HUMAN

Preventing Account Takeovers

HUMAN helps security and fraud teams prevent user account theft and abuse

Stop Cyber Criminals From Taking Unauthorized Ownership of Your Customer Accounts

Account takeover (ATO) attacks are when existing user accounts are compromised by cybercriminals. Often, these attacks run at scale and use sophisticated bots on compromised residential devices. ATOs cost little to carry out, have a high success rate, and have rippling advantages for cybercriminals. There are two main types of ATO:

Credential cracking is "brute force" breaking into accounts. Fraudsters obtain partial login credentials then use bots to try passwords at high volume and speed until they find a combination that works. The valid details are recorded and used elsewhere to log in to other accounts.

Credential stuffing is when attackers use stolen account credentials gathered from malware-infected machines or obtained from large data breaches. These stolen credentials are then tested against web applications to identify vulnerable accounts. Attackers then perform fraudulent transactions, steal PII, resell account credentials, or post fake content and reviews.

Risks Addressed

ACCOUNT RESELLING

THEFT OF USER PERSONAL INFO

TRANSACTION FRAUD

SPEAR-PHISHING

Safeguard Against Account Takeover

Today's sophisticated bots behave like real users and are designed to evade detection. As a result, businesses find it increasingly challenging to defend applications from automated attacks.

Even when apps function as intended, they are vulnerable to fraudsters using bots that mimic human behavior using mouse movements, keystrokes, and fake browser behavior. These sophisticated bots can easily evade bot detection features in conventional application security solutions that rely on behavioral monitoring or static lists, leaving your apps vulnerable to abuse.

Unlike traditional solutions, BotGuard for Applications combines superior detection techniques, internet-scale observability, and hacker intelligence to make bot or not decisions with no impact on page load times or friction on end-users. With this scale and speed, we can mitigate today and tomorrow's sophisticated bots.

Pain Points

Evolving threats

Novel attacks use thousands of residential devices to mimic human behaviors to access your applications that simple security measures cannot counteract.

Increased Risk

ATOs put your customers and your business at risk by exposing PII, preventing account access, and allowing attackers to perform fraudulent transactions.

Fraud and Identity Theft

When attackers gain unauthorized access to online accounts they can transfer funds, use stored credit card details or submit fraudulent credit applications.

Benefits to Your Business

Prevent Account Takeover

HUMAN's modern defense strategy stops account takeovers by sophisticated bots while providing friction-free access to your real customers.

Prevent PII harvesting

On protected pages, bots are blocked and can't harvest confidential information safeguarding your platform from a costly and brand damaging data breach.

Mitigate Risk

Gain peace-of-mind that your site is protected against the risk of scraping and PII harvesting by BotGuard's industry-leading detection precision and with minimal added friction.

The HUMAN BotGuard Advantage

Secure Accounts

For Real Humans Only:
Protect customer logins and new user registrations from account takeover attacks and PII harvesting while lowering captcha and multi-factor authentication friction for real humans.

Reduce Fraud

Prevent crime before it is committed:
Stop sophisticated bot attacks such as credential stuffing and cracking, which enable payment and wire transfer fraud, sensitive data theft, and other costly fraud-related losses.

Optimize Efficiency

Gain control and minimize losses:
Actionable insights help you reduce manual workflows and customize mitigation policies and responses to detect and prevent unwanted bot traffic from consuming time and infrastructure resources.

Powered by the Human Verification Engine™

BotGuard for Applications is powered by the Human Verification Engine combining technical evidence, machine learning, and continuous adaptation to deliver 'human or not' decisions with industry-leading accuracy, and minimal user friction.

We verify the humanity of 15 Trillion interactions per week, harnessing internet scale visibility and a decade of data to deliver continuously adaptive and mutually reinforcing protection to customers including the largest internet platforms.

Our Satori Threat Intelligence and Research Team takes down multiple large-scale attack networks every year, proactively identifying and reverse engineering new threats to inform our detection techniques with new indicators against emerging attacks.