CEQUENCE

The Aftermath of
Black Friday & Cyber Monday

A Growing Threat to E-Commerce

Average Potential Losses for Businesses per Hour

$2.58M

While the holiday shopping season brings joy for consumers, it also signals an alarming rise in cybercrime.

At Black Friday and Cyber Monday come to a close, malicious bot traffic and fraud attempts continue to surge, posing a significant threat to e-commerce businesses. Throughout December, as consumers rush to complete their holiday shopping, businesses can expect to see an average potential loss of $2.58 million per hour. With cybercriminals ramping up their efforts, understanding these trends is crucial for organizations to protect themselves from severe financial losses during the remainder of the holiday season. This report, powered by insights from the Cequence CQ Prime threat research team, highlights key security trends and provides actionable steps for businesses to stay ahead of evolving cyber threats.

Transaction Volume
E-Commerce Growth

This highlights the continued rise of e-commerce as businesses attract more consumers. However, with this growth comes an increased risk of exploitation by cybercriminals.

Malicious Traffic
A Growing Danger

This illustrates how the rise in legitimate transactions has been matched—and even surpassed—by an alarming increase in fraudulent activity. A larger attack surface means cybercriminals are leveraging new strategies to disrupt businesses and exploit vulnerabilities.

Potential Losses
The Financial Toll

Black Friday — Cyber Monday
Nov. 22 - Dec. 2, 2024

Potential Losses:

$681M

During this 11-day stretch, businesses faced an astounding **$681.12 million in potential financial losses**. This period marked the height of online shopping activity, making it a prime target for cybercriminals. Attacks during this time were dominated by tactics such as credential stuffing, fake account creation, and bot-driven inventory hoarding, all of which directly impacted businesses' bottom lines.

Month of December 2024
Dec. 3 - Dec. 31, 2024

Potential Losses:

$1.79B

The surge in malicious activity will not stop after Cyber Monday. Throughout December, as consumers rush to complete their holiday shopping, businesses can expect to see an **average potential loss of $2.58 million per hour, culminating in $1.79 billion in losses by year-end.** This extended threat window shows that cybercriminals capitalize on every opportunity, using sophisticated attack methods to exploit high-traffic times.

REAL WORLD APPLICATIONS

SMS Pumping Attacks Mitigated

Cequence Security's solution helped a major e-commerce company successfully mitigate an SMS pumping attack. The attackers exploited an account creation endpoint to trigger fraudulent SMS messages, resulting in significant financial losses.

The fraudulent activity cost the company $3,000 every four hours at peak. Cequence's advanced bot and API protection identified the attack early and blocked the account creation process, effectively preventing further financial damage. The attack was mitigated starting in early November 2024, with the attackers ceasing their activity by the end of the same month.

$3,000
Lost every 4 hours

Traffic Surge

Cequence Security ensured uninterrupted service despite a 125% increase in traffic.

A leading e-commerce brand experienced a **2.1 billion request surge** on Black Friday, with **11.5 million malicious attempts mitigated.**

Mitigating High-Impact Threats

From credential stuffing to scraping attacks, Cequence Security stopped cybercriminals in their tracks.

Credential Stuffing
Malicious Requests Mitigated:
970,000
Malicious IPs Blocked:
48,000

Scraping
Malicious Requests Mitigated:
691,000
Malicious IPs Blocked:
150,000

Total Traffic Handled for the E-Commerce Industry

Cequence Security safeguarded e-commerce platforms from a massive influx of malicious traffic, ensuring seamless customer experiences.

During the holiday week, Cequence Security managed 3.7 billion requests, blocking 317 million malicious requests.

317M
MALICIOUS REQUESTS

3.7B
TOTAL REQUESTS

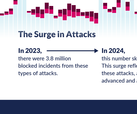
Total Mitigated Traffic
A Wave of Activity

Rise of Distributed Credential Stuffing and Token Farming
The Underestimated Threats

These attacks often go unnoticed because they use automated tools and hidden traffic. As businesses grow online, they become more vulnerable, giving cybercriminals a chance to exploit weaknesses and avoid detection, putting important systems and data at risk.

Distributed Credential Stuffing:
This is when cybercriminals use stolen usernames and passwords (often from past data breaches) to try to break into accounts. They use many different devices or IP addresses to hide their tracks and avoid getting caught.

Token Farming:
This involves using bots to gather special codes or credentials that allow access to restricted services or systems. Cybercriminals use this to exploit offers, access exclusive content, or carry out fraud.



The Surge in Attacks

In 2023, there were 3.8 million blocked incidents from these types of attacks.

In 2024, this number skyrocketed to 26.8 million, marking a 700% increase. This surge reflects the increasing sophistication and frequency of these attacks, as cybercriminals target high-value platforms with more advanced and automated tactics.

Key Takeaways

Malicious Traffic is Growing Faster Than Transactions
As legitimate e-commerce growth continues, cybercriminals are scaling their attacks at a faster pace. This imbalance highlights an urgent need for businesses to rethink their security approach.

Bot Protection Isn't Just for Cyber Monday
Bots are constantly evolving, with credential stuffing and token farming attacks seeing a massive rise. Businesses can't afford to let their defenses lapse after Cyber Monday ends.

The Financial Risk is Real
With up to $681 million in potential losses over the Black Friday-Cyber Monday period and $1.79 billion throughout December, the cost of inaction is steep.

The Christmas Rush Brings More Than Just Shoppers
Cybercriminals use the Christmas shopping rush to conduct their biggest fraud campaigns. Without robust bot management systems, businesses are at risk of fraud, pricing scraping, and a degraded customer experience.

Top 5 Tips to Defend Against Malicious Traffic

TIP 1
Agent-Centric AI Security

As digital threats evolve, Agentic AI security solutions rise to the challenge, surpassing traditional bot detection. By leveraging advanced machine learning, dynamically identify and mitigate sophisticated threats in real time, ensuring proactive and adaptive protection against malicious activity.

TIP 2
Enhance Fraud Detection Algorithms

Fraudulent transactions are on the rise. Strengthen your fraud detection systems to adapt to evolving threats like account takeover and credential stuffing.

TIP 3
Leverage Multi-Layered Security Solutions

Combine solutions like API protection, web application firewalls, and bot mitigation tools to address complex, multi-faceted attacks effectively.

TIP 4
Invest in Real-Time API Protection

As APIs become an increasingly attractive target for cybercriminals, it's crucial to implement real-time API security solutions to mitigate risk and protect sensitive data.

TIP 5
Monitor Traffic and Transactions 24/7

The rise in cybercrime doesn't take holidays. Constant monitoring of traffic and transactions can help businesses identify suspicious patterns and stop attacks before they cause harm.

The Holiday Rush Continues
Stay Ahead of Cybercriminals

With over a billion in malicious traffic already recorded, businesses must stay vigilant. The holiday shopping season isn't just about great deals—it's about protecting your revenue and your customers' trust. Investing in advanced bot and API protection will safeguard your business from malicious attacks, ensuring smooth and safe shopping experiences all month long.

Learn more about how Cequence Security's advanced API security and bot management solutions can protect your business from cyber threats throughout the holiday season and beyond.

Methodology
This report is based on analysis conducted by the Cequence CQ Prime threat research team, focusing exclusively on malicious traffic targeting the retail sector during the 2022 and 2024 holiday shopping seasons.

Key Data Points
Malicious Traffic Trends: Data was collected from Cequence's Unified API Protection (UAP) platform, focusing on blocked threats such as credential stuffing, token farming, and inventory fraud.

Potential Financial Losses: Calculations were based on the average value of blocked malicious transactions and their impact on retail revenue.

Year-Over-Year Comparisons: Insights reflect changes in threat activity between the 2022 and 2024 holiday seasons.

Limitations
Data represents only retail-specific activity and may not reflect trends in other industries.

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

Cequence Unified API Protection (UAP)