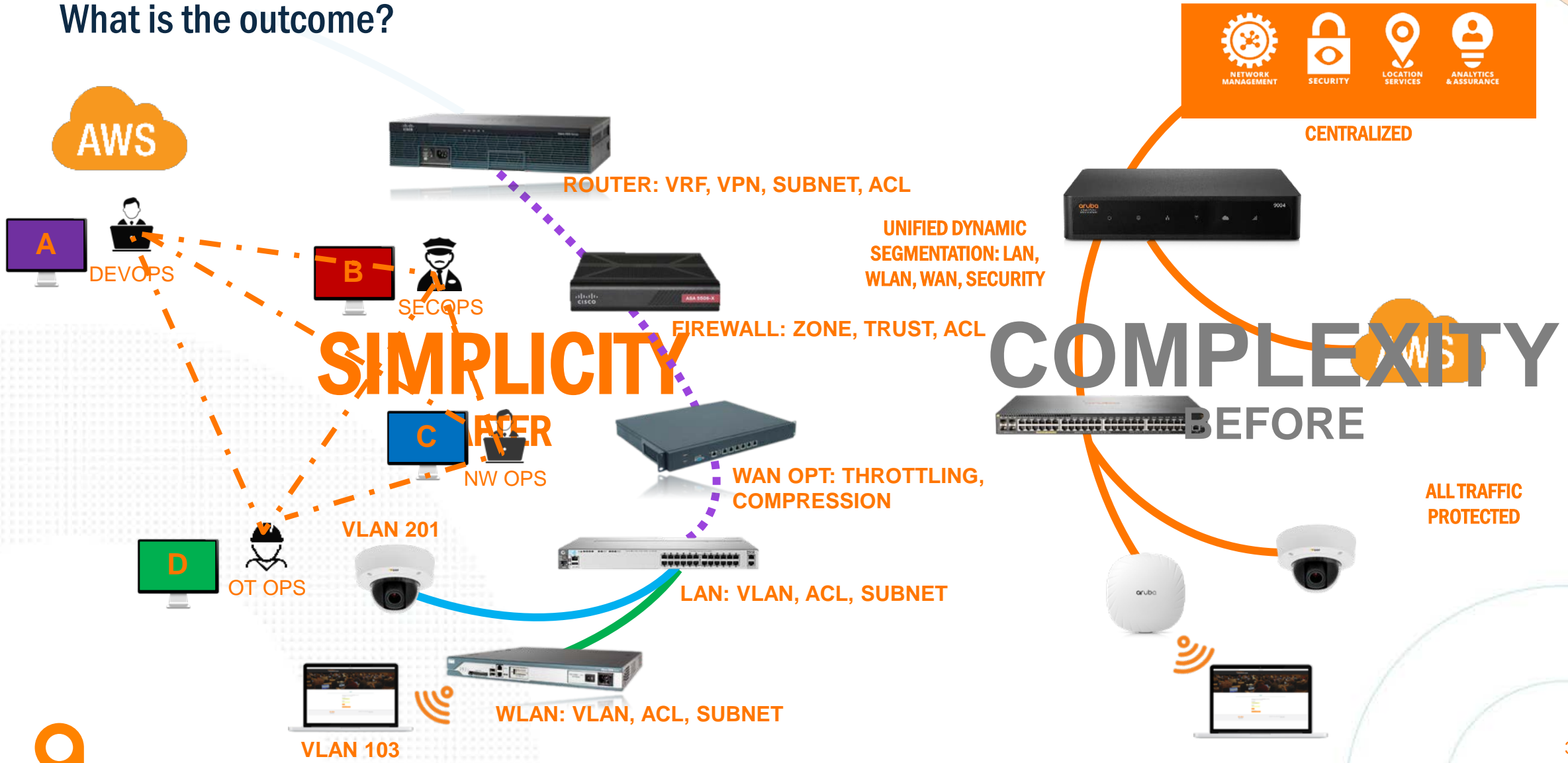| SD-WAN Seamless Orchestration	High-Performance Gateways with ZTP	Role/app-aware Dynamic Path Steering, SaaS Optimization
Orchestrated Cloud Connectivity	L3-7 Firewall Web content and reputation IDS/IPS	SD-LAN & Zero Trust

Aruba provides a scalable cloud-managed solution with a single pane of glass for LAN, WLAN, SD-WAN, and Security.

End-to-End SD-Branch Solution

What is the outcome?

AWS

A DEVOPS

B SECOPS

C NW OPS

D OT OPS

SIMPLICITY AFTER

VLAN 201

VLAN 103

ROUTER: VRF, VPN, SUBNET, ACL

FIREWALL: ZONE, TRUST, ACL

WAN OPT: THROTTLING, COMPRESSION

LAN: VLAN, ACL, SUBNET

WLAN: VLAN, ACL, SUBNET

CENTRALIZED

NETWORK MANAGEMENT   SECURITY   LOCATION SERVICES   ANALYTICS & ASSURANCE

UNIFIED DYNAMIC SEGMENTATION: LAN, WLAN, WAN, SECURITY

COMPLEXITY BEFORE

AWS

ALL TRAFFIC PROTECTED

34

SD-Branch Gateway Platforms

	Model
VPNC	7280
VPNC Large Branch (2.5.0)	7240
	7220
	7210
	7205
Medium Branch VPNC	7030
	7024
	7010
Small Branch GW	7008
	7005

Virtual Gateway (AWS + Azure)

VGW-4GB
AWS
Azure 2.5.2

VGW-2GB
AWS
Azure 2.5.2

VGW-500MB
AWS + AZ

NEW BGWs

9004-LTE
GA: June 2020

Available

Available

Please check supported Central version for new 9000 series gateways.

SD-Branch Subscriptions

License Features	Foundation Tier		Advanced Tier	
	Foundation	**Foundation Security**	**Advanced**	**Advanced Security**
Aruba Central Management – BGW/VPNC	Yes	Yes	Yes	Yes
Orchestration: Tunnel, Route, Cloud Security	Yes	Yes	Yes	Yes
Dynamic Path Steering	Yes	Yes	Yes	Yes
Link Redundancy	Yes	Yes	Yes	Yes
Application Aware Policies	Yes	Yes	Yes	Yes
High Availability (Active-Standy, Active-Active)	Yes	Yes	Yes	Yes
Web Content Filtering	Yes	Yes	Yes	Yes
Role Based Access Policy	Yes	Yes	Yes	Yes
Full SD-LAN Control	Yes	Yes	Yes	Yes
Layer 7 Stateful Firewall	Yes	Yes	Yes	Yes
IPSEC VPN	Yes	Yes	Yes	Yes
Client VPN	Yes	Yes	Yes	Yes
Anti-Malware		Yes		Yes
Intrusion Detection/Prevention System		Yes		Yes
Security Dashboard		Yes		Yes
Emerging Threat Intelligence*		Yes		Yes
SaaS Express			Yes	Yes
Recommended Platforms	700xx/72xx/90xx	90xx	70xx/72xx/90xx	90xx

Thank You

https://www.arubanetworks.com/products/networking/sd-wan/