

F5 Introduces AI-Powered Solution That Blocks Fraud Missed by Existing Technologies and Improves Online Experiences for Users

Oct 06, 2020 7:00 AM

Shape AI Fraud Engine™ protects businesses and consumers while reducing workloads for fraud teams

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: [FFIV](#)) today introduced [Shape AI Fraud Engine \(SAFE\)](#), a new SaaS solution that eliminates fraudulent online transactions that get past existing fraud tools. Leveraging Shape's industry leading expertise, SAFE utilizes a battle-tested AI engine to evaluate each online transaction across a variety of telemetry, environmental, and behavioral signals to accurately understand user intent and block human fraudsters—before the fraud occurs.

Legacy fraud tools rely on weak data signals and static rules to try to catch increasingly clever fraudsters. Often, these tools can't clearly determine if the user's intent is good or bad, and resort to putting additional burden on good users to prove their legitimacy through hurdles like multi-factor authentication (MFA) challenges. The result: bad experiences for good users, as well as financial losses and frustration when fraudsters get by ineffective defenses.

In contrast, SAFE is a fully managed, AI-powered offering that stops fraudsters in real time, resulting in up to 90% less friction for known good users. As a fully managed service that can detect and block evolving threats, SAFE protects modern and traditional applications, helping organizations accelerate digital efforts and lessen the often-overwhelming workload on fraud teams.

The Impact of Modern Fraud

Businesses need a totally new approach to online fraud prevention. Most find they are still losing tens of millions of dollars annually to online fraud, despite a growing collection of fraud tools in their arsenal. Juniper Research [estimates](#) that online fraud losses—from sources including new applicant and account fraud, account takeover fraud, loyalty program fraud, and digital payments fraud—are projected to exceed \$48 billion per year by 2023.

“The need for innovation in fraud prevention becomes more urgent when you factor in the accelerated shift to online channels driven by the current global health situation,” said Sumit Agarwal, Vice President, Analytic Products at F5, and co-founder of Shape. “We're seeing fraudsters launch increasingly sophisticated attacks that take advantage of COVID-driven shifts and overall economic distress.”

SAFE overcomes today's industry challenges in the following ways:

- **Stops fraud, faster:** SAFE identifies fraudulent transactions along the entire user journey, from new account creation and login to checkout, send payment, and other actions. SAFE uses AI to accurately detect and block malicious intent, and has the intelligence to help applications scale and adapt performance, security, and other important services as needed. SAFE typically identifies twice as much fraud per month when compared to other current fraud tools. One large North American bank detected 250% more account takeover fraud in

60 days with SAFE than with their existing tools, resulting in the elimination of an additional \$10M in fraud losses per year.

- **Reduces friction for real customers:** Fear of fraud can cause organizations and application owners to impose friction on legitimate users because their existing fraud tools can't accurately distinguish real customers from fraudsters. Through a combination of proprietary telemetry and advanced AI, SAFE significantly reduces friction on legitimate activity by safely removing MFA challenges for known good users.
- **Increases effectiveness of fraud teams:** SAFE actively blocks fraud without the need for fraud teams to write or maintain rules, and is delivered as a fully managed service, with ongoing tuning done by Shape fraud experts. In addition, by stopping fraud at the application perimeter, SAFE reduces the amount of time and resources fraud teams have to expend on manual investigations. For one customer, SAFE identified that 67% of fraud cases could be safely blocked instead of investigated. For another, SAFE identified 33,000 malicious transactions in a six-week period that could be blocked instead of investigated.

Leveraging the Power of the Shape Network

Application owners face two core sources of online fraud against their applications: bots and other forms of malicious or abusive automation, and real humans with bad intent. Through machine learning, Shape distinguishes automated traffic (bots) from humans, as well as malicious traffic from benign, and provides dynamic defenses to prevent fraud and abuse, while enhancing user experience. SAFE leverages analytic insights gained from defending many of the largest and most attacked applications in the world to accurately identify and stop fraudsters in real time.

SAFE is part of a comprehensive solution set from F5 that helps modern applications protect themselves with the aid of AI. Today's [adaptive applications](#) grow, shrink, defend, and heal themselves based on the environment they're in and how they're being used, which can enable organizations to increase revenue, reduce costs, improve operations, and better protect users.

Availability

Shape AI Fraud Engine is now available. Please contact a [local F5 sales office](#) or visit [ShapeSecurity.com](#) for additional product and service availability information.

About F5

F5 (NASDAQ: [FFIV](#)) is a multi-cloud application security and delivery company that enables our customers—which include the world's largest enterprises, financial institutions, service providers, and governments—to bring extraordinary digital experiences to life. For more information, go to [f5.com](#). You can also follow [@f5networks](#) on Twitter or visit us on [LinkedIn](#) and [Facebook](#) for more information about F5, its partners, and technologies.

F5, Shape, and Shape AI Fraud Engine are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

This press release may contain forward-looking statements relating to future events or future financial performance that involve risks and uncertainties. Such statements can be identified by terminology such as "may," "will," "should," "expects," "plans," "anticipates," "believes," "estimates," "predicts," "potential," or "continue," or the negative of such terms or comparable terms. These statements are only predictions and actual results could differ materially from those anticipated in these statements based upon a number of factors including those identified in the company's filings with the SEC.

Source: F5 Networks

View source version on [businesswire.com](https://www.businesswire.com/news/home/20201006005456/en/): <https://www.businesswire.com/news/home/20201006005456/en/>

Nathan Misner
F5 Networks
(206) 272-7494
n.misner@f5.com

Holly Lancaster
WE Communications
(415) 547-7054
hluka@we-worldwide.com

Source: F5 Networks