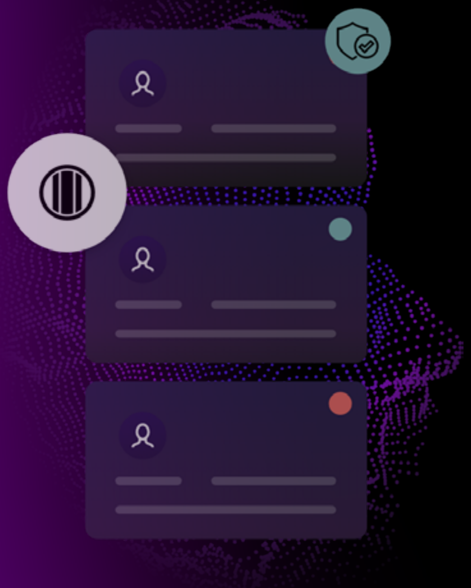
# Holiday Readiness Guide: Stop Fraud in its Tracks

Bot traffic will surge before the holiday shopping season. Is your business prepared to fend off attacks? HUMAN Security on Google Cloud will help you stave off those holiday bot blues!



HUMAN Google Cloud

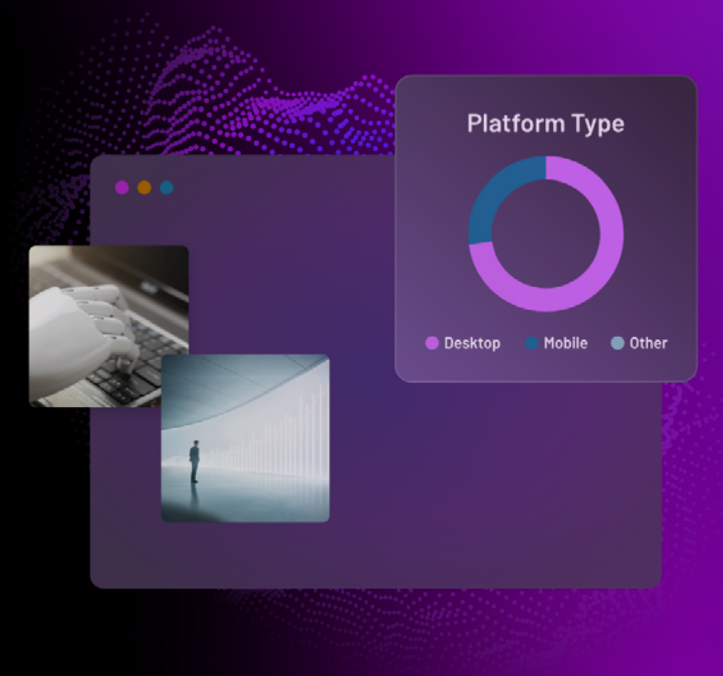
# Bad Bot Traffic Surges in October. Is Your Business Prepared?

Consumers are predicted to spend over $260 billion with e-tailers in the U.S. this 2023 holiday season. Without adequate bot protection, millions of businesses will face reputational and financial damage from bots taking over accounts, making fraudulent purchases, manipulating inventory, scraping proprietary content, inflating engagement with media, and hoarding hot products.

## Holiday season cybercrime has a significant impact on e-commerce businesses, these include:

- Chargebacks and lost revenue resulting from fraudulent purchases that require you to refund customers.
- Lost revenue as bots tie up your inventory, sending shoppers to competitor sites.
- Regulatory fines for PCI DSS non-compliance if your customers' payment data is exposed due to leaky forms or Magecart/digital skimming attacks.
- Increased infrastructure costs and latency as greater bot activity taxes your bandwidth and slows website performance.
- Damage to brand reputation and consumer trust that follows a data breach or fraud incident.
- Poor decision-making based on skewed web data that includes bot activity.
- More significant burden on internal resources (such as customer service, fraud, and IT teams) tasked with responding to security incidents.
- Loss of competitive edge due to scraping bots stealing, analyzing, and reposting product and pricing information.

SCROLL >>>



**4.8 BILLION**
**unique devices on the internet.**

**HUMAN observes**
**3 BILLION**
**every month.**

## Trusted Partners for Trusted Security

The Human Defense Platform on Google Cloud protects your business with advanced, automated, and sophisticated solutions that are quick and easy to deploy within days.

- **HUMAN verifies 20 trillion interactions** every week with up to 2,500+ signals parsed through 350+ algorithms to reach a single critical decision - bot or not.
- **There are approximately 4.8 billion unique devices on the internet**, and HUMAN observes 3 billion every month.
- **The Human Defense Platform operates on Google Cloud** and is available on the Google Cloud Marketplace for easy procurement.
- **The Human Defense Platform** cost counts towards satisfying your Google Cloud financial commitment and conveniently appears on your Google Cloud billing.
- **HUMAN Security on Google Cloud automatically scales** to meet spikes in bot traffic so you can have peace of mind that your digital assets are serving people and not bots during the holiday season.

Disparate point solutions cannot provide the Human Defense Platform's unmatched scale, speed, and precision, combined with the capabilities of Google Cloud.

SCROLL >>>

# Our Platform Ensures:

**LOW LATENCY**

**MARKET-LEADING ANALYTICS CAPABILITIES**

**COMPREHENSIVE SUPPORT FOR HUMAN'S SECURITY SOLUTIONS**

**RAPID DEPLOYMENT**

**CUSTOMIZABLE SOLUTIONS TO MEET YOUR SPECIFIC NEEDS**

HUMAN ensures a modern, cloud-native solution that leverages the capabilities of Google Cloud. Let's look at how our solution can protect your customers at every step of the user journey this holiday season - and beyond.

# Protect Your Customer

Your customer is at risk from the moment they enter your website throughout their journey to check out and beyond. No online business is immune to bots.

However, HUMAN Security on Google Cloud safeguards the entire customer journey to protect your customer and business.

Let's look at the attack surfaces during your customer's journey.

SCROLL >>>

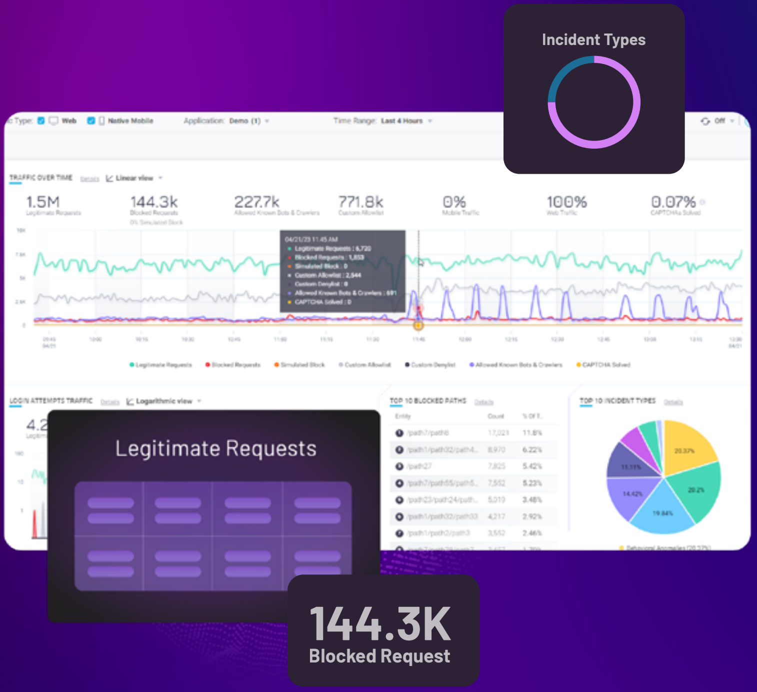
# Your Website is an Attack Vector

Your homepage is your digital front door, and bots are knocking 24/7/365.

## Modern bots can do exceptional damage to your business by:

- Taking over existing accounts or creating fake accounts to commit fraud or account abuse.
- Capturing product and pricing information from your web pages allows competitors to analyze your strategy and repost your content.
- Posting fake reviews and ratings to influence purchasing decisions, tearing you down, or propping up competitors to encourage your customers to choose competitors'  products.
- Skewing your web engagement metrics so future decisions about ad spend, marketing campaigns, and product inventory are made using bad data.

## Bad bots remove your competitive edge, stealing your content, customers, and revenue.



04/21/23 11:45 AM
- Legitimate Requests : 6,720
- Blocked Requests : 1,853
- Simulated Block : 0
- Custom Allowlist : 2,544
- Custom Denylist : 0
- Allowed Known Bots & Crawlers : 691
- CAPTCHA Solved : 0

| Entity | Count | % Of T... |
|---|---|---|
| /path7/path8 | 17,021 | 11.8% |
| /path1/path32/path4... | 8,970 | 6.22% |
| /path27 | 7,825 | 5.42% |
| /path7/path55/path5... | 7,552 | 5.23% |
| /path23/path24/path... | 5,019 | 3.48% |
| /path1/path32/path33 | 4,217 | 2.92% |
| /path1/path2/path3 | 3,552 | 2.46% |

# Solution

**HUMAN Scraping Defense** safeguards your web and mobile applications from web scraping bots. Our solution uses behavioral profiles, machine learning, and real-time sensor data to accurately identify sophisticated scraping bot attacks.

**HUMAN Data Contamination Defense** filters out bot-generated traffic from real human traffic. It improves your marketing analytics and metrics, detecting and removing bot traffic from organic and paid data sources, ensuring you are not counting clicks from bots. This enables you to confidently make decisions about your marketing programs and budgets.

# Account Pages can be Exploited

From login and account creation to navigating through an account post-login, cybercriminals exploit your accounts to commit all types of fraud, putting your business reputation at risk.

Malicious bots attempt logins with stolen usernames and passwords to gain unauthorized access to user accounts. They can also create very realistic fake accounts. From here, they can:

- Change account credentials, shipping addresses, or emails in existing accounts.
- Make fraudulent purchases with stored payment cards, gift cards, account balances, or loyalty points.
- Post fake reviews, commit return fraud, and steal stored personal identifying information (PII).
- Create fake accounts en masse to take advantage of sign-up and promotional offers.

# Solution

**HUMAN Account Takeover Defense** stops automated credential stuffing, brute forcing, and account takeover (ATO) attacks. Our module blocks login with compromised credentials, rendering them useless before ATO fraud occurs. It also identifies suspicious post-login activity and remediates breached accounts to prevent fraud. The solution secures online accounts with multilayered defenses at each step of the attack chain.

**HUMAN Account Fraud Defense** detects and prevents cybercriminals from creating new accounts using fake or stolen identities. Using behavioral analysis, the solution applies continuous authentication to monitor account abuse throughout the customer journey on your website or web app. It detects and prevents fake account creation attempts in real-time, blocking automated abuse and targeted, human-led fraud.

SCROLL >>>

# Shopping Cart Pages Are High Risk

Before customers can make a purchase, they must add an item or service to a shopping cart. Bots are programmed to do this at millisecond speed and at a scale that humans can't compete against.

Bots repeatedly add the same product to their shopping cart, depleting your inventory and driving your customers to shop elsewhere. They can also snatch up high-demand goods before real shoppers can. This disappoints customers and forces them to buy those coveted items on secondary markets at inflated prices.

# Solution

**HUMAN Transaction Abuse Defense** prevents automated bots from hoarding your inventory. It detects and blocks malicious bots on your web and mobile applications — in real-time with unparalleled accuracy. It also stops scalping in its tracks by performing detection out-of-band without adding yet another layer of traffic processing. The enforcement is done inline, and bots are blocked close to the edge. This preserves page load performance and user experience.

SCROLL >>>

# Your Checkout Page is a High-Value Target

The final action for any e-commerce customer is completing a purchase or redeeming a promotional offer. Ensure your checkout page is protected so your customers will keep coming back.

Bots can make fraudulent purchases with stolen credit, debit, and gift cards. They can also drain account balances and loyalty points. Cybercriminals inject malicious client-side code to manipulate your payment forms and skim your customers' credit card data when they check out, destroying your customer's trust in your business. Bots can also make fraudulent purchases with stolen credit cards and snatch inventory to resell on secondary markets.

## Solution

**HUMAN Client-side Defense** uses advanced behavioral analysis to stop Magecart/digital skimming and other client-side supply chain attacks on your website. It provides complete visibility and control over first-, third-, and nth-party scripts running on the client side.

**Human Challenge: The Frictionless CAPTCHA** keeps your buyers on the path to purchase, stopping fraud while protecting your revenue. The **Human Challenge** is only served to risky user profiles, meaning that only 0.01% of human users will ever see it. Solve times for the Human Challenge are 4-6x times faster than market equivalents, and abandonment rates are 3-5x times lower, smoothing your real customer's buying journey.

**HUMAN Transaction Abuse Defense** also stops carding bots from making fraudulent purchases that force you to refund your customers. HUMAN detects and stops sophisticated bots with various mitigation actions, including hard blocks, honeypots, misdirection, and serving deceptive content—all without adding unnecessary friction to the user experience.

SCROLL >>

> "In just one hour of one day, if we had not had HUMAN in place, we would have seen about **34,000 hits** on our backend payment processor. **That's about $3,100 (in fees) in just an hour**."

*Lee Tarver,*
*Senior Manager of Information Security Architecture and Engineering,*
***Sally Beauty***

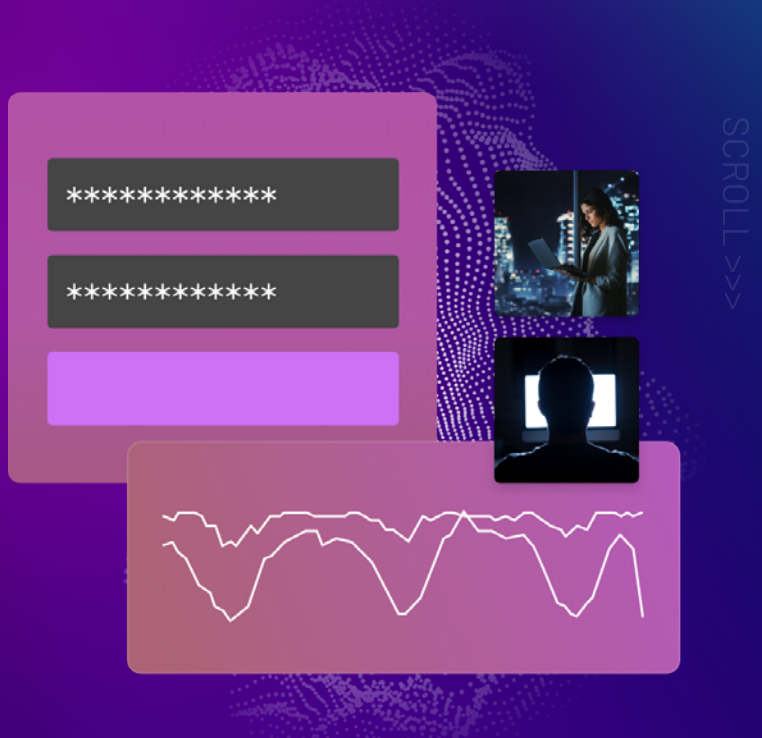
# HUMAN Security on Google Cloud Keeps Fraudsters and Grinch Bots Away

The Human Defense Platform on Google Cloud offers advanced bot mitigation solutions to stop automated fraud on websites, mobile applications, and APIs.  Using behavioral analysis and 300+ machine learning algorithms, HUMAN detects and mitigates:

- Account takeover attacks
- Account fraud
- Transaction abuse
- Scraping
- Data contamination
- Client-side attacks

Our solutions seamlessly operate on the Google Cloud infrastructure to disrupt fraud and abuse everywhere along your customers' journey.

HUMAN is powered by a modern defense strategy built on the three pillars of **visibility, network effect,** and **disruptions and takedowns**. This enables the platform to protect against bad bots with speed, scale, and precision.



## VISIBILITY

**Detection at unmatched scale**

More than 20 trillion digital interactions are verified per week, and more than 3 billion devices are observed monthly to provide actionable intelligence

## NETWORK EFFECT

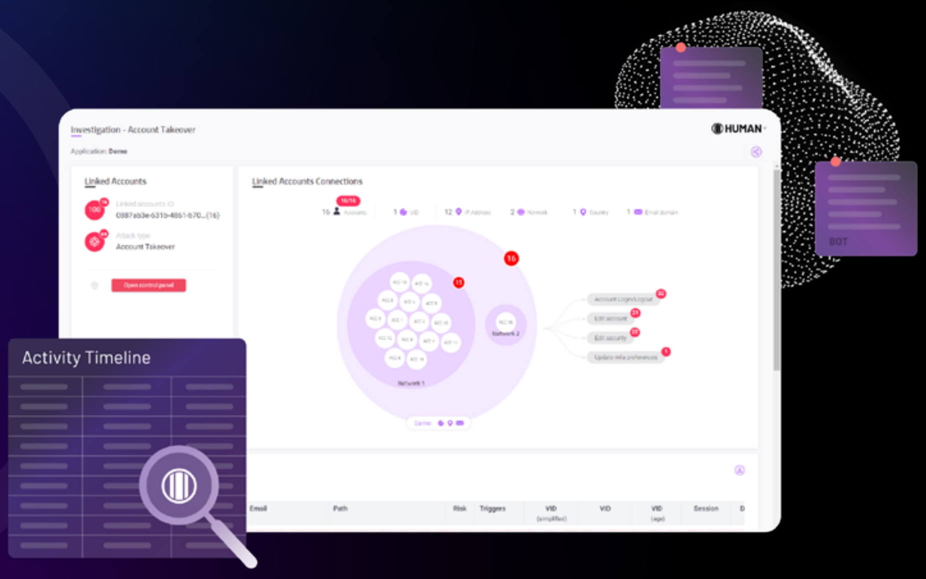
**Collective protection across the internet**

2500 dynamic network device and behavioral signals are parsed through 350 algorithms (technical, statistical, and machine learning)

## DISRUPTIONS & TAKEDOWNS

**Raise the cost of every digital attack**

10+ years of experience combating adversary attack vectors, tools, and methodologies to disrupt cybercrime through takedowns, deception, and other innovations



# Unleash Unrivaled Cybersecurity: Defend Today, Disrupt Tomorrow with HUMAN on Google Cloud.

Our unmatched visibility allows us to monitor the pulse of cyberthreats across the web, whether a bot attack on a single customer or a more significant attack hitting multiple organizations. With our network effect, we share knowledge, deploy protections for all our customers, and disrupt cybercrime with every mitigation action. We don't just block real-time threats but execute a range of responses that increase the cost to bad actors and deter future attacks.

By using modern defenses to disrupt the economics of cybercrime, the Human Defense Platform on Google Cloud delivers comprehensive protection leveraging the pillars of modern defense to combat tomorrow's cybersecurity threats today.

**Let us show you how to block bots and stop online fraudsters**

CLICK HERE >>> **FIND OUT MORE NOW** <<< CLICK HERE