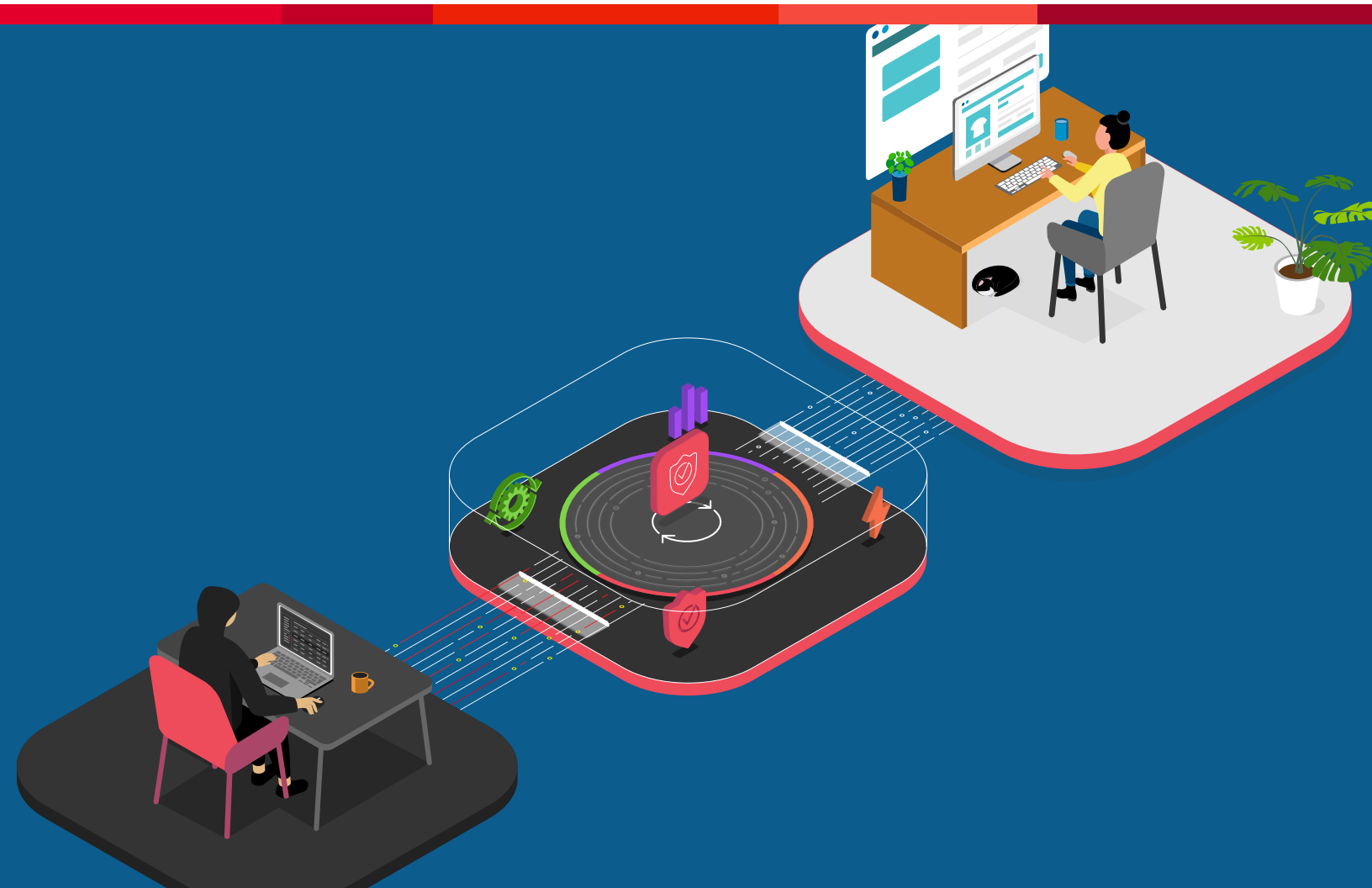
Prevent Account Takeover

As organizations offer new and innovative ways to transact with their customers, fraudsters have jumped on the opportunity to exploit digital channels such as funds transfers, shopping, loyalty reward programs, and more—leaving security and fraud departments struggling to combat increasing fraud costs, frustrated customers, and damage to brand reputations.



KEY BENEFITS

Bot Defense
Prevent sophisticated, human-emulating automation and retooling.

Account Protection
Monitor every transaction for signs of fraud or risky behavior.

Authentication Intelligence
Securely reduce friction to improve customer experience.

Security and Fraud Convergence
Provide common platform for historically siloed teams.

Flexible Deployment
Fits into your existing infrastructure.

Account takeover (ATO) continues to be the most prevalent and expensive attack targeting financial institutions, e-commerce businesses, and many other organizations. Once an account is compromised, a fraudster may drain bank accounts of their funds, purchase goods or services, access payment information for use on other sites, or engage in another nefarious activity. According to Javelin Strategy and Research in their 2021 Identity Fraud Study, ATO fraud resulted in over $6B in total losses in 2020.[1]

Fraud Starts with Automation but Doesn't End There

ATO often starts with bot-driven attacks like credential stuffing—where previously stolen user credentials and personally identifiable information (PII) are leveraged to automate logins into user accounts. Many of these attacks are commoditized and can be blocked with traditional security solutions like rule-based web application firewalls. Unfortunately, sophisticated fraudsters retool and up-level their automated emulation of human behavior to bypass these defenses, and it's these attacks that lead to a large percentage of fraud loss. If still challenged by defenses, and motivated enough, attackers pivot to manually log into accounts or even leverage human click/labor "farms" for scale—effectively bypassing anti-automation solutions completely to conduct fraudulent activity that can lead to significant fraud losses.

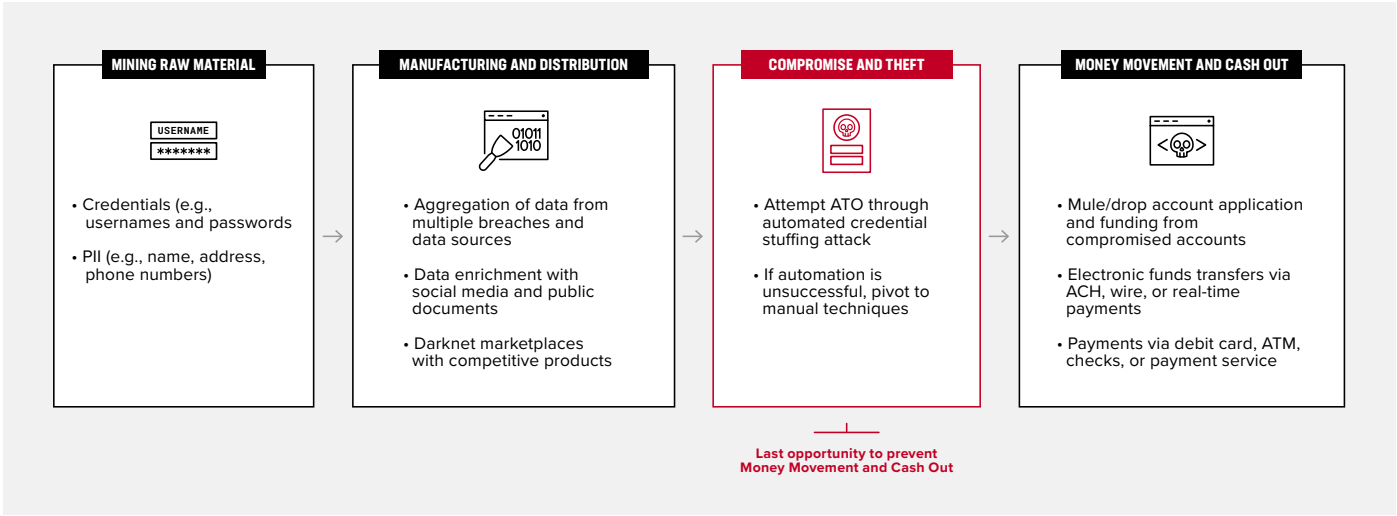


Figure 1: ATO fraud value chain. Illustration of the process of account takeover from a fraudster's perspective.

KEY FEATURES

Collective Defense Network

- Curate and analyze network, device, and environmental telemetry signals to detect anomalous behavior.
- Identify criminals' very first attempts to weaponize publicly available and actively exploited credentials.
- Perform real-time access verification on protected resources and block requests using previously stolen credentials.

Adaptive Security

- Perform real-time obfuscation to neutralize reconnaissance and profiling.
- Quickly adapt to fraudster retooling activities.
- Evaluate the intent of automated or human traffic based on previous fraud records and hundreds of telemetry signals to maximize efficacy of closed-loop AI models.

Improved Operational Efficiencies

- Reduce fraud while maintaining false positive baselines.
- Remove complex risk scoring and manual fraud rules.
- Deliver single high-fidelity outcome for each transaction.
- Improve the customer experience by minimizing (or eliminating) user friction such as CAPTCHA and MFA.

Security and Fraud Must Work Together

Both security and fraud teams have their own monitoring and detection tools, which target specific aspects of the fraud value chain and can aid in the stopping of fraud. But the problem is that there is no overlap in responsibility or data sharing among these teams. Security ops teams monitor and respond to security alerts and automate/orchestrate security measures. Fraud analysts focus on incident response—e.g., investigating suspected fraudulent payments—and tuning authentication rules based on false positives and false negatives. Fraudsters have gotten smart enough to target the seams in the organizational siloes of these teams.

Fraud teams, for example, may have zero visibility into the security incidents that can signal potential fraud before it occurs—an automated credential stuffing attack that leads to ATO. As a result, fraud teams spend unnecessary time on reactive analysis and mitigation efforts that could have been avoided if security and fraud teams had simply shared intelligence.

Ideally security and fraud teams can collaborate to stop fraud across the entire user journey in a way that does not impact the customer experience. By stopping automated and retooled attacks, fraud teams can more effectively focus on human/manual fraudster activity at all points of the kill chain. This results in dramatic improvements in fraud detection and prevention rates, reduced fraud losses and operational costs, and limited (if any) friction added to the customer experience.

Prevent ATO with F5

F5 provides a comprehensive security and fraud solution that delivers the ability to converge security and fraud teams to stop ATO and fraud while enhancing operational efficiency. The platform monitors traffic in real time and applies intelligence to mitigate human and automated fraud before it impacts the business—without disrupting the customer experience.

Powered by AI and data-driven insights generated by evaluating billions of transactions a day, F5 provides a real-time engine that first identifies fraudster activity at all points of the kill chain, such as login, account creation, account grooming, and other activities that precede the final step of fraud. Once determined whether an application request is from a fraudulent source, the platform then performs an enterprise-specified action, such as blocking, redirecting, or flagging the request for subsequent analysis.

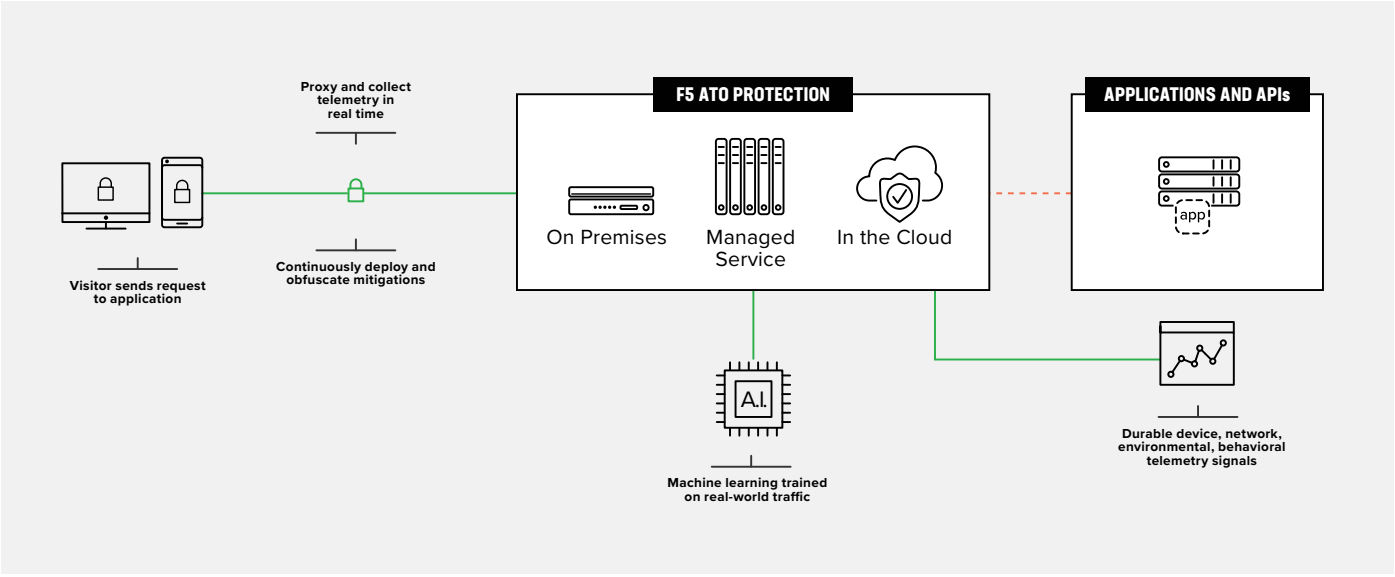


Figure 2: Prevent large-scale fraud with account takeover protection from F5.

To learn more, explore F5 Online Fraud Prevention Solutions.

[1] https://www.javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud