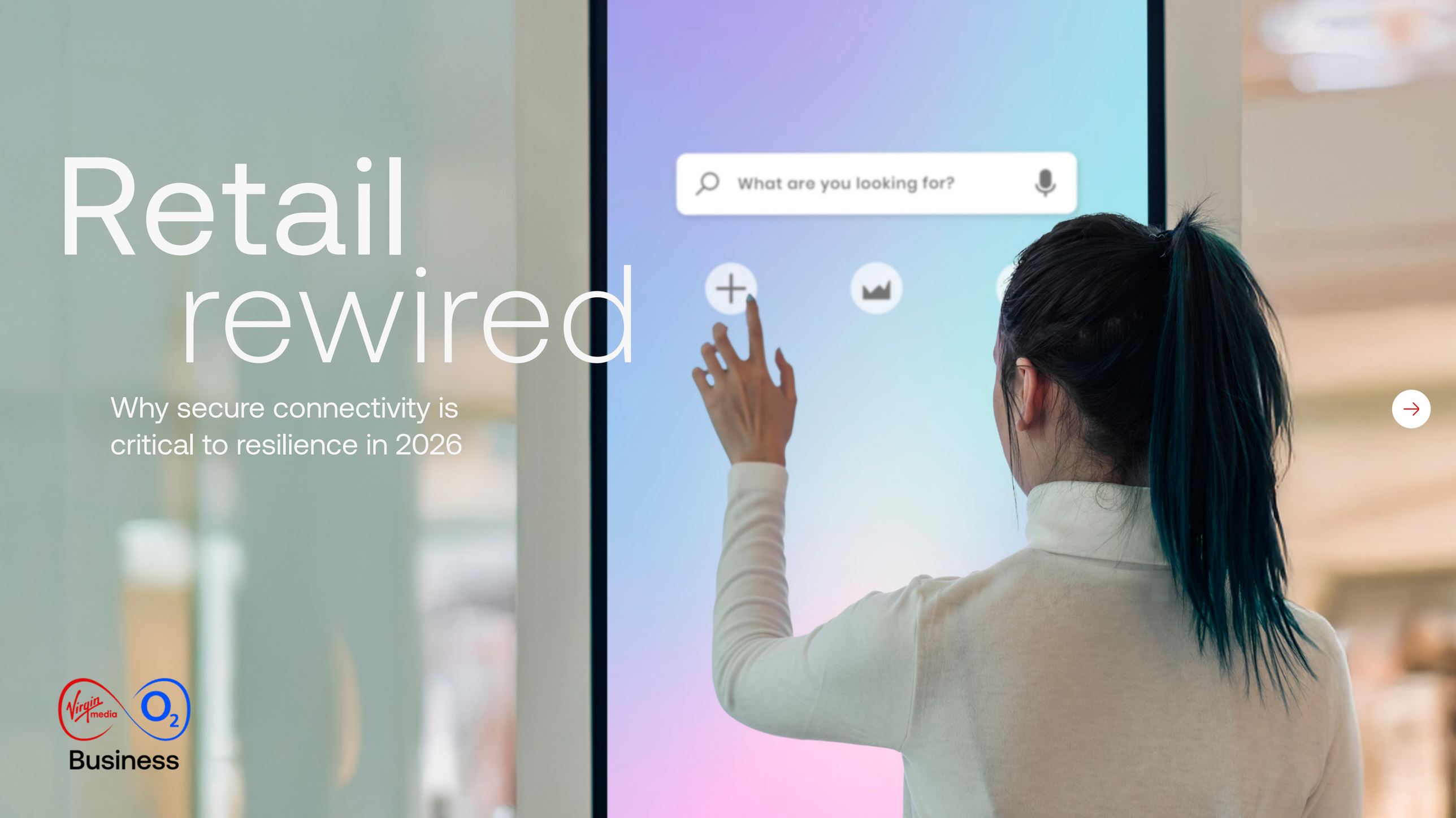
Retail rewired

Why secure connectivity is critical to resilience in 2026



Business

Retail in 2026 is demanding and volatile

UK retail is facing a contradiction: customers expect everything instantly, yet the industry backdrop is fragile.

With sales volumes falling in Q4 2025 despite a December rise,[1] growth is not guaranteed.

The stakes are high:

- Cyber attacks sometimes manage to stop trade, not just steal data
- A sustained cyber disruption could wipe out an entire quarter's margin
- The Payment Card Industry Data Security Standard (PCI DSS) v4.0 is demanding stricter controls

Resilience is no longer just an IT metric – it's a way to protect revenue.

Secure connectivity now sits at the centre of operational risk, brand trust and investor confidence.

Your network keeps your business trading.

Keeping up with your customers

Online and in store are now one. Customers just see your brand.

This shift requires inventory and payments to sync in real time. If your network lags, the customer sees the cracks and loyalty drops.

The pressure on your stores

Stores have evolved into showrooms and fulfilment hubs.

This relies on data flowing securely between thousands of locations. If that flow stops, the experience breaks. A customer travelling to a store for a sold-out item (because systems didn't sync) is a customer lost.

Operating in a tighter market

The Q4 sales dip in 2025[1] proves you must do more with less. Efficiency is everything.

Every minute your team spends fighting poor connectivity is a minute they aren't selling. And reducing operational friction is often the fastest way to protect your margins.

New risks for UK retailers

Connectivity links your sites together. But it can also expose them if it's not managed right.

Modern retail estates are complex mixes of older infrastructure, cloud platforms, third-party logistics partners and pop-up locations.

Cyber attackers are targeting your people

The National Cyber Security Centre (NCSC) has warned that criminals are targeting weaknesses aggressively. But they're not always hacking firewalls with complex code – they're phoning help desks and tricking staff into giving them access.

This 'social engineering' bypasses your technical defences by exploiting human nature.[2]

Retail environments are particularly vulnerable to this. With high staff turnover and busy, high-pressure environments, it's easier for a criminal to pose as 'head office IT' and convince a store employee to reset a password or download a file.

When these attacks happen, the damage is not just theoretical. It's measured in days of lost trading and millions in recovery costs.

Remember the major cyber attack on Marks & Spencer in April 2025? The financial impact was estimated to be £300 million.[3]

Modern cyber threats attack your operations, causing chaos by:

Taking down point of sale (POS) systems so you can't trade

Freezing supply chains so stock doesn't move

Stopping payments so cash flow stalls

Compliance isn’t optional

Let’s not forget the regulator. The arrival of mandatory PCI DSS v4.0 in 2025 changed the game. It requires you to prove your environment is secure, encrypted and constantly monitored.

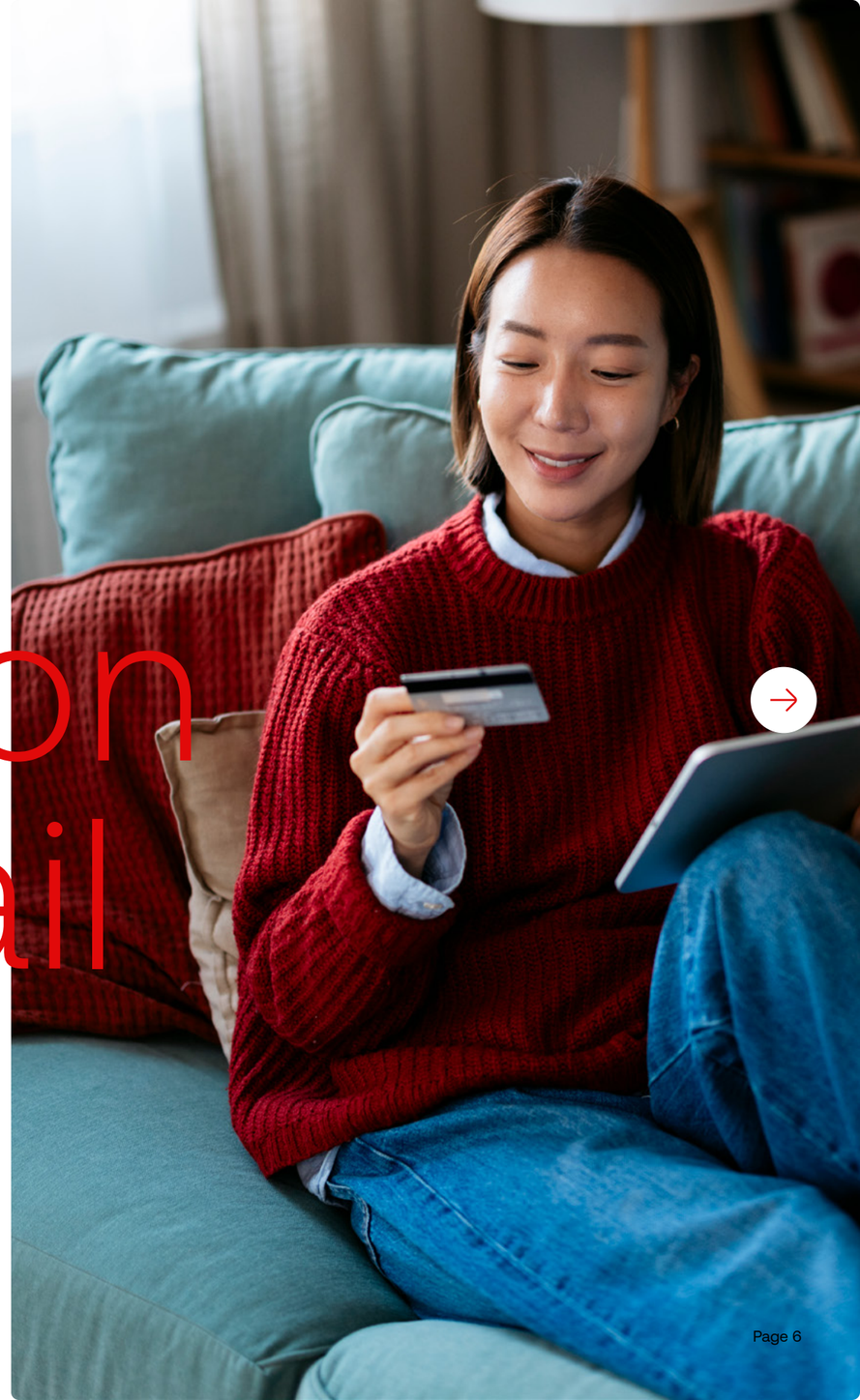
This isn’t just about avoiding fines. It’s about the ability to trade.

If you can’t prove you’re handling payment data securely, you risk losing the ability to take card payments entirely. In a world where cash usage continues to drop, that’s a major threat.

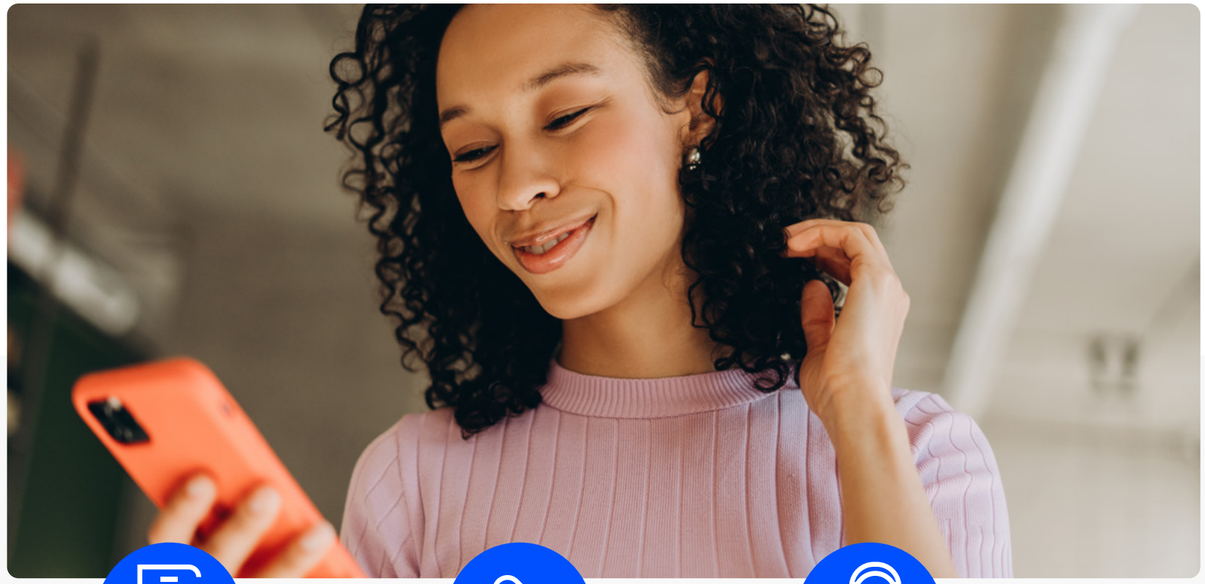
PCI DSS v4.0 also puts a heavy focus on visibility. You need to know what’s happening on your network at all times. If you still have a fragmented network where every store has a different setup, achieving that level of visibility is nearly impossible.

Why secure connectivity is the foundation of modern retail

We need to move past the idea that connectivity is just about bandwidth or speed.



In 2026, your network defines your customer experience. It's the nervous system of your business.



When your network works, you get...

Real-time stock accuracy
so you never promise an item you don't have

Fast, reliable checkouts
that keep queues short and customers happy

Smooth digital journeys
that link your app to the aisles without friction

Empowered staff
who have the answers at their fingertips, rather than having to run to the back office

It also means you can run your business better.

You can send pricing updates to electronic shelf labels in seconds rather than hours. You can monitor energy usage in real time to cut costs. You can use video analytics to understand footfall patterns and optimise store layouts.

But if your network fails...

Your revenue breaks too. We've all seen the signs of digital outages:

- Handwritten 'cash only' signs taped to the door
- Abandoned baskets in the aisles
- Frustrated staff trying to explain why they can't process a return

Downtime destroys trust faster than a bad review. And in a volatile market, you can't afford to turn away revenue because your internet connection dropped or a cyber attack took your systems offline.

The reputational damage of your systems going down can last long after the connection is restored.

The tech powering stronger resilience

Retailers are moving away from fragmented, store-by-store networks to centrally managed architectures such as SD-WAN, This reduces outages, improves visibility and closes security gaps across the estate.

Combined with cloud-delivered security approaches like secure access service edge (SASE), this can provide the visibility, control and protection required across multi-site estates.

For environments that need high-performance wireless coverage or support for growing internet of things (IoT) estates, 5G private networks can provide fast, reliable and secure on site connectivity. This is especially beneficial to locations where traditional fixed infrastructure is hard to extend.

The launchpad for what comes next

A strong digital foundation also lets you try new things.

Whether it's AI-driven operations that predict stock shortages before they happen or personalised offers sent to customers' phones as they walk in the door, none of it works without secure, always-on connectivity.

But you can't build a modern retail experience on older infrastructure.

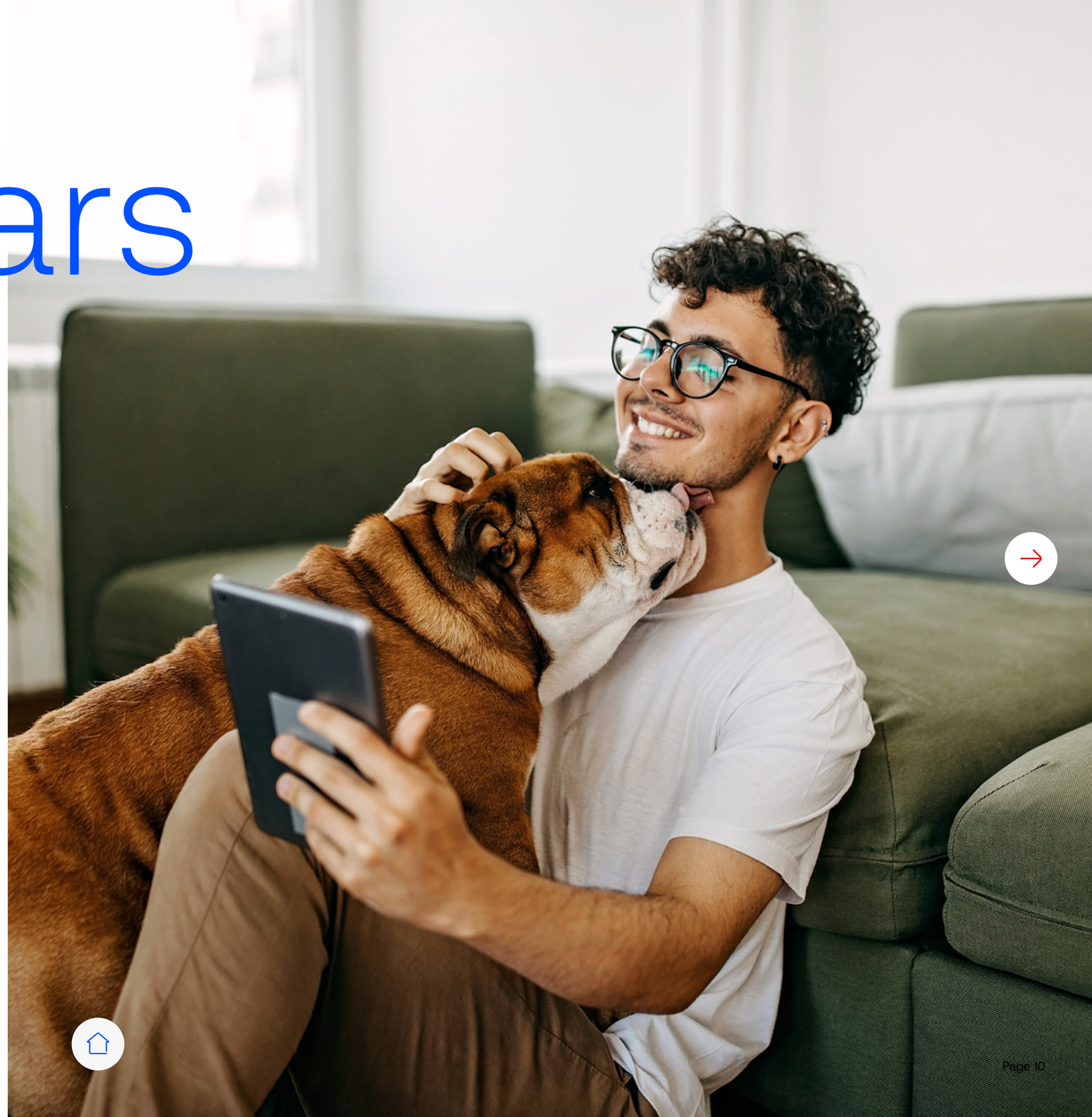
If you want to use tablets for assisted selling or deploy mobile POS so staff can take payments anywhere in the store, you need a network that's designed for mobility and security, not just for tills at the front of the store.

The 5 pillars of retail resilience

To stand up to all these challenges, you need to focus on five key areas.

They're not just tech upgrades – they're **operational safeguards** that protect revenue, brand trust and customer loyalty.

They represent the difference between surviving and thriving.



1.

Always-on operations

Disruption happens. Diggers go through cables, storms take out power lines and hardware fails.

But your customers should never feel it.

You need a network that keeps the lights on and the tills ringing, even when something goes wrong.

This means moving away from single points of failure. It means having backup connections like 4G or 5G mobile data that kick in automatically if your fixed line drops. It means your staff can carry on serving customers without panic and your payments keep processing.

2.

Embedded trust and security

Security cannot be something you bolt on at the end. It has to be built into the way you work, following the NCSC's retail-specific advice.

Every connection point needs to be secure by default.

This SASE concept means that security policies travel with the user and the data, rather than just sitting at your head office firewall.

Whether a store manager is accessing the payroll system from the back office or a buyer is signing in from a coffee shop, the access is secure.

3.

Real-time data for real-time decisions

You can't run modern retail on yesterday's numbers.

You need a network that lets data move instantly across your estate, giving you a single, accurate view of stock and sales.

This visibility enables you to make better decisions.

If a specific line is selling out in Manchester but sitting on the shelves in Birmingham, real-time data lets you spot that trend and move stock to where the demand is. It stops you from marking down stock that could have been sold at full price elsewhere.

4.

Friction-free digital journeys

Whether a customer is buying on Instagram, checking their loyalty points on your app or tapping a card in store, the process should be instant. Any lag, buffering or failure sends them straight to a competitor.

Your network needs to prioritise this traffic. It should know that a payment transaction or a stock check is more important than a guest WiFi user streaming a video and it should allocate bandwidth accordingly.

This ensures the things that make you money always come first.

5.

A future-ready, scalable foundation

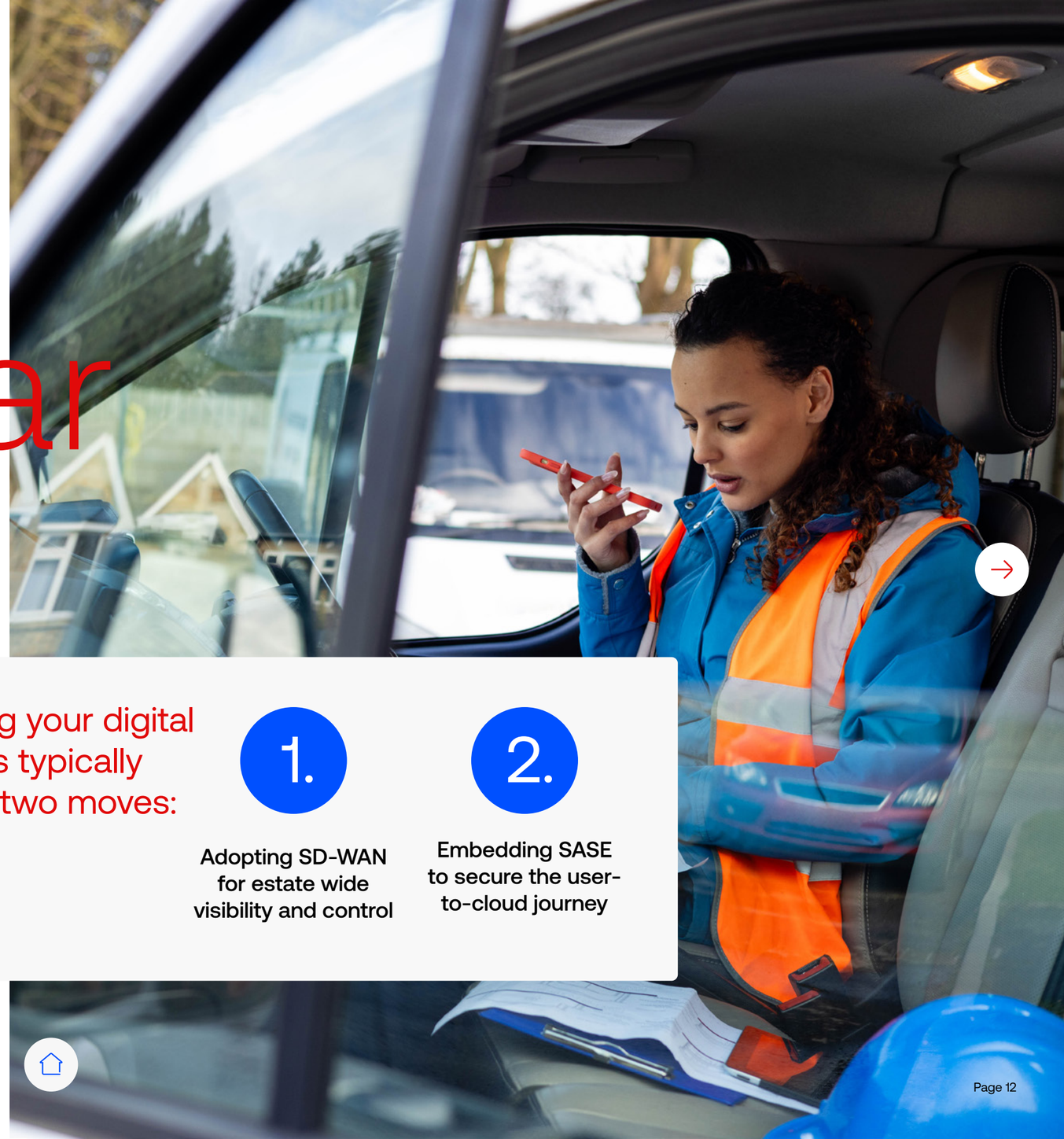
The tech you use today won't be what you use tomorrow. You need a digital foundation that can flex and grow as you roll out new formats, automation and AI tools.

If you want to open a pop-up store for the holiday season, you shouldn't have to wait weeks for fixed-line connectivity to be installed. A modern, resilient network allows you to set up secure connectivity over 5G within hours.

Tech like 5G private networks are helping retailers extend secure, high-performance connectivity into new formats, from pop ups to backroom areas. Since you don't have to wait for fixed lines, you can start trading immediately, as well as providing critical connectivity for automation solutions.

Priorities for the year ahead

There are some clear strategic moves you can make this year to protect your business.



Modernising your digital foundations typically centres on two moves:

1. Adopting SD-WAN for estate wide visibility and control

2. Embedding SASE to secure the user-to-cloud journey

Your 2026 retail resilience checklist

Strengthen your digital core

Move away from a patchwork of older networks and suppliers. It's hard to secure what you can't see.

Look for centrally managed architectures like SD-WAN that give you complete visibility and control over your whole estate from a single screen. This lets you spot issues before they become outages.

Embed security everywhere

Close the process gaps. Technology is only half the battle and you need to support your people too.

Make sure your helpdesk verification processes are as secure as your firewall to stop social engineering attacks. Ensure that every device, from the CEO's laptop to the warehouse scanner, is verified before it touches your network.

Simplify your estate

Complexity is the enemy of security. A complicated network is hard to fix, hard to secure and expensive to run.

Simplifying your infrastructure makes it easier to patch vulnerabilities and faster to roll out new experiences.

Treat compliance as a positive

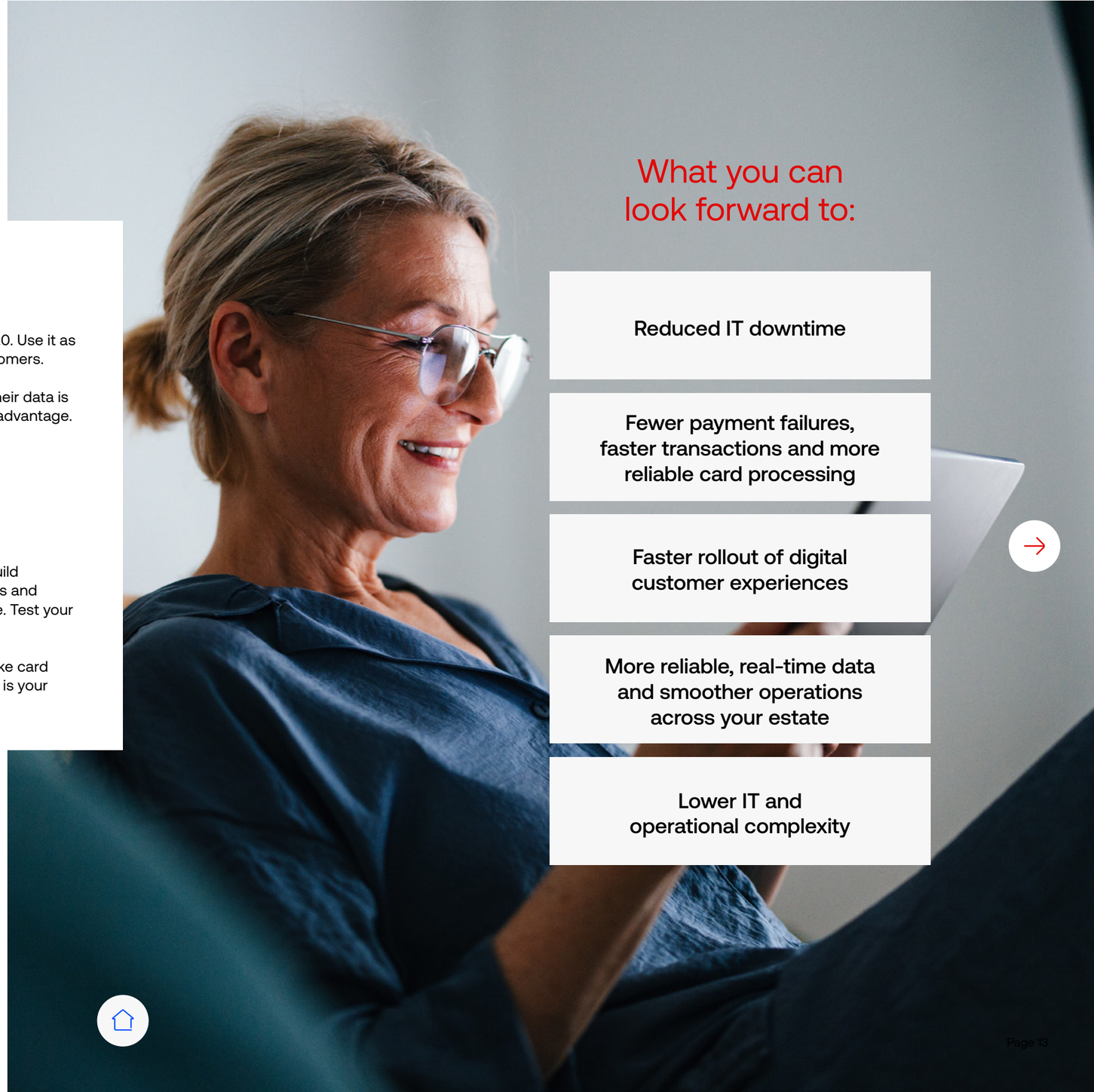
Do not just tick the boxes for PCI DSS v4.0. Use it as a framework to build trust with your customers.

When you can tell your customers that their data is safe with you, it becomes a competitive advantage.

Design for resilience

Assume things will sometimes fail and build systems that cope. Ensure your payments and customer services have backups in place. Test your disaster recovery plans regularly.

If the internet goes down, can you still take card payments? If the answer is no, fixing that is your priority.



What you can look forward to:

- Reduced IT downtime
- Fewer payment failures, faster transactions and more reliable card processing
- Faster rollout of digital customer experiences
- More reliable, real-time data and smoother operations across your estate
- Lower IT and operational complexity

Have you got the right digital backbone for the future?

Retailers who invest in secure, modern digital foundations will be the ones who win in 2026.

You'll be the ones delivering the experiences customers love, protecting your revenue from attacks and growing with confidence.

Resilience is not just about preventing bad things from happening – it's about having the strength to keep moving forward, no matter what the market or world throws at you.

It's about turning your network from a utility into a competitive asset.

Explore our retail hub to see how we're helping retailers build secure, connected and future-ready operations.

Virgin media O2 Business

Want to check how resilient your business currently is?

Get in touch today

1. Office for National Statistics 2026: Retail sales, Great Britain: December 2025
2. National Cyber Security Centre 2025: Incidents impacting retailers
3. BBC News 2025: https://www.bbc.co.uk/news/articles/c93llkg4n51o