Swish and Cloudflare provide the Department of Homeland Security with Volumetric DDoS protection while improving customer experience

Introduction

The Department of Homeland Security is the federal executive department responsible for public security as-a-whole. This includes everything from counterterrorism to maritime and border security, to coordinating response to natural disasters, to protecting our country's leaders. With over five hundred public facing sites across the agency, security is always a top priority but when the HTTP/2 Rapid Reset vulnerability was uncovered, a record-breaking attack, DHS, like many other large organizations, started investigating what would protect the agency's IT systems from an attack of this magnitude. Security experts reported that HTTP/2 Rapid Reset peaked at 201 million requests per second, three times bigger than previously recorded attacks.

The Problem

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Needless-to-say, DHS was greatly concerned over the potential impact of such an attack on their mission to protect national security. They needed a more robust security solution that would protect the agency from a volumetric DDoS attack without impacting citizens or their mission.

At the same time this unprecedented attack surfaced, DHS was looking at improving customer experience as mandated in OMB's "Delivering a Digital-First Public Experience," M-23-22. This memorandum requires government agencies to establish a framework for the next decade of digital modernization so that there are common standards for delivering online tools and experiences that meet the expectations of citizens.

201
million

"HTTP/2 Rapid Reset attack peaked at 201 million requests per second, three times bigger than previously recorded attacks."

https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack

The Solution

Swish was brought in based on the depth of their cybersecurity expertise and their customer experience practice. Swish also has many years of working with DHS which was important since they were looking for a solution that would cover their more than five hundred public facing sites. Swish recommended Cloudflare Enterprise with Swish Success Services. Cloudflare offers the world's first connectivity cloud that enables customers to regain control of their technology and security environment by reducing complexity and improving visibility across on-premises, public cloud, Security-as-a-Service (SaaS), and public internet domains. Cloudflare uniquely provides robust network and application security for internet-centric applications while also providing performance enhancing capabilities via their content delivery network and protocol optimization techniques.

The high-performance FedRAMP certified architecture that Cloudflare provides was advantageous in enhancing DHS's customer experience with a 50% improved response rate, while also protecting their applications from volumetric DDoS attacks and other sophisticated application-layer attacks. This combination of performance and security capabilities delivered against multiple high-priority mission outcomes.

Summary

DHS needed the assurance that their large, distributed IT environment was protected against volumetric and other sophisticated attacks from the public internet, like HTTP/2 Rapid Reset, which could significantly impact national security. At the same time, they were working to meet the mandates of M-23-22 with improved user experience for citizens and constituents. Cloudflare and Swish proved to be exactly what they were looking for. Today, DHS has more robust application security with the ability to efficiently manage at scale across many teams using modern Infrastructure-as-Code (IaC) which can be pulled left into DevSecOps activities. Furthermore, they lowered their costs while increasing capabilities and simplifying operations in comparison to previous solutions.

About Swish

Swish is a provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for customers. Since 2006, Swish has delivered high-performance solutions and services to the Federal Government market ensuring that customer's digital service capabilities, performance, and security exceed expectations and requirements. Swish is a Service-Disabled, Veteran-Owned and HUBZone certified Small Business.

To learn more, please visit:
www.swishdata.com

1420 Spring Hill Road Suite 320
McLean, VA 22102

P 703.635.3324 / E info@Swish.com

swish

CS-Cloudflare-0524