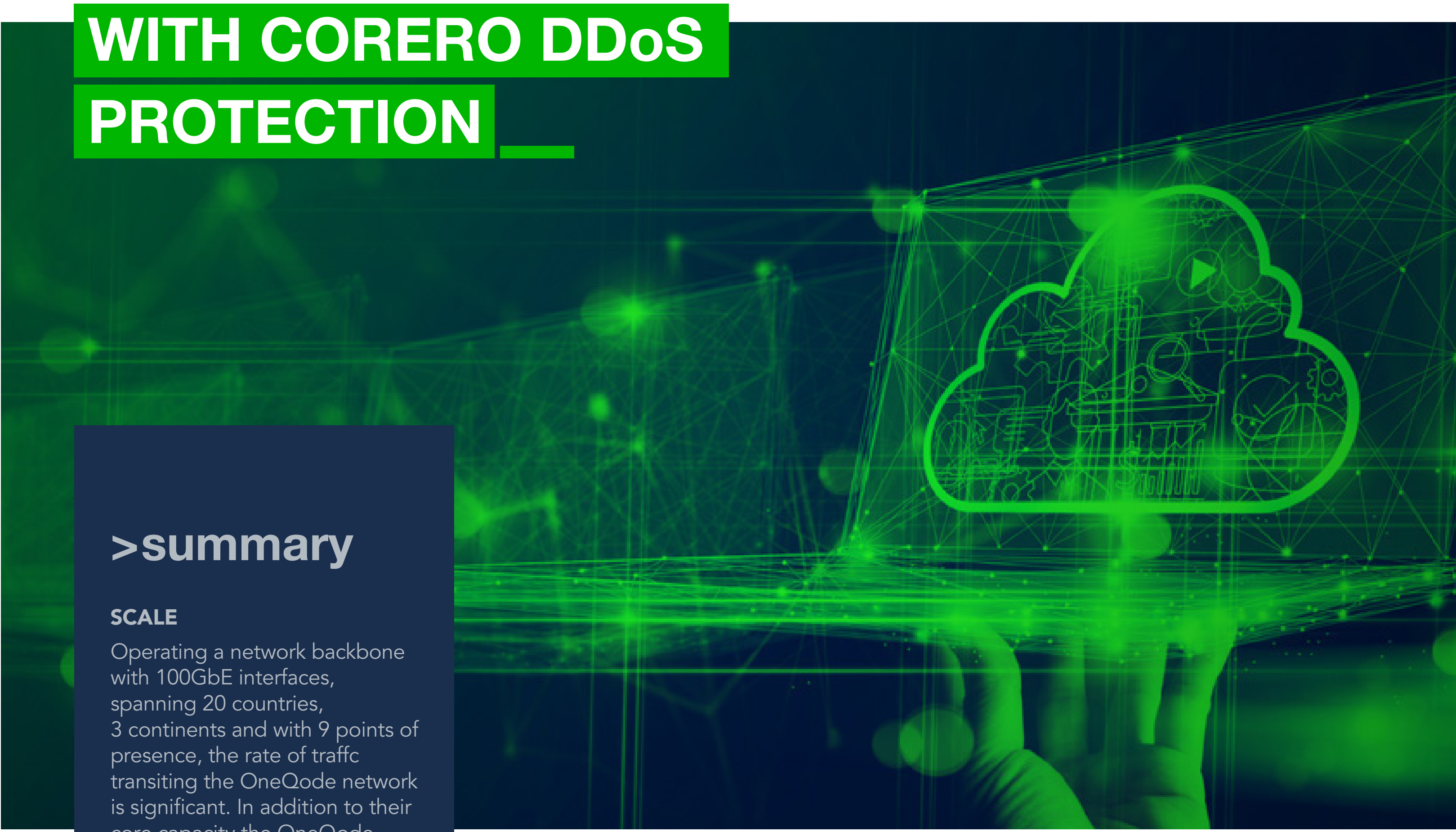
CASE STUDY

ONEQODE BOLSTERS THE LATENCY-SENSITIVE APAC ONLINE GAMING EXPERIENCE WITH CORERO DDoS PROTECTION



>summary

SCALE

Operating a network backbone with 100GbE interfaces, spanning 20 countries, 3 continents and with 9 points of presence, the rate of traffc transiting the OneQode network is significant. In addition to their core capacity the OneQode network manages a network edge with diverse peering from multiple carriers.

SOLUTION

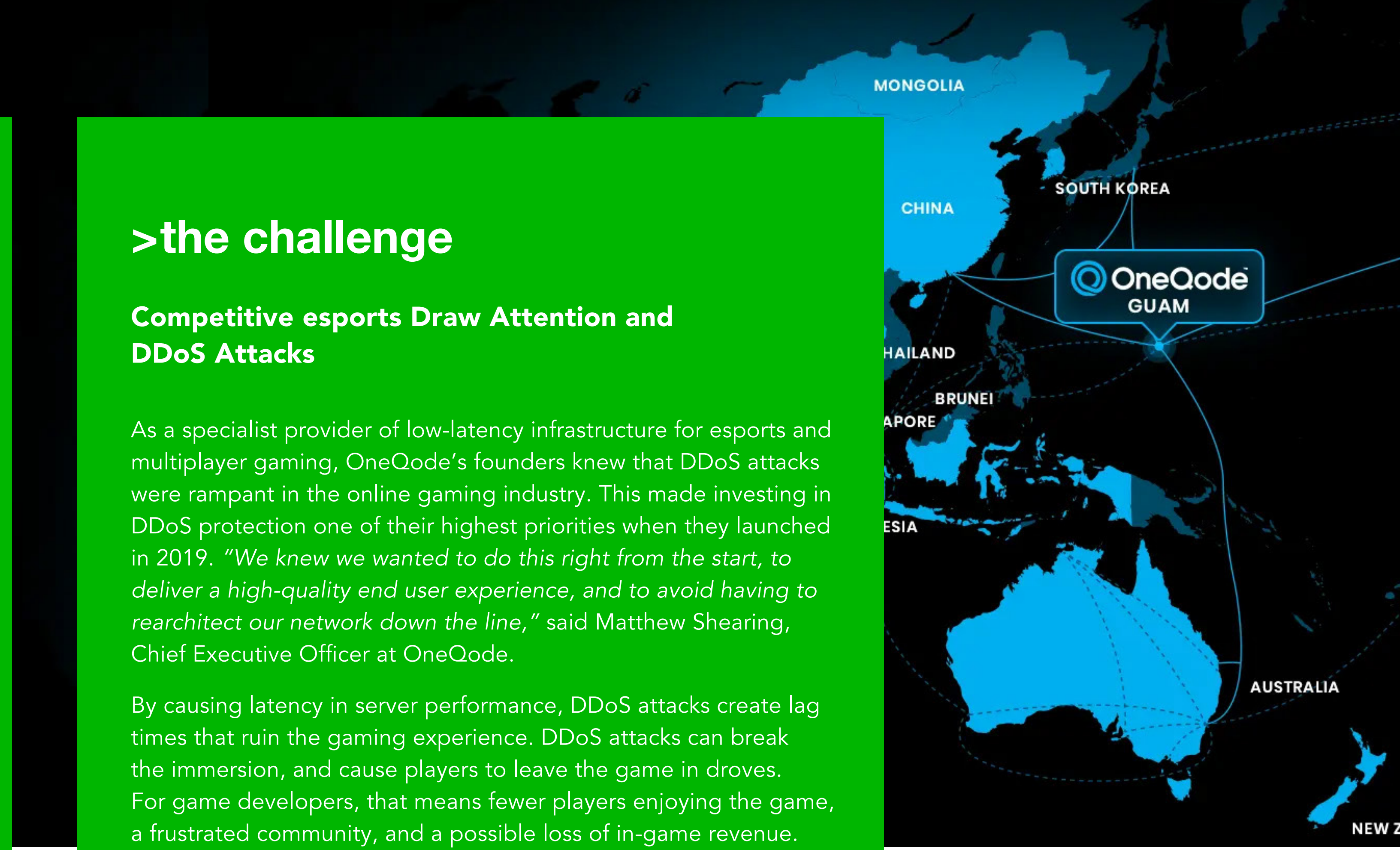
Corero SmartWall® Follow the sun support 24x7x365

DEPLOYMENT MODEL

In order to neutralize DDoS attacks in real-time and avoid any downtime while traffic is being analysed, the Corero SmartWall® solution is positioned at the network edge. This Datapath model ensures an always-on, automatic detect and mitigate service in real-time.

Headquartered in Australia, OneQode is a global infrastructure as a service (IaaS) company operating a latency-optimised international carrier network and high-performance cloud platform.

Built by gamers, for gamers, OneQode's network infrastructure is scaled for the demands of real-time, lag-free applications. OneQode works primarily with game industry customers helping them deliver consistent, high-fidelity, low-latency multiplayer experiences. OneQode's infrastructure provides a backbone for many of the 1.45 billion gamers in Asia Paciffc (APAC), the largest region gamers globally. These hundreds of millions of gaming customers demand ultra-low latency connectivity with zero downtime.



>the challenge

Competitive esports Draw Attention and DDoS Attacks

As a specialist provider of low-latency infrastructure for esports and multiplayer gaming, OneQode's founders knew that DDoS attacks were rampant in the online gaming industry. This made investing in DDoS protection one of their highest priorities when they launched in 2019. *"We knew we wanted to do this right from the start, to deliver a high-quality end user experience, and to avoid having to rearchitect our network down the line,"* said Matthew Shearing, Chief Executive Officer at OneQode.

By causing latency in server performance, DDoS attacks create lag times that ruin the gaming experience. DDoS attacks can break the immersion, and cause players to leave the game in droves. For game developers, that means fewer players enjoying the game, a frustrated community, and a possible loss of in-game revenue. For some games, this can be the kiss of death that results in an almost complete collapse of the game's multi-player base. Furthermore, in the competitive esports arena, a DDoS attack can influence the betting market on competitive games, either contributing to a financial gain for an attacker or disrupting the overall gambling market for a game.

>the results

Corero gives OneQode's game developer customers peace of mind, because their servers and cloud instances maintain consistent network performance, with no disruption or performance degradation in the event of a DDoS attack.

It is particularly important for their customers (gamers) that traffic is never diverted to a scrubbing facility when an attack happens. There's no spike in latency for players (which can kill the gaming experience), and they can continue to play without even knowing there's an attack underway. *"The real reward is that gamers notice nothing,"* said Shearing.

Corero's DDoS defence-filtering technology deployed across the OneQode network protects servers from disruptive attacks, without kicking existing players from games. During the first genuinely cross-regional Asia-Pacffic CS:GO tournament, gamers from as far afield as Mongolia and Australia were able to compete online with under 100 milliseconds of latency.

> *"In short, our DDoS protection means our customers can reduce player churn and improve the overall online experience for their users,"* said Shearing.

Thanks to OneQode's unique APAC network architecture, this was an historic first for the APAC gaming community. Unbeknownst to players, over the course of 5 days, OneQode's DDoS-protection systems mitigated 856 separate attacks, including one that would normally be a game-ending attack — allowing games to continue uninterrupted.

>why OneQode chose Corero

Real-time performance is a core part of OneQode's strategy - and a priority when it comes to DDoS mitigation.

"We needed a solution provider whose solution could keep pace with our network and enable us to maintain uninterrupted, low-latency connectivity in the face of high-throughput attacks. In this regard, Corero is unmatched, the definitive choice when performance under pressure matters," said Ben Cooper, Chief Architect. *"Corero's system is flexible and scalable- enabling us to place scrubbers all over the world and control them via a single pane of glass. We looked at several DDoS solution providers and selected Corero as their DDoS solution meets our needs, in terms of protection and guaranteed latency."*

Automation Eliminates Manual Intervention

Corero keeps OneQode's network clear of bad traffic, and the Corero dashboard provides real-time, single-pane visibility of attacks. Because the Corero SmartWall® solution is automated, OneQode's IT security analysts don't have to manually intervene to handle DDoS attacks, which gives them peace of mind, increases their productivity and efficiency, and gives them time to tackle other tasks." *Corero provides hands-off DDoS protection, which frees up time for our security team, so they don't have to think about it"* added Cooper.

An Unusual Implementation

Corero hardware is located at every entry point to OneQode’s global network.

> *Shearing said “We have an unconventional setup, whereby the systems are run in the traffic path to ensure the fastest attack response possible with always-on monitoring. While this makes it more capital intensive to deploy a new point of presence, it ensures traffic across our network is free from disruption - enabling us to serve gaming customers better.”*

Automation Eliminates Manual Intervention

OneQode provides DDoS protection at no cost to its customers, as a value add. *“Many in the industry charge per Mbps for DDoS protection - so their customers pay every time they’re attacked, which isn’t fair. It should be a standard feature, so we made it one,”* said Shearing.

Easy User Interface

“One of our favorite features of the Corero SmartWall is that it’s user-friendly, which makes it easy to train and onboard new staff,” said Shearing,*“ In future, OneQode will enable customers to set their own Corero rules for their OneQode services via the customer dashboard.”*

>Corero Smartwall at a glance

- Operates in real-time, 24/7.
- Surgically and automatically removes DDoS attack traffic, before it reaches critical systems, eliminating downtie, ensuring optimal performance and maximum availability.
- Delivers line-rate, always-on distributed denial of service attack protection, in a solution that scales to tens of Terabits per second of protected throughput.
- Prevents impact from even the most sophisticated DDoS attacks ranging from volumetric floods, to state exhaustion incidents.
- Delivers comprehensive forensic-level analysis before, during, and after attacks.
- Ensures that legitimate traffic is not impacted by false positives.
- Inspects every inbound packet header and payload data, surgically removing the DDoS packets without disrupting the delivery of legitimate network traffic.
- Corero’s Smart Rules leverage heuristic and closed-loop policy, so rules can be reconfigured and deployed on-the-fly, thereby responding rapidly to evolving, sophisticated DDoS attacks.
- Detects and mitigates attack traffic in under a second; not minutes or tens of minutes, as with traditional DDoS protection solutions.

US HEADQUARTERS ✉ info@corero.com **EMEA HEADQUARTERS** ✉ info_uk@corero.com