VERSA

SOLUTION BRIEF

Replace Legacy VPNs with Modern, Zero Trust Access

Secure Connectivity without Compromise: Reduced Latency, Superior User Experience, and Lower TCO with Versa ZTNA

Traditional VPNs were never designed for today's cloud-first, distributed workforce. Versa Zero Trust Network Access (ZTNA) delivers modern, secure remote access by connecting users directly to applications through identity and context-driven controls, ensuring minimal latency and superior user experience. Part of Versa's Unified SASE platform, ZTNA seamlessly integrates security and networking for advanced protection, optimized throughput, and reduced operational complexity.

Challenges: VPNs No Longer Fit Today's Enterprise Reality

Legacy VPNs fail to meet the needs of modern enterprises. Built for centralized network architectures, traditional VPNs create performance bottlenecks, expose organizations to security risks, and burden IT teams with costly infrastructure that doesn't scale. As organizations embrace cloud services and distributed workforces, these limitations directly impact user productivity, security posture, and operational costs.

Legacy VPN Pain Points

VPNs Impact User Experience and Performance

ISSUE

Traffic forced through centralized gateways create congestion, latency, inconsistent performance.

IMPACT

Frustrated users, lost productivity.

VPNs Expand Security Risk

ISSUE

Users gain broad network-level access once connected.

IMPACT

Increased risk of breach, IT/security teams burdened with continuous patching.

VPNs Are Complex, Costly, and Impossible to Scale

ISSUE

VPN management is costly (manual deployment, license management, multiple consoles).

IMPACT

High operational costs, fragmented visibility for IT/security teams.

Organizations need a remote access model built for the cloud era, one that removes implicit trust, improves performance, and simplifies operations.

Versa Zero Trust Network Access (ZTNA)

Versa ZTNA replaces VPNs with secure, per-application connectivity delivered through a global cloud edge, connecting users directly to authorized applications via authenticated sessions. Organizations gain strengthened security, accelerated performance, and streamlined operations.

Fast, Reliable Direct Access

Versa intelligently routes traffic to the optimal Versa Cloud Gateway (VCG), delivering direct-to-application access that improves performance, reduces latency, and eliminates bottlenecks. Users experience faster, more stable access to SaaS, cloud, and private applications regardless of location.

Unified SASE Platform for Streamlined Operations

Versa's Unified SASE architecture natively integrates ZNTA with Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Secure SD-WAN. All capabilities run on a single policy engine and management console, eliminating complexity and providing end-to-end visibility.

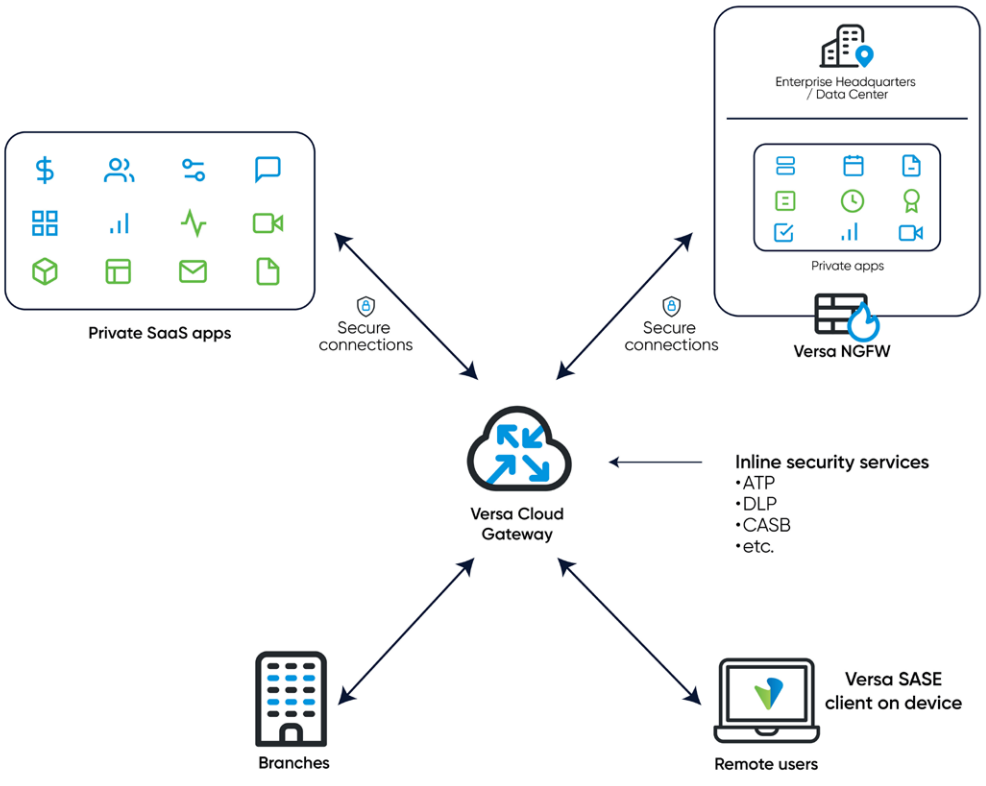
Zero Trust Access that Minimizes Breach Risk

Versa ZTNA enforces least-privilege, per-application access after authenticating users and applying policy via the VCG. Users access only what their role requires, reducing the attack surface and eliminating common VPN vulnerabilities.

Inline Security

Versa ZTNA inspects all traffic in real time using integrated inline SSE controls, delivering comprehensive threat protection without additional appliances or performance impact. It aligns with Zero Trust frameworks such as NIST 800-207 and provides detailed analytics, identity-based controls, and activity logs for audit-ready compliance.

How Versa ZTNA Works



- User authenticates via Versa SASE client
- User identity, device posture, group membership, and other contextual signals evaluated
- Versa establishes authenticated per-app sessions, enforces security policies
- Traffic intelligently routed through VCG
- User gains direct access to apps

Versa ZTNA Key Benefits

- **Exceptional User Experience:** Direct-to-app connectivity delivers up to 70% faster access with more consistent, stable sessions across all devices and locations.
- **Stronger Security with Zero Trust:** Contextual, per-application gives granular access and prevents lateral movement, reducing security risk.
- **30–40% Lower TCO:** Vera's Unified SASE architecture reduces point products and consolidates policy management, lowering management overhead.
- **Compliance Made Easy:** Automated logging, identity-driven controls, and framework alignment keep organizations audit-ready and in compliance.

Customer Spotlight

A global enterprise replaced thousands of legacy VPN endpoints with Versa ZTNA to modernize its remote access strategy.

The company saw immediate performance improvements, a sharp reduction in VPN-related tickets, and a 50% decrease in administrative workload thanks to centralized management and Unified SASE consolidation.

Why Versa

Versa ZTNA delivers strong, scalable security built for modern, distributed workforces. Versa integrates Secure Security Edge (SSE) services and industry-leading SD-WAN for a unified SASE platform. Its cloud-native architecture scales elastically with demand, delivering high-performance, Zero Trust access for on-premises, hybrid, and cloud environments. Flexible user- or bandwidth-based licensing makes it easy for organizations to adopt and expand secure access without adding complexity.

To learn more about how Versa ZTNA replaces VPNs with modern, secure access, request a demo.

Explore Versa ZTNA

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