THALES
CYBERSECURITY

Trust at the Checkout: Protecting Data to Protect the Retail Relationship



cpl.thalesgroup.com

Table of Contents

Introduction	3
Why is the Retail Industry Under Threat?	4
The Threats Affecting Security Teams	5
Loyalty and Compliance Economics	6
The Compliance Reality	7
About Thales	11



Introduction

Trust Is The New Differentiator

Budgets are tight, products are expensive, and consumer sentiment is at a 70-year low. That means customers are about as intolerant as they've ever been.

Meanwhile, according to the Thales 2026 Digital Trust Index, retail is operating in a major trust deficit: only 10% of respondents pointed to the sector as the one they trust most when it comes to online interactions.

They say trust comes on foot and leaves on a horse: organizations that mishandle customer data, have unnecessary friction in customer experiences, or suffer breaches are all but sending away trust on a stallion. However charming your shop associates are, if you don't respect your customers' data, time, and experience, they won't stick around.

Today, protecting customer data is inseparable from protecting the customer relationship.



Why is the Retail Industry Under Threat?

71%

of retail organizations reported an increase in **credential theft** and **misappropriated secrets** in 2025



Retailers are high value targets for cybercriminals. Much of the reason for this is that they hold an enormous volume of personal, financial, and transactional data. Attackers can either sell that data on the dark web, or use it to inform targeted phishing campaigns, takeover customer accounts, steal finances directly, or sell on the black market.

However, there's more to the story.

Retailers have always held a trove of valuable information. That doesn't explain why the threat to retailers is becoming more severe year over year. The 2026 Thales Data Threat Report - Retail Edition provides a plausible explanation: **71% of retail organizations reported an increase in credential theft and misappropriated secrets in 2025.**

The fact is, many retailers are woefully unprepared for the reality of protecting cloud data.

The Threats are Real

Tool Sprawl

Tool sprawl is the first problem. 76% of retail organizations have five or more data protection tools, and the average retailer has seven.

Data protection stacks consisting of multiple siloed tools create coverage gaps. Fragmented telemetry forces teams to jump between dashboards, making it harder to spot attacks. Inconsistent policies lead to configuration errors that attackers can exploit. Alert fatigue proliferates as alerts from multiple tools bury critical warnings. Meanwhile, incident response slows as teams lose hours validating data across conflicting systems.

Poor Data Visibility

Tool sprawl leads to poor data visibility. Only 37% of organizations have complete knowledge of where their data is stored, and only 41% said they can classify all their data.

It's something of a tired adage, but one that still rings true: you can't protect what you can't see or understand. When retailers lose track of their data, they have no way of knowing how sensitive it is, how well it is guarded, or even if a cybercriminal has already stolen it.

Data Encryption Failures

When retailers fail to understand and classify their data, they inevitably fail to encrypt the data that matters most: 47% of retailers' sensitive cloud data remains unencrypted on average.

Encryption is the last line of defense against cybercriminals, meaning that even if attackers do enter a retailer's network, the most valuable data is unusable. Without it, even a minor breach can become a major incident.

Transaction Layer Risk

By their nature, retailers must share customer data across open, public networks. They rely on third-party payment gateways and banking networks for payment processing, transmitting delivery details to courier partners, and routing data across touchpoints for omnichannel synchronization.

When that data is in transit, it is vulnerable to interception, including man-in-the-middle attacks, packet sniffing, and eavesdropping on insecure connections. Only by protecting data in transit can retailers ensure business continuity, preserve customer trust, and deliver seamless customer experiences.

The encryption gap matters here, too. If retailers fail to encrypt and tokenize data in transit, it becomes much more vulnerable to interception.

The Stakes: Loyalty and Compliance Economics

A big part of the problem is that too many retailers view security as merely a cost center. In reality, it's essential for preventing massive financial losses, protecting customer relationships, and even driving revenue.

The IBM Cost of a Data Breach Report 2026 found that the global average breach cost rose 12%, reaching a record of USD 4.99 million after a brief dip in 2025. Retailers saw costs continue to climb, rising from USD 3.54m to USD 3.80m year on year.

Of course, much of these costs arise from activities like crisis management, public relations, downtime, and post-breach response. But customer churn is also an enormous contributor.

Consumers today are more cash-strapped than they have been in a long time. If an organization suffers a breach, customers are not going to risk identity theft or stolen funds. Many will immediately withdraw from loyalty programs and take their business elsewhere.

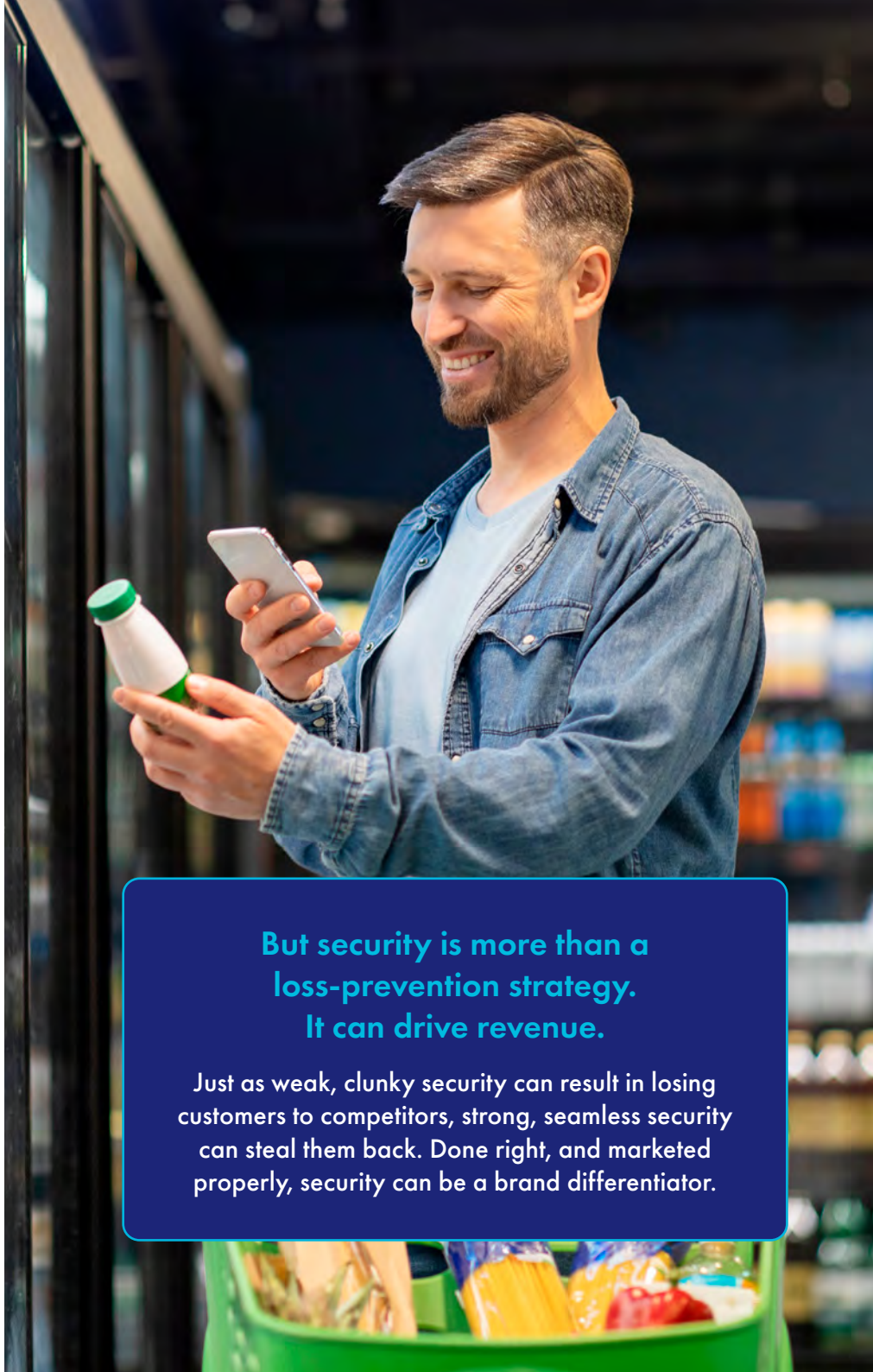
Moreover, modern consumers demand hyper-personalized experiences. For retailers, that means collecting huge volumes of data - including real-time location tracking, purchase histories, and zero-party preference data.

Customers will only provide that information if they trust the retailer to protect it: according to the Thales 2026 Digital Trust Index, 69% of consumers trust companies more when MFA is used, and 68% say the same about passkeys.

The same is true for omnichannel experiences across mobile apps, e-commerce websites, physical point-of-sale (POS) systems, and social media shopping channels. Every touchpoint is a potential entry point. If a consumer's account is compromised on the app, they will stop using both the app and stop shopping at physical stores.

That said, security cannot come at the cost of experience.

As their money is worth less in real terms, consumers demand speed and value. However secure a retailer is, if they implement heavy-handed, friction-filled security checks to prevent fraud, organizations will abandon their carts for a smoother competitor.



But security is more than a loss-prevention strategy. It can drive revenue.

Just as weak, clunky security can result in losing customers to competitors, strong, seamless security can steal them back. Done right, and marketed properly, security can be a brand differentiator.

The Compliance Reality – PCI DSS 4.0

According to the Thales 2026 Data Threat Report, Retail Edition, 67% of retail organizations that failed a compliance audit reported at least one cloud breach, compared with 33% of those that passed all audits.

As such, the simplest indicator of whether a retailer is doing security right is whether or not they can pass compliance audits, including GDPR, state privacy laws, and, most importantly, PCI DSS 4.0. The ability to pass these PCI DSS 4.0 audits, in particular, is an indicator of healthy baseline security, as the requirements map directly to the key weaknesses listed above. The most relevant PCI DSS 4.0 requirements are as follows:



PCI DSS Requirement 3: Protect Stored Account Data

Requirement 3 governs any cardholder data sitting at rest. The core mandate is to keep as little of it as possible (known as data minimization) and render all stored cardholder data unreadable through encryption, tokenization, hashing, or truncation. Sensitive authentication data like CVVs, PINs, and track data, however, cannot be stored at all after transaction authorization.

Requirement 4: Strong Cryptography in Transit

Requirement 4 mandates strong encryption for cardholder data crossing public networks, using only trusted, valid, non-expired certificates and keys. Protocols must not allow fallback to weaker or deprecated versions.

Requirement 10: Log and Monitor Access to System Components and Cardholder Data

This requirement mandates detailed audit logs capturing every user's access to cardholder data. They must cover who accessed what, when, and what action the user took.

Retailers must protect logs from tampering, review them daily for anomalies, retain them for a minimum of 12 months (with the most recent 3 months readily available), and include time-synchronized timestamps across systems for event correlation.

Requirement 12.5: Document and Validate PCI DSS Scope

Requirement 12 mandates that organizations must document and confirm their PCI DSS scope. That includes the full boundary of systems, networks, and processes that touch cardholder data, documented and confirmed once every 12 months and whenever there's a significant environmental change.

At minimum, this scoping exercise identifies all data flows across payment stages: how data enters, where it moves, where it's processed, and where it lands.

Compliance is Just a Starting Point

That said, compliance is merely a baseline, not a ceiling. It will help prevent retailers from losing customers, but it's unlikely to differentiate them from their competitors.



How Thales Helps Strengthen Customer Relationships

With Thales, retailers can go beyond just meeting PCI DSS 4.0 requirements. They can lock down data, while offering seamless customer experiences that differentiate them from their competitors. Two specific solutions offer the most value.

Data Security Solutions Protect Data at Rest

Thales CipherTrust Data Security Platform helps retailers discover, analyze, protect, and control sensitive data anywhere with next-generation unified data protection. Once retailers have located that data, they must render it unreadable.

Get a consistent data-security approach across structured and unstructured data, cloud, SaaS, on-premises, hybrid/multi-cloud, and AI ecosystems, with **Thales CipherTrust DSPM** that pairs visibility with actionable insights and meaningful remediation

CipherTrust Platform's encryption and key management capabilities encrypt cardholder data at the file, database, and application level while centralizing key lifecycle management in FIPS-validated hardware. This closes the unencrypted data gap that many organizations have. Even if perimeter defenses fail, the data itself is worthless to whoever gets it.

Moreover, because CipherTrust Platform is a unified data protection platform, it addresses the tool sprawl issue. It consolidates discovery, encryption, key management, and tokenization into a single platform, giving security teams one place to enforce policy instead of stitching together multiple disconnected tools. That, in turn, eliminates coverage gaps.

Thales CipherTrust Tokenization, meanwhile, removes raw account data from the environment entirely.

Rather than storing an actual PAN, retailers store a token that has no exploitable value outside the original system. This shrinks PCI DSS scope significantly, since the systems that only ever touch tokens are no longer part of the cardholder data environment in the same way.

CipherTrust Tokenization also means that retailers can keep supporting the workflows customers expect, like chargebacks, returns, and loyalty programs, without ever holding the raw sensitive data those workflows would otherwise require.

HSMs Secure the Transaction Layer

Thales payShield HSMs and Luna HSMs operate at the transaction layer itself - the moment a customer dips, taps, or enters their card online.

As a dedicated payment HSM, payShield handles point-to-point encryption, key management, and credential issuing at the point of sale and in e-commerce environments. Luna HSMs provide the general-purpose cryptographic foundation, generating, storing, and protecting the keys that underpin encryption, tokenization, and digital identity across the wider environment. Together they act as the trust anchor for the transaction from the instant it begins.

payShield HSMs underpin the PCI DSS 4.0 cryptography and key management requirements, but also the customer-facing experience itself. They work in the split-second between a customer presenting a card and a transaction clearing, where trust has to be established instantly and invisibly. Get that layer wrong, and no amount of downstream encryption or tokenization changes the fact that the transaction itself was exposed.

Together, Thales Cybersecurity solutions address the full lifecycle of cardholder data. That means from the moment it's captured at the point of sale, however long it needs to be stored, to the workflows built around it long after the transaction is complete.



Data Protection is a Prerequisite for Customer Relationships

Strong data protection is the infrastructure that helps retailers build customer relationships. It enables omnichannel loyalty schemes, protects customer trust, and proves that retailers take their customer's data protection seriously.

With consumer sentiment at a historic low, and customer wallets not stretching as far as they used to, that trust is the only way to prevent customers from abandoning a brand - and can even help retailers differentiate themselves from competitors.

If you're a retailer struggling to provide strong, seamless security for your customers, Thales can help. Find out more about how our solutions protect data, provide seamless customer experiences, and strengthen customer relationships.



About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.



THALES

CYBERSECURITY

Contact us

For contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com

© Thales - November 2026 • HP • v3