



**Country Lockdown
Solution**

CASE STUDY

Enhancing network security with FastNetMon

ABOUT THE CUSTOMER

A leading North American insurance corporation, specialising in life insurance and a broad array of financial products and services. A leading North

American insurance corporation, specialising in life insurance and a broad array of financial products and services.

The Challenge:

The insurance industry is highly susceptible to cyber threats due to the sensitive nature of the data involved. The corporation faced specific challenges related to potential intrusions from certain geographic regions, which were identified as high-risk due to recurring unauthorized access attempts and other security threats.



There's a need to implement a solution that could preemptively block traffic from specific regions to ensure compliance and enhance security.

THE FASTNETMON SOLUTION & IMPLEMENTATION

The corporation opted to utilize FastNetMon's country lockdown capability, a sophisticated feature designed to block traffic from specified countries. This decision was driven by the need for a robust security measure that could be seamlessly integrated with their existing network infrastructure. The technical team at the insurance corporation followed a structured approach to implement the

country lockdown feature. FastNetMon Advanced was set up with BGP peering and integrated with the GeoIP2-Country database for IP source identification. A block list of countries was defined, with an allow list for essential traffic. The system executed a script for country lockdown, using BGP to announce blocked prefixes. Continuous monitoring ensures security while allowing necessary business traffic.



Results:

The implementation of the country lockdown feature provided several benefits:

Scalability and Flexibility:

The solution provided the flexibility to quickly adjust the list of blocked countries based on evolving threat intelligence and compliance requirements.

Enhanced Security Posture:

By blocking potentially harmful traffic from high-risk countries, the corporation significantly reduced its exposure to cyber threats originating from those regions.

Compliance Assurance:

The feature supported compliance with industry regulations that mandate specific geographic restrictions, thereby protecting the corporation from potential legal and financial penalties.

Operational Efficiency:

The automation of the blocking process through BGP announcements ensured that the network's security measures did not require manual intervention, thereby saving time and reducing the likelihood of human error.



FastNetMon delivers versatile DDoS detection software for companies at any scale. With extensive experience in the telecom, mobile, and cloud computing industries, we take pride in preventing DDoS attacks and protecting our customers' networks to the highest standard.

Learn more at: www.fastnetmon.com | sales@fastnetmon.com | +40 742 991 619