NETSCOUT ARBOR EDGE DEFENSE AND/OR ARBOR CLOUD CASE STUDY

Technology & Business Solutions Provider uses NETSCOUT DDoS protection to help people, clients and communities move into the digital future

Introduction

This case study of NTT is based on a September 2021 survey of NETSCOUT Arbor Edge Defense and/or Arbor Cloud customers by TechValidate, a 3rd-party research service.

Challenges

The business challenges that led NTT to evaluate and ultimately select NETSCOUT Arbor Edge Defense and Arbor Cloud:

- NTT agrees that NETSCOUT Arbor Edge Defense product and Arbor Cloud DDoS Protection service help their company solve cybersecurity challenges by:
  - Detecting, and mitigating DDoS attacks that impact availability of network, services, or stateful security devices
  - Detecting and blocking inbound IoCs, brute force password attempts and reconnaissance
  - Detecting and blocking outbound IoCs or communication from compromised internal devices communicating with attacker command and control infrastructure
  - Stopping DDoS attacks or other cyberthreats embedded in encrypted traffic

Use Case

The key features and functionalities of NETSCOUT Arbor Edge Defense and Arbor Cloud that the NTT uses:

- The primary reason their organization uses NETSCOUT Arbor Edge Defense and Arbor Cloud solutions for security operations:
  - Effectively **stop complex DDoS attacks** as efficiently as possible before they impact network, business-critical applications or services
  - Effectively **stop state-exhaustion DDoS** attacks before they impact stateful network devices such as firewall, VPN gateways or load balancers
  - Complement cloud-based DDoS protection from our ISP/CDN provider with on-premises DDoS protection using Arbor Edge Defense
  - Enhance end-user and customer productivity with improved network availability, reliability, and responsiveness
  - Improve security posture and faster time to detect and respond to threats on-prem and in the cloud
- Rates NETSCOUT Arbor Edge Defense and Arbor Cloud solutions **extremely important** or **important**:
  - Arbor Edge Defense for stopping inbound and outbound threats at perimeter
  - Arbor Cloud DDoS protection service for stopping volumetric DDoS attacks
  - NETSCOUT threat intelligence powered by ATLAS® and ASERT to stay informed of latest cyberthreats
  - Arbor Managed Services for day-to-day DDoS management and optimized protection

Results

NTT achieved the following results with NETSCOUT Arbor Edge Defense and Arbor Cloud:

- Reduced their Mean Time to Resolution (MTTR) by **50 – 79%** with NETSCOUT Arbor solutions.
- Considers the value NETSCOUT Arbor Edge Defense and Arbor Cloud as **"Significantly Better"** compared to alternative solutions.
- Plans to utilize the following solution along with NETSCOUT Arbor Edge Defense or Arbor Cloud for their security management:
  - Logrhythm SIEM

Company Profile

Company:
NTT

Company Size:
Global 500

Industry:
Telecommunications Services

About NETSCOUT Arbor Edge Defense and/or Arbor Cloud

Arbor Edge Defense acts as a network edge threat intelligence enforcement point where it blocks inbound cyber threats (e.g. DDoS attacks, IOCs) and outbound malicious communication – essentially acting as the first and last line of perimeter defense for an organization. The Arbor Cloud service delivers a fully managed, best-practices hybrid defense from the data center to the cloud – supported by the world's leading experts in DDoS attack mitigation.

Learn More:

☐ NETSCOUT

☐ NETSCOUT Arbor Edge Defense and/or Arbor Cloud

Source: Soumen Biswas, MS Engineering Team Lead - SOC, NTT