# Multinational Bank Thwarts DDoS Attack to Repair Productivity Losses and Rescue Reputation

## The Situation

On a Friday evening after typical closing time, a multinational bank based in Africa had to resort to enabling geo-blocking on their network to stop a merciless DDoS attack. The bank had been enduring the attack for most of the day, placing both their ISPs under extreme strain. Neither of the two ISPs had any proper DDoS mitigation capabilities.

The attacks suffered were suspected to be part of the campaign that had been ongoing in Sub-Saharan Africa for several months. A group with access to a substantial botnet claiming to be Fancy Bear had been targeting the financial sector in various countries at the end of 2019.

https://www.zdnet.com/article/a-ddos-gang-is-extorting-businesses-posing-as-russian-government-hackers/

Due to the geo-blocking, the banking customers were now cut off from the rest of the world. The attack was volumetric in nature and was targeted at their web services infrastructure. The network would have eventually come down under the pressure and all bank activity would have stopped.

The productivity hit would be costly, and the bank's reputation was in jeopardy. They needed immediate help to stop the attack and put DDoS identification and mitigation measures in place to stop future attacks.

## The Details

Once they realized they were under attack, the bank's NetOps and SecOps staff researched DDoS Mitigation options and were directed to the Arbor Cloud™ DDoS Mitigation Service by a mutual partner. The NETSCOUT® Arbor team jumped on to a conference call with the customer and informed the customer about the Arbor Cloud Emergency Provisioning Service. Furthermore, the NETSCOUT Arbor team established that the customer had a /24 IPv4 prefix, which would make invoking traffic redirection to Arbor Cloud using Border Gateway Protocol (BGP), a valid mitigation strategy.

In parallel to the emergency provisioning of the Arbor Cloud DDoS mitigation service, the next step was for the customer to repurpose a decommissioned server in order for the NETSCOUT Arbor team to get a virtual AED installed and configured. A demo or purchased physical appliance would be days away at best. At 8am Saturday the team started again and worked through to Sunday. The team received the server and installed and configured ESXi, and the virtual AED. The AED was installed in front of the CPE (router) as the customer was running NAT on the device. 27 hours later, we had the customer back online with a working virtual AED.

Most of Sunday was spent with the Arbor Security Operations Center (SOC) team getting the signaling and GRE tunnel configured. In the following days, we ran several successful tests in terms of auto signaling to Arbor Cloud. With cloud signaling configured for the AED and Arbor Cloud, the customer was now able to leverage intelligent, automated signaling to request an upstream Arbor Cloud mitigation. Once the attack traffic had been eliminated, clean traffic was returned to the network and the network was back up and running.

The customer did suffer some reputation and financial loss from being offline for two days but with the help of Arbor Cloud, the damage was minimized.

## The Results

Once the attack was mitigated and the bank returned to business as usual, we worked with them on a properly scaled, day-to-day solution that they can rely on to continue identification and mitigation of DDoS threat traffic, without impact on the remaining network or organizational productivity.

To our knowledge, they have experienced very little down time and they rely on this solution so much that they purchased two AED appliances, one for their primary network and a second for their Data Center. That was followed up with another two AEDs for their sites in another African country, alongside NETSCOUT Professional Services doing in-country training and installation.

CONTACT AN EXPERT ▶

**Because of the Arbor Solution to the emergency DDoS attack the customer was able to limit the costs of the organization's lost productivity and maintain business continuity going forward.**

## Intelligently Automated, Best Practice Hybrid DDoS Protection, Backed by Global Visibility and Threat Intelligence

The facts are clear – DDoS attacks continue to rise in size, frequency and complexity. Modern-day DDoS attacks are a dynamic combination of:

1. Volumetric
2. TCP State Exhaustion
3. Application-layer attack vectors

Industry-best practice for DDoS defense is a multi-layer, or hybrid approach that takes into account the different types and targets of DDoS attacks. Just as important, the solution must have an intelligent form of communication between these two layers backed by up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks.

### In-Cloud Protection

Arbor Cloud™ is an ISP agnostic, in-cloud, fully managed DDoS Protection service. Employing 14 scrubbing centers located throughout the US, Europe and Asia, Arbor Cloud provides over 11 Tbps of global mitigation capacity. Enterprises can seamlessly integrate their on-premise Arbor Edge Defense (AED) protection with Arbor Cloud to obtain comprehensive DDoS attack protection. Service Providers can also use Arbor Cloud for extra mitigation capacity and expertise.

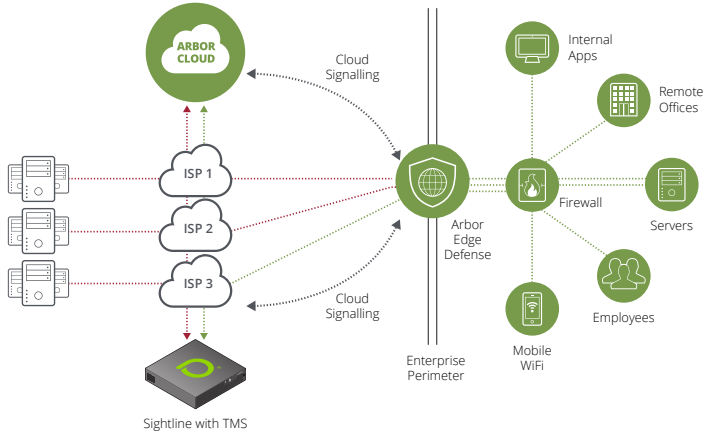
### On-Premise Protection

For larger networks and more experienced DDoS attack mitigation teams, Arbor Sightline and Arbor Threat Mitigation System (TMS) provide pervasive network visibility and DDoS attack detection. Upon attack detection, Arbor Sightline can automatically re-route attack traffic to the Arbor TMS for surgical mitigation of all types of DDoS attacks. For smaller networks, Arbor Edge Defense (AED) is an always-on, in-line, DDoS attack detection and mitigation solution which can stop in-bound DDoS attacks. For larger DDoS attacks, AED's Cloud Signaling™ will intelligently link to Arbor Cloud.

### Global Visibility and Threat Intelligence

Arbor Security Engineering & Response Team (ASERT) leverages a 20-year, worldwide deployment of Arbor products and third-party intelligence – otherwise known as ATLAS® – to gain unmatched visibility into global threat activity. The global insight derived from ATLAS/ASERT continuously arms all Arbor products and services in the form of features, integrated workflows and the ATLAS Intelligence Feed (AIF).

| Arbor Products | |
|---|---|
| **Arbor Cloud DDoS Protection Products and Services** | • A fully managed, tightly integrated combination of in-cloud and on-premise DDoS protection.<br>• 24/7 managed DDoS protection with 14 scrubbing centers around the world providing over 11 Tbps of mitigation capacity. |
| **NETSCOUT Arbor Edge Defense** | • Always-on, in-line, detection and mitigation of DDoS attacks ranging from sub 100 Mbps to 40 Gbps.<br>• Can stop inbound and outbound DDoS attacks, malware, and C2 communication. |
| **Arbor Sightline & Threat Mitigation System (TMS)** | • Arbor Sightline provides pervasive network visibility and DDoS attack detection.<br>• Arbor TMS provides out-of-path, stateless, surgical mitigation at up to 400 Gbps per 2U device. |
| **Arbor Sightline with Sentinel** | • Intelligently optimize mitigation based on infrastructure capability to block attacks in the most efficient and scalable way.<br>• Share attack data and request mitigation help from other networks.<br>• Detailed reporting to see exactly what is being dropped, where, and why. |




NETSCOUT

**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



SECSS_011_EN-2001 04/2020