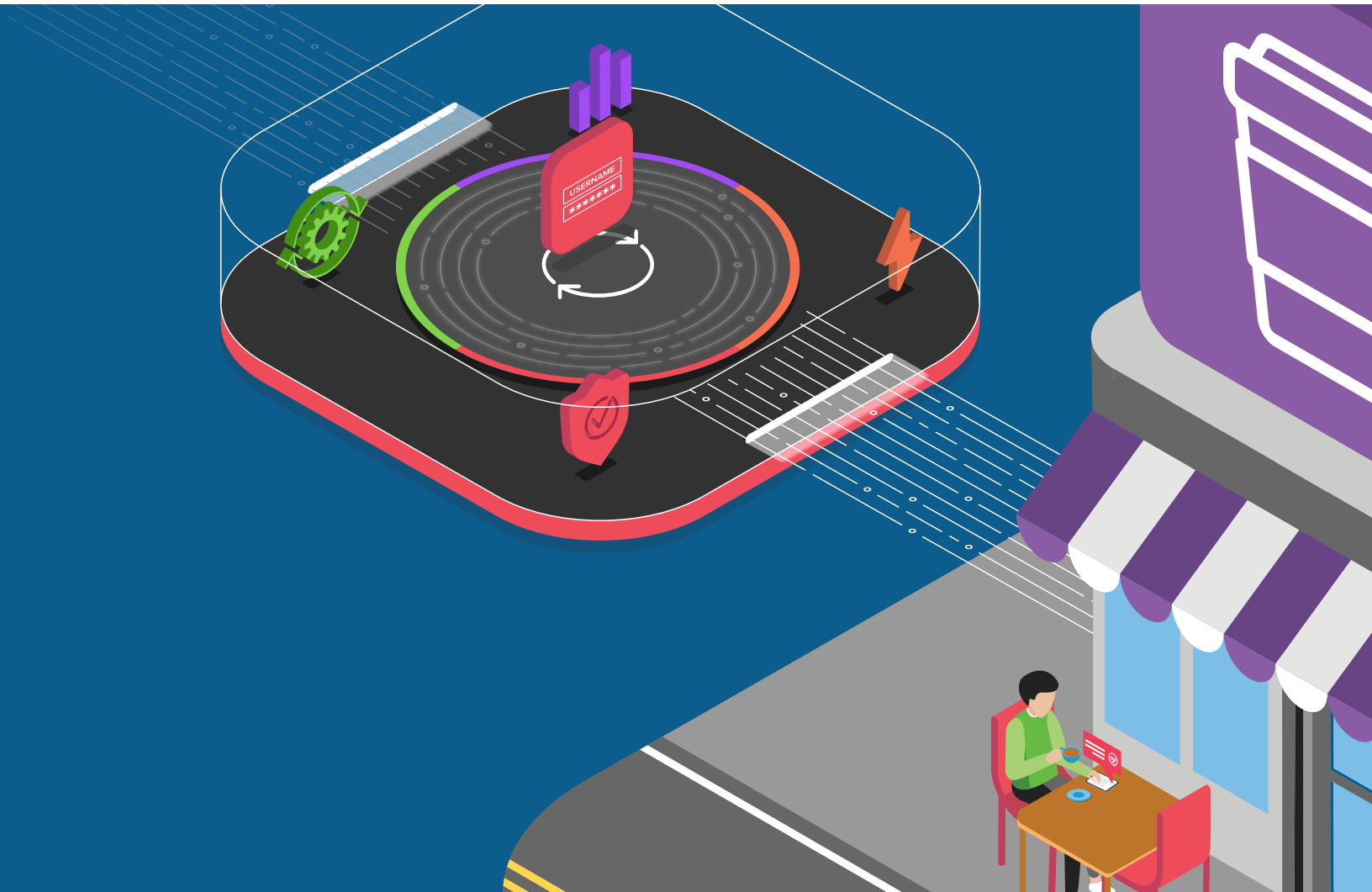
Improve Top-Line Potential and Reduce Bottom-Line Pressure

The most sophisticated attackers will retool and adapt against all countermeasures, using techniques that leverage human behavior to evade detection.



KEY BENEFITS

Better Business Outcomes
Business leaders do not need to choose between customer satisfaction and protection or top-line revenue and bottom-line fraud losses when using an integrated solution that removes unwanted automation, stops human-driven fraud, and improves customer experience.

Highest Real-World Security Efficacy
F5 can uniquely provide long-term, ongoing effectiveness because its AI algorithms are trained on attack profiles and risk surfaces of similar organizations.

Improved Insights
F5 provides insights and context to fraud-management ecosystems that help identify fraudulent transactions in real time across the entire user journey.

Not all attacks result in fraud. While automated attacks disrupt insights—leading to poor visibility and bad business intelligence—and disrupt performance by causing degradation and downtime, they may or may not lead to fraud.

When the value of the target account is high enough, fraudsters leverage human click-farms and manual hacking. In essence, attackers may start with a low-cost automated attack, and then quickly adapt to employ either techniques that emulate human behavior or manual attacks that use real humans. The net results are the same: account takeover, fraud, loss, and a damaged brand.

The difference between automated and human-driven fraud is fiction, truth, and intent.

Are you human?
Are you who you say you are?
What is your intent?

Unwanted automated traffic is fiction. The goal is to remove fiction without friction in order to evaluate truth and intent on clean human traffic to detect fraud.

Current predictions are that attacker frameworks will leverage trained artificial intelligence (AI) models to bypass security.[1]

F5 observed an average of 232.2 million malicious login attempts per day with a 0.05 success rate. That translated to 116,106 successful account takeover attacks every day, with an average of $400 stolen from each account.

Balancing Security and Customer Experience

1 IN 3 CUSTOMERS WILL LEAVE A BRAND THEY LOVE AFTER JUST ONE BAD EXPERIENCE.[4]

Already grappling with the rapid shift to online commerce and user expectations while pivoting to a new normal, business leaders face a difficult choice. They can implement layers of security controls such as CAPTCHA and multifactor authentication (MFA) to verify human behavior and identity, potentially frustrating users, or reserve part of their budget to pay for anticipated fraud losses.

Juniper Research estimates online fraud losses will exceed $48 billion per year by 2023.[2]

Organizations commonly reserve portions of their marketing and advertising budgets to cover anticipated fraud losses.[3]

One industry survey found that 92% of customers would completely abandon a company after 2 or 3 negative interactions.[5]

Fraud is a Human Problem

Fraud is a human problem more than a technical one. Therefore, the best approach to online fraud protection is to react as attackers adapt, remove unwanted automation (fiction), and evaluate truth and intent without frustrating users and compromising the user experience. Technology can enable the business to address these issues at scale by stopping attacks that can otherwise lead to fraud while maximizing customer engagement across web and mobile applications.

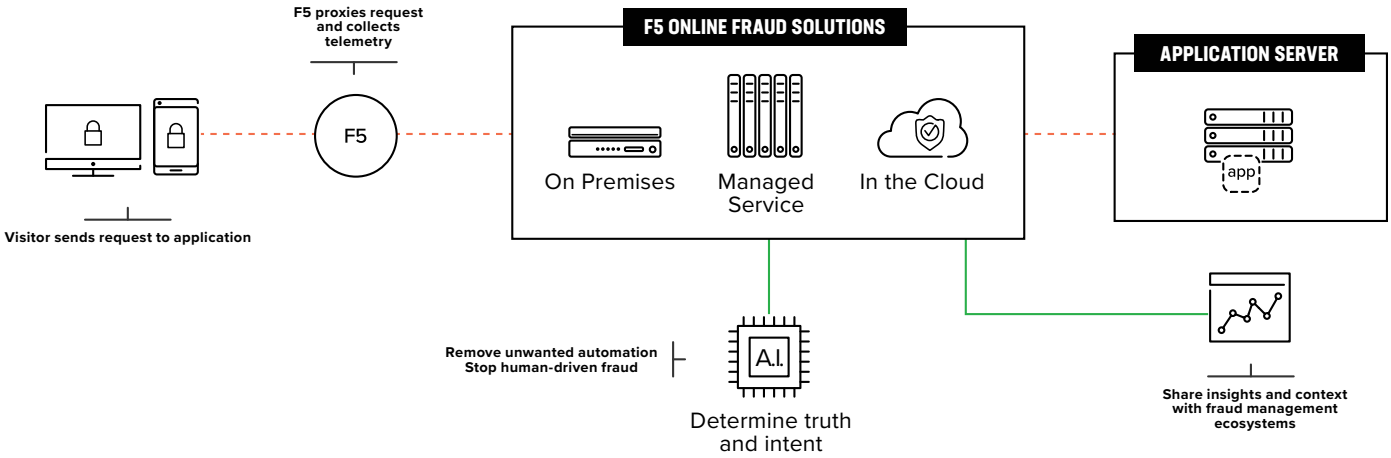


Figure 1: Organizations can stop human-driven fraud by reacting quickly as attackers adapt and removing unwanted automation– without frustrating users or compromising the user experience.

In addition to maintaining efficacy and resilience as attackers retool and adapt to countermeasures, online fraud protection must provide insights to fraud-management ecosystems. This will enable organizations to identify fraudulent transactions in real-time across the entire user journey and share actionable intelligence with business leaders to optimize real customer interactions.

BOTS ARE INCREASINGLY USED FOR COMMERCIAL AND RETAIL FRAUD.

Financial losses and damage to reputation due to fraud are very real fears to 40+% of online merchants.[6]

KEY FEATURES

- Protects digital initiatives such as online commerce, customer loyalty, credit programs, and brand awareness
- Defeats attacks that can result in compromise, revenue/customer loss, and damaged brand
- Slashes operational losses caused by fraud
- Removes high-friction mechanisms such as authentication prompts, CAPTCHA, and multi-factor authentication (MFA) to optimize customer experience
- Removes unwanted automation and shares insights and actionable intelligence with business leaders on real customer digital interactions
- Provides insights and context to fraud-management ecosystems to help identify fraudulent transactions in real-time across the entire user journey

Conclusion

F5 Online Fraud Detection is a closed-loop AI solution that removes fiction in order to evaluate truth and intent on clean human data. This approach provides a fraud resolution in real time without affecting the user experience—improving top-line potential while simultaneously reducing bottom-line pressure.

F5 provides the highest real-world security efficacy to protect the most critical assets from the most sophisticated cybercriminals.

To learn more, explore F5 Online Fraud Detection.

[1] Shape Security Predictions 2020, found at https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape Security Predictions 2020 Report - Emerging Threats to Application Security.pdf

[2] Shape Officially Joins F5 to Defend Every App from Fraud and Abuse, found at https://blog.shapesecurity.com/2020/01/

[3] Advertising Fraud Losses to Reach $42 Billion in 2019, Driven by Evolving Tactics by Fraudsters, found at https://www.juniperresearch.com/press/press-releases/advertising-fraud-losses-to-reach-42-bn-2019

[4] PwC Consumer Intelligence Series Customer Experience, found at https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/pwc-consumer-intelligence-series-customer-experience.pdf

[5] 37 Customer Experience Statistics You Need to Know for 2021, found at https://www.superoffice.com/blog/customer-experience-statistics/

[6] 451 Research, Voice of the Enterprise: Customer Experience & Commerce, 2020, found at https://451research.com/services/customer-insight/voice-of-the-enterprise