TPX®
Your sidekick for smart IT

Your Network Wasn't Built For the Way You Work Today

Fix Performance, Secure Access Everywhere, and Simplify IT with One Partner

Every employee login, customer interaction, and cloud application runs through your network. When it falters, the business feels it immediately. Phone calls freeze, applications stall, and productivity grinds to a halt. But here's what most organizations don't realize: the problems they're experiencing aren't just network problems. They're symptoms of a deeper architectural mismatch.

Businesses rely on hybrid work, cloud apps, and distributed teams. The networks supporting them were designed for offices, perimeter security, and predictable traffic patterns. That gap between how your network was built and how your business operates is where performance breaks down, security gaps appear, and IT complexity compounds.

This whitepaper explores the root causes of modern network struggles and explains how an integrated, managed approach can turn disconnected modernization efforts into one connected strategy.

THE CHALLENGE:

What's Breaking Your Business Isn't Just 'the Network'

Ask any IT leader about their biggest headaches and you'll hear the same themes: apps feel slow or inconsistent, remote access frustrates users, security gaps keep expanding, and IT spends more time managing vendors than driving strategy. These feel like separate problems. They're not.

> **The network is no longer a place. It's the experience of every app, everywhere.**

The underlying issue is that most business networks were never architected to support the way organizations work today. They were expanded and patched over time, rather than designed end-to-end. The result is an environment that generates ongoing operational challenges: performance issues, security vulnerabilities, and operational complexity that strains internal teams.

Common symptoms include:

- Applications that perform inconsistently across locations and devices
- Remote users relying on VPNs that introduce latency and security risk
- Expanding attack surfaces as devices, users, and apps multiply
- IT teams stuck managing a fragmented stack of vendors instead of advancing the business

THE ROOT CAUSE:

Most Networks Were Never Designed for This

The honest diagnosis: the infrastructure supporting most mid-market businesses was built for a different era. It was designed around physical offices, not hybrid work. It assumed a defined perimeter, not identity-based access across any device, anywhere. And it grew through accumulation, with one vendor added, one circuit upgraded, one appliance patched, rather than thoughtful, end-to-end architecture.

This patchwork approach creates three persistent challenges that no single bandwidth upgrade or firewall refresh will fix:

1. Performance gaps that live inside the LAN, not at the ISP, where aging switches, misconfigurations, and poor traffic routing create bottlenecks that more bandwidth cannot resolve
2. Security posture built around the perimeter, leaving remote users, cloud apps, and mobile devices exposed to modern threat vectors
3. Operational complexity driven by multiple vendors, disconnected tools, and the lack of a unified view — meaning issues take longer to diagnose, and no single team owns resolution

More bandwidth doesn't fix these problems. More hardware doesn't either. What's required is a fundamentally different approach to how network investments are aligned, operated, and improved over time.

WHAT WE'RE SEEING:

Modernization Is Happening, But It Is Happening in Pieces

Organizations are not ignoring modernization. In fact, many have invested significantly over the past several years. They have increased bandwidth. They have deployed SD-WAN. They have upgraded firewalls. They have adopted cloud applications. They have enabled remote work.

Yet performance complaints persist, security teams still struggle with visibility, and IT teams remain trapped in reactive operations. The issue is not a lack of investment. The issue is that modernization often happens through isolated projects rather than as a coordinated strategy.

Pattern 1 - WAN Modernized, LAN Forgotten

Organizations invest in bandwidth and SD-WAN expecting application experience to improve, only to discover that bottlenecks live inside switching, Wi-Fi, segmentation, or traffic handling that was never modernized with the same level of discipline.

Pattern 2 - Security Modernized at the Site, Not the User

Firewalls continue to protect the site perimeter, but users increasingly access applications from outside that perimeter. Security investments remain site-centric while work has become user-centric, leaving VPNs and fragmented access policies to carry more weight than they were designed for.

Pattern 3 - Ownership Fragmented Across Vendors and Teams

Different teams, vendors, and tools often own different parts of the environment. When users experience slow applications or access problems, the issue can move from carrier to firewall to LAN to security vendor without a single owner accountable for the complete experience.

> **The problem is not that organizations have failed to modernize.**
> **It is that modernization has happened in pieces.**

WHAT GOOD LOOKS LIKE:

A Modern Network Must Do Three Things Well

When a network is working the way it should, three capabilities come together seamlessly. Think of these not as separate projects, but as one connected challenge that requires one connected answer.

1. Deliver Consistent Application Performance

Users shouldn't have to think about the network. Applications should load quickly, video calls should be clear, and performance should be consistent whether someone is working from headquarters, a branch, or their home office. Achieving this requires optimizing the entire path, including not just the internet circuit but also SD-WAN routing, LAN switching, and Wi-Fi connectivity.

2. Secure Users Everywhere They Work

Security can't stop at the office door. With employees accessing business applications from any device, on any network, security needs to follow the user, not the building. Modern secure access means moving beyond VPNs to identity-based access that verifies who is connecting, what device they're on, and what they're authorized to do, every time.

3. Eliminate Operational Complexity

IT teams are stretched. Every additional vendor, every disconnected tool, every reactive firefight pulls focus away from strategic work. A modern network simplifies operations: one partner, one SLA, and one team that owns the complete environment from design through ongoing optimization.

> **Not separate problems. One connected challenge, and it needs one connected answer.**

THE MISSING LAYER:

Operational Alignment Is the Missing Layer

Most organizations already have many of the technologies required for a modern network. What they often lack is the operational alignment to make those investments work together.

Performance is managed separately from security. Secure access is managed separately from networking. Monitoring is separated from lifecycle management. Vendors optimize their portion of the environment, but nobody owns the complete outcome.

That is where a managed services approach creates value. A unified operating model aligns performance, secure access, monitoring, change management, and ongoing optimization around a single objective: delivering reliable, secure application access for every user.

> **The goal is not to replace every component. The goal is to make the pieces work together.**

THE TPX APPROACH:

You Don’t Need More Tools. You Need a Complete Network Strategy.

Successful modernization does not treat internet connectivity, SD-WAN, LAN, Wi-Fi, secure access, and ongoing optimization as separate initiatives. These capabilities need to be aligned under a complete network strategy built around performance, security, and operational accountability. That does not necessarily mean replacing existing infrastructure. In many cases, the more practical approach is to identify where current investments are working, address the gaps between them, and introduce new capabilities in a phased, coordinated way.

Pillar 1 - Performance:

Address the Entire Path, Not Just the Circuit

Application performance depends on more than the internet connection. Problems can emerge at the handoffs between connectivity, SD-WAN policy, firewall inspection, switching, Wi-Fi, and the user’s device.

Improving performance therefore requires visibility across the entire application path. This makes it possible to identify bottlenecks at their actual source rather than temporarily masking them with additional bandwidth.

The intended outcome is a faster, more consistent application experience across headquarters, branch locations, and remote environments, with fewer recurring incidents and support tickets.

Pillar 2 - Secure Access (SASE):

Move Protection Beyond the Perimeter

Firewalls remain important for protecting physical locations, but users and applications now operate well beyond the traditional network perimeter.

A modern secure access strategy extends policy to the user, device, application, and connection context. SASE and Zero Trust approaches can help organizations move beyond broad network access and legacy VPN models toward more precise, identity-based access to individual applications.

This creates a more consistent security posture while reducing unnecessary exposure and improving the experience for users working in the office, at home, or while traveling.

Pillar 3 - Operational Alignment:

One Partner Accountable for the Outcome

Many providers and internal teams are responsible for only one portion of the network. Yet performance and security issues frequently occur at the intersections between connectivity, SD-WAN, firewalls, switching, Wi-Fi, and secure access.

A coordinated managed operating model brings these functions together under shared monitoring, change management, escalation, and optimization processes. The objective is not simply to consolidate vendors. It is to establish clearer ownership of the complete user and application experience.

With broader visibility and defined accountability, organizations can reduce troubleshooting delays, limit vendor finger-pointing, and resolve root causes more efficiently.

THE STRATEGY:

A Unified Operating Model for Networking and Secure Access

At a strategic level, the objective is not to rip-and-replace existing infrastructure with a single-vendor hardware stack. It is to create a managed services framework that coordinates the capabilities an organization already depends on with the modernization services it needs next. This framework brings together three integrated areas: performance, secure access, and managed operations.

Performance
- Internet & SD-WAN
- LAN & Wi-Fi
- Traffic optimization

Secure Access
- Identity-based access
- SASE & Zero Trust
- VPN replacement

Managed Ops
- Design & deployment
- Ongoing optimization
- Quarterly reviews

> **We don't just connect your network.**
> **We help run it as one connected system.**

THE DIFFERENCE:

Technology Alone Doesn't Solve This

Many organizations attempt to modernize through a combination of internal IT effort and multiple specialized vendors. Each investment may be reasonable on its own, but the operating model becomes fragmented. The result is reactive troubleshooting, resource strain, and complexity that compounds over time.

Here's what that looks like in practice compared to a TPx-managed approach:

DIY / In-House	With TPx
Multiple vendors	One partner
Reactive troubleshooting	Proactive management
Internal resource strain	Proven processes
More firefighting	More forward progress
Unpredictable performance	One SLA, predictable outcomes

With TPx, businesses gain enterprise-grade network and secure access management as a predictable monthly service. The value is not just deployment. It is ongoing coordination, tuning, reporting, and accountability across technologies that often operate in silos.

CUSTOMER OUTCOMES:

What Customers Gain with TPx

The business value shows up in the outcomes IT leaders care about most:

- **Faster application performance** across every location and device
- **Secure remote access** without the friction or risk of legacy VPNs
- **Reduced IT workload** with fewer tickets, fewer firefights, fewer vendor calls
- **Simpler operations** with fewer vendors and a single point of accountability
- **A network that scales** as the business grows, without a rip-and-replace
- **Continuous improvement** built in through quarterly reviews and proactive optimization

WHY CUSTOMERS CHOOSE TPX:

What Sets TPx Apart

There is no shortage of networking and security vendors. What distinguishes TPx is the combination of end-to-end ownership, managed services discipline, and a model designed to keep improving after initial deployment.

- **Managed from design through optimization:** TPx carries the operational burden so your team does not have to.
- **Works with what you have:** TPx integrates with existing infrastructure and identity tools, including Microsoft Entra ID and Okta.
- **Proven managed services model:** Mid-market expertise backed by structured processes refined across thousands of networks.
- **Continuous optimization:** With our SASE solution quarterly business reviews and proactive tuning keep the environment aligned to business needs.

YOUR PATH FORWARD:

A Practical Path to Modern Networking

Modernizing your network does not require a disruptive overhaul. TPx uses a phased approach that addresses the highest-impact areas first and builds toward a unified operating model over time:

01

Assess

Understand your current environment, including performance, security, and operations.

02

Stabilize

Fix the biggest pain points first, focusing on application performance and secure access for remote users.

03

Modernize

Unify networking and security under one managed services platform, built for how you work today.

> **No rip-and-replace required.**
> **We work with what you have.**

CONCLUSION:

The Network You Have Wasn't Built for This. The Network You Need Is.

The gap between how your network was built and how your business operates today is real, and it's costly. Performance issues frustrate your team, security gaps create risk, and operational complexity drains IT resources that should be driving the business forward.

Closing that gap does not require more tools, more vendors, or a complete infrastructure overhaul. It requires aligning existing and future investments under a common operating model.

The organizations making the most progress recognize that performance, secure access, and operational simplicity are no longer separate initiatives. They are connected outcomes of the same modernization strategy.

TPx helps organizations make that shift. End-to-end. Fully managed. Ready when you are.

Start with a Network & Security Assessment to identify performance gaps, evaluate your secure access readiness, and get a clear modernization roadmap.

Visit TPx.com or call (866) 603-0624 to speak with a TPx networking expert.