VERSA

WHITE PAPER

September 2025

Beyond the Buzz: Why the Coffee Shop Approach Isn't Enough for Modern Branches

Contents

Are Today's Branches Ready to Operate Like Coffee Shops?

The coffee-shop model, inspired by public Wi-Fi simplicity, promises easy, Zero Trust access to corporate apps—no matter the location.

But for today's branch environments, it falls significantly short.

Branch networks today must handle growing volumes of IoT devices, bandwidth-heavy collaboration apps, and critical on-prem systems. They need performance, visibility, and Zero Trust enforcement across both WAN and LAN (wired, Wirelss and IoT). Treating every branch like a coffee shop may work for remote users—but it's not enough for secure, high-performing, modern branches.

Further, one of the main customer concerns is that the Coffee Shop model often relies on endpoint agents or specific configurations to enforce Zero Trust policies and traffic routing. Dependencies on agent-based systems introduce several challenges including,

1. How to handle brown or black out condition
2. Many IoT or OT devices do not support client software
3. Compatibility issues across devices and operating systems
4. Increased overhead for IT teams to manage updates and configurations
5. Limited visibility into unmanaged or headless devices
6. Redesign the traffic flow to make sure no traffic bypasses the SSE gateway
7. Degraded security posture when agents fail or are misconfigured.

Ultimately, while the model sounds frictionless, its reliance on endpoint enforcement can compromise Security, scalability, and user experience.

In Reality, Branch Networks Need to Offer Much More

Some SASE vendors are jumping on the bandwagon, claiming the coffee shop model is a one-size-fits-all solution, ignoring real-world branch complexities. Their claim to provide direct-to-app connections to their Zero Trust architecture ignores facts about how branch infrastructure plays a key role in ensuring reliable connectivity. Sadly these companies have no networking background and do not understand how reliable networks are built. Let's examine the dynamics that make a standalone Coffee Shop model insufficient for today's branch requirements.

Return to Office is Accelerating, Demanding Higher Performance

The return to office is accelerating—nearly 90% of companies have implemented some form of in-office or hybrid work model in 2025. Office occupancy rates in major cities have crossed 70%, up from under 40% in early 2023. This surge is putting pressure on branch networks to deliver higher bandwidth, reliable connectivity, and stronger on-prem security. With more users and devices back onsite, branches must support seamless access and performance to SaaS apps and defend against rising security threats. In addition, users require select applications to be prioritized in comparison to others for productivity and collaboration while securing application traffic accessed on direct internet breakout.

Real-time Applications Require More than Just Connectivity

Real-time and collaboration apps are key to business agility, enabling faster decisions and seamless teamwork. But they require more than basic connectivity—they demand high performance with low latency, minimal jitter, and reliable uptime. There are many apps competing for the same last mile connectivity – streaming, database backups, software upgrades. To support business critical apps, networks must prioritize traffic, adapt in real time, and ensure consistent and best user experience.

Client-less Devices are More Vulnerable to Attacks

Coffee shop networking architecture relies on clients installed on the device to carry traffic to security gateways that enforce security policies. Yet, IoT devices that cannot support a client are rapidly growing at branch locations. Without the client, the IOT devices in the branch are open to attack. Branches need perimeter firewalls to protect the client-less devices which is missing in the coffee shop networking architecture.

Unmanaged Devices Creates Unlimited Risks

BYOD introduces unmanaged, variable-risk endpoints—employee phones, partner laptops, guest devices, that often-run outdated OSs, unsanctioned apps, weak configs, and unknown posture. These endpoints expand attack surface via phishing, credential theft, rogue hotspots, data leakage, and lateral movement once on the LAN. Traditional security falls short because it relies on agent-only enforcement, and siloed tools that lack identity awareness, real-time posture checks, and port-level micro-segmentation. The result is poor visibility, inconsistent policies and enforcement, precisely when continuous, identity- and risk-based controls are needed.

Segmentation is Key to Controlling Lateral Movement

Threats like ransomeware can spread laterally within a branch when the internal network is treated as a single, flat trust zone. Once an attack gains access through compromised endpoint, IoT or stolen credentials, they can move east-west to access other systems. To protect from threats that exploit unsegmented VLANs, device vulnerabilities and credentials, networks require micro-segmentation to isolate users, devices and application. This containment ensures precise, role-based access preventing threats from easily spreading across branches by enforcing least-privilege at the switch/AP port, allowing only explicitly permitted east-west flows, and continuously validating user and device posture. High-risk endpoints can be automatically quarantined, inter-segment traffic is monitored and logged, and access is limited to what the job requires—shrinking the blast radius across every site.

Security Should be Enforced from Edge-to-Cloud

Enterprises need a flexible model in which some security inspections are made at every edge locally for latency-sensitive apps, compliance and data sovereignty, while others are enforced in the cloud for scale and SaaS access. Most solutions are either cloud-only or on-prem, forcing teams to juggle two control planes, duplicate policies, and direct access that lets traffic bypass the security gateway. When connectivity changes or data must stay within a Geo, they can't shift enforcement to the edge without losing enforcements or keep cloud inspection without impacting performance.

Branches Are Becoming the New Campus, Creating More Exposure to Threats

Branches are evolving into mini campuses, hosting local apps and services like FTP, SIP/VoIP, printers, and APIs which require secure, low-latency access from other branches and external partners. Traditional hub-and-spoke and VPN concentrators struggle here by hairpinning traffic through data centers, breaking SIP/FTP with NAT and access policy inconsistencies. The result is poor performance for east-west traffic, static firewall rules, and risky allow policies that exposes branch networks to threats.

Visibility and Data Should be Unified to Enable Mean Time to Resolution

Customers are challenged with deploying and managing separate wired, wireless, WAN, and security platforms that forces IT teams to juggle between multiple consoles, operating systems and events/logs creating operational silos, operational overhead, and slowing issue resolution. They require a unified platform that will empower them to deploy faster, correlate events rapidly and gain control over their wired and wireless network seamlessly while keeping their IT teams lean and efficient.

Scalable and Reliable Connectivity is Key for Today's Enterprises

Regardless of the number of users, devices and applications, the branch and campus network should enable connectivity at scale while ensuring bandwidth requirements are met. Unfortunately, with coffee shop models in which each user are considered as a separate branch network, separate VPN connectivity needs to be built converging at a security gateway. This puts significant resource constraints as a single choke point , inheriting the problems of VPN concentrators, impacting connectivity and application performance.

Exposure of IP addresses can Lead to Breaches

Within a branch network, a user's workstation must know the printer's IP to reach it on the local LAN, and basic mechanisms (ARP, L2/L3 addressing) expose that address within the segment; NAT or ZTNA masking only works within routing boundaries. As a result, users connected using a coffee shop models can inherently be forced to expose these IP addresses and credentials while accessing internal devices which can create opportunities for hackers to infiltrate networks.

Let's not Forget the Rapid Adoption of AI

The surge in AI applications and models is reshaping branch operations but also straining bandwidth, performance, and security. These data-heavy tools demand low-latency connectivity and real-time access, while introducing new risks that traditional networks can't fully manage. Branch networks must adapt with AI-aware performance and security capabilities.

The Right Approach: Augment Coffee Shop Model to your Branch Transformation Strategy

An effective branch transformation requires more than decentralization. Whereas it demands a unified approach that enforces at every edge, while prioritizing and routing application traffic intelligently based on SLAs. A comprehensive solution that combines SD-WAN and SD-LAN is key to delivering secure, high-performance branch connectivity.

Deliver Flexible Branch Deployments for All Use Cases

Robust and Secure Connectivity on any WAN Links
The right solution should deliver connectivity across any WAN links including MPLS, LTE/5G, broadband, and satellite links, intelligently steering traffic based on real-time network and application SLAs. This ensures optimal performance, bandwidth utilization, and seamless user experience for today's demanding applications, whether they're hosted in the cloud, data center, or consumed as SaaS. Additionally, security should be integrated and on-prem at every edge, protecting users and applications directly accessing the internet with integrated NGFW, URL filtering, IPS, and Zero Trust policies—all within a single unified platform.

Peak Performance with Application-aware Application Assurance
The right solution should feature accurate app detection with Deep Packet Inspection (DPI), SLA-based monitoring, and smart path selection. In addition to tracking key performance metrics, such as bandwidth, latency, jitter, and packet loss, it should monitor and measure application-based SLAs—such as round-trip delay, delay variation, transmit utilization, forward/reverse loss, and packet loss percentage to enable optimal performance and dynamic path selection including load balance and failover based on real-time conditions.

Traffic Prioritization with Quality of Service
The right solution should deliver QoS by identifying traffic conditions and prioritizing applications in real-time to maintain consistent performance even during congestion or link degradation. With comprehensive Quality of Service (QoS) combined with dynamic identification of applications, including encrypted traffic helps prioritizes them based on business-criticality. With features such as traffic policing, queuing, and WAN optimization like Forward Error Correction and Packet Duplication, Versa ensures consistent application performance—even during congestion or network degradation—optimizing user experience across all WAN links.

Extending Zero Trust across the infrastructure
To ensure users, applications and devices are protected within a branch, security should be enforced at all edges – WAN, LAN and in the cloud. The right solution should enforce Zero Trust on-prem to continuously evaluate and inspect based on risks, posture management and threats both in-line and real-time.

Extending Zero Trust Network Access (ZTNA) into the WAN and LAN enables granular control over access for corporate, guest, and IoT devices based on identity, risk assessments, device posture, and privileges. This enforces Zero Trust policies within the Branch itself, creating a software-defined security perimeter previously not possible.

Complete IoT Visibility and Security with Micro-Segmentation
Unlike traditional LANs that rely on macro-segmentation using VLANs and basic identifiers like MAC addresses, the right solution should deliver micro-segmentation to control lateral movement of threats that can lead to exploitation of vulnerabilities. With adaptive micro-segmentation to isolate users and devices within the LAN it should provide granular access control based on identity, device posture, and privileges. By accurately identifying devices including headless IoT/OT devices, it should enable assigning them to the correct microsegment, ensuring real-time tracking, isolation, and lateral movement monitoring.

Protecting BYOD Devices from Blind Spots and Unknown Vulnerabilities
The right solution should automatically discover and fingerprint every device, including headless devices like client-less IoT/OT and BYOD and tie access to risk assessments and real-time device posture. It must enforce least-privilege at the closest point (AP/switch/edge) with continuous verification and controls that work even without agents. Policies and visibility should be unified end to end from user/device to port to WAN path to application, with correlated telemetry to speed triage.

Providing Edge-to-Cloud Enforcements with Zero Bypass
The right solution should offer the same security that can be enforced locally at the edge or in the cloud without switching tools. It automatically inspects traffic where it makes the most sense based on latency, data conformance, and compliance, shifting between edge gateways and cloud SSE while keeping the same policies, rules, and enforcements. Additionally, it should ensure traffic is encrypted by default, while inspection is done close to the perimeter and enable seamless forwarding to the cloud based on access, policies and threats detected.

Zero-Trust Connectivity for Branch-Hosted Services

The right solution should ensure secure access to branch-hosted services by automatically discovering and local services like FTP, SIP/VoIP, printers and APIs, creating the right access policies and enforce security at a per user, device, and application level. Traffic should be forwarded based on the optimal branch-to-branch path with SLA-based routing and QoS for better performance. External access should be inspected and policed based on Zero Trust while enforcing posture checks and continuous risk assessments to ensure zero exposure to threats and malicious traffic into the branch.

Protecting IP addresses within the Network

Proponents of coffee shop networking often highlight the perceived benefit of IP address hiding, suggesting it adds a layer of anonymity and protection for users. However, this same advantage can be more effectively achieved with SD-WAN, which inherently abstracts and masks endpoint IP addresses while securely routing traffic through enterprise-controlled policies. Moreover, in coffee shop networks, the supposed privacy benefit breaks down as soon as users interact with local resources like printers, since their IP address must be exposed to complete those connections. With SD-WAN organizations gain the protective value of IP address hiding without subjecting employees or data to the inherent disadvantages of relying on insecure public Wi-Fi.

Single Console for Wired, Wireless, IoT and Security for Complete End-to-End Visibility

The right solution should provide a single-console management unifies WLAN, switching, SD-WAN, and security, while AI-driven optimization and automated troubleshooting reduce IT workload and accelerate problem resolution. As a result, IT teams should be empowered to manage more with less effort, reduce downtime, and focus on strategic initiatives instead of firefighting network issues.

Comprehensive Observability (DEM) from User to Applications and Everything In-between

The right solution should provide end-to-end visibility from user to application—monitoring traffic patterns, performance, and anomalies in real time across LAN, and WAN to quickly detect and resolve issues

These insights can help IT leaders quickly identify bandwidth bottlenecks, anomalies, and performance issues. Additionally, the right solution should provide Digital Experience Monitoring (DEM) for end-to-end visibility from the user to the application with native integration across SD-LAN, SD-WAN, and SSE, enabling monitoring at every edge.

Coffee Shop Branch Might Work Well in Certain Situations

For small branches with fewer than three employees, a "coffee shop networking" model is often the best fit. Treat the location like remote workers on an untrusted connection and use client-based ZTNA/SSE for per-app access, relying on commodity broadband or 5G with a small Wi-Fi access point with no branch routers, switches, or site-to-site tunnels. This keeps cost and complexity low, enables same-day onboarding, and still enforces central policies and visibility. As headcount or local shared services (printers, POS, cameras) grow, you can step up to a full SD-LAN/SD-WAN when needed.

Prepare your Branch Networks for Future Demands with Versa

Modern branch networks demand far more than only a "coffee shop model." Today's branches require secure, high-performance connectivity, advanced traffic prioritization, and deep visibility—across both WAN and LAN environments. Versa meets these needs with a unified solution that combines Secure SD-WAN and Secure SD-LAN, delivering reliable connectivity across all WAN links, enforcing Zero Trust security at the edge, segmenting IoT devices with micro-segmentation, and providing end-to-end observability from user to application. This holistic approach ensures operational agility, security, and performance that the basic decentralized, internet-only model simply cannot deliver.

VERSA

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054, +1 408.385.7660, info@versa-networks.com, www.versa-networks.com