

# 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



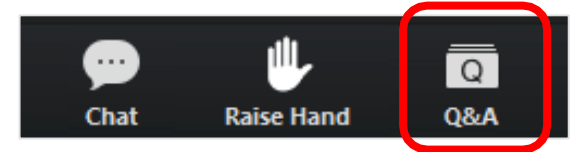
- All lines are muted during the webinar



- 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

---

**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

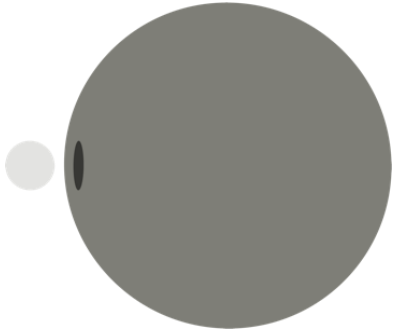
500+ Global Edges

## The SSE mission

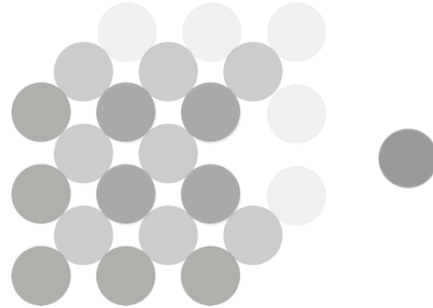
To elevate secure access to power a modern workplace where people, and technology, work in harmony.



# Select where your journey begins



Start by replacing VPN for zero trust remote access



Start with zero trust third-party access

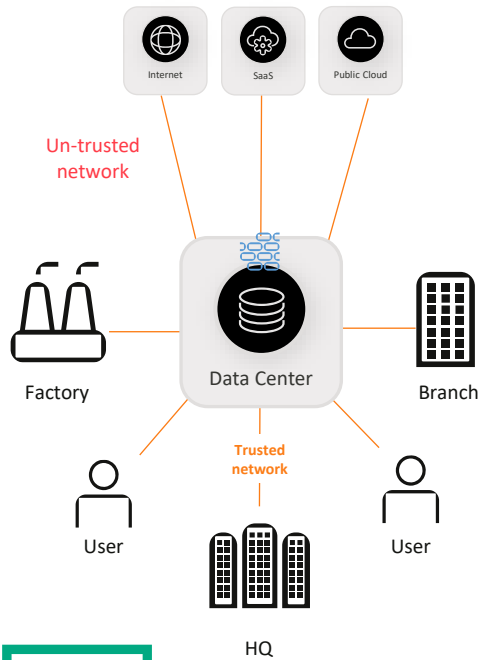


Modernize to reduce network infrastructure and costs

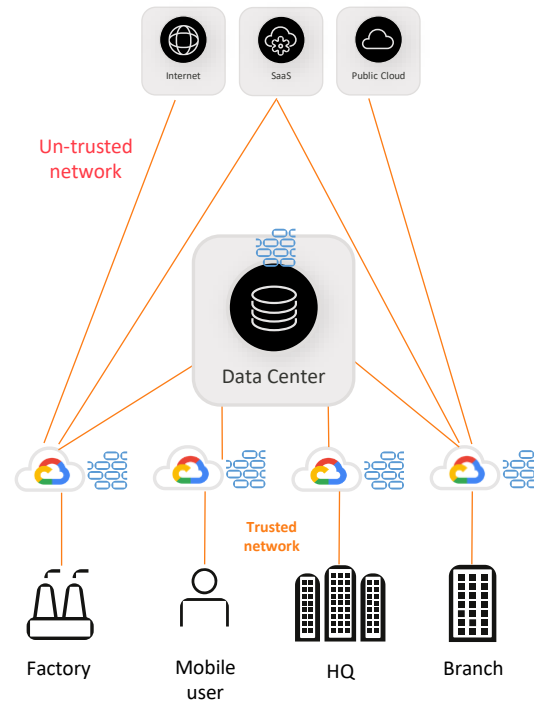


# The approaches for accessing business resources

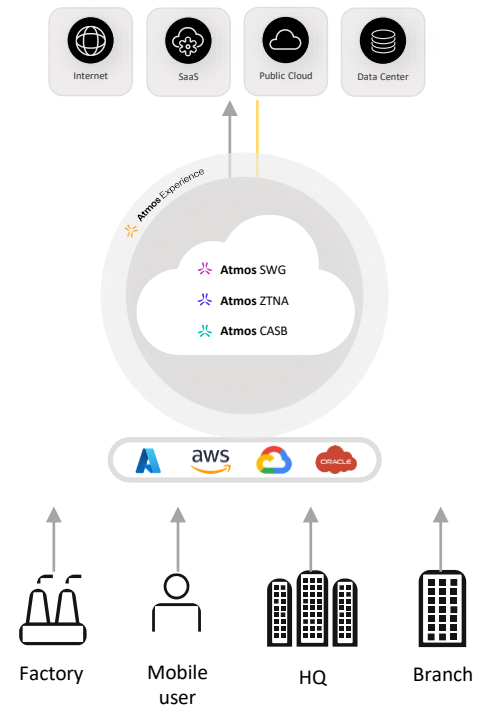
## Hub and spoke network + perimeter-based security



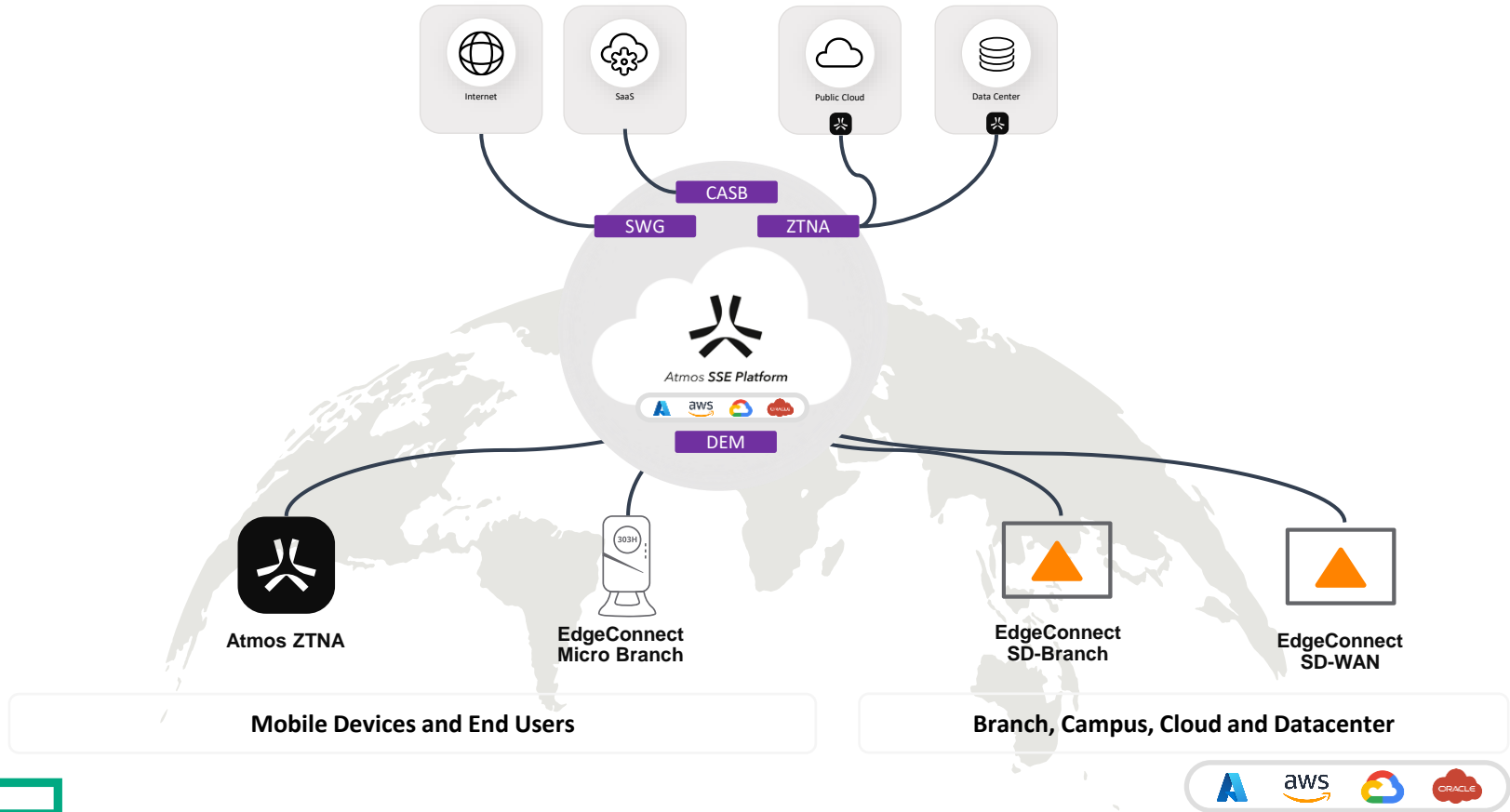
## Virtualized cloud firewalls with customer-hosted PoPs



## 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.)

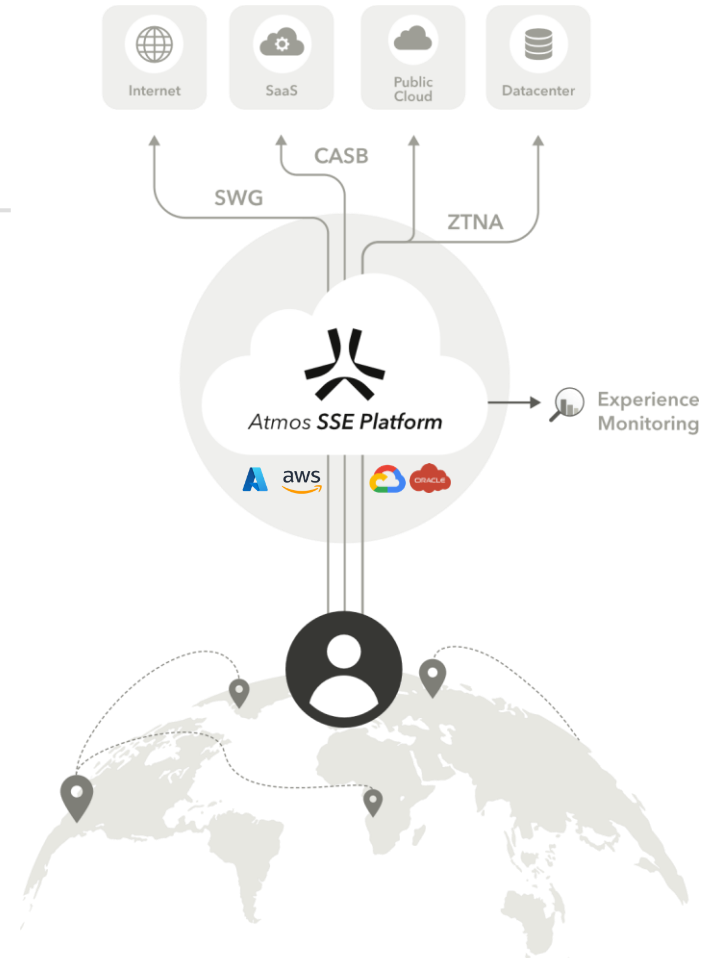
---

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

---

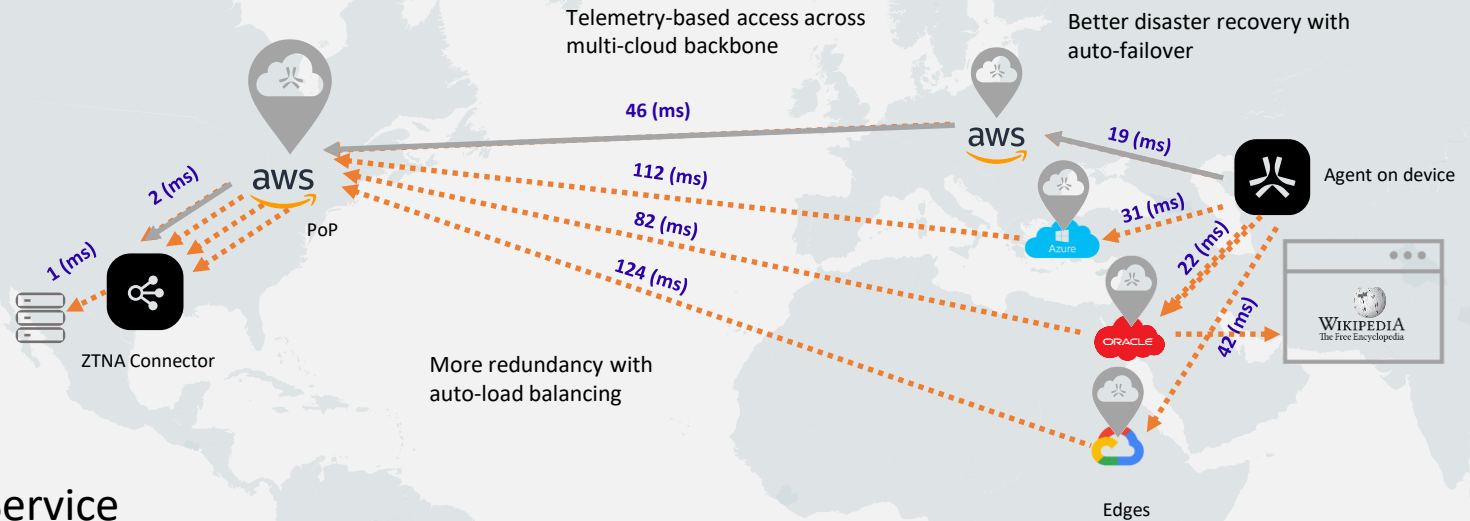
We enable users to access resources with or without an agent

---



# Distributed cloud architecture:

High reliability, availability, and scale



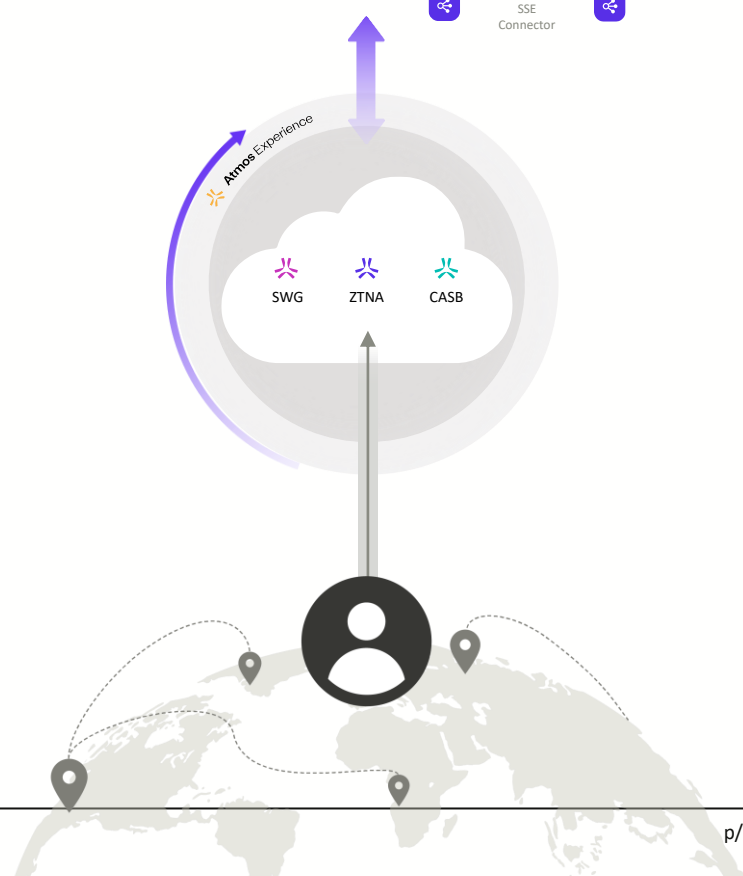
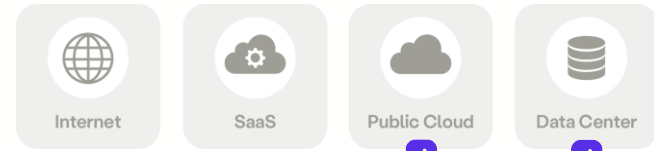
## Network-as-a-Service

- 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

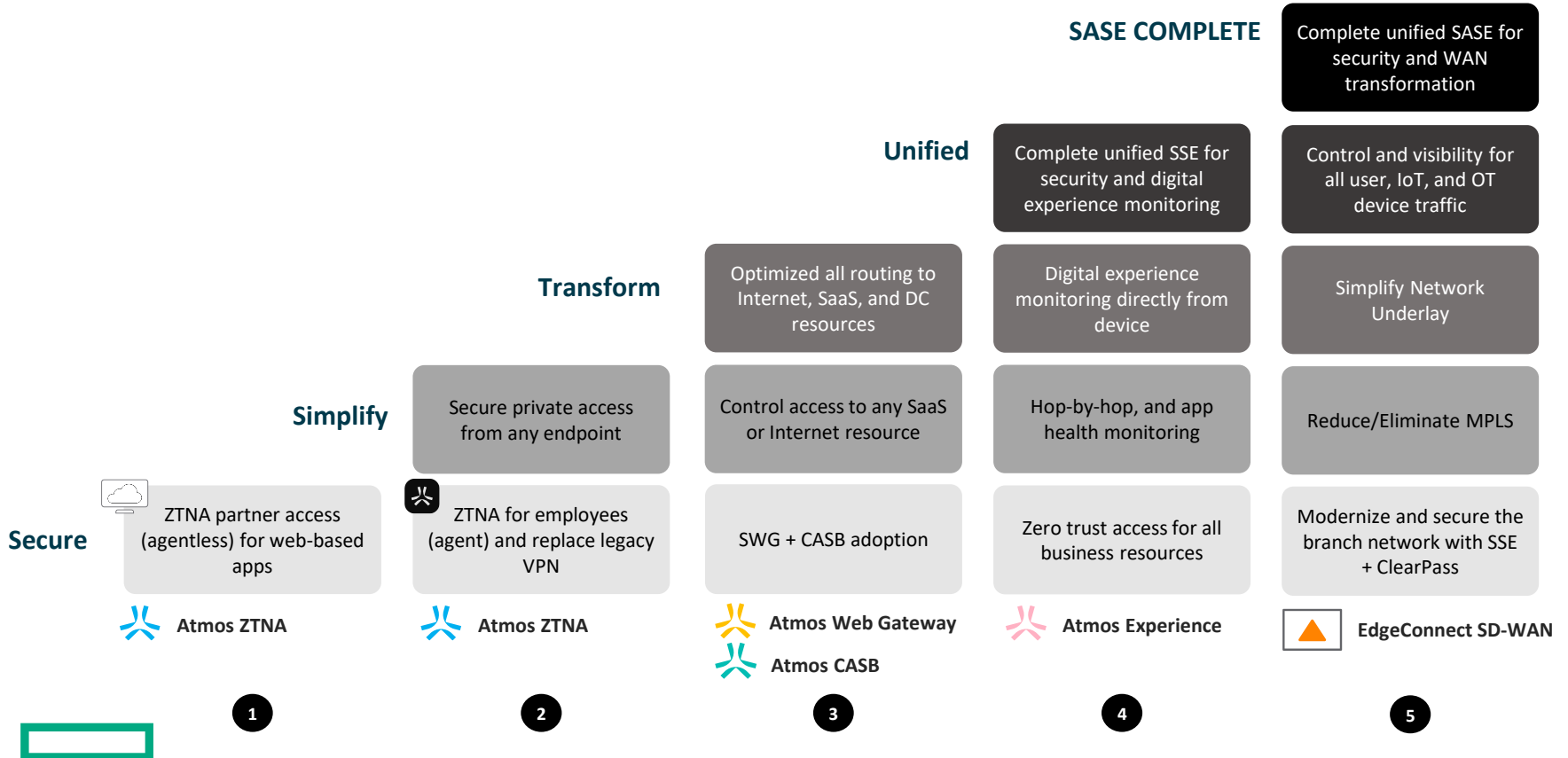
# Importance to your business

- 1 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

1 - 10



# 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](http://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**

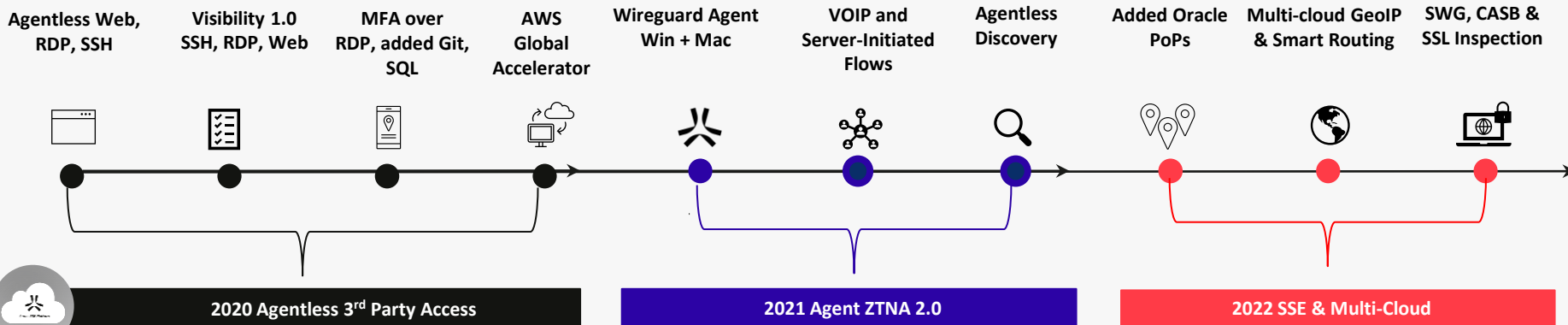
Monday, May 6th at 9 AM PT / 12 PM ET

([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

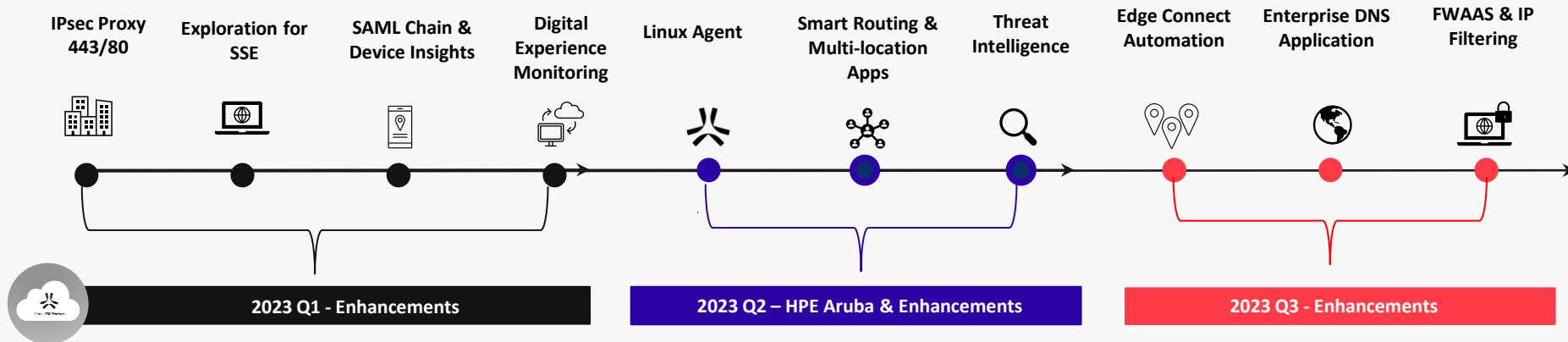
## Visibility into malicious activity

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

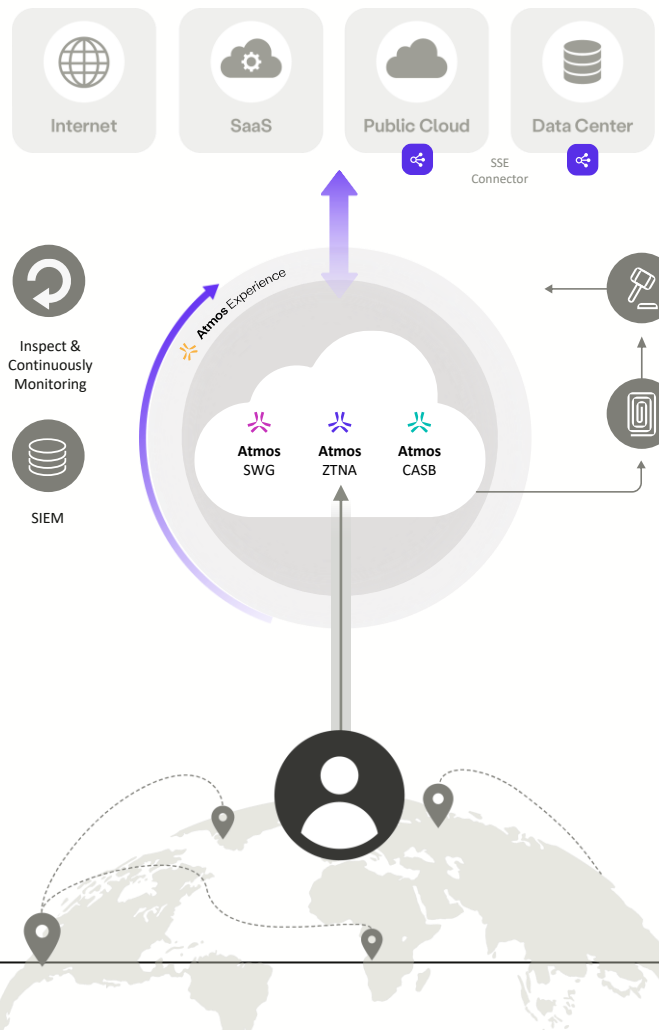
Q1 JAN 2024

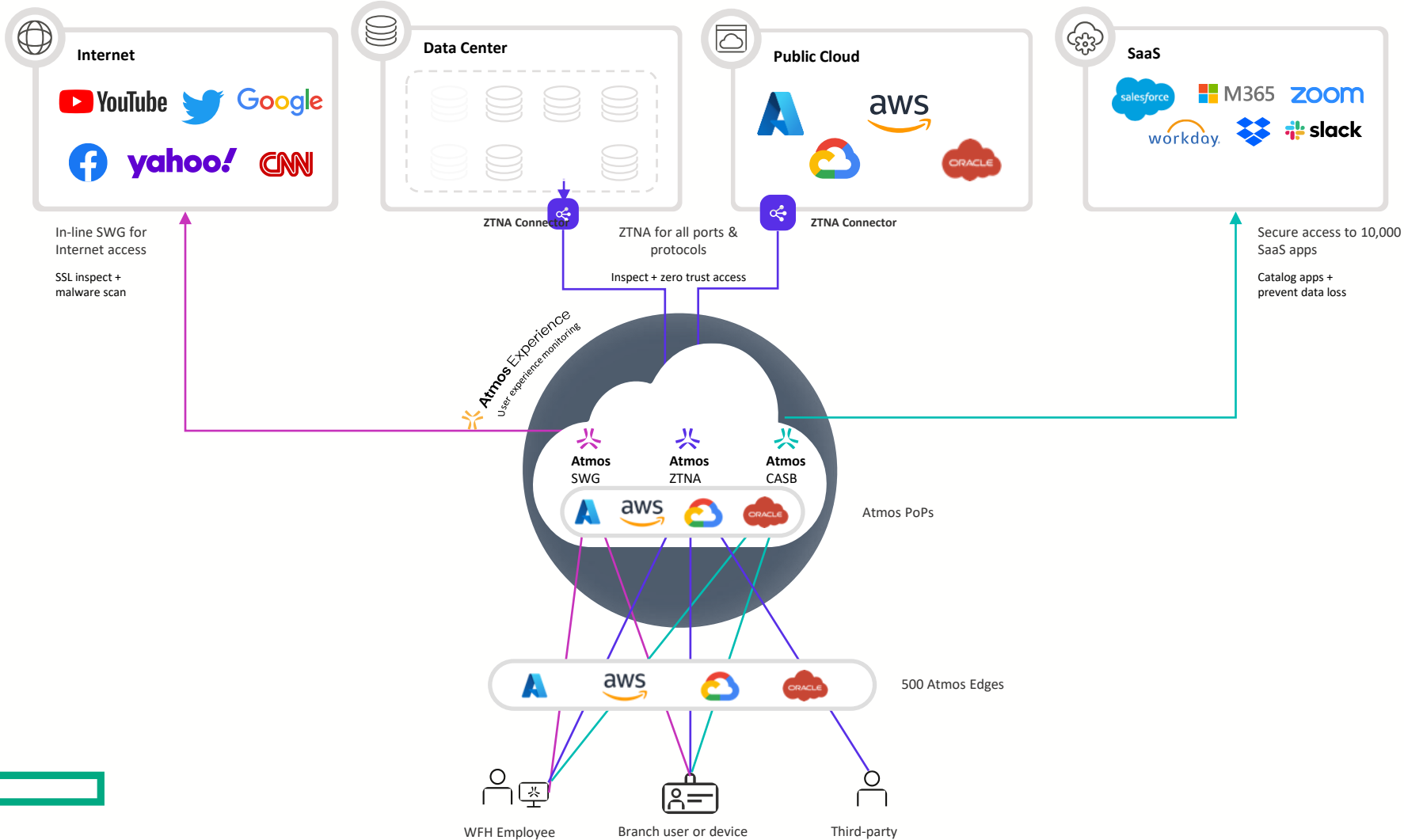
Q2 APR 2024

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	

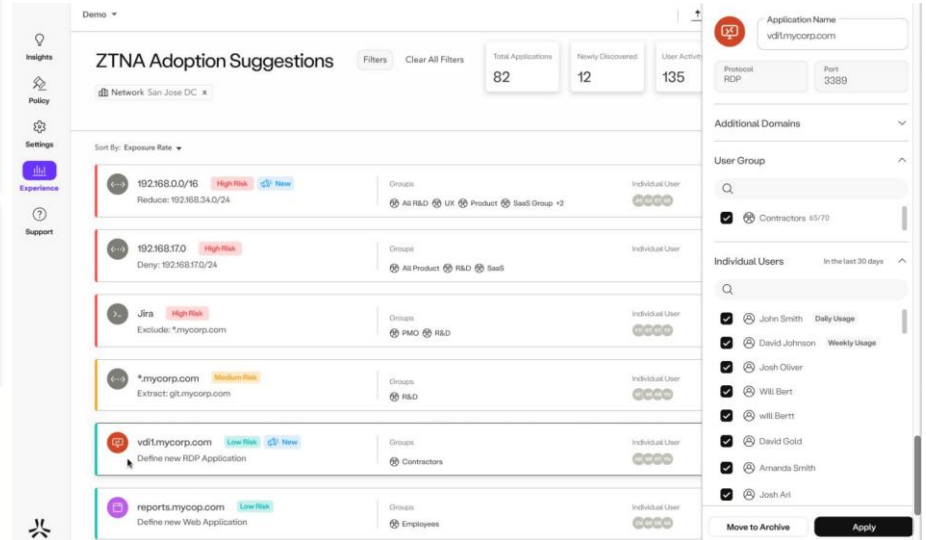
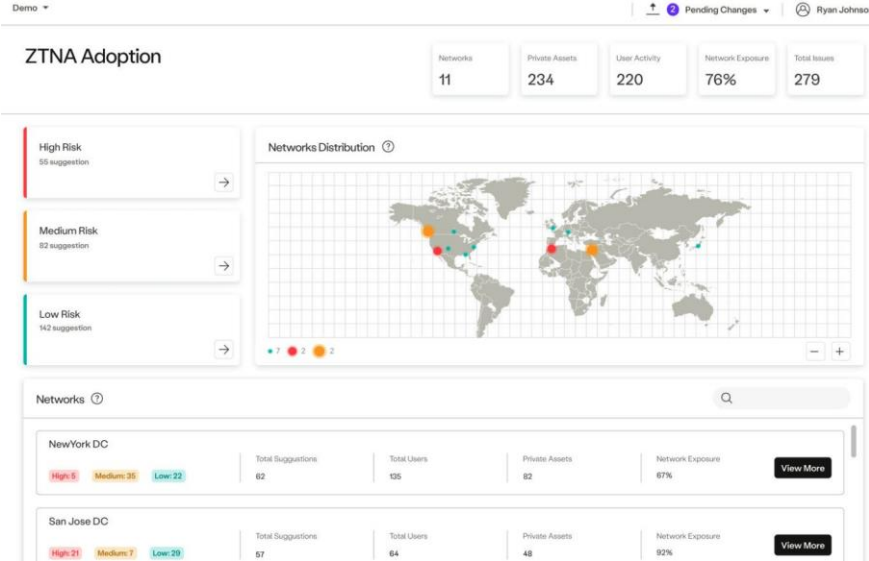
# Enable work from anywhere

- 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





# 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

The image shows two overlapping configuration windows from a Palo Alto Networks management console.

**Edit External Web Profile**

- Name: Client SSL Inspection
- Description (Optional):
- Session Settings:
  - Enable SSL inspection
    - A Root Certificate is required in any circumstance where Axis must proxy and decrypt HTTPS traffic intended for a website.
  - Enable visibility for user sessions
- Name: Malware and PII
- Category: Data Rules
- Home Page Address: /Home Page
- Data Rules:
  - 1. DLP For SSN: Allow
  - 2. All Files - Downloads and uploads: Scan
  - Any Other File: Allow
- Buttons: Cancel, Submit

**New SaaS Application**

- Select Application: Drop
- Name: Avnet DropBox
- Description (Optional): Securely share
- Category: Cloud File Sharing
- Connector Zone: Public
- Home Page Address: /Home Page

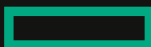
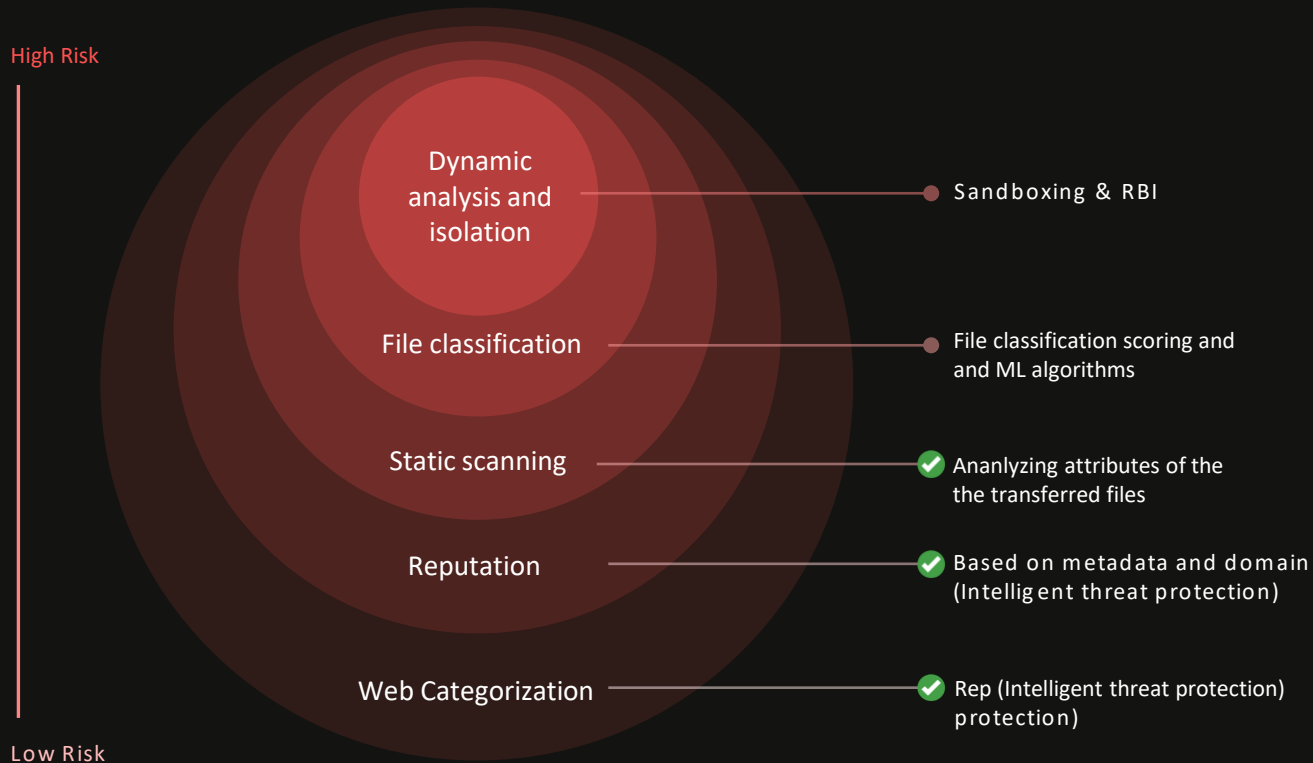


# Threat Prevention

## 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.

The screenshot shows the 'File Security Profile' configuration page. The interface includes a sidebar with navigation options: Insights, Policy, Settings, Experience, and Support. The main content area is titled 'File Security Profile' and features a 'Filter' search bar. Below the search bar, there are two tabs: 'Profile' (selected) and 'File Matcher'. The 'Profile' tab displays a table of file security profiles. A tooltip indicates that 'File matchers are matched in order of rule priority'. The table lists three profiles, each with a list of rules and their corresponding actions.

Name	File Rules
Images profile	<ul style="list-style-type: none"><li>1 PDF files (Block)</li><li>2 Image files (Allow)</li><li>3 Project Alpha (Allow)</li><li>4 Executables (Fast Scan)</li><li>5 Default File Security Profile (Deep Scan)</li></ul>
Images profile	<ul style="list-style-type: none"><li>1 PDF files (Block)</li><li>2 Executables (Block)</li><li>3 Default File Security Profile (Allow)</li></ul>
Images profile	<ul style="list-style-type: none"><li>1 PDF files (Deep Scan)</li><li>2 Executables (Block)</li><li>3 Default File Security Profile L... (Allow)</li></ul>
Default File Security Profile	Default File Matcher (Default File Security Profile lorem ipsum)



# 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

The screenshot displays a network monitoring interface. At the top, it shows 'Demo', 'Pending Changes', and the user 'Ryan Johnson'. The main section is titled 'Network' and includes filters for 'Last 1 Hour', 'Filters', and 'Clear All Filters'. A search bar is present, and the total number of rows is 11,899. Below the search bar is a table with the following columns: First Data Received, User Name, Device Name, Destination Address, Status, Total Latency, Protocol, Port, and Application Name. The table contains several rows of data, including successful and failed connections to various services like Salesforce, Google, and Office 365. Below the table, there is a section titled 'John Smith Route to 192.198.17.80' showing a hop-by-hop network path diagram. The path starts at 'John's MacBook' (Source) and goes through 'John's wifi' (Local Wifi), 'Verizon' (ISP), 'N. Virginia' (Pop Location), 'London' (Pop Location), and 'EU Center' (Connector Zone). Latency values are shown between hops: 100 ms between Source and Local Wifi, 10 ms between Local Wifi and ISP, 17 ms between ISP and Pop Location, 20 ms between Pop Location and Pop Location, and 35 ms between Pop Location and Connector Zone. A 'Wifi Signal: Low #1 2.4GHz' warning is displayed below the Local Wifi hop.

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..	10.1203.241	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

Source: John's MacBook (100 ms) → Local Wifi: John's wifi (10 ms) → ISP: Verizon (17 ms) → Pop Location: N. Virginia (20 ms) → Pop Location: London (35 ms) → Connector Zone: EU Center

Wifi Signal: Low #1 2.4GHz

# Unified visibility across every business resource

Demo
Apply Changes
chris@axissecurity.com

Insights
Policy
Settings
Experience

## Exploration

Last 7 days Filters [ ]

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		eufa-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	/loydsbanking.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		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	GET	mail.google.com	/mail/u/0/	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	GET	chat.google.com	/serviceworker.js	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Mark Santino	POST	chat.google.com	/u/0/webchanne..	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	GET	clients6.google.com	/drives/v2/interna...	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	POST	chat.google.com	/u/0/webchanne..	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	OPTIONS	clients6.google.com	/drives/v2/interna...	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	POST	mail.google.com	/mail/u/0/	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	POST	contacts.google.com	/SocialPeopleL...	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:52	View	Justin David Brio.	POST	mail.google.com	/cloudsearch/req...	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
03/10/23 13:10:51	View	Justin David Brio.	POST	contacts.google.com	/SocialPeopleL...	200	Success		HTTPS	443		Web-based Email	24.62.133.115	United States		Agent	Google Mail - Gmail
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	ge-loc.apple.com	/colls/wloc	200	Success										

Insights
Policy
Settings
Experience
Support

Demo
Pending changes
Admin123

## Activity Exploration

Last 30 Minutes Filters Clear All Filters

John Smith x Jira x

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	Cor
01-12-22 08:08:43	View	John Smith	atlassian.net	/download-files-portal	Success	Jira	
01-12-22 08:08:36	View	John Smith	atlassian.net	/page-does-not-exist	Error	Jira	Cor
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

### Operation System

- Windows (80%)
- iOS (10%)

### Event Type

- Page View (25%)
- File Upload (27%)
- Login (28%)
- File Download (20%)

### Status

- Success (85%)
- Error (2%)
- Block (13%)



# One policy to easily control access to all apps

- Insights
- Policy**
- Settings
- Experience

## Policy

Filter..

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

New Rule

Priority	Enabled	Name	Users	Context	Destinations	Action	Profiles
1	<input checked="" type="checkbox"/>	SSH internal	Daniel Reisel	Any	Any Application	Allow	Default Profiles
2	<input checked="" type="checkbox"/>	High Risk Nations	Any	<ul style="list-style-type: none"><li>Iraq</li><li>Russia</li><li>North Korea</li></ul>	Any Application	Block	Default Profiles
3	<input checked="" type="checkbox"/>	Block Malware, Gambling, Dropbox Uploads	All Full Time Employees...	<ul style="list-style-type: none"><li>Windows Baseline</li><li>Mac Baseline</li></ul>	<ul style="list-style-type: none"><li>DropBox - Managed</li><li>Box Managed</li><li>Pornography and Adult</li><li>Malware Sites</li><li>Gambling</li></ul>	Block	Client SSL Inspection And 5 Default Profiles
4	<input checked="" type="checkbox"/>	All Employees - Managed Devices	All Full Time Employees...	<ul style="list-style-type: none"><li>Windows Baseline</li><li>Mac Baseline</li><li>iOS Device Posture</li></ul>	<ul style="list-style-type: none"><li>Salesforce</li><li>All Employee Apps</li><li>VOIP</li><li>SSL Exclusion Category</li></ul>	Allow	Default Profiles
5	<input checked="" type="checkbox"/>	All Employees - BYOD	All Full Time Employees...	Any	<ul style="list-style-type: none"><li>All Employee Apps</li><li>SSL Exclusion Category</li></ul>	Allow	BYOD Policy And 5 Default Profiles
6	<input checked="" type="checkbox"/>	Accounting Team - Accounting Apps	Accounting	Any	Accounting Apps	Allow	Default Profiles
7	<input checked="" type="checkbox"/>	HR Team - HR Apps	Human Resources	<ul style="list-style-type: none"><li>Windows 10 + patches</li><li>Crowdstrike Enabled</li></ul>	HR Apps	Allow	Default Profiles
8	<input checked="" type="checkbox"/>	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	Allow	Contractors RDR Profile

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

Policy ID	Policy Name	Target	App	Access	Profiles
5	All Employees - BYOD	All Full Time Employees...	All Employee Apps SSL Exclusion Category	Allow	BYOD Policy And 5 Default Profiles
6	Accounting Team - Accounting Apps	Accounting	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	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	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...	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 Application	Block	Default Profiles
Default	Web Traffic Default Rule	Any	Web Traffic	Allow	Client SSL Inspection And 5 Default Profiles

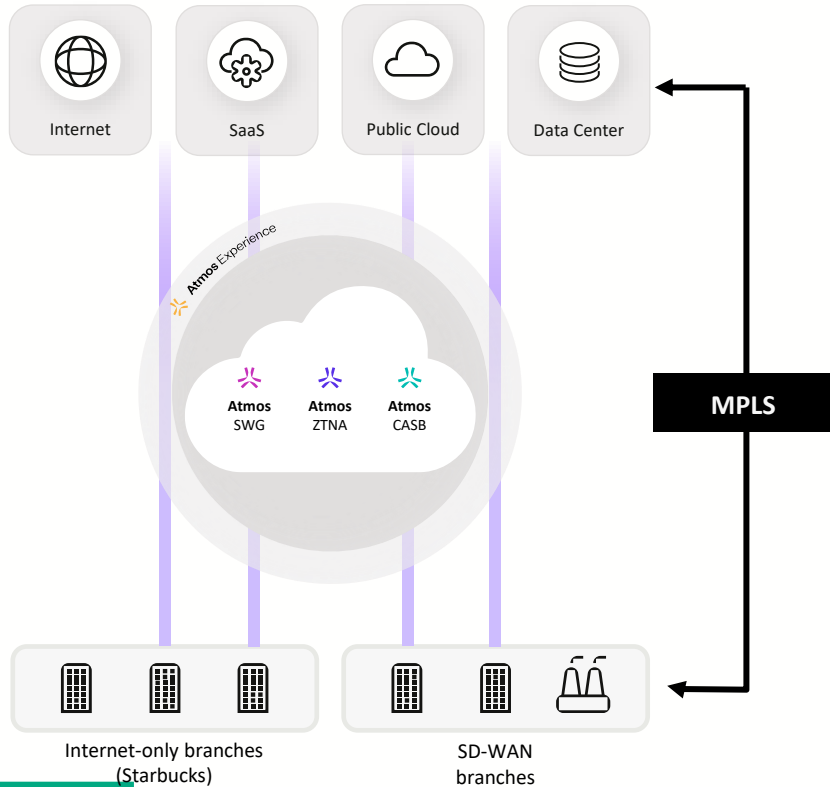
Securely enable developer workflows

Support



# Secure branch connectivity

Internet WAN + SD-WAN



Reduce costs and complexity at branch

Provide a fast, secure user experience

Support headless device traffic

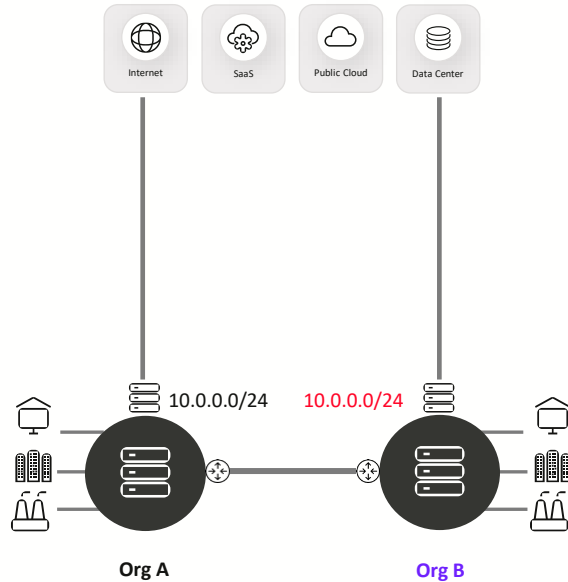
“By 2023, to deliver flexible, cost-effective scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020.”

**Gartner**



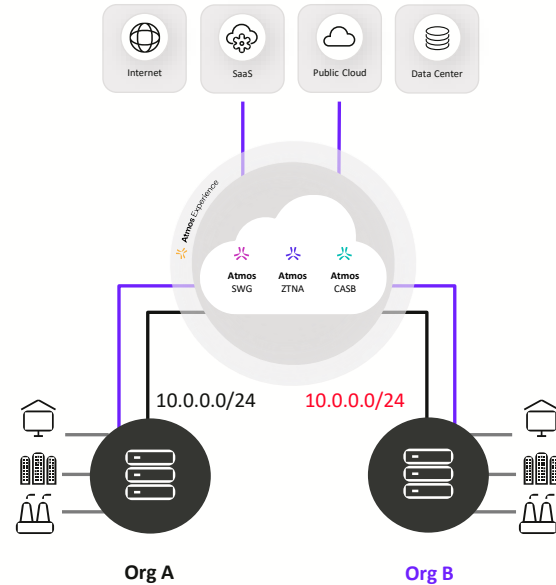
# Accelerate M&A and divestitures

## 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



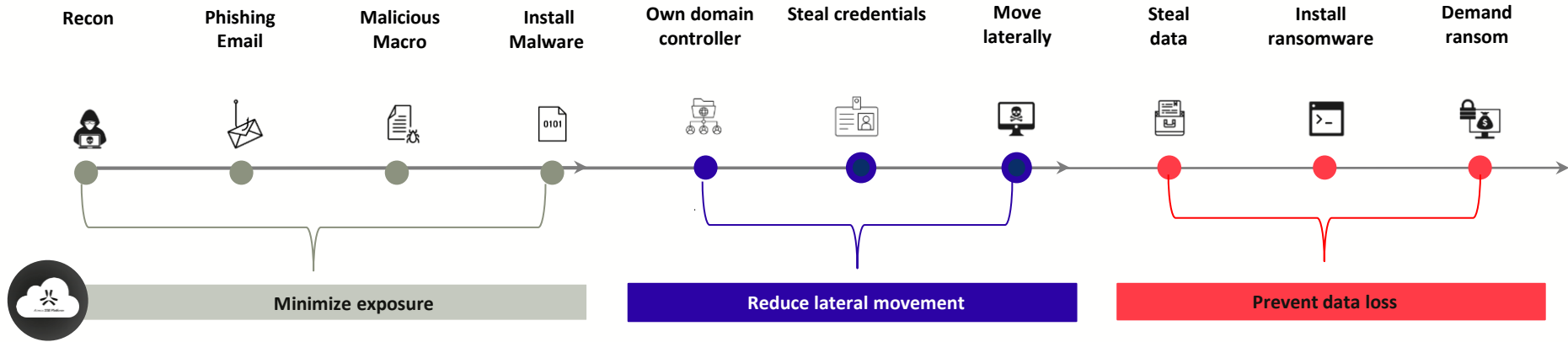
- Networks left as is, no need to consolidate
- Standardized security across both companies
- Users have direct-to-app access w/o network access

# 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
Agentless Web Application Rewrite Engine	X		
<b>Security</b>			
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