

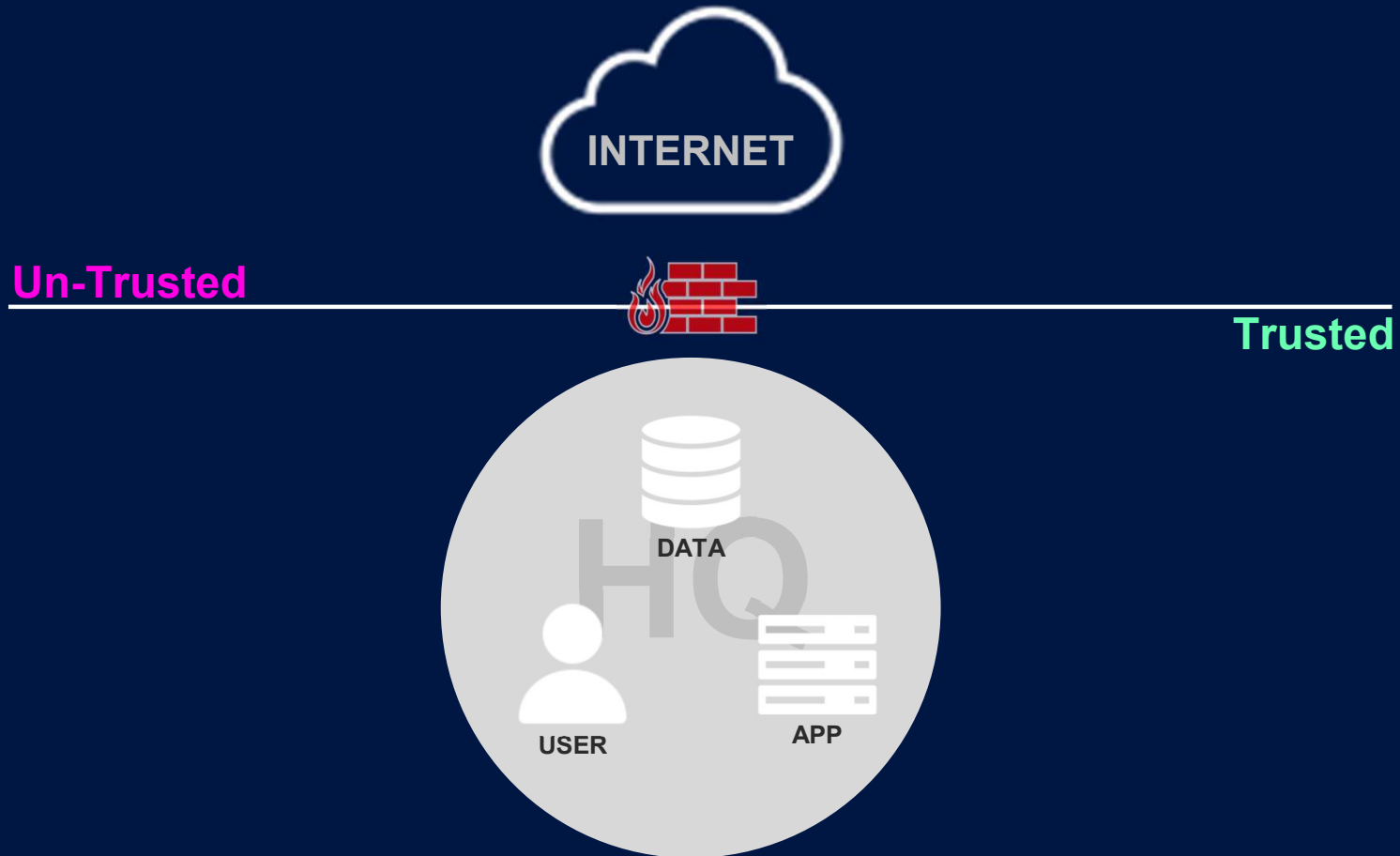
Evolution von Zscaler Private Access (ZPA):

Workload Segmentation, Branch
Connectivity, Microsegmentation

Matthias Mader, Solutions Consulting



Früher war alles einfacher

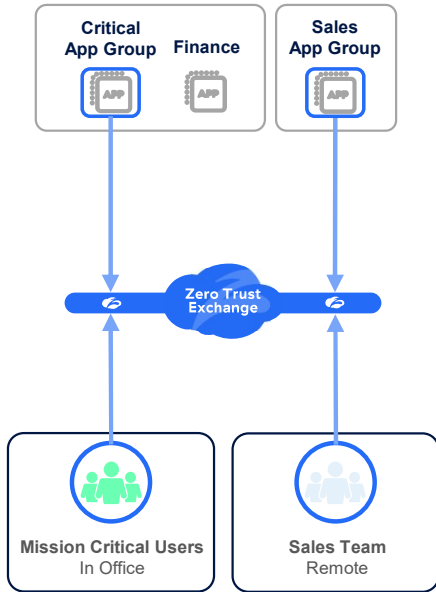


04

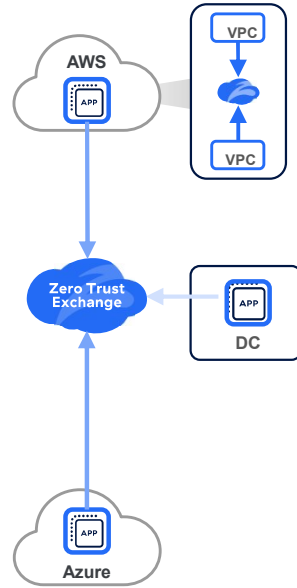
Areas of Zero Trust Segmentation



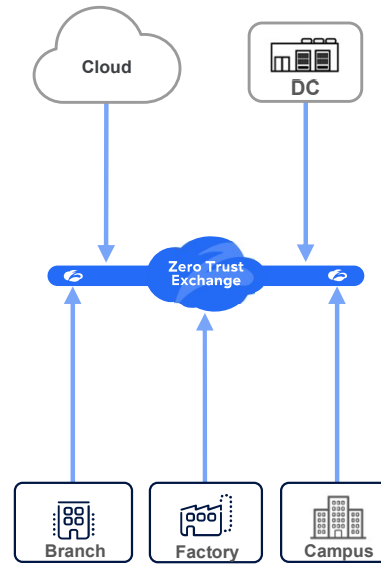
1 User Segmentation



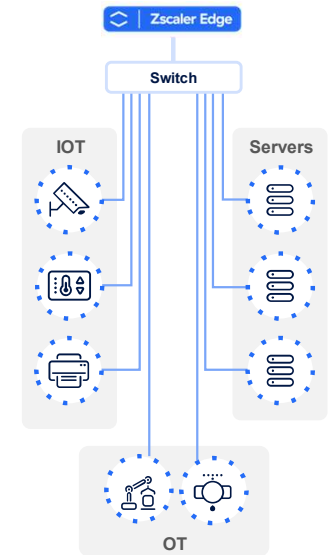
2 Workload Segmentation



3 Branch/Campus Segmentation



4 Device Segmentation



01



User Segmentation

Network segmentation complexity jeopardizes security



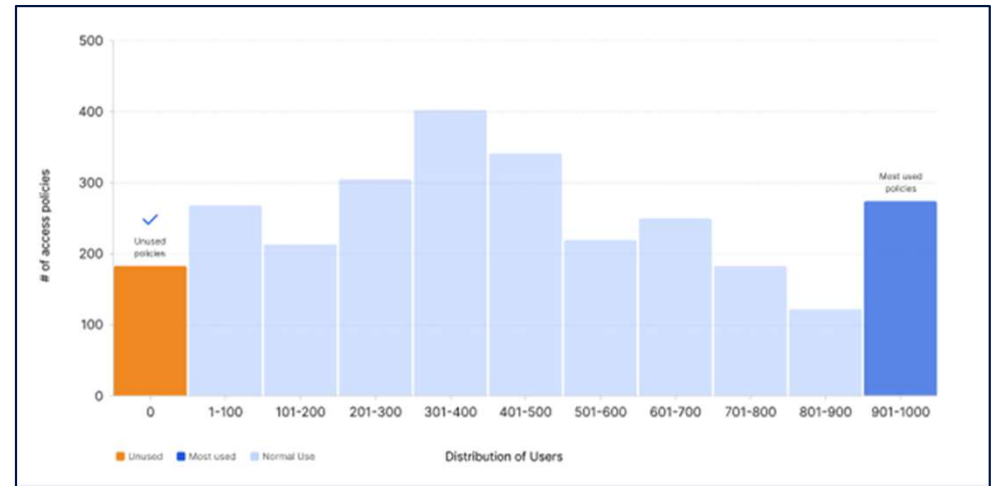
95% of security breaches are due to human error or inadequate access control measures*
53% of enterprises breached via VPN vulnerabilities say threat actors moved laterally**

VPN
<h2>Network Segmentation</h2> <ul style="list-style-type: none">• Manual, slow and complex policy configuration• Constant upkeep needed• Security gaps, further increased with third party access

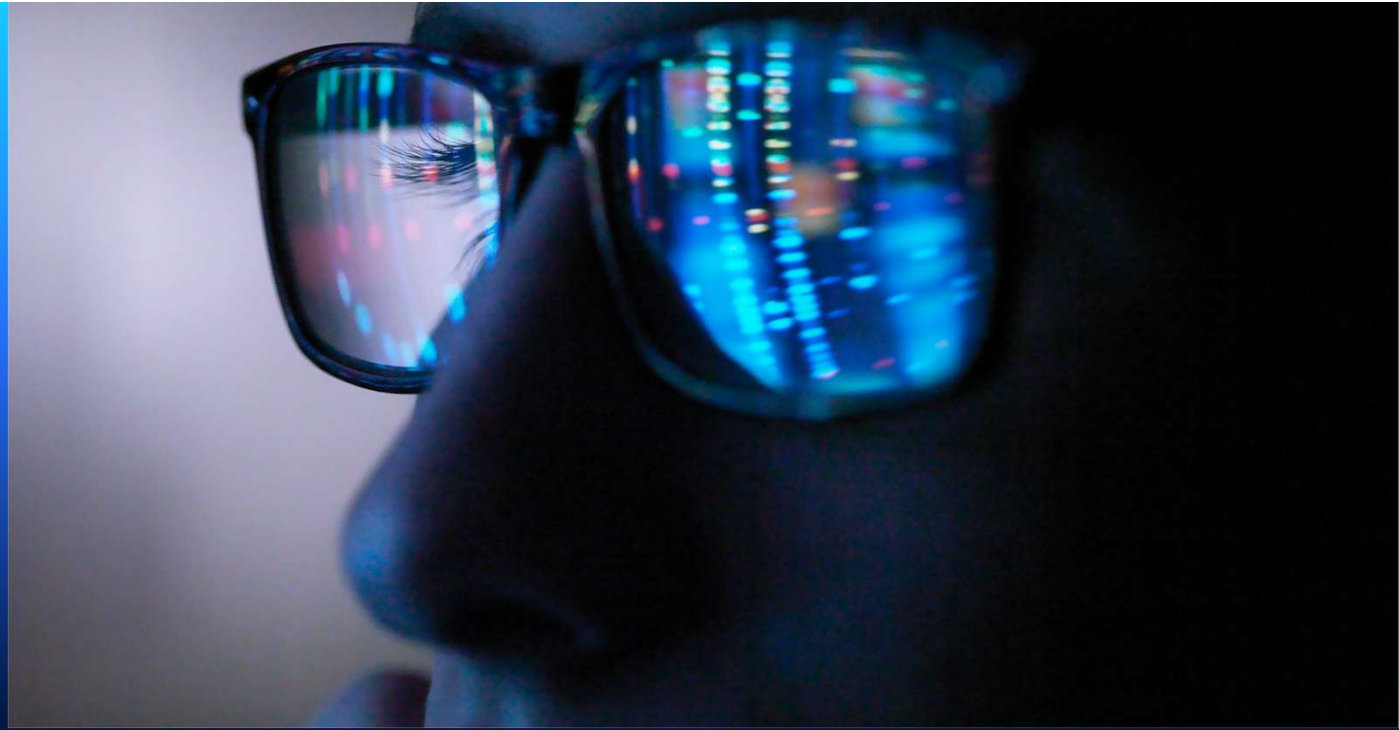
ZPA: User-to-App Segmentation	
<h2>Zero Trust User-to-App Segmentation</h2> <ul style="list-style-type: none">• Connect user to app without placing them on the network• App discovery• Application and User-focused granularity of segmentation	<h2>Introducing AI-powered Segmentation & Insights</h2> <ul style="list-style-type: none">• Analyzes application traffic to intelligently segment apps and recommend policies• Customer-preferred groupings• Optimized policy generation



*2023 State of Segmentation Akamai
** 2024 VPN Risk Report

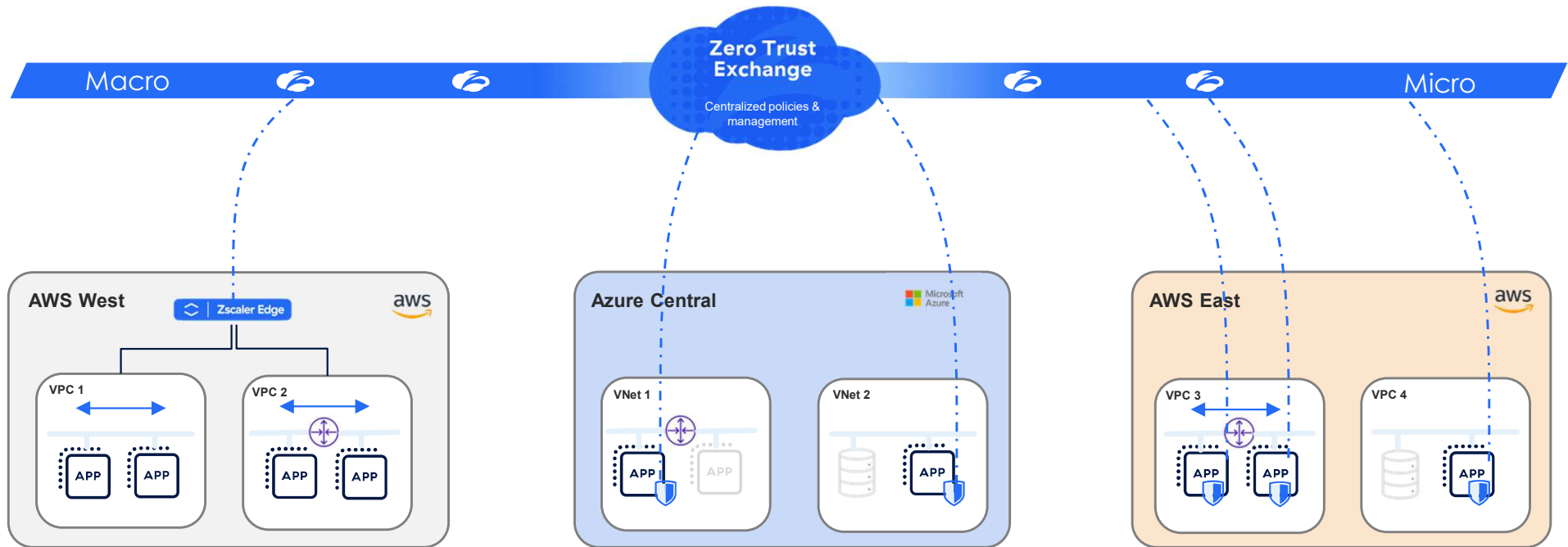


02



Workload Segmentation

Zero Trust Segmentation for Cloud Workload



Activity by Workload
Fingerprint, inventory by cloud-native attributes

Enforce by Workload
inter & intra subnet within VPC/VNET

Intelligence by Workload
Automated policy builder, ML-based analytics

03

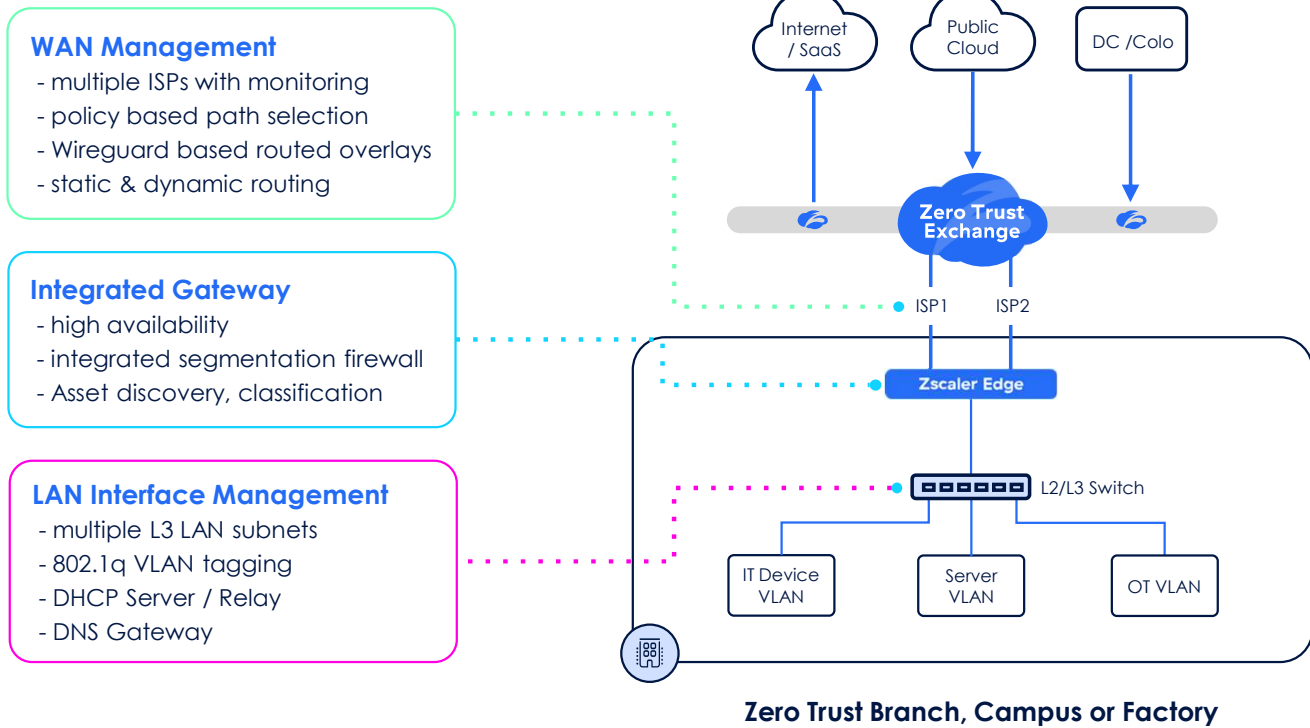


Branch/Campus
Segmentation

Secure External Branch & Factory Communications



Secure inbound and outbound connectivity — all you need is an ISP connection



Use Case

- ✓ Café like branches
- ✓ M&A Integration
- ✓ Full SDwan replacement
- ✓ China Connectivity (Users & Sites)

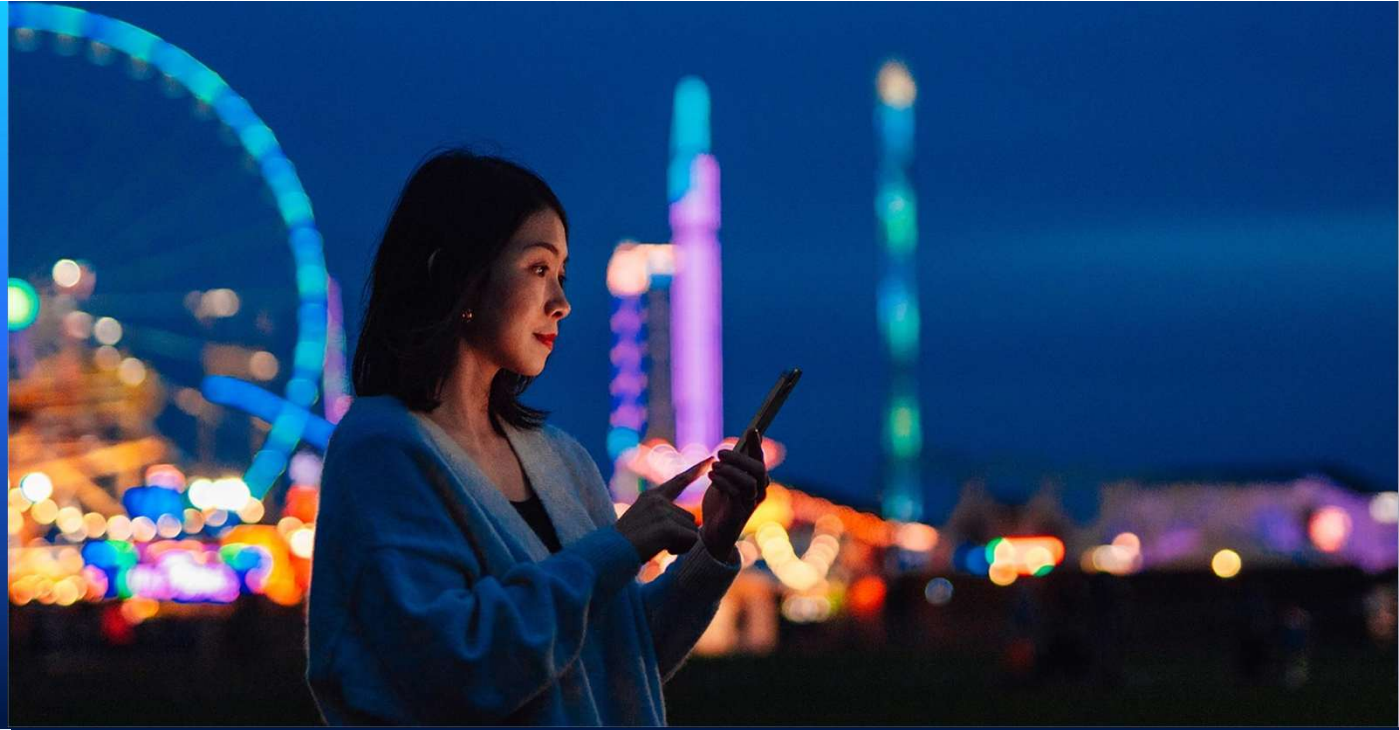
What Gets Eliminated

- ✗ **Networking**
- MPLS
- Traditional SD-WAN
- North – South Firewalls (VPN)

Benefits

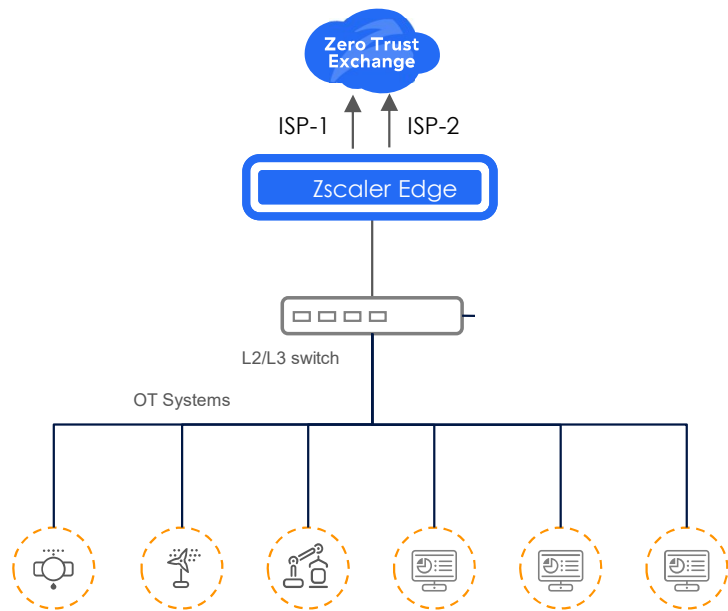
- ✓ No inbound IP ports exposed
- ✓ Reduced routed overlays, simplified connectivity and operations
- ✓ Built in Zero Trust; Lateral threat movement prevention

04



Device Segmentation

Zero Trust Branch with Device Segmentation



Use Key Value

- All-in-one appliance
- eliminate firewall, NAC, SDWAN
- Built with Zero Trust principals
- Simplified network, reduces the operation
- Cafe' like Branches

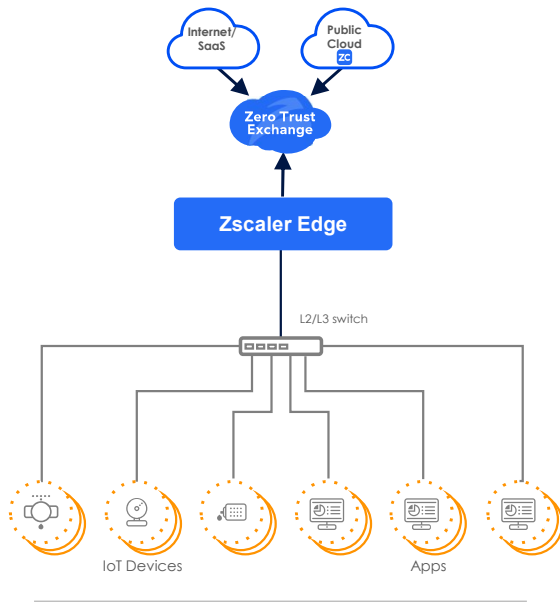
What we eliminate

Branch Appliances		Security Appliances	
	SDWAN		Agents
	NAC appliances		Firewall

Key Use Cases

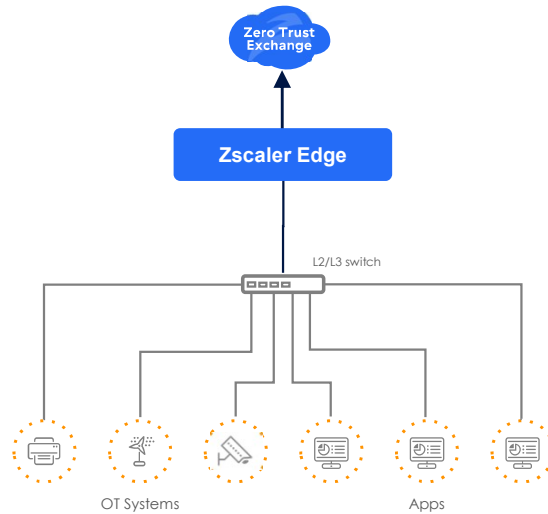


Secure External Communication



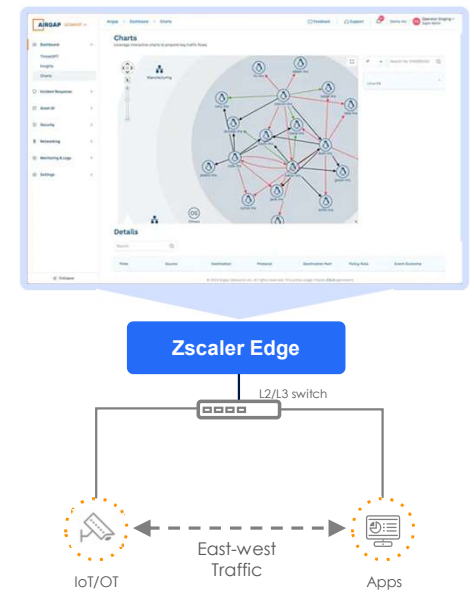
No firewalls, VPNs or route tables to manage
Eliminate lateral movement and attack surface
No route table propagation, overlapping IP okay

Secure Internal Communication



Ring Fence every endpoint in a network of "1"
Automatic isolation of unknown MAC addresses
Integrates with asset management systems

Gain Asset and Traffic Visibility



Automatic device discovery and classification
Realtime automapping and policy management
Querying, tagging and alert monitors

No lateral movement — without the complexity of ACLs or NAC

Vielen Dank

“never trust always verify”

