



Bots, automation, and fraud

The convergence of cybersecurity for eCommerce

Bots automate repetitive tasks, raise brand awareness, and engage customers early in their buying journey. But in the wrong hands, bots and automation are powerful tools that can be used to compromise customer accounts, abuse shopping cart and checkout functions, and unfairly take business away from real customers. Security and fraud teams must converge to stop criminals who exploit business logic with sophisticated bots and automated attacks that prevent your eCommerce platform from reaching its highest potential.

Business enablement bots

Search engine bots

Crawl the Internet, fetching data used by search engines

Aggregator bots

Collect and consolidate multiple data sources (or bots) into a single bot

Commercial bots

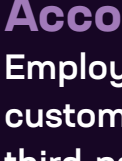
Monitor news feeds, customer reviews, ad networks, etc., to gain additional customer insights

Chatbots

Provide real-time, interactive customer service through text or voice responses

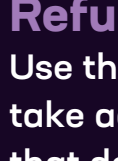
Bots and automated attacks

Login and sign-up



Credential stuffing

Leverage stolen credentials and distributed botnets to automate large-scale account compromise



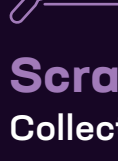
Fake accounts

Automate new account opening to abuse discount, promotion, and customer loyalty/reward programs



Account takeover

Employ techniques to take over customer accounts and commit third-party fraud via automation, human click farms, the dark web, and social engineering



Refund fraud

Use thousands of fake accounts and take advantage of return processes that do not require return to store to gain store credit/gift cards, and then sell them for cash

Shopping cart/checkout



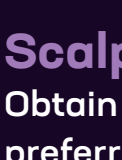
Card cracking

Identify missing credit/gift card parameters, such as expiry dates and security codes, by trying different values



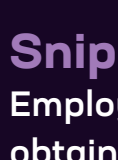
Scraping

Collect proprietary data that can lead to intellectual property theft and competitive price manipulation



Denial of inventory

Reserve significant numbers of items in shopping carts, usually in fake accounts



Cashing out

Buy goods or obtain cash with a validated stolen payment card or account data

Forms



Expediting

Speed up usually slow, tedious, or time-consuming actions for individual gain and/or deceit



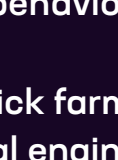
Skewing

Manipulate metrics with link clicks, page requests, or form submissions that alter odds, likes, pricing, visitor counts, poll results, or reviews



Scalping

Obtain limited-availability and/or preferred goods/services for sale later for profit



Sniping

Employ last-minute bids or offers to obtain goods or services unfairly

The industrialized attack lifecycle

It starts with malicious automation and ends with ATO and fraud.

HERE'S THE CYBERCRIMINAL PLAYBOOK:

- 01 Credentials are stolen or acquired from the dark web.
- 02 Bots and automated tools are used to abuse business logic in login, sign-up, shopping cart, checkout, and form functions.
- 03 Attackers retool to circumvent security countermeasures by spoofing network, device, and behavioral characteristics.
- 04 Criminals pivot to use human click farms, stolen tokens from the dark web, real-time phishing proxies, social engineering, and manual hacking.
- 05 Compromise leads to ATO, fake accounts, fraud, and the inability of prospective customers to transact.

Threat ecosystem at a glance



- How fraud impacts the business**
- Bottom-line operational losses
 - Top-line transaction and revenue abandonment
 - Lost customer trust
 - Damaged brand
 - Regulatory fines
 - Poor business and marketing insights

How to stop automated and manual fraud

Security and fraud teams should unite to prevent ATO and fraud by protecting the entire customer journey—while maximizing the customer experience.

F5 solutions operate as an integrated platform to mitigate bots and automated attacks, maintain resilience as attackers retool, and prevent spoofing and bypass while removing friction and authentication challenges for trusted customers—preventing compromise and bottom-line fraud losses, and maximizing revenue potential.

HERE'S HOW IT WORKS:

- 01 Gain visibility across data centers, clouds, and web/mobile/API endpoints.
- 02 Protect customers across the entire user journey from login and sign-up to shopping cart, checkout, and form submissions.
- 03 Collect device, network, and environmental telemetry, including browser signals, missing or tampered tokens, network traffic, and HTTP headers.
- 04 Encrypt and obfuscate all telemetry to thwart reconnaissance and prevent bypass by sophisticated attackers that spoof signals to evade detection.
- 05 Mitigate malicious automation, such as network-level attacks using cURL and highly distributed botnets.
- 06 Maintain resilience and efficacy as attackers adapt and retool to circumvent mitigation countermeasures using CAPTCHA solvers, headless browsers, web stack emulators, anti-fingerprinting tools, stolen tokens from the dark web, malicious scripts, or even when attackers move from targeting web to mobile and API endpoints.
- 07 Confuse attackers to stay one step ahead by employing the best mitigation technique for each situation (block, drop, alert, redirect, transform) to neutralize attacker ROI and encourage attack abandonment.
- 08 Identify truth and intent to accurately mitigate fraudulent transactions using custom signal collection, highly trained AI, and real-time and retrospective analysis via 24x7x365 security operations centers.
- 09 Remove unnecessary authentication challenges for trusted customers to minimize friction and maximize conversion, loyalty, and revenue.
- 10 Ensure better business outcomes by minimizing fraud and false positives while simultaneously maximizing the customer experience.

Better together

Security, fraud, and customer experience for eCommerce

To compete in a digital-first world, organizations need to delight customers without compromising security. The F5® Application Delivery and Security Platform (ADSP) mitigates malicious automation and stops fraudulent transactions with the highest security effectiveness while removing friction and unnecessary authentication for trusted customers.

F5 ensures better business outcomes

- Less fraud, less friction, less effort
- Improved conversion, retention, loyalty
- Increased top-line revenue
- Decreased bottom-line fraud losses
- Reduced complexity
- Increased operational efficiencies



For more information on how to protect retail and eCommerce platforms, visit f5.com/solutions/ecommerce.

