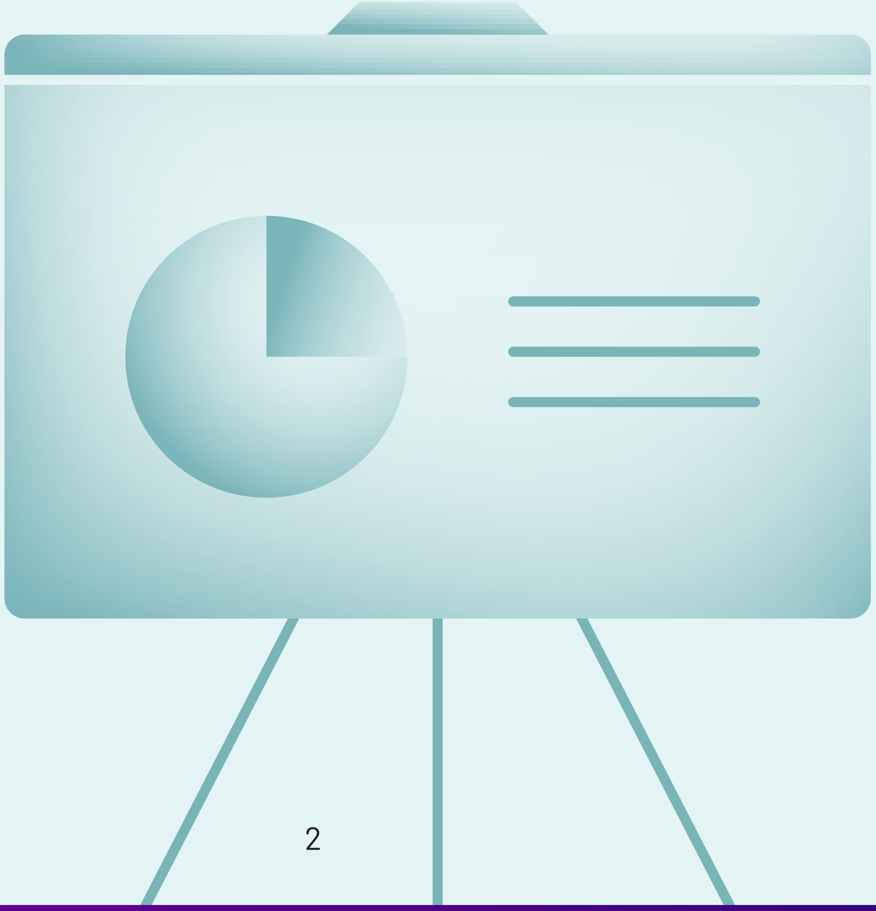
HUMAN

YOUR DIGITAL TRANSFORMATION IS BEING SABOTAGED
THE SURPRISING IMPACT OF SOPHISTICATED BOTS

Digital transformation promises business growth — it provides value to customers by using emerging technologies and skills to support new business models. Data-driven decisions are the lifeblood of this digital transformation. When data is poisoned, stolen, or misused for malicious intent, this slows business progress and results in poor customer experience and satisfaction.

In this paper, we'll explore how sophisticated bot attacks are contaminating digital transformation trends including automation, data analytics, and application architectures, then explain why solving these bot attack challenges should be part of every security strategy in 2022.



DIGITAL TRANSFORMATION IS HERE

According to an MIT Sloan Management report[1], digital leaders who embrace the advantage offered by digital transformation outperform their peers in every industry. Four out of five organizations increased their digital transformation budgets due to COVID-19[2] but this was only one factor in driving this change with **55%** of digital leaders believing that they will suffer financial loss or market share, to their competitors, if they do nothing[1]. Businesses want to reduce costs or increase revenue and the MIT study shows that those organizations that embrace digital transformation are, on average, **26%** more profitable[1].

The organizational change that drives digital transformation can be split into three main areas.

CUSTOMER EXPERIENCE

Improving customer experience with better processes — **72%** are excited about digital transformation to create better relationships with customers[2]

APPLICATION ARCHITECTURE

Choosing the right technology for your transformation — **86%** using cloud-native technologies to accelerate business outcomes[3]

DATA ANALYTICS

Getting your customer marketing data right — **91%** of customers are more likely to buy when you know their name and recommend products based on their purchase history[4]

However, **sophisticated** bots can hold your digital transformation strategy back. Bots are used in the attack path for **77%** of cybercriminal attacks[5]. Cybercriminals use bots for automation and scale in their attacks so security strategies that stop bots make it significantly harder for fraudsters to scale their attacks and sabotage your digital transformation.

HOW ARE BOTS SABOTAGING DIGITAL TRANSFORMATION?

Customer Experience

ACCOUNT TAKEOVER (ATO)

Account takeover attacks are when existing user accounts are compromised by cybercriminals. Often, these activities 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.

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. Given the high amount of password reuse, botmasters have high success rates in stealing account information and can perform fraudulent transactions, steal PII, resell account credentials, or post fake content and reviews.

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.

DENIAL OF INVENTORY & STOCKOUTS

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.

PAYMENT FRAUD

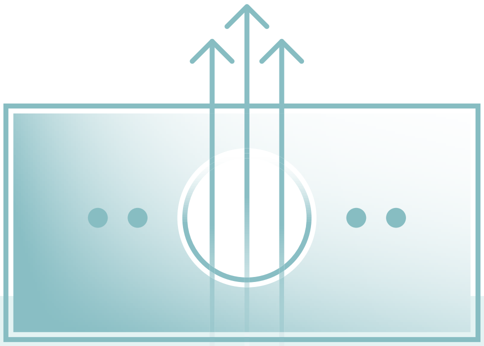
In payment fraud attacks, cybercriminals use sophisticated bots and lists of stolen credit card details on e-commerce sites to buy goods to then sell for a profit. Carding attacks focus on abusing the checkout page with stolen credit card information.

Criminals buy the lists of stolen credit card numbers, including security data such as CVV values, on criminal marketplaces. They then initiate bot attacks to test their cards by attempting small purchases to build a list of valid cards. When they've proven the card details are valid, the fraudsters will deploy sophisticated bots to use the verified card details to make e-commerce purchases, steal from accounts, and buy gift cards.

Gift cards are then sold at discounted prices or used to buy premium items like phones, televisions, and computers that can easily be sold on auction sites.

IMPACT

The impact to the organization can be substantial. Loss of customer confidence in the platform, increased support costs to deal with the customer problems created by bots, and the potential loss of revenue from customers. Many organizations attempt to solve this bot problem with a CAPTCHA solution. These have been shown to be ineffective at preventing bots but very effective at irritating customers — in a survey recently conducted by Human[6], **40%** of users stated that they had quit a login or transaction process from CAPTCHA frustration.



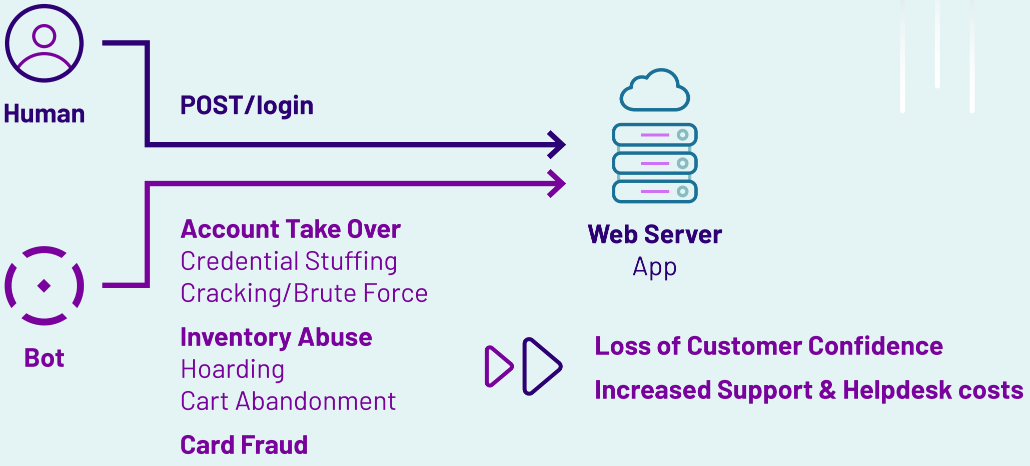


Diagram 1 - Customer Experience Impact

Customer Experience Case Study

The application team at a well known online bank considered that the bot management feature provided by their content delivery network (CDN) would be adequate to stop bots. However, the team was suspicious that sophisticated bots were breaching their defenses so they engaged Human in an attempt to discover if this were true.

Human immediately discovered that **14%** of their application traffic was from sophisticated bots whose activity was passing through the CDN's bot management feature completely undetected. The bots created fake accounts that the criminals then used to apply for loans, then transferred the proceeds to their external accounts.

With Human's guidance, the customer implemented friction in the form of multi-factor authentication when Human BotGuard detected bot activity. Because Human's 'bot or not' decisions are so accurate, that meant that the mitigation friction was effective in stopping the bots, but the real Human users could keep using their accounts without disruption from MFA — and the potential call center calls this new friction could create. The online banking provider kept these customers happy — and avoided fraud losses. What Human enabled them to do was to perform these major security updates in a controlled manner, without thousands of clients calling the helpdesk at once about problems gaining access to their account. Because the bank trusted Human's accuracy they were able to target their MFA friction effectively and only apply friction to the bots.

Data Analytics

CONTENT SCRAPING & PII HARVESTING

Web scraping isn't always bad, and good bots continually crawl websites to capture pricing data and product descriptions. Platforms like search engines and insurance comparison sites aggregate scraped data to make it easy for Humans to find the information they're looking for. However, malicious bots are also crawling your site and scraping your content with more sinister motives, using it to compete unfairly with your business or selling it on the dark web to criminals.

Fraudsters harvest PII by exploiting vulnerabilities in JavaScript or other code used to build websites and web applications. Software developers often use off-the-shelf code to add new capabilities and features to apps and websites. This approach can introduce unintended vulnerabilities that allow your adversaries to inject malicious code into your website, particularly where a vulnerability is well-known.

FAKE LIKES, CLICKS AND FORM FILLS

Businesses use all data at their disposal to make the best possible decisions and move audiences towards conversion. However, sophisticated bots look and act more like Humans than ever before and interact with all aspects of your marketing efforts. Unfortunately, when these bots enter your systems, they put all of your digital marketing investments at risk.

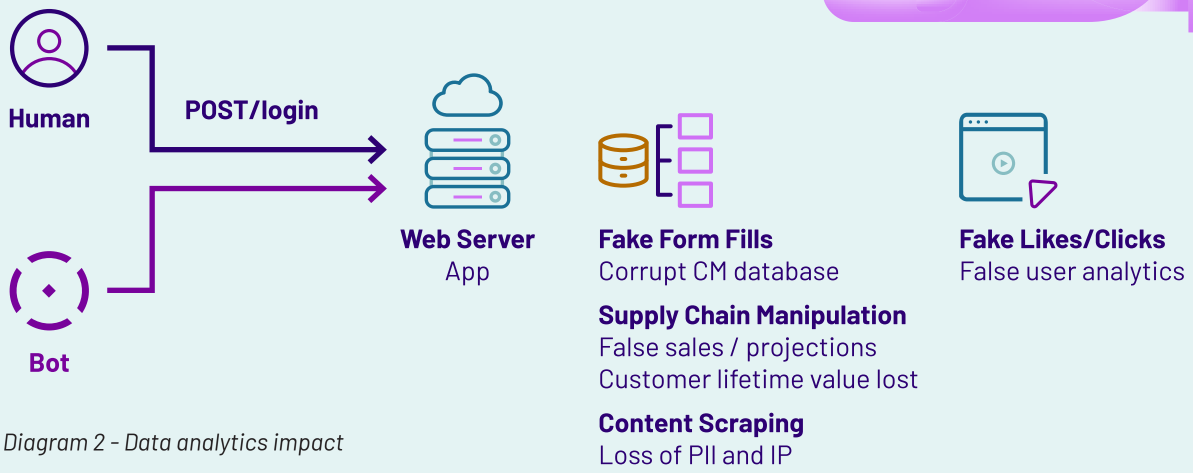


Diagram 2 - Data analytics impact

IMPACT

Bots can have a damaging impact on your organization's data and it's likely that **25%** of the database that you're marketing to is fake, fraudulent or bot[7]. Bots can be used to manipulate your application with fake likes and clicks or fake form fills, which risk poisoning your data and your CRM system. Bots can also disrupt your supply chain and scrape your site for pricing information or sensitive data. In the 2021 Marketing Fraud Benchmarking Report[7], **90%** of respondents used their own customer databases for email marketing and **82%** used it for remarketing and retargeting advertising campaigns. Both of these signal a challenge for marketers. Email marketing directed at fraudulent contacts may raise compliance issues, and remarketing and retargeting is wasted marketing budget when it's being done to fake or fraudulent contacts.

Data Analytics Case Study

A global entertainment company was using two leading bot management solutions to protect its digital purchase experience but bots were still getting through. A core function specifically designed to protect customers from fraud was under direct attack by sophisticated criminals.

The business was marketing this feature in their platform as fraud-free, but they were finding this difficult to deliver. The application team engaged Human to assist and Human engineers deployed the BotGuard detection tag on the platform. The Human team discovered that this platform was under attack from a bot net that was circling through 20 different bot agents and more than 14,000 home-user IPs to evade detection by the business's defenses.

The bots were highly sophisticated and mimicked Human behavior including typical daily browsing patterns to evade detection. The bots took information from sports leagues websites to determine when events were taking place, news sites so they could see what was trending, important events that might generate the most profit, even government sites to check covid restrictions in different locations as these would influence price and demand.

Bot detection products were already in place but this activity was completely missed by the Web Application Firewall (WAF) feature the customer had implemented. The customer has now implemented Human BotGuard at a number of points in their platform preventing event reservation fraud and millions of fraudulent event ticket sales and has greatly improved customer experience.

Application Architecture

NEW ACCOUNT FRAUD

Sophisticated bots can quickly and easily create large numbers of fake new user accounts. The accounts are either completely fake or are created using details where the real Human is unaware of the fraud. These new phony accounts are then used to carry out malicious activity, such as payment fraud, special offers and discount abuse, and spam and misinformation spreading.

Creating a new account needs to be quick and easy, so your consumer isn't frustrated and lost. You want users to create accounts to provide offers and discounts and ensure they become long-term clients. Customer accounts also help you monitor customer behavior enabling you to make sound business decisions. However, sophisticated bots can use that same easy system to register new account after new account to use for their cybercrimes.

CLOUD COMPUTE COSTS

There are quantifiable costs to your business of the cloud compute services wasted in serving bots that are scraping your site for pricing information, and, as we covered earlier in this paper, there are the costs in denial of service, and in bots buying up all your stock, sending customers elsewhere.

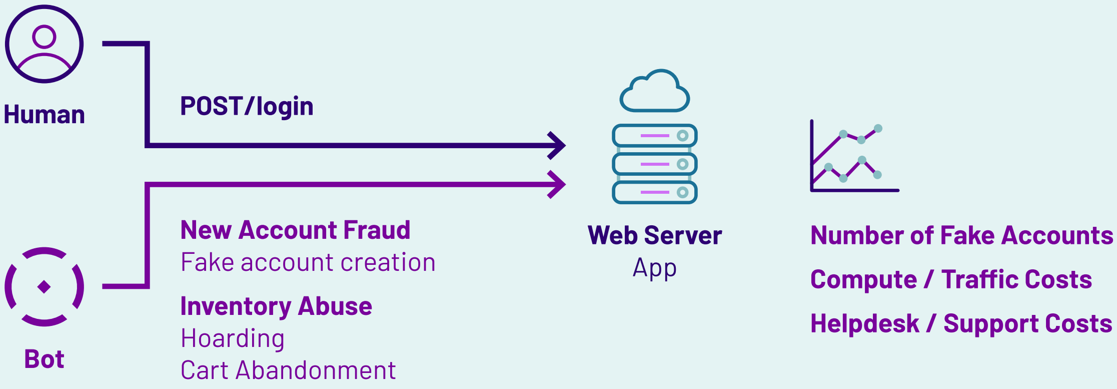


Diagram 3 — Application and Compute Costs Impact

Application and Compute Costs Case Study

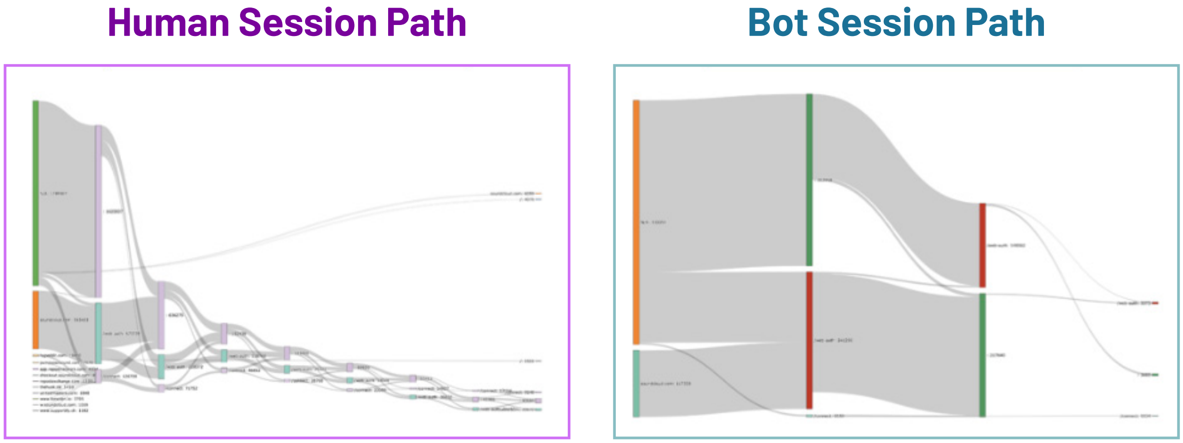
Sometimes unwanted automation isn't coming from somewhere halfway around the world. As your business becomes more successful it's natural that your local competitors will begin to take a closer look at how you're achieving this success. However, with automation, competitive price scraping can cost your business significant amounts in computing costs.

An online retail company and Human uncovered a major competitive price scraping operation costing millions of dollars in unwanted infrastructure load and fraud with significant impact to its user experience. The competitor used bots for price scraping to gain a competitive advantage. The business now has the evidence to confront their competitor and have them address the issue. By deploying Human BotGuard, the business discovered that **70%** of the traffic to their platform was coming from price scraping bots. From the customer's own calculations every one percent reduction in bot traffic led to a **$250,000** per year savings in infrastructure-as-a-service costs and the internal staff costs of dealing with the problem.

HOW HUMAN CAN REDUCE THE IMPACT OF SOPHISTICATED BOTS

It can be difficult to tell what traffic is Human and what traffic is bot and this is where conventional defenses like WAF and CAPTCHA can let you down. This is why most enterprise security leaders are looking to specialist bot management solutions rather than WAF or CDN bot management feature add-ons as the most effective way to solve their bot problem[8].

Sophisticated bots and real users both use your web applications as they were designed to be used. In figure 4, you can see the comparison here between a Human session path and a bot session path. Both get to the same end result, buying something, or leaving a comment, but the Human path is much more meandering, less direct that the bot. The bot selects and buys, then exits. The Human checks for alternatives, reads reviews, looks at delivery costs. Human sees trillions of events like these and analyzes these data so we can determine the difference between bot and Human activity. These differences inform the signals that we use to determine whether what's accessing your site is Human or not. In the past, WAFs and CAPTCHAs have been used but these are not enough to outwit sophisticated bots.



Human Session Path

Bot Session Path

Diagram 4 — Humans experience your site by traversing sections of it sporadically whereas Sophisticated Bots interact in a direct and decisive manner.

WHY HUMAN?

What's different about Human and competing bot management suppliers is, perhaps surprisingly, ads. Everytime an ad is served to you online it goes through an auction process where your attention is sold to the highest bidder. This process is secured by Human.

Advertisers don't want to advertise to bots and Human's business is founded on detecting bots to prevent this. Human has been detecting bots for more than 10 years and is the dominant supplier of advertising bot detection technology. More than **85%** of global advertisements are verified through Human and Human secures **15 Trillion** interactions weekly, making every ad on the internet a sensor for Human.

Knowing what sophisticated bots look like requires seeing them and as we see them all over the internet, more than any vendor because of this reach, almost every ad collects bot signal for Human. So we've already observed **85%** of users in our advertising security solution before seeing them on your web applications.

That's why we consistently find bots and abuse other bot mitigation providers do not and when you search shop stream or socialize online, you're contributing to our Human Collective protection.

So if you suspect your digital transformation is being sabotaged, **please get in touch**. By deploying a single line of code on your site we can show you the surprising impact of sophisticated bots on your business.

Resources:

[1] The Digital Advantage: How digital leaders outperform their peers in every industry

[2] https://hbr.org/resources/pdfs/comm/microsoft/Competingin2020.pdf

[3] https://www.dynatrace.com/cio-report-automatic-and-intelligent-observability/

[4] Personalization Pulse Check | Accenture

[5] Based on a model using publicly available data (from LexisNexis Risk Solutions) and Human data.

[6] Human Survey 2021

[7] https://resources.Humansecurity.com/all-content/2021-marketing-fraud-benchmarking-survey-and-report-2

[8] https://f.hubspotusercontent30.net/hubfs/3400937/ESG%20eBook%20-%20Human%20-%20May%202021.pdf

About Us

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. We have the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today we verify the humanity of more than 15 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To **Know Who's Real**, visit **www.humansecurity.com**.