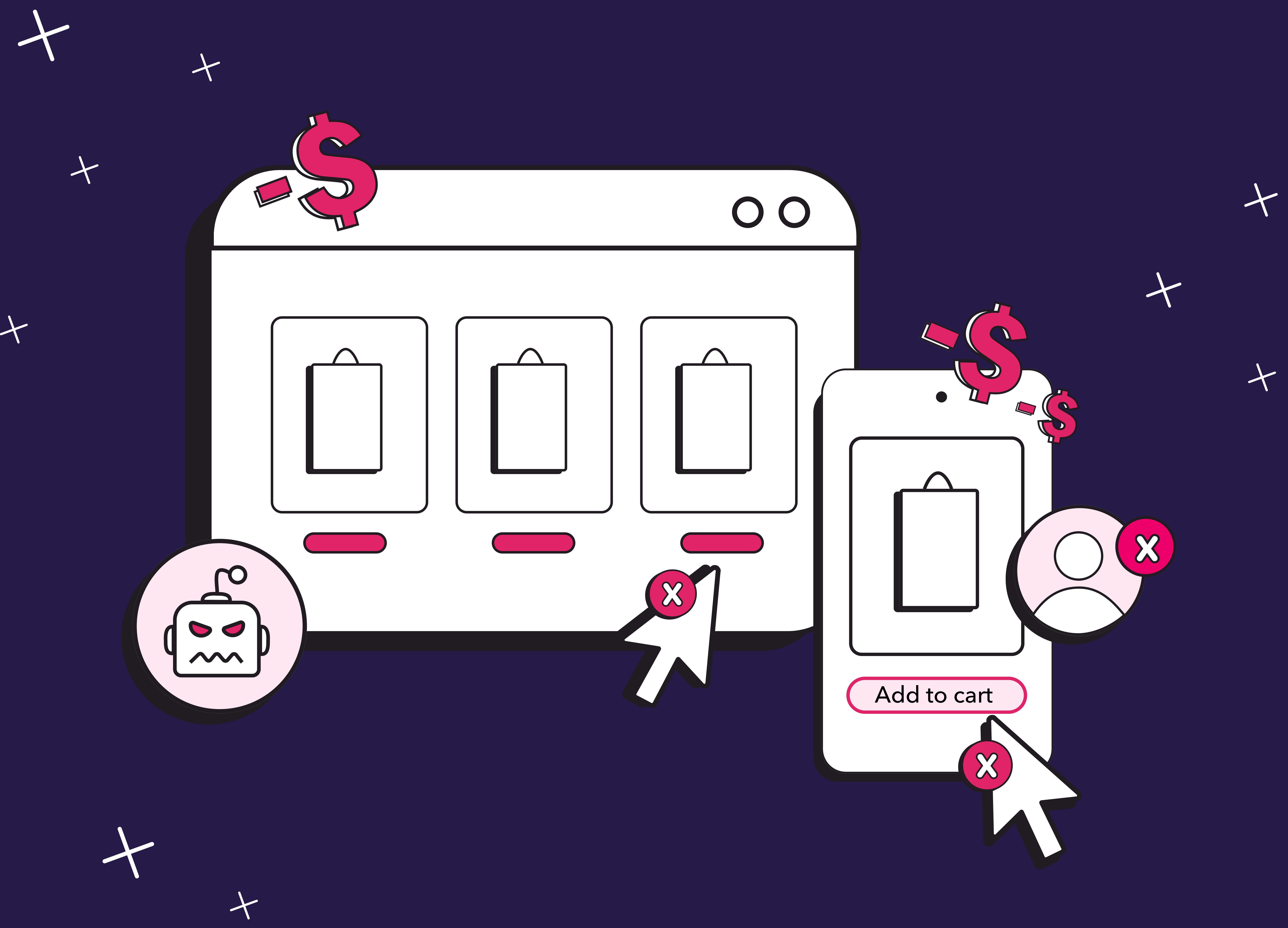
Fake Traffic Doesn’t Take a Holiday

How Bots & Fake Users Impacted the 2023 Holiday Shopping Season



Introduction & Methodology

According to Digital Commerce 360, online sales continued to grow year over year during the 2023 holiday season. In fact, spending increased to $221 billion, up 4.9% compared to 2022. As online eCommerce continues to drive sales for retailers at an increasing rate, it becomes even more important that businesses make the most of every site visit, interaction, and transaction.

NRF National Retail Federation

"2023 Holiday to Reach Record Spending Levels"

CNN BUSINESS

"Energized shoppers break one-day holiday sales record"

AP

"American Consumers Are Feeling Much More Confident as Holiday Shopping Season Peaks"

Unfortunately, this eCommerce growth has also led to a proliferation of bots, fake users, and malicious actors looking to derail retailer goals.

We analyzed **400 million** visits to retail and eCommerce websites during the 2023 holiday shopping season (Black Friday through New Year's Eve) and compared it to data from 2022. The analysis leverages CHEQ technology, which applies more than 2,000 cybersecurity challenges to each visitor, including tests on behavior, device attributes, browser signals, and network indicators.

2023's Holiday Traffic Headaches:

- Malicious automation tools that can expose sensitive data and customer information
- Bots and scrapers that can undermine pricing models and unique product offerings

Fake Traffic = Real Threats

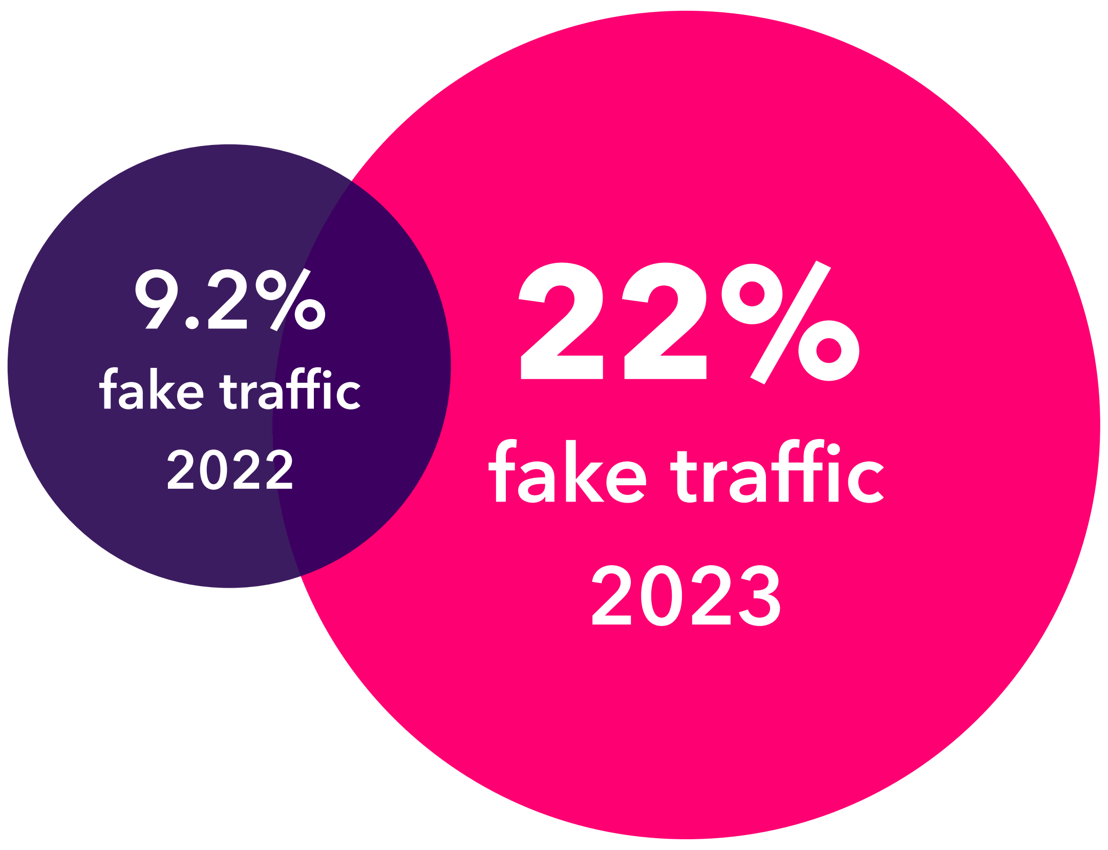
Cart stuffing and denial of inventory that harms genuine customer experience

Promotional and advertising abuse that disrupts marketing funnels and drains budgets

Skewed metrics that negatively influence decision-making

Holiday Research Results

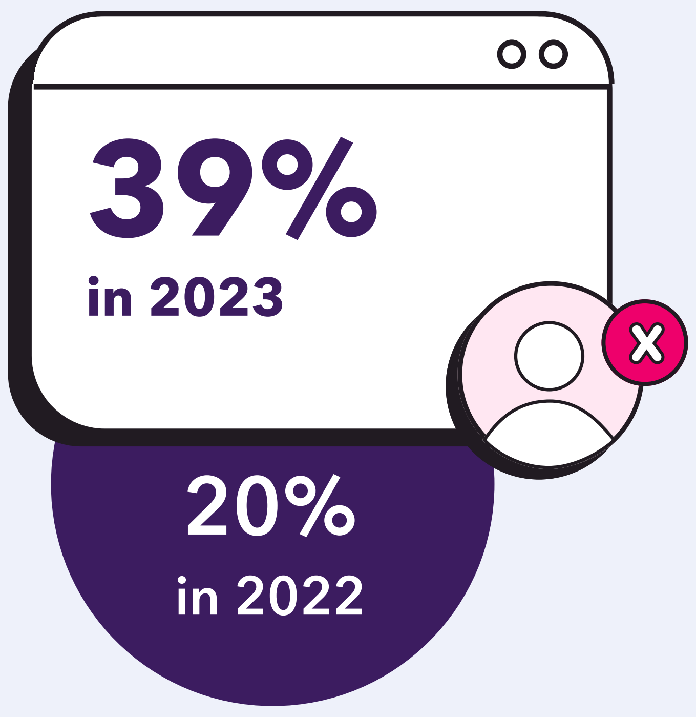
Fake Traffic Rates During the Holiday Season
2022 vs. 2023



● 21.8% of traffic to retail websites during the **2023 Holiday Season** (Nov. 24 - Dec. 31) was comprised of bots and fake users.

● 9.2% of traffic to retail websites during the **2022 Holiday Season** (Nov. 25 - Dec. 31) was comprised of bots and fake users.

Desktop vs. Mobile



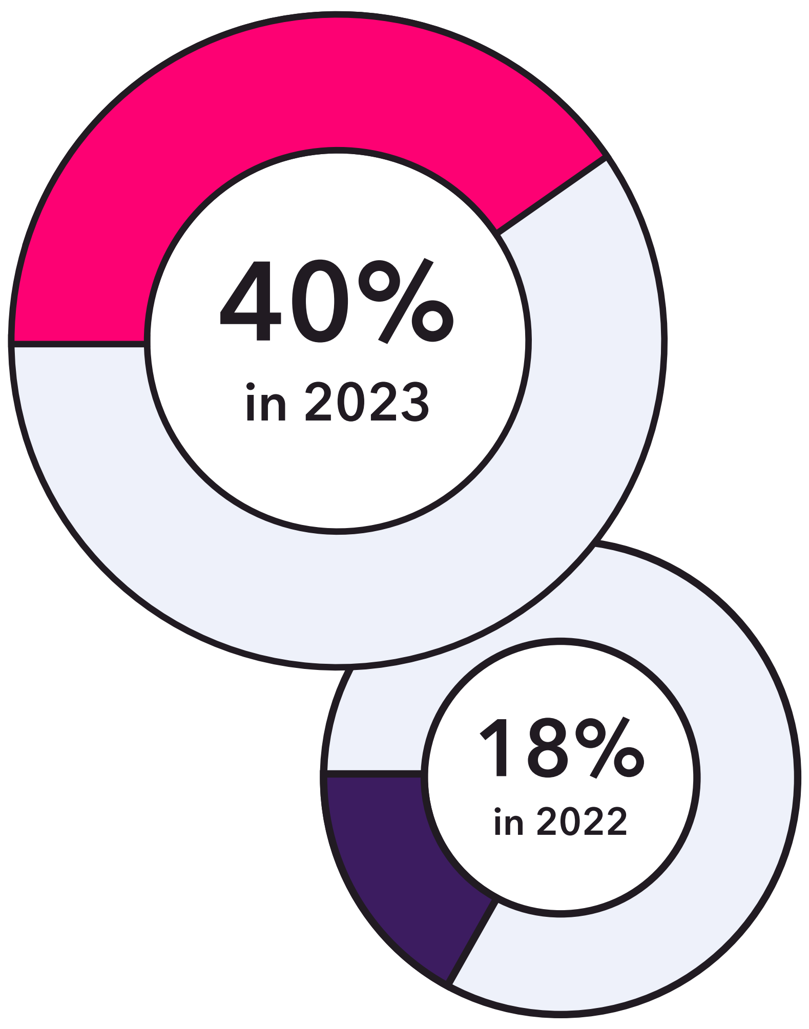
When looking at only Desktop devices in 2023, the fake traffic rate was even higher, at 39.2%. This could be due to the ease at which bots can be created and deployed via desktop.

For Mobile devices in 2023, the fake traffic rate was slightly lower than the overall average, at 12.3%. However, mobile fake traffic is still posing a significant threat to business continuity and brand reputation.

Direct Traffic Disappointments

Direct Traffic rose to the top of the naughty list in 2023. This type of traffic is also known as "dark traffic" because it refers to website visits that have no defined source or referring site. The term Direct Traffic can be misleading because it can be the result of users typing in your website URL, as opposed to arriving on your site from clicking on an ad or search engine result, but it can also be the result of nefarious activity.

An increase in authentic direct traffic can be a sign of strong brand recognition, but an increase in fake direct traffic could mean your business is falling victim to brute-force targeted attacks.



What eCommerce Leaders Can Do

With bots and fake users accounting for **one in four** visitors on retailer websites during the peak of the holiday shopping season, eCommerce professionals may be wondering what they can do to identify and mitigate potential threats in their day-to-day.

Diagnosing common challenges:

For unexplained spikes in traffic

Check for commonalities or abnormal patterns. Are you getting an influx of traffic all coming from a new region you've never serviced, or through a channel that rarely generates that much traffic? Consider working with your security or analytics team to analyze additional granular attributes.

For low conversion rates

Unless a bad actor is using stolen credentials to make a purchase, fake traffic typically drives down conversion rates by driving up page traffic without converting. If one or multiple products see sudden or abnormal drops in conversion rates, dive deeper to investigate the quality of that traffic.

For fake or polluted customer data

Seeing your database and/or retargeting pools polluted with junk? Investigate the sources and commonalities. Look for misaligned information such as contact names that don't match the email name, SMS area codes from excluded geographies, and garbled text.

For cart stuffing

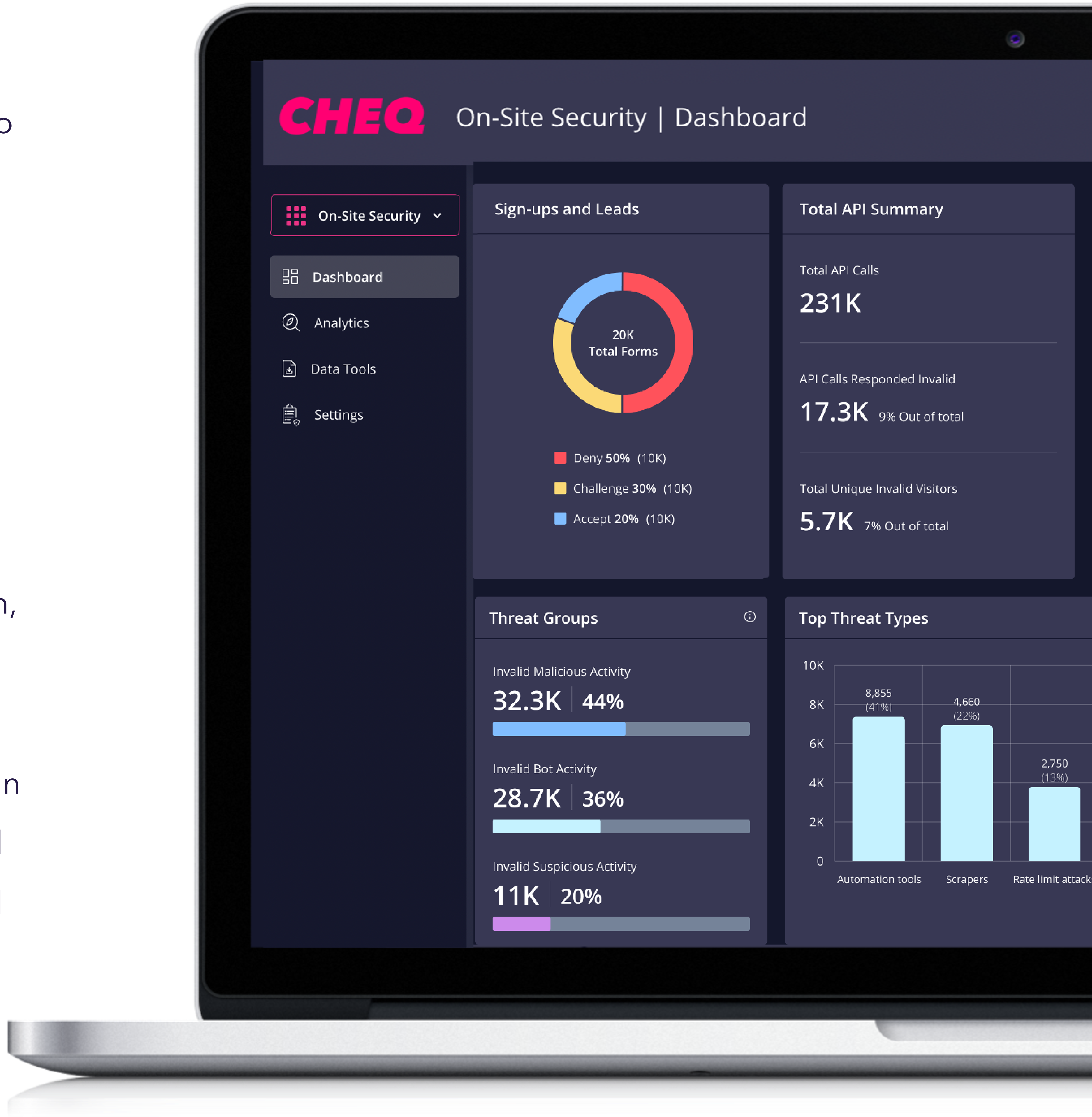
If your customers are experiencing denial of inventory with a corresponding dip in your sales, reduce the amount of time an item is allowed to be sitting in a cart without completing a purchase in order to block bots from hoarding inventory and preventing real purchases.

Get proactive protection with CHEQ

The team at CHEQ has years of experience tackling these specific issues and staying ahead of new and sophisticated threats to retailers. Since 2016, we've worked with leading retail brands to protect their campaigns, websites, funnels, and data from bots and fake users. Reach out today to learn more.

About CHEQ

CHEQ is the leader in Go-to-Market Security, trusted by over 15,000 customers worldwide to protect their metrics, marketing efforts, and customer data from those with potentially malicious intent online.



Powered by award-winning cybersecurity technology, CHEQ offers the broadest suite of solutions for securing the entire GTM org from threats to business continuity, brand reputation, and marketing effectiveness.

Schedule a demo today to learn how CHEQ can help you block fake traffic on your website and keep your go-to-market operation clear of bad leads and malicious actors.

Customers Love Us on G2

Leader 2023

Easiest To Do Business With 2023

Best Support 2023

Momentum Leader 2023