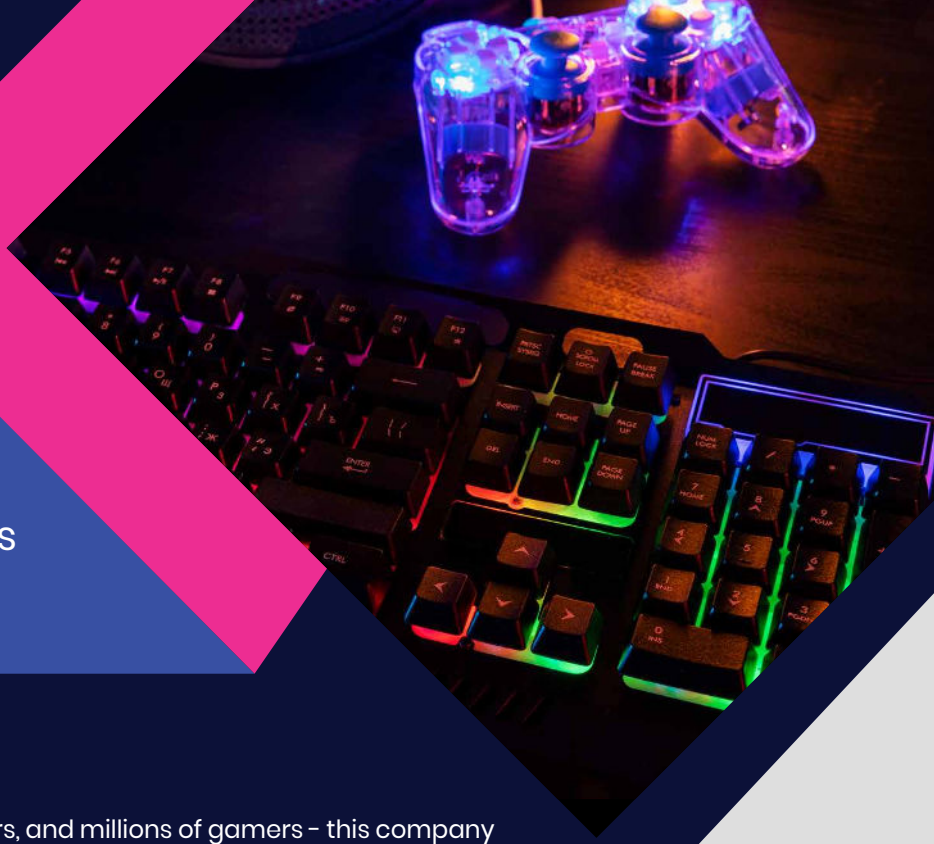
MAZEBOLT



Case Study: Gaming

Top Gaming Company Adopts RADAR™ to Get Back Online

Overview:

With over 6,000 employees, hundreds of partners, and millions of gamers - this company is one of the leading publicly traded companies in the gaming industry. The company specializes in online casino games with integrated online solutions to gaming operators and partners. As a world-wide leader it drew the attention of threat actors and suffered from relentless DDoS attacks with significant financial implications following several weeks of intermittent service disruptions and downtime. The company needed to uncover its true DDoS exposure and risk, while effectively securing its online services.

The Challenge:

As a top provider of online gaming to operators worldwide and a digital entertainment publisher, the company has been a top target for DDoS attacks, caught in a snowball effect, that damaged its ability to function. With millions of Daily Active Users (DAU) and significant Average Revenue Per User (ARPU), every minute of downtime resulted in millions of dollars in losses.

But despite the significant investment in hybrid DDoS protection solutions from top-tier vendors, they continued to suffer damaging downtime. Due to the nature of their 24/7 business, the company couldn't allow maintenance windows to perform DDoS tests. They needed to maintain 100% uptime with zero disruption to gamers.

The Group's CISO understood that solving the DDoS threat was a top priority and was looking for innovative solutions that could provide complete visibility into the company's DDoS security posture. This was when he encountered MazeBolt and was intrigued by the ability to run continuous vulnerability assessments without disruption and zero downtime.

The Gaming DDoS Threat

- Loss of revenue from users, and in-game ads - millions per hour of downtime
- High risk of customer churn – both partners and gamers
- DDoS attacks often include ransom demands during tournaments or official game launches

The Solution:

After a short POC that exposed significant vulnerabilities without any operational downtime requirements, RADAR was deployed downstream to each of their mitigation layers. Continuous simulations identified severe vulnerabilities in layers 3 and 4, with critical misconfigurations in the CPE (on-premises DDoS protection) and Scrubbing Center (cloud-based protection).

MAZEBOLT

RADAR's findings:

- The company's DDoS protection was vulnerable to **45%** of attack vectors launched.
- Mitigation solutions deployed relied heavily upon **reactive and manual** protection procedures previously not disclosed to the company.
- All in all, over **190 DDoS vulnerabilities** were uncovered.

Once RADAR provided initial vulnerability data, MazeBolt's Professional Services team established a new streamlined process with the company and its mitigation vendor in order to prioritize remediation and make sure all online services were protected – without compromising the company's crucial uptime and availability.

Still targeted with DDoS attacks, remediation was underway, and over 120 vulnerabilities were closed within 6 weeks. The company realized that the several consecutive weeks of intermittent downtime and disruption was actually blind luck on the part of the attackers – it could have been much worse.

THE BENEFITS:

- The company experienced zero downtime since remediation started.
- In less than 6 months, using a prioritized action plan for continued remediation, MazeBolt professional services, and the company's mitigation vendor, were able to have over 96% DDoS vulnerabilities remediated.
- RADAR enabled fully automated DDoS protection allowing complete damage prevention and moving away from a heavy reliance of "smart human processes" And damaging emergency response scenarios.
- The company expanded its DDoS coverage to Layer 7 vulnerabilities.
- Since deploying RADAR, the damaging time-to-mitigation
- (TTM) SLAs and the need for emergency response scenarios have been eliminated.

> Once MazeBolt showed us how vulnerable we were, we realized we've deployed RADAR in the nick of time. Since RADAR was deployed, we have experienced no more disruption or downtime."
>
> **CISO,**
> **Leading Gaming Company**

Continuous RADAR simulations and remediation provided the company with the necessary insight and data to validate the effectiveness of its DDoS protection, to block DDoS attacks automatically - and to adopt a new approach to DDoS security with RADAR: Preventative, Proactive, automated Protection.

MazeBolt is pioneering a new standard in DDoS security. RADAR™, an industry-first patented solution, empowers organizations to identify and remediate vulnerabilities in every layer of DDoS protection. Global enterprises, including financial services, insurance, gaming, and high-security government environments, rely on MazeBolt to prevent damaging DDoS attacks.