Part of F5

Shape Defense™

AI-POWERED WEB AND MOBILE FRAUD PREVENTION FOR ORGANIZATIONS OF ALL SIZES

ATTACKS ON WEBSITES AND MOBILE APPS DRIVE FRAUD, RISK, AND BAD CUSTOMER EXPERIENCES

Every day, web and mobile applications face an onslaught of sophisticated attacks with one commonality: instead of exploiting application vulnerabilities, attackers abuse an applications's functionality as it was intended for legitimate users. These imitation attacks - delivered by bots and other forms of automation - simulate human behavior using highly sophisticated attack tools, with the goal of conducting crime or disrupting business.

Shape Defense protects online businesses from such sophisticated attacks that would otherwise result in large scale fraud. Companies get the visibility, detection and mitigation outcomes they need to slash fraud, reduce cloud hosting, bandwidth and compute costs, improve user experiences, and optimize their business based on real human traffic.

WORLD-CLASS PROTECTION

Designed to meet the needs of a broad range of organizations, Shape Defense delivers world-class application protection that leverages the power of the Shape network.

AI-powered: Through the use of advanced AI and ML, Shape Defense accurately determines in real-time if an application request is from a fraudulent source and when it is, mitigates, while allowing legitimate human users without introducing additional friction.

Collective defense: Shape Defense customers benefit from everything Shape learns through the large protection network we operate. Every 24 hours, Shape blocks more than one billion fraudulent log-in attempts and other transactions, while ensuring that more than 150 million legitimate human transactions are kept safe.

Omnichannel protection: Shape Defense can be deployed to protect web and mobile applications, as well as HTTP APIs. The company's mobile SDK is deployed on more than 200 million iOS and Android devices worldwide.

Easy to deploy and flexible to implement: Shape Defense can be implemented in a variety of modes, including deployments as quick as 30 minutes, to suit the needs of the organization and to best mitigate any attack traffic the business experiences. And Shape Defense is managed through simplified administration that does not tax your security team to operate.

PROTECTION AGAINST BOTS AND OTHER AUTOMATION ATTACKS

Shape Defense protects against the most sophisticated credential stuffing, account take over attacks, carding, and the rest of the OWASP Automated Threats to Web Applications list. Shape Defense delivers continuous protection even when attackers retool, ensuring durable protection is sustained.

Account Takeover

Stop fraudsters from rapidly testing stolen credentials on your login applications, which means they can't take over accounts in the first place.

Inventory Hoarding

Ensure your campaigns and most in-demand items and are sold directly to your customers, not to scalpers.

Gift Card Attacks

Ensure gift card value, loyalty points and other stored value remains in your customers' hands.

Carding

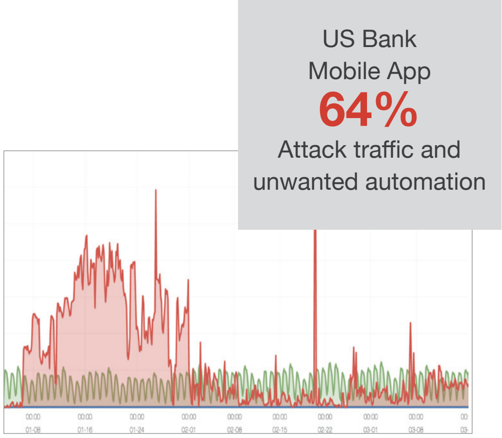
Prevent criminals from using your checkout pages to validate stolen credit cards.

Scraping

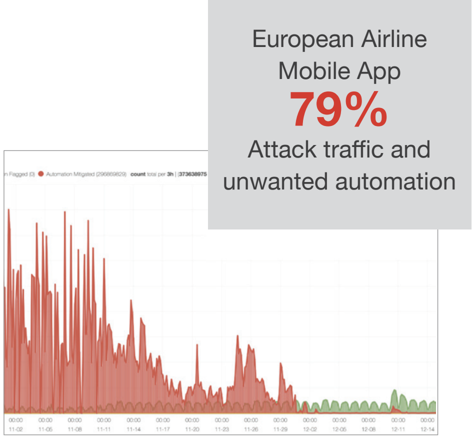
Control how scrapers and aggregators harvest data from your website, allowing you to protect sensitive data and manage infrastructure costs.

Marketing Fraud

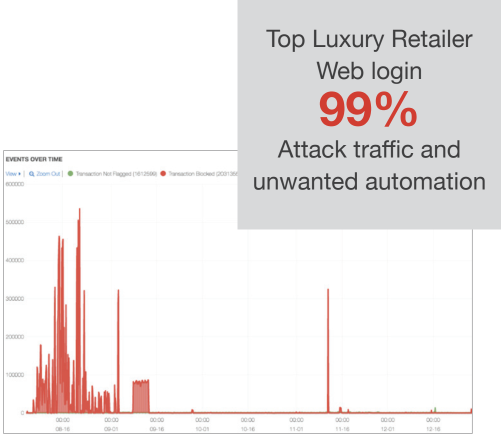
Ensure your business analytics and marketing spend are driven by real human users and not automated bots.



US Bank
Mobile App
64%
Attack traffic and
unwanted automation



European Airline
Mobile App
79%
Attack traffic and
unwanted automation



Top Luxury Retailer
Web login
99%
Attack traffic and
unwanted automation

Every customer Shape has ever protected had started out with more than 50% fake traffic before Shape began to mitigate.

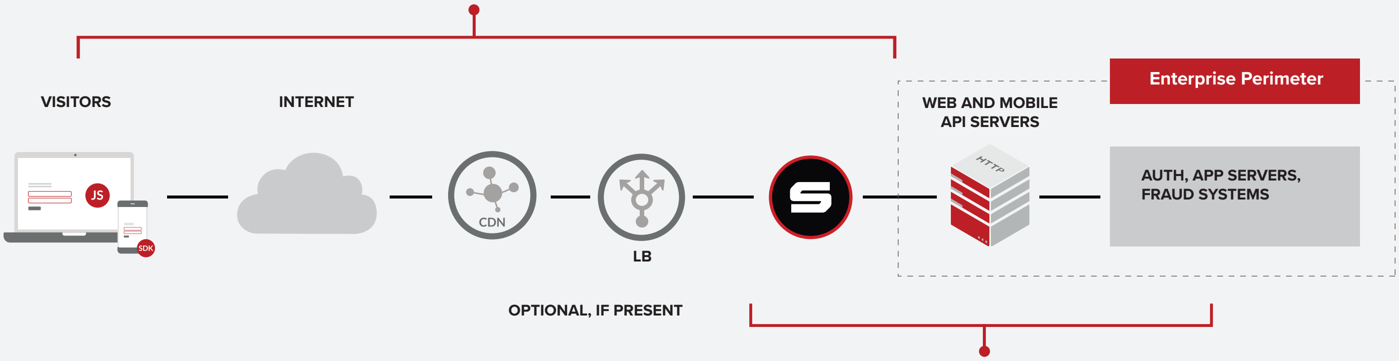
HOW SHAPE DEFENSE WORKS

Shape Defense uses a patented two-stage process to deliver highly accurate real-time detection and mitigation, as well as to provide sustained protection through attacker retooling.

Stage 1 evaluates each transactions across a set of proprietary risk factors that include network, activity, user, device and account factors. These risk factors are evaluated in light of everything Shape has learned across it's global customer base. Shape's innovative Stage 1 sees all traffic - including mitigated automation traffic - and also includes insights learned from detecting fraudulent activity across other Shape clients (aggregated defense from aggregated insights).

Shape's unique Stage 2 defense counters the attackers' evolution with an after-action machine learning and human analysis. Specifically, our Stage 2 defensive system leverages three tiers of supervised and unsupervised learning and provides unparalleled protection. Shape AI Cloud analyzes all transactions to proactively recognize retooled attacks.

Stage 1. Shape realtime component
identifies and stops bad users in real-time
can be deployed inline alongside CDN /
load balancer / application server.



Stage 2. Shape AI Cloud
analyzes all transactions to proactively
recognize retooled attacks.

PROTECT YOUR ONLINE BUSINESS TODAY

Protect your online applications from credential stuffing, account takeover, unwanted scraping, carding and other sophisticated online attacks and automation traffic that would otherwise result in large scale fraud, inflated operational costs, and additional friction for your users.

shapesecurity.com | sales@shapesecurity.com | +1 (650)-399-0400