5 BEST PRACTICES:

Preparing Your Ecommerce Site for Maximum Holiday Success

Exclusive Cloudflare data from Cyber Weekend 2019, with best practices for enhancing site performance and security to improve profitability in the holiday season and beyond

1-888-99-FLARE | enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE®

Table of Contents

CLOUDFLARE

New Realities for Holiday Season Ecommerce

For online retailers, Cyber Weekend 2019 delivered plenty of holiday cheer, with record-shattering revenues topping $28.4 billion in the US, and as much as $90 billion worldwide.[1]

But challenges abound. This Cyber Weekend online retailers faced rising competitive pressures, escalating consumer expectations, and mounting security challenges—all of which should guide their plans for 2020.

The Ultimate Sales Bonanza Goes Mobile

On the one hand, opportunities are plentiful—just look at mobile.

On Thanksgiving, mobile accounted for 63% of site traffic on 45% of all sales, compared to 24% a year ago.[2] And on Cyber Monday, purchases via smartphone topped $3 billion for the first time—a staggering 46% increase from 2018.[3]

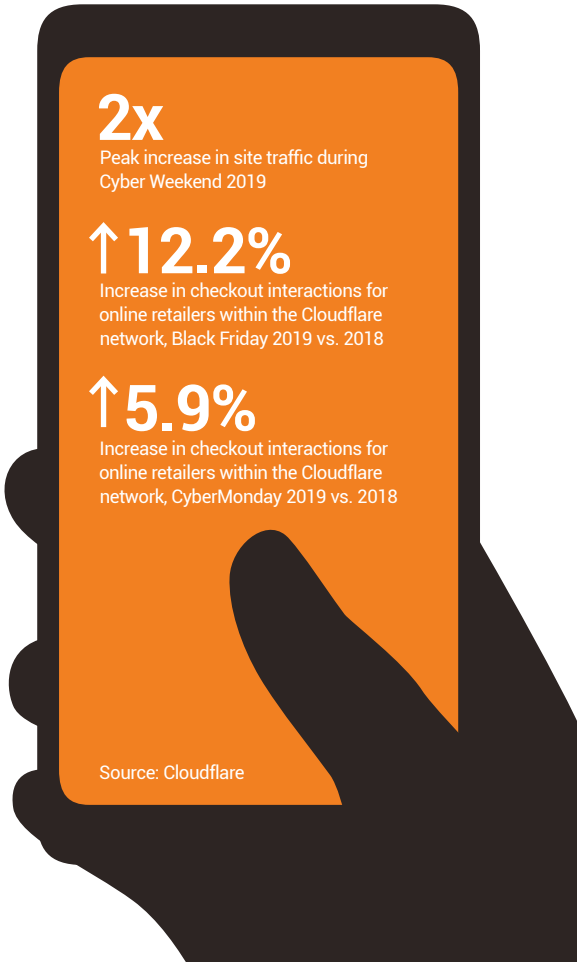
A Rapidly-Evolving Competitive Landscape

For all the glad tidings delivered this holiday season, Amazon still accounted for nearly half of all US ecommerce revenues in 2019.

In addition, Amazon is no longer alone. In 2019, Chinese ecommerce giant Alibaba transacted $38 billion in just 24 hours[4]—eclipsing all the revenues US-based online retailers generated from Thanksgiving through Cyber-Monday *combined*.

To fend off these and other rivals, retailers must deliver elegant, effortless shopping experiences backed by bulletproof cloud, commerce, and logistics capabilities.

Cont'd Next >>



The Rising Threat from Cybercrime

Unfortunately, retailers aren't the only ones looking to make out like bandits during the holiday season. Cyber-thieves are out to exploit breached login credentials to hijack customer accounts for illegal shopping sprees.

In the US, losses from account takeovers (ATOs) now top $4 billion per year.[5] Worldwide, payment fraud could exceed $30 billion in 2020.[6] And hackers injecting malicious code into websites to steal credit card information are expected to represent a major threat to the retail sector in the year ahead.[7]

But fighting back means striking the right balance. With shopping cart abandonment rates already hovering at 70% or higher, retailers must find new ways to harden their defenses without increasing customer friction.

Best Practices for a Successful Holiday Season

This Cloudflare report outlines strategies for overcoming the challenges of preparing ecommerce websites for major events, whether it's a one-day super sale, or an entire holiday season.

Many of the actionable insights featured in this eBook are based on Cloudflare data from Black Friday through Cyber Monday 2019, prevailing industry trends, and insights from leading online retailers within the Cloudflare global cloud network.

To identify these best practices, Cloudflare measured traffic across ecommerce sites that were identified via HTTP Archive and supported by the Cloudflare global network from November 29 through Monday, December 2, 2019.

Using fully-anonymized data from these referenceable domains via HTTP Archive, we examined daily pageviews and resulting checkout interactions, as well as cyberattacks and other threats identified and mitigated within the network during the busiest shopping days of the year.

We were then able to gain insights into the factors shown to most negatively impact performance, as well as mitigation strategies that have proven effective for retailers within our network.

By combining our findings with a survey of trends research from third-party sources, we were able to bring broader context to our analysis. What emerged from this investigation are 5 best practices for maximizing ecommerce success during the 2020 holiday season and beyond.

ABOUT CLOUDFLARE

Cloudflare is a leading security, performance, and reliability company on a mission to help build a better Internet.

Trusted by over 25 million Internet properties, our integrated cloud platform helps brands and retailers improve the performance of their web properties, while also safeguarding customer data and transactions.

- Network spanning 200+ cities and over 90 countries
- Within 100 milliseconds of 99% of the Internet-connected population in the developed world
- An average of 50 billion daily cyber threats blocked in Q4, 2019
- 35 Tbps total network capacity

CLOUDFLARE®

BEST PRACTICE #1

Maximize the Customer Experience, Especially on Mobile

According to PwC, 54% of holiday shoppers prefer the convenience of shopping via their smartphones, computers, and even in-home voice assistants like Alexa over a trip to the store.[8]

During the 2019 holiday season, mobile accounted for nearly half of all online sales. On Black Friday, as much as 64% of all payment transactions were initiated through a mobile device.[9] And by 2021, as much as 72.9% of all online purchases may be made this way.[10]

In short: Mobile has become the primary driver of ecommerce growth. But fair warning: As more consumers (and retail competitors) embrace all things mobile, customer experience (CX) will separate ecommerce winners and also-rans. Here are some steps for making the most of the mobile channel.

Cont'd Next >>

Less Latency, More Conversions

For mobile customers, visual content is key to the shopping experience, just as on the desktop. Crisp product images, 3D renderings, robust product videos, and eye-popping visual commerce features such as VR and AR simulations can help stimulate interest and boost purchase confidence. They can also result in a 60% to 70% increase in shopping cart values.[11] But latency can be a deal killer.

A number of factors can significantly undercut customer engagement with visual content and commerce features, either through increased latency or other performance issues. Retailers seeking to maximize the benefits of visual content and commerce features should:

- Optimize for device types and network connectivity to minimize performance degradation
- Avoid embedding raw video files like MP4 and MOV files, which slow down load times
- Leverage content delivery networks with advanced compression and caching capabilities

> *"We are looking at better agility, better response time in terms of support. Better operational capabilities... Our homepage loads faster, your first view is much faster."*
>
> **Karan Tewari** Manager, Platform Engineering
>
> falabella
>
> (VIEW CASE STUDY)

Cont'd Next >>

Balance Dynamic Features with Performance Requirements

Dynamic webpages and AI-enabled features that present relevant page content and predictive product recommendations play an increasingly important role in the success of ecommerce sites. Not only does it enhance the buying experience and help to generate higher conversion rates, it also helps build brand loyalty and boost customer lifetime values.

But retailers deploying site-wide personalization should also be aware of how page performance is impacted. Pages that require extensive JavaScript, or dynamic page assets, can potentially take longer to load than a comparable page with static images and no personalization.

Optimize for Speed—and SEO

Whether it's researching new products or making a mobile purchase via mobile device, instant gratification is the name of the game. That means merchants must make it as easy as possible for customers to find their products via organic search.

Google's mobile-first indexing assesses how well your website performs on mobile, which in turn impacts where your store appears in search results, including desktop. To enhance the customer experience while maintaining or improving search rankings, we recommend that retailers:

- Build responsive sites that ensure webpages and images automatically adjust for screen size
- Run performance tests to optimize visual content load speeds using widely available online tools
- Leverage Google AMP to accelerate page load times and enhance the mobile experience

> *"Speed is a huge factor in customer conversion—one of our team's core goals to sustain business growth is making sure all of our sites are fast and responsive. Cloudflare has helped us achieve that, and much more."*

Andy Dean Technical Operations Manager

ALLSAINTS

(VIEW CASE STUDY)

BEST PRACTICE #2

Disaster-Proof Your Cyber-Weekend Surge

Retail site traffic within the Cloudflare global network surged more than 200% during Cyber Weekend, peaking at 21.5 million page views on Black Friday, compared to 11.3 million average daily pageviews earlier in the month. Cyber Monday saw traffic temper only moderately, to 18 million pageviews.

According to Cloudflare data, checkout interactions for Black Friday increased 12.2% year-over-year, while Cyber Monday's checkout interactions rose nearly 6%. Checkout interactions are defined as the rate at which users clicked to checkout pages and shopping carts as a measure of purchase intent. It is not an indicator of whether those transactions were completed, or for what dollar amount.

Breaking Down the Numbers

When matching these pageviews and checkout interactions with publicly reported retail sales data, some interesting patterns emerge. Black Friday saw the highest number of online shoppers, who collectively spent $7.4 billion[15], while Cyber Monday saw fewer online shoppers spend $9.4 billion[16]—$2 billion more—despite fewer total transactions. It seems Black Friday remains a monumental shopping event in terms of volume, while Cyber Monday is reserved for purchases of higher-ticket items.

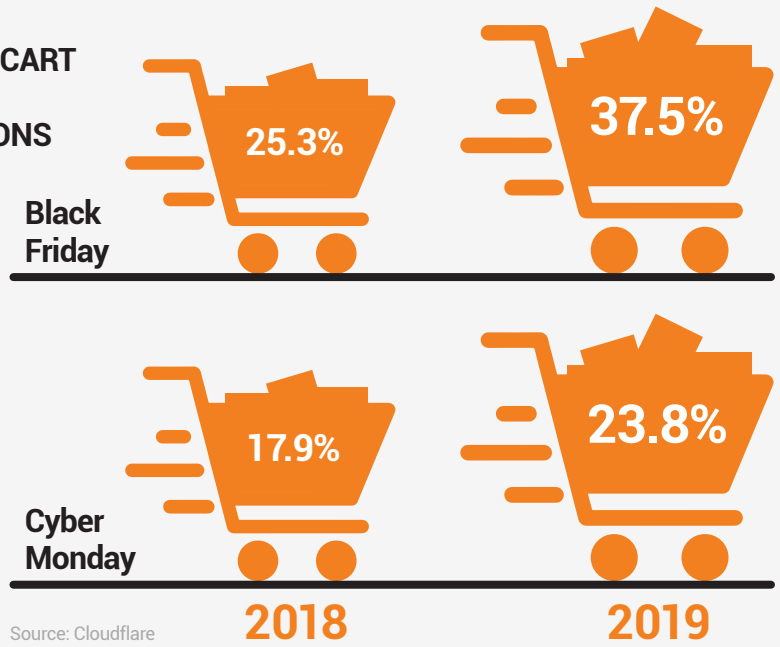
One Site's Outage is Another Site's Opportunity

These riches were not shared equally. According to reports, a number of merchants suffered website, mobile, and app glitches that cost them millions. In fact, one major brand-name retailer was plagued by as much as 12 hours of downtime that may have cost it 40% of its Thanksgiving Day digital sales.[17]

But many retail sites remained up and operating flawlessly throughout this crucial holiday weekend. Some of the smart ways these and other top merchants maximize uptime and availability during this kind of peak selling event include the following.

Cont'd Next >>

SHOPPING CART CHECKOUT INTERACTIONS



Source: Cloudflare

Make Plans to Crush It, Not Crash It

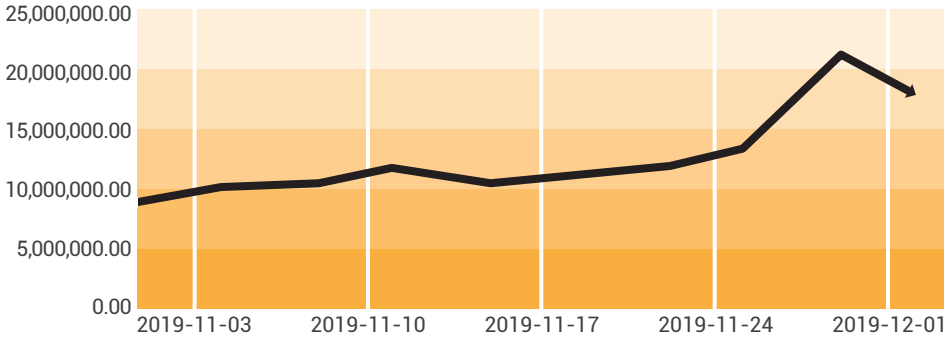
When websites aren't able to handle the increased traffic and transaction volumes that Cyber Weekend is famous for, fickle customers won't hesitate to take their purchases elsewhere. And that's if they can even access your site.

To avoid downtime and the financial and reputational damage that come with it, plan ahead. Start by building a forecast of your capacity requirements based on growth in traffic and sales volumes for each of the last three to five years. Then run load tests of internal and external systems at a minimum of 200% of your estimates peak traffic levels.

Cont'd Next >>

DAILY PAGE VIEWS FOR RETAILERS WITHIN THE CLOUDFLARE GLOBAL NETWORK,
Nov. 1 through Dec. 1, 2019

Source: Cloudflare



Up Your Infrastructure Game

Downtime doesn't just mean your website or app has been knocked completely offline. It can also mean missing page elements or checkout friction or failures. Worldwide, that can contribute to as much as $4 trillion in lost revenues each year as shoppers give up on transactions.[18] Not exactly a festive experience for the customer or the merchant.

Whether you're hosting servers on-premise or in the cloud, make sure you're able to support your forecast workloads. In the event your site goes down, you also need to ensure traffic can fail over to an alternate site. Your hosting provider should provide you with options for co-located site migrations in the event of a disaster or outage.

- Performance test third-party applications driving API traffic to your site
- Mitigate traffic spikes with rate limiting to prevent infrastructure overload
- Load balance traffic across multiple sites in the event of a server outage
- Implement health monitoring to prevent traffic from being directed to a downed server

49%
Percentage of Black Friday shoppers who say they will abandon a cart if they receive any error message at checkout
-RetailTouchPoints[19]

17%
Percentage of Black Friday shoppers who say they immediately shop a competitors' site if they receive an error message at checkout
-RetailTouchPoints[20]

2%
The increase in conversion rates Walmart achieved after speeding load times by 1 second
-The Drum[21]

Cont'd Next >>

"Black Friday is one of the most important days for our merchants every year, and 2019 was the biggest of them all. With the support of Cloudflare, we were able to handle the demand and deliver lightning-fast responses to shoppers globally."

Charles Ng Production Engineering Manager

shopify

Beef Up Cyber Security, Too

From Black Friday through Cyber Monday 2019, Cloudflare mitigated 189 million cyberthreats against online retailers in the US alone. In fact, attack rates in the US eclipsed most other regions, with Germany seeing the second highest attack rates worldwide, with 118 mllion mitigated threats. By comparison, Great Britain saw 27 million mitigated threats.

As the data points out, larger economies with significant cultural or religious celebrations taking place in December experienced a dominant share of cyberthreats over Cyber Weekend.

On the following pages, we'll look at some of the most common attack modalities, which can cause significant damage to site security, performance, and uptime. We'll also share some key strategies for mitigating them.

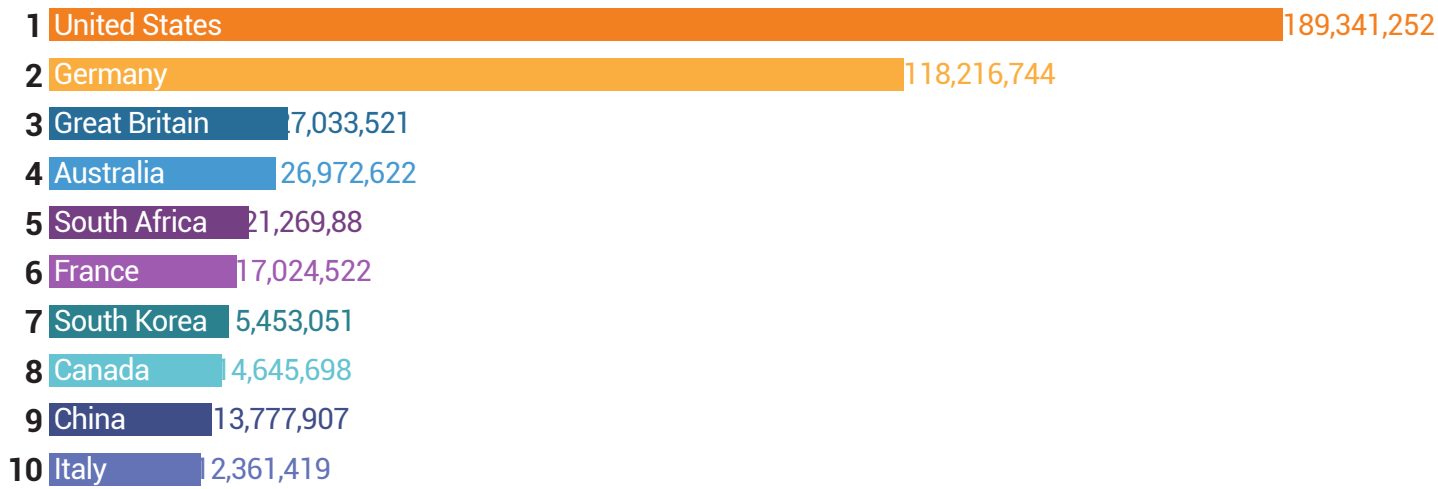
189+ million

Cyberthreats against US online retailers
Black Friday through Cyber Monday 2019

442+ million

Cyberthreats against online retailers in Top 10 countries under attack
Black Friday through Cyber Monday 2019

TOP 10 COUNTRIES EXPERIENCING CYBER THREATS
Black Friday through Cyber Monday 2019
Source: Cloudflare



BEST PRACTICE #3

Deck Your Defenses Against DDoS Attacks

Effective disaster-proofing includes preparing for an onslaught of Distributed Denial-of-Service (DDoS) attacks from malicious actors seeking to take your hosting servers offline by flooding them with traffic from compromised devices and networks.

Whether the aim of these malicious assaults is to cripple your conversions, divert shoppers to rivals, hold your site ransom, mask customer data theft, or simply damage your brand, holiday shoppers will place the blame squarely on you. Retailers seeking to avoid these scenarios should consider the following when readying their forward defenses.

▶ Prepare for 5G-Powered Attacks

5G's faster speeds and lower latency will be a boon for retailers seeking to introduce new services and site features. But as 5G enables a growing number of connected consumer gadgets, cybercriminals, rogue competitors, hacktivists and others will seek to exploit the poor, or often non-existent, security controls on many new smart devices.

The staggering amount of traffic that threat actors may be able to generate through compromised devices connected to 5G networks may quickly exhaust resources within site infrastructures, forcing IT teams to over-provision capacity[22]—a proposition that should be factored into holiday traffic forecasts.

Cont'd Next >>

Don't Discount Smaller Attacks

According to industry-wide estimates, as much as 33% of all cyberattacks perpetrated against online and mobile merchants involve DDoS.[23]

Yet even as the ecommerce sector must be mindful of the risk associated with ultrahigh bandwidth attacks, as many as three-quarters of DDoS attacks come in at 5 Gigabits per second (Gbps) or less.[24]

Often, these low-speed, application layer (L7)-based attacks are designed precisely to fly under the radar and target one or more service gateways and application layers so they need less overall traffic to knock your site offline.

Move Up to Cloud-based DDoS Mitigation

One strategy for addressing these threats is to expand investments in your existing infrastructure to absorb the workloads generated by DDoS attacks.

But merchants are likely to find traditional DDoS solutions are simply unable to adapt to the growing complexity of attack methodologies, and are rendered useless against attacks that exceed an organization's network capacity.

A better idea: Deploy a scalable, cloud-based mitigation solution to neutralize threats from DDoS attacks of any scale or sophistication. To keep your store up, running, and off your customers' naughty lists, consider solutions that:

- Provision services at the network edge for maximum agility in mitigating rapidly-evolving threat modalities
- Offer unlimited and unmetered mitigation, so your site remains resilient against DDoS attacks of any form or complexity
- Use global threat intelligence to protect against the most sophisticated attacks
- Integrate seamlessly with other security, performance, and analytics solutions and existing business processes

> *"Cloudflare helps our online business perform at its best. It's the ultimate solution for site security and performance."*
>
> **Sam Wolf** Founder & CEO
>
> LUCKY VITAMIN
>
> (VIEW CASE STUDY)

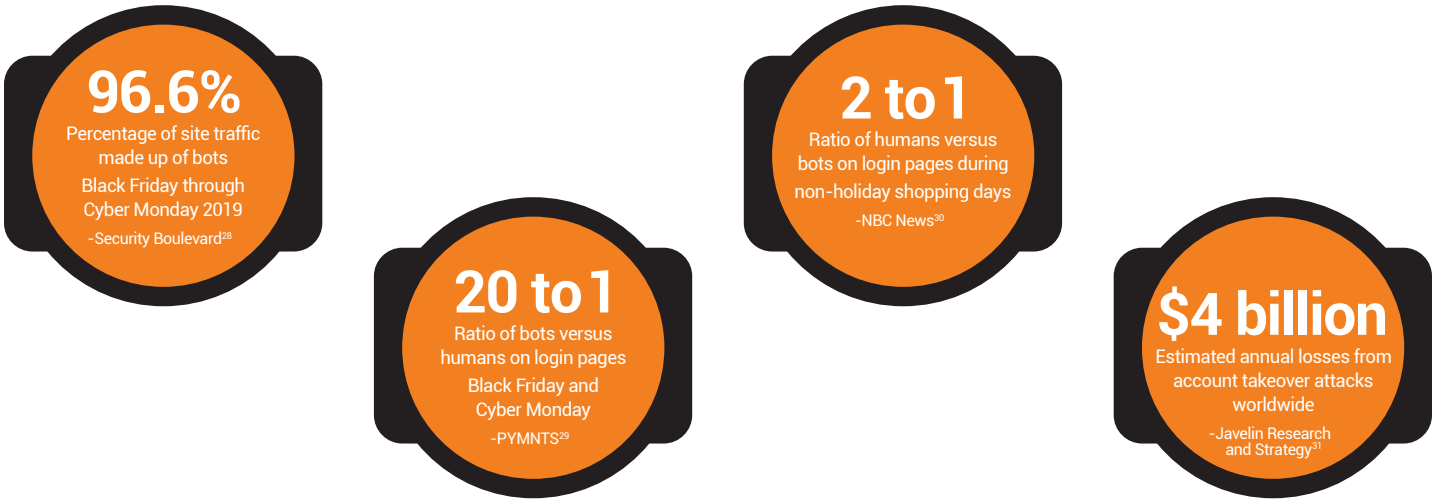
BEST PRACTICE #4

Prevent Bot-based Account Takeovers

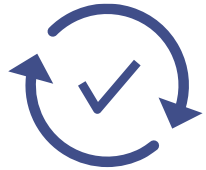
Cyber-Weekend is peak credential-stuffing season for online retailers. In 2019, cybercriminals launched a record number of bot attacks that use stolen login credentials to hijack customer accounts for illegal shopping sprees.

For some retailers, malicious bots made up as much as 97% of site traffic leading into the holiday weekend.[25] On Black Friday and Cyber Monday, two-thirds of all traffic to login pages were bot-based account takeover attempts.[26]

It's easy to see why. According to eMarketer, card-on-file information saved within customer profiles will drive more than $26 trillion in online retail purchases worldwide in 2020[27]. With large-scale data breaches continuing to drive down the cost of stolen logins, online merchants will remain the #1 target for credential-stuffing bot attacks looking to make illegal purchases. But there are ways to fight back.



▶ Implement CAPTCHA Challenges



Increasingly, holiday bot attacks are also designed to swipe those ultimate stocking stuffers—gift cards. Either through ATOs or guest-purchase logins, cyberthieves leverage bots to quickly validate stolen gift card numbers and then either sell them on the black market, or fraudulently purchase items they can then sell online.

Implementing CAPTCHA challenges at login can help block bot-based account takeovers and illicit guest-purchase logins. These challenges take the form of questions on pages where bot traffic is suspected to help determine whether the user is a human or a bot.

Cont'd Next >>

Deploy Rate Limiting

Rate limiting can help prevent site scraping. A real user isn't likely to request content from several hundred pages within a few minutes or seconds. Any "user" that does is mostly like a bot. In 2019, Cloudflare used rate limiting to mitigate almost 6% of all detected attacks against US-based online merchants from Black Friday through Cyber Monday.

Enlist a Bot Management Service

To minimize the impact security measures such as CAPTCHA challenges can have on the customer experience, it's also wise to deploy a bot management service. These cloud-based services leverage advanced machine learning to sniff out malicious bots and block their login attempts without creating additional user friction. For best results, it's best to seek out solutions that:

- Go beyond just scouring large numbers of access attempts at any one time
- Detect and disrupt more advanced, "low and slow" bot attacks that more closely mimic human behavior
- Leverage global threat intelligence networks so attacks on one retailer are recognized and blocked by all

This one move can pay dividends all year round. According to researchers, online retailers may have lost as much as $10 billion in 2019 due to bot attacks, either through missed sales, wasted man hours, or customers fleeing a site after it or some of its functionality stops functioning.[32]

Look for smart retailers to deploy bot management services in order to avoid these kind of losses in the year ahead.

> *"I'm very bullish on Cloudflare's ability to identify threats—because of the volume and diversity of Internet traffic they handle, they're positioned to leverage that data to detect and mitigate the most sophisticated DDoS and malicious bot attacks."*

Aaron Suggs Director of Engineering

Glossier.

(VIEW CASE STUDY)

BEST PRACTICE #5

Secure Your Store, Your Customers, and Your Brand

No pre-Cyber-Weekend checklist is complete without assessing website security, third party applications, and web services such as APIs.

In addition to guarding against data breaches, other vulnerabilities to prepare for include cross site scripting (XSS) attacks that enable hackers to impersonate customers or trick them into revealing personal information. They also include SQL injection (SQLi), which targets the way databases execute search queries in order to manipulate product catalogs or prices and potentially complete fraudulent purchases.

In the runup to the 2019 holidays, online retailers in the US and UK were hit with these and other forms of attack.

Beyond the immediate financial losses, brand loyalty can often be the first casualty of such breaches. Nearly one-third (32%) of customers say they would stop shopping with a retailer if their personal information is stolen from them.[33]

Arm Up for Battle

The global nature of the Internet exposes shoppers to attacks launched from different locations and involving various levels of scale and complexity.

To properly extinguish these threats, you must secure your online store, third-party applications, and web services such as APIs from common vulnerabilities such as SQLi and XSS attacks as well as from data breaches. Any serious game plan will include the following.

Cont'd Next >>

8.7% **Percentage of attacks against online merchants involving cross-site scripting (XSS)**
-Total Retail[34]

8.2% **Percentage of attacks against online merchants involving SQL Injection (SQLi)**
-Total Retail[35]

Deploy a Web Application Firewall

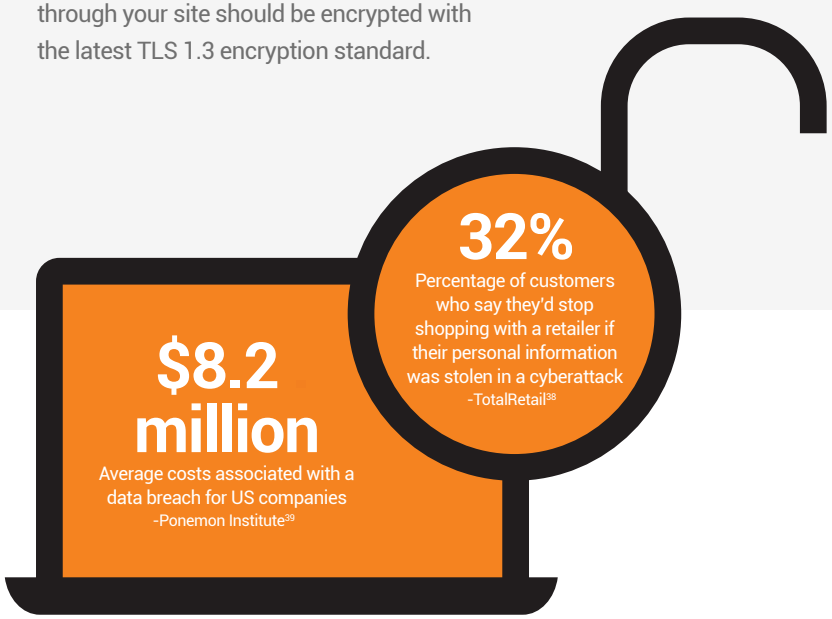
Mitigating SQL injection and cross-site scripting attacks isn't particularly difficult. But with all the moving parts involved with operating a robust ecommerce site, mistakes can still be made, and hackers can still come up with inventive new zero day attacks to exploit those vulnerabilities.[36]

As a result, a web application firewall (WAF) is essential to digital channel operations. WAFs detect and block XSS and SQLi attacks and are required for PCI-DSS compliance to protect customers payment details and other personal information. They also filter out malicious code and provide comprehensive security against malware and hacking attempts on embedded web applications.

Encrypt *All* Your Data

Online and mobile retailers store highly sensitive information about users, including card-on-file and other personal information—making them prime targets for hackers. To keep all that information safe, all data that is exchanged or delivered through your site should be encrypted with the latest TLS 1.3 encryption standard.

TLS 1.3 not only hardens the security of your encrypted connections, but also reduces latency and optimizes performance. That matters to retailers, who can lose as much as $4 million annually for every millisecond they lag behind competitors.[37]



How Cloudflare Can Help Make Holiday Ecommerce a Breeze

The challenges that come with preparing your ecommerce site for Cyber-Weekend success can be daunting. But Cloudflare is here to help.

Trusted by over 25 million Internet properties, our integrated cloud platform helps brands and retailers improve the performance of their web properties, while also safeguarding customer data and transactions during the holidays and every day of the year. Our services and solutions can help online and mobile retailers:

Enhance CX for More Conversions

- CDN
- Argo Smart Routing
- Image resizing and optimization
- Video streaming
- Accelerated web content
- AMP support

Ensure Store Uptime and Availability

- Load balancing
- Managed DNS
- DDoS mitigation
- Virtual backbone
- Rate limiting

Secure Customer Data and Transactions

- Bot Management
- Web Application Firewall
- TLS 1.3

Leverage Networked Intelligence Powered by Machine Learning

With Cloudflare, an attack in Bangladesh bolsters your security in Omaha. An undersea cable is cut? Your customers are automatically re-routed—without disrupting your business. The Cloudflare global network analyzes traffic to over 25 million Internet properties worldwide, spanning over 1 billion unique IP addresses per day, to keep your ecommerce site up and running.

> *"Cloudflare helps keep us online, provides a faster site experience to our end users, and protects our customers sensitive information."*

Steven Ou Founder and CTO

TOUCH OF MODERN

(VIEW CASE STUDY)

Prepare Now for Cyber-Weekend— It Just Takes 5 Minutes

See just how easy it is to join the Cloudflare revolution, and be ready for your next sales event, or the entire holiday season, in as little as five minutes.

cloudflare.com/ecommerce

CLOUDFLARE

Footnotes

1 Adobe Digital Insights "2019 Holiday Shopping Trends," Nov. 1, 2019-Dec. 31, 2019

2 Levy, Nat, "Holiday e-commerce spending already hitting records as Amazon and others gear up for peak shopping season," GeekWire, November 29, 2019

3 Perez, Sarah; Lunden, Ingrid "Cyber Monday totaled $9.4 billion in online sales, smartphones accounted for a record $3 Billion," Techcrunch, December 3, 2019

4 Pham, Sherisse, "Singles Day sales for Alibaba top $38 billion, breaking last year's record," CNN, November 12, 2019

5 Groenfeldt, Tom, "Credit Card Fraud is Down, But Account Fraud That Directly Hurts Consumers Remains High," Forbes, March 18, 2019

6 Nilson Report, "Payment Card Fraud Losses Reach $27.85 billion," November 21, 2019

7 Lerner, Dov, "The Holidays Are a Prime Time for Cybercrime," Total Retail, November 15, 2019

8 PwC, 2019 Holiday Outlook

9 LexisNexis Risk Solutions, "Bots on Mobile Devices Fuel Holiday Shopping Cyberattacks," Dec 16, 2019

10 Statistica, "Global Mobile Retail Commerce Sales Share 2016-2021," October 7, 2019

11 PYMNTS.com, "Look at the Pretty Pictures: Behind Visual Commerce's Rise," November 12, 2019

12 Yahoo! Finance, "Personalization Drives 5X Conversion Rates During Black Friday and Cyber Monday," December 9, 2019

13 Kapur, Ajay, "Site speed is the new competitive battleground in ecommerce," DigitalCommerce360, April 16, 2019

14 Think With Google, "The 3 areas brands should invest in to improve consumer experiences on mobile," Date Here???

15 Liao, Shannon, "Black Friday pulls in a record $7.4 billion in online sales as many turn to mobile orders," CNN Business, December 1, 2019

16 Lucas, Amelia, "Cyber Monday online sales hit record $9.4 billion, boosted by late-night spending spree, Adobe says," CNBC, December 3, 2019

17 Crets, Stephanie, "Site glitches and downtime plague retailers during Cyber 5," DigitalCommerce360, December 4, 2019

18 Pioryshkina, Kate, "5 Steps to Creating the Perfect Mobile Checkout," Destination CRM, September 18, 2019

19 Taylor, Glenn, "Costco Thanksgiving Day Site Outages Cost an Estimated $11 Million," Retail TouchPoints, December 2, 2019

20 Taylor, Glenn, "Costco Thanksgiving Day Site Outages Cost an Estimated $11 Million," Retail TouchPoints, December 2, 2019

21 Solanki, Ricky, "Why a slow website is killing your conversions," The Drum, August 28, 2019

22 HelpNetSecurity, "Most decision makers expect 5G to impact their cybersecurity strategy," October 29, 2019

23 Reynolds, Roy, "DDoS Attacks on Retailers are Getting Sneaky—it's Time to Rethink Your Denial of Service Protection," Premier Construction News, October 2019

24 Reynolds, Roy, "DDoS Attacks on Retailers are Getting Sneaky—it's Time to Rethink Your Denial of Service Protection," Premier Construction News, October 2019

25 Popken, Ben, "'Grinch bots' are here to ruin your holiday shopping," NBC News, November 30, 2019

26 Thatha Pavan, "Nearly Two-Thirds of Traffic Was Bad Bots on Login Pages of E-Commerce Firms this Holiday Season," Retail IT Insights, December 16, 2019

27 EMarketer, "Global Ecommerce 2019," Date Here??

28 Thatha, Pavan, "Nearly Two-Thirds of Holiday E-Commerce Traffic Was Bad Bots," Security Boulevard, December 17, 2019

29 PYMNTS.com, "'Grinch Bots' Ramp Up Cybercrime During Holidays," December 2, 2019

30 Popken, Ben, "'Grinch bots' are here to ruin your holiday shopping," NBC News, November 30, 2019

31 Groenfeldt, Tom, "Credit Card Fraud is Down, But account Fraud That Directly Hurts Consumers Remains High," Forbes, March 18, 2019

32 Wodinsky, Shoshana, "Bots Will Cost Ecommerce Sites $10 Billion in 2019," Adweek, November 26, 2019

33 Keenan, Joe, "Macy's Suffers Online Magecart Card-Skimming Attack, Data Breach," My Total Retail, November 19, 2019

34 Lackey, Zane, "It's the Most Wonderful Time of the Year … for Hackers," Total Retail, December 9, 2019

35 Lackey, Zane, "It's the Most Wonderful Time of the Year … for Hackers," Total Retail, December 9, 2019

36 Porup, J.M. "What is Cross-Site Scripting (XSS)? Low-Hanging Fruit for Both Attackers and Defenders," CSO, April 19, 2018

37 Eianav, Yoav, "Amazon Found Every 100ms of Latency Cost Them 1% of Sales," Date Here??

38 Lackey, Zane, "It's the Most Wonderful Time of the Year … for Hackers," Total Retail, December 9, 2019

39 Ponemon Institute, "2019 Cost of a Data Breach Report," Date Here??