NETSCOUT

| CASE STUDY |

Large European Financial Organization Implements a Proactive DDoS Defense With on Premise Devices

Ensures Availability of Information to Their Clients

OVERVIEW

The Challenge

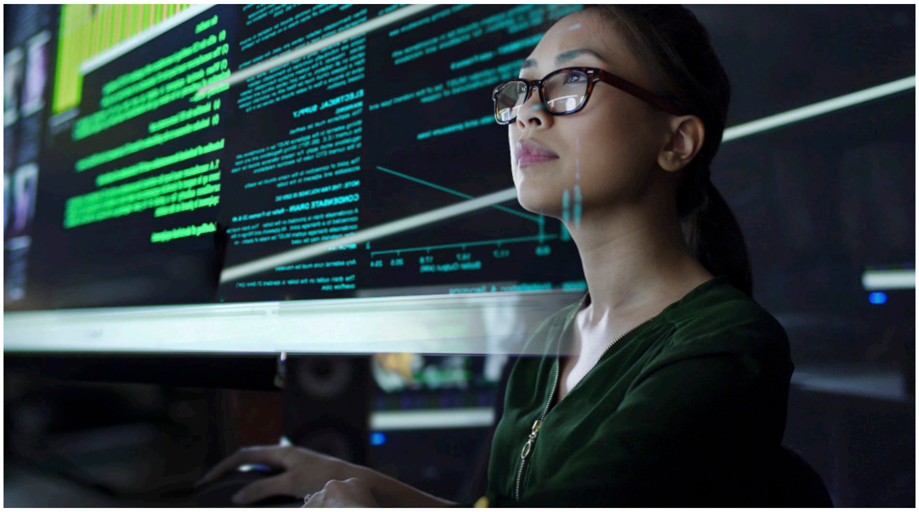
Reactive posture and prioritization of mitigation activity by employing ISP and infrastructure capacities only, causes untimely network downtime resulting in critical business risks and potential reputational loss.

The Solution

- 2 Arbor Edge Defense (AED) with AIF
- 1 Arbor Cloud ESS
- 3 Years of Support

The Results

Upon completion of solution installation, immediate extortion campaign threat and consequent attack is mitigated leading hacker to abandon any further activity.



Customer Profile

One of the largest financial centers operating in Western Europe ensures the flow of information and money between its financial market players. This organization offers currency exchange services, financial information and banking services with the aim of increasing efficiency, quality, and innovative capacity for the banking value chain. Their services are considered business critical to some of the largest organizations in Europe.

The Challenge

Due to the critical nature of the infrastructure the organization operates and manages, and the reliance on that infrastructure by their valued customers and partners, the organization, through a CIO driven initiative, decided to explore more proactive and centrally controlled measures for security monitoring and mitigation of potential DDoS attacks. Another driver of this initiative was the organizations concern over meeting newly implemented banking regulations around infrastructure security specifically focused on DDoS activity. This initiative forced them to look at what services their ISP was providing around DDoS attacks and led them to two issues with this reliance on their ISP. One was that the ISP was not set up to handle larger mitigations at specific customer sites due to the fact that the ISPs mitigation capacity could be spread pretty thin during a regional attack. And two, an ISPs priority is to protect their backbone. They were also concerned that the ISP mitigation activity would take place on devices not in their physical datacenter but in remote locations which could lead to delays before regaining control and stopping the onslaught which could in turn lead to exorbitant costs in monetary and reputational measures. They also took a hard look at what they currently had in place within their network infrastructure to battle any incoming DDoS attacks. This was also deemed underpowered and not acceptable. The result of this introspection was that they were currently too dependent on outside management of the risks that come from potential DDoS attacks. They needed to find a solution to bring that risk management in house to ensure more control and quicker reaction time.

The Solution

Initially the customer approached NETSCOUT® to discuss a cloud solution. But after listening to the customers issues with the ISP options and their internal infrastructure concerns, NETSCOUT recommended a hybrid solution to cover all of the requirements of the RFP. NETSCOUT recommended on premise AEDs as a first and last line of network defense and a license for Arbor Cloud to augment mitigation activity during larger DDoS attacks working in concert with the AEDs. They were very impressed with the ability of the AEDs to connect with Arbor Cloud through cloud signaling to coordinate all mitigation activities. NETSCOUT employed our professional services and managed services teams to get the software and devices installed and configured to meet the customer's needs.

The Results

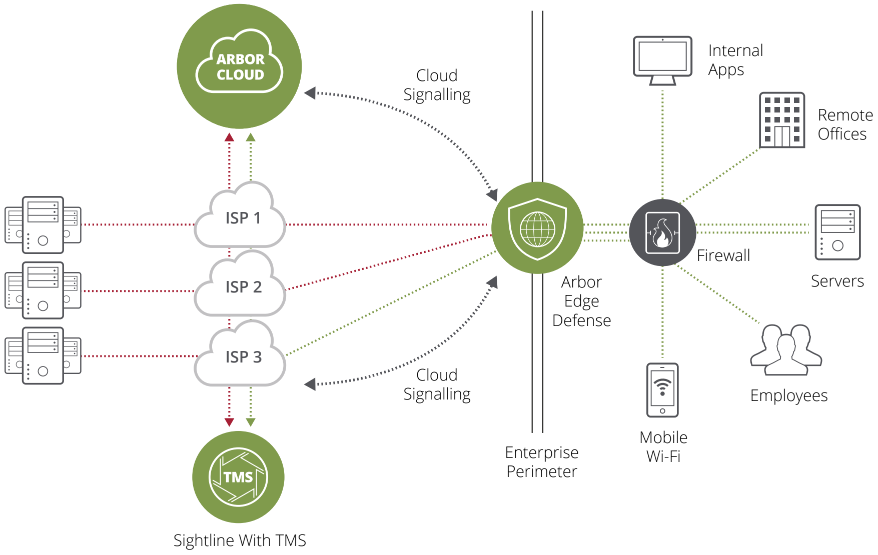
An interesting situation revealed itself and showcased the results this deal. Soon after the installation and configuration of the two AEDs and Arbor Cloud, the organization fell victim to a variety of extortion campaigns. From the NETSCOUT perspective this could not have been a better test for our products. The extortion campaigns were threatening multiple attacks of up to 2TBs each. The organization was confident in the solution due to a successful POC that took this type of attack into consideration, so they did not react to the hackers and soon the attacks did come.

The attacks were mitigated in a timely manner and the hackers AS numbers were broadcast to other devices and stakeholders including their ISP. Once the hackers realized what had happened, they abandoned any further attacks on the organization.

LEARN MORE

For more information about NETSCOUT solutions visit:

https://www.netscout.com/



Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us