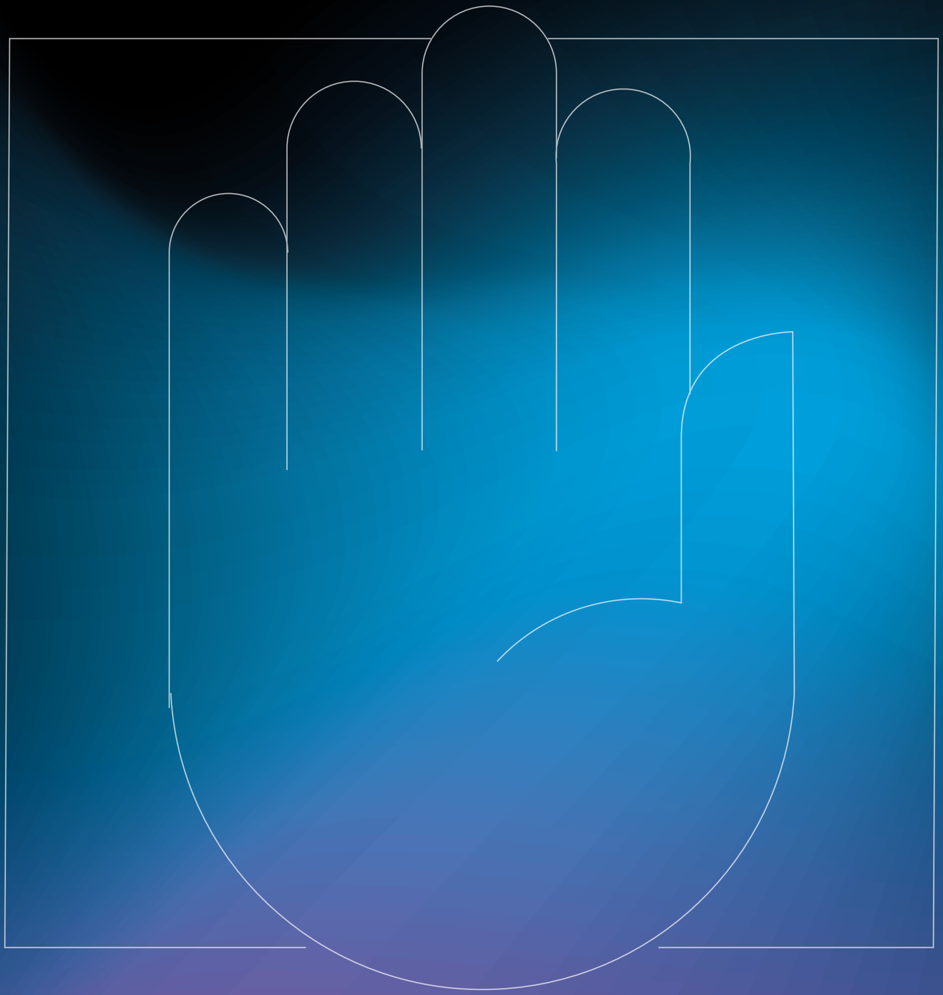
QRATOR LABS



Use case — Popular Travel Website

DDoS attacks and Bot Attacks Comprehensive Protection for a Popular Travel Website

Company background

One of the most **popular websites** for travelers, it was initially created as a schedule for suburban trains and evolved into an informational and commercial service that allows users to purchase trains and flight tickets, book hotels, or buy package tours.

The **website's** monthly audience is over 20 million people, with 80% of them being highly loyal visitors who value the portal for its exceptionally high level of service.

"Not only do we provide straightforward information about travel destinations, but also strive to offer users detailed data so they can plan their trips conveniently. On our platform, you can read reviews about landmarks, tourist routes, hotels, and even special train compartments, and then immediately purchase a tour or tickets to the cities and countries that interest our visitors," said the **travel website's Technical Director**.

Challenges

The flip side of the portal's popularity is the interest of cybercriminals it attracts. The 20-million audience ensures stability and profitability for the website's business. However, a company of such a scale could become a victim of extortion or be engaged in unfair competitive practices, as bitter rivalry in the Travel segment increases the likelihood of targeted DDoS attacks aiming to disrupt the portal's operations.

There is a clear seasonal threat correlation with the intensity of attacks rising during holidays and vacations when travel services are mainly in high demand.

Even brief service interruptions during high season not only can damage the company's reputation but also result in significant direct losses.

Challenges

Denial-of-service attacks are not the only threat the web portal faces. Using bots, criminals can engage in content theft and brute force attacks to gain access to user accounts. This can result in the theft of users' personal data, passport information, or payment details. Ultimately, these attacks may be conducted for competitive parsing purposes.

These **website** security threats presented several challenges for the **travel website's** team:

○ Prevent DDoS attacks;

○ Pay special attention to mitigation of L7 (Application layer) attacks;

○ Ensure protection of users' accounts, including their personal data.

Solution

"Several key criteria guided us in choosing a **DDoS protection solution**. These included the ease of service connection, its invisible operation and lack of impact on network performance, and low latency traffic filtering. We finally settled on **Qrator Labs solutions for DDoS mitigation**, hacking attempts and bot protection," explains the Technical Director.

The comprehensive security of website is ensured by two **Qrator Labs** solutions:

○ **Qrator.AntiDDoS** ensures continuous availability of the web resource and neutralizes DDoS attacks;

○ **Qrator.AntiBot** blocks malicious bot activity, including content parsing (searching and downloading content) and brute force hacking attempts — passwords, encryption key guessing, etc.

Experience

The travel portal has been using **Qrator Labs solutions** for over six years that helped to prevent several large-scale hacker attacks. One was organized by parser bots and lasted about two weeks. **Qrator.AntiBot** allowed detection of brute force activity and blocking traffic from illegitimate IP addresses as soon as they sent in their initial request, preventing its execution on the server's side.

In 2020, yet another more destructive Application-level attack was mitigated. The attack lasted for several hours, aiming to knock down the website's availability. The **Qrator.AntiDDoS** solution blocked all malicious traffic right at the perimeter using deep behavioral, correlation analysis, and traffic monitoring. These capabilities enable the **Qrator Labs** filtering network to effectively counter potentially devastating threats, ensuring the operability of the client's web resources 24/7.

Experience

"**Qrator Labs** has been providing protection for our site for six years, and during all this time, our users have not experienced any disruptions in its operation or cybersecurity incidents related to privacy. DDoS attacks are no longer a threat to us — they are automatically and instantly prevented by **Qrator Labs solutions**. Thanks to reliable protection, our business has gained guaranteed continuity, and we provide users with a high-quality service 24/7," emphasized **the website's Technical Director**.

QRATOR LABS

Use case — Popular travel website

2023