VERSA

WHITE PAPER

September 2025

Why VPNs Are an Open Door for Ransomware, and How Versa ZTNA Closes It

Contents

VPNs: Designed for a Different Era

VPNs were originally designed to extend the enterprise perimeter at a time 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 this has become a liability in today's distributed and 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 all been tied directly 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On top of that, VPN concentrators are high-value targets because they are exposed to the internet and often run outdated TLS stacks or weak default cipher suites.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 and device posture, considers context such as geolocation or risk signals, and terminates sessions if posture changes midstream. Applications are hidden from the internet and only exposed through outbound-initiated connections, eliminating the attack surface represented by VPN concentrators. 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.

Key benefits include:

- Continuous verification of user identity, device posture, and risk signals.
- Application-level segmentation that blocks lateral movement.
- No inbound gateways exposed to the internet.
- Rich telemetry for SIEM/SOAR correlation and incident response.

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 are easy to deploy but 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" may satisfy compliance, but true threat detection requires full 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.

Why Versa ZTNA Stands Out

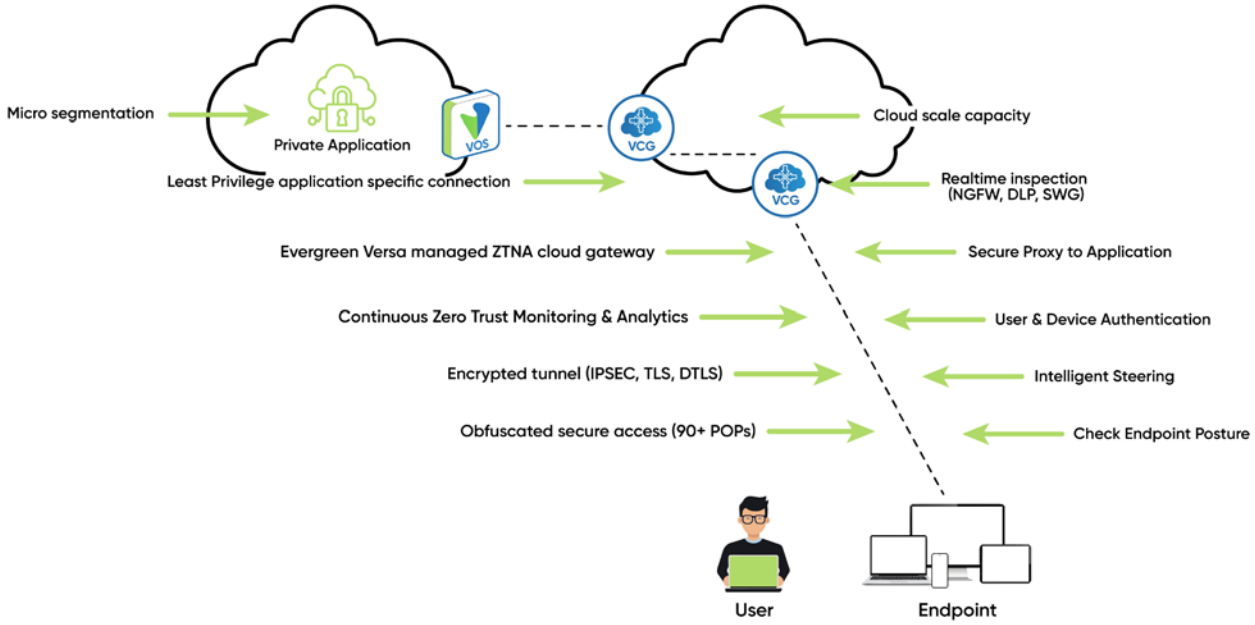
Versa approaches ZTNA not as a bolt-on, but as an embedded capability of its Unified SASE platform. This means the same policy framework that governs firewalling, secure web gateway, CASB, and SD-WAN also governs Zero Trust access. For security architects, that translates into consistent enforcement, 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 validated continuously, incorporating device posture signals such as OS patch level, endpoint security status, or certificate health. If posture changes during a session — for example, an endpoint AV agent is disabled — Versa can revoke or restrict access dynamically.

Versa also brings full 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.

Versa ZTNA Overview



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 still running 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 because it integrates ZTNA into a full 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

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