5 Tips to Boost Peak Season Sales When Brand Loyalty Is Dead

Commerce industry playbook

The commerce industry is facing a complex network of pressures

Workforce

- New employee expectations
- Growing wage pressures

Technology

- **Service delivery innovation**
- **Omnichannel gaining traction**

Decreased brand loyalty

- Lingering economic uncertainty
- Weak customer confidence
- Value-conscious behavior

Global factors

- Rising inflation
- Global supply chain disruptions
- Sustainability awareness
- Geopolitical tensions

Commerce organizations are battling for shrinking wallet share

Macroeconomics and inflation threaten discretionary spending, causing customers to tighten their belts.

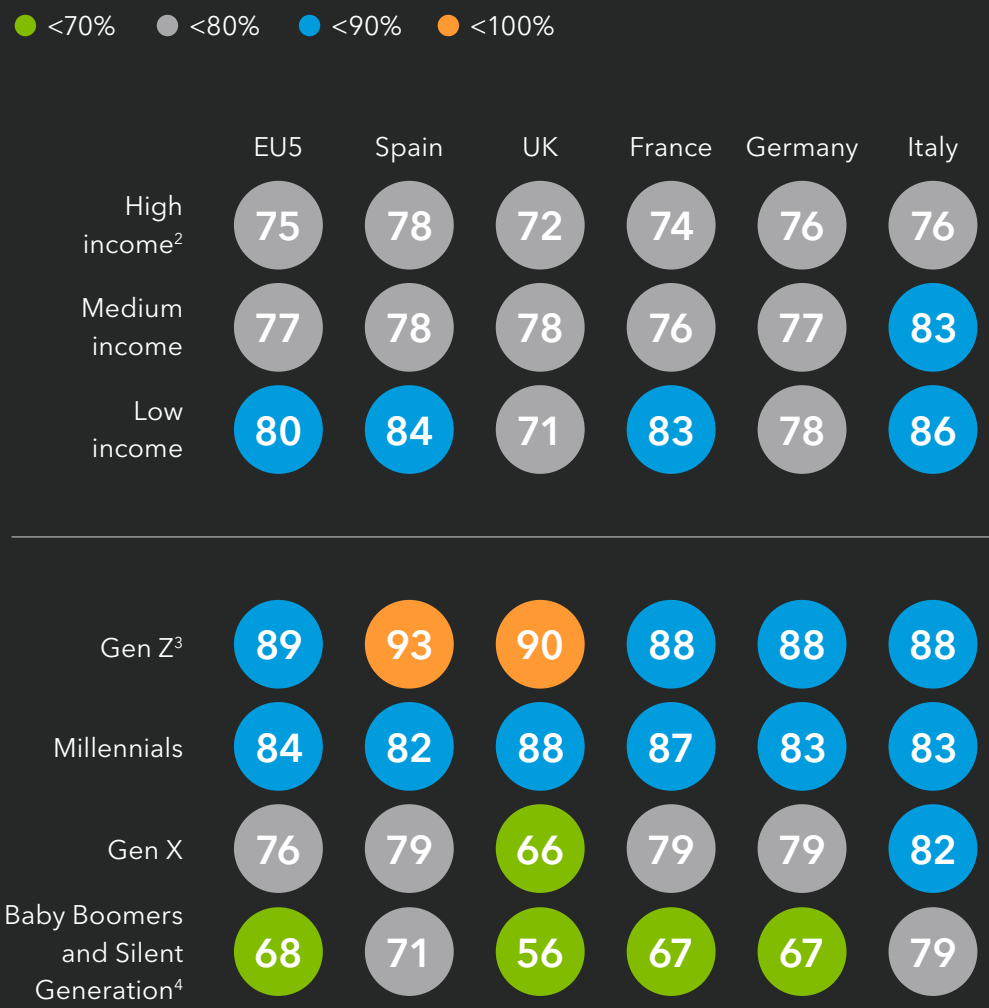
Year-over-year growth in fashion retail sales, %

Note: China includes mainland China only; Europe includes Western and Eastern Europe.

Source: McKinsey Global Fashion Index; McKinsey State of Fashion Forecasts

Consumers traded down to cope with price increases.

Percentage of respondents changing their shopping behavior and trading down, by generation and income[1].



Note: EU5 = Spain, UK, France, Germany, and Italy
[1]Question: Within the past 3 months, have you done any of the following when purchasing [product]?
[2]High (n = 1,344); medium (n = 2,027); low (n = 1,151). Thresholds are based on individual country statistics.
[3]Gen Z = ages 18-26 (n = 769); millennials = ages 27-42 (n = 1,232); Gen X = ages 43-58 (n = 1,496); baby boomers and Silent Generation = ages 59+ (n = 1,525).
[4]The demographic cohort born between 1928 and 1945, preceding baby boomers.

Source: McKinsey ConsumerWise EU5 Sentiment Data, Nov. 2023 (n = 5,022)

Even holiday spending has been restrained

While consumer spending still picks up during the holiday season, shopper spend per visit has declined even lower than mid-pandemic levels.

2021 – 2023

40% in ANZ

21% in Japan

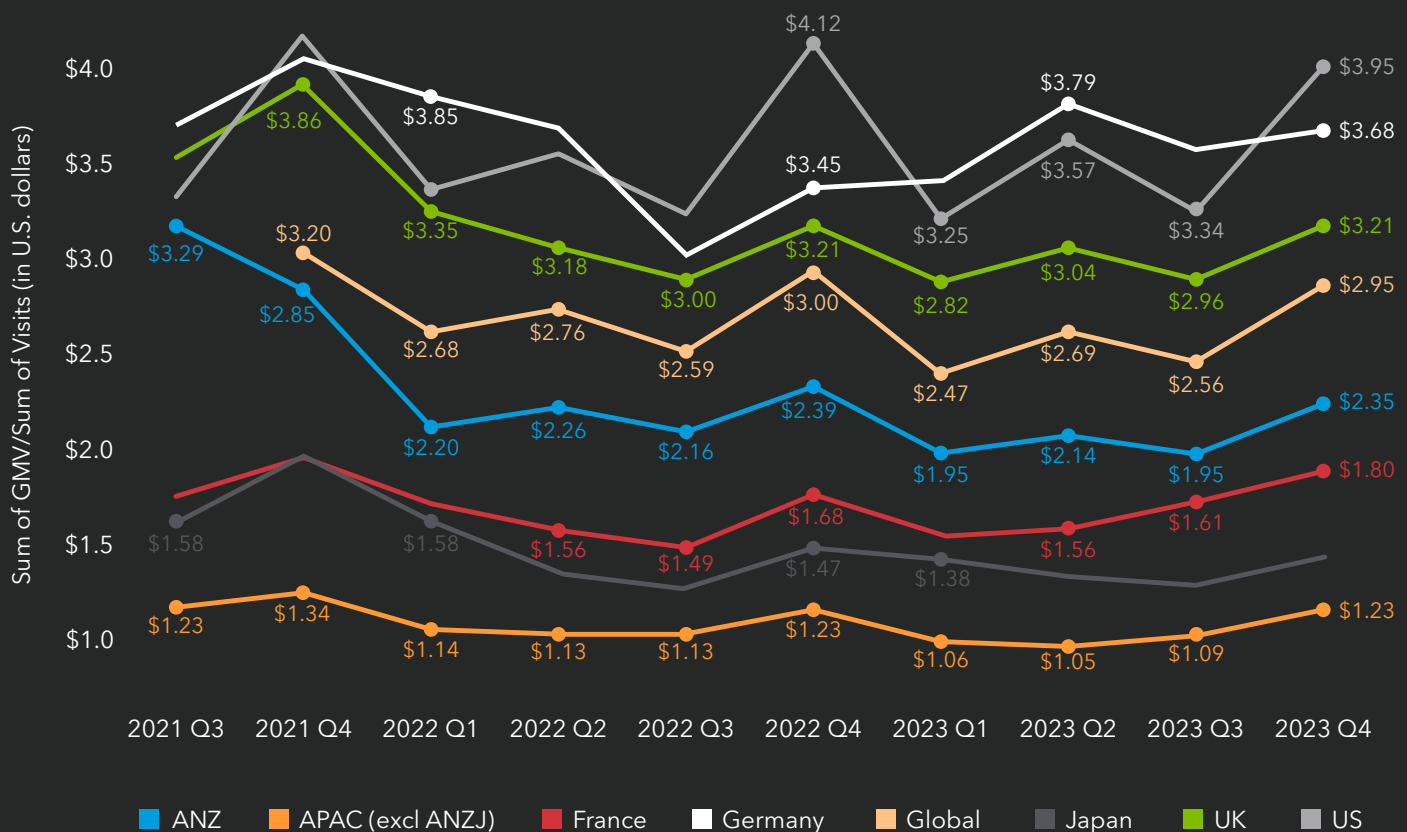
17% in UK

8% in APAC (excluding ANZ and Japan)

5% in US

Shopper spend per visit

Multiple values



Source: Salesforce

Customers are increasingly price driven

Macroeconomic pressures have driven customers to be price conscious and seek better deals instead of prioritizing product quality.

Consumers say they've switched brands for the following reasons

Base: Consumers who switched brands in the past year

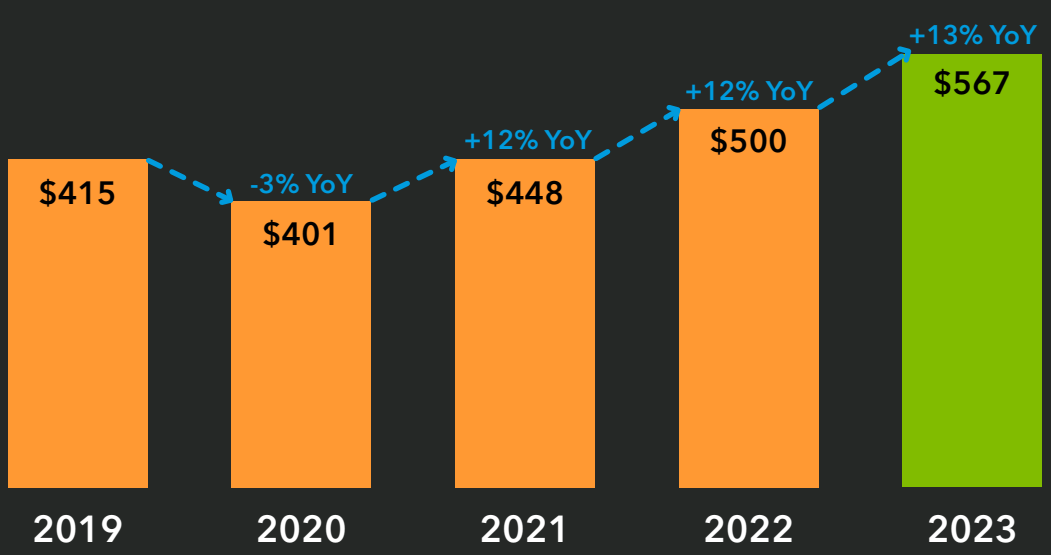
Source: The Connected Customer, Salesforce

Hype events can help boost sales

Whether it's El Buen Fin in Mexico, the lead-up to the Diwali festival in India, Cyber Monday in the United States, or Boxing Day in Australia, there's increasing demand for online retailers to provide fast and consistent experiences across their online channels during these peak sales periods.

Consumers increase their spending during Black Friday-Cyber Monday (BFCM) year over year, reaching new highs

Average expected BFCM week spend



Question: "Approximately how much do you expect to spend on gifts (for others and yourself) during BFCM?" (n = 956)

Source: 2023 Deloitte Black Friday-Cyber Monday survey analysis

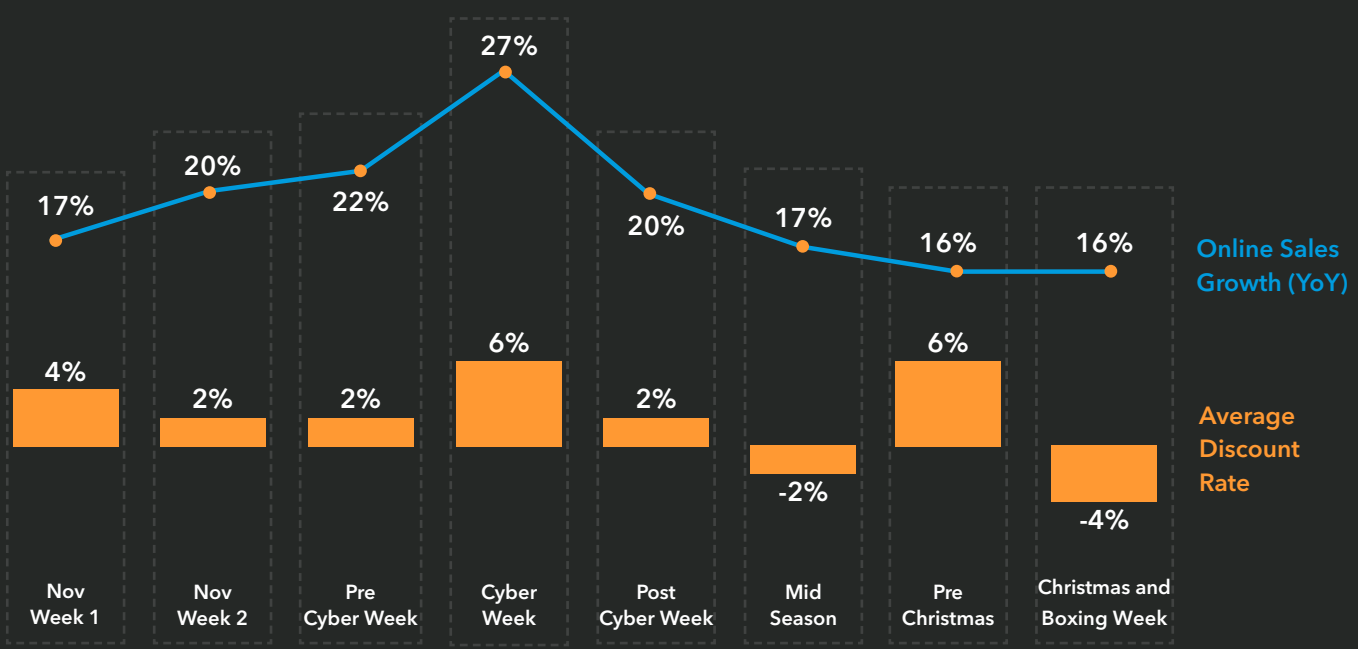
But customers will wait for the best deals

Customers have wised up to flash sales and are delaying or planning their purchase decision for these events.

Even though they hurt margins, flash sales and offers are now part of the cost of business for ecommerce players.

Instead of launching a flash sale event on a single day, retailers now opt to release a few specials each day, as the risk and complexity of a one-day launch outweighs the potential additional revenue.

When did shoppers spend, and when did they score the best discounts?



Source: Salesforce

Flash event customers are driven by deals, not brands

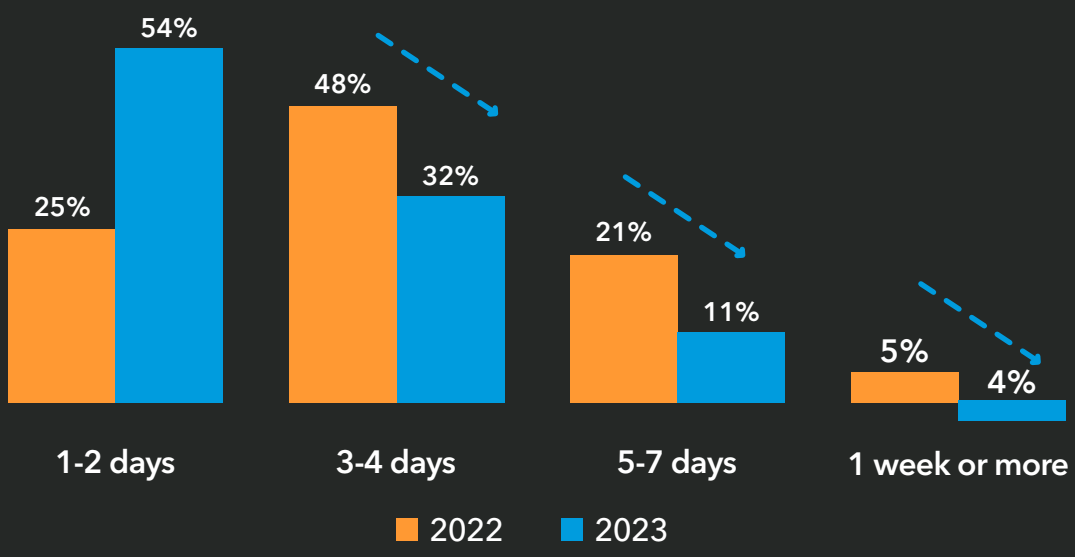
There is diminished brand loyalty as customers are willing to wait for deals. However, they expect fast delivery and some degree of personalization when they do make that purchase.

1 in 2 customers will wait for deals during online sales.

2 in 3 customers will purchase again if there is some degree of personalization.

At the same time, customer tolerance for delivery delays has declined – **9 in 10 customers** expect online orders to arrive in four days.

How long customers are willing to wait for online orders beyond the expected delivery date, 2022 & 2023



Note: Parcel Monitor collects billions of anonymized parcel tracking data points from more than 130 countries annually.

Source: Parcel Monitor

> Gen Zers … have so much information and so many options available to them so quickly that it can be overwhelming and keep them from deeply experiencing one product or brand.

– Alfonso Dolce, CEO of Dolce & Gabbana in an interview with McKinsey & Company

How do retailers boost peak season sales when brand loyalty is declining?

5 tips to boost peak season sales

1. Protect loyalty accounts (and points)
2. Prevent brand impersonation
3. Protect customers during hype events
4. Ensure third-party visibility
5. Bake in future-proof resilience

Tip #1:
Protect loyalty accounts (and points)

Leading retailers are forging emotional connections with loyal customers through long-term brand-building exercises – sealing product and shopping relevancy at every opportunity.

Brands now bake respect for their loyal customers' preferences into their omnichannel marketing communications, personalized recommendations, reward options, and payment alternatives.

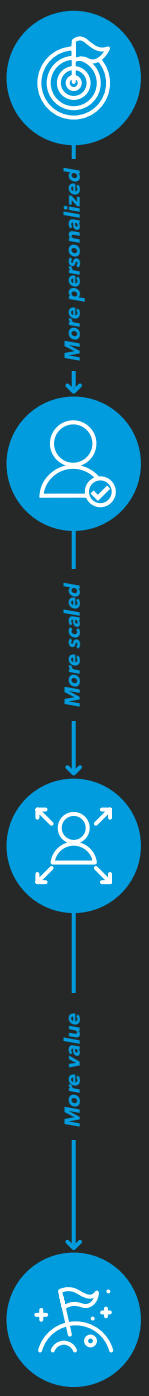
However, curating the right brand experience for your loyal customers requires extensive customer data, and in some cases, financial information. All of this data can be collected, sold, and traded, or even compiled for extensive profiles that can later be used for crimes such as identity theft.

According to Akamai research, cybercriminals target vulnerabilities in the existing workflow and supply chain to steal personal information or cash out reward and loyalty points.

Protecting loyalty program data (and points) is the first step to ensuring that you can continue to deliver true value to your regular customers.

Quickly detect and stop malicious activity without adding friction

The loyalty evolution: From program to platform



Base functionality and targeting

Establish loyalty program with basic functionality (e.g., earn and burn, offers) with the ability to personalize at a high level.

Interconnected designs with customer-level targeting

Introduce advanced features (e.g., surprise and delight, paid) and unlock microsegmentation/ customer-level targeting.

Expanded loyalty value proposition with internal and external assets

Connect company's own services, offerings, and external partnerships in one integrated experience to fulfill customers' cross-sectoral needs.

New monetizable businesses built on top of loyalty

Build new sources of value – services, formats, and journeys – with assets created by loyalty (e.g., data, paid/subscription programs, retail media network).

Source: McKinsey & Company

Tip #2:
Prevent brand impersonation

Customers won't hesitate to click on links from their favorite brands – especially when expecting special deals during hype events. They may willingly give away their credentials and payment information when they trust the brand.

Protecting the brand is critical when threat actors are targeting commerce customers with fake websites and accounts. If the online experience is not secure, customer satisfaction dips, and revenue follows downhill.

Unfortunately, fraud and abuse continues to plague the commerce sector, with threat actors constantly shifting their tactics and techniques to evade detection and follow the money.

Audience hijacking is estimated to disrupt 15% – and sometimes more – of a brand's total ecommerce site visits. These unwanted behaviors can take several forms, including unauthorized ad injections performed by price comparison and coupon extensions.

Retailers must be able to quickly detect and stop abuse – without adding unnecessary friction to the customer path to purchase.

Prevent online fraud and abuse, and strengthen your site integrity

87%

said that preventing malicious ad injection from causing financial harm to customers was very or extremely important (51% said this was extremely important).

87%

said that providing better control over the end-to-end customer journey to improve customer experience was very or extremely important.

83%

said that preventing unauthorized ad injection from interrupting customer experience was very or extremely important (100% said at least somewhat important).

82%

said that preventing browser extensions from redirecting customers to competitors' sites was very or extremely important.

Source: Awareness of Audience Hijacking Among Online Retailers (Only available in English)

Tip #3:
Protect customers during hype events

Because hype sale events last such a short time, it is challenging to manage from the defender's point of view and requires some preparation.

Thanks to high-profile events, malicious bots target commerce customers through more web scraping and scalping attempts.

It's very important for the bot management product to be able to detect the typical attack vectors by default and have an adequate response strategy applied.

Protecting each step of the workflow is essential to have as many opportunities as possible to screen the traffic to differentiate bots from humans.

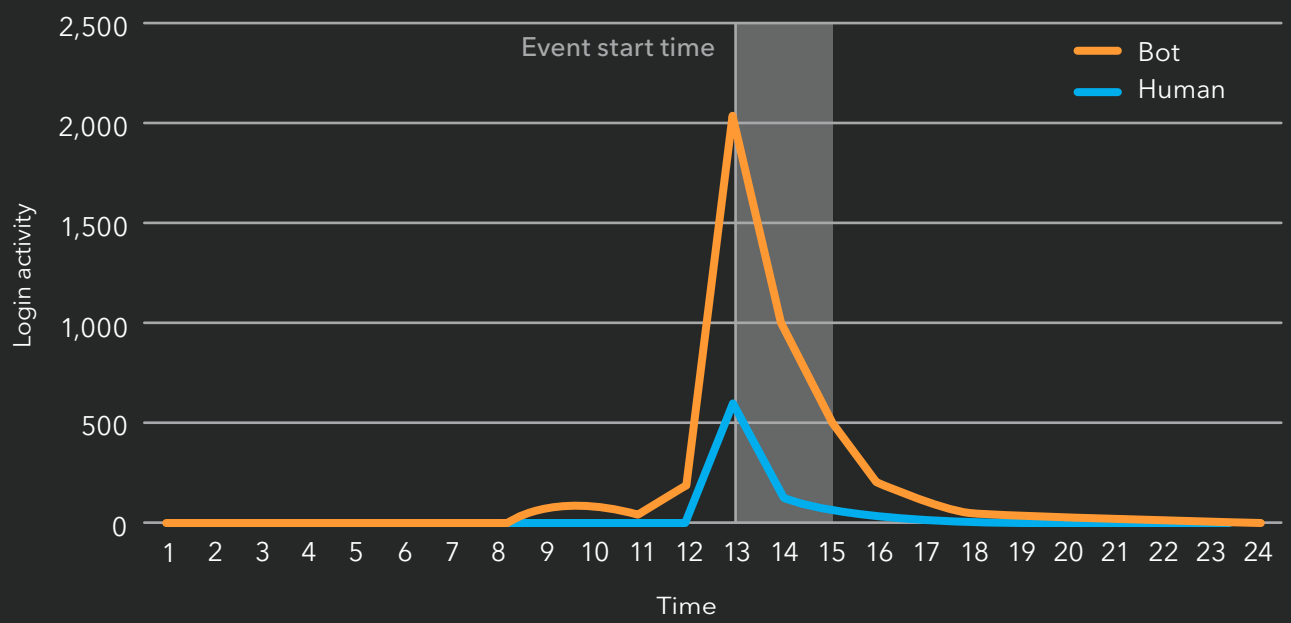
This starts before the event itself, and having a rolling sales window approach ensures a consistent experience for customers regardless of where they are based around the world.

As other countries and geos come online, retailers should leverage automated processes within their CDN to push this traffic to the site and allow different segments to view sale content. Stop the most dangerous, evasive bots before they erode customer trust.

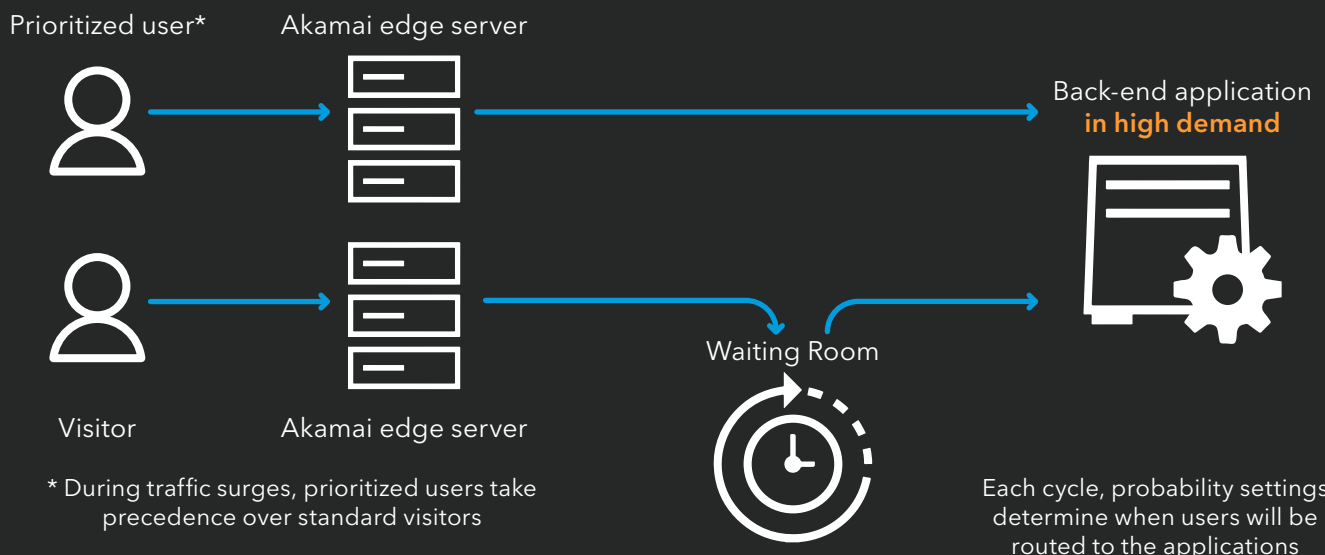
Stop the most dangerous, evasive bots, before they erode customer trust

Exceptional digital experience during hype events necessary for customer retention

Hype event traffic pattern – checkout endpoint



Prioritizing which traffic gets access to the back-end infrastructure



Tip #4:
Ensure third-party visibility

Brands are embracing live streaming during hype events.

In fact, over 60% of the top 58 Tmall/ Taobao live-streaming channels, each with over RMB 100 million in gross market value, are operated by brands rather than individual influencers.

During the 2023 Double 11 sale in China, live streaming contributed 20% of total sales.

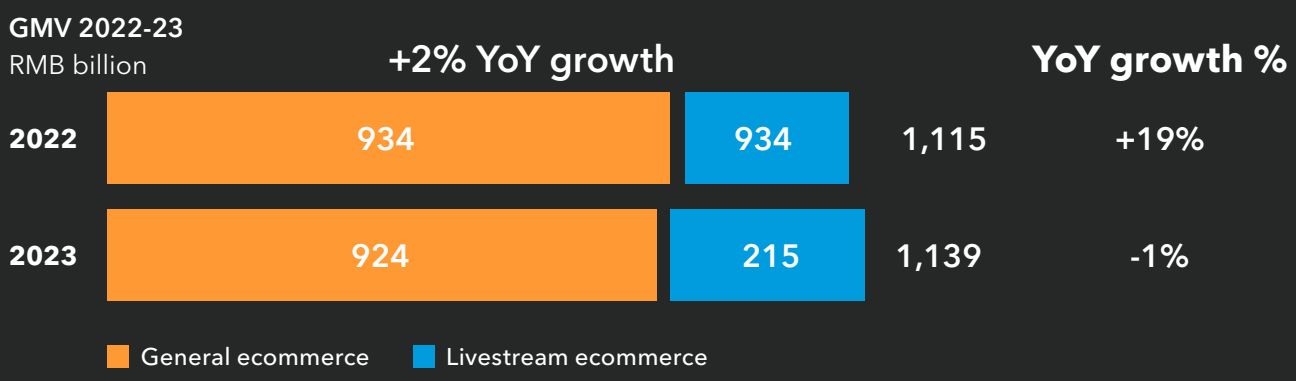
Delivering such rich and engaging digital interactions requires ecommerce organizations to partner with third-party organizations through APIs.

Typically, half of the JavaScript that the commerce vertical uses comes from third-party vendors, who tend to use open-source libraries.

This can expose retailers to new vulnerabilities in client-side attacks like web skimming and Magecart attacks, where JavaScript libraries are abused via exploitation of security flaws.

It is critical to put mechanisms in place that detect these attacks to remain compliant with new PCI DSS v4.0 requirements.

Double 11 shopping festival GMV growth



B2C ecommerce including Tmall, JD, PDD, et al.
Including Diantao (Taobao livestreaming), Douyin, Kuaishou, et al.
GMV on general B2C ecommerce platforms, e.g., Tmall, JD, PDD, and Diantao; Top 10 categories comprise 82.2% of total GMV

Source: Press search; Syntun, McKinsey & Company

Tip #5:
Bake in future-proof resilience

A potential ransomware attack may mean store operations and online commerce grind to a halt as critical systems and servers are inaccessible. The goal of these campaigns is disruption rather than financial enrichment. The attackers understand that if they go after a business's ability to make money and support their customers, that business will be more willing to pay a higher ransom.

It could also mean that credit card data and sensitive customer information is stolen and sold on the dark web, causing further damage to brand reputation and the bottom line. Cybercriminal groups offering ransomware as a service are some of today's biggest threat actors focusing on business disruption and reputational damage.

As a result of this relentless game of cat and mouse, defenses of the past can't keep up. Traditional cybersecurity methods often focus on the perimeter to keep ransomware and other attacks out of the corporate IT environment. Perimeter-based strategies are less effective against modern attacks due to infrastructure changes such as the migration to the cloud and a distributed workforce.

Network segmentation not only prevents an attacker from moving laterally and reaching strategic assets and crown jewels in the network, but also helps reduce the blast radius by creating boundaries between servers in the network and limiting the network traffic among them.

As running an online commerce site increases in complexity, retailers strive to balance the demands for security and agility, often firefighting point problems instead of directing their digital strategy. The focus will need to shift from cyber response to cyber resilience.

Top-tier organizations trust Akamai to deliver performance that protects trillions of digital interactions worldwide.

BONUS: CISO Checklist for a Successful Hype Event

- ☐ Do we have any postmortem or success stories from last year's sales period we can review?
- ☐ Can we analyze previous years' traffic, through Google Analytics or other tools?
- ☐ Can we review traffic patterns from this year, and ask ourselves: What does the year-over-year (YOY) or month-over-month (MOM) traffic look like?
- ☐ What is our social media following like compared with last year – do we have a larger presence in our social following that could affect avenues of traffic to our site?
- ☐ How many email addresses do we have in our CRM, and what are our typical click-through rates for these types of campaigns?
- ☐ How much of our in-store traffic is supporting our online channel?
- ☐ Do we understand the demographic of our holiday shoppers? Are they baby boomers who look online to find a deal before shopping in a store? Or are they the 22% of millennials that plan to not set foot inside a retail store?
- ☐ What sort of geographic traffic do we have? Are we catering to an audience across different countries or time zones, which may impact the waves of traffic that occur on the site?
- ☐ Are we aware of what the split of traffic is between desktop and mobile?
- ☐ What kind of devices usually access our site? Are they high-end devices, or low-end devices that might not be as responsive?
- ☐ Have we ensured we are mobile friendly?
- ☐ Are we running any TV or radio commercials that may lead to a spike in traffic at certain times of the day?
- ☐ How are we planning on distributing our sales URLs to our customers? Email, social, TV, or other channels?
- ☐ Can we segment our customers into groups such as repeat purchasers, highest-basketed customers, and other key value segments – whether through third-party analytics, or other A/B targeting tools, that allow us to cookie or differentiate our high-value customers?

In Summary

Over 50% of commerce websites use third-party scripts on which they have little to no visibility, increasing overall risk. The fact that there are so many new types of APIs enabled by cloud services creates major architectural challenges for IT security to accurately discover, inventory, analyze, test, and protect APIs today.

Visibility and observability consume time and scarce resources. The current tech talent crunch imposes a challenging limit for CISOs to conduct the monitoring necessary to protect the digital experience.

As a result, many commerce organizations lack visibility across their entire API estate, leaving them vulnerable to a variety of attacks and threats.

Leading enterprises are turning toward a more strategic effort with trusted partners who can offer a comprehensive solution to combating fraud and fending off hackers.

Simpler is better for lean security teams. Gain the unfair advantage by partnering with a vendor that has scale, capacity, reach, and visibility into what's happening on the internet.

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences – helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 05/24.