NoPorts

The World's Only Truly Zero Trust, Zero-Vulnerability Remote Access Solution

Executive Summary: Eliminate the Single Point of Failure

> In an era defined by catastrophic data breaches stemming from remote access vulnerabilities, "best practices" security solutions (VPN and centralized ZTNA solutions) present an unacceptable risk: the centralized single point of failure. Our NoPorts product is the only remote access solution built on a peer-to-peer (P2P) architecture that is closed by default, making all your services invisible to attackers, and requiring zero implicit trust in us or any third-party vendor.
>
> We challenge the status quo: Complexity is the enemy of security. Our solution replaces the spiraling complexity of open ports and centralized brokers with a single, radically simple security principle: Closed by Default.

Architectural Comparison
(Risk vs. Resilience)

Feature	Legacy VPN	Centralized ZTNA e.g., Zscaler, Netskope	NoPorts True P2P Zero Trust
Exposure	✕ Open Firewall Ports (Static IP)	! Centralized Reverse Proxy	✓ Invisible /Zero Exposed Ports on Endpoints /No Public IP required
Trust Model	✕ "Castle-and-Moat" (Trust after authentication)	! "Never Trust, Always Verify" (But trust the vendor's proxy)	✓ True Peer-to-Peer Zero Trust
Attack vector	✕ The Entire Network; VPN Concentrator	! The Vendor's Proxy and Keys	✓ Direct Process-to-Process; No Lateral Movement
Lateral Movement	✕ High Risk (Broad network access)	! Medium Risk (May require management of virtual subnets)	✓ Zero Risk (Direct process connection)
Core Weakness	✕ Broad Access and Open Ports	! Trust in Vendor Infrastructure (Keys held centrally)	✓ No Single Point of Failure

The Business Value: Security, Performance, and Simplicity

Security should never be a trade-off for performance or simplicity:

Metric	NoPorts Advantage
Radical Security	Eliminates the single point of failure and all public exposure of your assets.
Performance	Direct connection ensures low bandwidth, high stability, and speed—providing great performance for demanding applications.
Operational Simplicity	Simple firewall rules, no VPNs, no static IPs, no networking hassles—radically simpler infrastructure management.

The Failure of Legacy Remote Access Solutions

Recent high-profile cyberattacks highlight that the primary vector for enterprise compromise is the remote access gateway.

> **VPNs:**
>
> The “Moat-and-Castle” Failure - VPNs grant broad, network-level access once a user is authenticated, allowing a compromised account to move laterally across the internal network. This is not a theoretical risk; it is the documented reality: According to the 2024 VPN Risk Report, "53% of enterprises breached via VPN vulnerabilities say threat actors moved laterally," demonstrating a critical failure to contain threats at the point of entry. Furthermore, VPN servers and SSL-VPN portals are public-facing, creating a persistent, identifiable target for attackers.

> **Centralized ZTNA:**
>
> The "Trust the Vendor" Paradox : Most ZTNA solutions replace the VPN with a Reverse Proxy gateway. This is a single, centralized point of entry managed by the vendor. This model is fundamentally Brokered Trust—not true Zero Trust—because you must implicitly trust the vendor's security posture. You could say they are “One Trust” solutions.
>
> - **The Key Risk** - The proxy holds essential assets like TLS certificates and session encryption keys. A breach of the vendor's central server means an attacker gains control over a massive surface of enterprise traffic and resources. This is why this trust model can be summarized as "Blame-as-a-Service," allowing the CISO to outsource fault, but not eliminate risk.
> - **Real-World Precedent** - Critical flaws have been discovered in leading ZTNA solutions (e.g., authentication bypasses and privilege escalation against major vendors), demonstrating that relying on a centralized vendor for your gateway security is a catastrophic single point of failure (Source: Secpod Research on ZTNA Vulnerabilities and DEF CON presentation by Amberwolf).

NoPorts: The World's Most Secure Architecture

We eliminate the very concept of a security gateway or centralized proxy, making it invulnerable to the attacks that plague every other solution.

True Zero Trust: No Implicit Trust Required

Our solution operates a peer-to-peer (P2P) connection. The connection is direct and process-to-process, bypassing all virtual subnets and centralized proxies. This means keys, traffic, and access decisions are fully decentralized and reside only on the authenticated endpoints. There is no central vendor infrastructure to hack.

- **Least Privilege & Impact Containment** - Even if one individual atSign is compromised, the impact is strictly limited to what that atSign has access to, fundamentally constraining the spread of a breach.

Architectural Simplicity

We make your assets invisible to the internet. Open only explicitly is the complementary phrase for our architecture. There are no exposed attack surfaces, no public IP is exposed, and no network routes exist until an explicit, cryptographically verified connection is established. This radical simplicity virtually eliminates the attack surface because "Complexity is the enemy of security."

Open Source Security (Auditability)

Unlike closed-source ZTNA platforms, our solution is open source and uses an open protocol. This massive difference allows for transparency, independent review, and auditable assurance, giving your team a level of trust that no closed vendor can match.

Eliminate Lateral Movement

By establishing a direct process-to-process connection, We eliminate the virtual subnet/firewall layer, removing a final, critical attack vector for lateral movement.

Zero Trust Means Zero Compromise

The reality is this: If your remote access solution relies on a centralized VPN or ZTNA proxy, you are one zero-day vulnerability away from a catastrophic lateral movement breach. Our solution is the only solution built on a peer-to-peer, process-to-process architecture that eliminates this central risk.

We offer the ultimate convergence of security and efficiency: no exposed attack surfaces, no vendor trust, and the fundamental protection of the Disabled-to-Enabled principle. For executive leadership, the choice is clear: move beyond perimeter-based failures and centralized paradoxes. Choose the only truly decentralized, closed-by-default platform to ensure continuous security, high-speed performance, and radical operational simplicity.

NoPorts is not just a security solution; it is architectural risk elimination.