VERSA

SOLUTION BRIEF

Versa Secure SD-LAN™

Extend the same software-defined fabric you already run in the WAN into your campus and branch LAN.

The LAN Is the Last Silo in the Enterprise Network

Campus and branch LANs are still managed as a silo, apart from the WAN and the security stack. They are refreshed on a fixed hardware cycle without the operating model underneath ever changing, which risks locking the organization into another multi-year commitment to proprietary switching.

Mixed-vendor LANs, with separate switching, wireless, and access-control products, multiply the management planes, policies, and escalation paths that IT teams must maintain. Flat, macrosegmented architectures let a single compromised device move laterally across users, IoT, and OT devices.

Zero Trust enforcement generally stops at the WAN edge or the remote-access layer, leaving the physical campus network itself outside continuous, identity-based validation.

5-7 YEARS

between campus switch refresh cycles, regardless of what changes underneath

How do you modernize the LAN without repeating the same cycle for another seven years?

Unify LAN, WAN, SSE, and SASE Under One Fabric

Versa Secure SD-LAN extends the VersaONE software-defined fabric from the WAN into the campus and branch LAN, running LAN, WAN, SSE, and SASE on one operating system, VOS. Policy is centralized, configuration is automated, and Zero Trust enforcement reaches the network edge rather than stopping short of it.

One Fabric, One OS

LAN, WAN, SSE, and SASE run on VOS under a single control plane, managed through VersaONE and Concerto. No second console and no second policy model to keep in sync.

Zero Trust to the Edge

Zero Trust and microsegmentation are enforced as close to the endpoint as the deployment allows, constraining east-west movement across users, IoT, and OT devices.

Software-Defined, Hardware-Flexible

Scale switching on demand instead of committing to a proprietary, vendor-specific refresh cycle. The hardware follows the architecture rather than dictating it.

Why This Matters

Turn the next refresh into a modernization moment

Campus switch refresh cycles happen every five to seven years regardless of what changes underneath. Secure SD-LAN makes the next refresh the point at which the operating model changes, rather than the point at which it is committed for another cycle.

Because the model is software-defined, capacity is added when a site needs it instead of on a vendor calendar.

Extend the platform you already trust

Organizations already running the Versa fabric in the WAN can extend the same policy, segmentation, and Zero Trust model into the LAN without adding a separate product set or building a new skill set.

For an existing SD-WAN deployment this is the lowest-risk path to a modern LAN: an expansion rather than a parallel architecture.

Close the last high-trust zone

Zero Trust programs typically land with remote access first and the WAN edge second. The physical campus is usually where they stop.

Pushing enforcement and microsegmentation to the edge closes one of the last unsegmented, high-trust zones left in the enterprise network, and does so within the platform already in production.

One policy model, one console

Zero Trust programs typically land with remote access first and the WAN edge second. The physical campus is usually where they stop.

Pushing enforcement and microsegmentation to the edge closes one of the last unsegmented, high-trust zones left in the enterprise network, and does so within the platform already in production.

What to Require of an SD-LAN Solution

Unify LAN, WAN, SSE, and SASE under a single software-defined fabric, managed from one control plane rather than stitched together from separate products.

Push Zero Trust enforcement and microsegmentation as close to the endpoint as possible, rather than stopping at the WAN or remote-access edge.

Stay software-defined and hardware-flexible, so the estate scales on demand instead of following a proprietary refresh cycle.

Use Case	Who It Is For	The Situation	Why Versa
Campus Switch Refresh	Network infrastructure and IT operations leaders facing an upcoming or in-flight campus switch refresh.	Aging or end-of-life campus switches, often across several vendors, force a refresh decision. The default path repeats another five to seven year lock-in cycle, keeps switch, NAC, and firewall management siloed, and leaves Zero Trust enforcement stopping at the WAN edge instead of reaching the endpoint.	One platform running LAN, WAN, SSE, and SASE under common management. Zero Trust enforcement pushed to the endpoint. Hardware flexibility that breaks the proprietary dependency, letting the customer scale switching on demand instead of buying another vendor-specific generation.
Extend SD-WAN into the LAN	Network architects and engineers at organizations already running SD-WAN, typically responding to an internal security or segmentation mandate.	Existing SD-WAN customers need east-west segmentation and Zero Trust in the campus, but the default path treats it as a fresh evaluation or a point - product decision. That adds a separate vendor stack and leaves the design dependent on a small number of people who understand the LAN.	Already running SD-WAN makes the LAN a natural, low-risk extension, with no separate stack to buy or manage. Zero Trust and microsegmentation are built in, meeting segmentation requirements out of the box, and one console shortens mean time to resolve versus a tribal - knowledge model.
Microsegmentation	Security and network architects focused on lateral-movement risk and least-privilege enforcement.	Flat or under-segmented LANs allow lateral movement across users, IoT, and OT devices, leaving organizations exposed to east-west threats even where perimeter and WAN security are mature.	Zero Trust, segmentation, and centralized management are built into the same platform, cutting complexity across multi-site environments. A software-defined, hardware-flexible model avoids proprietary lock-in and builds on infrastructure the customer has already deployed.

The Opportunity Ahead

Secure SD-LAN establishes a single, software-defined architecture for unified networking and security from the data center to the device. For organizations approaching the next legacy hardware cycle, it is the point at which the campus network stops being the exception to the architecture and becomes part of it.

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

Part# FAQ_VERSAONE-01.0