NEXUSGUARD

Politically-fueled DDoS attack targets international airport authority, disrupting real-time information exchange for operators and passengers. The airport authority is responsible for handling:

- Tens millions of flights annually
- 100+ airlines and 180 destinations
- 1 flight per minute during peak hours

Nexusguard DDoS+ Protection Keeps Busy, World-class Airport Flying High

When one of Asia's busiest airports faced turbulence from hackers, administrators turned to Nexusguard to help ensure uninterrupted uptime — and keep passengers updated in real time.

Attackers target one of Asia-Pacific's busiest hubs

An airport authority responsible for handling millions of Asia-Pacific flights every year recently fell victim to cyber attacks during a time of civil unrest. True to the state-of-the-art modernity and efficiency of its host city, the airport is renowned for world-class customer service and the real-time delivery of up-to-the-minute flight information. As such, airport administrators make it their mission to ensure the uninterrupted availability of crucial flight data and airport services that travelers depend on.

Beyond on-premise infrastructure

Already an attractive target, the airport's website was further exposed to cyber threats during a period where "hacktivists" supporting democracy protestors were eyeing a variety of government assets. Lacking comprehensive reporting and monitoring tools, the airport authority required additional protection beyond its existing on-premise infrastructure. Furthermore, to meet the needs of countless travelers and airport personnel, the airport's website had to be able to be back up and running immediately after an attack.

From among several leading Content Delivery Networks (CDN) and Managed Security Service Providers (MSSPs), Nexusguard was chosen because it could guarantee immediate provisioning and the flexibility required to handle emergencies and compatibility with existing applications. Additionally, Nexusguard's solution stood out for its transparency, monitoring, and data-analysis capabilities.

NEXUSGUARD

An untimely DDoS attack calls for emergency provisioning

On September 30, 2014, the airport authority came under attack, its datacenter saturated by volumetric traffic. In an attempt to minimize collateral damage to other customers, the datacenter black-holed the authority's server IP, which blocked access to the airport's website and services, including real-time flight information for passengers.

In response, administrators made an emergency request to Nexusguard for immediate provisioning, a process that typically takes up to three days in the industry. Despite the fact that the authority had yet to sign a formal agreement with Nexusguard, its website was protected by Nexusguard's anti-DDoS platform within three hours, resulting in the immediate resumption of online services.

More than just DDoS protection

Nexusguard's DDoS mitigation platform was able to integrate fully with the airport authority's infrastructure, without the need to invest in additional hardware or skilled security personnel. The authority's data security team migrated its web services seamlessly to Nexusguard, automatically gaining Layer-3, Layer-4, and Layer-7 protection against DDoS and web attacks. Beyond complete cyber protection, Nexusguard's DDoS+ Protection service also enhanced the authority's ability to analyze crucial website data and comply with government regulations and reporting requirements.

In the end, it was not Nexusguard's technology or expertise alone that prevented a severe outage to the authority's web services. Rather, it was a combination of customizable solutions, flexibility, and speed that allowed the airport operator to keep its promise of top-notch customer service and ensure a positive — and uneventful — airport experience for travelers.