HPE Aruba Networking Security SSE

Transformation Realized

Dan Parelskin, Director SSE Engineering
Dave Muhlbradt, SSE Engineering

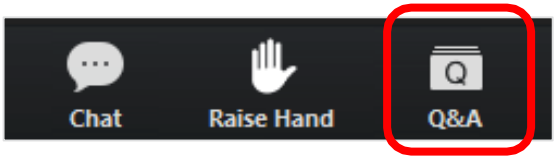
Before we begin...

- Listen by computer audio or dial-in

- All lines are muted during the webinar

- Ask *questions by selecting "Q&A"* and to report any webinar difficulties

- Webinar is being recorded & will be emailed to all attendees



Partner Technical Webinar Series

New HPE Aruba Networking Secure Access Service Edge (SASE)

Session 1: SASE Technical Solutions Overview
Monday, March 11th at 9 AM PT / 12 PM ET

Session 2: HPE Aruba Networking Security SSE
Monday, April 1st at 9 AM PT / 12 PM ET

Session 3: Security Service Edge (SSE) Demo
Monday, May 6th at 9 AM PT / 12 PM ET

(Click here) to register for the webinar series

Agenda

HPE aruba networking

- Security Service Edge (SSE) Overview
- Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Digital Experience Monitoring (DEM)
- DNS Flow, DNS App, DNS Solutions, etc.
- Demo

About Axis

Exited stealth in 2020

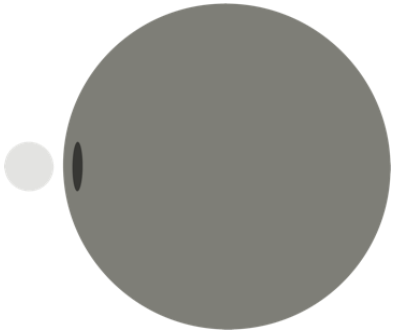
Acquired by HPE in 2023

500+ Global Edges

The SSE mission

To elevate secure access to power a modern workplace where people, and technology, work in harmony.

Select where your journey begins



Start by replacing VPN for zero trust remote access

Start with zero trust third-party access

Modernize to reduce network infrastructure and costs

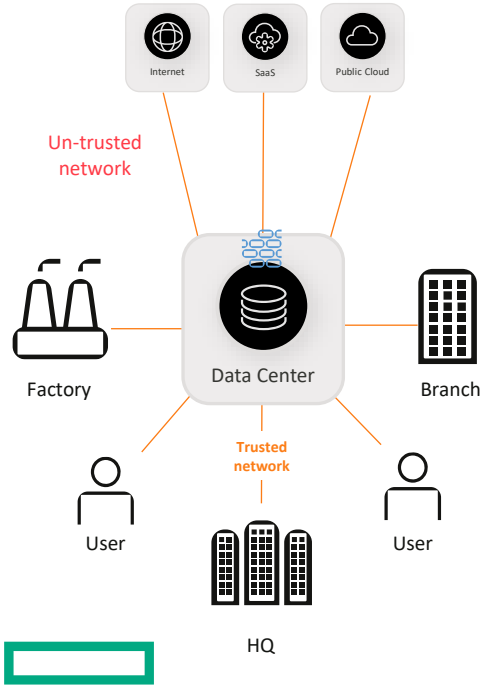
CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

P&G

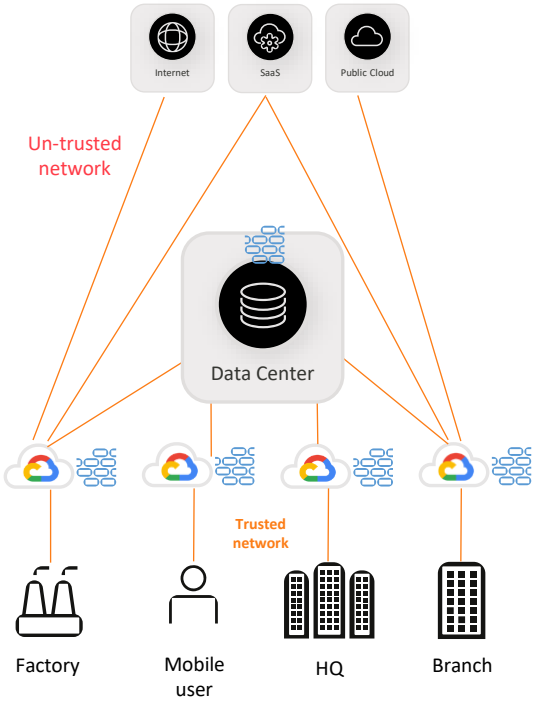
Visionworks

The approaches for accessing business resources

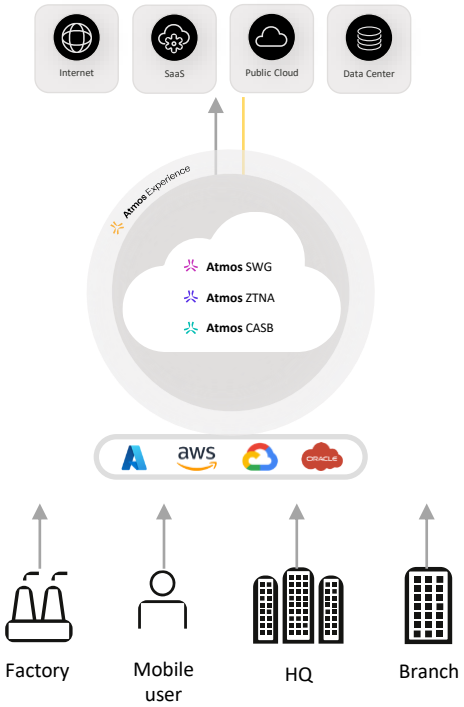
Hub and spoke network + perimeter-based security



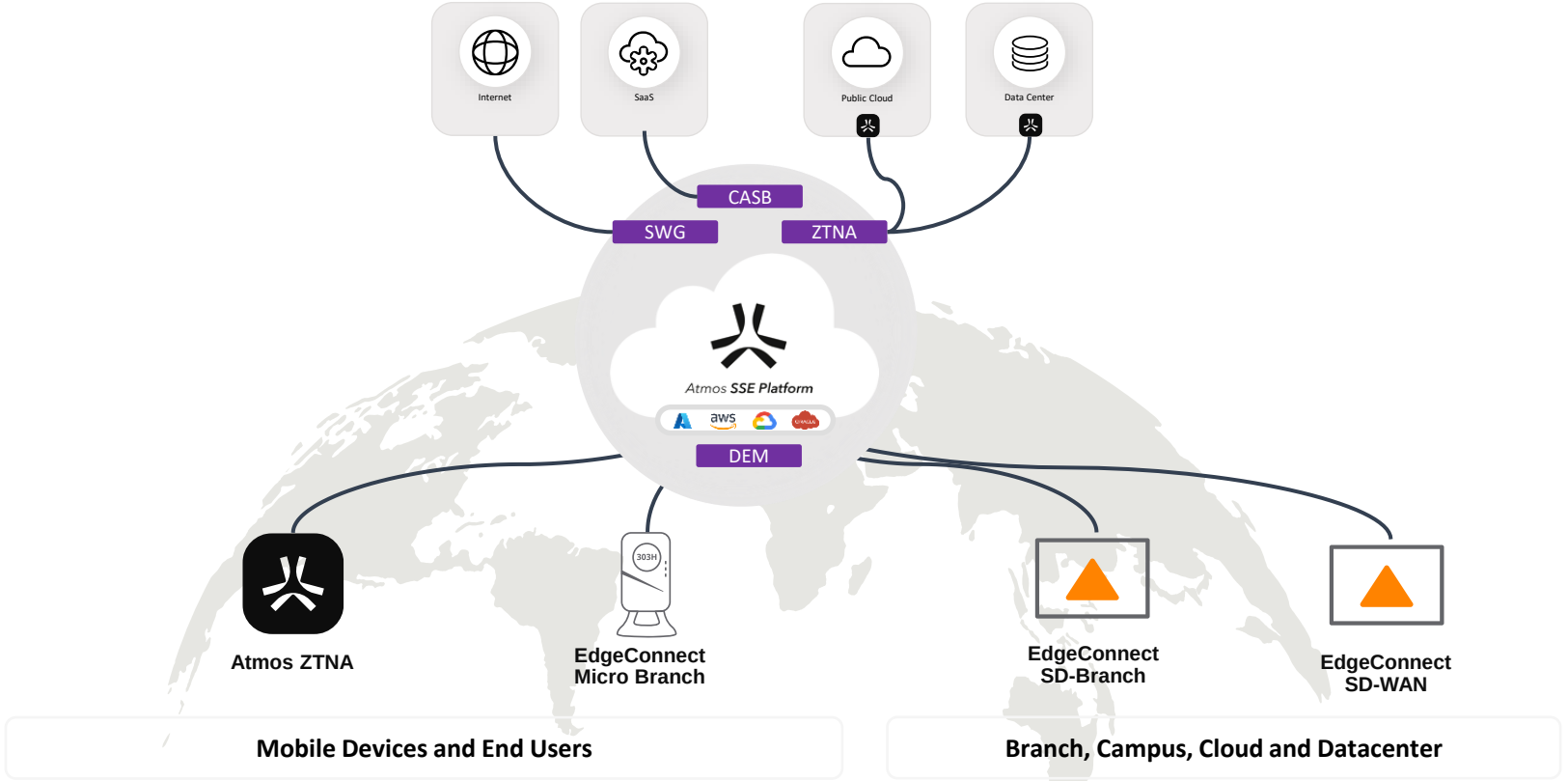
Virtualized cloud firewalls with customer-hosted PoPs



Connectivity-as-a-Service via cloud



Unified SASE helps transform networking



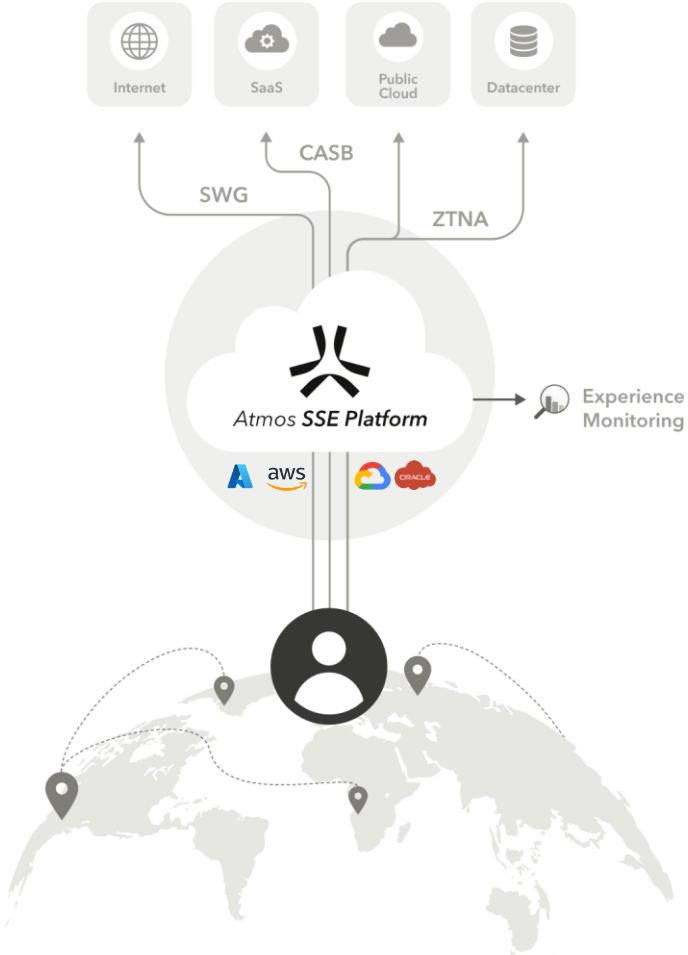
Axis
differentiators

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.)

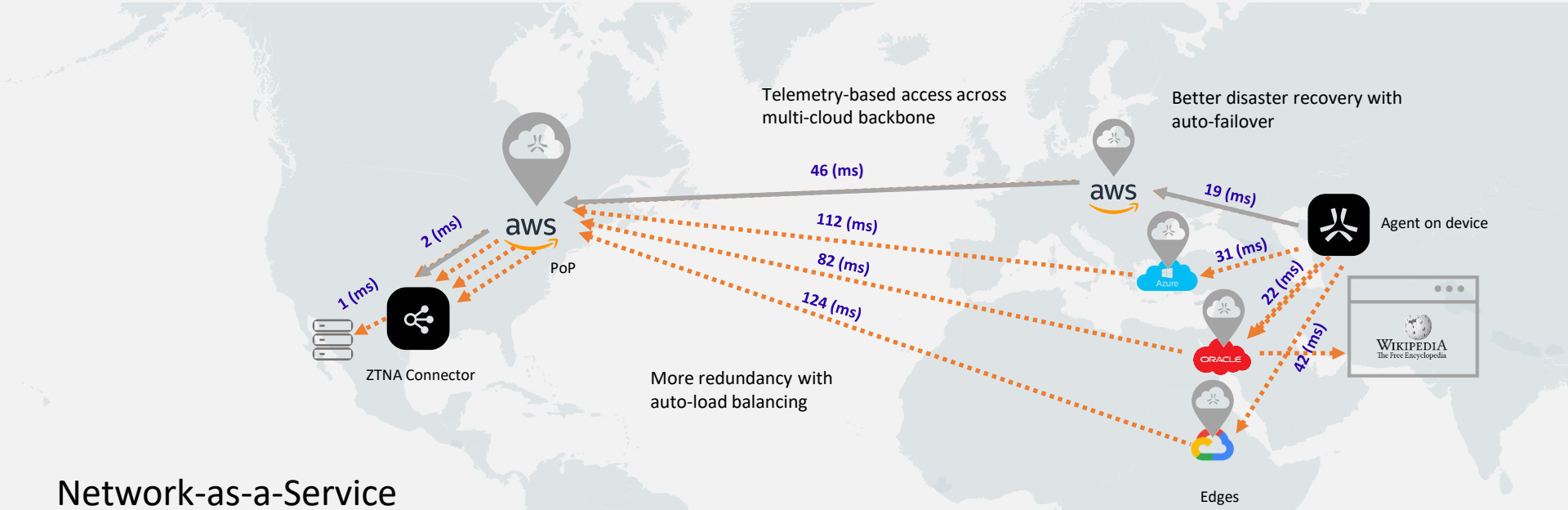
We harmonize access across the world via a cloud-backbone of AWS, Azure, Google and Oracle

We enable users to access resources with or without an agent



Distributed cloud architecture:

High reliability, availability, and scale

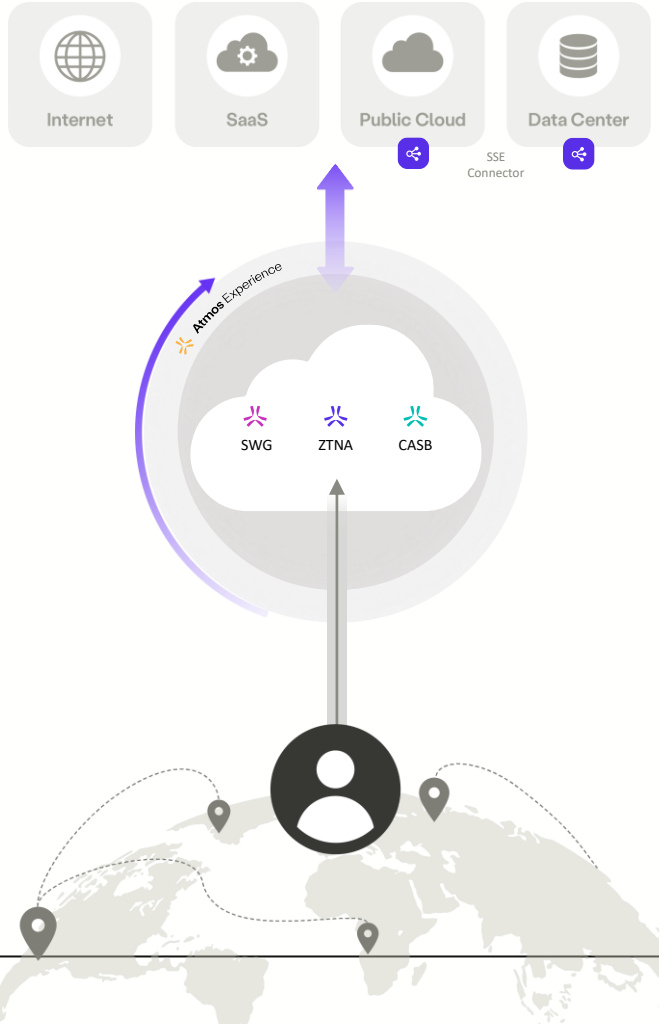


Network-as-a-Service

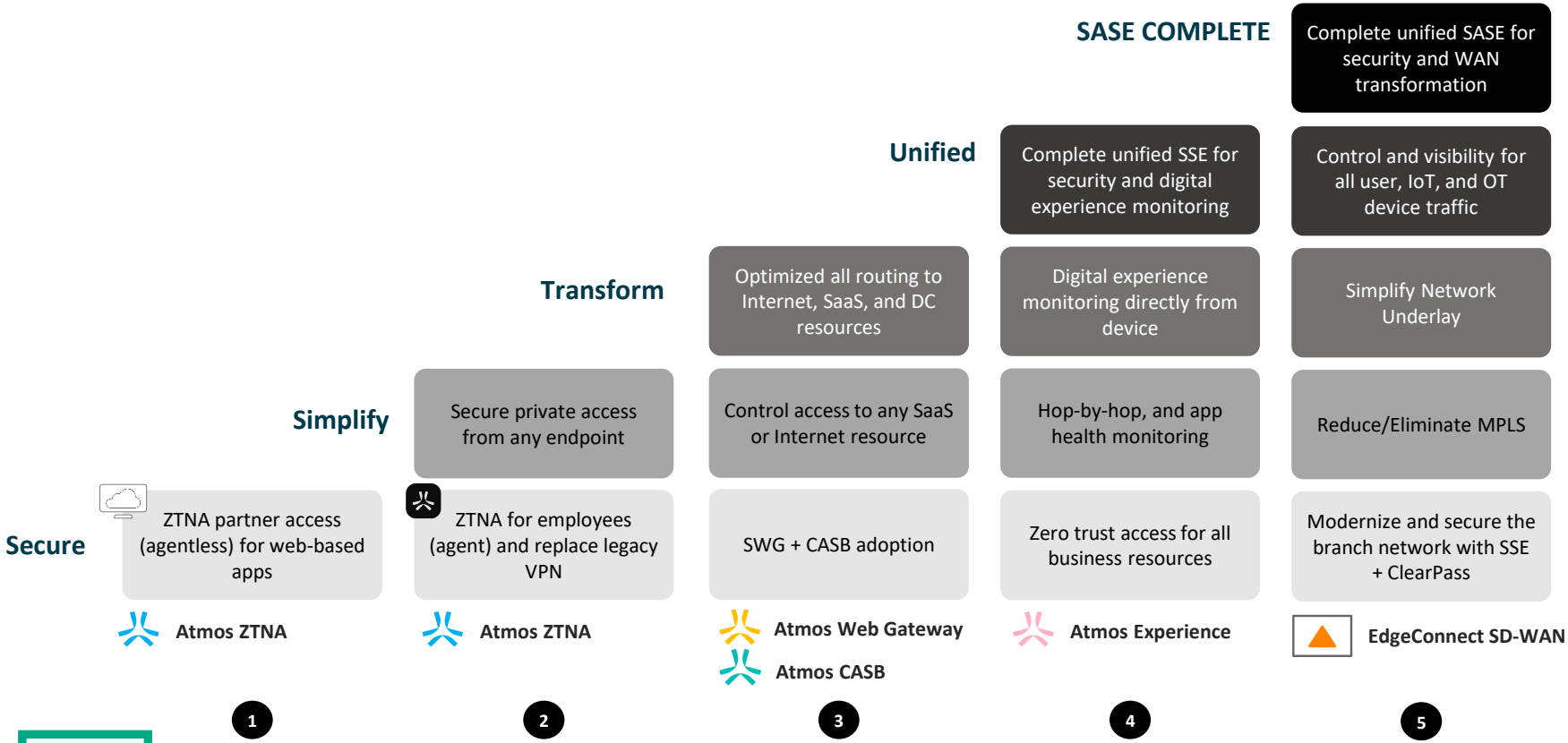
- PoP per session vs. PoP per user
- Geo-proximity routing (great for SWG)
- Smart routing based on latency (great for ZTNA)
- Extreme high availability & performance

Importance to your business

		1 - 10
1	Simplicity for admins to deploy & manage	☐
2	User experience & performance	☐
3	Resilience, uptime & availability	☐
4	Security inspection & controls in SWG, ZTNA, CASB	☐
5	Least privilege, mapping users to internal apps	☐
6	Full VPN replacement & server-initiated flows	☐
7	Single Vendor SASE (SSE + SD-WAN)	☐
8	Unmanaged device access, agentless ZTNA	☐



The journey to network transformation



Realize immediate business value from day one

End-to-end visibility across application access events

In minutes, employ adaptive policies to automate security and protect assets

Use cloud scale to ensure user productivity, and reduce IT tickets

100% cloud-service for fast deployment, and optimized CapEx and OpEx

Demo

Questions

Partner Resources

Partner Ready for Networking portal
https://partner.hpe.com/aruba

Arubapedia for Partners
https://afp.arubanetworks.com

My Learning / The Learning Center
www.mylearninghpe.com

Channel SE(CSE)
Regional channel support

Partner Technical Webinar Series

New HPE Aruba Networking Secure Access Service Edge (SASE)

Session 1: SASE Technical Solutions Overview
Monday, March 11th at 9 AM PT / 12 PM ET

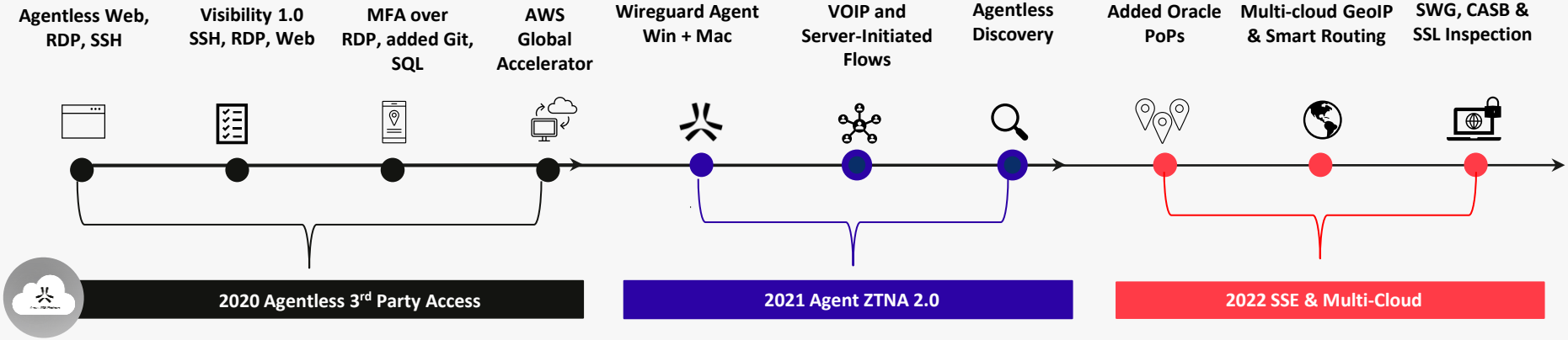
Session 2: HPE Aruba Networking Security SSE
Monday, April 1st at 9 AM PT / 12 PM ET

Session 3: Security Service Edge (SSE) Demo
Monday, May 6th at 9 AM PT / 12 PM ET

(Click here) to register for the webinar series

Thank you

Axis Roadmap - Past, Present & Future



Reduce the attack surface
Prevent applications from being discovered by placing them behind Axis – Web, SSH, RDP protected, no VPN

Inline inspection
User event & content inspection for visibility into user activity and for threat detection

DLP for Traffic
Inline controls enforce disable download, copy & paste etc. policies for users and servers

Least-privileged user access
Securely connect authorized users to specific apps, without placing them on the corporate network - no ACLs needed

Server initiated flows
Ensure VOIP, RDP, Patching, and much more can initiate flows back to user devices (vs only user initiated)

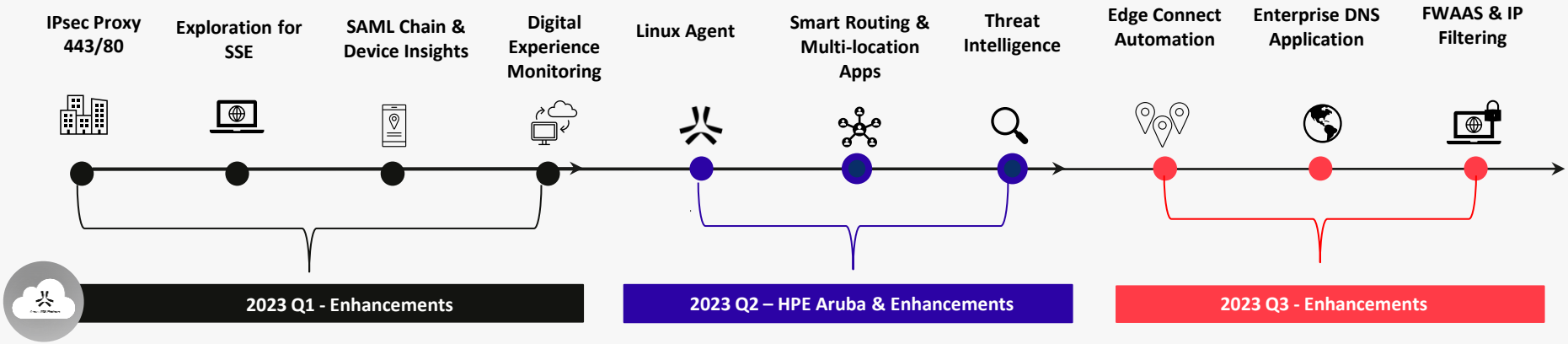
Agentless / Rewrite Discovery
Allow admins to generate a one time discovery link to ensure agentless applications are fully understood with simple admin suggestions for quick, confident configuration.

Unified SSE Platform
A truly unified agent, infrastructure and policy across all SSE including ZTNA, SWG and CASB

Visibility into malicious activity
View employee and third-party user activity across ZTNA, SWG and CASB in one solution.

Multi-Cloud Resilience
Maximize performance and resilience by sending users through the best PoP across AWS, Azure, GCP and Oracle

Axis Roadmap – 2023 so far…



IPsec Proxy
Unique IPsec Proxy allows admins to connect to a single load balanced FQDN for the best performance and resilience across multiple cloud PoPs vs a single PoP / IP.

Exploration for SSE
First of its kind ability to see flows across ZTNA, SWG, CASB all in a single data lake. Search and filter based on event type, user, file hash and more.

DEM
Real user data with hope by hop metrics and device performance for user experience analysis , troubleshooting and architectural insights.

Linux Agent
Support for Ubuntu (18 or higher), Fedora (26 or higher), Debian (10 or higher), RHEL (with desktop environment), CentOS (with desktop environment)

Smart Routing & Multi-Location Apps
Ability to assign multiple connectors to an app to ensure users route the best possible connector based on real time rout trip time (RTT) analysis.

Threat Intelligence
Prevent users from accessing websites that could be harmful leveraging reputation and domain-age based telemetry to provide greater end user protection.

Edge Connect Automation
Seamlessly send SDWAN and branch traffic through SSE for Security policy enforcement with the click of a button. Single vendor integrations offer 40 to 50 times faster updates in large enterprises vs Zscaler.

Enterprise DNS Application
Assists ZTNA admins in VPN replacements by automating and limiting access so DNS resolves seamlessly in large complex networks.

FWAAS / IP Filtering
Expands the IPsec capability from DNS and URL Filtering on 443/80 to any port with IP based filtering on policy and IP reputation.

Atmos Roadmap '23

Product

	Q3 AUG 2023	Q4 OCT 2023	Q1 JAN 2024	Q2 APR 2024
Security	Tenancy Restriction	Advanced Web Security		Deception
	IP Filtering	Cloud Firewall	Device Isolation	RBI
DLP	OCR	ML Content Classification	EDM	MIP Classification
Integrations	EdgeConnect Automation	O365 API CASB	SalesForce, GApps, API CASB	Teams, Zoom, Hangouts - QoS
	CASB Suites Support			Aruba Roles Integration
Analytics	Activity Exploration	SSE Dashboard	Application Auto Discovery	Query AI
		DEM+	Application Health	Shadow IT
Manageability	Warning Page	Agent Notification Center	Account Entitlement Page	GLCP Integration
		SPs Support		
Connectivity	ZTNA Advanced DNS	Bandwidth Control	Connectors Multi-PoP	IPv6 Advanced Support
		ZTNA via SD-WAN	Branch User Authentication	Quantum Safe Encryption
Global Deployment	SWG Localization	Connectors Self Update	Terraform Providers	
	China PoP		Federal Market Compliance	

Enable work from anywhere

0 Connector makes an outbound request

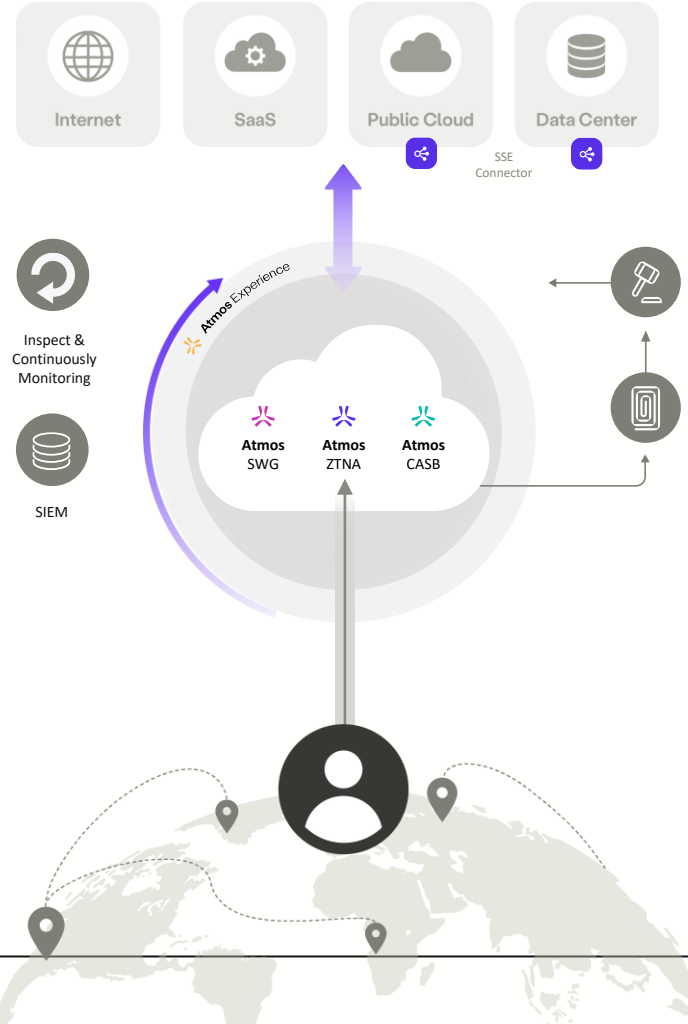
1 User requests access (agent or agentless)

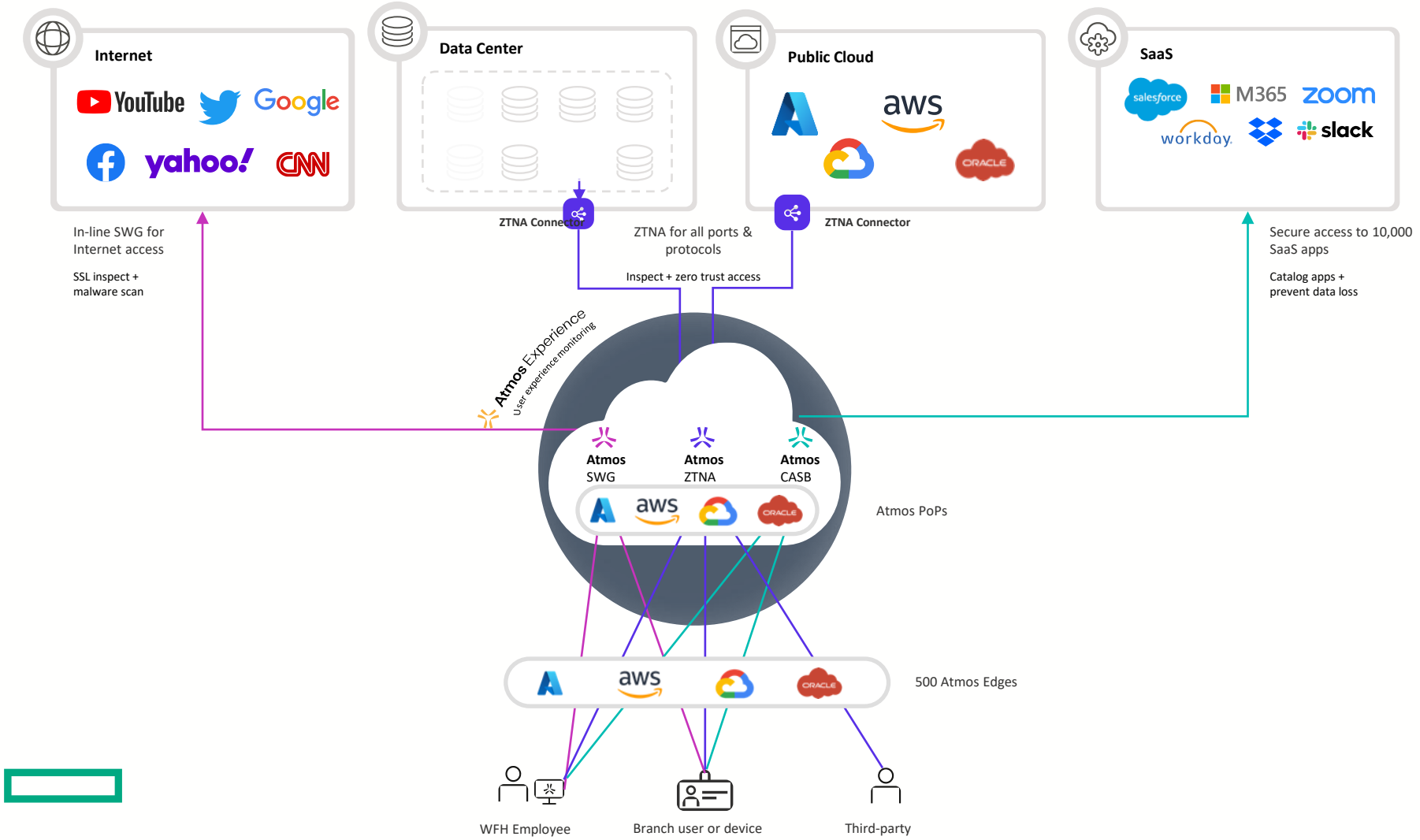
2 Mediates request to internal app

3 Identity + MFA verified + Policy evaluated

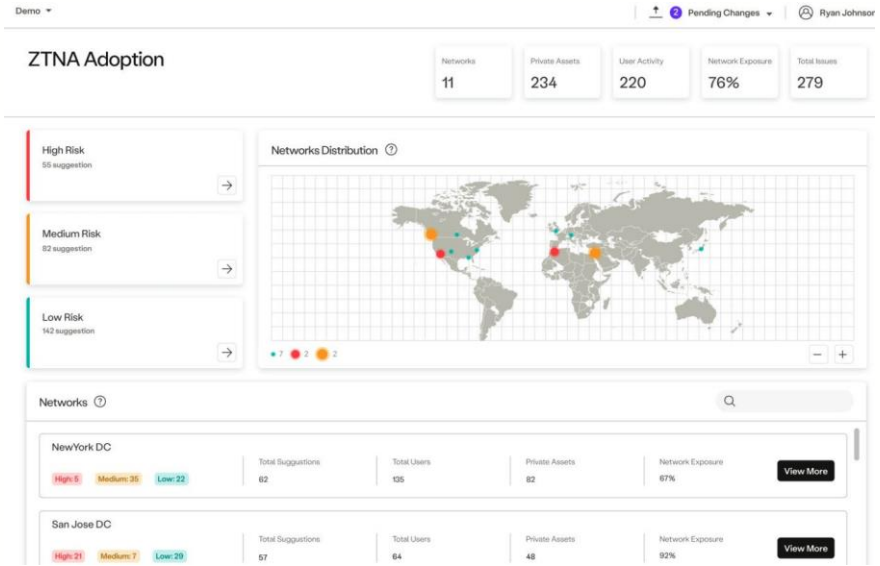
4 SSE Edge brokers 1:1 connection

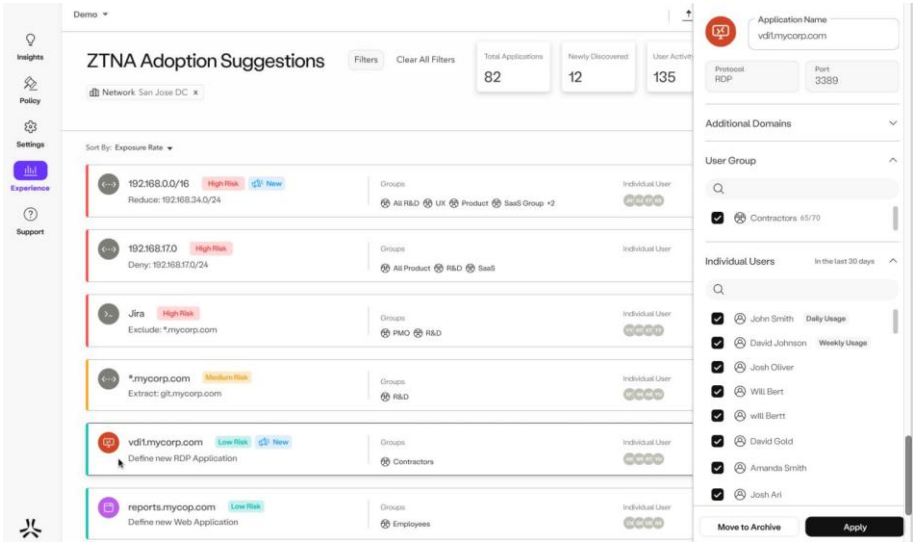
5 Continuously inspects, adapts, and protects data




Internet
YouTube
Google
yahoo!
CNN
Data Center
Public Cloud
aws
ORACLE
SaaS
salesforce
M365
zoom
workday.
slack
In-line SWG for Internet access
SSL inspect + malware scan
ZTNA Connector
ZTNA for all ports & protocols
Inspect + zero trust access
ZTNA Connector
Secure access to 10,000 SaaS apps
Catalog apps + prevent data loss
Atmos Experience
User experience monitoring
Atmos SWG
Atmos ZTNA
Atmos CASB
Atmos PoPs
500 Atmos Edges
WFH Employee
Branch user or device
Third-party

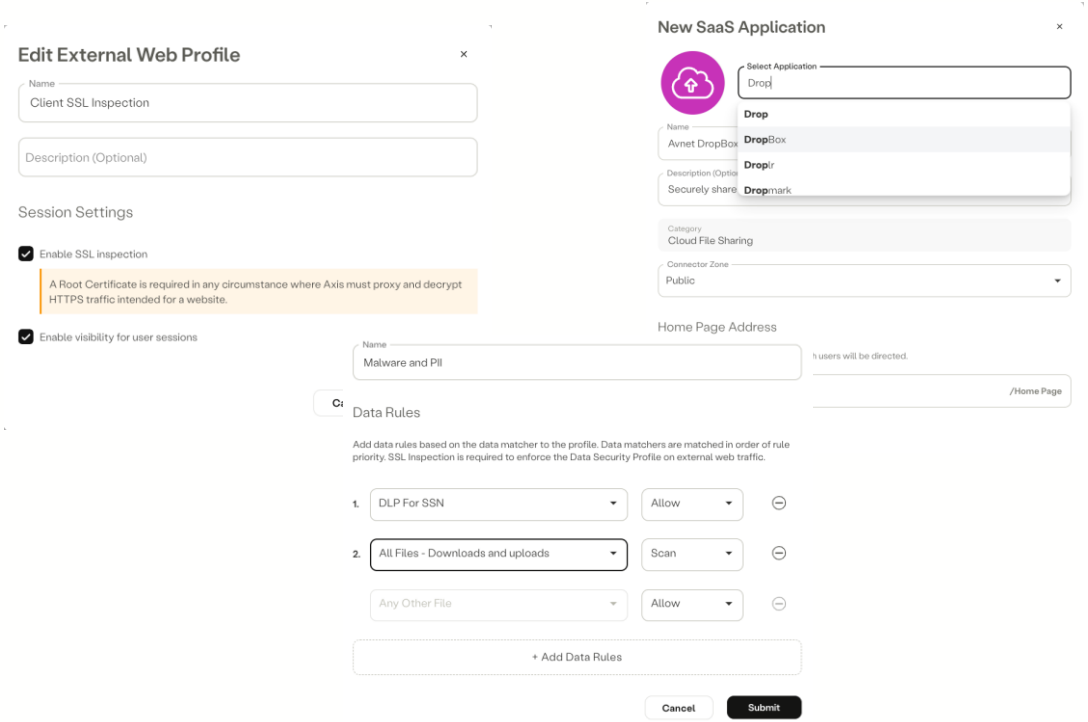
ZTNA adoption guidance to simplify first steps





Get viz & control for Internet & SaaS traffic

- Full SSL inspection
- Proactive malware scanning:
  - Send uploaded files to be scanned
  - Send downloaded files to be scanned
- In-line CASB tracks activity for +10,000 SaaS apps
- All part of single SSE code-base

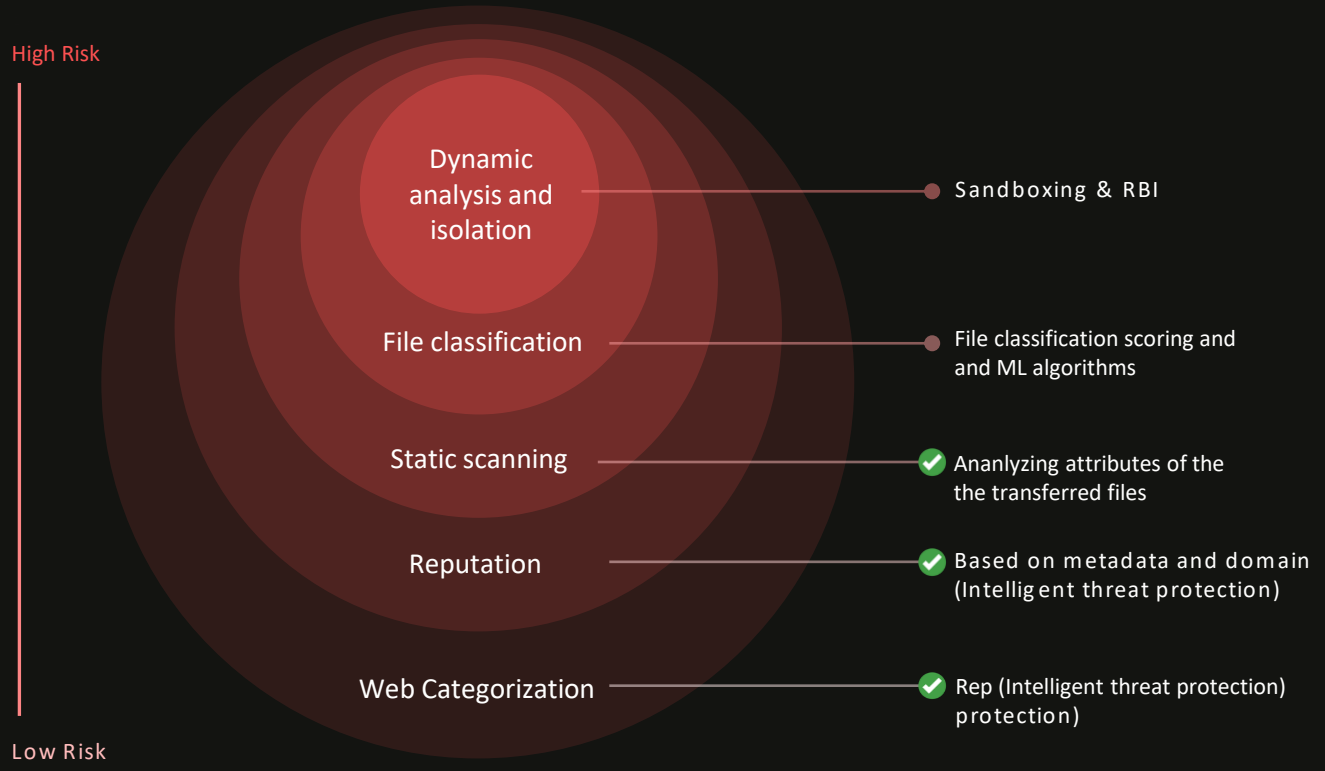


Threat Prevention

Multi Tier model

Reverse correlation between the risk and the utilization.

Most use-cases will be sufficient with the lower 2 tier, while a more sophisticated malware will require a more advanced approach such as file classification and dynamic scanning.



Unify DLP across all data

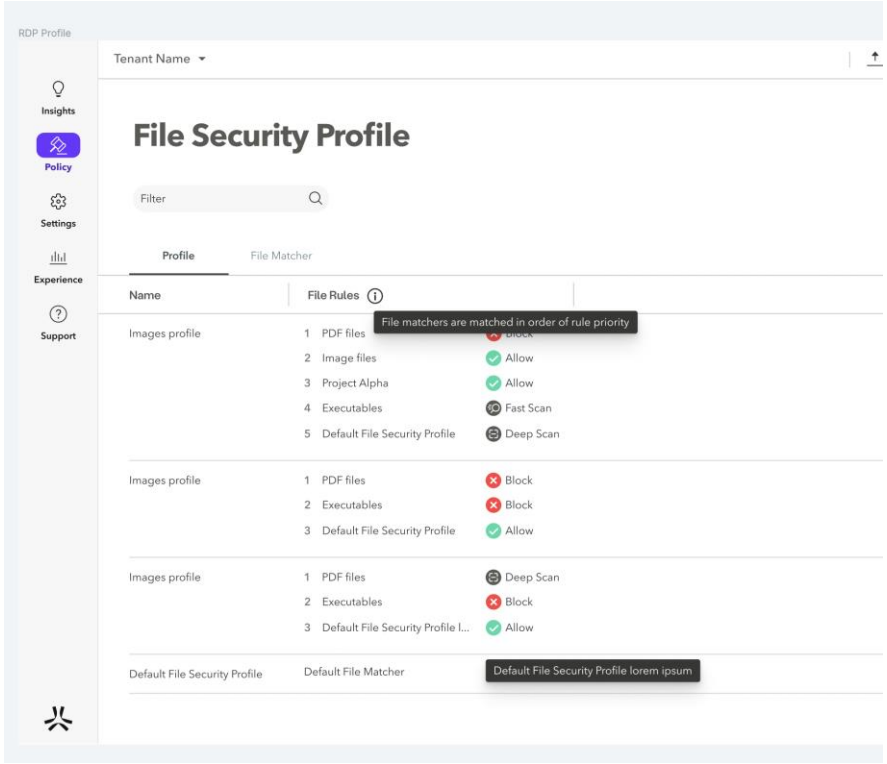
Easily control the flow of your data with DLP functionality across SWG, CASB, and ZTNA traffic.

- **File Content Control**
  Control data transfer within files based on patterns. Allow only specific file types to be uploaded / downloaded

- **File Metadata Control** Control file transfer based on various metadata attributes *(name, type, size)*

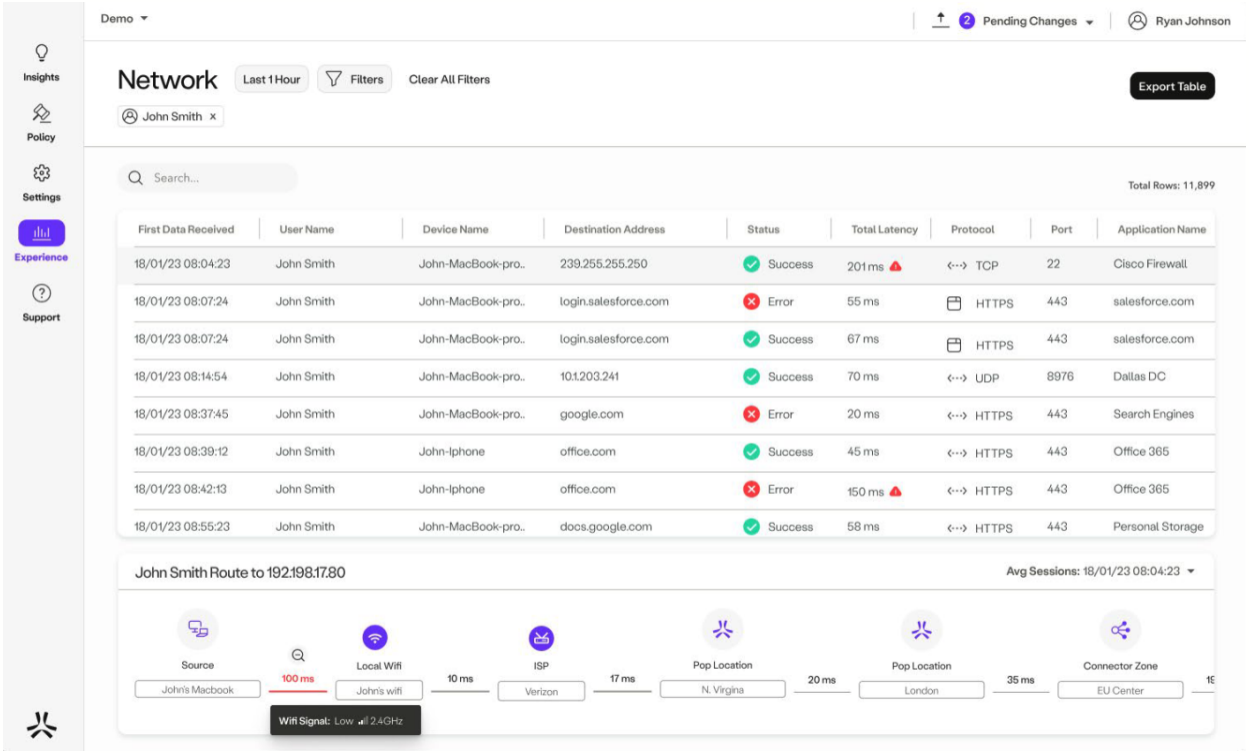
Regex support with OCR

Searches a string of characters (text. .gif, .png, .jpeg images) for patterns and applies controls.

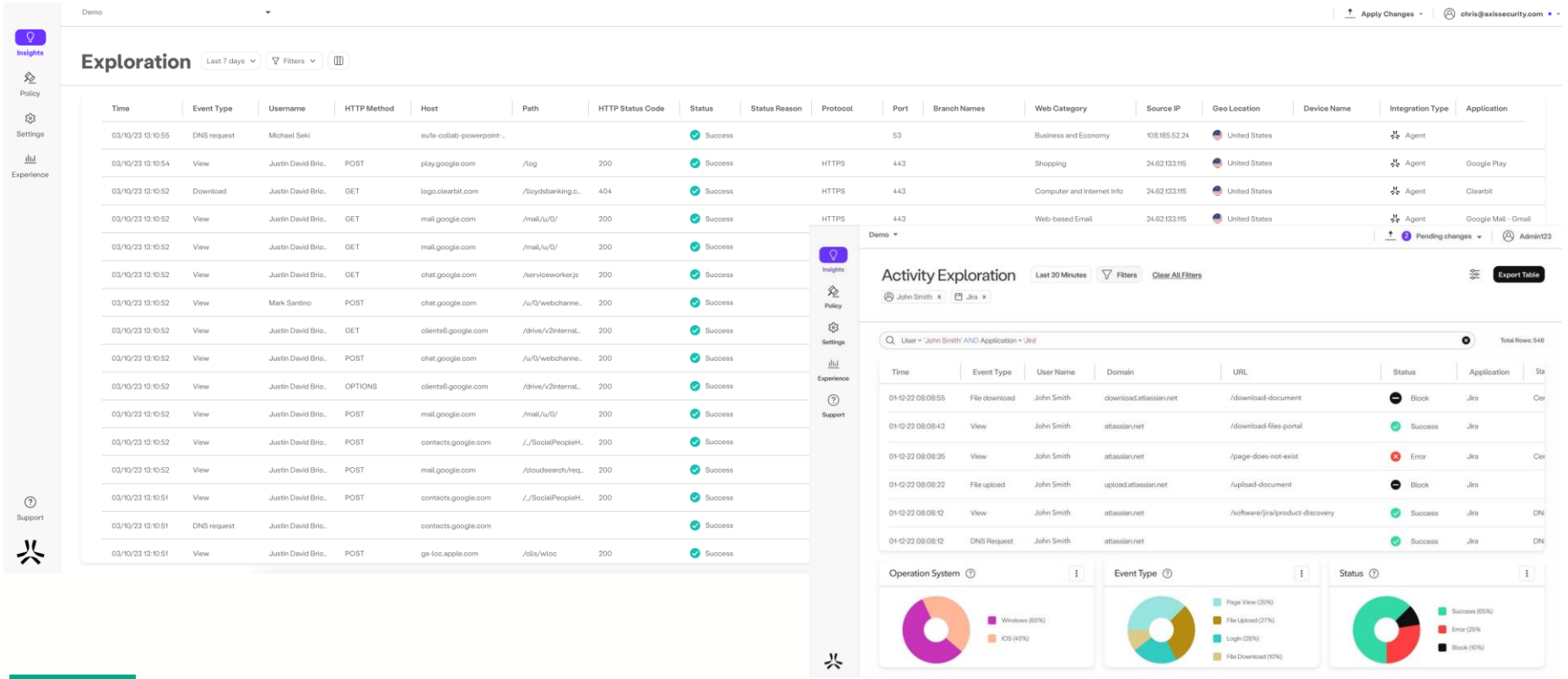


And ensure a great user experience too

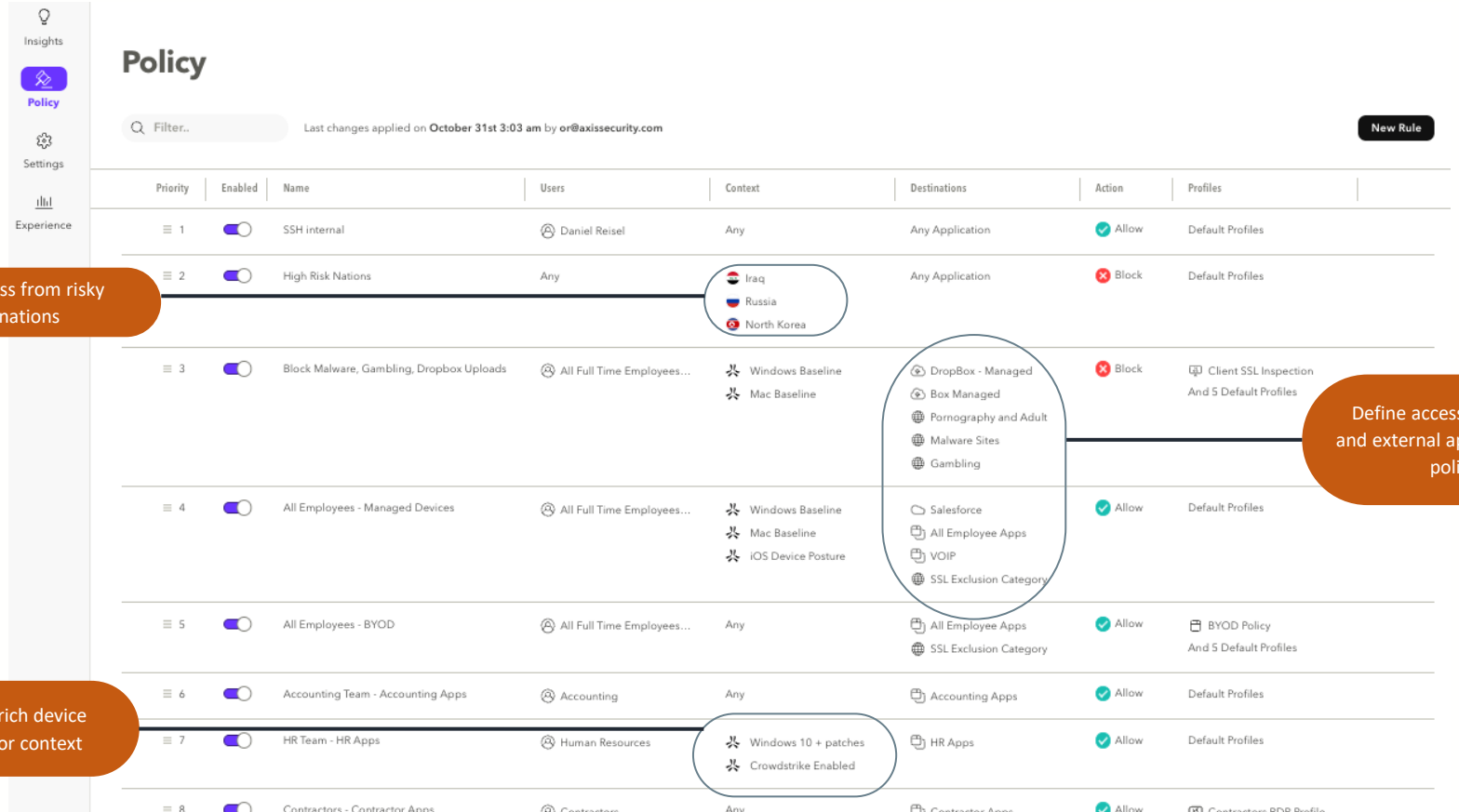
- Dynamic monitoring of user experience issues
- Endpoint telemetry i.e. CPU, resource consumption, memory use
- Unified application health monitoring
- Hop by hop network path metrics between users and business apps

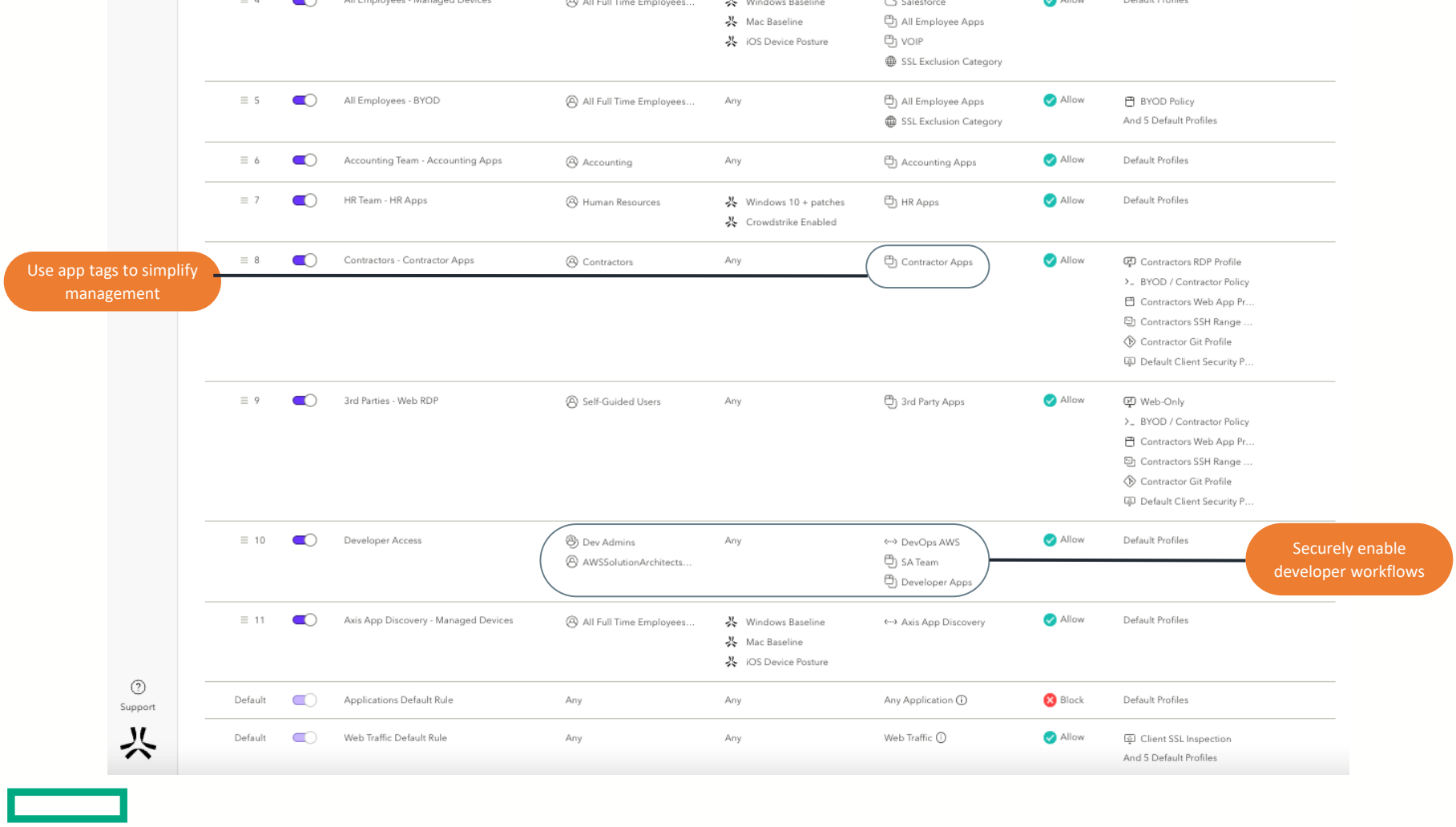


Unified visibility across every business resource



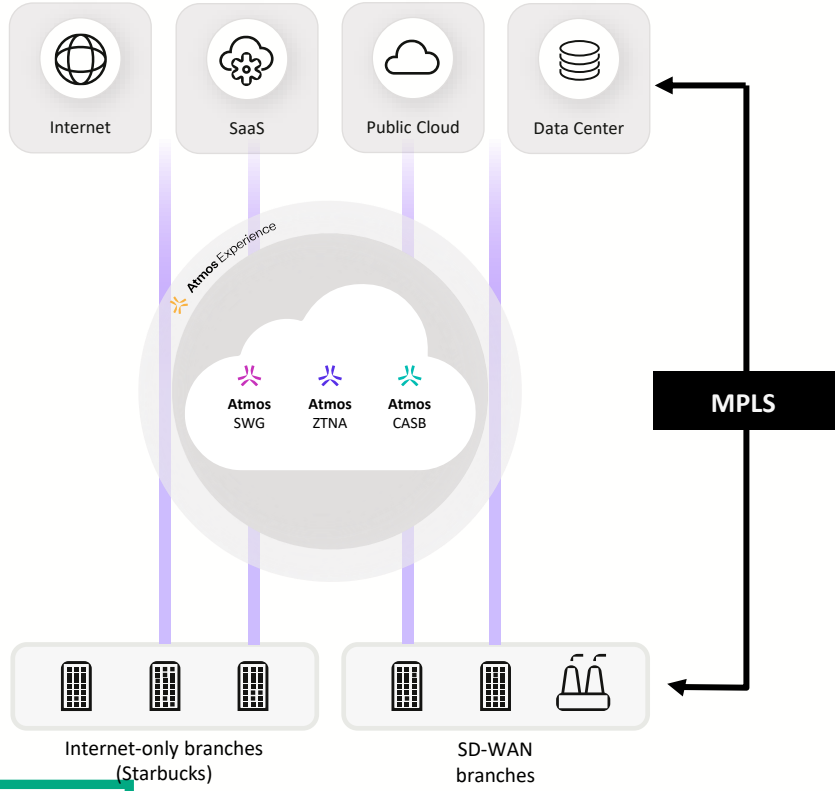
One policy to easily control access to all apps




Use app tags to simplify management
Securely enable developer workflows
Support

Secure branch connectivity

Internet WAN + SD-WAN



Reduce costs and complexity at branch

Provide a fast, secure user experience

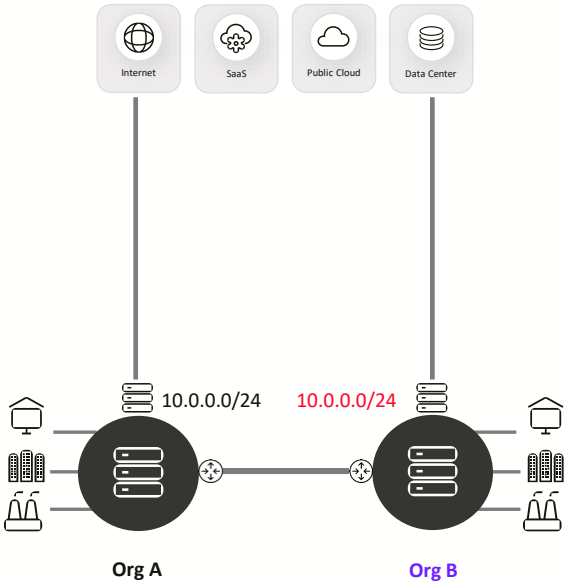
Support headless device traffic

"By 2023, to deliver flexible, cost-effective scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020."

Gartner

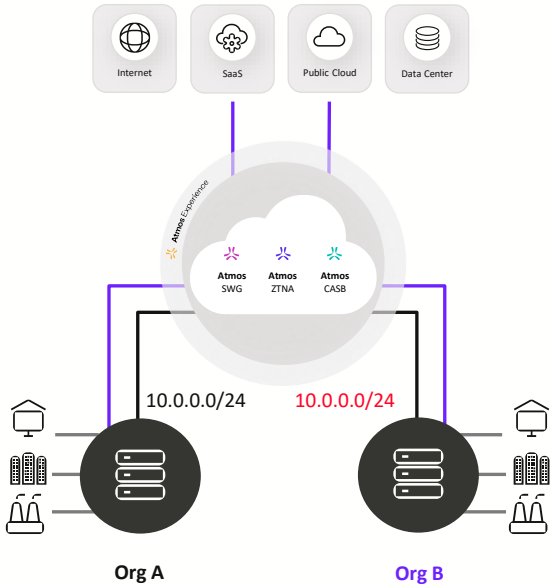
Accelerate M&A and divestitures

M&A with **traditional networking**



- Network convergence and NATing for IP overlaps
- Security standards often not on par
- Requires ACLs via firewalls for network access

M&A with **Atmos**

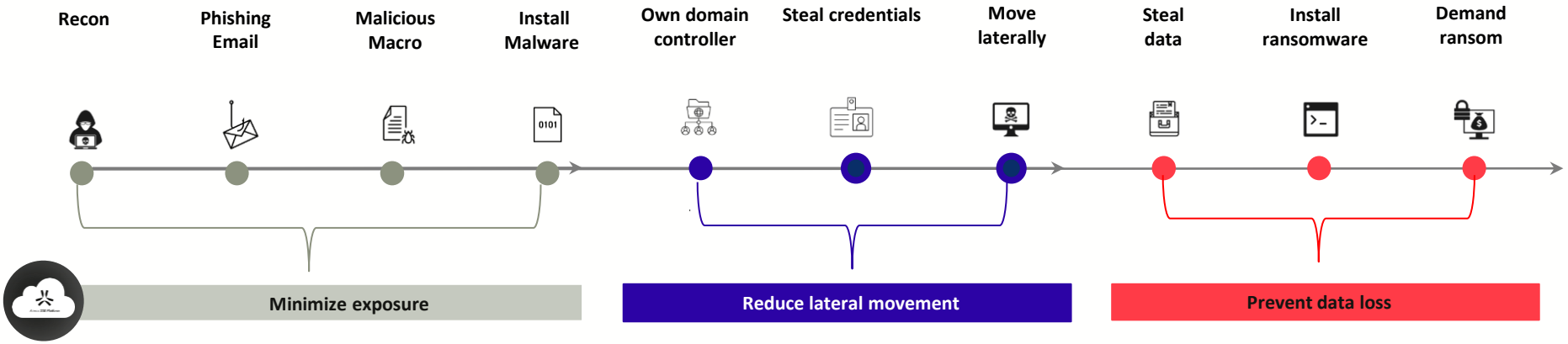


- Networks left as is, no need to consolidate
- Standardized security across both companies
- Users have direct-to-app access w/o network access

First step to SSE - Next-gen ZTNA

Coverage	Axis Security	Zscaler ZPA	PAN Prisma Access
SaaS Solution	X	X	X
Cloud Native Multi-Cloud Infrastructure (AWS, GCP, Oracle for 400+ PoPs)	X		
Single Policy SSE - ZTNA, SaaS, DEM	X		
Supports Agentless Web, SSH, RDP, Git, DB (Native)	X		
Supports Agentless SSH & RDP (over Web)	X		
Provides Agentless User Portal (optional)	X		
Agent for User Device Thick Client Support	X	X	X
Support for Client to Server	X	X	X
Support for Server to Client	X		X
Support for P2P / VOIP	X		X
Agentles Web Application Rewrite Engine	X		
Security			
Integration with SSO / MFA	X	X	X
No Inbound Ports / Cloaks Network for DDoS Defense	X	X	
Segmentless / Unlimited Least Privilege (No Segment, Port or Wildcard Overlap)	X		
Visibility - Layer 7 Session Audit Log (Web, SSH, RDP, Git, DB)	X		
Control - Layer 7 Download / Upload / etc. (Web, RDP, SSH)	X		
Control - Layer 7 Copy/Paste (RDP, SSH) & Print (RDP)	X		
MFA for Native RDP Protocol	X		

Preventing ransomware with Atmos



Eliminate the attack surface
Prevent applications from being discovered by placing them behind Axis – RDP protected, no VPN

Inline content inspection
Content inspection for visibility into user activity and for threat detection

Least-privileged user access
Securely connect authorized users to specific apps, without placing them on the corporate network - no ACLs needed

Server-to-Server segmentation
Enable least privilege server-to-server communications to protect networks from ransomware

DLP for Traffic
Inline controls enforce disable download, copy & paste etc. policies for users and servers

Visibility into malicious activity
View employee and third-party user activity, file downloads, protocols used, and SSH commands