perimeterx | Case Study

Top Regional Bank

Stops Account Takeover Attacks and Improves Performance During Peak Traffic Periods

Company

With nearly $27B in assets, this leading regional bank has been growing rapidly with 250 locations in the Southeast and has been recognized as one of the top performing banks in the nation.

Problem

Like many businesses, the pandemic accelerated the bank's digital transformation journey. As more of its customer interactions went online, so did the number of fraud attempts. The bank discovered that its traditional cyber defense tools such as web application firewalls (WAFs) and multi-factor authentication (MFA) could not keep up with the flood of automated bot attacks.

Leaders at the bank were concerned about account takeover (ATO) attacks, also known as credential stuffing attacks. Login pages on the bank's website were being inundated with bot-driven credential stuffing attempts, as almost 70% of the requests to those pages came from malicious bots. This resulted in customers being locked out of their accounts as automated bots cycled through username-password combinations and hit bad login attempt limits. While MFA reduced the likelihood of customer accounts getting breached, the locked accounts caused customers to flood the bank's help desk with calls and made blocking bots a top priority for the organization.

The bank realized it needed a solution that was purpose-built for bot mitigation with the ability to distinguish between bots and legitimate human users, and to integrate at both the application and infrastructure levels.

> "Almost 70% of the requests to our login and authentication pages were coming from malicious bots. While we had implemented an MFA solution, it saw an exponential increase in the number of bots attacking the login and authentication pages that fed into the MFA process. This led to a heightened risk of breach and increased security costs related to MFA."
>
> **CISO**, Top Regional Bank

Solution

The bank determined that the escalating bot attack volume had to be addressed and the attacks mitigated. The bank's security team introduced PerimeterX Bot Defender to their technology stack to address their need for a versatile, machine learning (ML) based bot management solution to protect its website, mobile apps and APIs from automated bot attacks.

The PerimeterX team worked with the organization's security team to quickly create a strategy to address its issues and rapidly deploy a solution to stop the escalating bot attacks. The strategy included the following:

Increase the accuracy of bot detection: Utilizing the bank's existing WAF to detect automated bot attacks required continuous tuning and configuration changes that were laborious and time consuming. In spite of this additional effort, a large number of malicious requests were reaching the login pages through the WAF. Bot Defender was able to accurately differentiate between malicious bots and legitimate users and effectively block unwanted traffic.

Require no infrastructure changes: Bot Defender integrated seamlessly with the bank's WAF, its multi-factor authentication (MFA) solution and its edge infrastructure, which saved the team time, money and hassle usually required when replacement and reconfiguration is required. Coupled with its behavior-based analytics and highly accurate detection capabilities, Bot Defender had immediate impact.

Ensure a flexible architecture: PerimeterX helped the team at the bank architect a solution that placed Bot Defender between the WAF and the MFA. Architecting the solution to limit the number of requests that reached the MFA pages enhanced performance and throughput.

> "With Bot Defender, we have been able to precisely detect and block even sophisticated bots that emulated human behavior, bringing the false positive rate below 0.01%. The solution significantly reduced the amount of time that our team was spending on automated fraud."
>
> **CISO**, Top Regional Bank

Results

The bank experienced immediate benefits from deploying Bot Defender — most importantly, restoring customer confidence by providing a frictionless but secure banking experience.

Enhanced bot detection accuracy eliminated uncertainty for the security team: Over the first 72 hours, Bot Defender protected 15.6 million page views. Bot Defender also accurately identified that 11.7 million, or 74.7%, of total page views were from malicious bots and blocked them.

Maintained the ROI on existing investments: Bot Defender seamlessly integrates with existing applications and infrastructure components such as WAFs, CDNs, web servers and serverless edge compute services. The bank was able to avoid huge cost outlays while deploying a highly accurate bot mitigation solution since it did not have to rip and replace existing web or security infrastructure.

Remediated customer dissatisfaction by eliminating credential stuffing attacks: Positioning Bot Defender in line with MFA helped the bank streamline traffic flow to its login pages. This eliminated credential stuffing attacks and resulted in mostly legitimate requests being handled by the MFA handlers. Overall performance increased, the number of account lockouts dropped and customer satisfaction soared.

About PerimeterX

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender, and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

perimeterx
www.perimeterx.com