CEQUENCE

Retail Threat Surge

Navigating the Cyber Storm of Peak Shopping

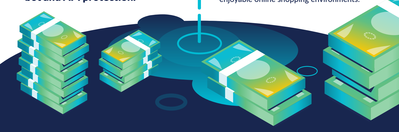
The excitement of major retail sales events and the holiday rush brings a flurry of activity, but also introduces risks that can impact both consumers and businesses. Increased traffic during these peak times often masks significant cybersecurity threats and financial losses. Whether you're a retailer aiming to protect your business or a consumer looking to stay secure, understanding these risks and the importance of robust protection is essential.

Retailers could lose up to

$60,000

every hour, without proper bot and API protection.

Retailers could lose up to $60,000 every hour without proper bot and API protection, especially during peak periods like Labor Day sales events. For businesses, this highlights the importance of investing in security. Consumers benefit from these investments as they contribute to safer and more enjoyable online shopping environments.



Sales/Promotion Vulnerability

Major sales events, such as summer promotions, lead to a notable rise in legitimate traffic, which can also conceal and even attract cyberattacks against businesses. For consumers, this means a higher chance of encountering fraudulent activity or losing out on limited edition items, while businesses face increased risk of compromised security and customer dissatisfaction.

During a recent major sales event for a Cequence retail customer:

Total blocked bot traffic surged

435%

compared to normal levels.

The volume of malicious traffic increased a staggering

2,724%

indicating a significant surge in malicious activity.

Effective Protection

Cost Savings

Cequence's API security and bot protection saved retail customers

$3.8M

during the Labor Day sales period by blocking over 26.7 million account takeover (ATO) attempts. For consumers, this translates to fewer disruptions and a more secure shopping experience.

26.7M

ATO attempts were made.

Threat Mitigation

During the Labor Day sales period, the retail sector faced a

79%

surge in blocked bot traffic from the previous year.

Additionally, the proportion of malicious traffic skyrocketed by

96%

leaping from approximately 10% to 20%.

19.8%

of traffic was blocked based on IP reputation, emphasizing the crucial role of achieving a strong Return on Security Investments (ROSI).

Unmatched Security

6.7B **API transactions were protected within the first week of the iPhone 16 debut.**

Since the release of the iPhone 16, Cequence has flawlessly processed over 6.7 billion API transactions for eight of the world's leading telecommunications giants, without a hitch.

37% **of that traffic was malicious,** showcasing the critical importance of our advanced security measures.

Enterprises should start demanding that cybersecurity solutions provide tangible, hard savings, not just the soft savings of potential protection from cyber attacks that the industry typically celebrates.

To mitigate these risks, retail businesses should consider these steps:

STEP 1

Practice, Practice, Practice

Review policies and procedures, and even run practice drills focused on your organization's unique risks. Consider the perspectives of the company, the customer, and the attacker.

STEP 2

Know What to Protect

Keep a detailed and up-to-date inventory of your public-facing applications and associated APIs that are on the front line of attack. You can't protect what you don't know exists, and many attacks succeed due to overlooked or unknown endpoints.

STEP 3

Prioritize Business Goals

Focus on what drives success for your business. If speed is key, optimize performance. If user experience matters, ensure secure and fast user validation using methods like canary headers, known IPs, and device IDs, and add extra checks for deviations.

STEP 4

Leverage Your Security Systems

Implement multi-factor authentication. Monitor your systems for unusual activity, especially during peak times.

STEP 5

Monitor User Activity

Track login patterns. For example, if a user typically logs in once a week but suddenly logs in 50 times in an hour from IP addresses spread across the world, this could indicate an account takeover attempt.

Navigating high-traffic periods and promotional events presents challenges for both businesses and consumers. By understanding these risks and investing in comprehensive security solutions, businesses can safeguard their operations and protect their customers from cyber threats. For consumers, this means a safer, more secure and enjoyable online shopping experience. Stay informed and secure to keep both shopping and business activities smooth and protected.

Retail enterprises - try a free API security assessment today:

www.cequence.ai/assessment/

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai

Cequence-RetailAttackInfographic-20240918