Akamai

SURVEY REPORT

# Awareness of Audience Hijacking Among Online Retailers

RETAILDIVE

Custom content for Akamai by studioID

Ecommerce revenue now comprises a larger percentage of overall retail sales than ever before. An analysis of data from the U.S. Department of Commerce shows that 19% of all retail sales transactions now take place online and that ecommerce spending has increased a remarkable 50% since 2019 — driven by the COVID-19 pandemic. To capture this valuable digital revenue stream, retail brands are investing heavily in personalization, loyalty programs, and optimizing website and online checkout experiences to drive bottom-line results.

But all these efforts are for nothing if customers are diverted to competitors' sites at the last minute — or worse, lured to phishing sites designed to steal their credit card numbers or personal financial data. This is exactly what audience hijacking tactics can do if you're not following the right strategy to protect your retail brand.

Audience hijacking is now a widespread phenomenon that involves unwanted — and sometimes even malicious — activities taking place within an online shopper's own browser. To enhance and personalize their in-browser experiences, many shoppers install browser extensions or plug-ins that find coupons or offer price comparisons. Sometimes these browser extensions are unknowingly installed on the consumer's device for malicious purposes. While retail businesses can leverage some of these extensions to funnel traffic to their sites — or retain customers there — other extensions can divert visitors away from the intended journey, allowing competitors and malicious actors to disrupt ecommerce experiences that retail brands have carefully crafted.

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. This occurs when such extensions inject competitor ads into the retailer's site and divert shoppers from completing a transaction. Another form of audience hijacking, affiliate fraud, results from an extension's operator hijacking a site visitor's journey to claim credit for affiliate sales they didn't actually make.

To better understand how industry stakeholders are thinking about this problem, we recently partnered with Retail Dive to survey more than 75 digital marketing, IT security, and technology leaders in retail or ecommerce organizations with at least 1,000 employees. Nearly all were familiar with the basic concept of audience hijacking (or customer journey hijacking, as it's also known), but few had access to the kind of visibility needed to determine the extent of the problem within their own company.

**19%**

of all retail sales transactions now take place online

**50%**

increase in e-commerce spending since 2019

**15%**

of a brand's total ecommerce site visits estimated to be disrupted by audience hijacking

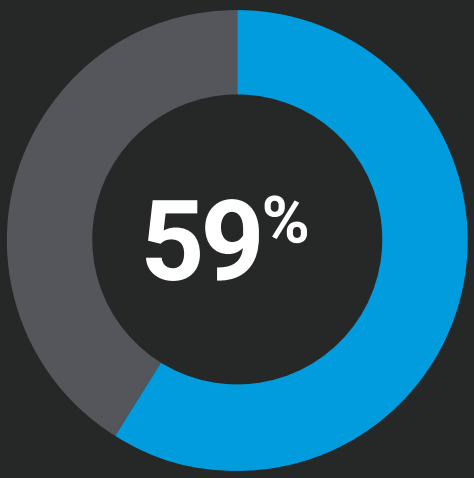
The results — along with current retail industry data, which reveals that cart abandonment for unknown and unknowable reasons remains frustratingly common — underscore why retailers can no longer ignore the problem of audience hijacking.

This was particularly true in 2022 as retailers faced mounting pressures, including inflation, waning consumer confidence, and economic uncertainty that's expected to last through 2023. As a result, many shoppers are tightening their budgets, making it more important than ever for retailers to drive online brand loyalty while curtailing inefficiencies and losses. In today's retail landscape, every sale matters.

Many retail organizations, however, lack actionable insights as to how pop-ups and browser extensions interact with user sessions, which can lead to audience hijacking. The good news: It's now possible to obtain the visibility necessary to reduce or even eliminate audience hijacking. New audience hijacking prevention technologies are available that can detect and protect against in-browser threats or unwanted activity occurring on a shopper's device when they visit your website. With the right solution in place, it's possible to analyze and monitor client-side browser sessions — without invading customer privacy — so that you can implement business rules or make informed decisions to better protect your customers and their digital journeys.

While audience hijacking is most commonly thought of as a security and fraud prevention solution, the technology can also enable you to protect — and possibly even increase — revenue. In this way, such solutions can help retailers drive better business outcomes — and profitability.

Read on to discover our top three findings from the survey.




of survey participants said that audience hijacking disrupts more than 15% of visits to their brand's site

**Finding 1:**

# Retailers understand that audience hijacking is a significant problem that is negatively impacting digital experiences on their sites — and costing their brands loyalty and revenue.

When asked, a significant majority of survey participants (85%) said they were at least somewhat familiar with the concept of audience hijacking. As many as 72% said that they were very or extremely familiar with it. This finding (Figure 1) highlights that — at least among stakeholders within midsized to large retail organizations — there's broad awareness of the problem.

How familiar are you with the concept of audience hijacking (sometimes also referred to as customer journey hijacking) and its impact on ecommerce and digital retailers?

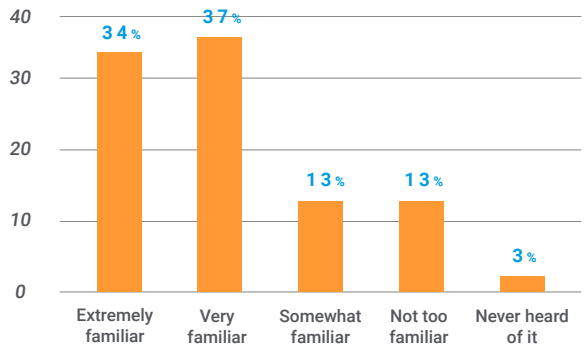



*Fig. 1*

Furthermore, when asked whether audience hijacking presented a major challenge to their organization, a large majority (82%) of survey participants generally agreed that it was. Nearly one-third of respondents (32%) strongly agreed with the statement (Figure 2).

To what extent do you agree or disagree with the following statement: "Audience hijacking presents a major challenge for my organization"?

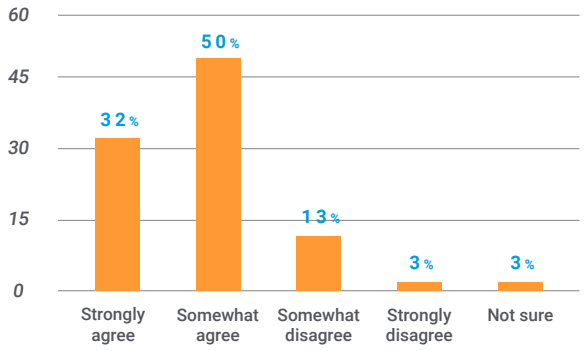



*Fig. 2*

What's more, a much larger percentage of respondents reported that unwanted pop-ups and malicious ad injections were disrupting a statistically significant number of visits to their brand's site (Figure 3). In fact, 59% said that more than 15% were impacted by audience hijacking tactics. Out of this same group, 16% of respondents reported that 25% or more of user sessions were being disrupted by some form of this malicious or unwanted activity. For large online retailers, this could equate to millions of dollars in lost revenue.

Although it represents a small subset of participants, it's still important to note that 6% of respondents had no idea how many digital purchasing journeys were interrupted or damaged by customer journey hijacking. For these retailers, audience hijacking blind spots might be creating a bigger threat to online revenue than they realize.

**What percentage of site visits or digital purchasing journeys do you believe are currently being disrupted by unwanted pop-ups and malicious ad injections created by scripts running in the shopper's browser?**

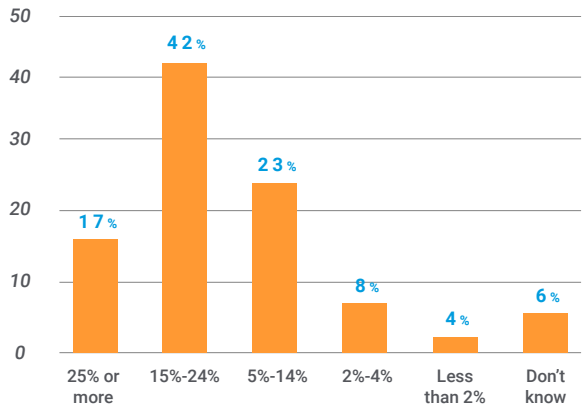



*Fig. 3*

When asked about specific aspects of their audience hijacking problem, respondents noted that most were seen as a significant problem or a severe problem.

## Problems with audience hijacking

**54%**
said that encountering fraudulent offers — which not only damage CX but also result in customer financial data theft or other material losses — was a significant or severe problem.

**50%**
said that having unwanted (and sometimes malicious) pop-up ads divert or redirect customers away from their ecommerce site was a significant or severe problem.

**49%**
said that affiliate fraud (in which third parties claim credit for affiliate sales they didn't make) was a significant or severe problem.

**44%**
said the fact that partnerships with third-party shopping app providers are less profitable than hoped for was a significant or severe problem.

**41%**
said that coupon browser extensions automatically injecting coupon codes at checkout for products customers may have been willing to pay full price for was a significant or severe problem.

It's worthy to note that while all the damaging effects of audience hijacking are perceived as problematic, those associated with fraud including customer-impacting fraud and affiliate fraud, which does direct financial harm to merchants — were more likely than any other to be ranked as a severe problem (22% said that fraud resulting in the theft of customers' financial data or other material losses was a severe problem; 18% said this of affiliate fraud).

**Finding 2:**

# Retailers lack visibility into exactly what's going on during site visits, particularly in terms of extensions, ad injections, and scripts running within the customer's browser.

Although today's retailers invest heavily in every aspect of digital experience management, they're still unable to explain why a large number of cart abandonments occur. As many as 82% of respondents say they lack visibility into the causes of cart abandonment for 5% or more of online transactions, or they simply don't know how often shopping carts are abandoned for reasons they can't determine. Of this group, 30% cannot explain cart abandonment for 15% to 24% of user sessions — a significant number of lost customer conversions (Figure 4).

This points to a critical lack of visibility at the moment of conversion, even though this moment is the most important point in purchasing journeys that digital retailers have spent millions to optimize.

How often are carts abandoned for reasons that marketing or digital experience teams within your organization cannot explain?

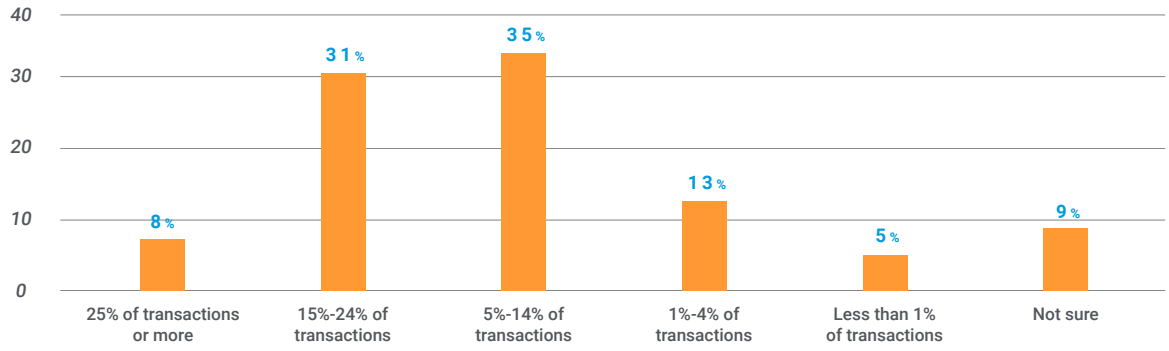



*Fig. 4*

Survey participants report that they've already implemented an array of tools and solutions to gain visibility into how browser extensions, add-ons, and customer-installed widgets (or software that's running within the shopper's browser, unbeknownst to them) impact sessions on their site (Figure 5). The largest group, comprising 67% of respondents, says that their organization has implemented a digital experience analytics platform to give them visibility into this area.

However, it's important to note that all or nearly all digital experience analytics solutions currently on the market provide insights into what's occurring on the host (retailer's) side of the session, not the client (customer's) side.

A minority (22%) of respondents said that their organizations rely on session recording to provide them with this visibility. Session recordings, however, need to be manually reviewed, a time-consuming process that makes it impossible to comprehensively monitor for fraudulent activity that may be taking place in as many as 15% to 24% of user sessions. There's also no way of identifying in advance which sessions are most likely to have been impacted by fraudulent or revenue-damaging activities.

We were surprised to see 51% of respondents indicate that they had implemented an audience hijacking protection platform leveraging artificial intelligence (AI) or machine learning (ML) to monitor client-side browser extension activities. While such solutions can and do provide deeper visibility into causes of cart abandonment and the incidence of affiliate fraud and coupon code/ad injection, they've only recently become available on the market, and market penetration, even among larger retailers, has not yet reached 51% (or anywhere close to it).

**What tools or solutions do you currently use to gain visibility into how browser extensions, add-ons, and other browser widgets interact with customer sessions on your ecommerce site?**

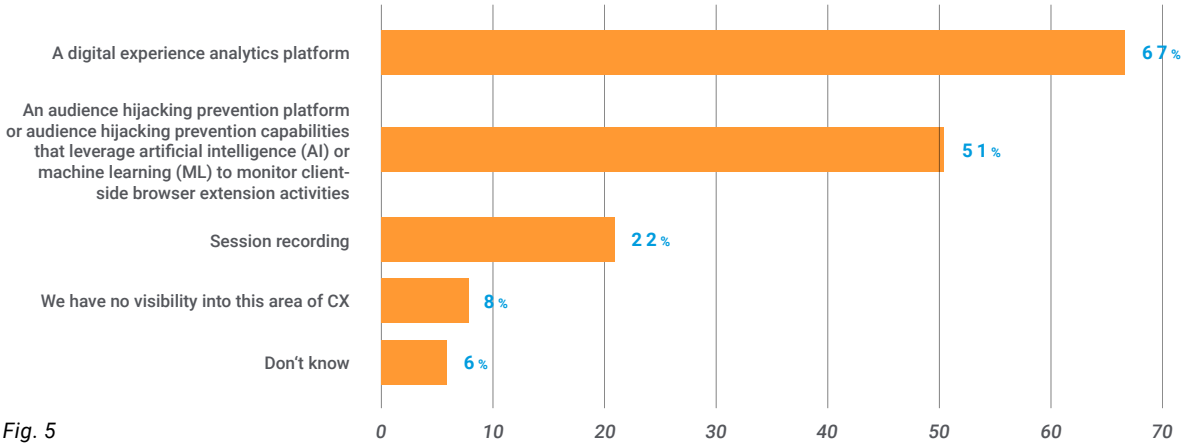



*Fig. 5*

We can only speculate, but we wonder if survey participants misunderstand the capabilities of their current digital experience management toolsets.

Our suspicions in this area were furthered by responses saying that having enhanced visibility into their customers' in-browser behaviors would greatly improve their ability to implement effective, evidence-based marketing strategies and improve customer experience (CX) (Figure 6).

When asked, 94% of survey participants said that such visibility would lead to an improvement in their ability to implement effective, evidence-based marketing strategies. And 68% of respondents said that enhanced visibility into in-browser behaviors would have a very large or extremely large impact on their ability to implement evidence-based marketing strategies and boost digital CX.

Having this visibility would also make it possible for retailers to assess whether their relationships with third-party browser extensions and shopping tools were helping or harming their revenue.

A majority of survey participants (83%) reported that their organization leverages either an in-house or partner-operated browser extension as part of an existing promotion strategy. Over one-third (35%) of respondents said their brand offered its own custom-built browser extension (which, presumably, could not be leading to revenue losses).

As many as 45% of those surveyed are partnering with third-party operators to leverage browser extensions to offer coupons or discount codes to online shoppers (55% of respondents said they do so). However, in many cases, retailers may be engaging in partnerships without a clear means of determining whether third-party extension operators like Amazon Assistant are, in fact, luring customers away from their site by showing them lower-priced offers elsewhere. There's a clear need for concrete evidence to reveal whether these partnerships are delivering the hoped-for value.

**How much would increased visibility into in-browser behaviors improve your ability to implement more effective, evidence-based marketing strategies and improve CX?**

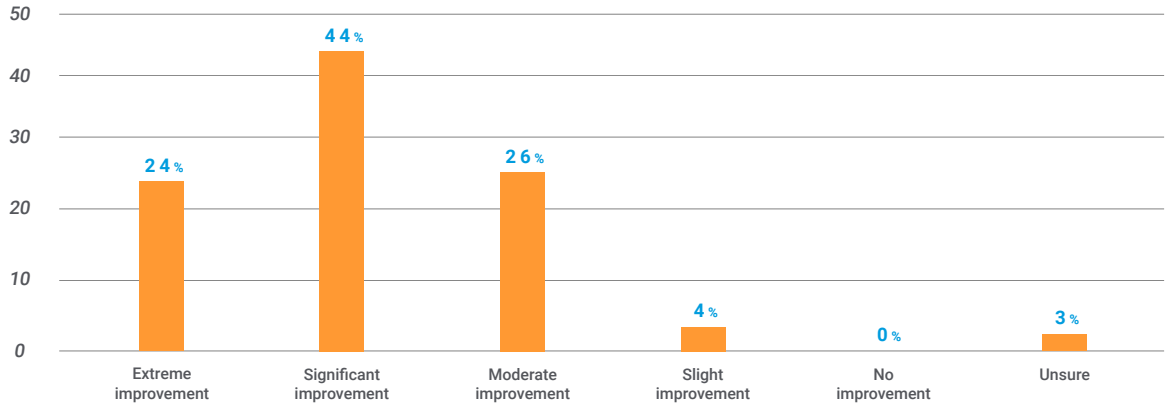



*Fig. 6*

**Finding 3:**

# Because of a lack of visibility, retailers tend to underestimate the likelihood that audience hijacking is causing churn or disrupting customers' digital journeys.

We saw this disconnection when 15% of survey participants said that audience hijacking wasn't a major challenge for their organization, yet 90% were seeing user sessions disrupted by such activities. Some admitted that they entirely lacked visibility into audience hijacking's prevalence.

This lack of visibility also surfaced when we observed respondents note the widespread inability to diagnose causes of cart abandonment in large numbers of sessions.

Regardless, audience hijacking continues to have a major impact on retailers (Figure 7). As many as 28% of respondents report that its biggest impact is revenue loss, and 23% say that it is compromising ROI on digital marketing investments. Nearly one-quarter of respondents (23%) indicate that audience hijacking has diminished their customers' loyalty, and 17% say it's causing fewer shoppers to make repeat purchases from their ecommerce stores.

**Describe the impacts of audience hijacking tactics on your business.**

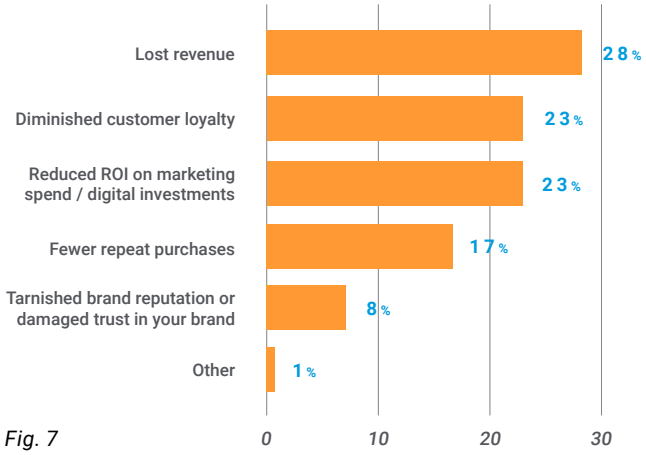



*Fig. 7*

In addition, when survey participants were asked about nine different use cases for an audience hijacking protection solution, most said that nearly all of the use cases were very or extremely important for their organization.

## Audience hijacking protection solutions

**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.

**80%**
said that blocking competitors' ads from appearing on their site was very or extremely important.

**76%**
said that reducing cart abandonment was very or extremely important.

**73%**
said that decreasing or eliminating affiliate fraud was very or extremely important (44% said this was extremely important).

**71%**
said that enhancing visibility into user sessions was very or extremely important.

Particularly given the economic headwinds that the retail sector currently faces, it's no surprise that every one of these priorities matters to stakeholders within this industry.

One piece of good news is that solving this problem is increasingly seen as a cross-organizational priority, with marketing, user experience (UX), IT security, IT operations, and fraud/risk management teams collaborating to address the problem and choose solutions (Figure 8). IT operations/security teams are involved in technology purchasing decisions in this area in two-thirds (67%) of respondents' organizations. Marketers or digital marketers are involved in more than half (51%) of organizations.

All too often, in the past, digital marketers and IT security professionals operated in silos and had little impact on one another's decision-making. It's encouraging to see that retailers may be moving toward a future in which this is no longer the case.

For today's midsized to large retail organizations, IT security, fraud prevention, user experience (UX), and digital marketing teams all have important roles to play in ecommerce revenue protection (Figure 9).

In our survey, 59% of respondents said that IT security and/or IT operations teams were responsible for protecting ecommerce revenue, but in nearly one-quarter of organizations (24%), marketing or marketing operations had a significant role to play as well, and in another 24% of companies, website management or UX also took on responsibilities in this area.

As many as 73% of survey participants said that marketing operations or CX/DX teams in their organization partner with IT or IT security teams when making decisions about which CX technologies to implement. This represents far more widespread collaboration than was common in the past.

Audience hijacking is a far-reaching problem, and the full extent of it is often difficult to understand, visualize, and measure. Such collaborative approaches are exactly what's needed to address the challenges of this scope.

**Which department or cross-functional team within your business would be responsible for purchasing a solution to prevent affiliate fraud?**

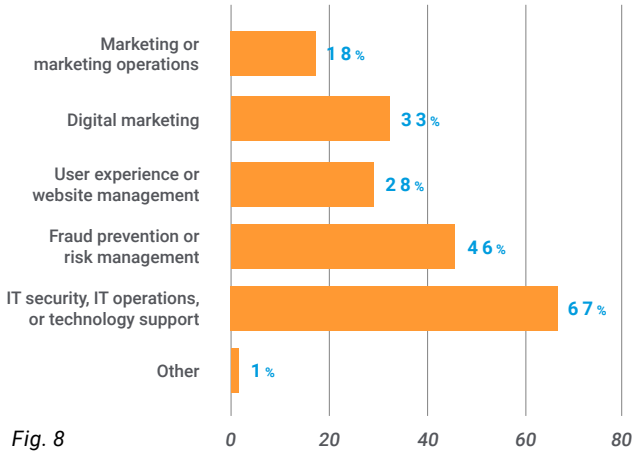



*Fig. 8*

**Within your business, which team or teams are responsible for ecommerce revenue protection?**

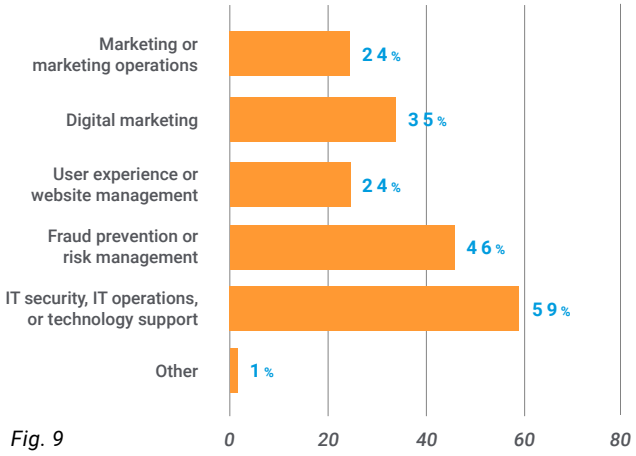



*Fig. 9*

# The future of audience hijacking protection

Amidst recession fears and mounting inflation, the current retail landscape is a challenging one. It's imperative that retailers maintain their margins and drive revenue in all possible ways if they're to emerge from these challenges on a strong footing. Preventing audience hijacking is an effective strategy for doing so: It protects carefully crafted online customer experiences, safeguards brand reputation, and helps reduce lost sales.

A new solution to the growing challenge of audience hijacking is now available. Akamai Audience Hijacking Protector can help retailers defend themselves and their customers from this growing threat across all online in-browser environments, including mobile. It gives digital retailers and ecommerce brands granular visibility into in-browser behaviors, with the ability to block audience hijacking tactics at the browser extension level. Audience Hijacking Protector also provides a comprehensive view into how affiliate fraud and malicious frameworks are impacting a brand's site traffic — and enables mitigation in real time. This helps to ensure that your customers will have successful engagements and consistent, frictionless online experiences to improve conversion rates and strengthen brand trust.

In the past, maintaining robust security and top-notch user experiences were often seen as objectives that were inherently at odds with one another. With Akamai Audience Hijacking Protector, you can address both issues through a holistic approach. This makes it possible to drive business value, reduce fraud, and take control of your customers' digital experiences — all at once.