

From network risk to recurring revenue

A four-market carrier faced attacks far larger than anything it could absorb. Rather than build scrubbing capacity, I paired Cloudflare's global network with a Kentik control plane we owned, then turned the protection into a multi-tenant service customers could buy.

ROLE

Product & Technology Lead

PERIOD

2023 – 2024

CONTEXT

ATN International (Brava Solutions), across four markets

4

markets protected by one automated platform

Seconds

from detection to mitigation, without waiting on a transit provider

Multi-tenant

designed for resale from day one

— The situation

For an island carrier, availability is the product. Attack sizes across the industry had grown past anything a group this size could absorb on its own, and mitigation depended on transit providers responding on their timescale.

— Build, buy, or partner

Building scrubbing centres meant capital cost across four markets and years to reach useful capacity. The answer was to rent the scale and keep the control: Cloudflare's global network absorbs the attacks, while detection, policy and tenancy stayed ours, on a Kentik control plane fed by the network's own telemetry.

— Two ways to survive

Mitigation runs in two independent phases: a fast network-level response that works even if the scrubbing provider is unreachable, and a precise scrubbing path that keeps customers online while the attack is absorbed elsewhere. Two independent paths meant an availability commitment I was willing to sign.

— What happened after

The service was validated end to end under a formal, signed acceptance test plan, including automated mitigation under simulated attack conditions. Because the platform was built tenant-aware from the start, the defensive spend became a product.

PRACTICE AREAS

DDoS Protection

Cloud

Product Development

Vendor Governance