GLOBAL GAMING COMPANY ZAPS DDOS ATTACKS IN REAL-TIME WITH ZAPR™

> *We have mitigated some pretty large attacks with A10 Networks Thunder TPS, and the response time is milliseconds. "It's amazing what Thunder TPS with ZAPR can do."*

Security Operations Center Manager | Global Online Gaming Company

CASE STUDY

COMPANY

Global Gaming Company

INDUSTRY

Technology

NETWORK SOLUTION

Thunder TPS

aGalaxy Centralized Management System

CRITICAL ISSUES:

- Ensure availability of massively popular online games as DDoS attacks evolve and grow

RESULTS:

- Leveraged a Zero Trust approach to improve game availability and user experience
- Mitigated 200 Gbps DDoS attack with no service interruption
- Increased security operations efficiency with automated DDoS detection and mitigation
- Avoided hundreds of thousands of dollars of spending on cloud-based DDoS scrubbing

INTRODUCTION

The global games market is big—and getting bigger. More than 2.5 billion people play online games, and the gaming industry racked up $152 billion in revenue in 2019, according to **Newzoo**. With a passionate fan base, this billion-dollar company is a top developer, publisher, and marketer of interactive entertainment. Its portfolio of games are both critically acclaimed and commercially successful, played by billions of people around the world.

CHALLENGE(S)

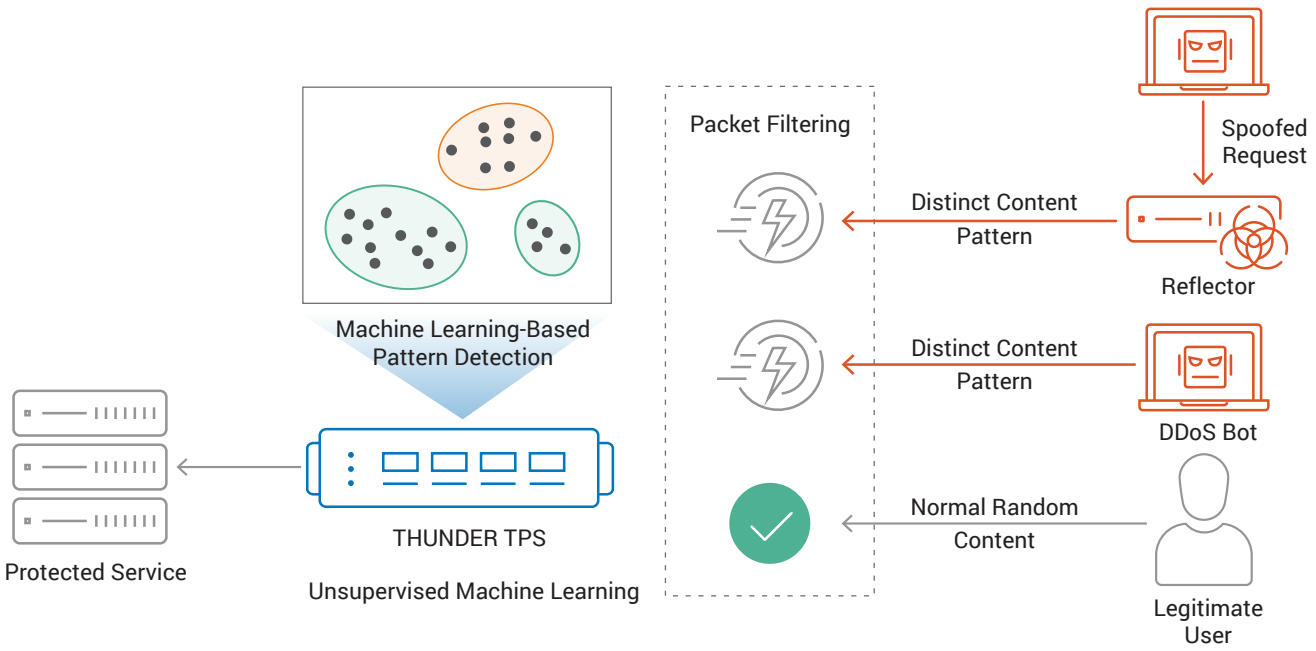
The gaming industry is no stranger to DDoS attacks, as gamers regularly use DDoS to try and to create an unfair advantage. With the rise of professional leagues and college esports programs, the stakes are getting higher. DDoS-for-hire services put digital weapons within the reach of anybody with a few dollars to spend.

This multibillion-dollar company decided to rewrite the rules of the DDoS game.

The company began by adopting a Zero Trust approach to cybersecurity. With the understanding that threats exist on its live gaming infrastructure at all times, the company trusts nothing and no one. Every gamer, every device, and every network flow is authenticated. Only players who have passed stringent checks can access games, and players' behavior is continuously verified. These validation measures are taken in real time and do not impact the gamer experience.

SELECTION CRITERIA

The company wanted to enhance its DDoS detection and mitigation to support its Zero Trust approach. The global gaming company had long relied on a cloud-based DDoS detection and mitigation service, but that approach was increasingly ineffective and expensive. To increase performance and lower cost, it wanted more effective DDoS detection and mitigation at the edge of its network. The network and security team conducted an extensive proof-of-concept test for appliance-based DDoS protection solutions.



SOLUTION

The gaming provider chose A10 Networks' Thunder® Threat Protection System (TPS) to detect attacks across its global network and mitigate DDoS attacks at the edge. Thunder TPS is the industry's highest-performance DDoS protection, providing unrivaled precision, scale, and automation.

Zero-Day Automation Protection (ZAP), an innovative set of intelligent automation capabilities, make Thunder TPS especially fast and effective.

ZAP automatically recognizes the characteristics of DDoS attacks and apply mitigation filters without advanced configuration or an operator's manual intervention. It has two components. Zero-Day Attack Pattern Recognition (ZAPR) provides dynamic attack pattern recognition through a machine learning algorithm and signature-generation blocking.

The company's network and security teams also use A10 Networks aGalaxy® Centralized Management System to centrally manage Thunder TPS appliances and mitigate attacks.

RESULTS

With real-time DDoS detection and mitigation from A10 Networks, the gaming company has maintained service availability without impacting the gaming experience—or the company's reputation and revenue stream.

"We had 1,500 DDoS attacks in the first nine months of 2019, and less than five of those attacks had impact on us," says the security operations center (SOC) manager at the gaming company. "With Thunder TPS, we are seeing 99.999 percent availability, and have had less than five minutes of downtime in more than a year."

Recently, a 163 Gbps DDoS attack was aimed at one of the company's action-adventure games. Once the attack was mitigated, the IT team decided to turn on the brand-new

> *"The global gaming company had long relied on a cloud-based DDoS detection and mitigation service, but that approach was increasingly ineffective and expensive."*

ZAPR capability on Thunder TPS on Friday night. It was just in time, because the company got hit with a 200 Gbps attack a few days later. Thunder TPS with the ZAPR capability automatically neutralized the monster attack with no impact on the gaming experience.

"We have mitigated some pretty large attacks with A10 Networks Thunder TPS, and the response time is usually milliseconds," says the SOC manager. "It's amazing what Thunder TPS with ZAPR can do."

The company has greater visibility into attacks as well as the ability to defeat growing attacks. With Thunder TPS detecting attacks, it can see 25 to 50 more attacks per week than with its legacy cloud-based DDoS protection service.

Automating DDoS detection and mitigation with Thunder TPS enabled the company to significantly reduce security OpEx. Eliminating the recurring costs of the cloud service saved the company hundreds of thousands of dollars a year.

With automation, the security operations team is more productive. A DDoS attack is no longer an adrenaline-pumping, all-hands-on-deck activity. When a DDoS attack comes in, Thunder TPS automatically mitigates the impact and reports its activities to the security operation center.

If security analysts want to investigate further, they can tap into the packets that Thunder TPS captured during the attack. That way, the team can ultimately ensure swift, accurate remediation actions as attacks evolve.

SUCCESS AND NEXT STEPS

With a Zero Trust approach, the global gaming company has been able to rewrite the rules when it comes to cybersecurity. Automated DDoS protection protects the gaming experience and the company's brand reputation.

The best DDoS protection, the company's SOC manager advises, is tailored to an organization's specific network configuration. "A10 does a good job letting you know what's available and what works for your needs. My advice is to work closely with the A10 engineering team. Thunder TPS does a great job for us."

ABOUT THIS GLOBAL GAMING COMPANY

This multi-billion enterprise is a top developer, publisher, and marketer of interactive entertainment. It designs games for console systems, personal computers, and mobile devices.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide. For more information, visit: **www.a10networks.com** and **@A10Networks.**

For more information, visit: **a10networks.com** and **@A10Networks**.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-CS-80202-EN-01 FEB 2020