

## CASE STUDY

### About NSFOCUS

NSFOCUS is an iconic network and cyber security provider for telecom carriers, BFSI, enterprises, healthcare, retail and SMBs. It has a proven track record of protecting over 25% of the Fortune Global 500 companies, including four of the five largest banks and six of the world's top ten telecommunications companies.

NSFOCUS delivers a holistic suite of security products powered by industry leading threat intelligence. These security products work in concert to protect you from massive volumetric DDoS attacks, Web threats and advanced persistent threats (APTs).

### Connect with NSFOCUS:

Blog: [nsfocusglobal.com/blog/](https://nsfocusglobal.com/blog/)

LinkedIn [@nsfocus](https://www.linkedin.com/company/nsfocus)

Twitter [@NSFOCUS\\_Intl](https://twitter.com/NSFOCUS_Intl)

Facebook [@nsfocus](https://www.facebook.com/nsfocus)

### NSFOCUS Website:

[www.nsfocusglobal.com](https://www.nsfocusglobal.com)

## Fortune Global 500 Energy Corporation Partners with NSFOCUS on Cloud DPS Holistic Solution and Advanced MSS

As one Fortune Global 500 energy company, this large-scaled company has a lot of business traffic across their network every day. Meanwhile criminal cyber activities and risks have increased since outbreak of the COVID-19 pandemic, not only because the pandemic has made working from home the new way of working for their employees, but attackers are using the pandemic as part of their cyber operations. The customer was eager to have a solid solution to protect their business and daily work. After carefully comparing solutions from different vendors, the customer selected NSFOCUS hybrid solution finally. This solution contains cloud-based DDoS Protection service (Cloud DPS) and on-premises Network Traffic Analyzer (NTA), offering real-time traffic detection and on-demand traffic scrubbing service while ensuring good traffic goes through. The customer also likes NSFOCUS Managed Security Service (MSS), too. This service is provided by NSFOCUS SOC team. With cybersecurity experts watching over the business, the customer can focus on their more important thing – growing their business.

### Protected by NSFOCUS Solution and SOC Team

With active-active on-premises NTA devices and 8 global Cloud PoPs deployed, NSFOCUS ensures the high service availability to provide continuous protection to the customer.

With Managed Security Service, the customer's business was protected 24/7 proactively. An experienced Technical Account Manager (TAM) was allocated to provide expert support related to the customer's security operations during the entire life cycle of the service. Periodic governance meetings were held to sync up with the customer on security status and make fine-tuned approach for better protection. Proactive tuning and optimization ensures the detection and protection policies always secure customer's business best.

# CASE STUDY

For more information, please contact:

**U.S.**

Tel: + 1 408-907-6638

**EMEA**

Tel: +44 (0) 20 3882 7025

**LATAM**

Tel: +55 11 3521-7124

Email:

[contato@nsfocusglobal.com](mailto:contato@nsfocusglobal.com)

**APAC**

Email:

[apmarketing@nsfocusglobal.com](mailto:apmarketing@nsfocusglobal.com)

**GCR:**

Email:

[gcrmarketing@nsfocusglobal.com](mailto:gcrmarketing@nsfocusglobal.com)

## Optimization of Detection and Protection Capability

Policy optimization is an inventory and reinforcement of the security capability. NSFOCUS SOC team delivered this service for the customer.

### Assets Reorganization

- Clear division of protection assets into Always-on, Auto Diversion, and Monitor Only to better suit customized diversion needs



### Alerts

- Delicate email notification setting to filter out invalid and distracting alerts and highlight the effective ones, thus improving the effectiveness and accountability



### Detection Adjustment

- Reorganize detection groups per business types like Web, VPN, DNS for clearer and business-oriented management
- 7-day traffic baseline study based on business types
- In-depth alerts and learning results analysis
- Application, effect monitoring and continuous adjustments for more accurate detection

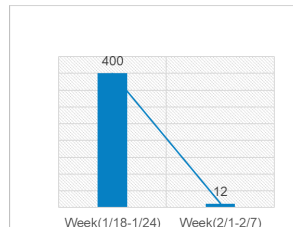


### Mitigation

- Reorganize protection groups per business types for more efficient and business-oriented policy management
- Apply appropriate policies for the differentiated business to avoid false positive or negative

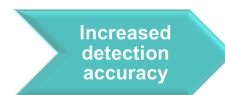
This numbers below shows the great improvement. The customer is very satisfied with the result.

Alert No Before/After Optimization



### 97% Relative improvement on false positive

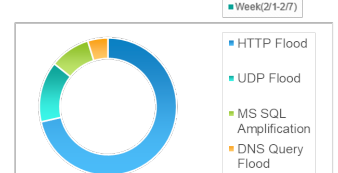
- Before policy-tuning, there are 400 alerts per week, however, after policy-tuning, only 12 alerts reported by the detection appliance.
- With alert log analysis and baseline study result comparison, the false positive accountability is decreased from 90% to 5%.



### Accuracy Up to 80%

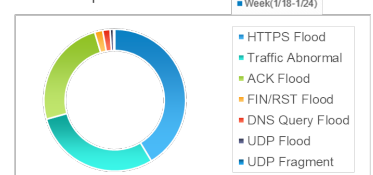
- Before policy-tuning, various DDoS attack type are detected. The majority are normal business traffic exceeding the improper threshold, leading to 85% false positives.
- After policy-tuning, the DDoS Attacks are mainly DNS and UDP. The number of business related attacks is greatly reduced, with accuracy increased up to 80%.

After Optimization



### DDoS Attack Event

Before Optimization



The optimization service boosted the customer's network security capability on both detection and protection:

- » Largely reduced false positive
- » Proactive and constantly fine-tuned protection policies set for different business traffic avoided blocking of intended traffic passing through