TNS MANAGED NETWORK SERVICES

Retailers guide

How to switch to a secure managed network

The challenge hanging over retail

Retailers today don't just run stores – they run networks. From payments to self-checkouts and digital signage, seamless connectivity is essential. But as businesses grow, managing networks, firewalls and Wi-Fi access points in-house becomes unsustainable.

Cybersecurity risks, integration challenges, and scaling issues only increase – especially with siloed legacy infrastructure and multiple vendors. That's why many retailers are turning to managed service providers.

Not all providers are created equal – this guide will help you navigate the transition.

What is a managed service provider?

A managed service provider designs, secures, maintains and manages a retailer's network – keeping stores, payment systems and business applications online, protected and ready to scale. Rather than burdening your in-house IT team, businesses can rely on 24/7 connectivity, built-in security and expert help.

70% of retail is still physical,[1] making store connectivity critical.

Step 1 – Assess your **current network connectivity challenges**

Before selecting a provider, identify your pain points:

1. **Are you experiencing bottlenecks**: Is downtime or multi-location management slowing you down?

2. **Are you looking to grow**: Is your network ready for more stores, IoT expansion or pop-up stores?

3. **Are you experiencing difficulty expanding to remote locations**: Is poor connectivity and an inconsistent customer experience across different channels or regions holding you back?

4. **How are your internal resources**: Does your IT team have the bandwidth and regulatory experience to manage security, compliance and integrations efficiently?

5. **Are you struggling with multiple vendors**: Is managing firewalls, Wi-Fi access points, and networking across multiple providers slowing down response times and troubleshooting?

6. **Is an upgrade imminent**: Are you experiencing security gaps and disruptions created by outdated devices and end-of-life hardware?

7. **Do you need to unlock third-party services**: Is accessing public cloud or other platforms essential for your business growth and integration strategy?

24% of cyberattacks target retail customers, putting data and transactions at risk.[2]

Step 2 – Find a provider who **fits your needs**

Now that you understand your needs, finding the right network solution is a critical investment for building fast, secure, and seamlessly connected retail operations. Your chosen provider should offer:

- **Multi-layer security**: PCI DSS certification and next gen firewalls are the gold-standard to protect payments, IoT, guest Wi-Fi, customer information and business data

- **Always-on connectivity**: Telco-agnostic providers with built-in failover across both wired and wireless networks ensure mission-critical operations stay running

- **Prioritising traffic**: SD-WAN prioritizes and routes time-sensitive traffic like payments and critical business applications, managed from a centralised location

- **Built to scale**: Support new stores, cloud apps and tech upgrades without costly overhauls

- **Real-time and proactive monitoring**: 24/7 visibility and management with real-time monitoring and troubleshooting to prevent disruptions before they happen

- **Complete management**: A solution that is designed, monitor and maintained by tech experts with zero-touch provisioning, deployment and management of connectivity services, routers, SIM cards and software licenses

- **Lower total cost of ownership**: A single, converged solution covering connectivity, security, and LAN networking reduces overall costs

- **Global and local expertise**: Strong carrier ties and compliance knowledge ensure seamless expansion

- **Simplified management**: One provider, one contract – less complexity, fewer vendors and lower costs

- **Centralized visibility**: Real-time reporting and self-service management via web portal or API for greater control

Downtime is a killer

Network failures can be expensive, and the bigger the business, the higher the cost. While small retailers lose an estimated $137–$427 per minute, enterprise retailers can lose over $16,000 per minute – or more than $1 million per hour.[3]

Apple lost $25 million during a 12-hour outage in March 2015

Facebook lost nearly $90 million during a 14-hour outage in March 2019

Delta Airlines lost $150 million during a 5-hour outage in August 2016

Choosing the right provider – **Why TNSLink for Retail**

Switching to a managed service provider is about more than just reducing IT headaches, it's about building a network that helps you grow, secures your business and lets you nail the customer experience.

At TNS, we do more than connect your stores – we support your business. TNSLink for Retail is built for businesses like yours, combining advanced SD-WAN technology with deep industry expertise.

We understand the challenges of scaling a multi-location retail network, so we've designed a secure, resilient, and tailored solution. With global carrier redundancy, zero-touch provisioning, and 24/7 local support managing network performance, TNS takes the complexity out of connectivity, so you can focus on growing your business and delivering seamless customer experiences.

Ready to transform your retail connectivity?

TNSLink for Retail is a fully managed, single-vendor solution for connectivity, networking, and security – keeping your stores, business applications, IoT devices, and cloud environments protected and seamlessly connected. **Visit tnsi.com/solutions/payments/connect/ for more information.**