NETSCOUT ARBOR EDGE DEFENSE AND/OR ARBOR CLOUD CASE STUDY

North American government uses Arbor Edge Defense to stop DDoS attacks

Introduction

This case study of a state & local government is based on a November 2021 survey of NETSCOUT Arbor Edge Defense and/or Arbor Cloud customers by TechValidate, a 3rd-party research service. The profiled organization asked to have their name blinded to protect their confidentiality.

Challenges

The business challenges that led the North American government to evaluate and ultimately select NETSCOUT Arbor Edge Defense and Arbor Cloud:

- The North American government company **strongly 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 North American government uses:

- Utilizes NETSCOUT Arbor Edge Defense and Arbor Cloud solutions for:
  - 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
- Utilizes the following:
  - AWS
  - Microsoft Azure
- Rates NETSCOUT Arbor Edge Defense and Arbor Cloud solutions **extremely 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 cyber threats
  - Arbor Managed Services for day-to-day DDoS management and optimized protection

Results

North American government achieved the following results with NETSCOUT Arbor Edge Defense and Arbor Cloud:

- Reported NETSCOUT Arbor solutions reduced Mean Time to Resolution (MTTR) by **50–79 %**.
- Rated NETSCOUT Arbor Edge Defense and Arbor Cloud, **"Best-in-Class"**, compared to alternative security solutions.
- Also using/planning to use the following security tool(s) with NETSCOUT Arbor solution.
  - Azure Sentinel
  - Splunk SIEM

Organization Profile

The organization featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Organization Size:
State & Local

Industry:
Government

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: TechValidate survey of a State & Local Government

Validated Published: Feb. 10, 2022 TVID: 199-ED4-D66

Research by TechValidate by SurveyMonkey