# A Top Five United States Financial Services Firm Secures the Customer Experience

## THE CHALLENGES

This bank was suffering increased network downtime due to ineffective attack mitigation methods and required on-premise DDoS protection to supplement its existing cloud-based DDoS mitigation service.

## THE SOLUTION

The bank implemented DefensePro, Radware's on-premise DDoS appliance with Radware's SSL attack mitigation solution.

## WHY RADWARE

Radware DefensePro's unique machine-learning capabilities for behavioral-based detection and automated attack signature creation set it apart from the competition. In addition, its SSL mitigation capabilities provide advanced detection and mitigation against encrypted attacks.

## BENEFITS

The bank has stopped nonvolumetric and network attacks and improved overall network availability without impacting or blocking legitimate users. In addition, the bank is able to mitigate SSL-based DDoS attacks without adding unnecessary latency or compromising user privacy.

As one of the largest banks in the United States, this financial services institution understands the importance of securing the customer experience for its digital consumer base. Accomplishing this means overcoming a series of unique challenges.

- The bank is bound by industry and federal regulations regarding the protection of customer banking information.
- It cannot afford downtime to its online services or an increase to network latency which negatively affect the customer experience.

The bank relied almost completely on a cloud-based DDoS mitigation service to safeguard its network and data centers. However, over the past year, it found that this cloud DDoS vendor couldn't mitigate nonvolumetric attack vectors, including encrypted SSL-based attacks, low and slow attacks and Burst assaults. With a certain percentage of these attacks penetrating the network, it became obvious that the bank required an on-premise DDoS mitigation solution to complement its cloud-based scrubbing service.

## THE CHALLENGES

With only cloud-based scrubbing for protection, the bank discovered nonvolumetric attacks were successfully penetrating its cloud mitigation provider and causing network downtime. As a result, it began relying on "black-holing" (dropping) network traffic, which impacted legitimate traffic that posed no threat. The bank's customers were being blocked and financial transactions were being stopped, resulting in lost business.

Worse, the incumbent cloud mitigation vendor could not handle encrypted DDoS floods. Because an encrypted request can take up to 15 times more server resources than a nonencrypted request, this meant that attackers could launch DDoS attacks with only a small amount of traffic. The bank had no method of protection against these attacks.

## THE SOLUTION

The financial services firm realized they needed to supplement their cloud-based DDoS protection with an on-premise DDoS mitigation solution. After evaluating the market, the bank implemented DefensePro, Radware's on-premise DDoS appliance that detects and mitigates a wide array of cyberattacks, such as zero-day DDoS attacks, IoT botnets, DNS and Burst attacks. It includes Radware's patent-protected SSL attack mitigation solution. This solution supports all common encryption standards and protects from all forms of encrypted attacks without adding latency and impacting legitimate traffic.

The bank was able to leverage DefensePro's unique machine-learning capabilities for behavioral-based detection and automated attack signature creation. These capabilities detect traffic anomalies against network baselines and automate on-the-fly signature creation to mitigate threats in real time without relying on rate-based mitigation strategies or "blackholing."

## BENEFITS

The bank has stopped nonvolumetric and network attacks and improved overall network availability without impacting or blocking legitimate users. In addition, the bank is able to mitigate SSL-based DDoS attacks without adding unnecessary latency and without compromising user privacy.