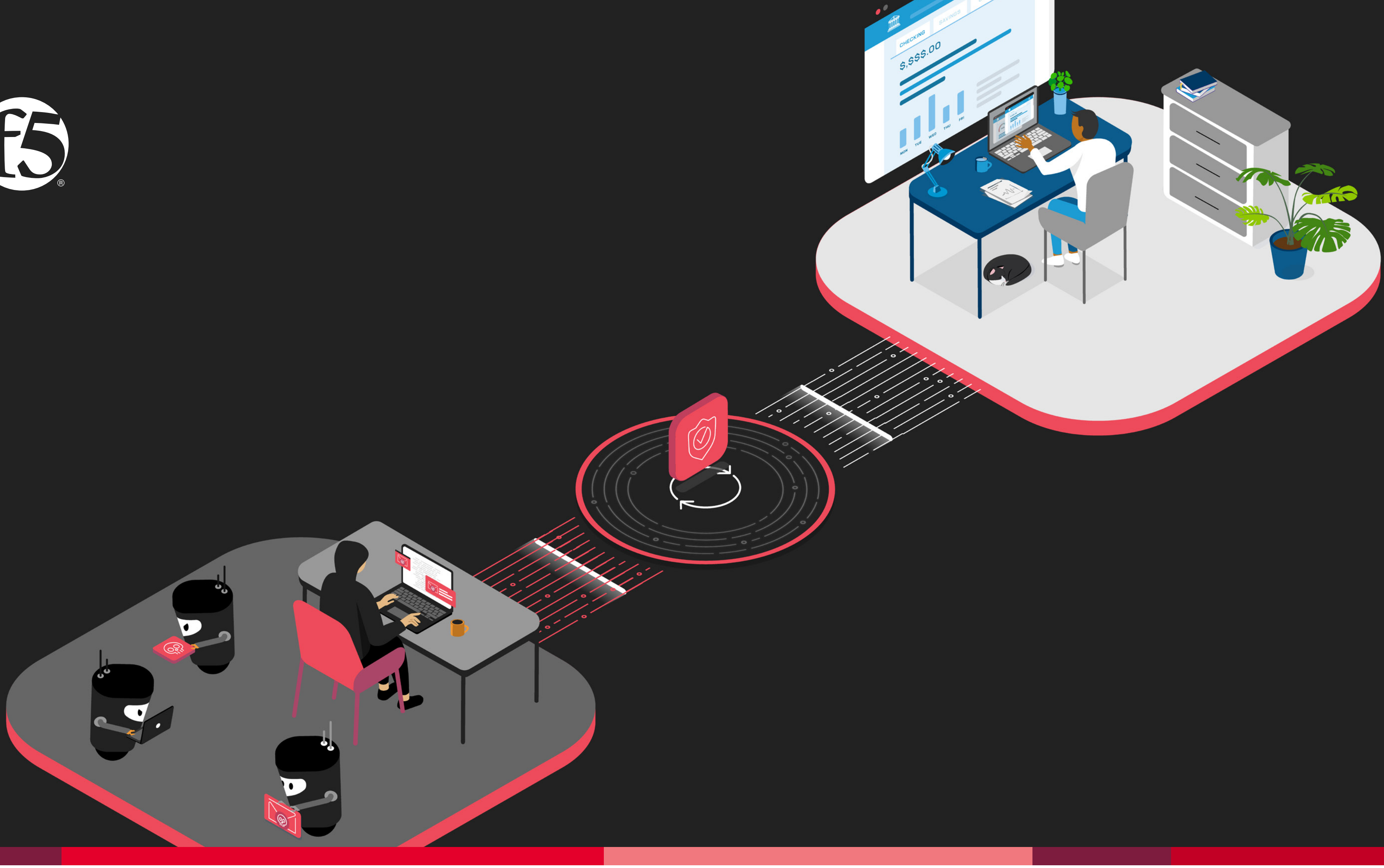


The New Era of Fraud: An Automated Threat

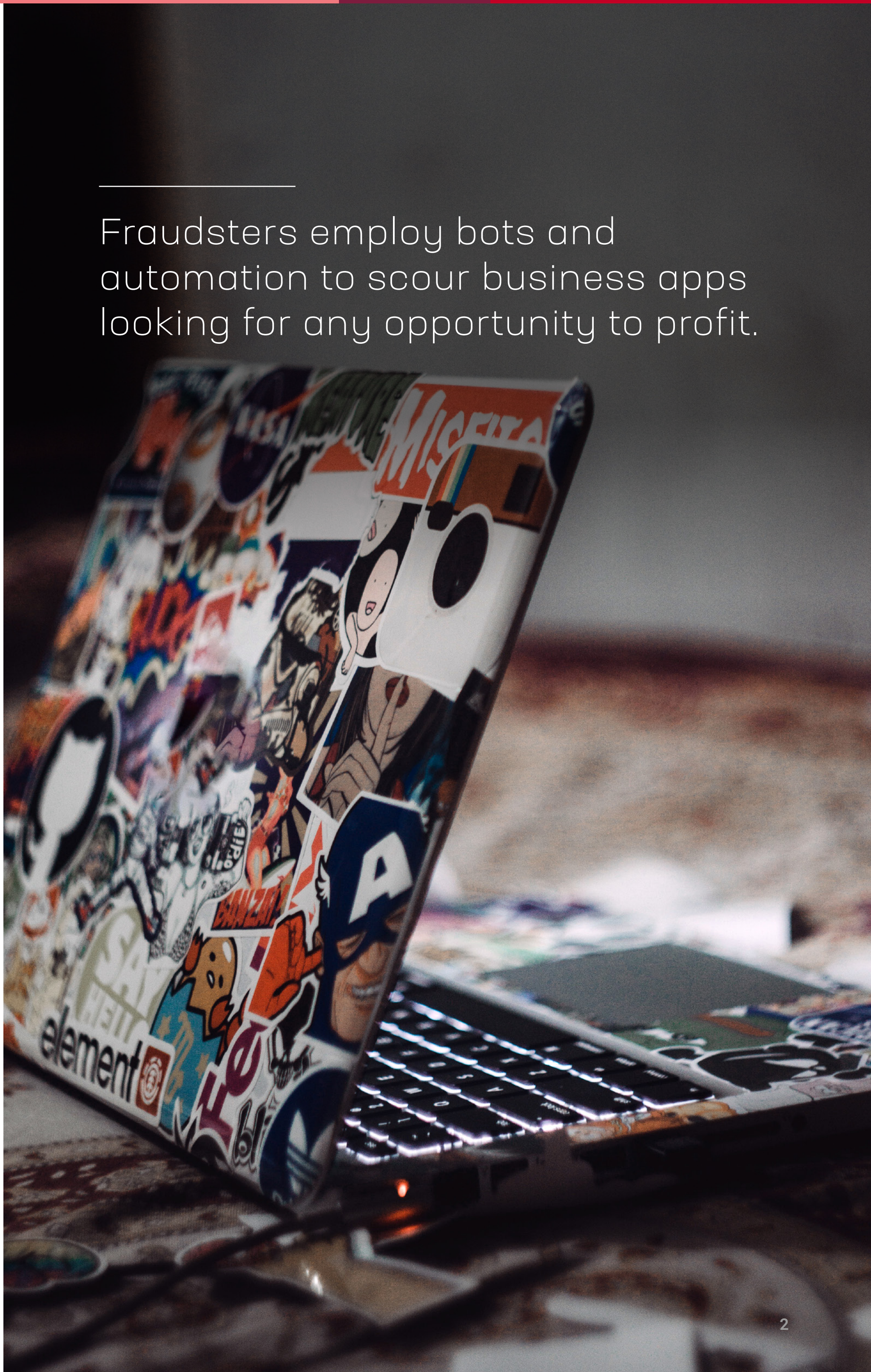
Introduction

Digital innovation has changed everything: the money is behind apps, so every online business is a potential target for fraud.

Banks and financial institutions used to be the primary targets of fraud. Why banks? “Because that’s where the money is,” to quote the notorious American bank robber Willie Sutton. While banks remain firmly in the crosshairs of fraudsters, the speed of digital transformation has made every online company a target for fraud and abuse.

Since the money is behind apps, every business with an online presence is a potential target for fraud. The same technology that helps us find airfare deals, sweet concert seats, or the best prices on the hottest Jordan shoes–that is, automation–can now be used by criminals to scale and adapt their attacks.

Fraudsters employ bots and automated attacks that scour apps looking for any opportunity to hijack business logic, take over customer accounts, and steal money. And since fraud targets business process weaknesses beyond software vulnerabilities, you may not even know when it is happening or have the best tools to protect your customer accounts, revenue, and brand.

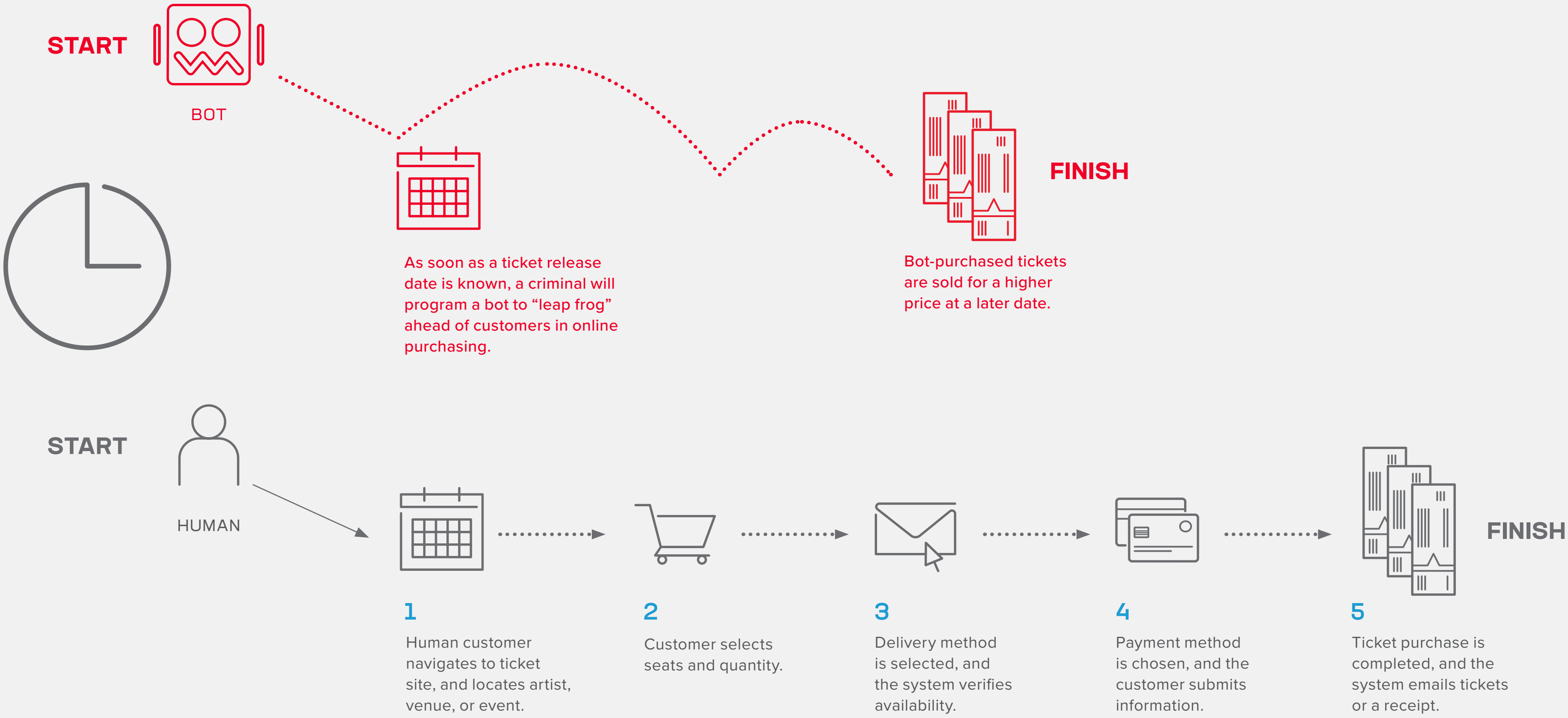


Fraudsters employ bots and automation to scour business apps looking for any opportunity to profit.

Customers vs. Bots

In this online ticket purchasing scenario, the deck is stacked against a legitimate customer trying to get to the finish line of making a purchase before a bot can grab tickets. When the tickets are sold out, a fraudster can sell them later at a higher price. The result is a frustrated customer and potentially longstanding damage to brand loyalty.

The Race for Online Tickets



START

BOT

As soon as a ticket release date is known, a criminal will program a bot to “leap frog” ahead of customers in online purchasing.

Bot-purchased tickets are sold for a higher price at a later date.

FINISH

START

HUMAN

1 Human customer navigates to ticket site, and locates artist, venue, or event.

2 Customer selects seats and quantity.

3 Delivery method is selected, and the system verifies availability.

4 Payment method is chosen, and the customer submits information.

5 Ticket purchase is completed, and the system emails tickets or a receipt.

FINISH

Know Your Enemy: The Many Faces of Fraud

Your ability to identify and thwart fraud will be perpetually tested by a wide range of creative, complex, and stealthy tactics that criminals use to evaluate and exploit digital processes. Being knowledgeable about fraud—and how bots and automation are employed to facilitate it—is a good first step on the road to effective detection and mitigation.

Business logic attacks

Not necessarily the result of flaws in code, these attacks take advantage of how an application works or how you do business. For example, attackers may try making small purchases on a web app (e.g., ordering a pizza) to validate stolen credit card numbers. Or registering in a coffee shop's rewards program 365 times to collect a free "birthday coffee" every day of the year.

Credential stuffing and account takeover

Often powered by bots, these attacks leverage readily available tools and compromised data from active data breaches or the dark web to gain access to customer accounts. Automated login requests using stolen username and password combinations can lead to account takeover (ATO) and provide a beachhead for fraud.

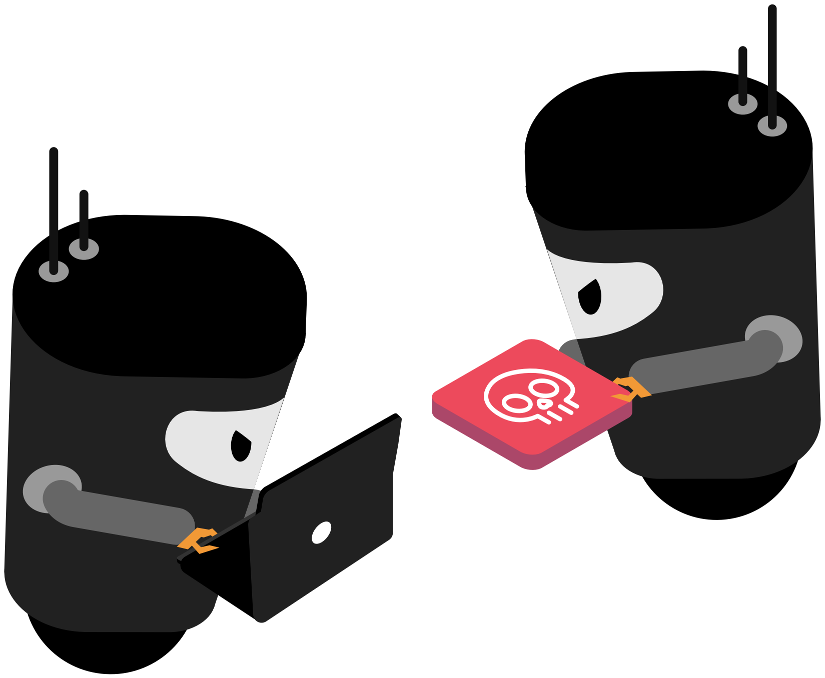
Bank accounts, online gaming accounts, and even hotel rewards points accounts are typical targets because fraudsters can gain financially from these accounts.

Scraping

Web scrapers traverse your digital properties to steal and repurpose intellectual property and content such as pricing information, published articles, and other such assets. This stolen content can be used by the fraudster to undercut pricing, poach potential visitors, or harvest customer information.

Gift card cracking

Attackers check millions of number variations on a gift card balance lookup application to identify card numbers that hold value. In some cases, the attacker will visit a retail location to identify numeric patterns in gift cards to assist with efforts to crack them using automation.



Scalpers

These bots purchase, hoard, and resell goods and services that are typically limited in supply such as concert tickets or in-demand sneakers. Scalpers buy up as much as they can so they can later resell the acquired goods for a substantial profit. Allowing or ignoring this kind of behavior can alienate your true customer base because customers will not be able to purchase directly from you, which acts as a denial of service and tarnishes your reputation as a reliable source.

Click fraud

Often powered by botnets of compromised computers, these tools mimic human behavior to facilitate a variety of purposes such as registering for accounts and clicking on ads, which falsely increases ad revenue. More advanced tools of this nature can defeat traditional security challenges and spoof controls used to delineate humans from bots and automation.

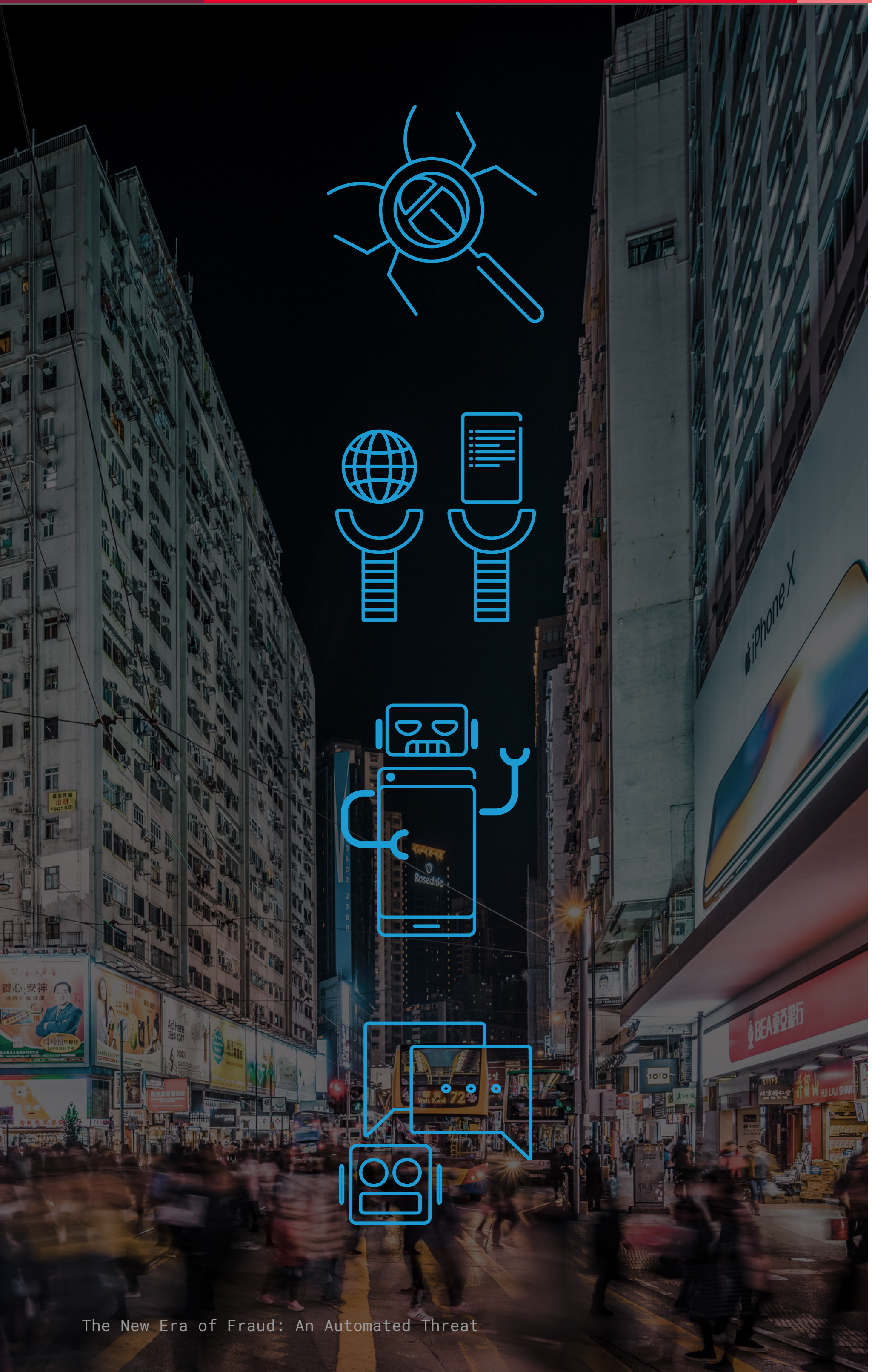
Fake accounts

Bad actors automate the creation and use of fake accounts to generate content spam, create fake product or service reviews, or commit financially motivated attacks such as reward abuse on retail sites and money laundering via online banking.

$48 Billion

Online fraud losses are projected to exceed $48 billion per year by 2023

ONLINE PAYMENT FRAUD: EMERGING THREATS, SEGMENT ANALYSIS & MARKET FORECASTS 2021-2025



Bots, Bots, Bots!

Bot-generated internet traffic has long surpassed human traffic.[1] Part of the reason for this is that regular people are increasingly find utility in the good bots, which engage customers through real-time chat and digital interactions, index and search the internet, find us the best travel deals, and fetch relevant content to display in our favorite web hangouts. As Siri, Alexa, and Google make bots available as personal assistants ready to respond to our commands, bots have become an essential tool for both businesses and consumers alike.

However, bots are also the fraudster's best friend. They are efficient and effective, and they don't ask questions, making them indispensable for the execution of malicious campaigns. Often the same technology that powers our favorite apps also enables fraud via bots.

Some bots are designed to pass themselves off as humans. Fraudsters use these social bots to promote products and services, and even manipulate public opinion via social media, discussion groups, product reviews, and public forums.[2]

Not all bots are leveraged for deception. Some autonomous programs crawl the internet looking for web application vulnerabilities to exploit. These are typically web applications that have not been properly updated or patched, and unaddressed information leakage can make the identificationof these relatively easy. Once the apps and vulnerabilities have been identified, the attackers can plan their exploits and use automation to carry them out at scale.

The most common attacks, however, are attackers that leverage bots, automated tools, and compromised data to maximize the ROI of their efforts to commit account takeover (ATO) and fraud. Credential stuffing has become the most popular attack as the success rate is attractive and the payout is potentially astronomical. In 2018 and 2019, the combined threats of phishing and credential stuffing made up roughly half of all publicly disclosed breaches in the United States.[3]

These attacks do not exploit application vulnerabilities or software weaknesses, but instead abuse human psychology (password re-use) and digital interfaces such as login forms. As such, bots are increasingly used for commercial and retail fraud.[4] Attacker frameworks are predicted to evolve even further to leverage trained artificial intelligence (AI) models to bypass security.[5]

> “**Credential stuffing** will be a threat so long as we require users to log in to accounts online.”[3]

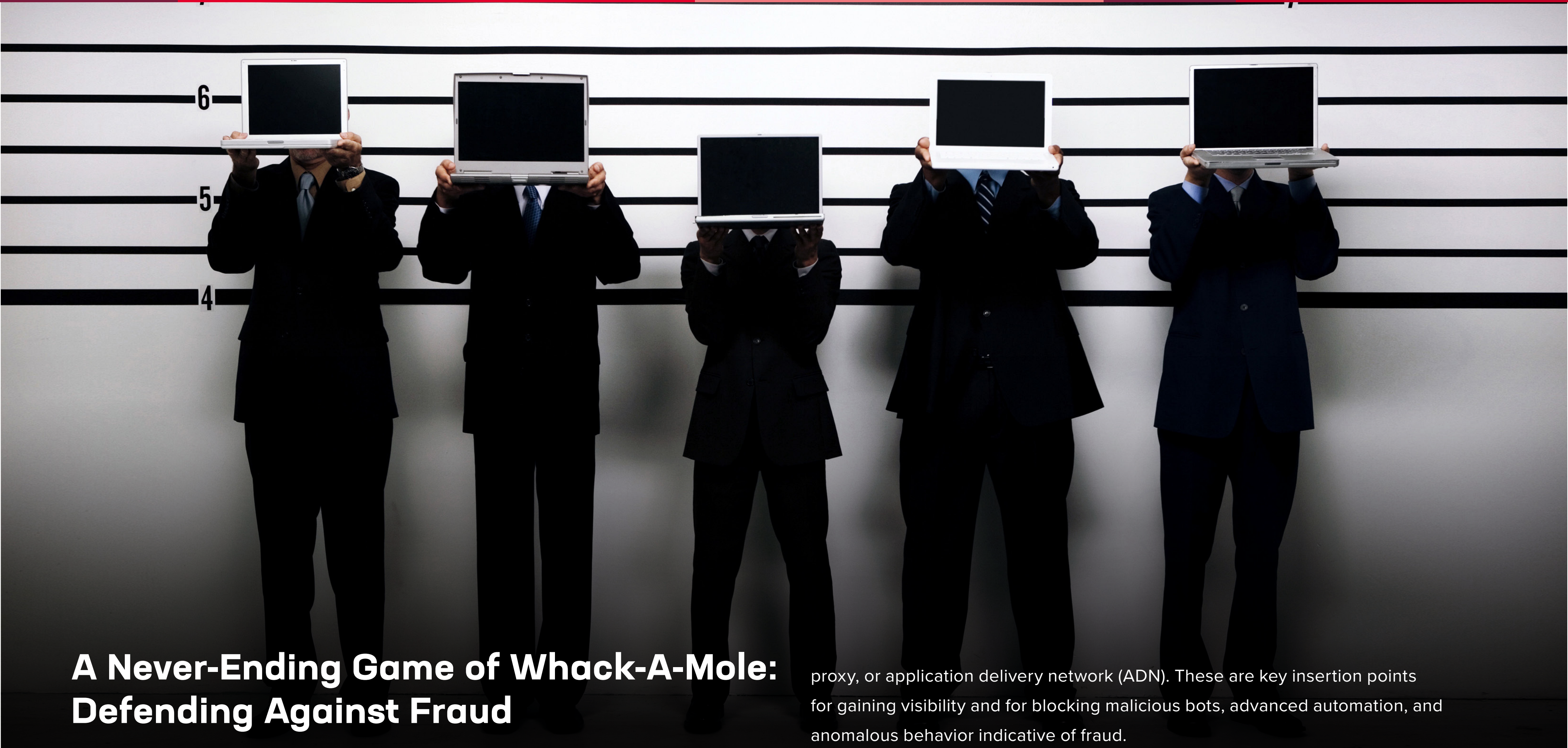
[1] https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass- human-2016-mary-meeker-code-conference

[2] https://www.theguardian.com/technology/2017/jun/19/social-media- proganda-manipulating-public-opinion-bots-accounts-facebook-twitter

[3] https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

[4] INTERNATIONAL BOTNET AND IOT SECURITY GUIDE 2020

[5] https://www.shapesecurity.com/app-security-and-fraud-summit/2020-predictions



A Never-Ending Game of Whack-A-Mole: Defending Against Fraud

Fighting fraud can feel like a never-ending game of whack-a-mole. Because fraudsters can be evasive and relentless, your defense must make success so difficult and impractical that the ROI becomes unattractive. While you will never achieve complete invulnerability, implementing defenses that make your applications a more challenging target will greatly increase the probability that criminals will focus their attention and efforts elsewhere.

The best defense is a managed service that can be integrated seamlessly into your existing architecture—whether through a web application firewall (WAF), reverse proxy, or application delivery network (ADN). These are key insertion points for gaining visibility and for blocking malicious bots, advanced automation, and anomalous behavior indicative of fraud.

Because attackers constantly retool to circumvent security countermeasures, there are several factors to consider when choosing a solution. First, your solution needs to see large volumes of traffic from numerous customers to obtain the large data sets needed to recognize attack patterns and trends. It should also collect durable network, device, and environmental telemetry signals and leverage AI and machine learning in conjunction with continuous monitoring by a Security Operations Center (SOC) to analyze and identify anamolous behavior.

Bot Mitigation

Bot mitigation protects web and mobile applications and API endpoints from sophisticated attacks that would otherwise result in large-scale fraud. A dedicated, outcome-based bot mitigation service can determine in real time if an application request is from a fraudulent source and then take an enterprise-specified action such as blocking, redirecting, or flagging the request. This provides resilient protection without assisting with the attacker's reconnaissance efforts, as the most skilled criminals will attempt to bypass security countermeasures and evade detection.

Collective defense

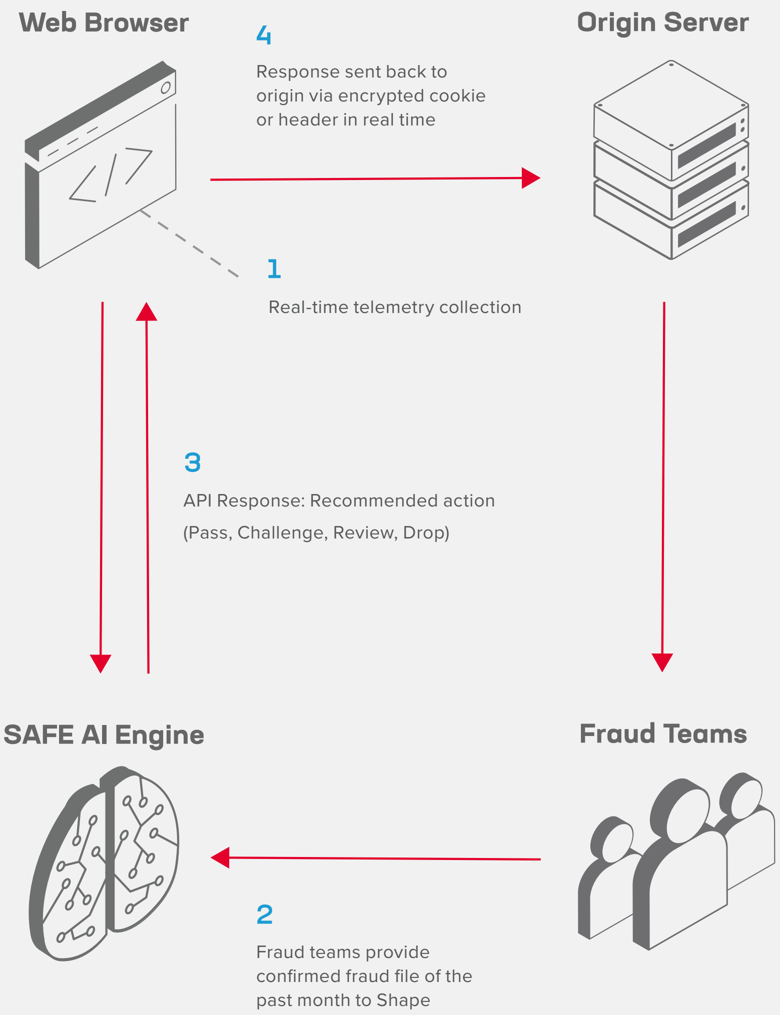
The amount of traffic that is seen by a managed service combined with behavioral-based detection is critical to accurately and effectively mitigating bots—especially the sophisticated bots that lead to fraud. By modeling threat intelligence across similar attack profiles and risk surfaces, security countermeasures can be deployed automatically for maximum effectiveness, no matter how an attacker retools in the attempt to bypass defenses. And when this collective defense network includes web, mobile, and API footprints of the world's most valuable brands, new attack techniques observed on one customer trigger immediate protection for all other customers.

Accurate and durable telemetry

Telemetry signals containing device, network, environmental, and behavioral signals can filter unwanted automation in order to distinguish between a real customer and a fraudster. Durable and accurate telemetry coupled with closed AI models trained on large data sets of traffic and historical fraud records bolster defenses by detecting anomalous behavior used in fraud. This can include copying and pasting activity, screen toggling, odd screen real estate usage, device affinity, environmental spoofing, and attempts to anonymize identity. Because motivated attackers constantly retool and may pivot to bypass anti-automation defenses, it is imperative to anticipate all potential tactics and protect against them. In other words, if your solution can effectively collect the right signals, you'll have more than a simple anti-bot solution.

Artificial intelligence and machine learning

Using comprehensive telemetry signals, AI trained by attack profile, risk surface, and historical fraud records, along with supervised and unsupervised machine learning, attacks can be detected without manual intervention, relaxing the burden on security and fraud teams.



1
Real-time telemetry collection

2
Fraud teams provide confirmed fraud file of the past month to Shape

3
API Response: Recommended action (Pass, Challenge, Review, Drop)

4
Response sent back to origin via encrypted cookie or header in real time

Automated security to combat retooling

Disrupting the attack ROI by making success impractical, or at least too costly to be feasible, is an effective deterrent. Skilled attackers adapt to security countermeasures by using advanced tools and manual interactions to spoof anti-automation algorithms. As such, security countermeasures must be continuously and automatically deployed to provide resilient protection and long-term efficacy against attackers that retool.

Frictionless auth

Effective defenses do not rely on vague risk scores and complex authentication rules. Instead, they release security and fraud teams from the operational burden of manual oversight, while freeing users from the friction imposed by legacy mitigations such as CAPTCHA and multi-factor authentication (MFA).

Real-time verification can be performed on protected resources by leveraging intelligence from the collective defense network and SOC monitoring. This intelligence enables organizations to block requests from devices affiliated with a compromised account, identities that previously exhibited suspicious behavior, and blatant attempts to use known stolen credentials.

Fraud: The Best Defense Is a Holistic Defense

Addressing fraud requires the right combination of strategy, technology, and diligence. While there is no simple solution to eliminate fraud, using bot mitigation that protects your apps and customers from fraud is your best defense. Insertion points help you apply the right protections right where you need them, regardless of architecture.

The combination of visibility, adaptive protection, access controls, threat intelligence, AI, and machine learning gives you the tools you need to shut down fraudulent activity—before it can take a toll on your business.

ABOUT F5

F5 powers applications from development through their entire lifecycle, so you can deliver differentiated, high-performing, and secure digital experiences.

Learn more about online fraud prevention at f5.com/solutions/stop-online-fraud

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com