CEQUENCE

Case Study

Poshmark Prevents Automated Attacks with Cequence

POSHMARK

Partnership Ensures That Only Legitimate Users Have Uninterrupted Access

Increased Account Takeover Attempts Alongside Rapid Growth

Poshmark, a prominent social commerce marketplace, enables users to buy and sell new and secondhand styles on the Poshmark website and mobile app. The ease, simplicity, and fun of the buying and selling experience has enabled millions of people around the world to bring their closet online with just a phone. As the marketplace grew, it attracted malicious activity that needed to be addressed to protect the company's brand reputation and preserve the end user experience. Poshmark's security team noticed an increase in the variety of new automated account takeover (ATO) attacks that used credential stuffing to compromise end user accounts. They saw this increase in attacks across both their web and API applications, neither of which had any API protection to detect or block these types of automated attacks.

Traditional Methods Disrupted User Experience

To identify and block suspected automated attacks, the security team had implemented a CAPTCHA challenge that disrupted the user experience and increased friction for user signup and login.

Poshmark needed a security solution that could block automated fraud attacks while improving the experience for buyers and sellers. Poshmark partnered with Cequence to deploy the Cequence Unified API Protection platform.

The Results

After implementing Cequence, Poshmark was able to block malicious bot traffic in real time before it reached their application. This also enabled Poshmark to dramatically reduce CAPTCHA challenges, streamlining the user experience and ensuring that only legitimate users were on their platform. Additionally, Cequence was deployed fully on AWS with multiple availability zones and Auto Scaling groups enabling Poshmark to scale up and down automatically as needed during important sales events or high-volume attacks.

Poshmark is now able to do the following:

- **Real-time Blocking:** Inline blocking of malicious bot traffic, ensuring that only legitimate user traffic reached their mission-critical applications.
- **Prevent Fake Accounts:** Block fake account creation used to conduct malicious activity across mobile and web sites.

Customer Profile

Poshmark is a leading online marketplace that enables users to buy and sell new and secondhand styles for women, men, kids, homes, and more. Founded in 2011 in Redwood City, California, Poshmark has over 100 million registered users in its vibrant community across the U.S., Canada, Australia, and India. Today, there are more than 200 million available listings on its platform.

Goals

- **Inline Blocking:** Real-time blocking of all malicious bot traffic with a very low false positive rate, ensuring that only real user traffic reaches the application.
- **Reduce CAPTCHA:** No longer rely on CAPTCHA as the primary way to identify bot activity.
- **Fast, Easy Deployment:** Quickly implement a new solution without disruption to buyers and sellers. Avoid integrating JavaScript SDKs into web and mobile applications which increase software and QA cycles for every product release.

- **Block ATO Attacks and Malicious Signups:** Significantly improve reliability and uptime while reducing fraud.
- **Preserve Marketplace Social Integrity:** Ensure comments originate from legitimate users on listed items and prevent fake comments from bots.
- **Minimize User Experience Friction:** Improve user experience by limiting CAPTCHA challenges to suspicious traffic, preventing malicious bot activity.

Success Metrics

- Reduced cancellations due to a decrease in malicious activity.
- Mitigated operational impacts like performance, reliability, and uptime.
- Improved the end user experience, reducing CAPTCHA challenges by 99.3%! Challenges were reduced from 2,600,000 logins to only 18,000 per week.
- Blocked over 609K attempted ATO attacks, saving an estimated $2,192,400[1] in potential account losses.
- Reduced hours spent by internal team members on manually battling malicious cyber attacks.

1 Based on a $3.60 account loss per account LexisNexis® True Cost of Fraud™ Study. https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices