

# SSR appliance portfolio



**SSR100** series for small to medium branches

**SSR400** series for small to medium branches

**SSR1000** series for large branch, campus or datacenter deployments



SSR120



SSR400



SSR1200



SSR1400



SSR130



SSR440



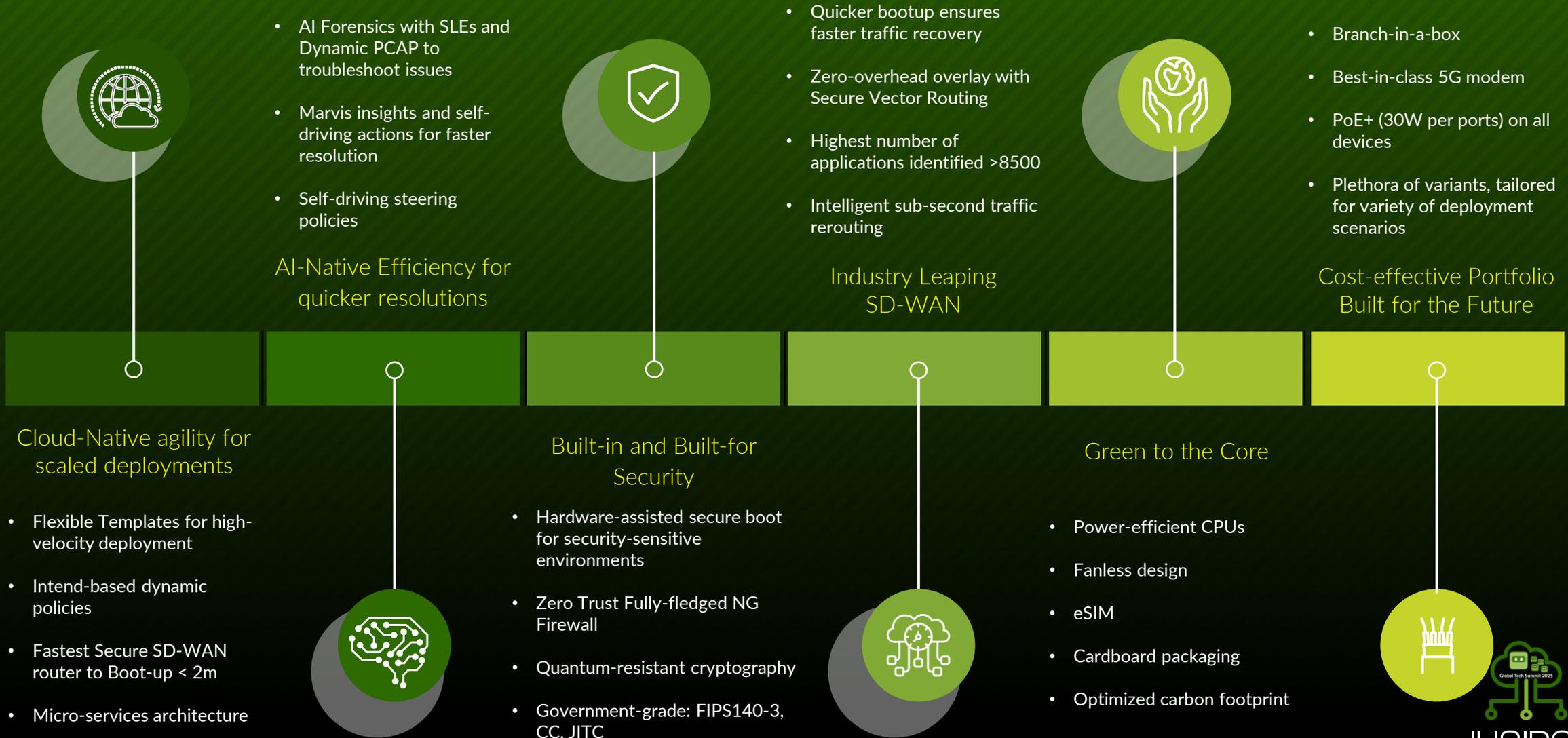
SSR1300



SSR1500

# AI-Native, Cloud-Native, Secure SD-WAN

## SSR400 Series SD-WAN Routers for Full-stack Enterprises



# SSR400 Line



# Flexible Templates

## What is it?

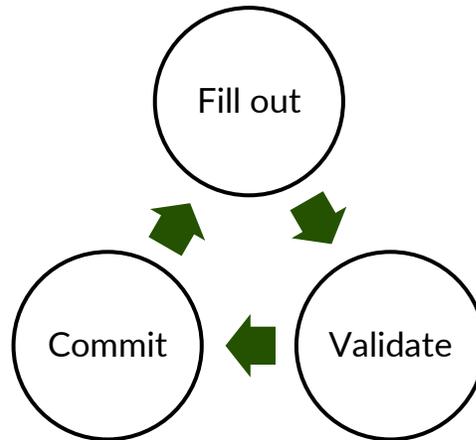
- Standardized configurations for high-velocity deployment
- Intent-based dynamic policies
- Enables automated Zero-Touch Provisioning (ZTP)

### Adjust Templates



Templatized deployment  
Parameterized template

### Push!

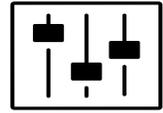


Deploying to production is a clear process

### Ship!



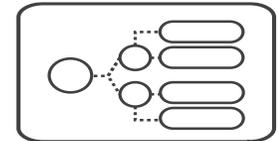
Zero Touch Provisioning.  
Plug & Play



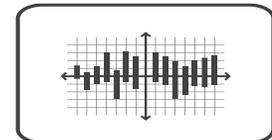
Simplify roll out



Fast turn up



Validate Deployment



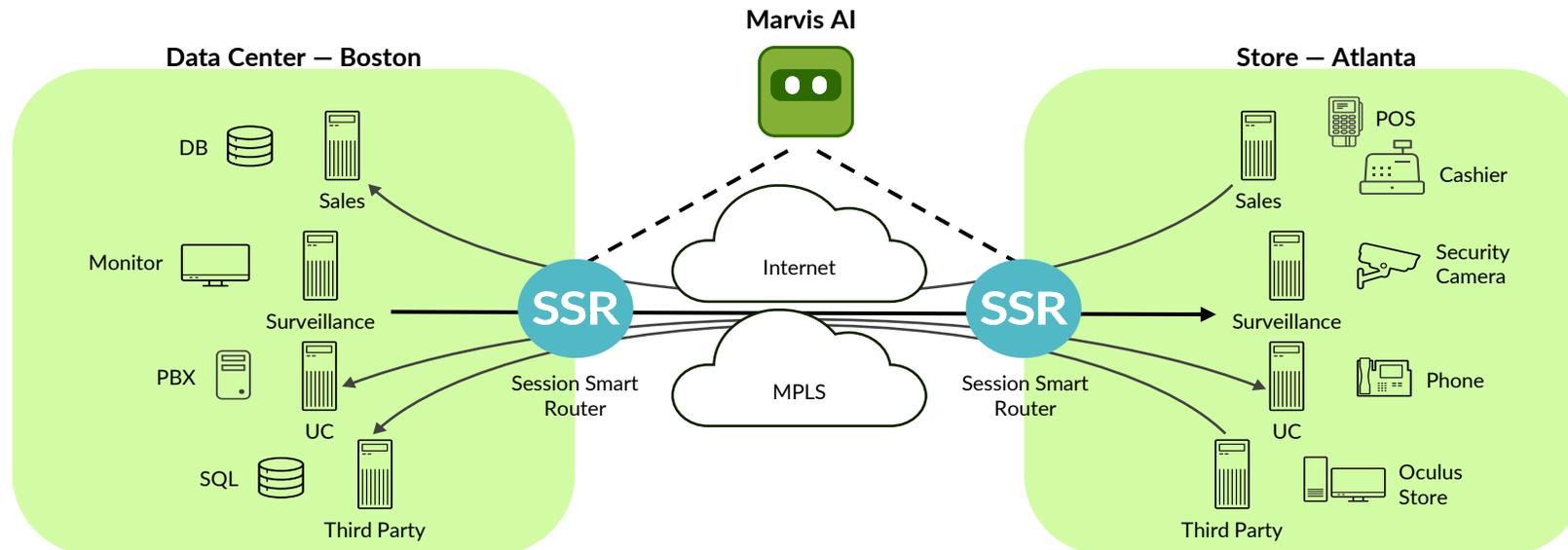
DevOps Automation



# Intent-based dynamic policies

## What is it?

- "Intent-based" means defining what the network should achieve (the desired business outcome) rather than manually configuring how it should achieve it.
- Define desired business outcomes, not complex configurations
- Network automatically configures and adapts in real-time
- Simplified management, always aligning with business goals



# Fast Boot-Up

## What is it?

- Fastest secure SD-WAN router to boot in under 2 minutes
- Minimizes downtime and ensures rapid recovery
- Enables high-velocity deployments with ZTP



# Micro-services Architecture

## What is it?

Mist's cloud-native, microservices architecture is a fundamental differentiator that delivers agility, scale, and resilience to your network.

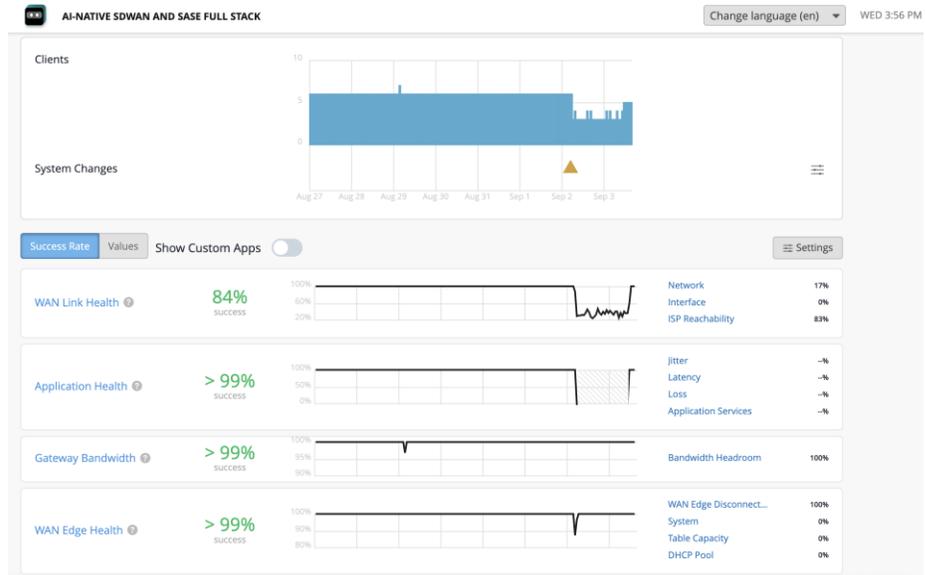
- Faster non-service affecting updates
- Unmatched resiliency and scale
- Greater agility and speed



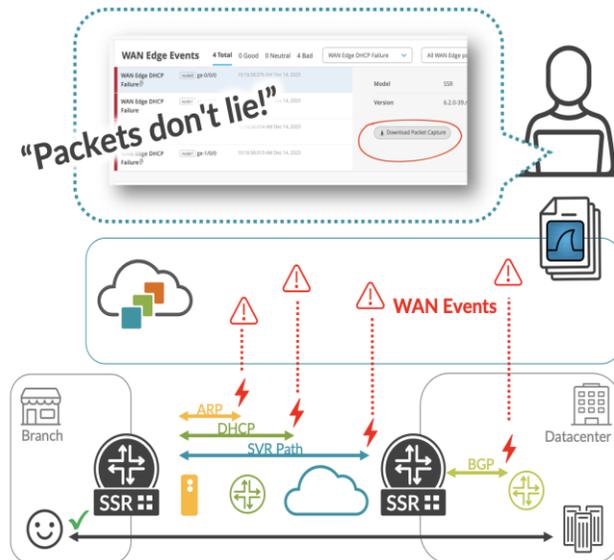
# AI Forensics

## What is it?

- AI-driven troubleshooting for proactive issue resolution
- Monitors Service Level Experiences (SLEs) to detect anomalies
- Automated root cause analysis
- Dynamic Packet Capture (PCAP) for on-demand forensics



## WAN Dynamic PCAP



**MARVIS**

troubleshoot teams calls from agrawalk-mbp

Troubleshooting Teams. Here is what I found on Oct 11th.

- Teams Call 12:02 PM – 12:26 PM on Oct 11th
- Teams Call 10:27 AM – 10:50 AM on Oct 11th
- Teams Call 10:00 AM – 10:29 AM on Oct 11th
- Teams Call 9:09 AM – 9:29 AM on Oct 11th

Troubleshoot application Teams

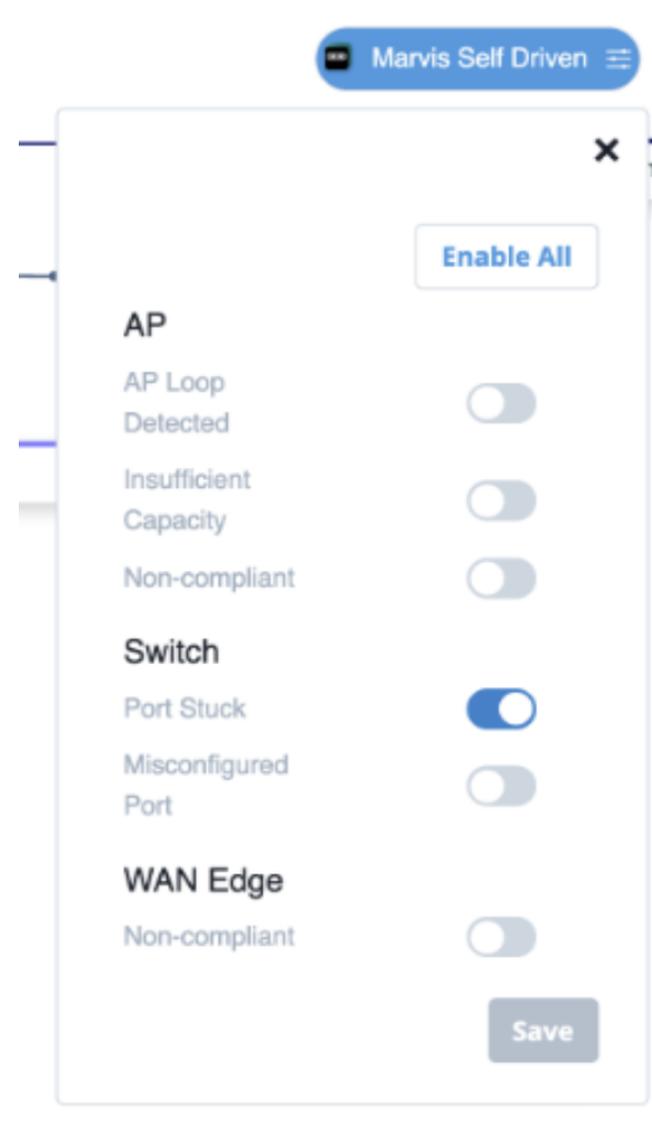
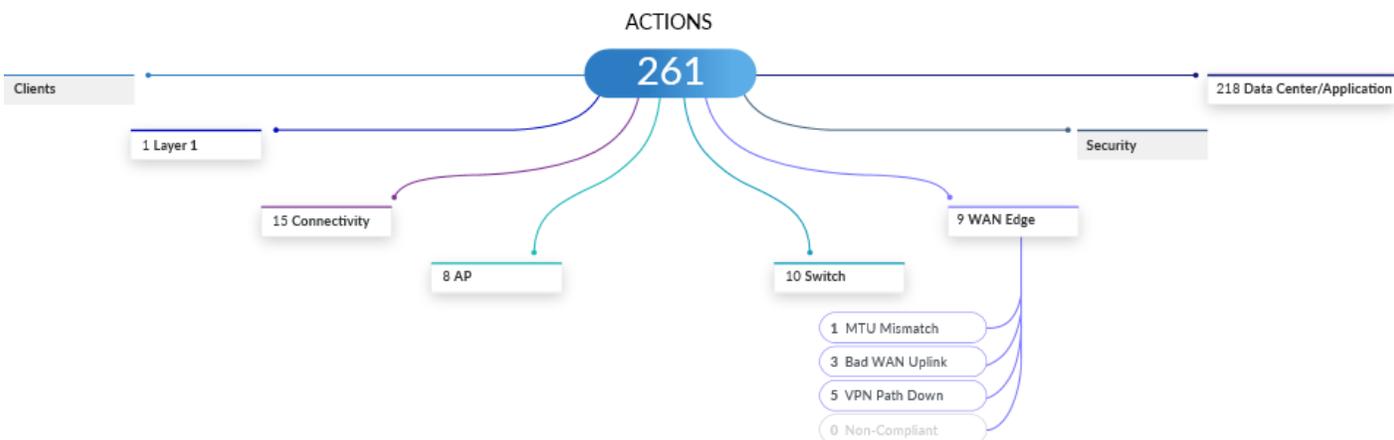
**Network Health**  
Teams call on agrawalk-mbp from 6:09 AM – 6:29 AM on Oct 11th

Network Health diagram showing connections between agrawalk-mbp, BASEMENT, Teams Server, kaushik-headend, and office.

# Marvis Insights and Self-Driving Actions

## What is it?

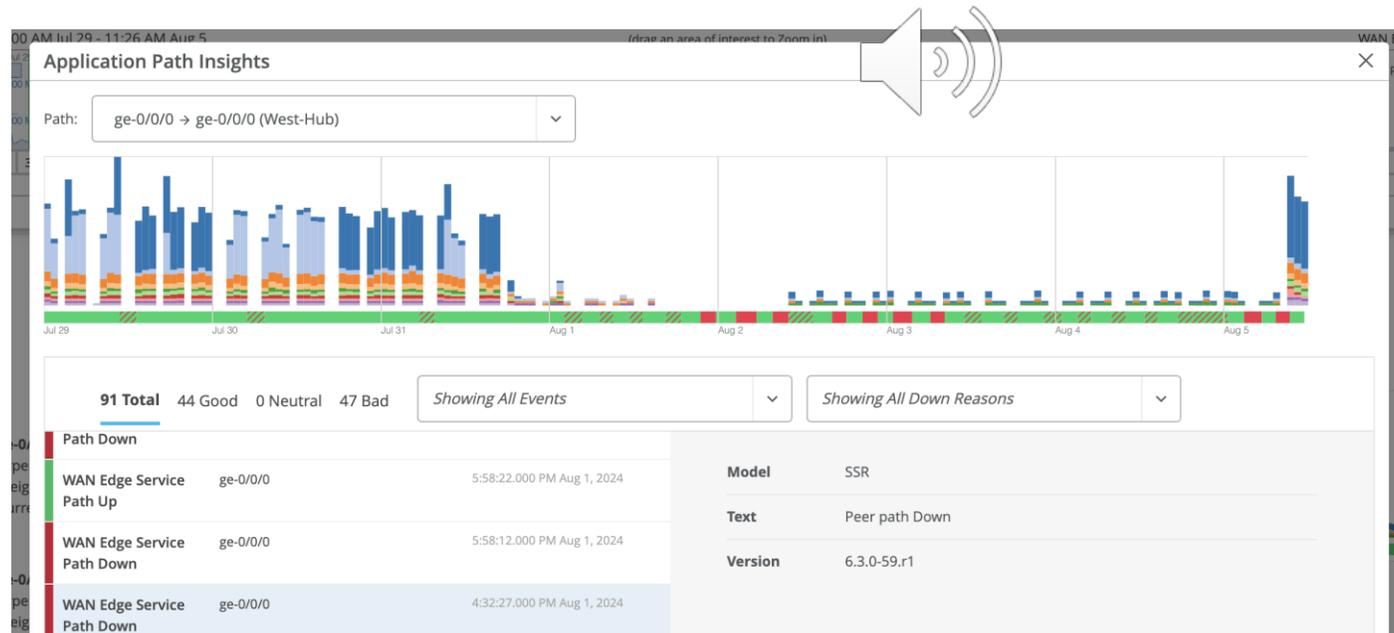
- AI-driven insights for clear recommendations
- Proactive identification of network issues
- Automated self-driving actions for rapid resolution
- Minimizes manual intervention and accelerates MTTR



# Self-Driving Steering Policies

## What is it?

- Real-time, dynamic traffic optimization
- Application-aware path steering
- Automated sub-second traffic rerouting for resilience
- Identifies unused policies for security optimization



## Application Path Insights

### Policies

Corp-User-Internet

### Active

Corp-User-Internet

M365

IoT

### Inactive

Guest-Breakout

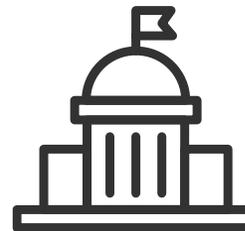
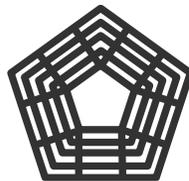
Zoom

Corp-User-LAN

# Hardware-Assisted Secure Boot

## What is it?

- Hardware-assisted Secure Boot is a hardware-rooted security mechanism that cryptographically verifies the integrity of the device's software during the boot process to prevent malicious tampering
- Ensures the authenticity of software from power-on
- Protects against tampered firmware and malicious code
- Establishes a hardware-rooted chain of trust for security-sensitive environments
- Ideal for security-conscious customers in highly regulated industries, such as government, defense, and finance, who require the highest level of assurance against malicious code and physical tampering.



# Zero Trust Fully-Fledged NGFW

## Session Smart Routing Security

- ✓ Deny by Default/ Zero Trust Model.
- ✓ Adaptive Encryption.
- ✓ Route Directionality, Policy Enforcement.
- ✓ Layer 3/Layer 4 DOS/DDOS.
- ✓ FIPS 140-3, CC, JITC Certified.
- ✓ Fine-grained segmentation.
- ✓ Centralized policy management.
- ✓ Quantum-Resistant Cryptography



## Advanced Security Pack

- ✓ IPS/IDS
- ✓ URL Filtering
- ✓ Anti-Virus
- ✓ Advanced Threat Prevention
- ✓ SSL Proxy
- ✓ DNS Security
- ✓ Security Assurance Dashboard

## Secure Edge Connectors to connect to any SSE

- ✓ Juniper Secure Edge
- ✓ ZScaler
- ✓ Axis Security
- ✓ Any 3rd Party SSE



# Quantum-Resistant Cryptography

## What is it?

- Quantum-resistant cryptography is a type of encryption designed to protect against the threat of future quantum computers, which are capable of breaking current cryptographic standards
- Proactive protection against future quantum attacks
- Protects against "harvest now, decrypt later" threats
- Ensures long-term data confidentiality for security-sensitive organizations
- Meets government and enterprise needs



# Government-grade: FIPS140-3, CC, JITC Certified

## What is it?

- **FIPS 140-3** is a U.S. government standard that validates the security of cryptographic modules used to protect sensitive data.
- **Common Criteria** is an international standard for evaluating the security of IT products, providing a globally recognized framework for independent third-party testing.
- **JITC** certification is a U.S. Department of Defense (DoD) process that validates and certifies information technology products for security, interoperability, and performance to ensure they can operate effectively within military networks.
- Customers in **government, defense, and other highly regulated industries** require these certifications to prove that the product meets stringent security, interoperability, and performance standards for use in their mission-critical and compliance-driven environments.



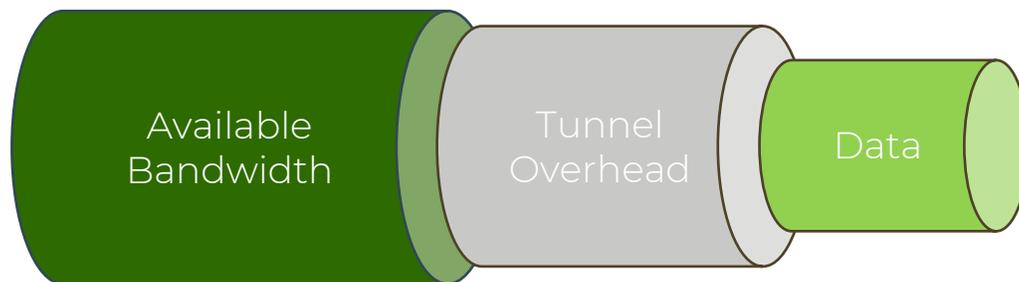
# Zero-Overhead Overlay with Secure Vector Routing

## What is it?

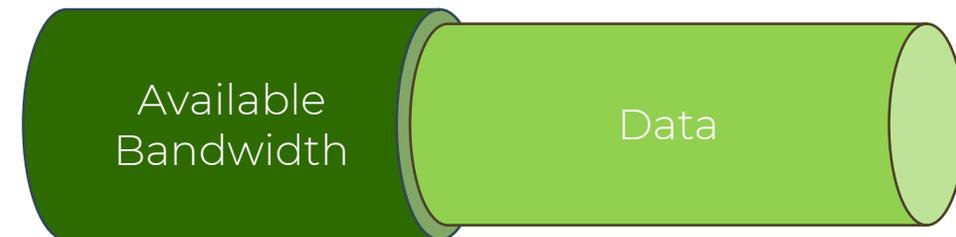
- **Secure Vector Routing (SVR)** is a technology that creates a secure, policy-driven network fabric without the performance overhead of traditional tunneling protocols, enabling efficient, end-to-end traffic steering.
- Secure, zero-overhead SD-WAN overlay
- Maximizes throughput and reduces latency
- Efficiently routes traffic without tunnels
- Reduces CPU and bandwidth consumption

- Minimal impact to available bandwidth
- Recover 30%-50% overhead
- Optimized adjacency management
- Distributed Analytics post-processed and accessed on-demand

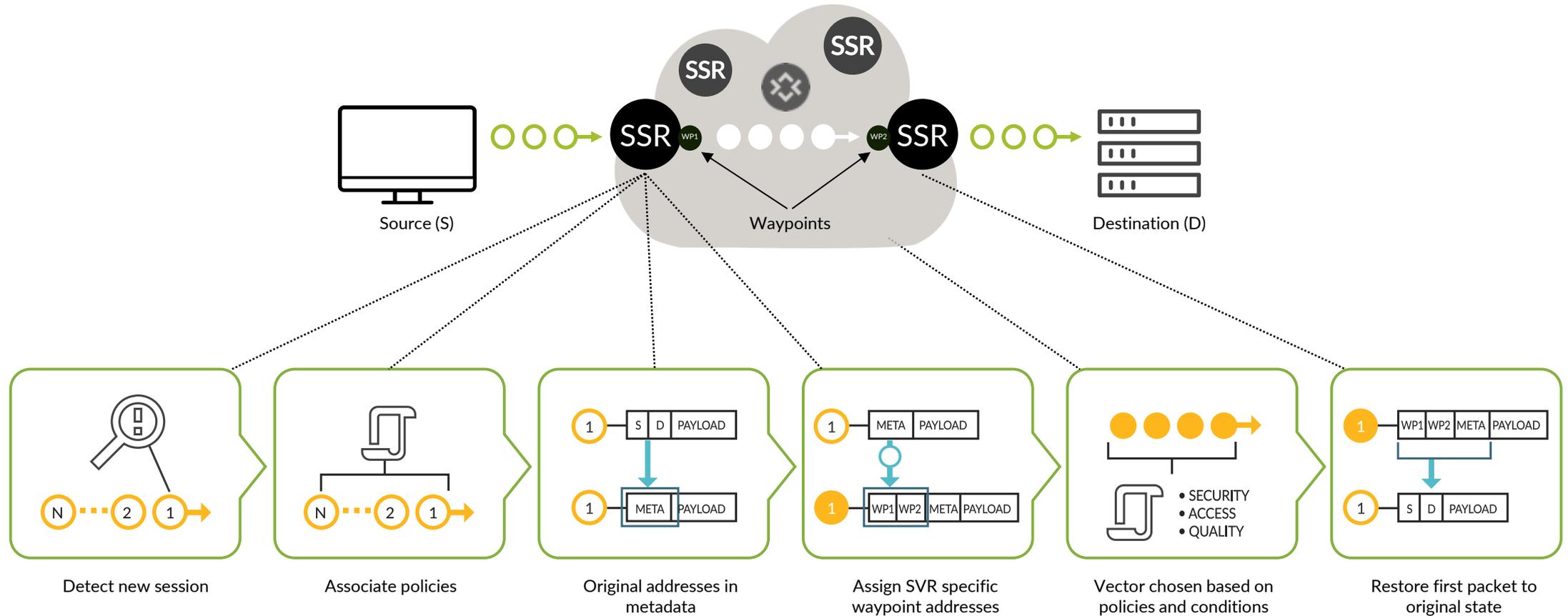
## Traditional Tunnel Burden



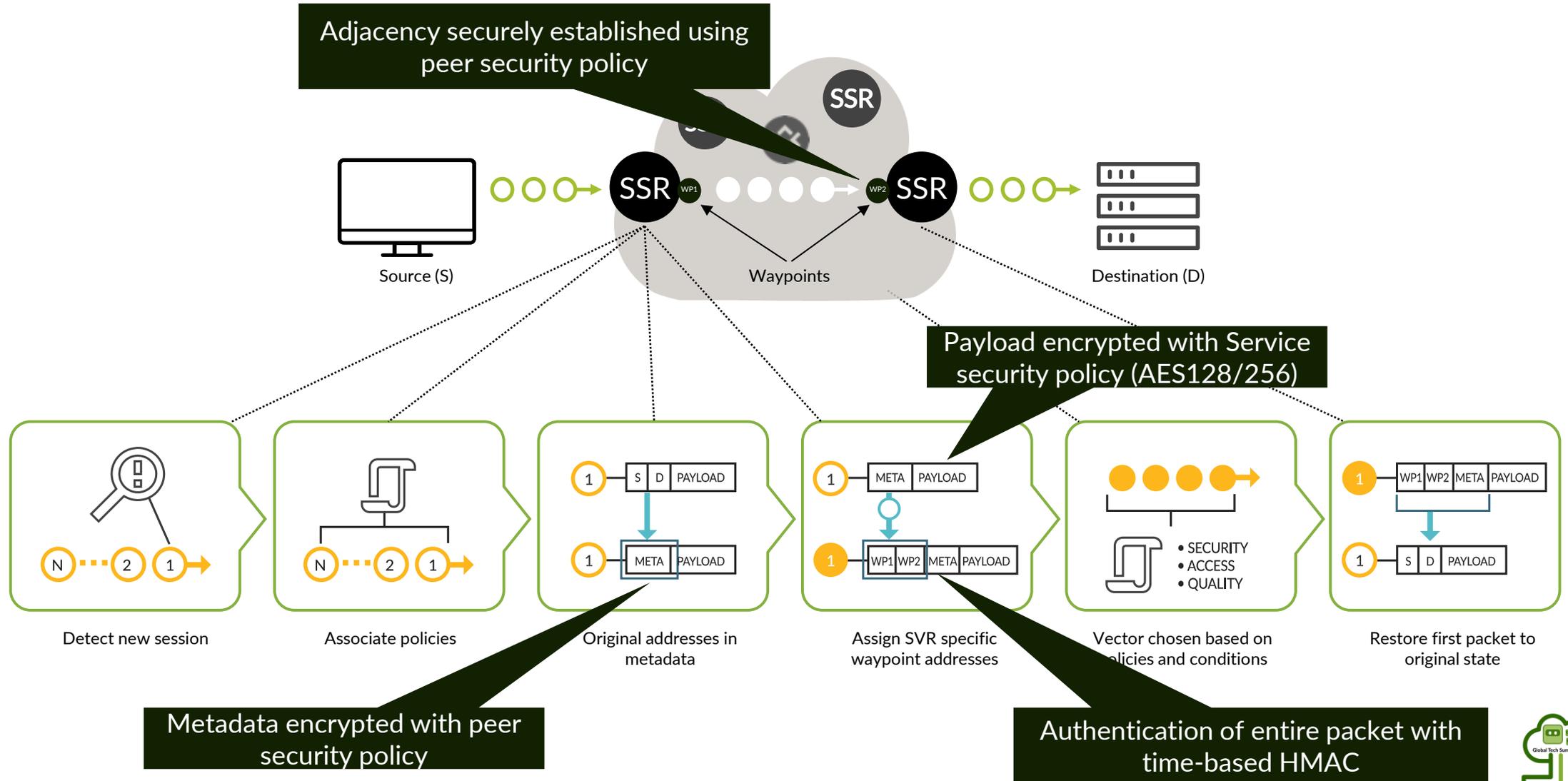
## Efficient Bandwidth Utilization with SVR



# Secure Vector Routing



# SVR Encryption and Authentication



# Positioning Secure Vector Routing (SVR)

## Positioning

- Fundamentally simpler
- Faster and more reliable
- Inherently more secure

## Questions to Discover Opportunities:

- "What kind of performance issues do your remote users or branch employees report with critical applications like voice, video, or SaaS apps?"
- "Tell me about your current branch hardware. How many different devices do you have to manage at each site?"
- "How are you currently securing your branch traffic? Do you have a separate security appliance, or is it a shared function?"

# Highest Number of Applications Identified Over 8500!

## What is it?

- Provides superior application visibility (>8500 apps) – more than double our competitors!
- Enables granular control and policy enforcement
- Guarantees a superior application experience
- Improves security posture by controlling all traffic



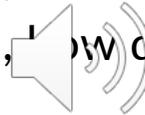
# Positioning Application Identification

## Positioning

- Superior application experience
- Granular Security and control
- Actionable insights

## Questions to Discover Opportunities:

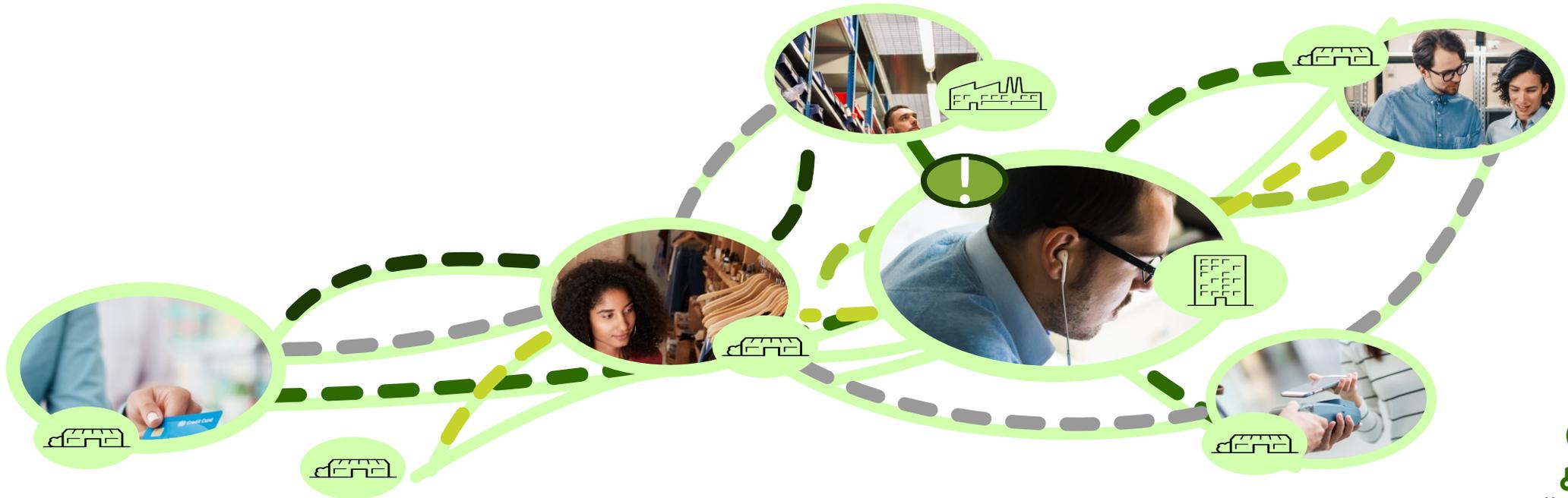
- "When users complain about a slow application, how do you currently identify what's causing the problem?"
- "What is your biggest concern about 'shadow IT' or unauthorized applications running on your network?"
- "How do you currently prioritize traffic for critical applications like video conferencing or a CRM system?"



# Intelligent Sub-Second Traffic Rerouting

## What is it?

- Proactive, intelligent traffic rerouting
- Sub-second recovery with no tunnel overhead
- Real-time path monitoring to prevent application disruptions
- Ensures a superior, uninterrupted application experience



Power efficient CPUs for decreased power consumption and optimized energy footprint

5G modem with eSIM and single world-wide SKU, Band 14 for FirstNet

Single or dual power input

Cloud LED with MIST color codes

QR code and out-of-the box ZTP for superior user experience



MACSEC on all ports

Fanless design for quiet operations and improved reliability

Future-proof USB-C ports (both console and storage)

PoE+ w/ 30W per port for all SKUs

Kensington lock for secure installation

# Who cares about this?

- Customers with strong Environmental, Social, and Governance (ESG) initiatives
- Customers with with massive scale where small efficiencies lead to significant savings

## Power-Efficient CPU & Fanless Design:

**Problem Solved:** High energy costs, cooling expenses, and a large carbon footprint. Fanless design also solves noise and maintenance issues.

**Customers:** Retail Chains, Healthcare Clinics, Government & Public Sector:

## eSIM & Cardboard Packaging:

**Problem Solved:** Logistical complexity of shipping, managing, and provisioning thousands of physical SIM cards and dealing with massive amounts of plastic waste.

**Customers:** Managed Service Providers (MSPs), Large-Scale Franchises

## Future-Proofed USB-C Ports:

**Problem Solved:** The lack of a standardized port for power and data on devices. This eliminates the need for different adapters and makes the SSR 400 a universal hub for modern peripherals and IoT devices.

**Customers:** Tech-Forward Enterprises, Temporary or Mobile Businesses

## MACsec on all Ports:

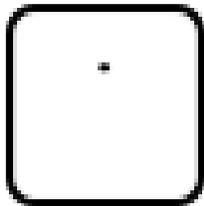
**Problem Solved:** Securing data traffic on the physical local area network (LAN) from physical snooping or man-in-the-middle attacks.

**Customers:** Financial Institutions, Government & Defense Contractors, Healthcare

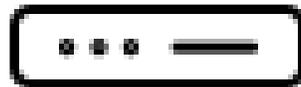
# Branch-in-a-Box

## What is it?

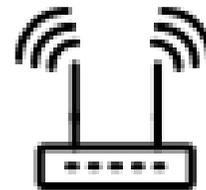
- **"Branch-in-a-Box"** is a solution that consolidates all the critical networking functions for a branch office - including WiFi, switching, SD-WAN, and security - into a single, easy-to-manage device.
- All-in-One Consolidation
- Integrated Connectivity
- Simplified Deployment
- Lower TCO



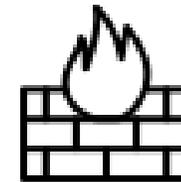
APs



Switches



Routers

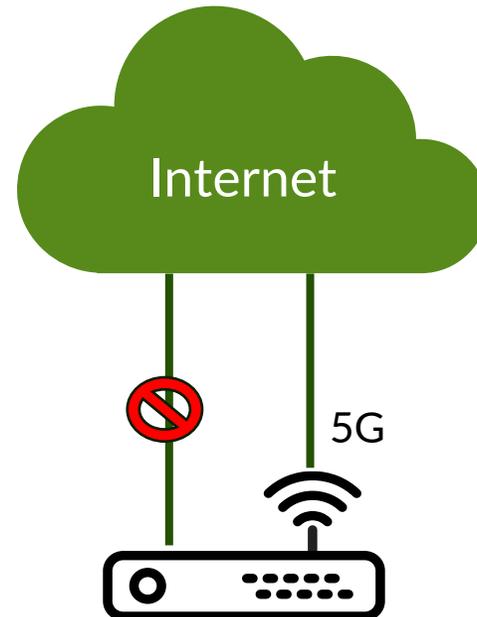


Firewalls

# Best-in-class 5G modem

## What is it?

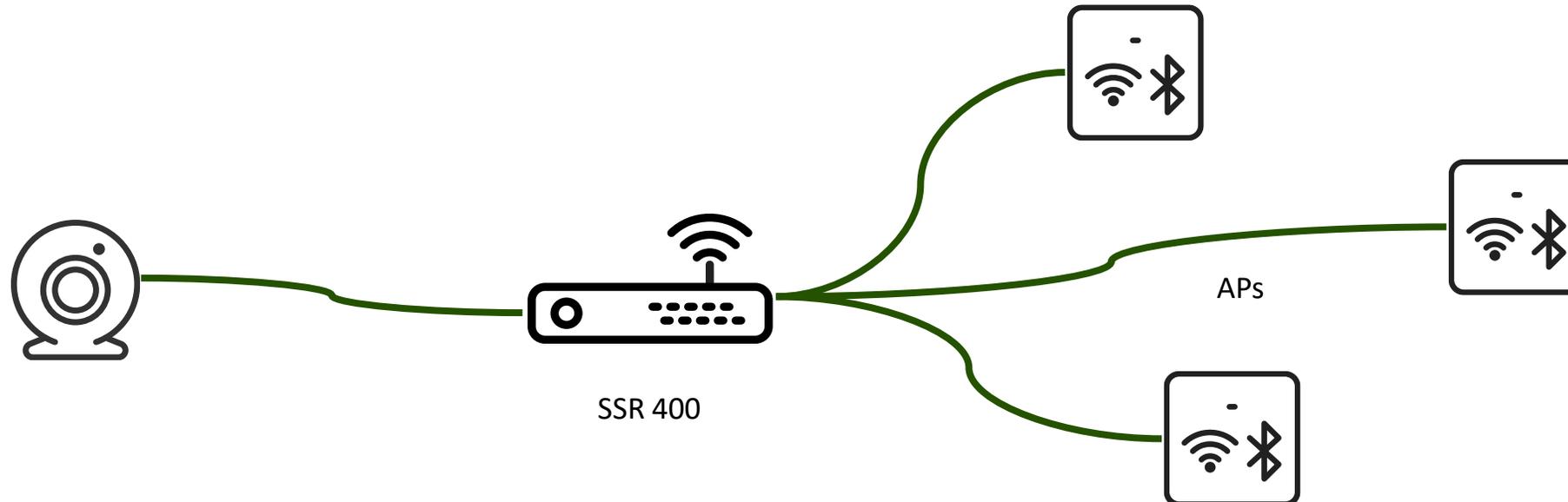
- All-in-one "Branch-in-a-Box" solution
- Integrated 5G for fast, reliable wireless WAN
- Eliminates need for separate modem and wiring
- Provides rapid failover for business continuity
  
- FirstNet
- Private LTE
- Private 5G



# PoE+

## What is it?

- Provides integrated PoE+ on all ports
- Eliminates need for separate power outlets and switches
- Simplifies branch wiring and reduces hardware sprawl
- Enables flexible device placement



# Plethora of Variants

## What is it?

- Wide variety of hardware variants
- Integrated WiFi
- Integrated 5G modem
- Ensures a perfect fit for every branch



# Product Line Variants



SSR400



SSR400-C



SSR400-W



SSR400-CW



SSR440



SSR440-C



# Product Line Variants – DUAL AC PSU



SSR440-2AC



SSR440-C-2AC



SSR440-RMK

# Value Proposition

Why are we delivering this feature?

- **IT Skills Gap and Branch Complexity**
  - “Branch in a Box” consolidation
  - AI-Native Management
  - Flexible Templates and ZTP
  - Microservices Architecture
- **High Costs and Inefficient Operations**
  - Reduced Hardware and Software Costs
  - Lower OpEx
  - Optimized WAN Utilization
  - Power-Efficient & Sustainable
- **Fragmented Security and an Expanding Attack Surface**
  - Native Zero Trust SD-WAN
  - Proactive Threat Protection
  - Policy Optimization
- **Poor Application Performance and User Complaints**
  - Intelligent Traffic Steering
  - Highest Application Visibility
  - Rapid Recovery



# Primary Market Segments



## Full-stack Enterprises

- Full-stack focus
- Inject SSR in Wireless/Wired-and-Wireless existing customers



## Federal/Local Government

- Centralized management for air-gaped deployments
- Mist management for civil agencies



## (Managed) Service Providers

- Grow our footprint
- Mist management lowers TCO
- Get on portfolio/certified list