GTT Greater Technology Together

SECURE AND COMPLIANT RETAIL

Protect every transaction, every store and every channel, and turn continuous PCI, NIS2 and GDPR compliance into customer trust.



A GTT SOLUTION BRIEF

June 2026

SECURE AND COMPLIANT RETAIL

Protect every transaction, every store and every channel, and turn continuous PCI, NIS2 and GDPR compliance into customer trust.

CONTENTS:

THE LANDSCAPE 3
WHERE GTT COMES IN 4
THE APPROACH 5
THE SOLUTION 6
THE GTT PLATFORM ADVANTAGE 7
THE PROOF 8
WHY GTT 9
RETAIL SUB-VERTICALS SERVED 10
ABOUT GTT 11



THE LANDSCAPE

Security has climbed to the top of the retail agenda, and it got there the hard way. The 2025 UK retail crisis made the threat concrete: a British retailer, lost an estimated £300M in profit and six weeks of online trading to a single ransomware attack. (Computer Weekly, 2025) Weeks later, the UNFI attack took the largest US wholesale food distributor offline for ten days, and shelves emptied across more than 30,000 locations. (Reuters, 2025) The bill keeps climbing once ransomware lands. The median demand for retailers has doubled to $2M, and 27% now sit above $5M. (Sophos, 2025) A breach is no longer an IT incident. It is a board event that can erase a quarter.

The pattern behind those headlines is broad. A 2025 Verizon Data Breach Investigations Report recorded 837 retail incidents and 419 confirmed breaches. System intrusion drove 53% of them, ransomware appeared in 44% of breaches and third-party involvement doubled in a single year from 15% to 30%. (Verizon, 2025) The storefront takes its own fire: bots now make up close to half of retail web traffic, and DDoS attacks hit 47.1 million globally in 2025, up 236% since 2023, with more than a third of Black Friday shoppers turning out to be bots rather than people. (Imperva, 2025; Cloudflare, 2025)

The global cybersecurity regulatory landscape is also expanding and becoming more complex, with stricter requirements, broader scope and increased enforcement across regions and industries. PCI DSS 4.0, the payment-card security standard, became mandatory in March 2025 with 64 new requirements, yet only 32% of organizations were ready. (PCI SSC, 2025; Protegrity, 2025) Its new mandates include isolating the cardholder data environment, the systems that store, process or transmit card data, from the rest of the store network, multi-factor authentication for all access to that environment and continuous rather than periodic monitoring.

Multi-country retailers carry the burden of additional regulations: NIS2, with penalties up to €10M or 2% of global revenue and personal board liability; GDPR, with a 72-hour breach-notification clock and fines up to 4% of global revenue; and 172 national privacy laws that each set their own rules. (European Commission, 2025) Two more now bind: DORA reaches retailers offering financial services such as buy-now-pay-later and branded cards, and the EU AI Act carries penalties up to €35M or 7% of global turnover for prohibited uses, both already in force and both landing on retailers that run AI for pricing, personalization and fraud. (European Commission, 2025) And security has now overtaken price as the top reason enterprises switch technology providers. (McKinsey, 2026)

837

retail security incidents in a year, with ransomware present in 44% of breaches.

Verizon, 2025

32%

of organizations were ready for PCI DSS 4.0 when the mandate took effect.

Protegrity, 2025

£ 300M

in profit erased by a single breach, plus six weeks of lost online trading at M&S.

Computer Weekly, 2025

$10.22M

average cost of a US retail data breach, up 18% year over year.

IBM, 2025







CONNECT ***SECURE*** ***SIMPLIF***

THE CHALLENGES FOR RETAIL	
Estates The Attackers Know Are Unwatched Most stores have no on-site IT, and 91% of ransomware hits outside business hours, so the detection window stays open through the night. *(Forescout, 2025)*	**Flat Networks Where One Breach Spreads** Retail is the highest risk sector of any for connected devices. POS, payment, cameras and guest Wi-Fi share one network, so a foothold in one corner can reach the till. *(Forescout, 2025)*
Compliance That Fragments At Every Border PCI DSS 4.0, NIS2, GDPR, DORA and 172 privacy laws impose different timelines and requirements, where one incident can trigger multiple overlapping obligations.	**The Expertise To Defend It Is Not In-House** 45% of retail ransomware victims cited a lack of in-house skills, the highest rate of any sector, so the work has to be sourced. *(Sophos, 2025)*

IN RETAIL, SECURITY HAS MOVED FROM AN IT COST LINE TO A BOARD-LEVEL QUESTION: THE DIFFERENCE BETWEEN TRADING THROUGH A PEAK AND LOSING A QUARTER'S PROFIT TO A BREACH.

WHERE GTT COMES IN

GTT builds security into the network rather than bolting it on after the fact. It runs at the network level, from the store edge to the cloud, so every transaction, data flow and session is protected by default rather than by exception. And because fewer standalone security appliances sit in each store, fewer devices land in PCI scope to audit and defend. Stronger and simpler at the same time, which is rarer than it sounds.

This matters most for the retailers who can't staff the problem, which is most of them. The global security talent gap hit 4.8 million people in 2025, up 19% in a year, and only about a third of organizations say they are adequately staffed. (ISC2, 2025) More than 90% of GTT's distributed customers already run their networking as a managed service with GTT, and security rides the same model: a 24/7 SOC handling detection and response, scaling with the estate rather than the headcount.

SECURITY THAT TRAVELS WITH THE NETWORK, NOT A STACK YOU BOLT ON AND MAINTAIN.

THE APPROACH

Many retail estates didn't start with a plan. They just grew. A new country meant a new ISP. A new requirement meant another point product. Every acquisition brought its own stack. Soon, no single team owned the result, and every change touched half a dozen contracts. GTT flips this. We start with a single operating model and one accountable partner for the entire estate.

FRAGMENTED MULTI-VENDOR ESTATE	THE GTT APPROACH
Security overlaid on a network someone else owns, with no single accountable SLA	One partner owns the global Tier 1 backbone and runs connectivity and security through it
10 to 15 providers, separate consoles, separate contracts and separate renewal cycles	One bill, one contact and one policy engine
Point tools added per site, so configurations drift from store to store	Centralized policy enforced from London to Los Angeles, consistent at every site
Periodic audits that snapshot compliance once and hope it holds	Continuous monitoring that keeps PCI DSS 4.0, NIS2 and GDPR audit-ready
Each new device and tool adds to PCI scope	A single-device store architecture reduces in-scope components

From periodic audits to continuous compliance

The old compliance model was a snapshot. An auditor visited and signed off, and the estate drifted until the next visit. PCI DSS 4.0 closed that gap by requiring continuous monitoring, and the network is where continuous becomes practical. With GTT, security policy travels with connectivity: when a new store, dark store or pop-up is provisioned, its security configuration deploys automatically alongside the link, so nothing opens unprotected. GTT provides certified network infrastructure, documented evidence for auditors and monitoring that runs without pause, which supports the shift from periodic checks to continuous compliance. Where a security uplift runs alongside a network migration, GTT can work around a retailer's peak-trading calendar, including the October to January change freeze, so cutovers never collide with peak.

THE SOLUTION

Secure Connect, SASE, built on Palo Alto Network's Prisma Access, Fortinet or HPE Aruba Networking, folds SD-WAN and cloud-delivered security into one service: firewall as a service, secure web gateway, zero-trust network access, a cloud access security broker and data loss prevention. Zero-trust is the part that matters most in retail. Every user reaches only the applications their role needs, and trust is never assumed. Stores get enterprise-grade security with no box to install on site. Remote workers and franchise partners get access scoped to the job, and policy is set once and centrally, so a rule written in one place holds everywhere.

On detection, GTT's Managed Detection and Response service runs 24/7/365 through a global SOC of CREST-certified analysts working to a 15-minute investigation SLA, and AI-assisted detection adds machine-speed triage for the malware-free intrusions that now slip past traditional antivirus. That gap is widening fast: 82% of 2025 intrusions left no malware behind, and the quickest break-in took 27 seconds. (CrowdStrike, 2026) On availability, DDoS Mitigation runs through 13 global scrubbing centers with 4 Tbps of capacity, filtering floods before they reach the storefront, with capacity pre-positioned ahead of the obvious pressure points like Black Friday and Singles' Day. The checkout page gets its own guard: controls aligned to the PCI DSS 4.0 payment-page script requirements, Requirement 6.4.3, aimed at the e-skimming attacks that surged through 2025.

Around these sit the rest of the layer. SSE cloud security delivers six converged services under one policy engine for retailers not yet ready for full SASE. Managed Firewall provides next-generation firewalling and intrusion prevention at every store and supports segmentation of the cardholder data environment. Network Segmentation, built from GTT EnvisionEDGE and SASE, splits the store into four zones that must never mix: payment systems; the corporate back-office; IoT and operational systems such as refrigeration, cameras and self-checkout; and guest Wi-Fi. That isolation shrinks PCI scope and contains lateral movement, which matters because more than half of IoT devices carry critical vulnerabilities and one in three breaches now involves an IoT device. (Forescout, 2025) Secure Remote Access gives encrypted per-seat access with MFA and single sign-on, and cloud security governance carries one consistent compliance posture across edge, private and managed public cloud.

Retail's biggest blind spot now sits outside the building. Third-party involvement in breaches doubled in a year to 30%. (Verizon, 2025) Among large US retailers, 97% were hit through a third party, and supply-chain breaches run $4.91M on average and take 267 days to find. (SecurityScorecard, 2025) The Blue Yonder ransomware attack stopped Starbucks, Sainsbury's and Morrisons at once, and the CDK Global breach reached roughly 15,000 car dealerships from a single point. GTT's answer is zero-trust access: every supplier, contractor and franchise partner reaches only the specific applications their role needs, so a compromise upstream has nowhere to spread.

Core Capabilities

- **Secure Connect SASE:** converged SD-WAN and SSE cloud security with zero-trust access for stores, franchise and contractors, under centralized policy
- **Managed Detection and Response:** a 24/7 CREST-certified SOC with a 15-minute investigation SLA, for retailers without an in-house SOC
- **DDoS Mitigation:** 13 scrubbing centers and 4 Tbps of capacity, SLA-backed protection for e-commerce through peak trading
- **Managed Firewall:** next-generation firewall and intrusion prevention at every store, supporting cardholder data environment segmentation, on-premise or cloud

- **SSE Cloud Security:** six converged services including ZTNA, secure web gateway, CASB, FWaaS, secure remote access and data loss prevention, under one policy engine
- **Network Segmentation:** isolation of POS and payment from IoT, guest Wi-Fi and back-office, reducing PCI scope and containing lateral movement
- **Secure Remote Access:** encrypted per-seat access with MFA and single sign-on for field managers, merchandisers and remote workers
- **Cloud security governance:** a consistent compliance posture across edge, private and managed public cloud

THE GTT PLATFORM ADVANTAGE

Security is embedded at every layer of the GTT Envision platform, not added on top of it. GTT Envision connects, orchestrates, virtualizes and automates the enterprise network, so security policy and network policy are managed in the same place.

GTT ENVISION EDGE

At the store, GTT EnvisionEDGE puts firewall, SD-WAN and SASE in a single device, which removes separate security appliances and cuts the number of PCI-in-scope components per site. Service-chained capabilities update in near real time as threats change.

GTT ENVISION CORE

At the core, GTT EnvisionCORE orchestrates security policy centrally, so a change made once is enforced across every site at the same time and the estate stays consistent and free of drift.

GTT ENVISION DX

GTT EnvisionDX Brings security dashboards alongside network visibility, so the team sees posture and performance in one view, and it captures the documented, audit-ready evidence that keeps a certification like Kiabi's PCI Level 1 sustainable across a distributed estate.

THE PROOF

The numbers below come from GTT's retail case studies, not a deck of hypotheticals.

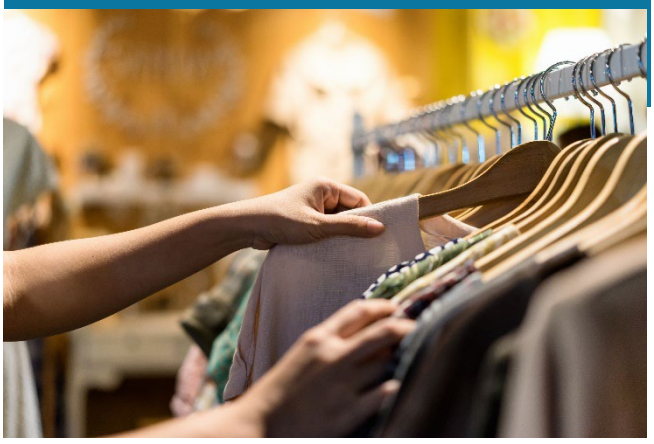
A Protected Storefront Through Every Peak

Distrelec, an electronics distributor trading across 15+ European countries, keeps 60,000 daily web visitors and more than 7,000 daily shipments moving at near 100% uptime. GTT protects the platform with cloud DDoS mitigation over the Tier 1 backbone, so traffic floods are filtered before they can reach checkout.



Compliance Proven At Scale

Kiabi runs 431 stores across 26 territories at more than 99.7% uptime and holds PCI Level 1 certification, the most stringent merchant tier. The audit-ready evidence GTT captures is what keeps that certification sustainable across a distributed estate, rather than a point-in-time pass that drifts the moment the auditor leaves.



Also proven

- Greenyard consolidated more than 30 providers to one across 25 countries, cutting cost and shrinking the attack surface that provider sprawl creates.
- Across the platform GTT stops more than 1M attacks a month before they reach a customer.
- Retailers using managed detection and response see 85% fewer breaches than those relying on a traditional MSSP alone. (Gartner, 2025)
- CREST-certified analysts staff GTT's global SOC and the platform holds ISO 27001, ISO 20000 and ISO 22301, SOC 2 and PCI certifications, with more than 2,000 security certifications across the team.

WHY GTT

One platform, one partner and a structural head start. The same SASE and SD-WAN technologies turn up on every side of a retail deal, so what separates providers is who owns the network underneath, how the managed service is run and whether security is engineered in or added later. Here is where GTT is built differently.

CONNECT WITH CONFIDENCE ON A GLOBAL TIER 1 BACKBONE AND FLEXIBLE ACCESS	SECURE EVERY TRANSACTION ON ONE PLATFORM, NOT A STACK OF POINT TOOLS	SIMPLIFY WITH END-TO-END DELIVERY OWNERSHIP
GTT runs a top-ranked global Tier 1 IP backbone with 80% of traffic on-net, so your security runs at the layer GTT owns and controls rather than over a network stitched together from regional carriers. Because the traffic stays on GTT's backbone, it can be inspected and segmented at the carrier layer, something an overlay-only provider with no WAN underlay cannot do. Flexible access through managed SD-WAN, 5G FWA and LEO satellite brings new, temporary and pop-up sites online in days, each one provisioned with its security configuration from the first day it trades, so nothing opens unprotected.	Security is built into the GTT Envision platform rather than layered on after the fact. Secure Connect SASE, Managed Firewall, MDR from a 24/7 CREST-certified SOC, DDoS Mitigation and network segmentation run as one managed layer under one policy engine, so a rule set once holds in every country and PCI scope shrinks instead of sprawling. GTT delivers the same Palo Alto Prisma Networks, Fortinet and HPE Aruba Networking platforms that show up in every enterprise RFP; what differs is managed delivery on a backbone GTT owns. Because GTT owns the backbone, the security and the cloud governance as a single control plane, posture stays consistent from the store edge to the public cloud, and GTT maintains PCI DSS 4.0, NIS2 and GDPR readiness across the estate.	Most providers bolt a managed service onto a network someone else owns. GTT owns the network backbone and the managed layer on top of it, so one partner is accountable for underlay and overlay, with one bill and one number to call. A co-management model keeps your team in control where it wants to be. The SOC runs the round-the-clock monitoring you would otherwise have to hire for, and continuous auditor evidence replaces the scramble before each assessment. Security uplifts are timed around each retailer's peak-trading windows, including the October to January freeze, so the work never collides with peak.

RETAIL SUB-VERTICALS SERVED

Where provider sprawl is worst depends on your corner of retail. The case for one partner stays the same:

SUB-VERTICAL	WHERE CONSOLIDATION SHOWS UP
Grocery & Food Retail	Margins of 1 to 3% cannot absorb a breach, POS dependence is heavy, and NIS2 now classifies major food retailers as Essential Entities, which triggers personal board liability.
Fashion & Apparel	Large customer-data repositories make brand trust the primary asset, and third-party breaches reach the brand through its suppliers.
General Merchandise & Big Box	High transaction volume and broad e-commerce exposure draw bot traffic and payment-page attacks at scale.
Luxury & Specialty	High-value transactions attract targeted fraud, and a breach damages the exclusivity the brand sells.
Health, Beauty & Pharmacy	Health-data regulations such as HIPAA in the US add another layer of compliance on top of retail payment standards.
Convenience & Fuel	Unattended payment at the forecourt, the fuel and pump area out front, put PCI compliance at the pump with no staff present, and every self-service terminal widens the surface to segment and monitor.
Consumer Electronics	High-demand launches draw bot-driven inventory hoarding, with one retailer seeing 20 million bot requests in 30 minutes during a restock. (Imperva, 2025)
Wholesale & Distribution	EDI systems, the structured messaging that moves orders between trading partners, and business email are prime targets; business email compromise moved $6.3B in fraudulent payments in 2024 (FBI IC3), and one breach can cascade across every downstream customer.

NEXT STEPS

Securing a distributed retail estate doesn't start with a rip and replace. It starts with seeing where the exposure actually is.



- **Assess the estate**. Map flat networks, unmanaged devices and PCI scope to find where a single foothold could spread and sequence the fix so the highest-risk sites and busiest trading windows are protected first. GTT can run a complimentary PCI scope and exposure assessment to start.
- **Embed security in the network**. Deploy Secure Connect SASE, four-zone segmentation, MDR and DDoS protection as a managed layer, with policy enforced centrally and compliance evidence captured continuously.
- **Talk to GTT**. Secure and compliant retail is one of four GTT pillars in GTT's retail framework, alongside resilient connectivity, cloud and operations, so the platform that protects the estate also connects it, runs its workloads and simplifies its operations.

**CONNECT EVERY STORE. PROTECT EVERY TRANSACTION.
TURN COMPLIANCE INTO TRUST.**

ABOUT GTT

GTT is a leading networking and security as a service provider for multinational organizations, simply and securely connecting people and agents to data and applications anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges. Built on our top-ranked global Tier 1 network, GTT Envision is a single global technology platform to connect, orchestrate, virtualize and automate enterprise networks, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, GTT Defense Halo™ security, internet, voice and other connectivity options, complemented by a suite of professional services and sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together. For more information, visit **www.gtt.net.**

Endnotes

External market sources.

1 Verizon, “2025 Data Breach Investigations Report (DBIR),” April 2025.

2 Computer Weekly, “M&S profits tumble after cyber attack,” 2025.

3 Reuters and CNN, reporting on the UNFI ransomware attack, June 2025.

4 McKinsey, “B2B Pulse,” February 2026.

5 PCI Security Standards Council, “PCI DSS v4.0,” 64 new requirements mandatory March 31, 2025.

6 Protegrity and Gatepoint Research, “PCI DSS 4.0 Readiness Survey,” 2025.

7 European Commission, NIS2 Directive, GDPR, DORA and EU AI Act enforcement provisions, 2024 to 2025.

8 Sophos, “The State of Ransomware in Retail 2025,” 2025.

9 Imperva and Thales, “2025 Bad Bot Report: Retail Cybersecurity Threat Landscape,” 2025.

10 Forescout, “2025 Riskiest Connected Devices Report,” 2025.

11 Cloudflare, “DDoS Threat Report for 2025 Q4,”

12 IBM and Ponemon Institute, “2025 Cost of a Data Breach Report,” July 2025.

13 ISC2, “2025 Cybersecurity Workforce Study,” December 2025.

14 Security Scorecard and Bitsight, “Supply Chain and Third-Party Risk Management 2025,” 2025.

15 CrowdStrike, “2026 Global Threat Report,” February 2026.

16 FBI Internet Crime Complaint Center (IC3), “Business Email Compromise,” 2024.

17 Gartner, “Cybersecurity Vendor Consolidation,” 2024.

18 Gartner, managed detection and response research, 2025.

