CEQUENCE

Case Study

Cequence Streamlines Poshmark's Online Experience, Preventing Automated Attacks

POSHMARK

Partnership Ensures That Only Legitimate Users Have Uninterrupted Access

Increased Account Takeover Attempts Alongside Rapid Growth

Poshmark, a prominent social marketplace, enables users to buy and sell new and secondhand styles on their 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 opened the company up to an increase in malicious activity that needed to be addressed to preserve the 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 the accounts of their users. They saw this increase in attacks across both their web and API applications, neither of which had any API protection to detect and block these types of automated attacks.

Traditional Methods Disrupted User Experience

To identify and block suspected automated attacks, the security team had enabled a CAPTCHA challenge that not only disrupted the user experience, but also created friction for user sign up and login.

They were looking for a security solution that could block automated fraud attacks while improving the experience for buyers and sellers. Cequence partnered up with the online retailer to help deploy the Cequence Unified API Protection (UAP) solution.

The Results

After implementing Cequence Unified API Protection, they were able to block malicious bot traffic in real-time before it reached their application. This enabled Poshmark to streamline the user experience and ensure that only legitimate users were on their platform.

Poshmark was now able to do the following:

- **Inline Blocking:** Real-time blocking of malicious bot traffic, ensuring that only legitimate user traffic reached their mission-critical applications.
- **Fake Account Prevention:** Blocked 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 80 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.
- **Easy and Quick Deployment:** Ability to quickly implement a new solution without disruption to buyers and sellers. They wished to avoid integrating JavaScript SDKs into applications which need software cycles across web and mobile applications for every product release.

- **Stopped Downstream Impact:** By blocking ATO attacks and malicious user signups, they were able to significantly reduce downstream impacts such as reliability, uptime, and fraud.
- **Real Comments:** Ensure that all new comments on listed items were from real users and not fake comments from automated bots.
- **User Experience:** An improved user experience, only delivering CAPTCHA challenges for suspicious traffic to prevent bot activity.

What They Achieved

- Reduced cancellations due to a decrease in malicious activity.
- Mitigated operational impacts like performance, reliability, and uptime.
- Reduced CAPTCHA challenges by 99.3%, no longer requiring a challenge for all logins.
- The online retailer reduced challenges from 2.6M logins to only 18K suspicious logins 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