



Retail Reimagined



Operational readiness during geopolitical tensions

While the physical toll of geopolitical tensions is the most devastating aspect, the cyberthreats escalating with recent crises have the potential to be highly disruptive to everyday life as we know it.

In the wake of what is currently unfolding, businesses need to reassess defensive postures and prioritize locking down attack surfaces to better maintain operational readiness and business continuity.

Organizations both near and afar must brace for potential repercussions in the form of crippling cyberattacks and intrusions.

Akamai recommends that organizations prioritize actions in the following areas:

- 1 Immediately review and implement CISA recommendations. See relevant [links here](#).
- 2 Review critical subnets and IP spaces, and ensure that they have mitigation controls in place.
- 3 Deploy DDoS security controls in an “always-on” mitigation posture as a first layer of defense, to avoid an emergency integration scenario and to reduce the burden on incident responders. If you don’t have a trusted and proven cloud-based provider, get one now.
- 4 Proactively pull together a crisis response team and ensure runbooks and incident response plans are up to date. For example, do you have a runbook to deal with catastrophic events? Are the contacts within the playbooks updated? A playbook that references outdated tech assets or people that have long left the company isn’t going to help.

If you require immediate assistance in the face of a DDoS attack, Akamai has security operations experts standing by to help.



DDoS Protection

[click to read](#)

To help stop the spread of a malware infection, consider doing the following:

- 1** Patch everything that needs a patch. Don't wait. If you can't patch due to logistical reasons, then selective WAF rules can temporarily assist and buy some time.
- 2** Backups. Do you have them? You should. Do they work? Test them. Most ransomware attacks go from bad to worse because the backups were flawed.
- 3** Segmentation is one of the most important steps you can take to improve your cyber resilience, as well as prevent the spread of malware (i.e., ransomware). In addition, implement MFA across the enterprise for layers of defense.
- 4** Explore custom WAF rules to match on certain geographic attributes to help reduce malicious traffic from unwanted geographies.

Tailor defenses to the latest applications and threats with Akamai's WAF solution



[WAF Solution](#)

[click to read](#)

Loyalty - a matter of trust?

To win consumer loyalty, an online retailer needs to intimately understand the customer base and deliver personalized, friction-free, omnichannel experiences.

At the same time, customers need to trust retailers not to abuse, lose, or misuse their data. Loyalty is essentially an exchange of trust.

Customer identity and access management (CIAM) solutions are usually the preferred choice to transform and expand a retailer's loyalty and membership program.

Off-the-shelf, cloud-based CIAM solutions are the preferred choice for many retailers. The ease of initial implementation, effort to operate and maintain it, and keeping it up to date with changing requirements dictated by technology, consumers, and regulators, makes ready solutions the go-to.

But loyalty program transformation and growth can be difficult to achieve when relying on outdated technology. Traditional workforce identity access management solutions were designed for record-keeping and not to scale, flex, and align with changing consumer expectations. That is why successful companies wishing to expand their loyalty or membership programs and initiatives are embracing CIAM solutions.

A robust CIAM solution eliminates the need to build and maintain costly platforms and homegrown applications – saving time, money, and IT resources. Because after all, customer loyalty and rewards programs and other membership initiatives are all about customer identity.



Case study: The omnichannel customer loyalty experience

This major organic grocery chain with stores throughout the United States, Canada, and the United Kingdom did not have a traditional customer loyalty program nor a digital presence to help it better understand its customers and their preferences.

To remedy the situation, the company determined that it needed to undertake a digital transformation and create a connected customer experience across multiple channels and devices.

The company decided on a strategy to make it easy for its shoppers to save time by decreasing the effort in meal planning and preparation. The grocery chain wanted to personalize the customer experience by capturing useful profile information and preferences for retargeting purposes.

To achieve these goals, the company needed a CIAM solution that would help it drive new customer experiences through digital channels.

The company established clear objectives such as enhancing shopper loyalty and creating a connected customer experience across devices and channels.

To meet its objectives, this grocery chain selected Akamai Identity Cloud, which helped the company build trusted digital relationships to improve the personalized shopping experience across multiple channels, resulting in greater value, revenue, and brand loyalty.

By leveraging the Identity Cloud collection of demographic, psychographic, and behavioral consumer data across its digital properties, applications, and devices, the company was able to gain an enriched 360-degree view of each individual shopper.

The grocery retailer started by deploying Identity Cloud on its website to create a more connected customer experience and provide additional reasons to engage with the chain.

Retail loyalty programs get results with Akamai

↑ 4x

Increased Coupon Downloads

↑ 9x

Increased Mobile App Use

↑ 4.7x

Increased Monthly Registrations

For example, its content management system enables customers to search and find recipes on its website. The site also makes content recommendations and presents circulars and specials. Users can easily sign in, manage dietary preferences, and save recommendations.

Once the user has established preferences, the site will customize and personalize the experience. For example, if the user is a vegetarian and navigates to the recipes section of the website, the vegetarian recipes will be prioritized at the top. The site will re-sort the content and map it to the taxonomy for the user's dietary preferences and restrictions, thereby providing a more precise, personalized website experience.

The company started to see an improvement right away in overall website traffic, as well as the number of logging-in users.

The grocery chain's next step was to extend the digital customer experience into the physical stores themselves. Using Identity Cloud, the company connected the same account login credentials to both the website and the mobile app.

This connected, omnichannel consumer experience extends once the customer returns home and starts cooking. They can seamlessly log into their account on their phone or tablet device and see the same recipes they saved on the website. They can "flip over" recipe cards and see the instructions on how to prepare the meals.

The overall Akamai-powered result became a very consistent, cohesive, omnichannel experience.

Akamai can help improve your customer experience by accelerating web performance, maximizing availability, and streamlining customer onboarding:



[Ecommerce](#)

[click to read](#)

Securing online retail during the holidays

Retailers worldwide breathed a collective sigh of relief after the holiday season.

Global supply chain issues, skyrocketing shipping costs, inflation, and domestic labor shortages have rapidly compounded problems within a sector already slammed by the COVID-19 pandemic.

Threat actors are aware of the increased pressure facing retailers (and consumers) globally and stand ready to take advantage of the industry's "make or break it" time of year.

While cybercriminals have an arsenal of attack vectors, tools, and exploits to leverage, malicious bots can pose a significant threat to online retailers – and their bottom line.

Bots can be broken down into two buckets – good bots and bad bots. Good bots, like Googlebot and Bingbot, crawl and index retailer websites to help improve search results. These types of bots are not built with bad intentions, and they respect rules as defined by the webmaster's robots.txt file.

However, malicious bots are purpose-built for a variety of nefarious activities like [credential abuse for account takeover \(ATO\) attacks](#), [grabbing limited inventory](#) ahead of real customers, Layer 7 application DDoS attacks, price scraping, [gift card fraud](#), and more. Juniper Research estimated that ecommerce fraud – oftentimes associated with bad bots – [increased 18% in 2021 to reach \\$20 billion in losses](#) for retailers globally.

With so much on the line, it comes as no surprise that Akamai observed bot operators out in full force, causing significant upticks in malicious bot activity leading up to and during the most recent online shopping mega-holidays like Christmas.

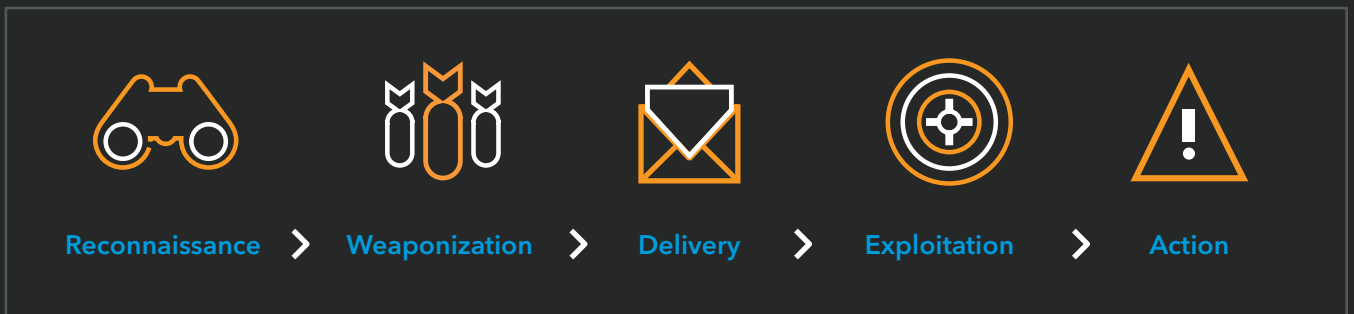
Keep ahead of the evolving bot landscape:



[Bot Manager](#)

[click to read](#)






Here's what businesses can do to help ensure bots don't ruin holiday cheer.

- *Be alert to evidence of an attacker moving through the ATO kill chain. For example, threat actors often start preparing for full-scale attacks with some testing, so you might see a small spike in failed logins in the days before major online shopping events.*
- *Keep in mind that discovering and stopping bot attackers early in the weaponization and delivery phases of the ATO kill chain means organizations can better defend against fraud and abuse.*
- *Tune your bot solution if you see more bots coming through. Note: Not all bot management solutions need manual tuning; check if yours does.*

See the full ATO kill chain infographic explainer here:



[Break the Account Takeover Kill Chain](#)
click to read

This is an edited version of a blog post written by *Susan McReynolds, Akamai*