INDUSFACE™

case study

Addressing the DDoS Challenges of an Online Shopping Application

Indusface AppTrana provides DDoS Protection for the Online Shopping Application – ShopClues

THE BUSINESS:

ShopClues is an Indian-based E-commerce platform that brings the sellers and buyers onto a managed platform to sell and buy online items such as electronics, home and kitchen accessories, fashion, footwear, and refurbished items.

Around 70% of their business is generated from the Tier-II and Tier-III cities of India. The business is spread across 30,000 cities in India. Approximately, there are 100 million monthly visitors online on their web application.

Being an E-commerce platform, their web application was always targeted by malicious hackers especially with the volumetric DDoS attacks, and hence, securing their digital asset was a priority. Here, ShopClues was looking for a robust managed Web Application Firewall (WAF) service that is managed by security experts to secure and expand their digital business.

CHALLENGES BEFORE INDUSFACE:

- The web application was constantly getting exposed to sophisticated volumetric DDOS attacks. This made the application slow to access for the end-users, and its fleet of web servers ran out of memory and CPU utilization leading to application downtime. This proportionately affected the digital business of the company.
- ShopClues initially tried to apply Geo-Fencing policies on their perimeter firewall and at the web server level, but attacks' trend changed and had started attacking from the allowed list of countries.
- The Application architecture includes a web portal for the user-login for browsing the items, reviewing the catalogue, and adding the items to the cart, etc. Followed by that, an API is used to securely push and fetch the dynamic data across the database and user interface. All the transactional journeys were routed through an API and hence, a huge volume of requests was observed on the API endpoints.
- The volumetric traffic was observed on both the web portal and API. On the web portal, brute force attempts were observed on the user login page and huge volumetric DDoS requests were hitting the API endpoints.

STRATEGY & RECOMMENDED SOLUTIONS BY INDUSFACE:

As the first layer of defence against such volumetric DDOS attacks, we have built a robust and highly scalable WAF (Web Application Firewall) infrastructure that scales seamlessly under high load. The edge points in these nodes protect against all the types of Layer-3, 4 attacks and ensure they do not cause any availability issues.

As the WAF's frontend is CDN, an additional layer of protection against Layer-3, 4 DDoS attacks is provided by the CDN infrastructure and WAF focuses on the Layer-7 DDoS protection.

As a resolution strategy, we applied multi-layered security. We implemented WAF protection for both the digital assets – web portal and API. Here are the steps in detail:

- We onboarded the Application and API with zero-downtime and activated the WAF protection from day 0 (i.e., WAF in block mode). We enabled the protection for OWASP Top 10 categories along with default WAF policies for DDoS and Bot protection.
- We also enabled IP reputation checks to block the badly reputed IP addresses.
- Also, Tor IP restrictions were implemented to block the users that were trying to mask their IP addresses.
- Further, we started implementing multiple custom rate-limiting WAF policies at multiple locations by reviewing the traffic pattern on the WAF and started identifying critical links.
- Approximately, more than 280K + attacks per month are getting blocked due to these custom rate-limiting policies for the API. Similarly, on the web portal, more than 720K+ attacks per month are getting blocked based on these custom rate-limiting policies.
- As a next step, we implemented custom WAF policies for protection against brute force attacks for the web portal.
- Also, Geo-Fencing was implemented for the WAF, wherein, only the selected list of countries of business interest was allowed access. The rest of the world was blocked.
- As a part of the managed service offering, for the application, our 24×7 MSS (Managed Security Service) team strictly monitored and fine-tuned the custom WAF policies to further strengthen the security posture.

RESULTS:

In addition to the default WAF policies, Indusface Apptrana (managed WAF) enabled the application-specific custom WAF policies to accurately detect and prevent volumetric DDoS attacks. The entire management, analysis, and strategic implementation of the custom WAF policies were done by our Managed security service team.

The multi-layered security approach helped us to prevent volumetric DDoS attacks. ShopClues's digital assets started functioning at optimum level and no downtime instances were observed further. They were now able to concentrate on their business while Apptrana managed WAF continued to detect and block the malicious attempts.

SPOTLIGHT

Customer

SHOPCLUES.COM

SOLUTIONS DEPLOYED

- Indusface AppTrana

ABOUT THE COMPANY

ShopClues is India's first and the largest managed marketplace, clocking more than 100 million monthly online shopping visitors on its website. Founded in July 2011 in Silicon Valley with 5cr listed products and over 500000 + merchants.

HEADQUARTERS

Gurgaon, India

SIZE

1350+ Employees; Valued at USD 1.1 Billion (in 2015)

INDUSTRY

E-Commerce

HIGHIGHTS

2.9 M +

API attack requests blocked in 30 days

6 M+

Web attack requests blocked in 30 days

720 K +

The total no. of attacks blocked by our custom rate-limiting policies