VERSA

SOLUTION BRIEF

Achieve Zero Trust Access Across Your Organization

Stronger Security, Better Performance, and Simplified Operations with Versa Unified SASE

Traditional perimeter-based security was never designed for today's hybrid workforce and multi-cloud environments. Part of Versa's Unified SASE and with a comprehensive suite of security functions, Versa SSE delivers modern, app-specific access with continuous verification and advanced protection. Versa SSE enforces least-privilege access, eliminates lateral movement risks, and provides complete visibility across all enterprise environments.

Challenges: Legacy Security Models Introduce Risk to Modern Workforces

Traditional perimeter-based, implicit trust security models fail to meet the needs of modern enterprises. Built for in-office work, these models break in today's hybrid workforce with multi-cloud environments, exposing organizations to security risks.

Legacy Security Pain Points

Perimeter-based Security Breaks Down in Modern Enterprises

ISSUE

Users connect from unmanaged networks, apps span multi-cloud/ SaaS environments, and data moves beyond corporate boundaries.

IMPACT

Legacy perimeter defenses can't enforce granular, identity-based controls, weakening security posture.

Implicit Trust Models Fails with Hybrid Workforces

ISSUE

VPNs provide unrestricted network access and create networking issues (traffic hair-pinning, over subscription, latency).

IMPACT

Compromised credentials enable lateral movement, data exfiltration, and ransomware.

Static Zero Trust Creates Security Gaps

ISSUE

One-time access policies lack continuous monitoring and per-app controls.

IMPACT

Operational complexity allows internal threat movement, slowing threat discovery. Risk profile changes result in security gaps over time.

Security Sprawl Increases Cost and Complexity

ISSUE

Disconnected tools accumulate over time, causing configuration drift and inconsistent enforcement.

IMPACT

Operational overhead and infrastructure costs continue to rise.

Limited Visibility Fuels Shadow IT

ISSUE

Fragmented security tools prevent unified monitoring and visibility of users, applications, and traffic.

IMPACT

Teams struggle to detect policy gaps, shadow IT, and threats in real time.

Organizations need a security model built for modern, distributed enterprises, one that enforces least-privilege access, provides full visibility, and enforces consistent Zero Trust security across all environments.

Versa Zero Trust Network Access (ZTNA)

Versa Security Service Edge (SSE) replaces legacy security models with a least-privilege, identity-driven approach that securely connects users to applications. Continuous verification reduces security risk while intelligent traffic routing ensures high network performance. Delivered as part of Versa's Unified SASE platform, SSE components like ZTNA, DLP, CASB, SWG, and Advanced Threat Protection (ATP) provide end-to-end visibility, integrated threat protection, and consistent policy enforcement across hybrid environments, all from a centralized console.

Enforce Zero Trust Everywhere with Least-Privilege Access

Versa ZTNA replaces legacy VPN's broad network-level access with granular, application-specific policies. Every session continuously verifies user identity, device posture, and contextual attributes, significantly reducing an enterprise's overall security risk and preventing lateral movement.

Gain Complete Visibility

Versa provides advanced reporting and analytics across security and networking, delivering comprehensive visibility into public and private applications. Organizations can easily identify and manage network access, detect security policy gaps, and reduce risks from Shadow IT.

Integrate Native Threat Protection and DLP

Versa's multi-layered defenses including SWG, CASB, and Advanced Threat Protection (ATP) continuously analyzes user, device, and application behavior to prevent threats. DLP prevents unauthorized data exfiltration across all data access points, while GenAI Firewall ensures secure AI use. These native capabilities eliminate the need for multiple, disparate security tools.

Scale Dynamically

Versa's distributed, cloud-native architecture with intelligent traffic routing dynamically scales to handle growing traffic, avoiding the constraints of traditional VPNs. This ensures secure, seamless access for users with consistent performance across cloud, on-premises, and remote environments.

Streamline Unified Policy Management

Versa unifies policy creation, enforcement, and visibility on a single platform. Identity-driven policies are consistently applied across users, applications, and environments, delivering least-privilege access with integrated threat protection and centralized management. This unified approach reduces operational complexity while enabling easier compliance, simplifying operator workloads, and reducing costs.

Versa ZTNA Key Benefits

- **Optimized user experience**
  User experience optimized through integrated SD-WAN, single-pass security, and intelligent traffic routing
- **Centralized visibility**
  Single-pane visibility across users, devices, and applications
- **Unified SASE platform**
  Versa SSE and Unified SASE delivers ZTNA, CASB, SWG, FWaaS, RBI, DLP, ATP, and SD-WAN
- **Flexible licensing**
  User- or bandwidth-based licensing streamlines procurement

Versa SSE Modules

- Zero Trust Network Access (ZTNA)
- Next Generation Firewall (NGFW)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Advanced Threat Protection (ATP)
- GenAI Firewall
- Secure Web Gateway (SWG)
- Intrusion Protection System (IPS)
- Digital Experience Monitoring (DEM)
- Remote Browser Isolation (RBI)

Why Versa

Versa SSE delivers Zero Trust security built for modern, distributed workforces. Its cloud-native architecture scales elastically with demand to deliver high-performance Zero Trust across the entire on-premises, hybrid, and cloud environments. Part of the Versa Unified SASE platform, Versa SSE works alongside industry-leading Versa SD-WAN to deliver a seamless, unified solution

To learn more about Versa Zero Trust, request a demo.

Explore Versa Unified SASE: SSE

Customer Spotlight

A healthcare organization with over 36 branch offices struggled to manage a patchwork of VPN and firewall systems. Remote clinicians faced delays when accessing large patient files through legacy VPN, slowing care delivery. After replacing VPNs with Versa SSE and ZTNA, the organization eliminated performance bottlenecks while enforcing secure, least-privilege access across all locations.

The result: reduced data breach risk and simplified HIPAA compliance management.

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