CLOUDFLARE

EBOOK

Peak shopping ready

Four pillars of secure omnichannel retail

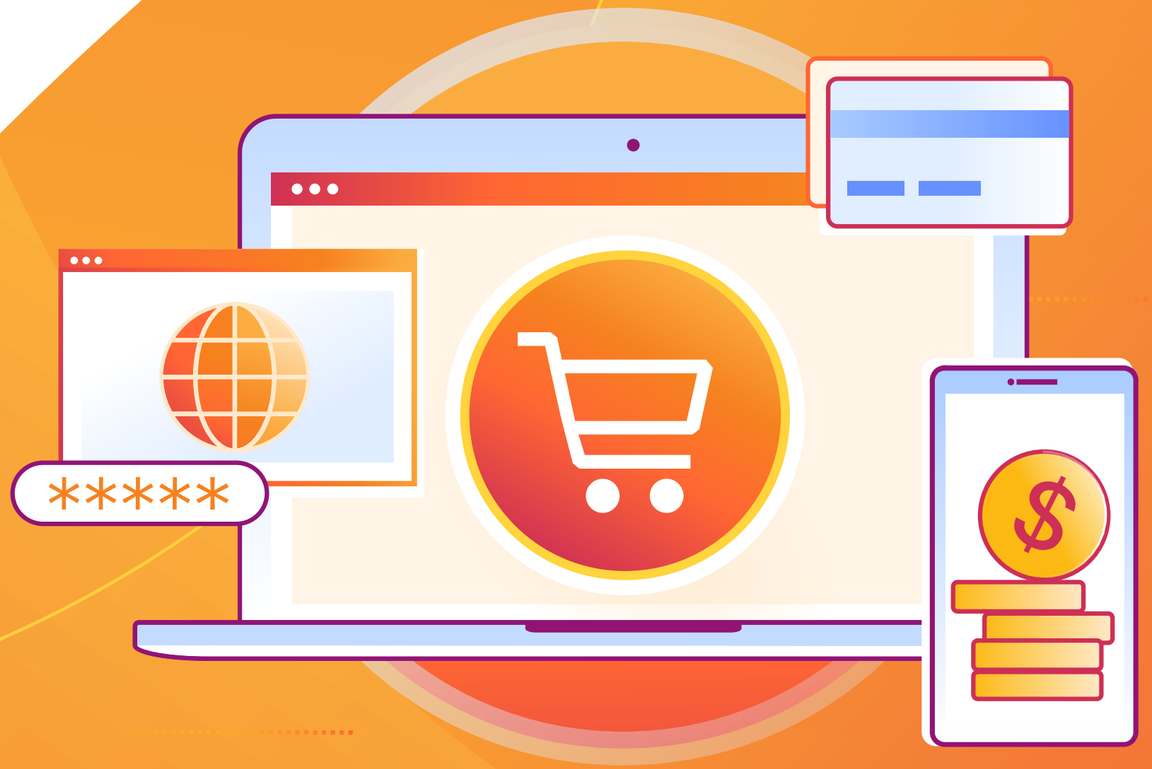


Table of contents

‘Tis the season for cyber risks and performance woes

The average **cart abandonment rate worldwide was 73.9%** in the 12 months ending July 2024[1]

73.9%

Downtime **cost retailers $287 million**, including lost revenue ($76 million) and security-related costs ($38 million) in FY2023[2]

287M

60% of surveyed US and European consumers say they **abandon purchases due to poor website user experience**[3]

60%

47% of supply chain leaders reported **systems could not handle unexpected volume spikes** during the 2024 holiday season[4]

47%

During Cyber Week 2024, **ecommerce bot activity surged to 103 billion requests**, representing up to 19% of traffic to online stores[5]

103B

There was a **200% increase in suspected fraudulent transactions worldwide** during Black Friday/Cyber Monday 2024 compared to 2023[6]

200%

Online shopping has seen the **biggest slowdown since 2012**, with **34% of US consumers delaying ecommerce** purchases due to tariff concerns[7]

34%

From code freeze to cash flow: Essential holiday IT strategies

From the first trickle of September's early-bird shoppers, to the flurry of post-holiday deal-seekers, the holiday season is an ultimate make-or-break moment for retailers.

This reality puts immense pressure on IT, security, and networking teams: site crashes, sluggish checkouts, unwanted bots, or disjointed omnichannel experiences are a direct path to lost sales. With consumers tightening budgets due to tariffs and economic headwinds, the stakes are even higher. For instance, 30% of shoppers plan to spend less during the 2025 Black Friday/Cyber Monday weekend.[8]

Before code freeze, ecommerce and retail technology leaders must prioritize strategies that protect and maximize revenue, and avoid operational chaos.

Read on for practical ways on how to protect customers, scale revenue, and avoid operational chaos this holiday season, including how to:

- **Optimize performance for holiday traffic surges**
- **Protect against fraud and threats to customer-facing apps**
- **Secure access to customer and supplier data**
- **Upgrade omnichannel experiences with real-time engagement**

By addressing these areas ahead of the "golden quarter," retailers can achieve their holiday goal: a boost in revenue cheer.

Priority #1: Optimize performance for holiday traffic surges

Excess demand strains infrastructure and teams

Operational resilience is non-negotiable in the holiday retail season. Customer retention and revenue growth depend on great user experiences, from any device: reliable website and app results; fast load times of media-rich experiences; and secure and seamless checkouts.

However, Internet applications deployed on a global scale are highly susceptible to outages or downtime due to spikes in traffic (whether legitimate or malicious), network latency, and server outages at the origin.

When retail and ecommerce infrastructure is overwhelmed with requests, apps can face challenges in performance (timely responses), availability (consistent uptime), and scalability (dynamic resource adjustment).

For example, without elastic cloud infrastructure, resource-intensive AI-powered experiences (voice/video-based AI assistants, virtual try-ons) can create latency. Additionally, increased requests to origin servers raise network and server load, increasing bandwidth, egress, and compute costs.

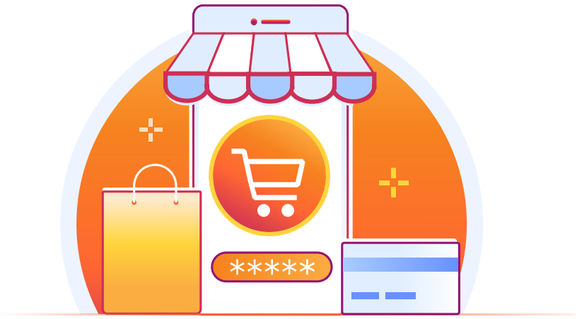
Although 70% of supply chain executives entered the 2024 holiday rush confident in their fulfillment systems, only 42% achieved successful system performance when demand hit its highest points.[9]

What is needed: Integrated application services with cloud-scale infrastructure

Downtime or degraded performance can be caused by a number of issues — from the expected (spikes in visits, more bandwidth-heavy product videos), to the unexpected (local ISP outages, bugs when deploying new app features), and malicious (credential-stuffing attacks, DDoS botnets).

Regardless of the cause of infrastructure strain, averting downstream problems requires an application services platform with cloud-scale infrastructure.

Assess if a vendor can easily and seamlessly absorb Internet traffic on the highest-traffic days* based on their SLAs for:



Content delivery, including:

- ✓ **A content delivery network (CDN)** to cache and optimize content at the edge for any customer's device, browser, and bandwidth needs
- ✓ **A cloud-native image pipeline** to optimize and dynamically serve images for any device/connection speed
- ✓ **End-to-end video streaming** that delivers video close to customers at the ideal quality

Traffic routing and distribution, including:

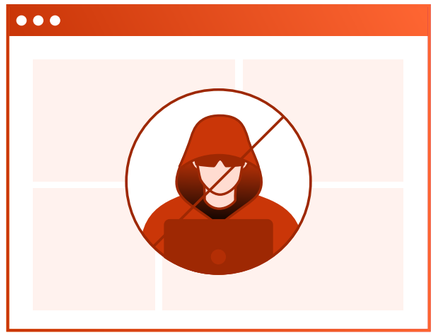
- ✓ **Load balancing** to distribute traffic among multiple servers, which enhances app availability and minimizes latency
- ✓ **Intelligent, real-time routing** of web traffic (such as to/from logistics portals) to the fastest network paths
- ✓ **Globally distributed routing** to absorb large-scale attacks while maintaining high availability
- ✓ **Virtual waiting rooms** to route excess visitors (for example, during a timed product release) in orderly queues

Edge delivery infrastructure, including:

- ✓ **Local failover** for store point-of-sale when cloud connections fail
- ✓ **Autonomous, edge-based protection** to mitigate DDoS and other attacks at scale
- ✓ **An app development platform** that lets you deploy AI-driven experiences from the edge

**Ideally, the vendor's network would be proximate to your retail store/warehouse footprint to minimize latency across delivery and fulfillment systems.*

Priority #2: Protect against fraud and threats to customer-facing apps



Dynamic hybrid environments complicate timely detection and response

Cyber attackers intensify their efforts during the holidays, mirroring consumer trends. Black Friday 2024, for example, saw significant increases in DDoS attacks and malicious bot activity on ecommerce platforms. Visa also reported a 200% surge in suspected fraudulent transactions globally during the 2024 Black Friday/Cyber Monday weekend compared to 2023 — largely attributed to attackers leveraging AI.[10]

As attackers accelerate their use of AI-enabled tools to bolster their efficiency, authenticity, and volume of attacks, retailers must take a proactive, predictive security posture.

At the same time, security must extend to the distributed retail workforce and real-time apps that are connected to the sprawling supply chain ecosystem. For instance, as Joe Ohr, COO of the National Motor Freight Traffic Association (NMFTA) described, "Criminals are increasingly using cyber tactics to impersonate drivers, falsify load documents, exploit digital load boards and reroute shipments. These tech-driven schemes are harder to detect — and far more costly."

The average cost of a retail data breach jumped 18% to $3.48 million from 2023 to 2024.[11]

Retail organizations took longer to identify and contain breaches compared to the global average across industries.[11]

What is needed: Security optimized for real-time systems and the mobile workforce

Many organizations recognize the value of a combined web application and API protection (WAAP) platform — which Gartner has called "the preferred choice for protecting public-facing services, as they combine broad scope, scale and security controls specific to web apps and APIs."[12] However, security must also extend to the mobile workforce and real-time internal systems — such as shipping and logistics APIs — across the retail chain.

To minimize attack surface risks while simplifying management, look for a unified security platform that can:

- **Provide robust threat intelligence** across many attack surfaces — and automatically apply this intelligence to all security services
- **Protect apps and delivery APIs against bots** attempting inventory scraping, credential stuffing, and other fraudulent activity
- **Throttle excessive and abusive requests** against apps and APIs across customer, store, and vendor touchpoints
- **Secure APIs from business logic-based fraud**, such as attacks targeting account creation and payment workflows
- **Enforce least-privilege access controls**, no matter where third-party partners (like delivery drivers) are located or data is stored
- **Hide internal systems and private applications** from the Internet and would-be attackers
- **Detect insider threats**, such as unsanctioned app usage, to prevent data leaks and compliance violations
- **Detect the use of leaked stolen credentials**, before end-user accounts are compromised
- **Continuously monitor for browser-based attacks** like payment skimming
- Encrypt sensitive payment data in transit with the latest TLS protocols, and **scan for PCI DSS (Payment Card Industry Data Security Standard)** compliance

Priority #3: Secure access to customer and supplier data

High-risk users and distributed systems need access to sensitive data

Retailers face heightened vulnerability due to their sprawling ecosystem of third parties (e.g., distributors, manufacturers, suppliers, warehouses), high employee turnover, and a mobile workforce that regularly handles customer payment and supplier data.

They are particularly susceptible to attack vectors beyond the corporate perimeter.

Phishing and social engineering attacks that target employees via email, SMS, and collaboration apps to steal credentials and defraud businesses

Double brokering scams where attackers steal payments and goods by impersonating transportation and freight companies who act as middlemen between suppliers and retailers

Ransomware holding critical systems hostage, as seen in the November 2024 ransomware attack on a supply chain management company servicing GAP, Walgreens, and others

Zero-day exploits that target vulnerable edge devices like unpatched firewalls, risky virtual private networks (VPNs), or improperly encrypted point-of-sale (PoS) systems

Poorly managed delivery APIs that may provide avenues for attackers to steal credentials or authentication tokens

For retailers handling large amounts of consumer data globally, traditional perimeter-based controls like VPNs are inadequate, and appliance-based tools struggle to comply with evolving standards like PCI DSS 4.0 and the EU General Data Protection Regulation (GDPR).

UK retailer Marks & Spencer incurred approximately £300 million in costs after an April 2025 cyberattack disrupted operations for weeks. Attackers broke in through social engineering techniques aimed at a third-party contractor.[13]

What is needed: A phased approach to zero trust for secure access

Retailers should ensure no one ever has completely unfettered, trusted access to all apps or resources within their systems. This requires ensuring no user or device is trusted by default, regardless of their location or prior access.

Enforcing the zero trust principle of “least privilege access” will give workers, third-party vendors, and systems access only to the data and systems absolutely necessary for their role.

While fully maturing to a zero trust architecture is typically a long-term undertaking, here are some of the fastest ways to start layering protections:

Conduct cybersecurity awareness training for employees before the inevitable flood of seasonal attacks begin. While this is not foolproof, the human element of certain attacks (such as phishing and double brokering scams) calls for a human defense.

Adopt an AI-powered email security service capable of proactively uncovering new phishing schemes, tracking new tactics used by threat actors in real time, and blocking campaigns before users can click on malicious links in texts or emails. Depending on your preferred vendor and deployment, this can take just a few clicks to start.

Implement multi-factor authentication (MFA) with hardware-based security to protect networks even if attackers gain access to employee credentials.

Migrate payment systems and other apps regularly accessed by in-store workers to ZTNA. Zero trust network access (ZTNA) verifies every request between any user and app based on identity, device posture, and other context. Look for a vendor offering clientless ZTNA (no need to install software on devices), which enables ZTNA deployment to remote workers in days, rather than weeks or months.

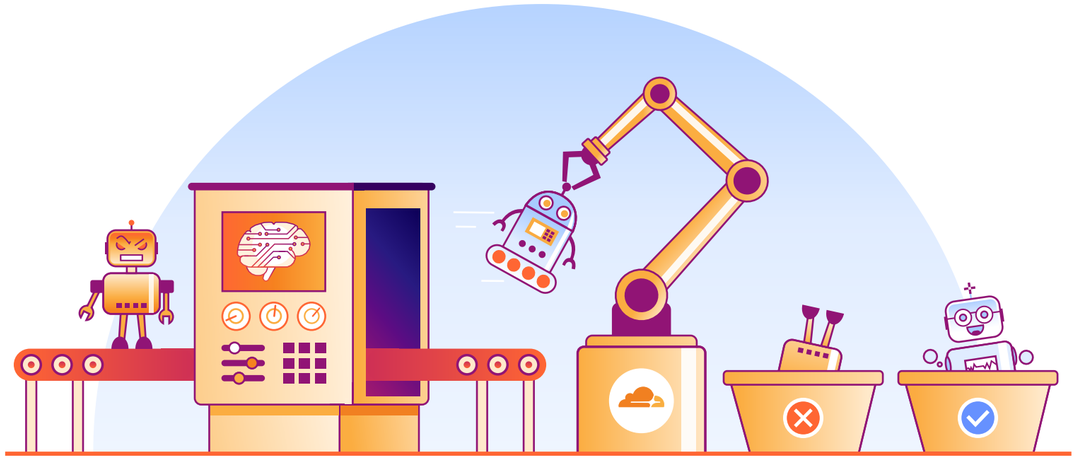
Priority #4: Upgrade omnichannel experiences with real-time engagement

Inefficient and disjointed infrastructure add friction

From ecommerce to in-store digital shelves, to AI agents (such as customer-facing, partner/supplier, store associate support, and internal development tools), real-time engagement is retail's next battleground.

With so many different ways to "click and collect" or "click but abandon," most customers (80%) are uncommitted to a specific type of shopping format or experience.[14] Retailers must deliver compelling, consistent experiences throughout.

However, legacy systems often make it difficult to bridge online and offline retail experiences in real time. For example, when customers:



...discover and research options:

- Slow loading times and site crashes during viral moments and peak traffic force customers elsewhere.
- Customer data silos hinder timely personalization and dynamic merchandising.
- Limited development architectures and GPU resources hinder support for AI-powered technologies.

...validate purchasing preferences:

- Content delivery bottlenecks add latency for high-impact visuals (virtual try-ons, "shop the look" searches, 3D product views, in-store screens).
- Product discrepancies, such as online pricing not honored offline or "phantom inventory," erode trust.
- Unlinked customer service channels waste customers' time.

...attempt to complete purchases:

- Attacks and false positives stop legitimate purchases, while real payment fraud slips through.
- Clunky mcommerce experiences, and missing payment or shipment options, drive cart abandonment.
- Dozens of specialized retail systems acting as islands create manual processes, delays, and other errors.

What is needed: Modernization options to bridge legacy retail and AI-powered omnichannel

While some of the world's largest retailers have successfully integrated AI, GenAI, computer vision, and other emerging technologies into their omnichannel strategies, others lack the necessary infrastructure — and risk falling behind.

Consider "Acme," a hypothetical, longstanding retail company with offices spanning multiple countries and thousands of employees (remote, contractors, developers). They operate hundreds of brick-and-mortar stores, as well as multilingual websites and apps for different audiences. Their distributed systems process vast amounts of data, often in silos.

For modern, real-time customer engagement, retailers like Acme need to connect all the systems that deliver:

- Personalized offers and loyalty programs
- Customer intelligence
- Dynamic demand and supply planning
- Real-time inventory management
- Data privacy and security

A connectivity cloud helps by delivering fast, secure "any-to-any" connectivity and programmability across environments — from legacy IT to systems that build or consume AI. This simplifies infrastructure and accelerates time-to-market for new retail experiences.

A connectivity cloud is a good fit for retailers looking to integrate how they:

Unify data, including real-time customer, product, and inventory queries, from multiple sources in numerous locations — without adding latency

Leverage an API-first approach to connect multiple specialized retail systems

Protect data, apps, and large language models (LLMs) at the edge

Run AI model inference at the edge, closest to customers and the mobile workforce, to help accelerate digital experiences

Dynamically process and deliver content, such as in-store video, augmented reality (AR), AI shopping assistants, and more from locations closest to users

Prevent site crashes, attacks, and breaches without slowing down legitimate transactions

Fulfill holiday shopper demands with Cloudflare's connectivity cloud

To some degree, all of the challenges described in this guide are driven by loss of control in the digital environment — or, put another way, the difficulty of managing an ever-expanding galaxy of apps, clouds, users, devices, network infrastructure, and more.

Cloudflare's connectivity cloud helps retailers of all sizes overcome this digital complexity. It is a unified platform of cloud-native security and connectivity services that protect, connect, and accelerate everything, everywhere.

With our extensive global network and an integrated suite of tools, Cloudflare ensures that organizations can harness the power of AI while safeguarding their systems, defending against emerging threats, and accelerating app development.

These services help retailers embrace the technologies they need to stay digitally advanced — and focus on what matters: increasing sales.

“With Cloudflare, we easily manage millions of customers and ensure their connections are working and secure before traffic reaches our infrastructure. It is seamless — buyers and sellers benefit without ever knowing Cloudflare is part of the equation.”

shopify

Learn more >

“Cloudflare is the first line of defense for all our public web and ecommerce properties. Everything is centralized, automated, and intuitive — we can see what’s coming and mitigate threats in real-time.”

FOSSIL

Learn more >

“Switching to Cloudflare, our system was 27% faster overnight. It improved our performance right off the bat — cache rates jumped immediately and things just started flowing … The UI was much simpler too — using Cloudflare rather than our legacy tool, I no longer felt like I was working in an early 2000s data center.”

PACSUN

Learn more >

“Every year we braced for the swarm of Black Friday visitors onto our websites. Now, thanks to the massive scalability of Workers and the Cloudflare global network, we know the system is not going to fall over during peak season — we no longer worry about whether our websites can handle the surges in traffic.”

THG

Learn more >

Ready to fortify your retail operations for the holiday season and beyond?

Cloudflare provides everything you need to accelerate your digital transformation, improve your operational efficiency, and deliver a best-in-class customer experience.

Contact us

to prepare for your most successful holiday season yet.

> **“In the past, we were always in planning mode — spending time figuring out if we needed to add hardware to support the next sales promotion. Black Friday took months of planning. Now we don’t have to give it a thought. Scaling happens automatically.”**
>
> **Michael Glauche**
> Cloud Infrastructure Architect, C&A

Resources

1. Feger, Arielle. “Cart abandonment benchmarks: Which categories have the highest and lowest rates.” Emarketer, 12 Dec 2024, https://www.emarketer.com/content/cart-abandonment-benchmark--which-categories-have-highest-lowest-rates
2. Mohanty, Anubhav, et al. “The hidden costs of downtime: The $400B problem facing the Global 2000.” Oxford Economics, 23 July 2024, https://www.oxfordeconomics.com/resource/the-hidden-costs-of-downtime-the-400b-problem-facing-the-global-2000/.
3. Storyblok. “60% of Consumers Abandon Purchases Due to Poor Website User Experience, Costing E-Commerce Companies Billions.” Storyblok, 20 Dec. 2022, www.storyblok.com/mp/poor-website-user-experience.
4. Lett, Josh. “Peak 2024: Why Only 42% of Supply Chains Hit Their Mark.” Retail Dive, 10 Feb 2025, www.retaildive.com/spons/peak-2024-why-only-42-of-supply-chains-hit-their-mark/739105/.
5. Jaisinghani, Avi, et al. “Grinch Bots strike again: defending your holidays from cyber threats.” The Cloudflare Blog, 23 Dec 2024, https://blog.cloudflare.com/grinch-bot-2024/.
6. “Visa Helps Holiday Shoppers Stay Secure, Blocking Nearly 85% More Suspected Fraud Globally This Cyber Monday Compared to Last Year.” Visa, 17 Dec. 2024, https://investor.visa.com/news/news-details/2024/Visa-Helps-Holiday-Shoppers-Stay-Secure-Blocking-Nearly-85-More-Suspected-Fraud-Globally-This-Cyber-Monday-Compared-to-Last-Year1/default.aspx. Accessed 11 Aug 2025.
7. Revell, Eric. “Trump’s Tariff Policies Reshape Online Shopping Habits, New Report Finds.” Fox Business, 2 July 2025, www.foxbusiness.com/economy/trumps-tariff-policies-reshape-online-shopping-habits-new-report-finds.
8. Reynolds, Justin Paul. “Report: How Brands Can Assuage Shoppers’ Concerns About Tariffs.” Chief Marketer, 3 Aug 2025, www.chiefmarketer.com/how-brands-can-assuage-shoppers-concerns-about-tariffs/.
9. Lett. “Peak 2024: Why Only 42% of Supply Chains Hit Their Mark.” www.retaildive.com/spons/peak-2024-why-only-42-of-supply-chains-hit-theirmark/739105/.
10. “Visa Helps Holiday Shoppers Stay Secure, Blocking Nearly 85% More Suspected Fraud Globally This Cyber Monday Compared to Last Year.” Visa, 17 Dec. 2024, usa.visa.com/about-visa/newsroom/press-releases.releaseId.21101.html. Accessed 11 Aug 2025.
11. Berthiaume, Dan. “The average cost of a retail data breach is…” Chain Store Age, 5 Aug 2024, https://chainstoreage.com/average-cost-retail-data-breach.
12. Gartner Research. “Critical Capabilities for Cloud Web Application and API Protection,” Gartner, 31 Aug 2022, www.gartner.com/en/documents/4018252.
13. Darley, James. “M&S Cyber Attack One of the Costliest in UK Retail History.” Technology Magazine, 10 June 2025, https://technologymagazine.com/articles/m-s-cyber-attack-one-of-the-costliest-in-uk-retail-history.
14. Russell, Zachary. “Survey: Majority of shoppers visit multiple retailers, compare prices.” Chain Store Age, 12 June 2025, https://chainstoreage.com/survey-majority-shoppers-visit-multiple-retailers-compare-prices.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-8087.2025AUG22