

# A Top European Bank Partners with Radware for DDoS Mitigation and SSL Attack Protection

## THE CHALLENGES

This financial services company was facing an increased rate of cyberattacks and required a new on-premise DDoS mitigation platform at its primary data centers in addition to protection from encrypted network attacks to protect web applications.

## THE SOLUTION

After evaluating the market, Radware's on-premise DDoS appliance, DefensePro, was implemented along with Radware's SSL attack mitigation solution.

## WHY RADWARE

Radware DefensePro's unique machine-learning capabilities for behavior-based detection and automated attack signatures set it apart from the competition, in addition to the robust SSL attack mitigation capabilities and the company's professional services.

## BENEFITS

The bank has eliminated security blind spots that exist due to encrypted attack traffic and leverages Radware's machine-learning and automatic signature creation to detect and mitigate attacks directed at individual or specific segments of the bank's network.



As one of the top 20 largest investment and financial services companies in the world, this firm has operations in over 70 countries worldwide. With an IT infrastructure as diverse as its global product and services offerings, the bank was seeking DDoS protection for its primary data centers in Germany, the United Kingdom, the United States and Singapore.

## THE CHALLENGES

In recent years, financial services has become one of the industries most targeted by cyberattacks. In addition to facing an array of attack vectors and threats, including hacktivist-backed campaigns and ransom-motivated assaults, it is also overcoming a hodgepodge of various network and application security challenges, including migration to the cloud, application exploits and encrypted traffic management.

This financial services company was no exception and, in recent years, was facing an increased rate of cyberattacks. The bank required a new on-premise DDoS mitigation platform at its primary data centers that could protect them from DDoS attacks without negatively impacting legitimate traffic.

In addition, with the percentage of encrypted network traffic increasing, the bank required a solution that could protect their web applications from encrypted floods. With these technical capabilities defined, the bank went to market and began evaluating a series of DDoS mitigation solutions.

Shortly after the start of the evaluation process, the financial services company suffered a series of high-volume DDoS attacks targeting its European data center that impacted application performance and availability. Seeking a rapid resolution to this emergency situation, the bank turned to Radware, which was able to rapidly implement an on-premise solution.

### THE SOLUTION

With the attack underscoring the importance of upgrading the bank's cyber defenses, the bank continued with the evaluation and, after extensive testing, rounded down the field to three vendors, from which Radware was selected the winner.

The final solution that was deployed at the bank's primary data centers was DefensePro, Radware's on-premise DDoS appliance that includes SSL attack mitigation to protect applications from encrypted attacks. The bank was able to leverage DefensePro's unique machine-learning capabilities for behavior-based detection and automated attack signature creation, which set Radware apart from the competition. These capabilities detect traffic anomalies against network baselines and automate on-the-fly signature creation to mitigate threats in real time.

To assist the bank's operations team with day-to-day solution monitoring and management, the bank elected to purchase custom training and additional assistance from Radware's professional services team.

### BENEFITS

Radware's SSL attack mitigation solution eliminated security blind spots that exist due to encrypted attack traffic leveraged in advanced attack campaigns. The solution also provides application-layer protection from encrypted floods without causing additional latency during peacetime. In addition, Radware's SSL mitigation solution includes flexible deployment options and certificate management which results in an easy-to-deploy-and-maintain solution.

The bank has been impressed with DefensePro's machine-learning and behavior-based algorithms. These capabilities allow DefensePro to accurately detect attacks without generating false positives and then automatically create signatures in real time to mitigate these attacks without impacting legitimate traffic.

Finally, Radware's ability to provide immediate assistance and mitigation for security emergencies has proved a perfect complement to the bank's in-house expertise. Radware's Emergency Response Team — a group of security experts that provides 24x7 security support services — assists the bank's network security team with real-time assistance during an attack as well as threat intelligence, signature updates and customizations for proactive consultation.

*This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.*

© 2018 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this case study are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.