Neto leverages Cloudflare to secure and supercharge their ecommerce platform

Neto is a cloud-based, omnichannel ecommerce platform that enables merchants to easily list their products on selling platforms such as Amazon Marketplace, eBay, Catch Marketplace, and their own web stores, and to manage all inventory and orders from a centralised place. Neto's platform is used by thousands of merchants, predominantly in Australia, ranging from single-shop sellers to large multi-warehouse retailers and wholesalers.

Neto's challenge: Build trust with customers by providing a high-performing, highly secure, reliable platform

As one of the largest ecommerce providers in Australia, Neto's platform receives between 85 and 90 million requests per day. "Performance, reliability, and security form the backbone of what we do," says Justin Hennessy, VP of Engineering. "We take security very seriously. Our merchants need a resilient platform that stays available and high-performing even during DDoS attacks, server failures, and other emergencies."

Achieving this high performance is challenging. As a SaaS provider, Neto is a major target for DDoS attacks, malicious bots, and other cyber attacks. In addition, because their solution serves online merchants, many of the requests hitting Neto's platform are bandwidth-heavy image traffic.

What's more, the platform must also be able to seamlessly and rapidly scale during busy seasons such as the winter holidays, when traffic can spike dramatically. "There cannot be a situation where it's Black Friday, and our platform goes down or starts running really slowly," says Hennessy. "That would destroy the trust we've worked so hard to build with our customers."

Achieving security and simplicity with SSL for SaaS, Bot Management, and Cloudflare WAF

Neto initially adopted Cloudflare in order to automate ongoing work that was taking up critical technical resources.

"SSL for SaaS was the primary driver of why we began using Cloudflare," Hennessy explains. "At the time, our merchant onboarding process, which included setting up SSL certificates for new customers, took a couple of days and only specialized personnel could work on it."

Cloudflare SSL for SaaS makes it easy for SaaS providers to enable SSL (TLS) on customers' CNAME vanity domains, removing the burden of SSL

Key Results

- Cloudflare Bot Management and Web Application Firewall (WAF) mitigate 15,000 to 16,000 cyber attacks per day
- Cloudflare SSL for SaaS allowed Neto to transform their previously complex merchant onboarding into an auto mated, one-click process
- Neto has seen a significant band width cost savings from Cloudflare caching; only 50% of traffic now goes to their origin server

> "We turned Bot Management on a couple of weeks ago, and on the first day, we blocked 2.4 million requests, which obviously has a pretty significant cost effect over time...without Bot Management, we would have had quite a big challenge dealing with that attack."

JUSTIN HENNESSY
Vice President of Engineering
Neto

certificate management. The solution transformed Neto's customer onboarding into a completely automated, one-click process that any employee can perform. "The ability to automate processes was the primary pain point that Cloudflare solved for us," Hennessy notes.

Neto has also benefited from the Cloudflare Web Application Firewall (WAF) and Bot Management. "We turned Bot Management on a couple of weeks ago, and on the first day, we blocked 2.4 million requests, which obviously has a pretty significant cost effect over time," Hennessy recalls.

From time to time, Neto experiences automated attacks against its platform. The sophistication of these attacks are increasing and, at times, the usual static methods of blocking the types of threats in question don't work. This is where Bot Management bridges the gap. "With the use of Cloudflare's logs, and assistance from Cloudflare's technical support team, we were able to identify, visualize, and mitigate the issues," Hennessy says. "Without Bot Management, we would have had quite a big challenge dealing with that attack."

Since then, Bot Management and the WAF have allowed Neto to block an average of 15,000 to 16,000 attacks per day.

"Security used to keep me up at night," says Hennessy. "The security of our platform is the key to a successful future, not just for us, but also for our merchants. Cloudflare helps to mitigate a lot of those fears."

Reducing bandwidth and improving performance with Cloudflare Global CDN and serverless computing

Now that Neto uses the Cloudflare global CDN to cache content, only 50% of their traffic goes to their origin servers, significantly reducing their bandwidth expenditures.

Neto also utilizes Cloudflare Workers, which allows developers to build serverless functions that run on Cloudflare's network, closer to their users, to direct web traffic to specific origin servers. They are working on using it to simplify some of the caching elements in their platform so that they can move them to the edge.

"With Cloudflare, especially Workers, Neto has the capabilities that we need to be creative about how we solve problems," Hennessy remarks. "It's also enabling us to simplify the complexity of our platform by pushing a lot of the custom things that we have built on the platform out to the edges, and do it in a very standardized and automated way."

> Cloudflare offers a full gamut of solutions to ensure performance, resiliency, and security without a lot of effort on our part. Thanks to Cloudflare, we can be creative about how we serve our customers and solve problems."
>
> **JUSTIN HENNESSY**
> **Vice President of Engineering**
> **Neto**

For an online copy please visit

https://www.cloudflare.com/case-studies/handelsblatt-media-group-digital-transformation/