atmosphere'23

BELGIUM

Because VPN's need a vacation too

Jan-Willem Keinke, Pre-Sales SE

19 October 2023

HPE aruba networking

SASE explained on a single slide

SASE is Secure SD-WAN plus SSE

Secure SD-WAN

- SaaS Acceleration
- WAN Optimization
- Tunnel Bonding
- Zero-Touch Provisioning
- Data Encryption
- Next-generation Firewall
- Granular Segmentation
- IDS/IPS and DDoS Protection

Security Service Edge (SSE)

- Zero Trust Network Access
- Cloud Access Security Broker
- Secure Web Gateway
- Firewall as a Service
- Remote Browser Isolation
- Data Loss Prevention
- Sandboxing

Delivered With The HPE Aruba SASE Portfolio

Secure Service Edge (SSE)

axis

Zero Trust Network Access (ZTNA)

PRIVATE APPLICATIONS

VPN Alternative – better UX, safer (Zero Trust), users not on network

Secure Web Gateway (SWG)

INTERNET ACCESS

Web proxy alternative – replace outbound security stack in DC

Cloud Access Security Broker (CASB)

SaaS APPLICATIONS

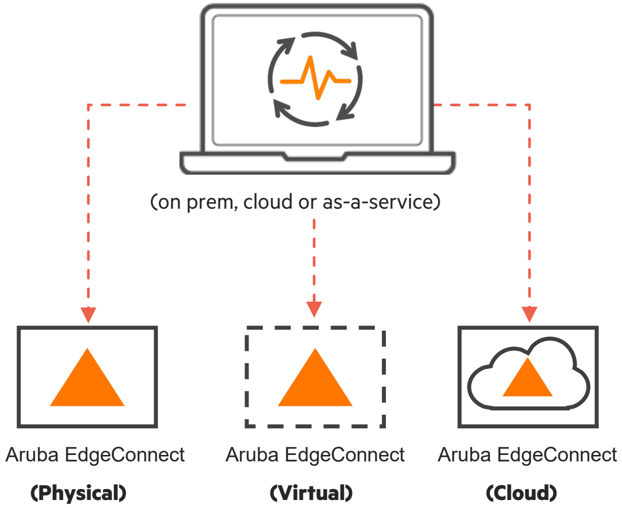
Protect users and data when using SaaS applications

Digital Experience Monitoring

PERFORMANCE MONITORING

Visibility – end to end view on user experience. Transform support desk.

Software Defined WAN (SD-WAN)



(on prem, cloud or as-a-service)

Aruba EdgeConnect **(Physical)**

Aruba EdgeConnect **(Virtual)**

Aruba EdgeConnect **(Cloud)**

Aruba Orchestrator

Centralized policy orchestration, monitoring and reporting

Aruba EdgeConnect

Unified SD-WAN edge platform: routing, security, SD-WAN and WAN Optimization

SECURITY

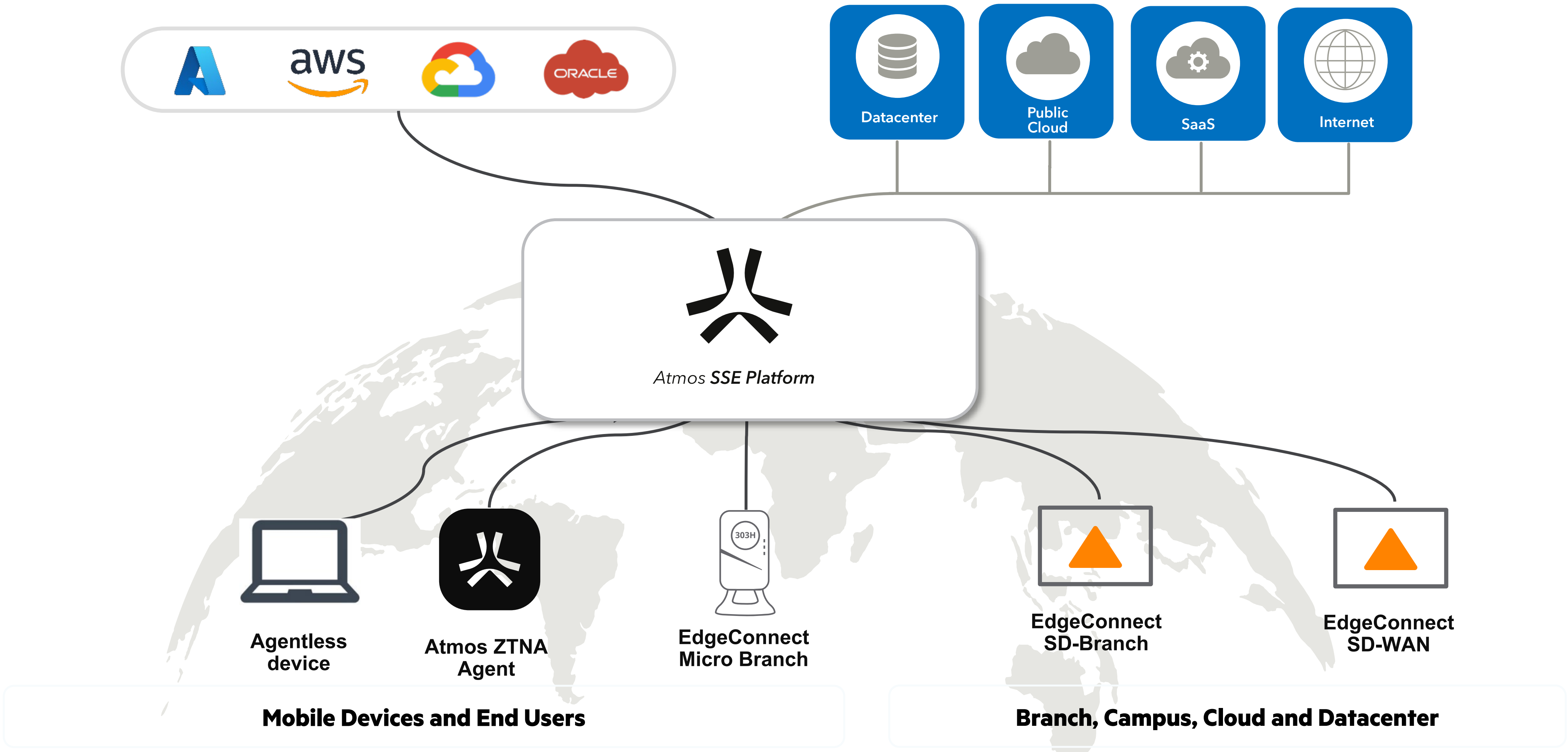
Aruba Advanced Security

Intrusion Detection and Prevention.

Aruba Boost WAN Optimization

On-demand WAN Optimization

Aruba SASE architecture



Mobile Devices and End Users

Branch, Campus, Cloud and Datacenter

Our differentiators – how we are better!

Unified access platform

Single: UI, policy engine, & data lake
(ZTNA, SWG, CASB, DEM)

Benefit: Significantly reduces management/operational overhead + reduces complexity

Simplify policy & inspect all traffic

for Internet, SaaS, and legacy apps
(SSH, RDP, VOIP, AS400, ICMP etc.)

Benefit: Inspect more than just SSL

Multi-cloud backbone with Smart Routing

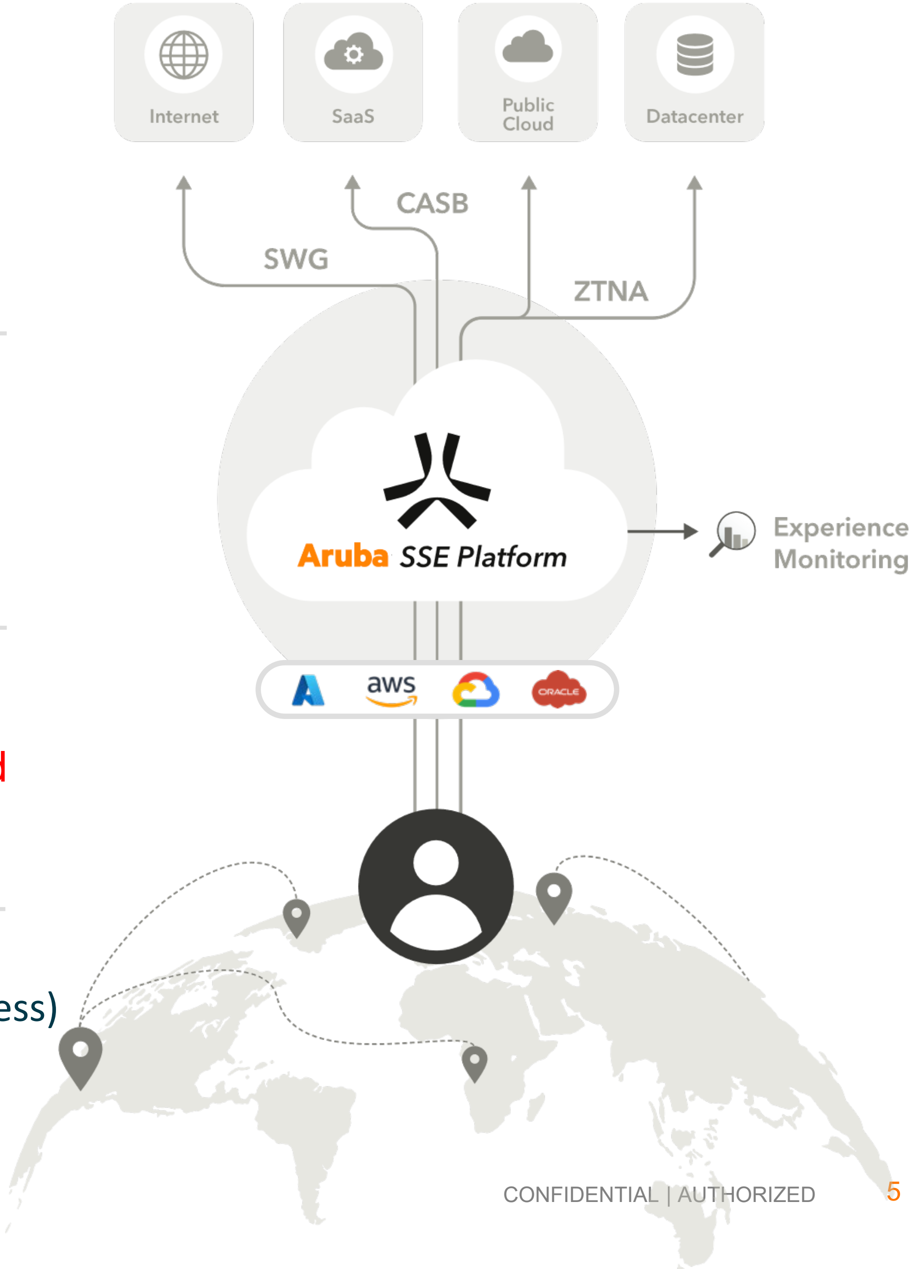
Harmonized access across the world with 350 NW acceleration on-ramps leveraging Azure, AWS, GCP, & Oracle

Benefit: Ever expanding connectivity options. Offer the best connectivity and performance anywhere

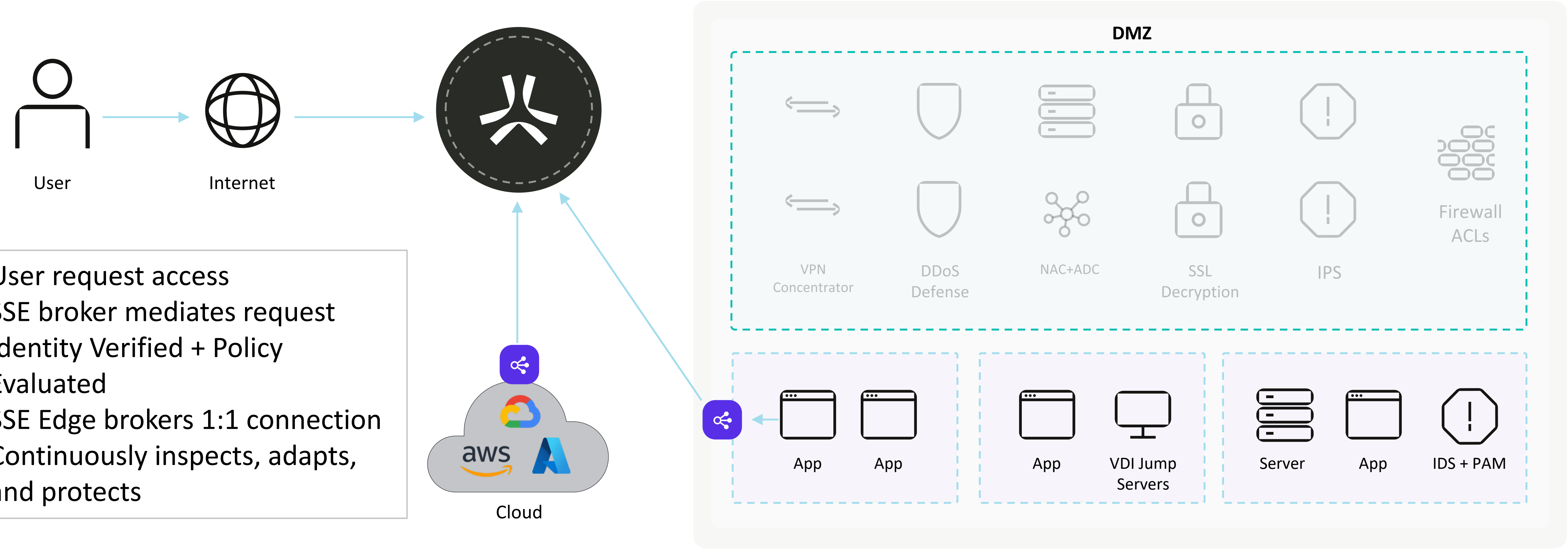
Agent or Agentless Zero Trust access

Agent – full SSE platform (parity with VPN capabilities)
Agentless – Zero Trust access to private Apps (Web/SSH/RDP/VNC/Git/DB Access)

Benefit: Completely eliminate VPN (incl. legacy e.g. VOIP) & support clientless 3rd party access



Axis delivers zero trust access for all



1. User request access
2. SSE broker mediates request
3. Identity Verified + Policy Evaluated
4. SSE Edge brokers 1:1 connection
5. Continuously inspects, adapts, and protects

The invisible network.

Inside-out connections make apps completely invisible and never exposed to the internet.

Application access, never network access.

Remote users only receive access to authorized applications without placing user or device on the corporate network.

Granular least privilege access.

App-to-user connections provide built-in app segmentation without complex network segmentation. One-to-one connections make lateral movement impossible for unauthorized users.

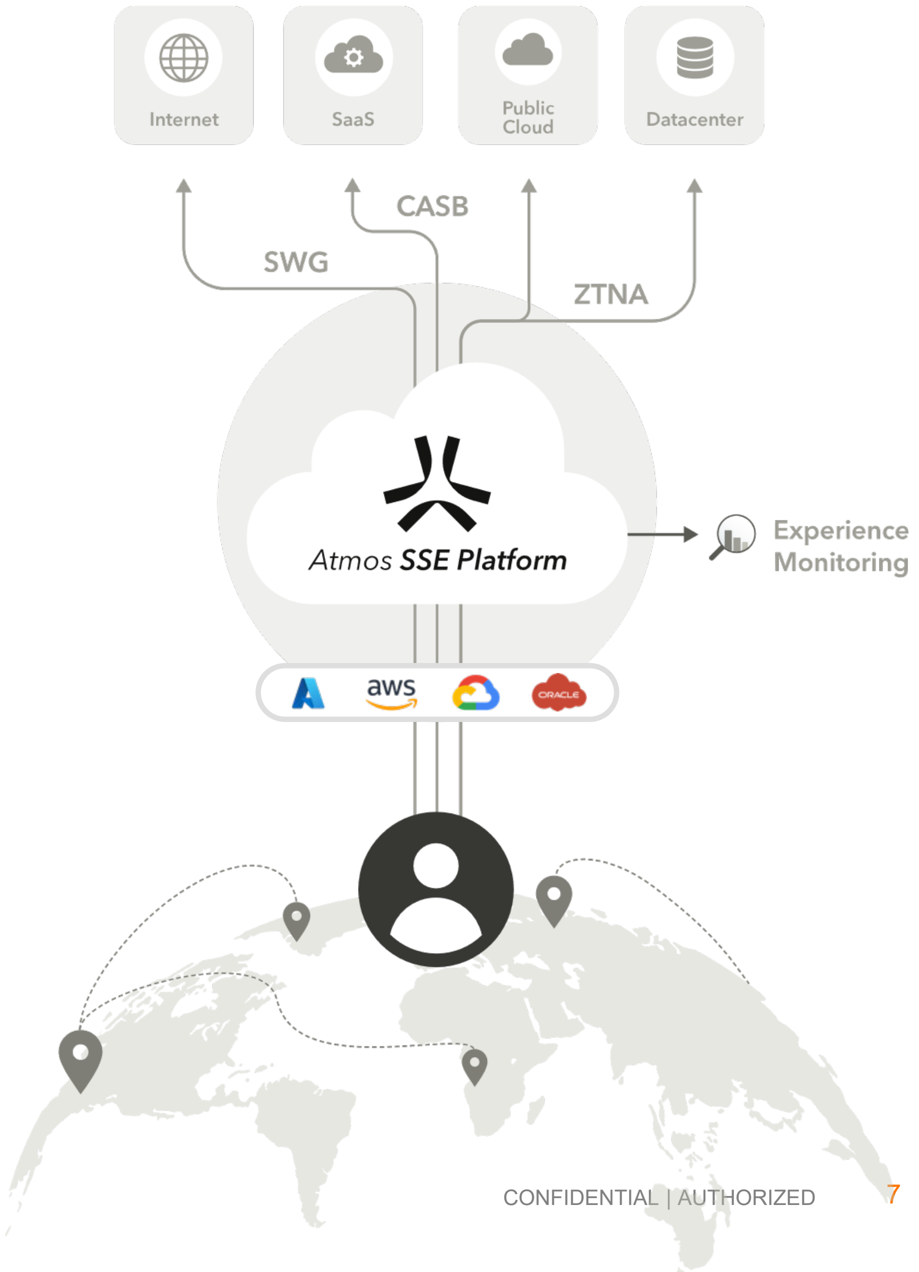
Why Aruba's SSE 2.0 Platform?

We focus on a unified access platform approach

We simplify policy & inspect traffic for Internet, SaaS, and legacy apps (SSH, RDP, VOIP, AS400, ICMP etc.)

We harmonize access across the world via a cloud-backbone of AWS, Azure, Google and Oracle

We enable users to access resources with or without an agent



Three-tiered cloud architecture

Tier 1 – Major cloud providers

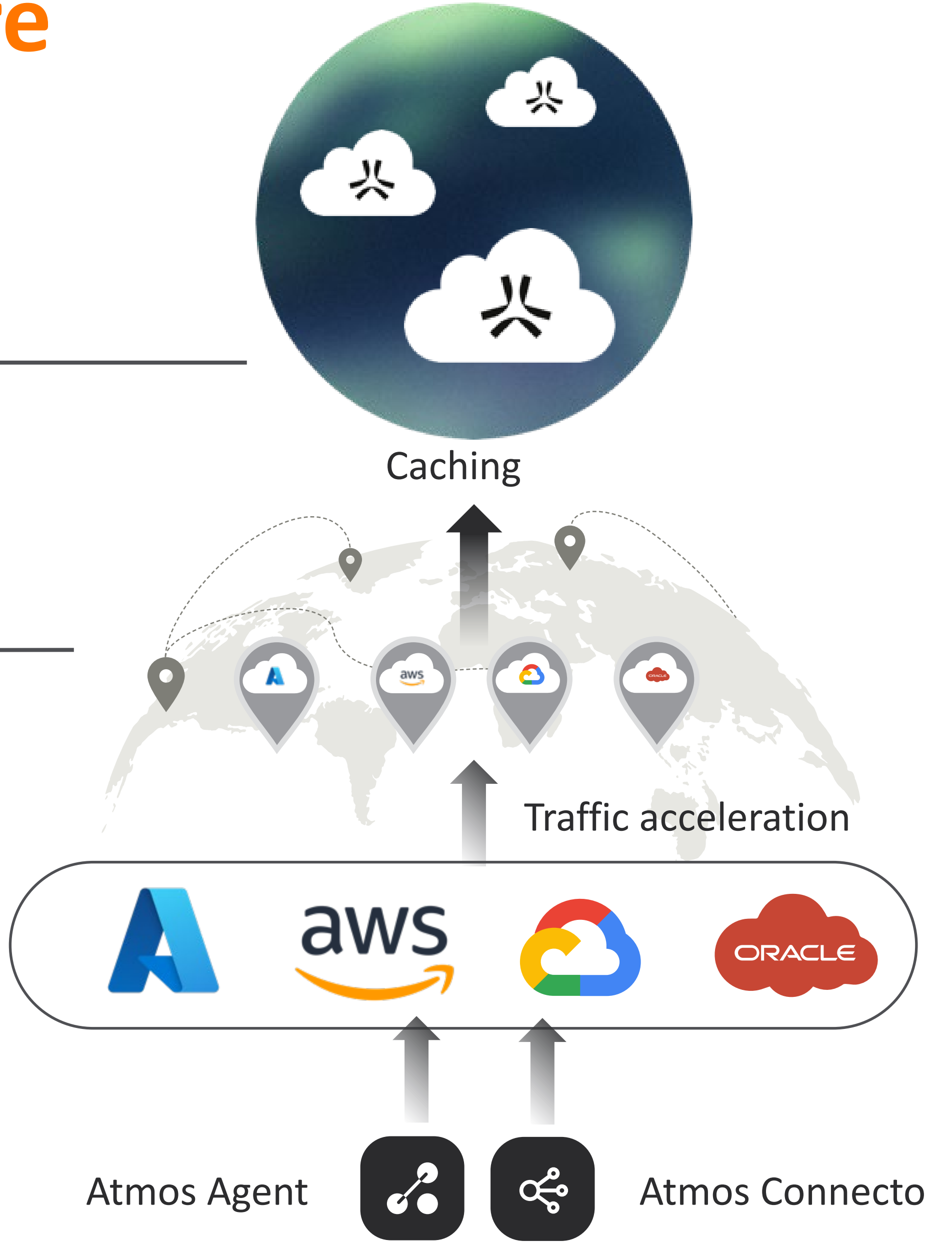
Main Clusters

Tier 2 – Cloud providers & local hosting services

Local PoPs

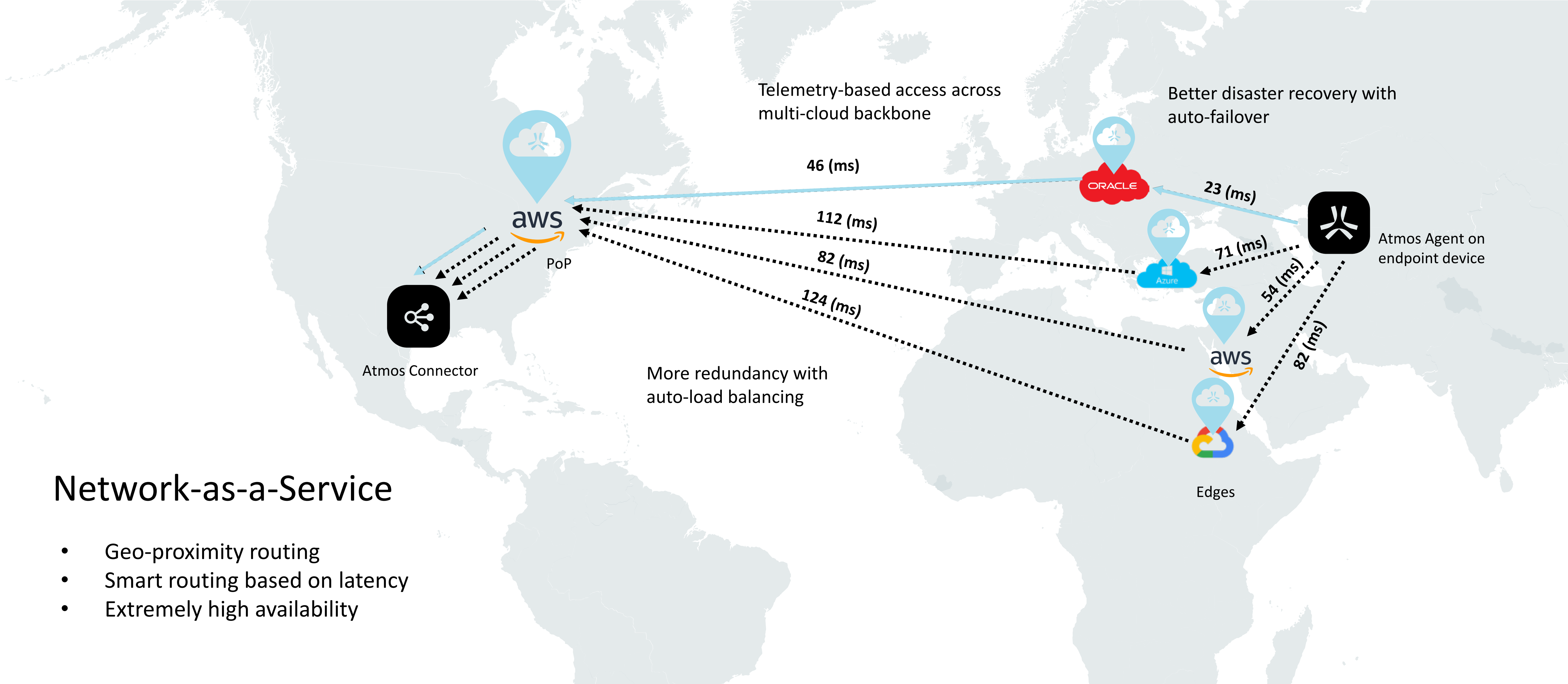
Tier 3 – Peered to local ISPs across the world

350 Edge Locations



Distributed cloud architecture:

High reliability, availability, and scale


Telemetry-based access across multi-cloud backbone
Better disaster recovery with auto-failover
46 (ms)
ORACLE
23 (ms)
aws
PoP
112 (ms)
82 (ms)
124 (ms)
71 (ms)
54 (ms)
82 (ms)
Azure
aws
Atmos Agent on endpoint device
Atmos Connector
More redundancy with auto-load balancing
Edges

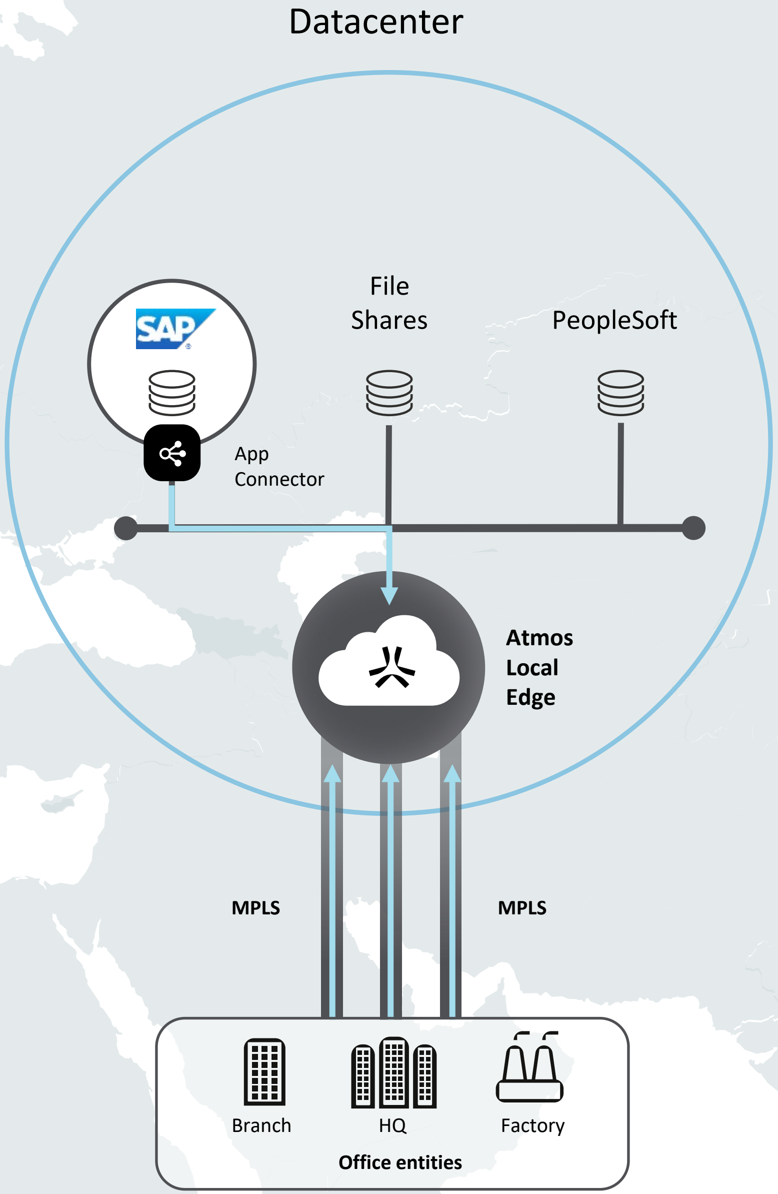
Network-as-a-Service

- Geo-proximity routing
- Smart routing based on latency
- Extremely high availability

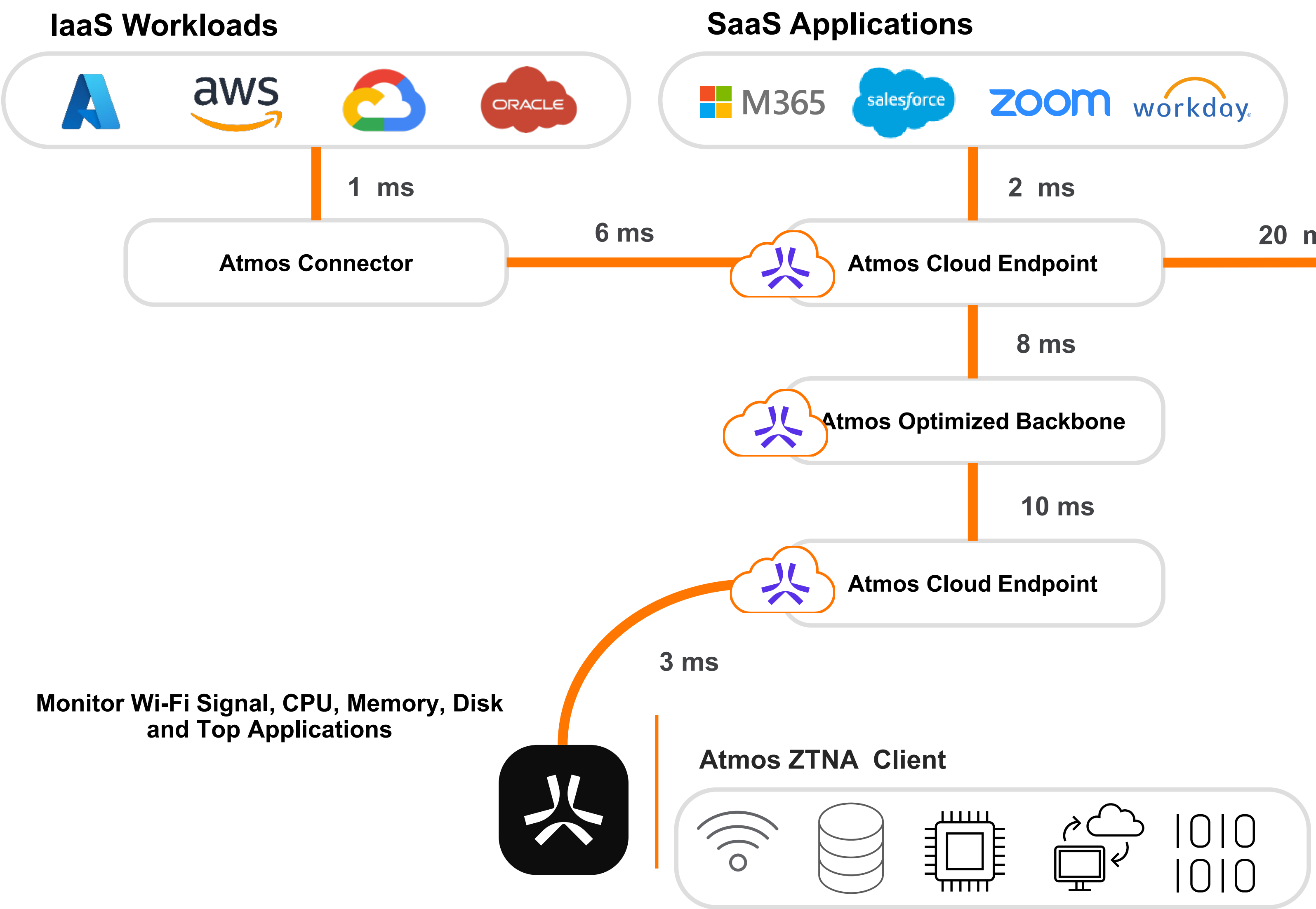
Bring zero trust on-premises

Think global. Act local.

- No hairpin to Internet-based PoPs
- Faster user experience
- Support all private user traffic (agent-based)
- Comply with regulations



Amplify User Experience



Improve user experience and rapidly troubleshoot problems with endpoint device monitoring and application performance monitoring.

Agent vs Agentless

What's the difference

Agent

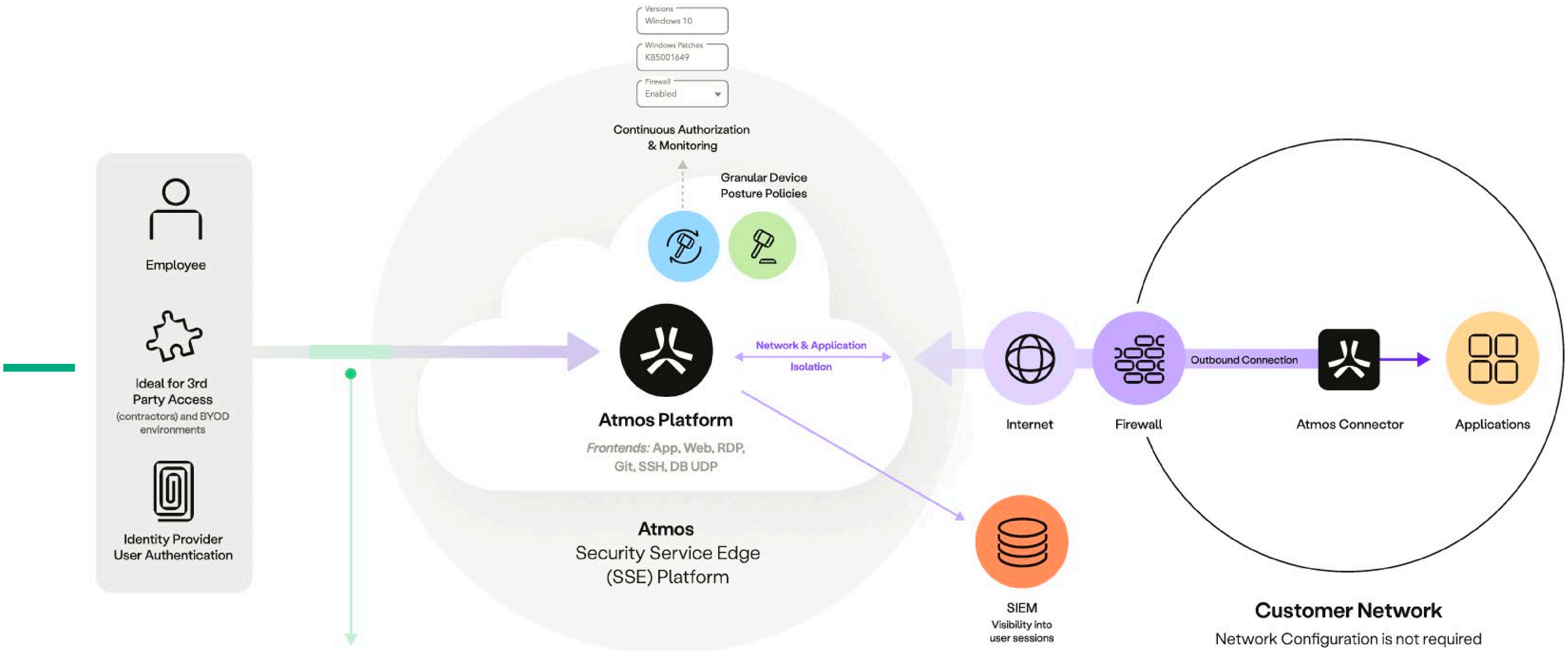
- Support for MacOS, iOS, Windows, Linux & Android
- Creates a Virtual Network Adapter that is connected to the Atmos cloud.
- Supports all TCP/UDP based applications
- Allows rules based on device posture. (AV status, installed apps, Disk encryption, patch status, rooted and much more
- Reports on Client details, stats on CPU, RAM and disk
- SSL inspection with Atmos root certificate
- Installed by User or via Device management

Agentless

- Supports any client. BYOD, Contracters, Cameras, HVAC, IoT
- Needs traffic to be routed to the Atmos cloud (i.e. SD-WAN)
- Limited App support: Web, RDP, SSH, Git and MS-SQL database
- SSL inspection possible when Atmos root-certificate installed

Demo

EdgeConnect SSE - ZTNA



Versions
Windows 10

Windows Patches
KB5001649

Firewall
Enabled

Continuous Authorization & Monitoring

Granular Device Posture Policies

Employee

Ideal for 3rd Party Access
(contractors) and BYOD environments

Identity Provider User Authentication

Atmos Platform

Frontends: App, Web, RDP, Git, SSH, DB UDP

Network & Application Isolation

Atmos
Security Service Edge (SSE) Platform

Internet

Firewall

Outbound Connection

Atmos Connector

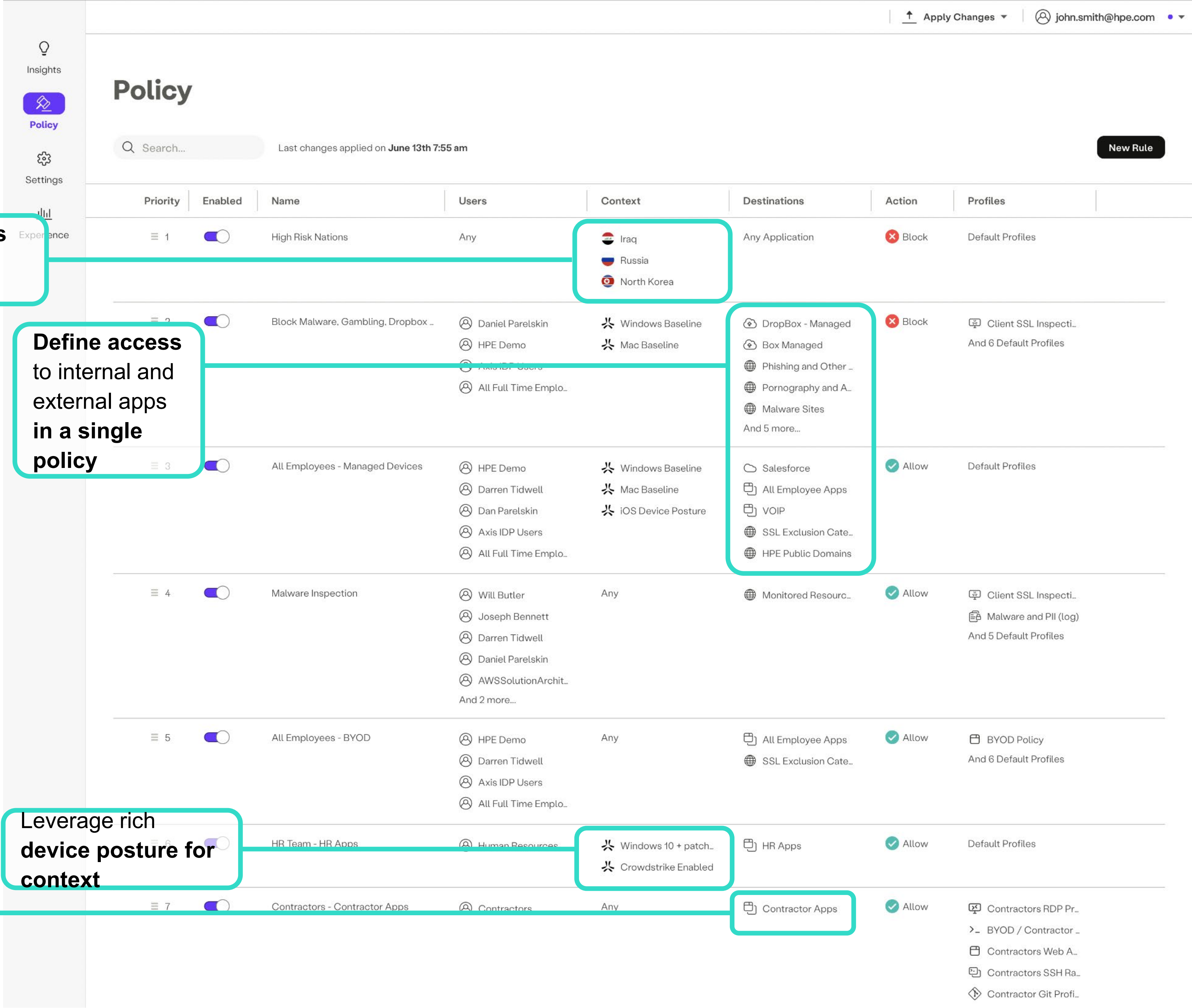
Applications

SIEM
Visibility into user sessions

Customer Network
Network Configuration is not required

A brokered connection to the app.
Users never directly access the network.

An Inside Look At HPE Aruba Networking SSE



Policy

Last changes applied on **June 13th 7:55 am**

Priority	Enabled	Name	Users	Context	Destinations	Action	Profiles
1	●	High Risk Nations	Any	Iraq Russia North Korea	Any Application	Block	Default Profiles
2	●	Block Malware, Gambling, Dropbox ...	Daniel Parelskin HPE Demo Axis IDP Users All Full Time Emplo...	Windows Baseline Mac Baseline	DropBox - Managed Box Managed Phishing and Other ... Pornography and A... Malware Sites And 5 more...	Block	Client SSL Inspecti... And 6 Default Profiles
3	●	All Employees - Managed Devices	HPE Demo Darren Tidwell Dan Parelskin Axis IDP Users All Full Time Emplo...	Windows Baseline Mac Baseline iOS Device Posture	Salesforce All Employee Apps VOIP SSL Exclusion Cate... HPE Public Domains	Allow	Default Profiles
4	●	Malware Inspection	Will Butler Joseph Bennett Darren Tidwell Daniel Parelskin AWSSolutionArchit... And 2 more...	Any	Monitored Resourc...	Allow	Client SSL Inspecti... Malware and PII (log) And 5 Default Profiles
5	●	All Employees - BYOD	HPE Demo Darren Tidwell Axis IDP Users All Full Time Emplo...	Any	All Employee Apps SSL Exclusion Cate...	Allow	BYOD Policy And 6 Default Profiles
		HR Team - HR Apps	Human Resources	Windows 10 + patch... Crowdstrike Enabled	HR Apps	Allow	Default Profiles
7	●	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	Allow	Contractors RDP Pr... BYOD / Contractor ... Contractors Web A... Contractors SSH Ra... Contractor Git Profi...

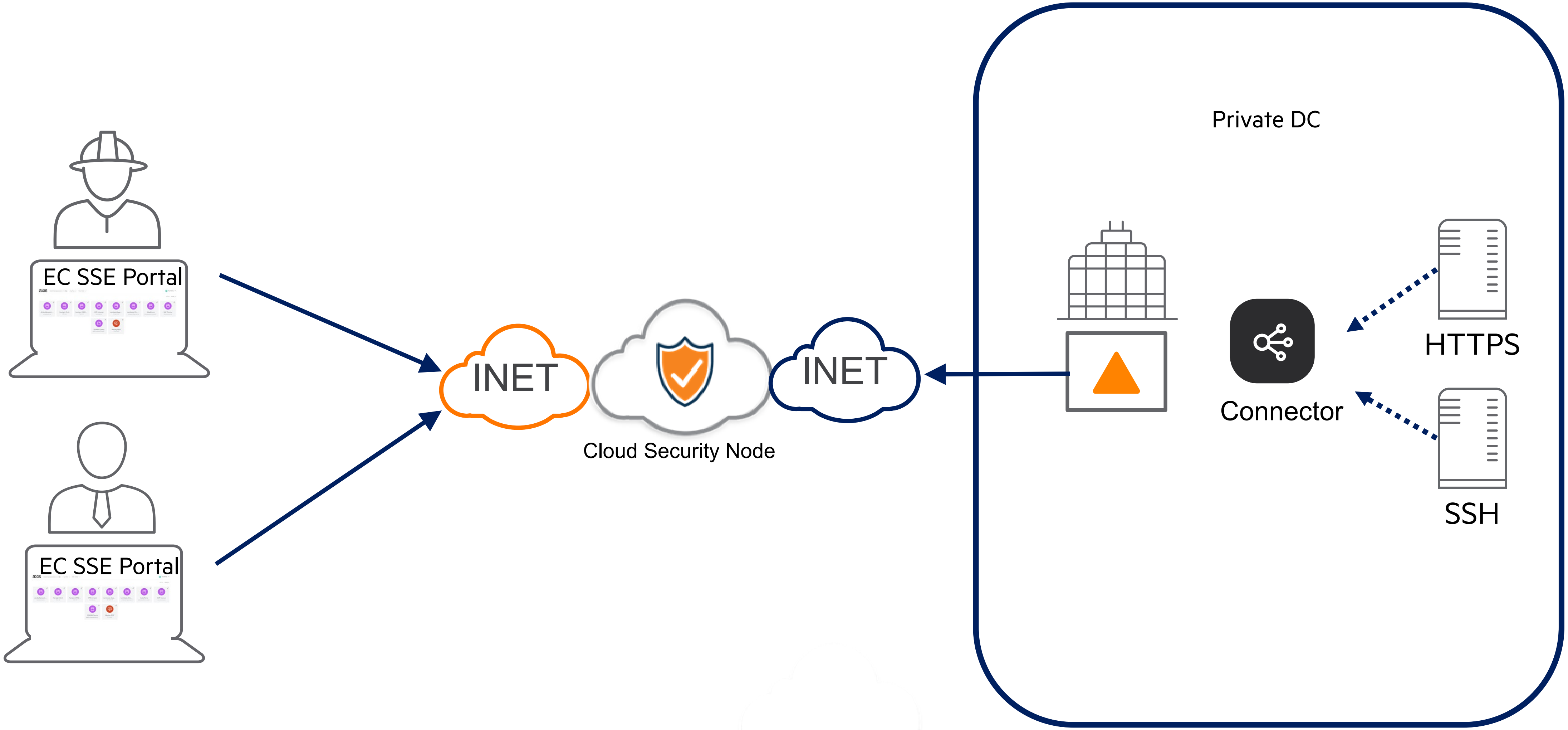
Block access from risky destinations

Define access to internal and external apps **in a single policy**

Leverage rich **device posture for context**

Use app tags to **simplify management**

Agentless, Secure Remote Access



DEMO #1
Direct access

https://atmosphere-web-hpearubajanwillemkeinke.axisapps.io/

DEMO #2

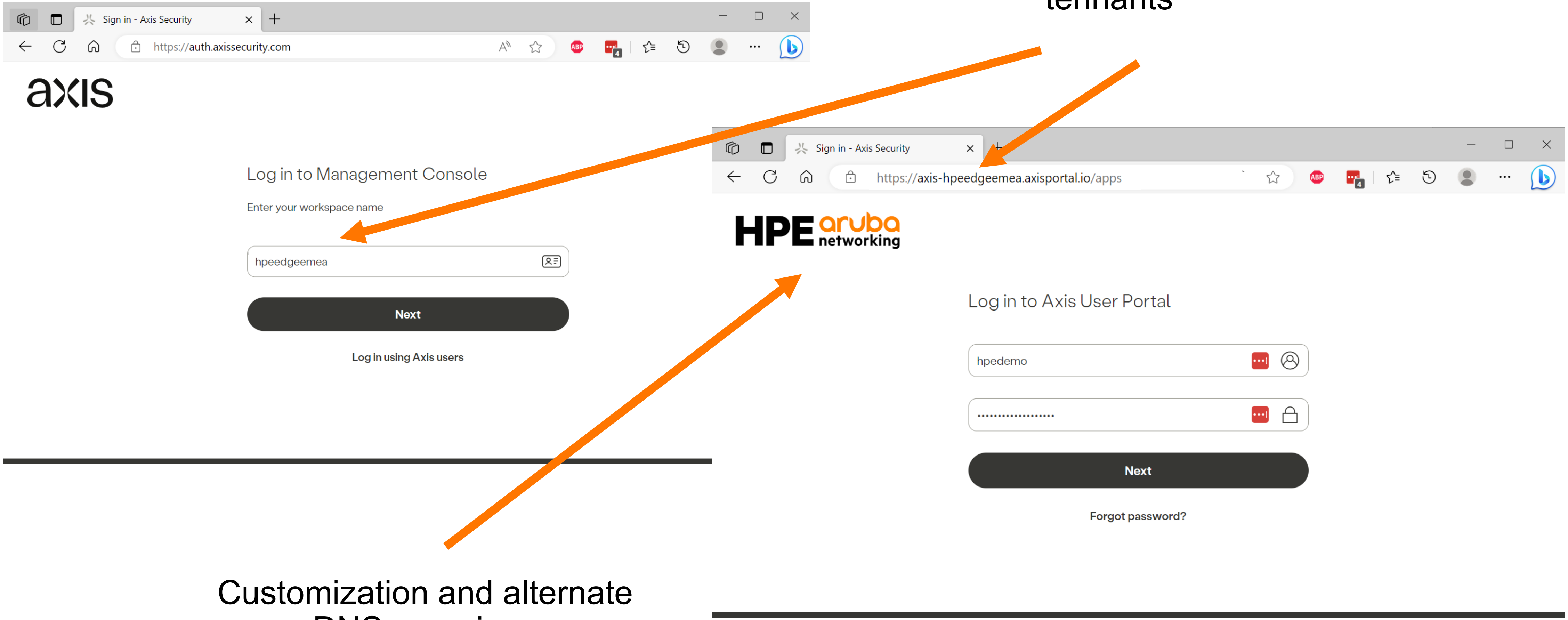
User: atm23

Pass: SecureEdge1

https://axis-hpearubajanwillemkeinke.axisportal.io/apps

Thank you

Two main sites: Management portal and App portal



Sign in - Axis Security

https://auth.axissecurity.com

axis

Log in to Management Console

Enter your workspace name

hpeedgeemea

Next

Log in using Axis users

Sign in - Axis Security

https://axis-hpeedgeemea.axisportal.io/apps

HPE aruba networking

Log in to Axis User Portal

hpedemo

••••••••••••••••••••

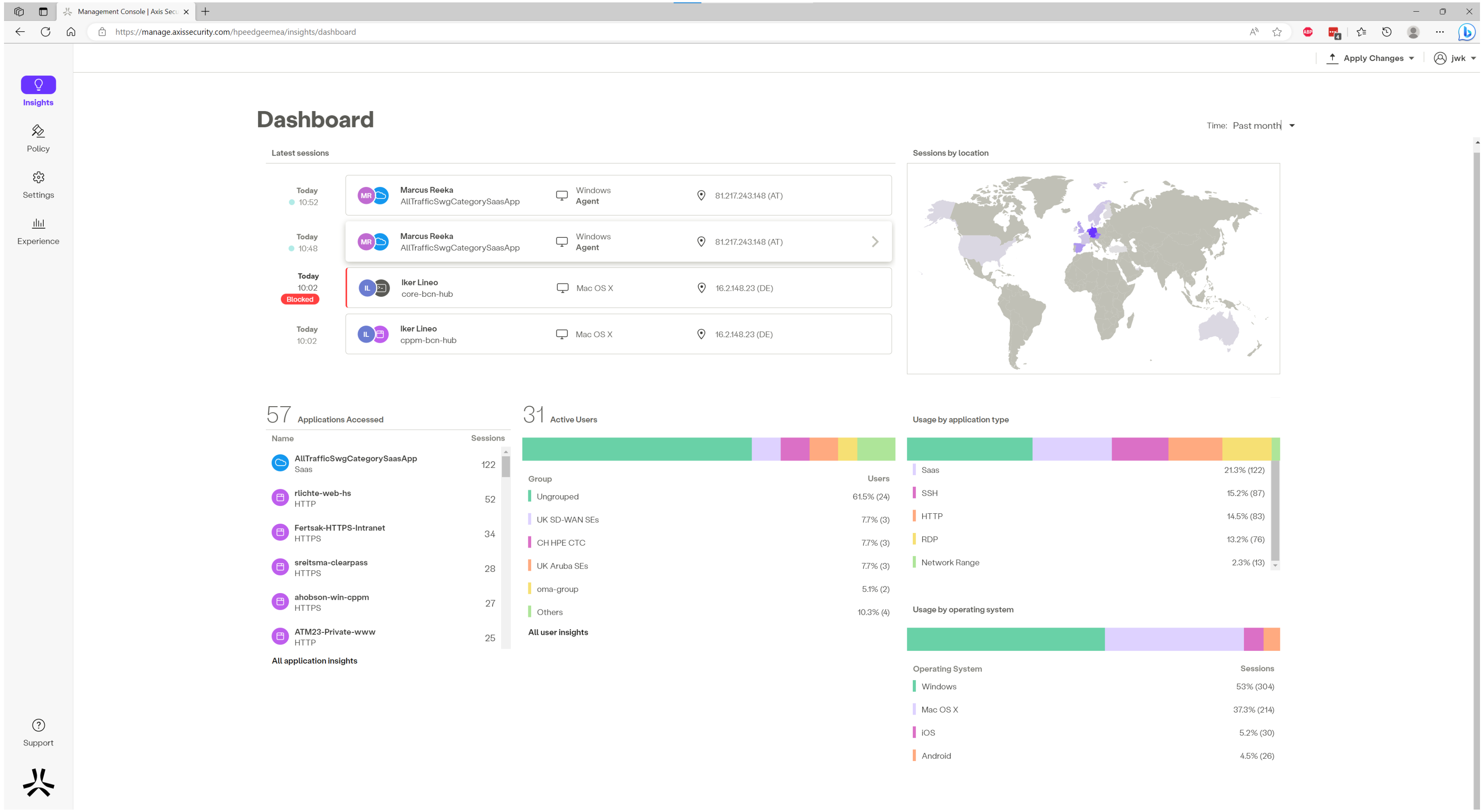
Next

Forgot password?

Customer identifier, separates tennants

Customization and alternate DNS mappings

Management Dashboard


Management Console | Axis Secu
https://manage.axissecurity.com/hpeedgeemea/insights/dashboard
Apply Changes
jwk
Insights
Policy
Settings
Experience
Support

Dashboard

Time: Past month

Latest sessions

Today 10:52	Marcus Reeka AllTrafficSwgCategorySaasApp	Windows **Agent**	81.217.243.148 (AT)
Today 10:48	Marcus Reeka AllTrafficSwgCategorySaasApp	Windows **Agent**	81.217.243.148 (AT)
Today 10:02 Blocked	Iker Lineo core-bcn-hub	Mac OS X	16.2.148.23 (DE)
Today 10:02	Iker Lineo cppm-bcn-hub	Mac OS X	16.2.148.23 (DE)

Sessions by location

57 **Applications Accessed**

Name	Sessions
AllTrafficSwgCategorySaasApp Saas	122
rlichte-web-hs HTTP	52
Fertsak-HTTPS-Intranet HTTPS	34
sreitsma-clearpass HTTPS	28
ahobson-win-cppm HTTPS	27
ATM23-Private-www HTTP	25

All application insights

31 **Active Users**

Group	Users
Ungrouped	61.5% (24)
UK SD-WAN SEs	7.7% (3)
CH HPE CTC	7.7% (3)
UK Aruba SEs	7.7% (3)
oma-group	5.1% (2)
Others	10.3% (4)

All user insights

Usage by application type

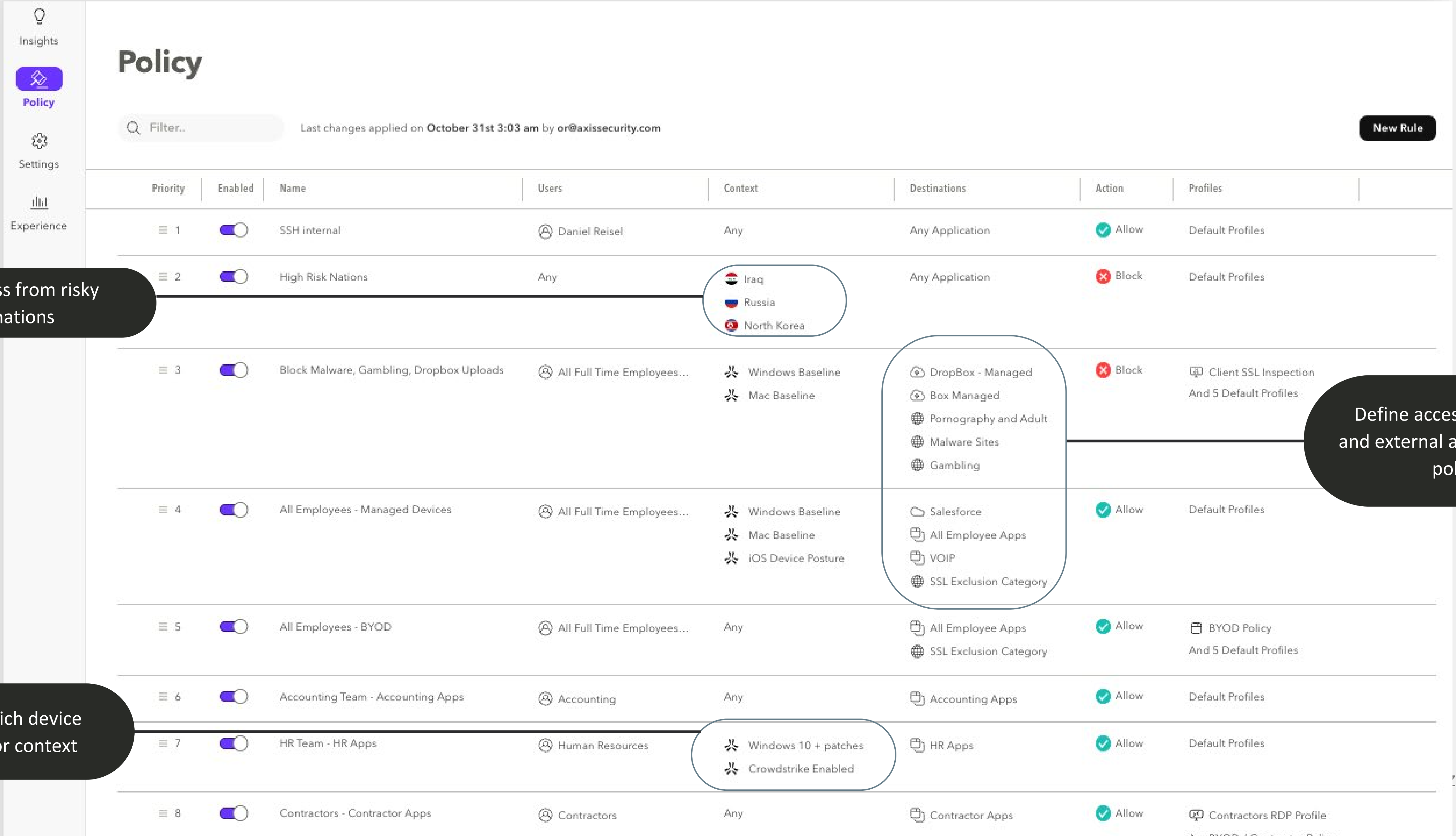
Saas	21.3% (122)
SSH	15.2% (87)
HTTP	14.5% (83)
RDP	13.2% (76)
Network Range	2.3% (13)

Usage by operating system

Operating System	Sessions
Windows	53% (304)
Mac OS X	37.3% (214)
iOS	5.2% (30)
Android	4.5% (26)

CONFIDENTIAL | AUTHORIZED 2

Axis makes policy impossibly simple



Policy

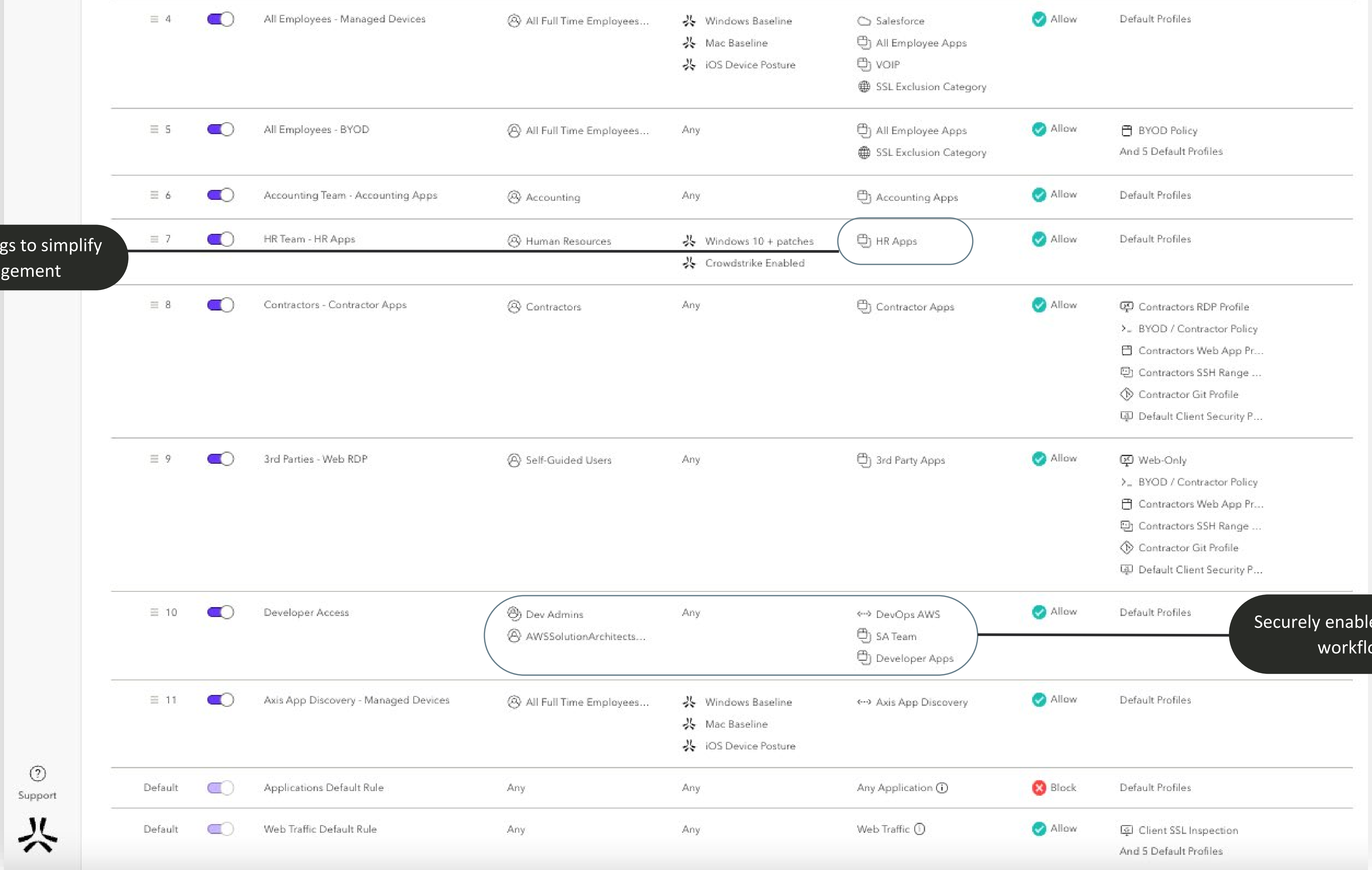
Last changes applied on **October 31st 3:03 am** by **or@axissecurity.com**

Priority	Enabled	Name	Users	Context	Destinations	Action	Profiles
1	●	SSH internal	Daniel Reisel	Any	Any Application	✓ Allow	Default Profiles
2	●	High Risk Nations	Any	Iraq Russia North Korea	Any Application	☒ Block	Default Profiles
3	●	Block Malware, Gambling, Dropbox Uploads	All Full Time Employees...	Windows Baseline Mac Baseline	DropBox - Managed Box Managed Pornography and Adult Malware Sites Gambling	☒ Block	Client SSL Inspection And 5 Default Profiles
4	●	All Employees - Managed Devices	All Full Time Employees...	Windows Baseline Mac Baseline iOS Device Posture	Salesforce All Employee Apps VOIP SSL Exclusion Category	✓ Allow	Default Profiles
5	●	All Employees - BYOD	All Full Time Employees...	Any	All Employee Apps SSL Exclusion Category	✓ Allow	BYOD Policy And 5 Default Profiles
6	●	Accounting Team - Accounting Apps	Accounting	Any	Accounting Apps	✓ Allow	Default Profiles
7	●	HR Team - HR Apps	Human Resources	Windows 10 + patches Crowdstrike Enabled	HR Apps	✓ Allow	Default Profiles
8	●	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	✓ Allow	Contractors RDP Profile

Block access from risky destinations

Define access to internal and external apps in a single policy

Leverage rich device posture for context



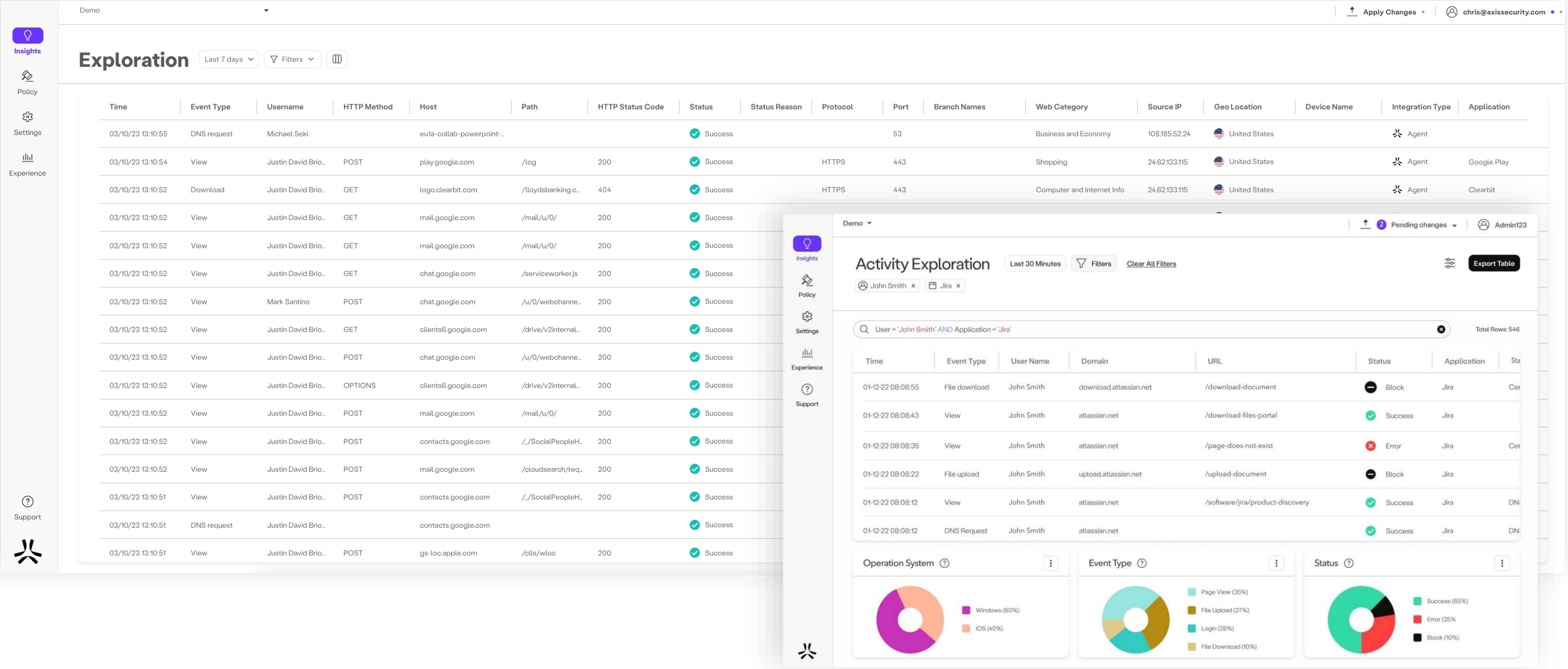
4	All Employees - Managed Devices	All Full Time Employees...	Windows Baseline Mac Baseline iOS Device Posture	Salesforce All Employee Apps VOIP SSL Exclusion Category	✓ Allow	Default Profiles
5	All Employees - BYOD	All Full Time Employees...	Any	All Employee Apps SSL Exclusion Category	✓ Allow	BYOD Policy And 5 Default Profiles
6	Accounting Team - Accounting Apps	Accounting	Any	Accounting Apps	✓ Allow	Default Profiles
7	HR Team - HR Apps	Human Resources	Windows 10 + patches Crowdstrike Enabled	HR Apps	✓ Allow	Default Profiles
8	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	✓ Allow	Contractors RDP Profile BYOD / Contractor Policy Contractors Web App Pr... Contractors SSH Range ... Contractor Git Profile Default Client Security P...
9	3rd Parties - Web RDP	Self-Guided Users	Any	3rd Party Apps	✓ Allow	Web-Only BYOD / Contractor Policy Contractors Web App Pr... Contractors SSH Range ... Contractor Git Profile Default Client Security P...
10	Developer Access	Dev Admins AWSSolutionArchitects...	Any	DevOps AWS SA Team Developer Apps	✓ Allow	Default Profiles
11	Axis App Discovery - Managed Devices	All Full Time Employees...	Windows Baseline Mac Baseline iOS Device Posture	Axis App Discovery	✓ Allow	Default Profiles
Default	Applications Default Rule	Any	Any	Any Application ⓘ	✗ Block	Default Profiles
Default	Web Traffic Default Rule	Any	Any	Web Traffic ⓘ	✓ Allow	Client SSL Inspection And 5 Default Profiles

Use app tags to simplify management

Securely enable developer workflows

Activity exploration

Unified visibility across all applications



Exploration

Time	Event Type	Username	HTTP Method	Host	Path	HTTP Status Code	Status	Status Reason	Protocol	Port	Branch Names	Web Category	Source IP	Geo Location	Device Name	Integration Type	Application
03/10/23 13:10:55	DNS request	Michael Seki		eu1a-collab-powerpoint-…			✓ Success			53		Business and Economy	108.185.52.24	United States		Agent	
03/10/23 13:10:54	View	Justin David Brio…	POST	play.google.com	/log	200	✓ Success		HTTPS	443		Shopping	24.62.133.115	United States		Agent	Google Play
03/10/23 13:10:52	Download	Justin David Brio…	GET	logo.clearbit.com	/lloydsbanking.c…	404	✓ Success		HTTPS	443		Computer and Internet Info	24.62.133.115	United States		Agent	Clearbit
03/10/23 13:10:52	View	Justin David Brio…	GET	mail.google.com	/mail/u/0/	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	GET	mail.google.com	/mail/u/0/	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	GET	chat.google.com	/serviceworker.js	200	✓ Success										
03/10/23 13:10:52	View	Mark Santino	POST	chat.google.com	/u/0/webchanne…	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	GET	clients6.google.com	/drive/v2internal…	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	POST	chat.google.com	/u/0/webchanne…	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	OPTIONS	clients6.google.com	/drive/v2internal…	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	POST	mail.google.com	/mail/u/0/	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	POST	contacts.google.com	/_/SocialPeopleH…	200	✓ Success										
03/10/23 13:10:52	View	Justin David Brio…	POST	mail.google.com	/cloudsearch/req…	200	✓ Success										
03/10/23 13:10:51	View	Justin David Brio…	POST	contacts.google.com	/_/SocialPeopleH…	200	✓ Success										
03/10/23 13:10:51	DNS request	Justin David Brio…		contacts.google.com			✓ Success										
03/10/23 13:10:51	View	Justin David Brio…	POST	gs-loc.apple.com	/clls/wloc	200	✓ Success										

Activity Exploration

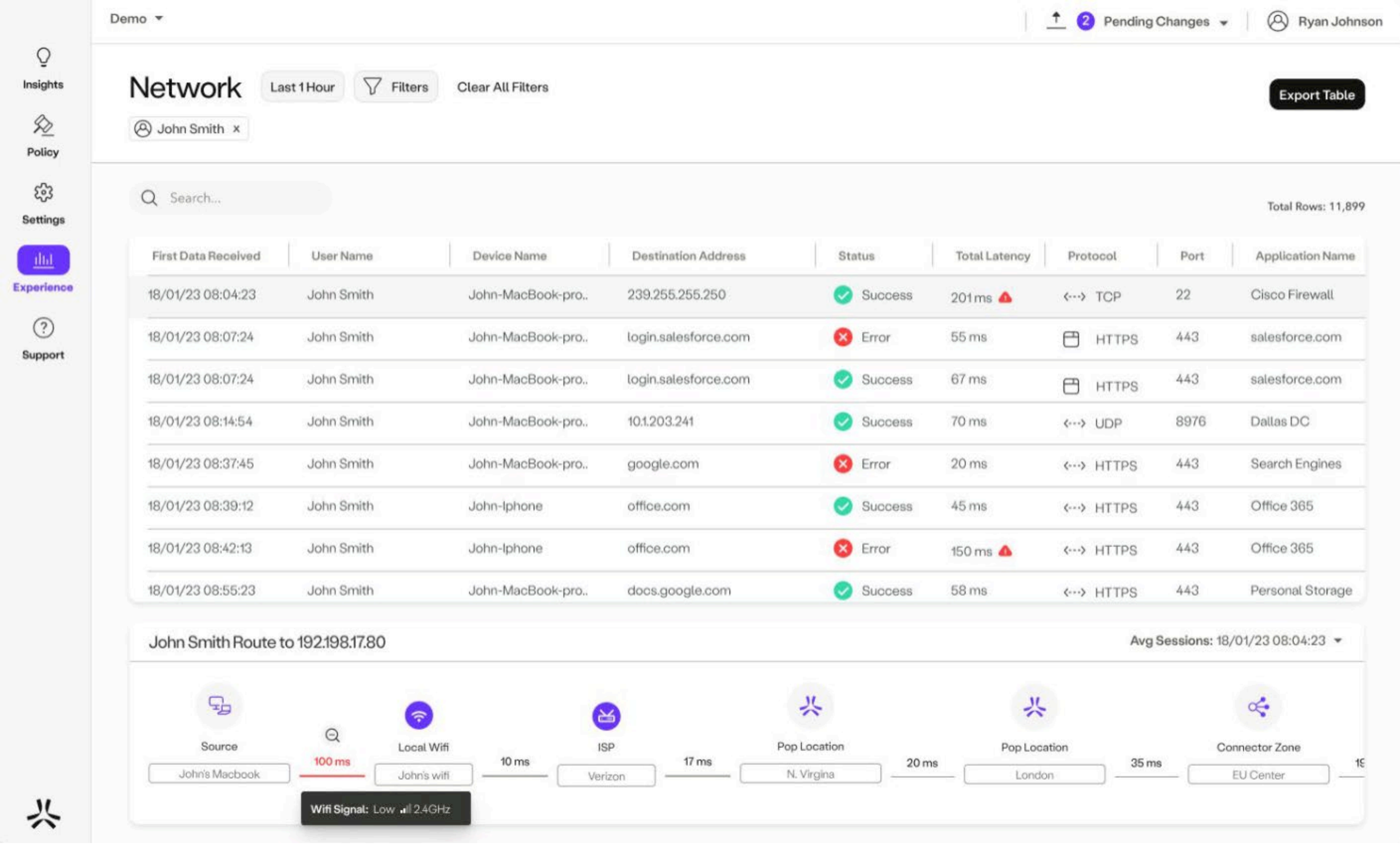
User = 'John Smith' AND Application = 'Jira'

Total Rows: 546

Time	Event Type	User Name	Domain	URL	Status	Application	Sta
01-12-22 08:08:55	File download	John Smith	download.atlassian.net	/download-document	● Block	Jira	Cer
01-12-22 08:08:43	View	John Smith	atlassian.net	/download-files-portal	✓ Success	Jira	
01-12-22 08:08:35	View	John Smith	atlassian.net	/page-does-not-exist	✗ Error	Jira	Cer
01-12-22 08:08:22	File upload	John Smith	upload.atlassian.net	/upload-document	● Block	Jira	
01-12-22 08:08:12	View	John Smith	atlassian.net	/software/jira/product-discovery	✓ Success	Jira	DN:
01-12-22 08:08:12	DNS Request	John Smith	atlassian.net		✓ Success	Jira	DN:

And Ensure a Great User Experience

- Dynamic monitoring of user experience issues
- Endpoint telemetry i.e. CPU, resource consumption, memory use
- Unified application health monitoring
- Hop by hop network path metrics between users and business apps



Network

Total Rows: 11,899

First Data Received	User Name	Device Name	Destination Address	Status	Total Latency	Protocol	Port	Application Name
18/01/23 08:04:23	John Smith	John-MacBook-pro..	239.255.255.250	Success	201 ms	TCP	22	Cisco Firewall
18/01/23 08:07:24	John Smith	John-MacBook-pro..	login.salesforce.com	Error	55 ms	HTTPS	443	salesforce.com
18/01/23 08:07:24	John Smith	John-MacBook-pro..	login.salesforce.com	Success	67 ms	HTTPS	443	salesforce.com
18/01/23 08:14:54	John Smith	John-MacBook-pro..	10.1.203.241	Success	70 ms	UDP	8976	Dallas DC
18/01/23 08:37:45	John Smith	John-MacBook-pro..	google.com	Error	20 ms	HTTPS	443	Search Engines
18/01/23 08:39:12	John Smith	John-Iphone	office.com	Success	45 ms	HTTPS	443	Office 365
18/01/23 08:42:13	John Smith	John-Iphone	office.com	Error	150 ms	HTTPS	443	Office 365
18/01/23 08:55:23	John Smith	John-MacBook-pro..	docs.google.com	Success	58 ms	HTTPS	443	Personal Storage

John Smith Route to 192.198.17.80

Avg Sessions: 18/01/23 08:04:23

atmosphere'23
BELGIUM

Building a secure Edge

Jan-Willem Keinke
Sales Engineer SD-WAN Benelux
Email: jwk@hpe.com

HPE aruba networking

ADVANTAGES OF AN APPLICATION DRIVEN WAN

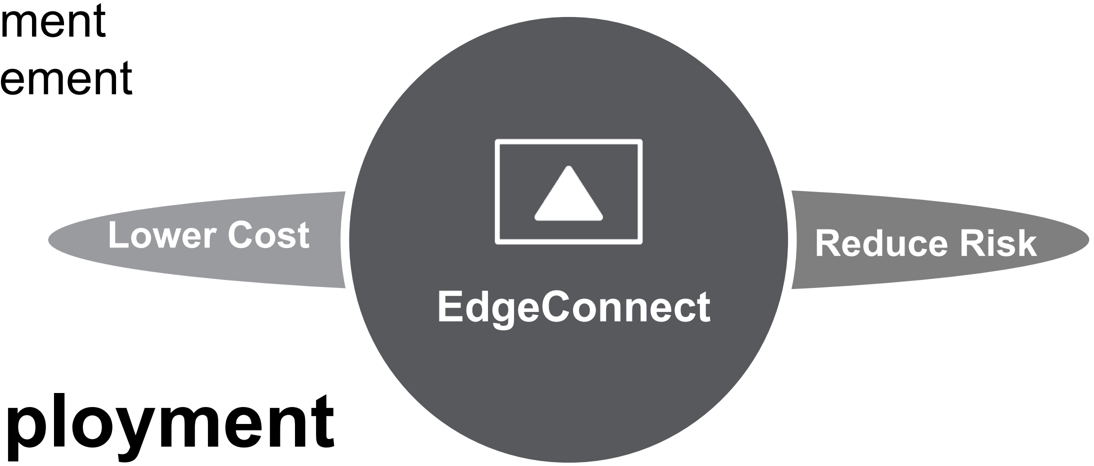
Savings

- WAN cost savings
- Automation savings
- Cloud security integration
- Eliminate branch equipment
- Simplified edge management

Performance

- Sub second session failover
- 10 x faster applications
- Performance Improvement for SaaS/IaaS
- Add / remove branches instantly
- Uptime during blackouts

Gain Competitive Advantage



Increase Business Agility

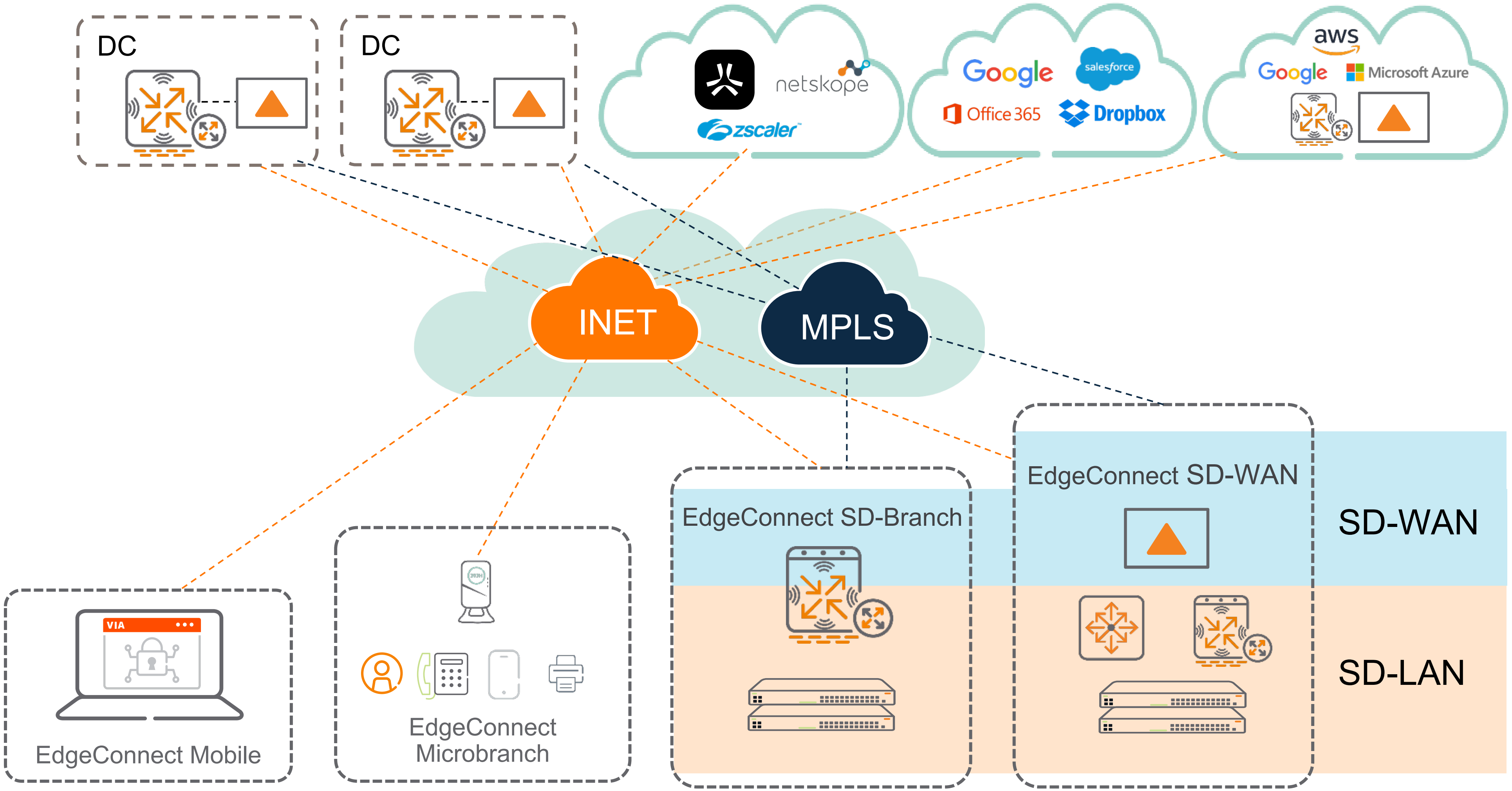
100x Faster Deployment

- Simple and flexible deployment models
- Comprehensive visibility

Security

- Segment your apps
- Automated policies
- UTM features
- ZBF within VRFs
- Cloud Security Integration

HPE Aruba's secure edge portfolio



EdgeConnect SD-Branch

EdgeConnect SD-WAN

SD-WAN

SD-LAN

EdgeConnect Mobile

EdgeConnect Microbranch

Max Mobility

Min Footprint

Max Integration
Converged LAN+WAN
Simple, prescriptive deployment

Optimal QoE
Independent LAN+WAN
QoE exceeds best underlay

Integration opportunities

Converged management

- Aruba Central w/ EdgeConnect site view
- Silver Peak Orchestrator w/Aruba WAN view

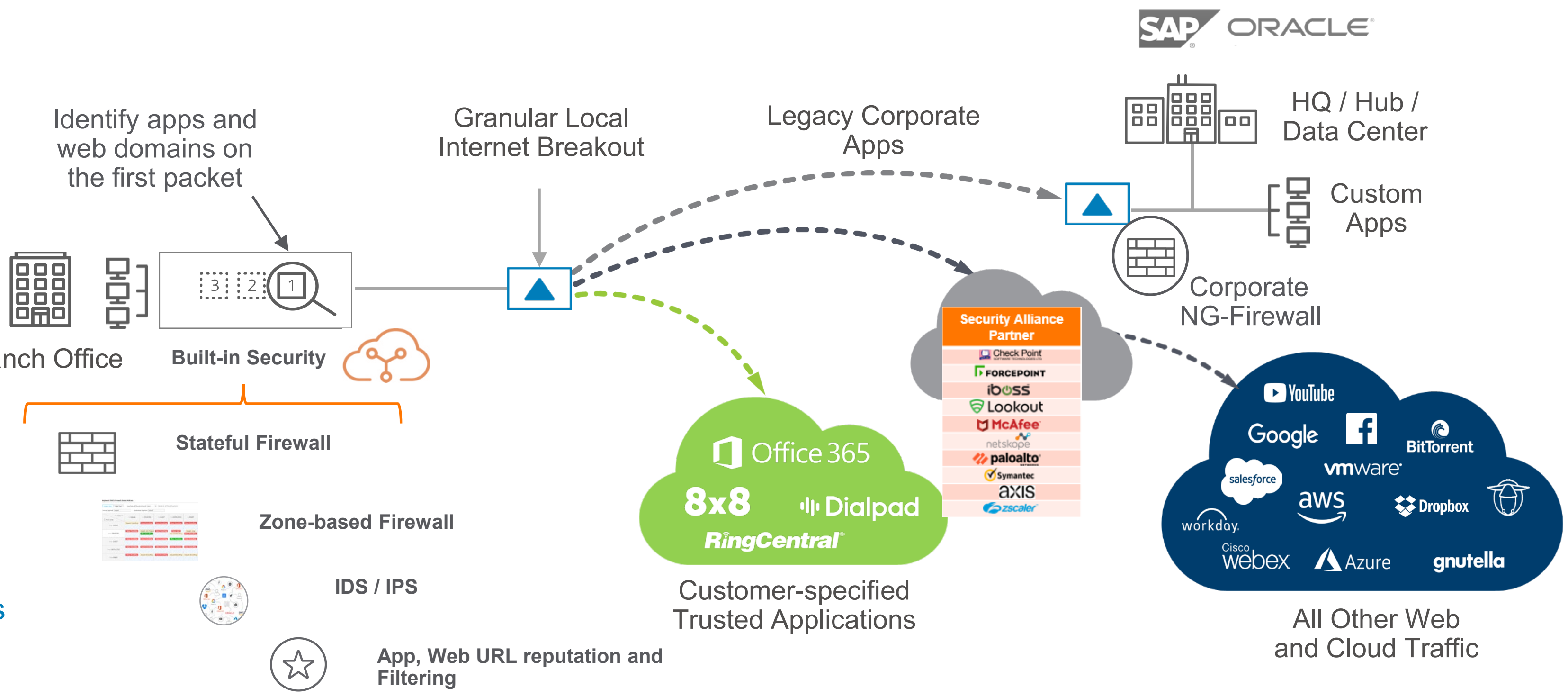
Cross portfolio security

- Clear Pass: Role based policy
- Dynamic segmentation
- Unified threat management
- Cloud security partners

Secure, adaptive internet breakout

– First-packet iQ™ enables application visibility and control

Check Point
FORCEPOINT
iboss
Lookout
McAfee
netskope
paloalto
Symantec.
Akamai
axis
zscaler



10,000+ Apps
300 Million+ Web Domains
Automated Daily Updates

Steer Apps Intelligently

Granular, intelligent breakout of SaaS and trusted internet-bound traffic directly from the branch

Improve App Response Time

Avoid added latency through direct access to where the app resides

Reduce Backhaul

Backhaul only untrusted traffic to corporate FW

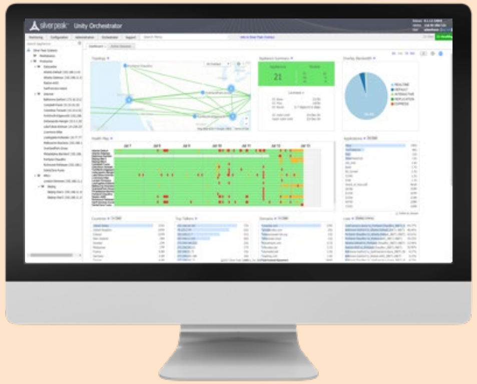
Save Valuable WAN Bandwidth

Avoid consumption of expensive MPLS circuits where not necessary

EdgeConnect Orchestrator

Your SD-WAN control center

What is EdgeConnect Orchestrator?



EdgeConnect Orchestrator

Orchestrate application policies across thousands of appliances, through a single pane of glass, driven by simple business intent policies.

Align **application policies** (QoS, security) with **business intent**

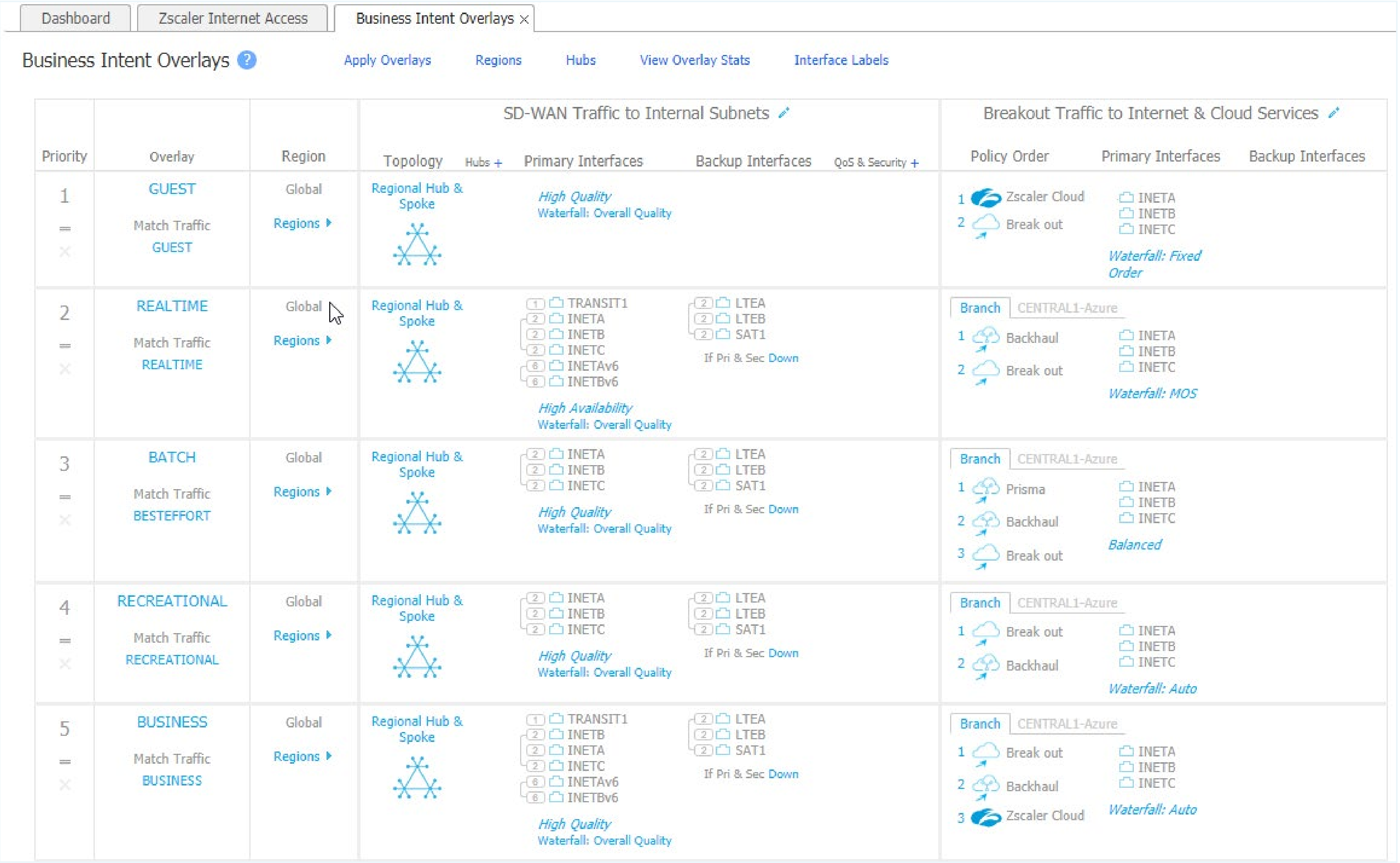
Secure, centralized visibility, control and administration of SD-WAN across thousands of sites

Extensive analytics, application & network performance measurements, & troubleshooting.

Automates & simplifies lifecycle management of SD-WAN

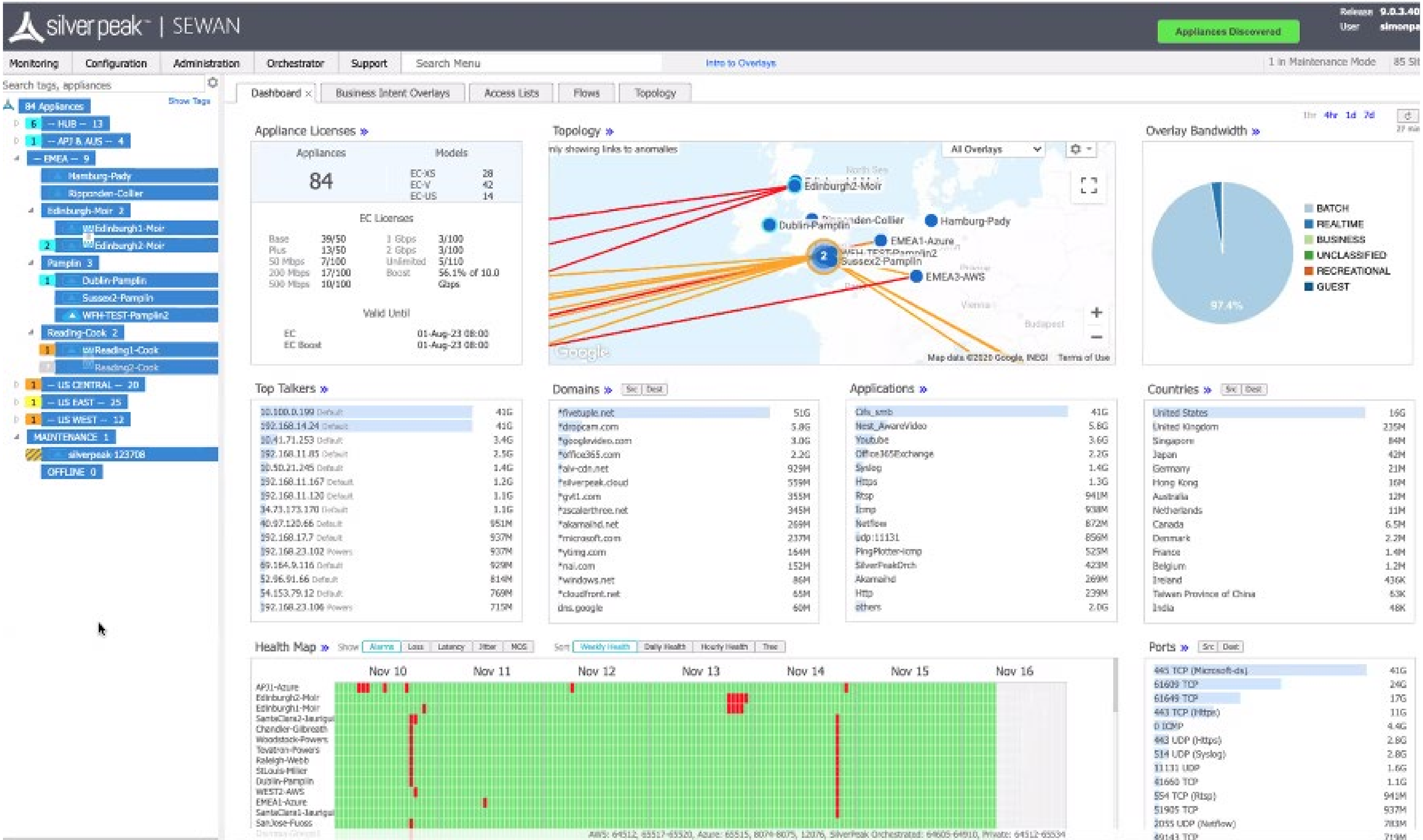
Orchestrates **end-to-end service chains** through partner APIs.

Business Intent Based Overlays



Business Intent Overlays

Priority	Overlay	Region	SD-WAN Traffic to Internal Subnets					Breakout Traffic to Internet & Cloud Services		
			Topology	Hubs +	Primary Interfaces	Backup Interfaces	QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	GUEST Match Traffic GUEST	Global Regions	Regional Hub & Spoke		High Quality Waterfall: Overall Quality			1 Zscaler Cloud 2 Break out	INETA INETB INETC Waterfall: Fixed Order	
2	REALTIME Match Traffic REALTIME	Global Regions	Regional Hub & Spoke		1 TRANSIT1 2 INETA 2 INETB 2 INETC 6 INETAv6 6 INETBv6 High Availability Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down		Branch CENTRAL1-Azure 1 Backhaul 2 Break out	INETA INETB INETC Waterfall: MOS	
3	BATCH Match Traffic BESTEFFORT	Global Regions	Regional Hub & Spoke		2 INETA 2 INETB 2 INETC High Quality Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down		Branch CENTRAL1-Azure 1 Prisma 2 Backhaul 3 Break out	INETA INETB INETC Balanced	
4	RECREATIONAL Match Traffic RECREATIONAL	Global Regions	Regional Hub & Spoke		2 INETA 2 INETB 2 INETC High Quality Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down		Branch CENTRAL1-Azure 1 Break out 2 Backhaul	INETA INETB INETC Waterfall: Auto	
5	BUSINESS Match Traffic BUSINESS	Global Regions	Regional Hub & Spoke		1 TRANSIT1 2 INETB 2 INETA 2 INETC 6 INETAv6 6 INETBv6 High Quality Waterfall: Overall Quality	2 LTEA 2 LTEB 2 SAT1 If Pri & Sec Down		Branch CENTRAL1-Azure 1 Break out 2 Backhaul 3 Zscaler Cloud	INETA INETB INETC Waterfall: Auto	



silver peak™ | SEWAN

Appliances Discovered

Release 9.0.3.40
User simonpa

Monitoring | Configuration | Administration | Orchestrator | Support | Search Menu | Intro to Overlays | 1 in Maintenance Mode | 85 Sit

Search tags, appliances

Show Tags

- 84 Appliances
  - 6 — HUB — 13
  - 1 — APJ & AUS — 4
  - — EMEA — 9
    - Hamburg-Pady
    - Ripponden-Collier
    - Edinburgh-Moir 2
      - Edinburgh1-Moir
      - 2 Edinburgh2-Moir
    - Pamplin 3
      - 1 Dublin-Pamplin
      - Sussex2-Pamplin
      - WFH-TEST-Pamplin2
    - Reading-Cook 2
      - 1 Reading1-Cook
      - Reading2-Cook
  - 1 — US CENTRAL — 20
  - 1 — US EAST — 25
  - 1 — US WEST — 12
  - MAINTENANCE 1
    - silverpeak 123708
  - OFFLINE 0

Dashboard × | Business Intent Overlays | Access Lists | Flows | Topology

1hr 4hr 1d 7d

27 min

Appliance Licenses »

Appliances

84

Models	
EC-XS	28
EC-V	42
EC-US	14

EC Licenses

Base	39/50	1 Gbps	3/100
Plus	13/50	2 Gbps	3/100
50 Mbps	7/100	Unlimited	5/110
200 Mbps	17/100	Boost	56.1% of 10.0 Gbps
500 Mbps	10/100		

Valid Until

EC	01-Aug-23 08:00
EC Boost	01-Aug-23 08:00

Topology »

nly showing links to anomalies

All Overlays

Map data ©2020 Google, INEGI Terms of Use

Overlay Bandwidth »

Top Talkers »

10.100.0.199 Default	41G
192.168.14.24 Default	41G
10.41.71.253 Default	3.4G
192.168.11.85 Default	2.5G
10.50.21.245 Default	1.4G
192.168.11.167 Default	1.2G
192.168.11.120 Default	1.1G
34.73.173.170 Default	1.1G
40.97.120.66 Default	951M
192.168.17.7 Default	937M
192.168.23.102 Powers	937M
89.164.9.116 Default	929M
52.96.91.66 Default	814M
54.153.79.12 Default	769M
192.168.23.106 Powers	715M

Domains » Src Dest

*fivetuple.net	51G
*dropcam.com	5.8G
*googlevideo.com	3.0G
*office365.com	2.2G
*aiv-cdn.net	929M
*silverpeak.cloud	559M
*gvt1.com	355M
*zscalerthree.net	345M
*akamaihd.net	269M
*microsoft.com	237M
*ytimg.com	164M
*nai.com	152M
*windows.net	86M
*cloudfront.net	65M
dns.google	60M

Applications »

Cifs_smb	41G
Nest_AwareVideo	5.8G
Youtube	3.6G
Office365Exchange	2.2G
Syslog	1.4G
Https	1.3G
Rtsp	941M
Icmp	938M
Netflow	872M
udp:11131	856M
PingPlotter-icmp	525M
SilverPeakOrch	423M
Akamaihd	269M
Http	239M
others	2.0G

Countries » Src Dest

United States	16G
United Kingdom	235M
Singapore	84M
Japan	42M
Germany	21M
Hong Kong	16M
Australia	12M
Netherlands	11M
Canada	6.5M
Denmark	2.2M
France	1.4M
Belgium	1.2M
Ireland	436K
Taiwan Province of China	63K
India	48K

Health Map »

Show: Alarms | Loss | Latency | Jitter | MOS

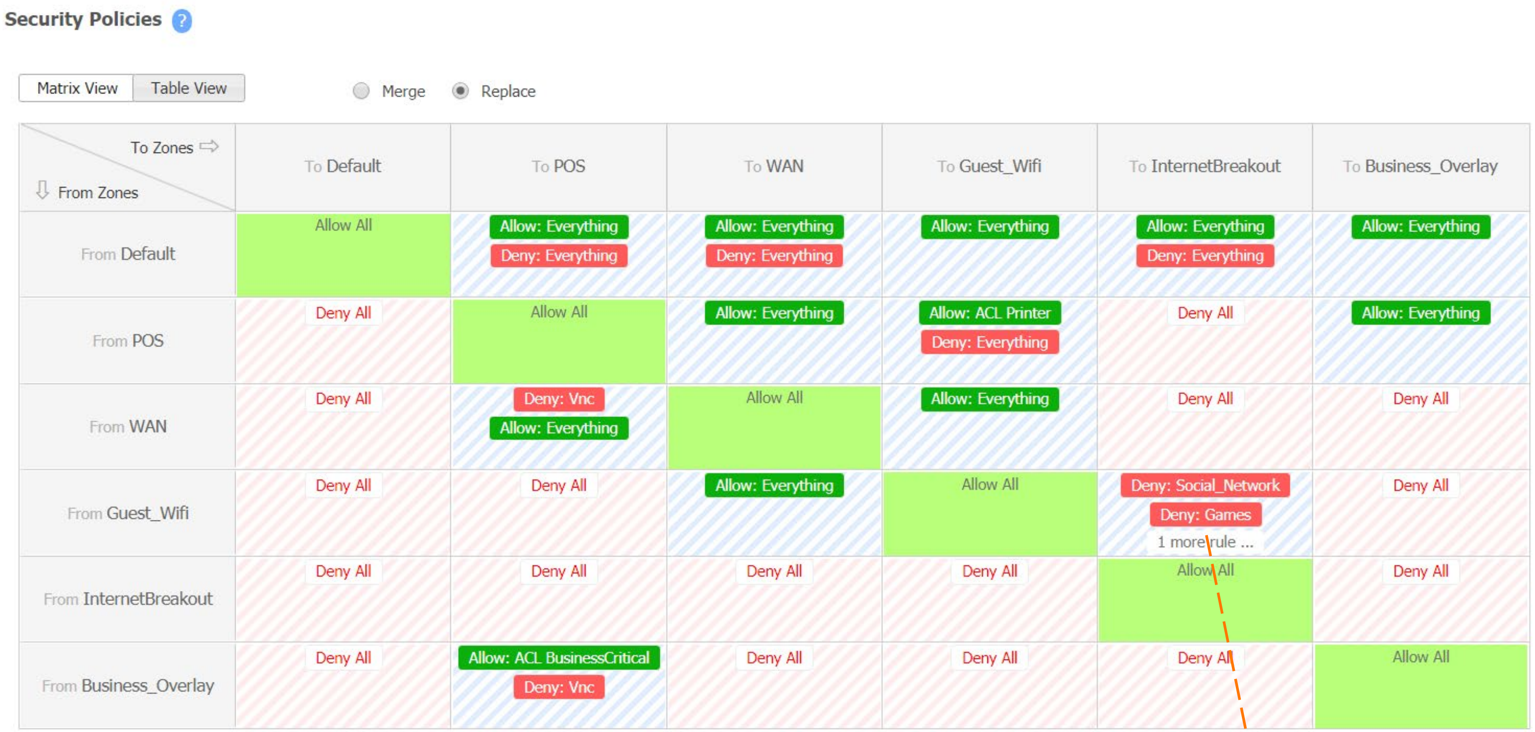
Sort: Weekly Health | Daily Health | Hourly Health | Tree

AWS: 64512, 65517-65520, Azure: 65515, 8074-8075, 12076, SilverPeak Orchestrated: 64605-64910, Private: 64512-65534

Ports » Src Dest

445 TCP (Microsoft-ds)	41G
61609 TCP	24G
61649 TCP	17G
443 TCP (Https)	11G
0 ICMP	4.4G
443 UDP (Https)	2.8G
514 UDP (Syslog)	2.8G
11131 UDP	1.6G
41660 TCP	1.1G
554 TCP (Rtsp)	941M
51905 TCP	937M
2055 UDP (Netflow)	783M
49143 TCP	719M

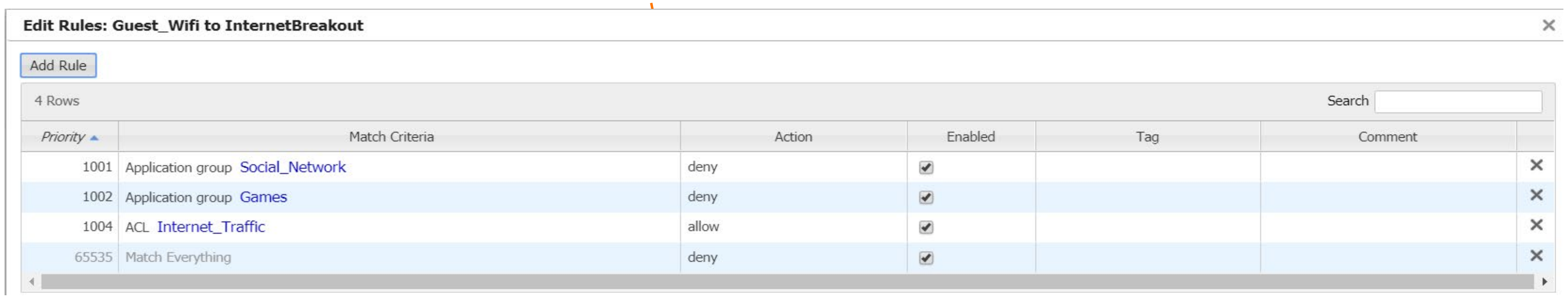
Security policy matrix



Security Policies ?

Matrix View | Table View   ○ Merge ● Replace

To Zones ⇨ ⇩ From Zones	To Default	To POS	To WAN	To Guest_Wifi	To InternetBreakout	To Business_Overlay
From Default	Allow All	Allow: Everything Deny: Everything	Allow: Everything Deny: Everything	Allow: Everything	Allow: Everything Deny: Everything	Allow: Everything
From POS	Deny All	Allow All	Allow: Everything	Allow: ACL Printer Deny: Everything	Deny All	Allow: Everything
From WAN	Deny All	Deny: Vnc Allow: Everything	Allow All	Allow: Everything	Deny All	Deny All
From Guest_Wifi	Deny All	Deny All	Allow: Everything	Allow All	Deny: Social_Network Deny: Games 1 more rule ...	Deny All
From InternetBreakout	Deny All	Deny All	Deny All	Deny All	Allow All	Deny All
From Business_Overlay	Deny All	Allow: ACL BusinessCritical Deny: Vnc	Deny All	Deny All	Deny All	Allow All



Edit Rules: Guest_Wifi to InternetBreakout ✕

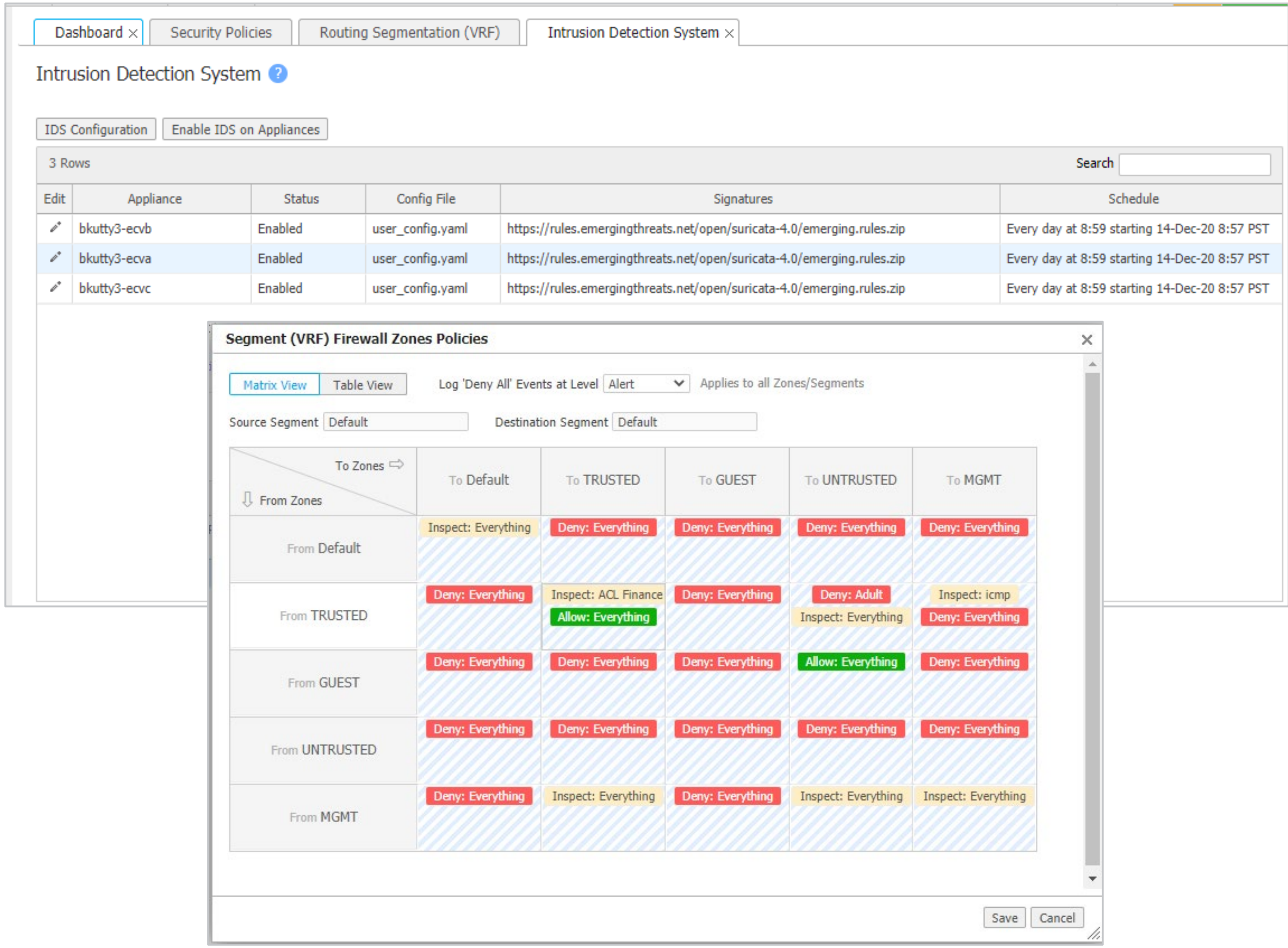
Add Rule

4 Rows   Search

Priority ▲	Match Criteria	Action	Enabled	Tag	Comment	
1001	Application group Social_Network	deny	☑			✕
1002	Application group Games	deny	☑			✕
1004	ACL Internet_Traffic	allow	☑			✕
65535	Match Everything	deny	☑			✕

EdgeConnect SD-WAN IDS Highlights

- Built-in signature-based intrusion detection
- Utilizes common Aruba UTM framework
  - Automated threat feeds (from Aruba Central)
  - Threat logging to centralized collector/SIEM
  - Threat logging to Central (future)
- Integrated with zone-based firewall enabling application-level selection for inspection
  - Allow, Deny, Allow & Inspect
  - e.g., “inspect all flows on Internet link”
- Add-on “Advanced Security” license



Intrusion Detection System

3 Rows

Search

Edit	Appliance	Status	Config File	Signatures	Schedule
✎	bkutty3-ecvb	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST
✎	bkutty3-ecva	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST
✎	bkutty3-ecvc	Enabled	user_config.yaml	https://rules.emergingthreats.net/open/suricata-4.0/emerging.rules.zip	Every day at 8:59 starting 14-Dec-20 8:57 PST

Segment (VRF) Firewall Zones Policies

Log 'Deny All' Events at Level: Alert

Applies to all Zones/Segments

Source Segment: Default

Destination Segment: Default

To Zones ⇨ / ⇩ From Zones	To Default	To TRUSTED	To GUEST	To UNTRUSTED	To MGMT
From Default	Inspect: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From TRUSTED	Deny: Everything	Inspect: ACL Finance Allow: Everything	Deny: Everything	Deny: Adult Inspect: Everything	Inspect: icmp Deny: Everything
From GUEST	Deny: Everything	Deny: Everything	Deny: Everything	Allow: Everything	Deny: Everything
From UNTRUSTED	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From MGMT	Deny: Everything	Inspect: Everything	Deny: Everything	Inspect: Everything	Inspect: Everything

Summary: Benefits of SD-WAN

- Complete control and visibility of WAN infrastructure
- Route application traffic, not packets, based on:
  - Business importance
  - Security requirements
- Built in Firewall, end-to-end segmentation and IPS/IDS security
- Automated integration with Cloud infrastructures and Secure Service Edge providers

Best-of-breed SASE architecture

Secure SD-WAN

- SaaS Acceleration
- WAN Optimization
- Tunnel Bonding
- Zero-Touch Provisioning
- Data Encryption
- Next-generation Firewall
- Granular Segmentation
- IDS/IPS and DDoS Protection

+

Security Service Edge (SSE)

- Zero Trust Network Access
- Cloud Access Security Broker
- Secure Web Gateway
- Firewall as a Service
- Remote Browser Isolation
- Data Loss Prevention
- Sandboxing

Demo

Thank you.