HUMAN

Prevent Denial of Inventory

HUMAN helps security and fraud teams stop fraudsters from automating inventory abuse

Denial of Inventory and Stockouts

Scalping, spinning, stockouts. A sophisticated storm of eCommerce abuse.

In denial of inventory attacks, fraudsters use sophisticated bots to add an item thousands of times to online shopping carts until the item's inventory is exhausted, creating a stockout. Competitors can then steal your customers by providing them with the products you can no longer sell.

With scalping or spinning attacks, cybercriminals utilize automated bots to buy highly-prized products, such as limited-edition sneakers and clothes, concert tickets, or in-demand toys and game consoles. Sophisticated bots set up fake accounts that scour product pages, then buy your best products to sell them at inflated prices on third-party sites or the black market.

Risks Addressed

COMPETITIVE ASSAULTS

DENIAL OF INVENTORY

SCALPING & UNAUTHORIZED RESELLING

Safeguard against Denial of Inventory

Sophisticated bots behave like real users and are designed to evade detection. As a result, businesses find it increasingly challenging to defend applications from these automated attacks. A sophisticated bot can imitate human behavior using mouse movements, keystrokes, and fake browser behavior, using your applications as you intended. As a result, traditional application security solutions that rely on behavioral monitoring or static lists to detect bots are increasingly side-stepped.

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

Frustrated customers

Stockouts created by bots scalping in-demand products from your site, disconnect real customers from both your product and your brand, taking their business elsewhere.

Poor experiences

Scalpers create unfair scarcity, profiting from your customer and your brand, destroying trust in ticketing platforms, eCommerce marketplaces, and auction sites.

Reduced efficiency

Sophisticated bots generate unnecessary traffic that slows down your app, raises your infrastructure and service expenses and wastes your product team's time.

Benefits to Your Business

Stop Competitive Assaults

BotGuard's page load protection stops bots from accessing pages at scale and scraping content, protecting your pricing information and valuable data from theft and abuse.

Prevent Denial of Inventory

Stop scalpers and spinners from stealing your profits and customers' trust.

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 Account

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.