Bots, Automation, and Fraud

The Convergence of Cybersecurity

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—resulting in account takeover (ATO) and fraud.

Security and fraud teams must converge in order to stop criminals that exploit business logic and the org chart with sophisticated automated and manual attacks.

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.

Automated and Manual Fraud

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

Account Takeover
Employ a variety of techniques to take over customer accounts and commit 3rd-party fraud by leveraging automation, human click farms, the dark web, and social engineering.

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

Gift Card Cracking
Identify and steal gift cards that have a positive balance.

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

Inventory Hoarding
Reserve significant numbers of items in shopping carts, usually in fake accounts, to manipulate pricing and scalp merchandise.

Aggregator Abuse
Leverage aggregators as a backdoor into banks in order to steal information, check account balances, and launder money.

Credit Application Fraud
Impersonate identities, open fraudulent applications or claims, and then bust out to exhaust earned credit through money laundering in coordinated 1st-party fraud schemes.

Client-Side Attacks
Capitalize on web page interdependencies and exploit the browser and/or client run-time environment with malicious scripts. Also known as Magecart, supply chain, formjacking, or skimming attacks.

Card Not Present Fraud
Use stolen credit card numbers to purchase items illegitimately or to launder money through gift cards/debit cards.

Refund Fraud
Leverage 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.

SIM Swaps and Port Outs
Compromise service provider portals and leverage social engineering to gain access to 2FA messages, move phone lines, and take advantage of promotional upgrade offers.

The Industrialized Attack Lifecycle

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

1. Credentials are stolen or acquired from the dark web.
2. Bots and automated tools are used to scale credential-based attacks against logon and create account functions.
3. Attackers retool to circumvent security countermeasures by spoofing network, device, and behavioral characteristics.
4. Criminals pivot to use human click farms, stolen tokens from the Genesis Marketplace, real-time phishing proxies, social engineering, and manual hacking.
5. Compromise leads to ATO, new account opening fraud, and potentially fraudulent transactions/money laundering.

Threat Ecosystem At-a-Glance

Crime Syndicate

Since valuable credential and PII data are obtained from external data breaches, these attacks are difficult to identify and stop.

ATTACK METHODS

Automated Attacks | Manual Fraud

After being blocked, sophisticated attackers retool and escalate their attacks with different tactics to bypass security countermeasures.

ATTACK TYPES

Account Takeover | Account Opening Fraud

Criminal organizations use a variety of methods including ATO, identity theft, synthetic identity fraud, and credit application fraud.

ATTACK TARGETS

Login Apps and APIs

Customer Accounts | Create Account
Reset Password | Add to Cart
Upgrade | Return

ATTACK GOALS

Steal money; abuse promotional, loyalty, and return policies; and obtain PII for future schemes.

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:

1. **Gain visibility** across data centers, clouds, and web/mobile/API endpoints.
2. **Protect customers** across the entire user journey from login and create account to all financial transactions and sensitive exchanges.
3. **Collect device, network, and environmental telemetry** such as browser signals, mouse and keyboard events, network traffic, and HTTP headers.
4. **Encrypt and obfuscate** all telemetry to thwart reconnaissance and prevent bypass by sophisticated attackers that spoof signals to evade detection.
5. **Mitigate malicious automation** such as network-level attacks using cURL and highly distributed botnets.
6. **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.
7. **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.
8. **Identify truth and intent** to accurately mitigate fraudulent transactions using custom signal collection, highly trained AI, and real-time as well as retrospective analysis by 24x7x365 Security Operations Center.
9. **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.

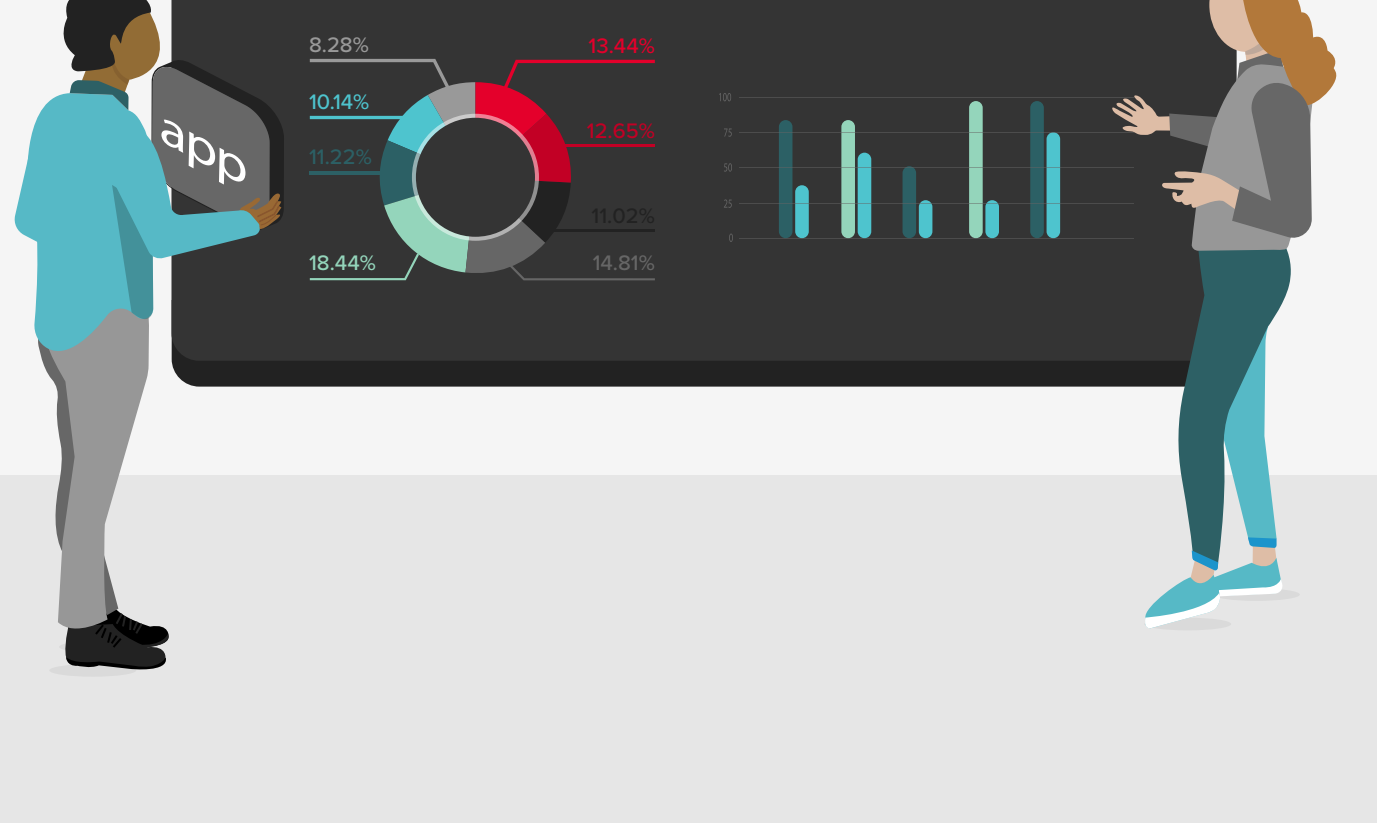
Better Together

Security, Fraud, and Customer Experience

To compete in a digital-first world, organizations need to delight customers without compromising security. F5 offers an integrated platform that 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 the F5 integrated platform for fraud prevention, visit f5.com/stopfraud.