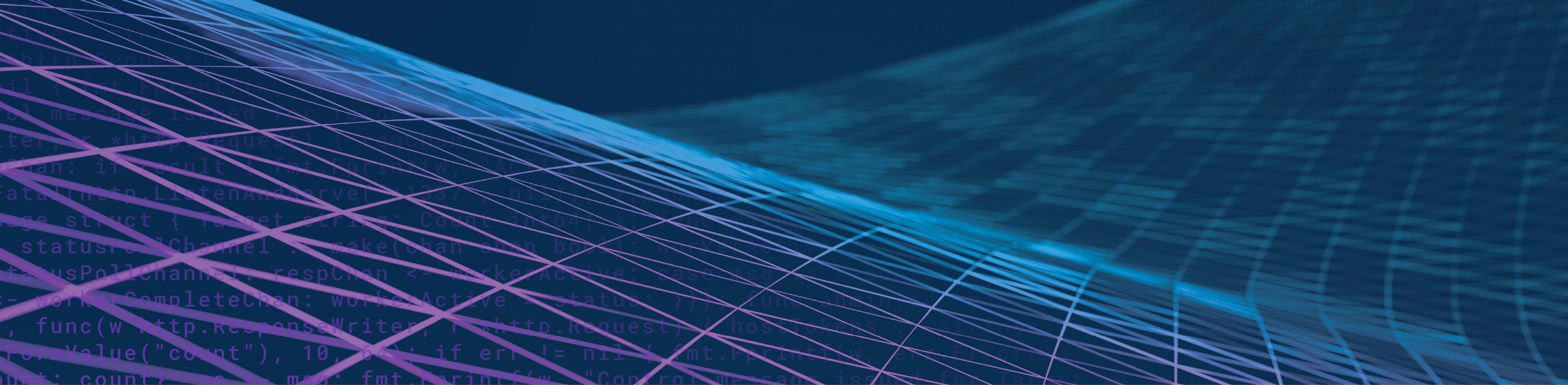
The 7 Myths of In-Browser Protection



It's no secret the internet exposes web-facing applications and assets to a diverse and complex array of cyberattacks. While organizations put significant focus on protecting their mission-critical applications against server-side attacks, many underestimate the damage that can be inflicted by client-side threats within the browser or within the web page itself. This blind spot leaves websites exposed to dangerous client-side vulnerabilities that can lead to fraud, sensitive data exfiltration – and damage to customer trust.

Let's break down some of the common misconceptions of in-browser protection to have a clearer picture of what's really at stake.

Myth 1

A Content Security Policy (CSP) is the most effective client-side defense

A Content Security Policy is a security standard that allows website operators to granularly control which assets can execute within the browser, including scripts. Content Security Policy response headers are used to maintain a list of approved domains considered to be legitimate and safe sources of executable code. They can be a critical part of your defense against JavaScript threats, but they take a ton of resources to maintain – and most client-side attacks occur while leveraging trusted sources. That's why it's important to understand the behavior of all scripts running on your site, even the trusted ones. Akamai Page Integrity Manager leverages behavioral technology to monitor all script execution behavior on a web page, collecting intelligence on scripts' actions and their relationships with other scripts. It then pairs this data with a multilayered detection approach that includes heuristics, risk scoring, artificial intelligence, and much more, to immediately identify suspicious activity.

94%
of websites today leverage at least one third-party script

Source: Third Parties, November 2021

Myth 2

A WAF protects my organization against web-skimming attacks

A web application firewall (WAF) is a security solution that protects web applications from common attacks by monitoring and filtering traffic, blocking malicious traffic entering a web application or unauthorized data leaving the app. WAFs are focused on protecting your connection between your servers and end users, but are not designed to protect your web application at the browser level. Because web-skimming attacks occur within the end user's browser through malicious code execution, WAFs are unable to detect nor mitigate.

Myth 3

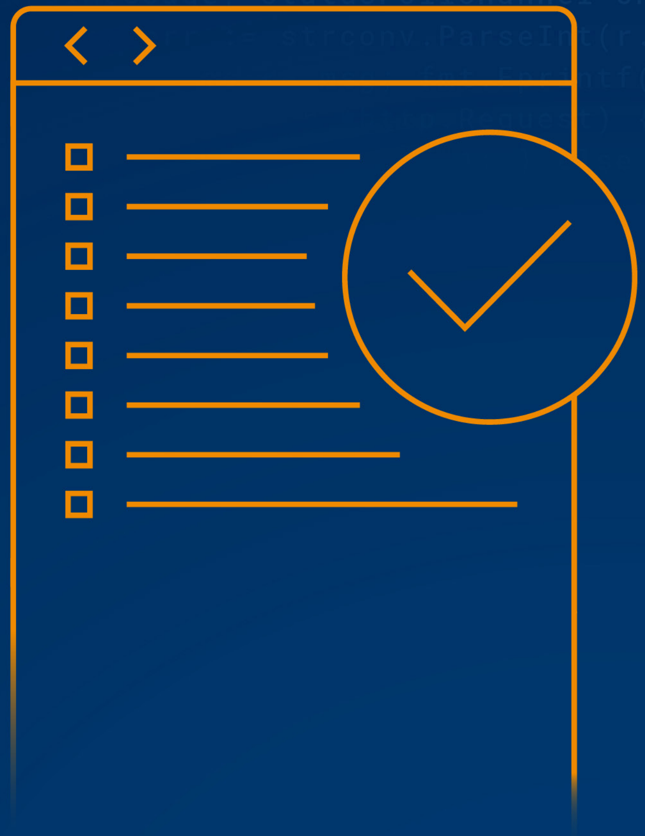
Magecart attacks do not happen as frequently today as they did in the past

Magecart attacks are more alive than ever – they're just getting harder to detect. Recently, our Akamai Threat Research team uncovered a global Magecart campaign targeting several ecommerce sites using sophisticated techniques, such as impersonating a well-known third-party vendor like Google Tag Manager or using Base64 encoding to camouflage malicious code. It's a game of cat and mouse, where threat actors try to bypass security measures and get smarter about how they execute web-skimming attacks to remain undetected. Akamai Page Integrity Manager monitors all behaviors of scripts, including how they interact with other scripts to expose any suspicious activity, and quickly defends against even the most advanced attacks. Learn more in our recent blog post.

Myth 4

I can wait to comply with the new script requirements for PCI DSS v4.0

In March 2022, the latest version of PCI DSS (v4.0) was released to address evolving threats to payment card data and critical market changes that have occurred since the previous release of PCI DSS v3.2.1 in 2018. As a part of new requirements 6.4.3 and 11.6, any organization processing payment cards online must now know which scripts run on their site, when those scripts change, and when each of those scripts stops running, to defend against in-browser script attacks. Though PCI DSS v4.0 does not take effect until 2025, you can't afford to delay protecting sensitive payment card data from being skimmed and exfiltrated from your website's payment pages. Akamai Page Integrity Manager can help accelerate PCI compliance today.



Myth 5

Audience hijacking isn't a major challenge for online retailers

Audience hijacking is the term used to describe unwanted and sometimes malicious browser activities that occur as a result of browser extensions or plug-ins installed on the client side. These unwanted activities can include affiliate fraud, unauthorized redirects to competing or malicious sites, unintended discounting, and distracting ad injections that can prevent a visitor from completing a purchase. Organizations estimate 15%–24% of their website's total site visits are disrupted by audience hijacking tactics.

What can that translate to? Lower conversion rates, a decrease in brand loyalty, and millions lost in potential revenue. Akamai Audience Hijacking Protector allows users to gain visibility into how common browser extensions are impacting site sessions, as well as how extension operators may be conducting malicious activity. It empowers you to decide which extensions are allowed to interact with your site, using granular policy setting at the individual extension level to block or allow activity.

Organizations estimate

15%-24%

of their website's total site visits are distrupted by audience hijacking tactics

Source: Awareness of Audience Hijacking Among Online Retailers, Retail Dive, February 2023

Myth 6

Digital experience platforms can provide visibility into in-browser activities and the impacts of browser extensions

A digital experience platform is a set of technologies that work together to optimize and deliver content-driven experiences. The current analytics that are delivered from these platforms only provide insights into what is occurring on the organization's side of a site session, and not the end user's. This means that while you can track how a site visitor is interacting with your site and their behaviors, you have no visibility into how the browser may be interacting with the end user. By understanding how browser extensions and unwanted browser activities may be affecting your site sessions, you gain a comprehensive view into your entire customer journey and can better define reasons for cart abandonment.

Myth 7

Coupon and price comparison extensions are not harmful to my business

This one is tricky – we get it. Everyone loves a good deal, and extensions like Honey, Rakuten, and Amazon Assistant can help online retailers drive conversion rates. These extensions, however, can have a darker side. Take, for example, a coupon extension that automatically inserts an exclusive offer code into the checkout page of users outside of your intended audience, causing mass discounting. Or Amazon Assistant automatically injecting an ad on your site offering your exact product or service at a lower price through a competitor. These extensions can lead to significant potential revenue loss and lead your most loyal customer astray. Akamai Audience Hijacking Protector supports dozens of the world's most popular browser extensions, and our advanced dashboard provides insights at the individual extension level – allowing users to analyze which extensions are actually beneficial to the business, and which are just not worth it to allow.

Across the global site traffic of Akamai customers, the number of site sessions impacted by coupon and price comparison extensions increased by

25%

between Black Friday and Cyber Monday

Source: Akamai Threat Research, 2022

How Akamai can help

It’s clear the risk of being impacted by a client-side attack is accelerating, and gaining visibility into in-browser behaviors and unwanted activity is critical to reduce risk. Akamai’s Page Integrity Manager protects websites from JavaScript threats – such as web skimming, formjacking, and Magecart attacks – by identifying vulnerable resources, detecting suspicious behavior, and blocking malicious activity. And to stop unwanted in-browser behaviors, Audience Hijacking Protector provides real-time visibility into browser activities occurring on your digital commerce site with granular analysis and mitigation options

Learn how Akamai’s application and API defenses and in-browser protection solutions can help you improve client-side security postures.