In 2016, when Denis Ivanov became the CTO of Shiekh Shoes, he realized the company had a popularity problem. Shiekh’s weekly online releases of hot new sneaker and clothing products drew many thousands of web shoppers seeking access to in-demand gear. The massive spikes in traffic sometimes drove Shiekh's sites offline or slowed response times to a crawl. Customers noticed and complained. Ivanov investigated and quickly realized that the majority of the traffic was coming not from human visitors but from bots. “I learned that there is a huge industry of people selling these automated tools, both individuals and sophisticated organizations,” said Ivanov.

During these product drops, bot operators bombarded the sites with automated attempts to purchase items as quickly as possible. Malicious bot operators would then turn around and resell their purchases in online marketplaces, such as eBay, for significant markup over the list price. “It wasn't organized but it acted just like an organized Distributed Denial of Service attack,” explains Ivanov. The situation got so bad that, when Kanye West released a new Yeezy shoe, the bot traffic not only took down Shiekh sites but also overwhelmed the switches and routers at Shiekh's hosting providers. This firehose of bot traffic forced the hosting provider to discard Shiekh's traffic to protect their data center infrastructure and other customers. Worse still, the attacks would start days before the actual hot product drop and not end for a day or two after, recalls Ivanov, “People had to work weekends to deal with it and just keeping our sites stable took away from other activities as we spent time putting out fires and figuring out how to solve this.”

Another problem Ivanov inherited was a massive account takeover attack on a subsidiary site, Karmaloop. Botnet operators bombarded the login page of Karmaloop with attempts to access customer accounts in order to validate email and password pairs. This happened over a weekend and required very fast action to resolve before the attack would significantly impact Karmaloop account holders by compromising their credit card information and allowing malicious hackers to place fake orders, request fraudulent refunds and returns, or simply sell the validated account information and credit card data on the Dark Web.

Shiekh Shoes sells cutting-edge shoes and sneakers and streetwear to an avid base of young customers. Based in Ontario, California, the company has 79 stores around the United States and a multi-million dollar online platform that comprises nearly 20% of the company's revenues. Shiekh operates multiple online brands including: ShiekhShoes.com, Shiekh.com, Karmaloop.com, TiltedSole.com and FBRKclothing.com.

The global market for streetwear is valued at roughly $300 billion, according to consultancy Bain & Company. The athletic wear market will grow by 7% to 8% in 2018 according to the 2018 McKinsey Business of Fashion “State of Fashion Report.” According to consumer sales tracker NPD Research, the sale of sport leisure sneakers (like those sold by Shiekh) grew by 17% in the U.S. in 2016, outpacing all other parts of the athletic footwear market. This massive market size makes a rich target for fraud attempts.
As soon as it became clear that bots were damaging Shiekh's reputation, forcing customers to seek products from other vendors, and killing performance, Ivanov began to research possible solutions. Shiekh required integration with the company's CDN provider Fastly because Shiekh did not want to make any code or configuration changes on their origin web servers. “A requirement that any solution that needed to sit on the origin servers was a deal breaker,” says Ivanov. By the same token, Ivanov wanted a SaaS solution rather than on-premises because this would not require maintenance on his end and would be easier to manage and scale depending on Shiekh's future growth.

PerimeterX easily met all of our requirements. We were impressed with the simplicity of the installation and the dynamic coverage for the latest generation of bot attacks.

Ivanov and his team determined that the PerimeterX Bot Defender product met all their requirements and were impressed with the simplicity of installation and the dynamic coverage of even the latest types of bot attacks. Whether it was a well-known sneaker bot or something completely new to the market, PerimeterX could stop the attack. On top of that, unlike other products, PerimeterX could accurately predict whether a visitor was a bot before Fastly served a webpage, potentially saving infrastructure costs.

“We needed a solution that could integrate on the edge, into our existing infrastructure without requiring the addition of a device or code on the origin servers.”

Ivanov

“The product performed exactly as we expected, accurately screening bots without impacting real users.”

Ivanov
Two days before a major Thanksgiving Sale Shiekh decided to implement PerimeterX Bot Defender to stop bot attacks quickly to avoid site outages during the largest online shopping weekend of the year. Within 24 hours Shiekh worked with the PerimeterX technical team to integrate PerimeterX Bot Defender into Shiekh’s Fastly CDN configuration files. Filtering bots from Shiekh’s sites also made real customers happy because it allowed them a much better chance of purchasing in-demand products. “It only required a few changes on our end and very little time spent by my team. We saw immediate results,” says Ivanov. PerimeterX was blocking over 99% of bot visitors within 24-hours of deployment. This allowed Ivanov and his team to stop worrying about unplanned outages and instead to provision additional web and network capacity for events to serve actual human shoppers. By predicting which visitors were bots and ignoring their page requests, PerimeterX saved considerable hosting and bandwidth costs.

“PerimeterX stood up the solution—shutting down ATO attacks—in less than 48 hours.”

Ivanov

To stop the account takeover attacks on Karmaloop, Shiekh also turned to PerimeterX for a rapid deployment. PerimeterX stood up ATO protection in less than 48 hours, effectively shutting down the attack and sending the malicious hackers away.

Best of all, PerimeterX has stopped bot-driven weekend fire drills cold, allowing Ivanov’s team to concentrate on infrastructure improvements and other core initiatives to drive growth rather than fight malicious bots.

“We were very impressed with how responsive the PerimeterX and Fastly teams were to get us this protection so quickly and solve our pain before any real damage was done,” says Ivanov. “Since then, the product has performed exactly as we expected, accurately screening bots but not impacting real users. We don’t worry about bots on the weekends anymore.”
ABOUT PERIMETERX

PerimeterX protects the world's largest and most reputable websites and mobile applications from malicious activities, future-proofing your digital business from automated bot attacks through predictive security intelligence with reinforcement learning techniques. PerimeterX Bot Defender, bot protection-as-a-service, safeguards web, mobile and APIs from account takeover attacks, scraping, checkout abuse, carding attacks and marketing fraud through a scalable, out-of-band solution easily integrated into your existing infrastructure. Our solution expands behavior-based detection by learning, in real-time, what a behavior looks like and incorporates this into predictive security intelligence, protecting websites from the latest generation of automatic attacks.

Named as one of Gartner's Cool Vendor in Unified Retail Commerce for 2017 and a leader in AI-based security products, PerimeterX is trusted by premium brands in the Internet Retailer Top 200 selling apparel, footwear, home improvement, sporting goods, athleisure, and other goods. PerimeterX Bot Defender is fully integrated into the Fastly stack through a VCL module, eliminating modifications on the customer's application, origin server or infrastructure creating a powerful predictive-based bot detection and mitigation solution. By extending the abuse policy to the edge, this significantly reduces malicious origin traffic, saving on backend server resources and reducing fraud.

REQUEST A DEMO

www.perimeterx.com/request-demo/