Part of F5

SOLUTION OVERVIEW

Shape Enterprise Defense

Prevent sophisticated fraud and cyberattacks on web and mobile applications

Attackers Simulate Humans to Commit Fraud on Websites and Mobile Apps

Web and mobile applications face an onslaught of sophisticated attacks with one commonality; instead of exploiting application vulnerabilities, attackers abuse an application's functionality. Imitation attacks simulate human behavior using highly sophisticated automated tools, thereby conducting fraud or unauthorized activity at scale. The most prevalent threats include:

Credential Stuffing
Attackers test lists of stolen credentials on the login application. Because end users often reuse passwords across different online accounts, any list of stolen credentials typically has a 0.5%–2% login success rate on a large website or mobile app, leading to account takeover and online fraud.

Unauthorized Aggregation
Attackers scrape valuable information from an enterprise website or mobile application and sell the data to competitors or use it for unauthorized purposes. This process presents an infrastructure burden and numerous security challenges.

Fake Account Creation
Attackers create user accounts in high volumes in order to perform various types of fraud. Shape has seen fake accounts used to exploit online reward promotions, conduct money laundering, and further disguise credential stuffing.

These types of attacks defeat traditional security controls, including Next-Generation Firewalls and Web Application Firewalls (WAFs), and common defense techniques, such as IP based blacklisting, rate limiting, and CAPTCHA.

ANY LIST OF STOLEN CREDENTIALS TYPICALLY HAS A 0.5-2.0% LOGIN SUCCESS RATE ON A LARGE WEBSITE OR MOBILE APP

Shape Enterprise Defense Prevents Fraud by Deflecting Automated Attacks

Shape Enterprise Defense protects web and mobile applications and API endpoints from sophisticated attacks that would otherwise result in large scale fraud. Shape Enterprise Defense determines in real-time if an application request is from a fraudulent source and then takes an enterprise-specified action, such as blocking, redirecting, or flagging the request.

Shape Enterprise Defense goes beyond traditional bot mitigation. By defending the world's largest companies for multiple years, Shape has developed expertise in not just identifying whether the request was made by a bot or human, but whether the request was made with malicious or benign intent. This provides enterprises full context into the user's transaction flow, enabling real-time fraud prevention.

How It Works

Shape Enterprise Defense can be deployed inline as a reverse proxy (1) on-premises, hosted within Shape's data centers, or in a Shape managed public cloud or consumed via the Shape API (2).

Client Signals

Shape collects advanced telemetry to enhance the ability of the defense engine to detect attacks. These signals are collected via JavaScript on web applications and an SDK on native mobile applications.

Shape Defense Engine

The Shape Defense Engine is the decision component of Shape Enterprise Defense that detects and mitigates automated transactions aimed at the enterprise's protected applications. It relies on hundreds of signals to deflect fraudulent requests by detecting automation at the network, browser, and user levels. The reverse proxy can be deployed on-premises, hosted within Shape's data centers, or in a Shape managed public cloud.

Shape AI Cloud

Shape AI Cloud analyzes all transactions to proactively recognize retooled attacks and autonomously deploy new countermeasures to mitigate attacks.

API-Based

Once the client signals have been submitted, the Shape API responds regarding whether the transaction was generated by an automated or human source and passes that information along to the origin server. The enterprise uses this API response to decide whether to allow or deny the traffic.

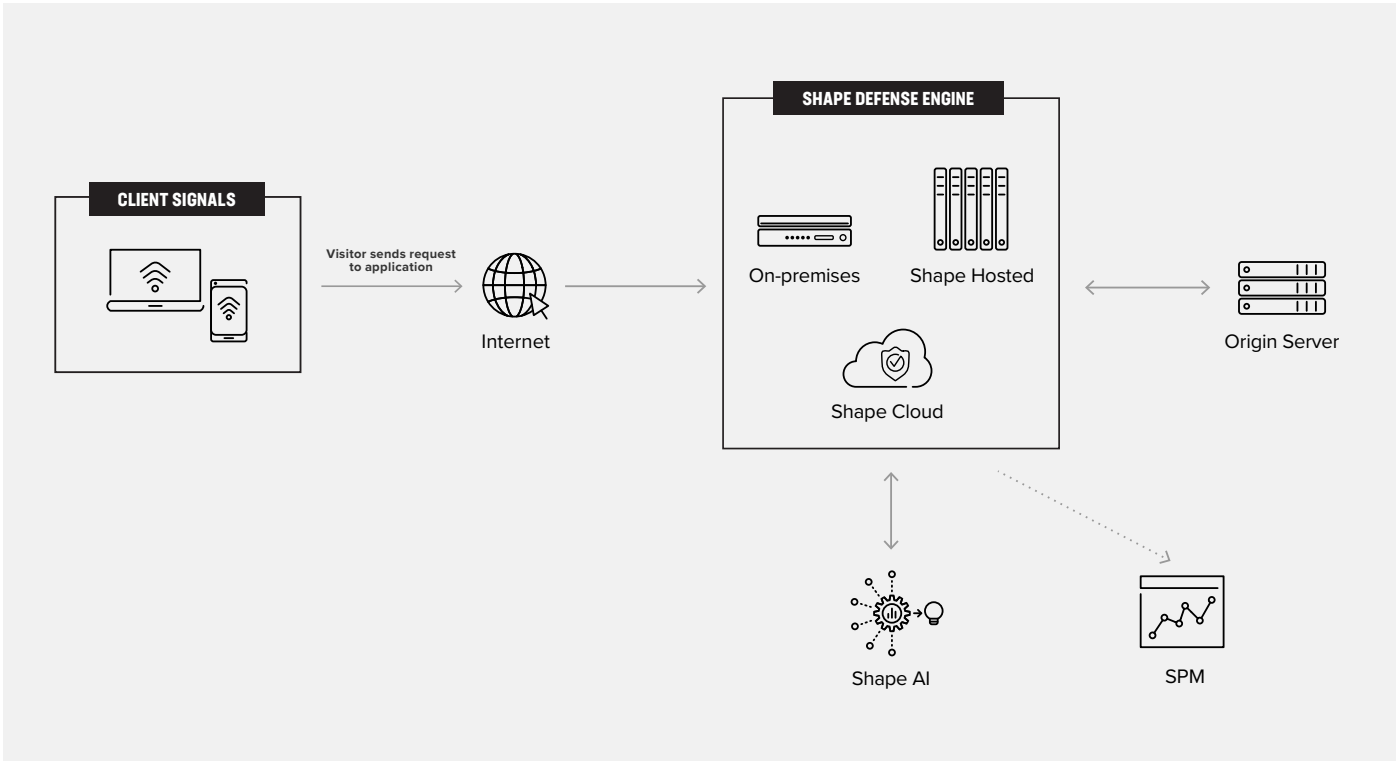

Figure 1: Reverse Proxy

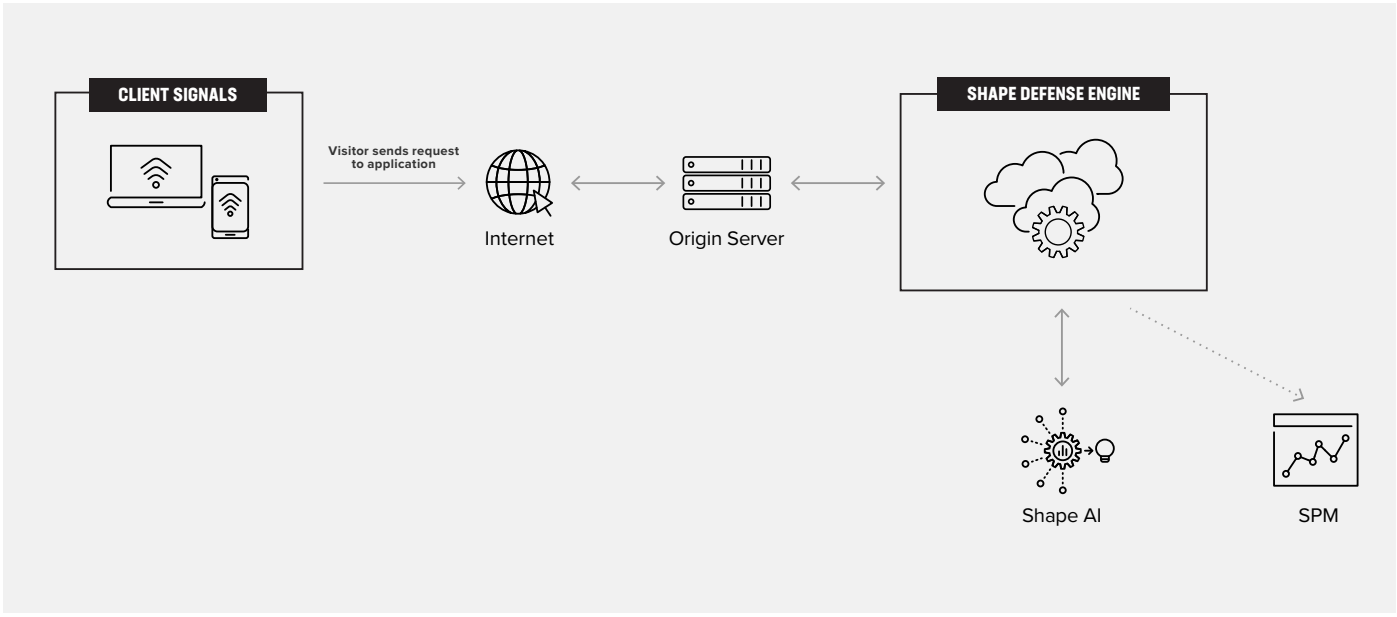

Figure 2: API-Based

Key Benefits of Shape Enterprise Defense

Detect Advanced Attackers that Retool

As soon as new countermeasures are deployed, 5%-10% of attackers will typically attempt to retool. Shape Enterprise Defense is designed to adapt and maintain full efficacy even as attackers evolve. Shape uses supervised and unsupervised deep learning methods to detect attackers' techniques and then autonomously deploy appropriate countermeasures. Because the Shape AI is trained on years of attack data from Fortune 500 companies, Shape is able to uniquely provide long-term, persistent efficacy.

Omnichannel Protection: Web, Mobile, and APIs

Once an enterprise introduces a strong defense for one application, attackers quickly begin targeting a different application, often shifting to other channels beyond web. Shape has solutions for websites, native mobile applications, and API endpoints, guaranteeing full enterprise protection.

Zero Effort to Operate

Shape Enterprise Defense is provided as a fully managed service so that attacks are deflected with virtually no effort from enterprise employees. The professional services team configures installations, monitors deployments, and maintains the technology on behalf of customers. Once deployed, the Security Operations Center monitors traffic 24/7 and provides incident response. Additionally, threat experts deliver regular briefings on attacks and industry intelligence collected across Shape's customer network, acting as an extension of an enterprise's security and fraud teams.

Collective Customer Defense

As soon as a new attack technique is observed on one customer, all other Shape customers are immediately protected from it. Shape customers include the largest companies in the world, including three of the Top 5 US Banks, five of the Top 10 Global Airlines, and three of the Top 5 Global Hotels. Because the most sophisticated attackers tend to target the largest B2C companies first, all customers benefit greatly from the aggregate attack dataset.

Flexible Deployment Options

Shape Enterprise Defense is architecture agnostic, designed to provide a unified security posture across all channels. The service can be deployed inline as a reverse proxy on-premises, hosted within Shape's data centers, or in a Shape managed public cloud or consumed via a Shape API.

Reduce User Friction

Using Shape allows customers to remove the burden of security from the end user. First, Shape's unique technology surgically identifies attackers without impacting legitimate users. Second, by preventing automated traffic from reaching the origin server, Shape also reduces server latency, improving performance. Lastly, because of Shape's efficacy, many companies

are able to reduce and/or remove high-friction mechanisms, including CAPTCHA and multifactor authentication, thereby improving the overall user experience.

To learn more, contact your Shape Security or F5 representative, or visit shapesecurity.com or f5.com.