INDUSFACE™

CASESTUDY

Enhancing Marico's Security Posture with Unmetered DDoS Protection, Risk-Based Monitoring and Autonomous Patching

SOLUTION HIGHLIGHTS:

- Marico was facing a **loss of over 1 crore INR in case of 80% cyber incidents**
- The company's **brand value was at stake** due to repeated defacement attacks
- Indusface worked with Marico as a security partner and successfully **protected over 150+ applications on AppTrana WAAP** with risk-based scoring & autonomous patching
- **Over 3 million cyber-attacks blocked per quarter**
- **Zero cases of targeted attacks registered in the past 3 years**

We do not have a special SOC for Application Security. As our AppTrana product license includes managed services, the Indusface team is the AppSec SOC for us.

– Head IT Infrastructure & Cyber Security, Mayuresh Purandare

ABOUT THE CUSTOMER & BUSINESS CHALLENGES:

- Marico Ltd. is an Indian multinational FMCG (Fast-Moving Consumer Goods) company operating in the global beauty and wellness space. Marico is present in over 25 countries across Asia and Africa. In the year 2023, the company recorded a turnover of INR 9,764 crores (USD 1.17 billion)
- Marico is best known for its flagship brands, such as Parachute, Saffola, and Hair & Care, to name a few
- During and post-pandemic, Marico faced the below-mentioned challenges at their organisation's level:

KEY CHALLENGE – 1: POOR MECHANISMS TO HANDLE TARGETED DDOS AND BOT ATTACKS

- The company consistently faced **DDoS** and **bot attacks (thousands of attacks/day),** which were targeted on their public-facing sites instead of their OT systems
- **Despite not having any payment interface** or **user information** on their website, the hackers consistently probed their site
- This was a case where the threat actors were attempting to **deface the website by taking it down.** Due to this, customer experience and the overall brand reputation started getting impacted significantly
- In fact, 80% of these attacks were marked as "critical/red" by Marico, which meant that the impact due to **each incident led to a loss of over 1 crore** to the company
- It was difficult for the organisation to identify these attacks and block them due to the shortcomings in the security framework and due to **limited checks** in place, like simple IP addresses
- The retail sector being an unregulated one, Marico decided to up its game in protecting its brand value & strengthening its security posture like any other regulated company, e.g. BFSI or healthcare

KEY CHALLENGE – 2 : DIGITIZING FASTER BUT SECURELY FOR THE UPCOMING AVENUES

- As the world saw a stupendous digitisation growth during COVID, Marico too had to start its own initiatives to interact with its consumers, distributors, and employees in a digital way
- They had plans to launch separate applications for each of their business stakeholders, and the time-to-market was critical. Key stakeholders included:
  - Consumers
  - Distributors
  - Business Partners
  - Members
- With multiple applications planned to market on time, they were worried about security aspects such as:
  - **Identifying vulnerabilities and fixing** them on a timely basis
  - Protecting from **flaws available in third-party**, open-source, and other vendor-managed tools
  - Staying **safe from application** attacks such as DDoS, Bot, API, and Zero-Day attacks
- Hence, they wanted an app sec vendor who could help them solve these challenges with specific requirements highlighted below

7 SPECIFIC NEEDS FROM THE VENDOR:

- Act as an enabler for the business rather than being a blocker in the time-to-market
- Provide **real-time risk-based detection and protection** for all apps and APIs on a **continuous basis**
- Ensure **scalable handling of DDoS traffic** to maintain site availability and block attacks beyond a threshold to avoid excessive charges
- Provide managed services with the product/firewall due to the limited size & bandwidth of the security team at Marico to take up additional tasks for themselves
- Block all kinds of bot, DDoS, API and zero-day attacks
- The additional layer of security provided by the vendor **shouldn't hamper the site speed** and the customer experience
- Offer **timely reports** with historical data for the CXOs and the board members

SOLUTION BY INDUSFACE:

- **Protection on 150+ applications from day 1**
  - Indusface deployed the AppTrana solution in block mode right from day 1 – incoming attacks on these applications were blocked with default rules

- **Unmetered Behaviour-based DDoS & bot protection**
  - AppTrana ensured **round-the-clock availability** of the applications from DDoS and bot attacks via auto-scaling features and unmetered protection. The customer was **charged only for the legit traffic** passed to their origin server
  - AppTrana's **behaviour-based analysis and** protection performed checks beyond static rate limits and IPs and made decisions based on inbound traffic received by the host, URI, geography, historical data and more.
  - In case of **targeted attacks like defacement** or low-rate botnet attacks, Indusface security experts provided 24*7 monitoring and alerted Marico's security teams in real time. The managed services by Indusface made sure that custom rules were deployed for targeted attacks in a **short TAT**

- **Risk-based automated-patching**
  - Indusface's automated scanning, regular pen testing, and protection against vulnerabilities (zero-day, third party and open source) allowed Marico to deploy apps and integrate with other providers without security concerns
  - In order to keep the pace of security patches with the speed of feature launches, Indusface delivered **SLA-backed virtual patching** at the AppTrana WAAP level and made sure that the **time-to-market was never compromised**

- **Increased the site speed by 2X**
  - AppTrana, with its built-in CDN, not only maintained the Marico's site loading speed but further improved it by almost 2X

- **CXO reporting & data for CERT-In requirements**
  - AppTrana **blocked over 3 million attacks every quarter** for Marico across all the sites, and Indusface provided quarterly details of all attacks targeted on their websites, including the scale of the attacks, type of attacks, and protection methods across various applications that have been deployed by custom rules.
  - With AppTrana's SEIM integration, Marico were able to record and process information internally for their **new CERT-In directives** such as incident reporting within 6 hours, recording and storing incident logs of 180 days and so on.

With the help of all the solutions mentioned above, Indusface became the only cloud WAAP vendor that blended into all the requirements that Marico had and worked with them as a business enabler to meet their security goals.

Within a span of 3 years, all the "critical" security issues highlighted by Marico, were safeguarded by Indusface and the overall security posture was improved with effective security controls and processes in place.

RESULTS:

- **Successfully protected over 150+ applications** catering to 4 different customer/business segments
- **Millions of** DDoS, bot, zero-day, and API **attacks** blocked in the span of 3 years
- Hundreds of **virtual patches** deployed
- Zero cases of defacement, account takeover and other targeted attacks registered since the deployment of AppTrana on each of the applications
- Regained **the brand reputation**