

Federal Agency uses Arbor Edge Defense and Arbor Cloud to keep their services running and secure

Introduction

This case study of a federal government is based on a September 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 Federal Agency to evaluate and ultimately select NETSCOUT Arbor Edge Defense and Arbor Cloud:

- Federal Agency **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 the availability of the 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 cyber threats embedded in encrypted traffic

Use Case

The key features and functionalities of NETSCOUT Arbor Edge Defense and Arbor Cloud that Federal Agency 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 firewalls, VPN gateways, or load balancers
 - Complement cloud-based DDoS protection from our ISP/CDN provider with on-premises DDoS protection using AED
 - 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 the 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

The Federal Agency achieved the following results with NETSCOUT Arbor Edge Defense and Arbor Cloud:

- Reduced their Mean Time to Resolution (MTTR) by **80 – 100%** with NETSCOUT Arbor solutions.
- Considers the value NETSCOUT Arbor Edge Defense and Arbor Cloud as **“Best-in-Class”** compared to alternative solutions.

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:
Federal

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](#)