



CUSTOMER SUCCESS STORY

## **Scoot Airlines Safeguards Passenger-facing Systems**



# **Scoot Airlines increases site speed by 80%, reduces look-to-book ratios, and safeguards passenger-facing systems with Imperva Bot Management (formerly Imperva Networks)**

## **Overview**

Scoot is the low-cost arm of the Singapore Airlines Group and has carried over fifty million guests to 63 destinations across 17 countries. Scoot was voted 2015, 2016 and 2017 Best Low Cost Airline (Asia/Pacific) by AirlineRatings.com and ranked in the Top 10 of the World's Best Low-Cost Airlines in 2015 by Skytrax.

## **Challenges**

### **Bad bots abusing Scoot's booking engine**

Like most airlines, Scoot's booking engine was being inundated by bad bots. Scoot has a partner API, but unauthorized OTAs, competitors, and meta search sites were using sophisticated web scraping bots to abuse the business logic of Scoot's booking engine. For example, an unauthorized OTA would query Scoot's booking engine looking for any ticket they could sell, skewing look-to-book ratio, and causing site slowdowns.

### **Bot traffic caused site slowdowns, customer complaints, and lost revenue**

According to Jason Chin, Scoot's VP IT, bot traffic was depriving legitimate customers of the opportunity to book air travel on Scoot's website.

"Bots were affecting our ability to fulfill our bottom line revenue," says Chin. "On average, we had a per transaction response time of about 10 seconds. But when bots flooded our booking site, it shot up to about a minute—sometimes even hanging. Bots were degrading our site performance by more than 50–80%, and it was happening once or twice a week. It became a big deal. We were fielding numerous complaints from customers unable to book, so they were going to our competitors."

**30%**

**More bad bots stopped**

**80%**

**Faster response times**

**Reduction**

**In the number of screen scrapers**

## Bot operators accessed Scoot's API servers through unwitting partners

Scoot was also fielding a lot of traffic because of novice software development practices at its travel partners. Having an authorized API key gave these partners booking engine access and—through them—bots triggered a huge number of calls. Every partner coming to book gets an ID and password. “We’d look at the high CPU usage of an incoming agent, then have to kill their session so the CPU would normalize to an acceptable level. We’d call that agent to let them know they were being hit by bots. If they didn’t take corrective action, we kept their session suspended.”

## Degradation of end-to-end customer experience including flight check-in and departure times

“Scoot uses Navitaire’s hosted passenger service system. It’s an end-to-end passenger experience that starts with buying a ticket to getting a seat change, a boarding pass—all the way to tracking who’s sitting in each seat on the actual flight. Bad bot traffic also caused slowdowns across passenger-facing systems including flight check-ins which can trigger delays in departure times. “Clearly, the illicit bot activity was hurting Scoot’s image,” says Chin.

## Bad bot incidents impacted staff resources across multiple departments

When each incident occurred, Chin had one to two staffers putting in extra hours to resolve the problem—not including what Navitaire was doing, which accounted for yet more personnel. Customer service was handling all the complaints coming into Scoot’s call center, amounting to more additional staff costs.

“Navitaire could have charged us for additional looks that would never convert to actual bookings, but they didn’t as they saw we were taking active steps to try and stop the bots, including using Navitaire’s Scraper Shaper solution,” says Chin. “We’d manually load IPs into Scraper Shaper for blocking, but today’s bots are intelligent and simply rotate through IPs or come in through proxy networks, proving this type of manual IP blocking ineffective.”

**We’d look at the high CPU usage of an incoming agent, then have to kill their session so the CPU would normalize to an acceptable level. We’d call that agent to let them know they were being hit by bots. If they didn’t take corrective action, we kept their session suspended.”**

Jason Chin, VP IT

## The Result

**Imperva wins the bake off by having the most experienced analyst team, and by catching 30% more bad bots than competing solutions**

Chin sought a different solution. “We became very familiar with solutions like Akamai Bot Manager. But it doesn’t proactively stop bots—it’s reactive. Despite lots of customizations in Akamai we were still losing the battle. It’s too resource intensive and the turnaround time isn’t quick enough. Further, Akamai doesn’t offer expert analysts to examine patterns and advise us as to which are good bots versus bad.

“We compared solutions on separate websites. Imperva blocked a far greater percentage of bad bots—more than 30%—than the other solutions we tried.”

### Fast, custom deployment on AWS in less than two weeks

Deploying Imperva took less than two weeks to set up—including matching it to the company’s AWS footprint. “Our implementation was very straightforward,” Chin says. “Once we had Imperva installed and fine-tuned, our experience has been great.”

### Reduction in look-to-book ratio and team resources

“The results we’ve obtained are really worth the investment. We’ve realized a substantial reduction in the number of bad bots and screen scrapers. Imperva helps us reduce the number of looks from other websites—especially from China and India, which contribute nothing to our bottom line,” says Chin.

“Imperva’s machine learning capabilities fight the bots in a way that my team could ever keep up with. Imperva’s machine learning continues to impress me. We can even adjust the machine learning setting up or down and see the potential impact on our traffic.

“We’ve greatly reduced our time spent monitoring and managing unwanted IPs, which has increased revenue from our website in a more cost-effective way.”

**“We compared solutions on separate websites. Imperva blocked a far greater percentage of bad bots—more than 30%—than the other solutions we tried.”**

Jason Chin, VP IT

## 80% faster response times and fewer customer complaints

“Scoot has more bookings coming in and we deal with far fewer passenger complaints. And site visitors experience an 80% faster response time,” says Chin.

## Protecting the APIs that power Scoot’s website and mobile app

“The next phase is to work with Imperva to block bots from scraping our partners’ sites via our API, and block bots using our mobile app emulating mobile devices,” says Chin.

## Preventing account takeover and safeguarding Scoot’s frequent flyer program

“As we introduce our frequent flyer loyalty program, we’ll be using Imperva to take precautions against bad actors trying to hack our login page.” Chin cites the ability to enforce more aggressive settings, such as a user’s browser having to prove its legitimacy, or a CAPTCHA being displayed after a given period of inactivity.

## Vigilant and dedicated support—plus analyst oversight

Chin recognized that his company’s core business isn’t analyzing and tracking bots, so he sought a managed service to help. “We use Imperva’s analyst managed service; they really know their job. We put in place whatever they suggest; this helps us continually improve. We have regular meetings with Imperva analysts—everyone works together.

“Support is both very professional and proactive. After being with Imperva a year now, it continues to meet our every expectation. I plan to renew our contract.”

**“Support is both very professional and proactive. After being with Imperva a year now, it continues to meet our every expectation. I plan to renew our contract.”**

Jason Chin, VP IT