VERSA

WHITE PAPER

October 2025

Secure Every Connection: How Versa ZTNA Replaces VPNs to Protect Users, Data, and Applications Everywhere

Contents

Executive Summary

The cybersecurity landscape has changed dramatically in recent years. Ransomware attacks are now weaponized to exploit the weakest link in enterprise access models: the VPN. Originally designed to connect remote users to corporate networks, VPNs were never intended to enforce Zero Trust principles or protect against modern lateral movement tactics.

Enterprises today face distributed workforces, SaaS proliferation, and hybrid cloud environments — all of which render perimeter-based VPN architectures obsolete. Attackers exploit stolen credentials, unpatched gateways, and implicit trust models to move freely once inside the network.

Versa Zero Trust Network Access (ZTNA) closes these gaps by enforcing identity, user posture, device posture, and context-based access to individual applications rather than networks. By embedding ZTNA within its Unified SASE architecture, Versa delivers inline threat prevention, continuous verification, and deep visibility — eliminating the ransomware pathways VPNs create.

The result:

- Reduced attack surface and ransomware exposure
- Improved compliance alignment (NIST 800-207, CISA, ISO 27001)
- Seamless user experience for remote and hybrid teams
- Lower total cost of ownership compared to managing fragmented VPN and security stacks

Market & Context

The Shift to Cloud and Hybrid Work

Enterprises have evolved far beyond the traditional on-premises perimeter. Applications now reside across multiple clouds, and employees, contractors, and partners connect from anywhere. VPNs, once a reliable access mechanism, have become a bottleneck — both in performance and security.

The explosion of SaaS applications and distributed endpoints has made implicit trust models untenable. In today's threat landscape, a single compromised credential can lead to enterprise-wide ransomware infection.

Compliance and Regulatory Drivers

Frameworks such as NIST 800-207, CISA Zero Trust Maturity Model, and mandates from sectors like finance and healthcare are now pushing organizations to adopt Zero Trust architectures. Compliance is no longer optional; it's a baseline expectation for maintaining cyber insurance and regulatory alignment.

ZTNA has therefore emerged not just as a security technology but as a compliance enabler — providing visibility, auditability, and granular control that traditional VPNs lack. In fact, the cost of cybersecurity insurance decreases when enterprises adopt zero-trust principles for their security.

VPNs: Designed for a Different Era

VPNs were originally designed to extend the enterprise perimeter when applications were hosted almost exclusively on-premises. The model was simple: authenticate a user, establish an encrypted tunnel, and grant them access to the internal network. That design made sense when the "inside" could be trusted, but it has become a liability in today's distributed, cloud-first environments.

For attackers, VPNs are attractive because they collapse security boundaries. A stolen credential or compromised endpoint is often enough to unlock broad access to the corporate network. Once inside, ransomware operators can move laterally with ease. This is not hypothetical — zero-day vulnerabilities in several VPNs have been directly tied to ransomware campaigns. Even when patched quickly, the lag between disclosure and remediation is enough for adversaries to weaponize these vulnerabilities.

On top of that, VPN concentrators are high-value targets because they are exposed to the internet and often run outdated TLS stacks or weak default cipher suites. Even where encryption is strong, VPNs are blind to the traffic they carry. Everything is funneled through a monolithic tunnel, leaving security teams without application-level visibility. Split tunneling adds another layer of risk, introducing policy inconsistencies and blind spots. The bottom line: VPNs offer an "all-or-nothing" access model, which makes them a favorite tool in the ransomware kill chain.

A VPN architecture introduces structural risks due to:

- **Credential theft = broad access:** a stolen password grants entry to the entire network.
- **Internet-facing concentrators** are prime targets and have been repeatedly exploited by ransomware groups.
- **Performance bottlenecks** from traffic hairpinning through central hubs degrade user productivity. A user may not recognize unusual device behavior, indicating a compromise, such as laptop lag, if poor user experience is common.
- **Operational fragility** with scrambling patch cycles, device driver conflicts, and appliance scaling headaches.

For ransomware operators, VPNs provide a single point of entry and an easy pathway for lateral movement across enterprise systems.

Zero Trust Network Access: Inverting the Access Model

Zero Trust Network Access (ZTNA) takes a fundamentally different approach by making access application-specific rather than network-wide, following a "Zero Trust" model. Instead of connecting users to the entire corporate network, ZTNA brokers access only to applications they are authorized to use, and only under the right conditions.

This model enforces continuous verification of user identity, user posture, and device posture, and considers context such as geolocation and risk signals, and terminates sessions if posture changes midstream. The device posture itself is derived from what versions of various components are installed and running on an endpoint, anomalous or risky behavior exhibited by the endpoint, and information relating to the endpoint that is derived from Endpoint Detection and Response (EDRs), User Endpoint Management (UEM), and Vulnerability and Threat Management (VTMs), which are installed on this device. Applications are hidden from the internet and exposed only through outbound-initiated connections, eliminating the attack surface presented by VPN concentrators.

The actual addresses of the applications can be hidden from users, and users' addresses can also be hidden from the applications. The actual identity of different users is also hidden from each other.

For incident responders, ZTNA provides richer telemetry. Every session is logged at the application level and can be correlated with threat intelligence or behavioral analytics.

The effect is that credential theft no longer translates into broad network compromise. An attacker who obtains a user's credentials may gain access to a single application, but lateral movement across the enterprise is constrained by design.

Core Principles of ZTNA

- **Never trust, always verify:** Every access request — user, device, or workload — is continuously validated before and during sessions.
- **Identity- and context-aware:** Access policies consider identity, user posture, device posture, geolocation, and risk signals in real time.
- **Micro-segmentation**: Users connect only to authorized applications, eliminating network-wide exposure.
- **Continuous verification:** Session trust is dynamic, with posture reassessments triggered by changes in device or user behavior.
- **Integration with existing controls:** ZTNA complements IAM, SIEM, CASB, and EDR ecosystems to create a cohesive security posture.

Credential theft no longer equates to full network compromise. At worst, an attacker may gain access to a single app — not the entire enterprise.

Choosing a ZTNA Provider

The market for ZTNA has grown quickly, but not all providers implement the model equally.

Some vendors offer cloud-only solutions that may force all traffic through a limited number of Points of Presence (PoPs), creating latency and data residency challenges. Others deliver ZTNA as on-premises appliances, which restores some control but replicates the operational burden of VPN concentrators. Hybrid approaches where ZTNA can be deployed across cloud PoPs, private data centers, and branch locations tend to align best with enterprises that have complex or regulated environments.

Another key difference is integration. Point solutions often operate as a separate silo, with their own policy engine disconnected from NGFW, SWG, CASB, or SD-WAN. This increases operational complexity, especially when scaling policies across thousands of users and applications. In contrast, platforms that unify ZTNA with the broader security stack provide consistency and reduce administrative overhead.

Granularity of control is also critical. Some providers stop at per-application access, while others support API-level segmentation, fine-grained posture checks, and conditional access tied to device state. For ransomware defense, this distinction determines whether an attacker can pivot once inside.

Finally, visibility matters. Limited logs showing only "user connected/disconnected" events may satisfy compliance requirements, but accurate threat detection requires complete per-session data, deep packet inspection, and integration with SIEM and SOAR workflows.

Drawbacks commonly observed with ZTNA providers include:

- **Delivery model:** cloud-only solutions may force traffic hairpinning through limited PoPs; appliance-based models recreate VPN fragility; hybrid deployment often provides the right balance.
- **Integration:** point ZTNA tools add silos, while platform-native ZTNA solutions unify policy with SWG, NGFW, CASB, and SD-WAN.
- **Control granularity:** advanced providers enforce posture-based, per-application, and even per-API policies.
- **Visibility:** Some vendors log only session start/stop, while others provide deep packet inspection and analytics.
- **Scale & resiliency:** a globally distributed, elastic fabric is critical to support hybrid and remote workforces.

Key Capabilities of Versa ZTNA

Versa ZTNA extends beyond basic access control by embedding Zero Trust principles directly into the VersaONE platform, ensuring consistency, scalability, and operational simplicity.

- **Granular, identity-aware access** – Enforces per-user, per-application, and even per-API segmentation.
- **Adaptive authentication** – Incorporates contextual signals such as user posture, device posture, OS patch level, and location.
- **Micro-segmentation and east-west isolation** – Prevents ransomware from spreading laterally.
- **Continuous verification** – Monitors device posture throughout the session, automatically revoking access if risk increases.
- **Inline threat prevention** – Includes IDS/IPS, DLP, and malware detection directly in the access path.
- **Seamless integration** – Unified policy framework across ZTNA, SWG, CASB, FWaaS, and SD-WAN.
- **Superior user experience** – Fast, direct-to-app access via the closest cloud edge, without traffic hairpinning or session drops.

Also, Versa does not expose private applications directly to the internet. With Versa, customers never need to keep open ports exposed—all access is brokered through the secure Versa Gateway, which establishes mutually authenticated connections and enforces policies before any session is allowed. This eliminates the need for a separate broker connector, ensuring applications remain completely invisible to unauthorized users, while authorized traffic benefits from inline inspection and complete visibility.

In addition, Versa's security capabilities extend beyond URL reputation; it leverages deep content inspection and behavioral analysis to evaluate traffic patterns, including GenAI applications, delivering richer controls than simple categorization. If a VOS instance (physical or virtual) is deployed in a physical or virtual data center, then depending on the instance type, VOS can serve as a VCG or as an on-premises VOS instance. It supports all or a subset of services, including later DDoS, NGFW, AV, IPS, DLP, lateral movement detection, and comprehensive micro-segmentation based on VM attributes and information derived from the entire Versa Ecosystem, such as Entity Confidence Score. As a result, it truly offers Zero Trust Everywhere (ZTE).

Architectural Flexibility

Versa offers deployment options aligned with modern hybrid enterprises:

- **Cloud-native:** Access through Versa global PoPs ensures low latency and elastic scalability.
- **On-premises:** Retain control for regulated environments with private data center hosting.
- **Hybrid:** Combine both models for maximum flexibility and compliance control.
- **Endpoint-initiated sessions:** Eliminate inbound gateways, minimizing the attack surface.

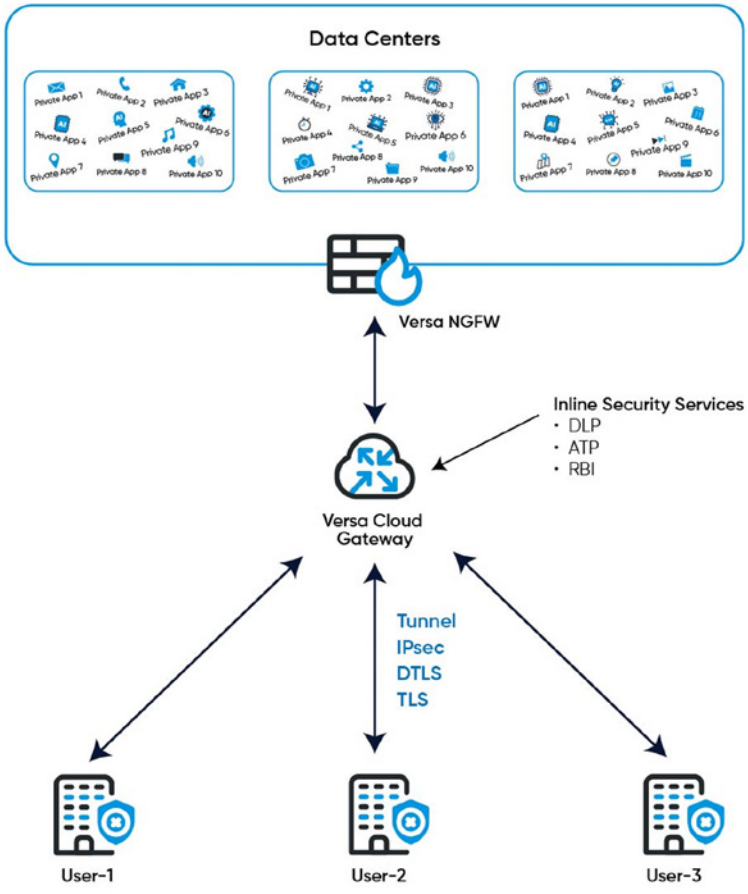
Integration with Versa SASE enables traffic inspection, logging, and policy enforcement at every edge — all managed through a centralized policy engine.

Architectural Choice to Futureproof Zero Trust Security: Versa ZTNA

While most ZTNA solutions claim to deliver Zero Trust access, their underlying architectures differ significantly in scalability, visibility, and security extensibility.

Versa's Unified Gateway Architecture

Versa unifies authentication, policy enforcement, and traffic inspection in a single component. Versa leverages standards-based TLS/DTLS/IPsec with hop-by-hop encryption, enabling inline inspection without compromising confidentiality. ZTNA traffic is tunneled to customer premises (virtual or physical) using standards-based protocols (IPsec). All tunnels are set up outbound from the SASE-Client to the SASE-Gateways, or from the Versa VNF at the physical or virtualized Data Center to the Versa SASE Gateway. This allows customers to leverage their existing Versa CPEs or 3rd party firewalls for connectivity. This removes unnecessary hops, enables inline inspection, and ensures traffic is secured using standards-based encryption protocols without deploying additional infrastructure in their DC/VPCs. The architecture is purpose-built for scalable, high-performance access with integrated security services.



Key advantages include:

- **Inline security service insertion** — Supports CASB, SWG, DLP, AV, IPS, Advanced Threat Protection, Remote Browser Isolation, and UEBA natively.
- **Uniform set of services for both internet and private access.** Access to enterprise resources (Private Access) is allowed from endpoints with Versa SASE Client as well as from those without it. In both Client-based and Clientless environments, access to enterprise resources is subject to strict multi-factor authentication, CASB, DLP, AV, IPS, ATP, RBI, and UEBA.
- **Elastic scalability** — No throughput ceilings or performance bottlenecks
- **Simplified operations** — Fewer moving parts
- **Routing intelligence** — built-in optimization ensures the best user to application performance across global environments. Irrespective of the location of the enterprise resource or the user accessing it, traffic would always be routed along a path through Versa Fabric, which yields the best user-to-application performance.

Strategic Advantages

- **Operational simplicity:** A unified control and data plane reduces administrative overhead.
- **Enhanced security**: Inline inspection of every file and session prevents ransomware spread and data exfiltration. The Secure Private Access solution also prevents lateral movement within a virtual or physical DC. East-West traffic within a DC can also be subjected to ZTNA, AV, IPS, and other services, all of which take into account user and device posture.
- **Linear scalability:** No connector sprawl or need for parallel deployments to meet bandwidth demand.
- **Compliance alignment:** Standards-based protocols map directly to NIST 800-207 and other Zero Trust frameworks.

For enterprises evaluating ZTNA platforms, these architectural differences are decisive in determining long-term scalability, visibility, and risk reduction.

Business and Security Outcomes

Organizations adopting Versa ZTNA report measurable improvements across security, compliance, and operations:

- **Reduced attack surface** – Applications are invisible to the internet; ransomware lateral movement is halted.
- **Faster partner/vendor onboarding** – Third parties gain secure, application-specific access in minutes.
- **Improved compliance posture** – Aligns with NIST 800-207 and CISA guidance for Zero Trust.
- **Enhanced productivity** – No latency from VPN concentrators; consistent access across geographies.
- **Lower operational cost** – Unified SASE framework replaces multiple point products, reducing management overhead.

Use Cases for Versa ZTNA

Versa's platform supports a range of scenarios that traditional VPNs and standalone ZTNA solutions struggle with:

- **Secure remote workforce access** – Enable employees to connect securely from any device, anywhere.
- Third-party and contractor access – Grant time-limited, policy-bound access to specific applications.
- **BYOD and unmanaged devices** – Enforce posture validation and risk scoring for untrusted devices.
- **Secure DevOps environments** – Protect CI/CD pipelines and internal APIs from lateral threats.
- **M&A integration** – Connect newly acquired entities securely without merging full networks.

The Versa ZTNA difference

Versa approaches ZTNA not as a bolt-on, but as an embedded capability of its Unified SASE platform. This means the same policy framework that governs firewalling, secure web gateway, CASB, and SD-WAN also governs Zero Trust access. For security architects, that translates into consistent enforcement, fewer silos, and reduced risk of policy drift.

Versa's architecture allows flexible deployment: ZTNA services can be consumed via Versa's global cloud PoPs, hosted in private data centers, or extended into branch locations. That hybrid capability makes Versa especially attractive in industries with strict data residency requirements or legacy workloads that cannot be migrated to the cloud immediately.

From a control perspective, Versa enforces application and even API-level segmentation. Sessions are continuously validated, incorporating device posture signals such as OS patch level, endpoint security status, and certificate health. If posture changes during a session — for example, an endpoint AV agent is disabled or based on information received from Versa SASE Client or Versa UEBA, EDR, or UEM installed on the endpoint — Versa can revoke or restrict access dynamically.

Versa also brings complete visibility and threat prevention into the access path. Unlike a traditional VPN, Versa can perform deep packet inspection on traffic flows, applying IDS/IPS, DLP, and malware detection inline. This allows ransomware command-and-control or data exfiltration attempts to be blocked before they spread laterally. Security operations teams benefit from detailed logs of every user session, integrated natively with SIEM and SOAR systems.

Operationally, Versa removes the choke points of VPN concentrators. Its distributed SASE fabric terminates connections close to the user, scaling elastically with demand and reducing latency. As a result, enterprises can eliminate exposed VPN gateways while simplifying operations.

VPN and ZTNA Comparison

Category	Legacy VPN Provider	Generic ZTNA	Versa ZTNA (Unified SASE)
User Performance	Traffic hairpins through concentrators; bandwidth collapse; video and file transfers stall.	Cloud-based models can add latency if traffic must traverse limited PoPs.	Direct-to-app access via closest cloud edge; fast, consistent performance without hairpinning.
Session Stability	Frequent disconnects, high reconnection latency, fragile mobile support.	Stable sessions determined by number of PoPs; reports of inconsistent roaming handoffs.	Seamless per-app sessions that persist across Wi-Fi, LTE, and roaming; zero tunnel drops.
Admin Overhead	Appliance patching, fragile drivers, emergency zero-day updates.	Separate ZTNA service with its own policy stack; limited integration with networking.	Centralized policy engine across ZTNA, SWG, CASB, FWaaS, SD-WAN; cloud-delivered updates.
Security Model	Broad network-level access enables lateral movement, exposed concentrators.	App-level Zero Trust access, no network exposure, limited inline security beyond access.	Per-app Zero Trust with inline IDS/IPS, DLP, and threat intel; apps hidden from internet.
Compliance & Risk	Hard to align with Zero Trust mandates; repeated patch scramble cycles.	Meets Zero Trust principles but with coverage gaps for hybrid workloads.	Audit-aligned Zero Trust controls, insurance-friendly posture, hybrid/cloud flexibility.
Cost & Licensing	Add-on licenses for scale; multiple point vendors for VPN + SWG + FWaaS.	Typically subscription-based with separate SKUs for different services; can increase TCO.	Unified SASE stack (ZTNA, SWG, FWaaS, SD-WAN) reduces vendor sprawl and lowers long-term cost.

Transitioning from VPN to ZTNA

Replacing VPNs is not a single cutover but a staged process. The first step is discovery: identify applications currently accessed via VPN and classify them by sensitivity. The next step is to onboard those applications into Versa ZTNA policies while continuing to run VPN for legacy workloads. Over time, more applications can be migrated under Zero Trust enforcement, with posture validation and segmentation applied progressively. Eventually, once coverage reaches critical mass, VPN concentrators can be decommissioned, removing one of the most targeted attack surfaces from the enterprise.

Conclusion

VPNs were built for a world that no longer exists. In today's threat landscape, their flat access model, reliance on internet-facing concentrators, and lack of granular control make them liabilities actively exploited by ransomware operators. ZTNA is the architectural correction, but effectiveness depends heavily on the provider chosen.

Versa stands out by integrating ZTNA into an entire SASE fabric, delivering granular access control, inline threat prevention, deep visibility, and flexible deployment options. For security architects, Versa offers a VPN replacement with a scalable security architecture aligned with the realities of hybrid and cloud-first enterprises.

Learn more about Versa ZTNA.

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