OCIRIS Values Corero for Inline, Instant DDoS Mitigation

Founded in 2003 as a data center hosting and cloud services company, OCIRIS offers core premium hosting services—cloud services, dedicated server, DDoS protection and IP connectivity—to leading companies in the world. OCIRIS is the company behind GPORTAL and the parent company of GPORTAL INC., in the USA, an industry leader in gaming infrastructure. GPORTAL hosts gaming servers for EA DICE's blockbuster games, Battlefield 3 and Battlefield 4 and many other Game Studios like Gamepires and Funcom. GPORTAL has evolved to become the number one end consumer game hoster, and was the first end consumer to become certified by Microsoft as an official, exclusive partner for players to rent their own private server on Xbox.

The Challenge

Headquartered in Munich, Germany, GPORTAL manages 5,000 bare metal servers in twelve data centers in twelve countries across North America, Asia and Europe, and is planning to roll out another two or three international data centers in the coming year. GPORTAL and its customers are routinely targeted by DDoS attacks. Each day the company sees approximately of 50 - 420 attempted DDoS attacks on its global infrastructure, targeting different servers and different clients. The attacks range from relatively small, sophisticated, state-exhaustion attempts to large multi-Gbps volumetric floods, with the largest attack weighing in at around 380 Gbps.

Prior to implementing a real-time automatic mitigation solution, GPORTAL suffered frequent outages, many of them serious, as a result of DDoS attacks. It had been able to block only a handful of attacks because its defenses consisted of some basic access control list rules on its data center routers. As the company quickly grew and DDoS attacks became more frequent and sophisticated with different patterns and multiple vectors, it became clear to GPORTAL that a comprehensive DDoS mitigation solution was required. "We needed an in-line appliance that focused on DDoS protection, so we tested several DDoS protection solutions via proof of concept tests over the course of several months," said Roberto Omezzolli, Founder and Chief Technology Officer, OCIRIS GmbH.

In 2015, GPORTAL chose the Corero SmartWall® Threat Defense System (TDS) because it provides inline protection and instant mitigation. Omezzolli reports that "98% of the attacks are now completely mitigated with the remaining attacks requiring surgical mitigation with the SmartWall FlexRule feature."

Other vendor solutions tested by GPORTAL in proof of concept trials didn't provide inline protection and took too much time to mitigate attacks, resulting in game players being knocked offline. Offsite, cloud-based, scrubbing services were not acceptable options because they not only suffer from delayed attack mitigation, they also introduce significant lag to the gaming experience, which would not be acceptable to GPORTAL's clients that are extremely latency sensitive. "The gaming industry depends on zero latency, and that requires proactive, real-time DDoS mitigation," said Omezzolli.

The Solution

GPORTAL deployed Corero's SmartWall DDoS protection to provide their customers with a high-quality service that has very low latency. GPORTAL chose Corero SmartWall TDS partly because it delivers the most sophisticated layer 3 to 7 DDoS volumetric protection, able to block attacks in real-time before they cause disruption to gaming sessions or enterprise applications.

The SmartWall TDS solution utilizes Corero innovation, automatically mitigating volumetric single and multi-vector DDoS attacks and incorporating custom defined filters for more sophisticated attack vectors. The SmartWall platform utilizes a high-performance scalable architecture that surgically removes DDoS attack traffic, while allowing good user traffic to flow uninterrupted.

The built-in SmartWall Analytics enables fast and deep traffic analyses, identifying patterns and anomalies in real-time, facilitating the creation of highly granular filters to detect, test, and mitigate new attack vectors in real-time. "Our DDoS protection is a big competitive differentiator in the game server industry," said Omezzolli. "The first thing our B2B customers ask is, 'Do you have effective DDoS protection?' because it is critical in the gaming and hosting industry to have smart and reliable DDoS protection. Other companies say they have DDoS protection, but in reality, they have only blocked attacks at their router; we wanted a real DDoS protection, so we can mitigate attacks from the very first packet after detection so we don't delay the mitigation at all."

"The SmartWall dashboard allows us to monitor network traffic and patterns in real-time, which allows us to adjust accordingly to create custom flex rules for new DDoS attack types to detect and mitigate them in real-time, before they reach our clients and cause disruption to gaming sessions or enterprise application use," said Omezzolli. "And if one of our customers complains about 'rubber banding' we can show that customer the history so s/he can see attacks that were mitigated."

"We have one of the best DDoS protection services, and it comes standard as a service for all of our 60,000 clients around the world. As a result, we deliver reliably fast and seamless gaming experiences as well as quick provisioning times—for an unpredictable number of global users, around the clock, every day.

"One of our goals is to offer the most powerful, reliable network with lowest latency for our gamers," said Omezzolli. "Thanks to the Corero SmartWall our customers enjoy smooth, fast, real-time gaming experiences with 99% uptime."

The Implementation

The Corero SmartWall are deployed in-line at the network edge, in front of traditional network security infrastructure devices, to ensure packets are inspected and attacks mitigated before they could impact any downstream servers or applications. This deployment model allows GPORTAL the ability to meet its uptime service levels.

Omezzolli recommends the Corero solution because it performs extremely well, at a very competitive price. GPORTAL is pleased with the excellent support provided by the Corero Security

Operations Center and the relatively fast implementation. "There were a few challenges and issues, but Corero's support team is very responsive, so within two months we reached a point where we had everything in place, working extremely well," said Omezzolli.

The company first rolled out the Corero solution in its Frankfurt, Germany Data Center. With the latest deployments, they also have protection in the United States, both East and West Coast, the UK and Asia. This multi-site deployment enables GPORTAL to mitigate close to the source of an attack, before it fills the transit pipes of the entire network.

"We're very pleased that GPORTAL users are now able to take advantage of the most up to date and effective DDoS protection that is currently available," said Omezzolli. "Corero SmartWall devices allow us to focus on providing a high-quality service to our clients, rather than having to manually intervene when a DDoS attack occurs."
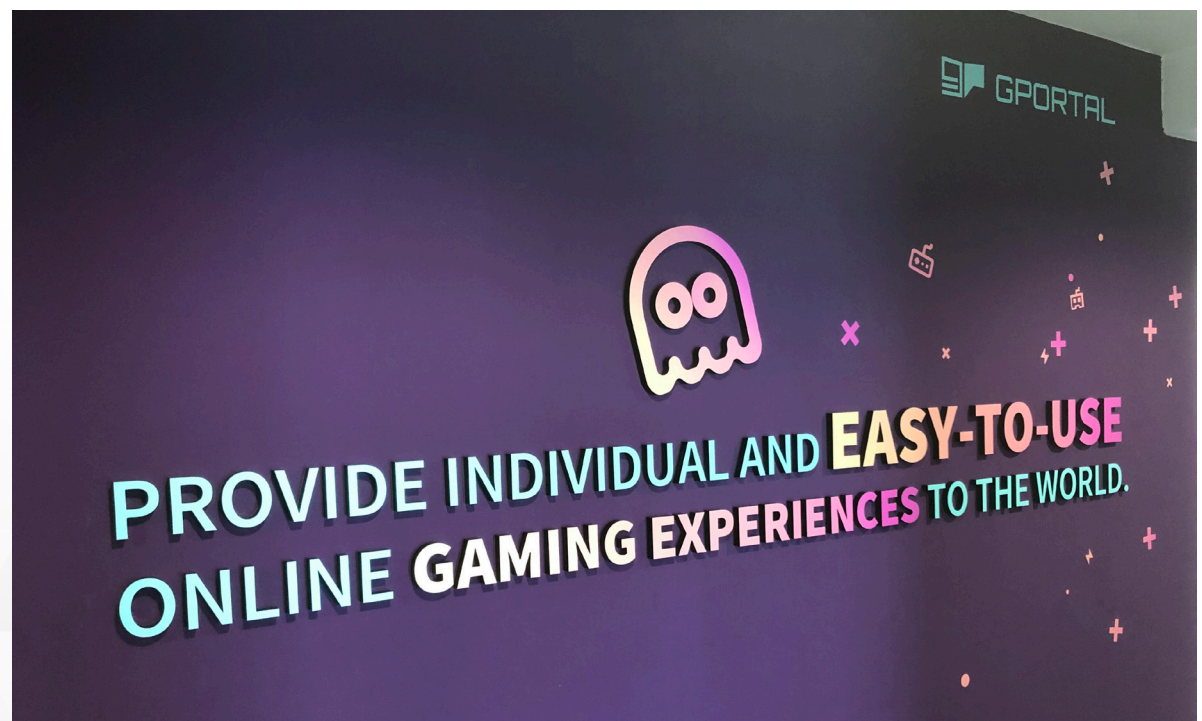
Corero SmartWall At a Glance

» Surgically removes attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.

» Offers line-rate, in-line, denial of service protection from 20Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of performance.

» Prevents everything from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.

» Delivers comprehensive visibility for attack analysis and forensics.

The Results

» Maintains maximum levels of availability for applications and mission-critical systems, in the face of a DDoS event.

» Enables GPORTAL to mitigate DDoS attacks locally, at each of their multiple locations around the world.

» Flexible deployment configurations allow the SmartWall solution to best meet the needs of GPORTAL's individual customers.

» High-quality service allows GPORTAL staff to focus on providing peace of mind to its clients, instead of spending time on manual intervention when a DDoS attack occurs.

corero

As the DDoS threat landscape continues to evolve, enterprise, hosting and service provider customers around the world rely on Corero for industry-leading defense systems to provide 24/7, automatic attack mitigation services, with threat visibility, sophisticated reporting and analytics. For over a decade, Corero has been providing state-of-the-art, highly-effective, automatic DDoS protection solutions.

For more information, visit www.corero.com