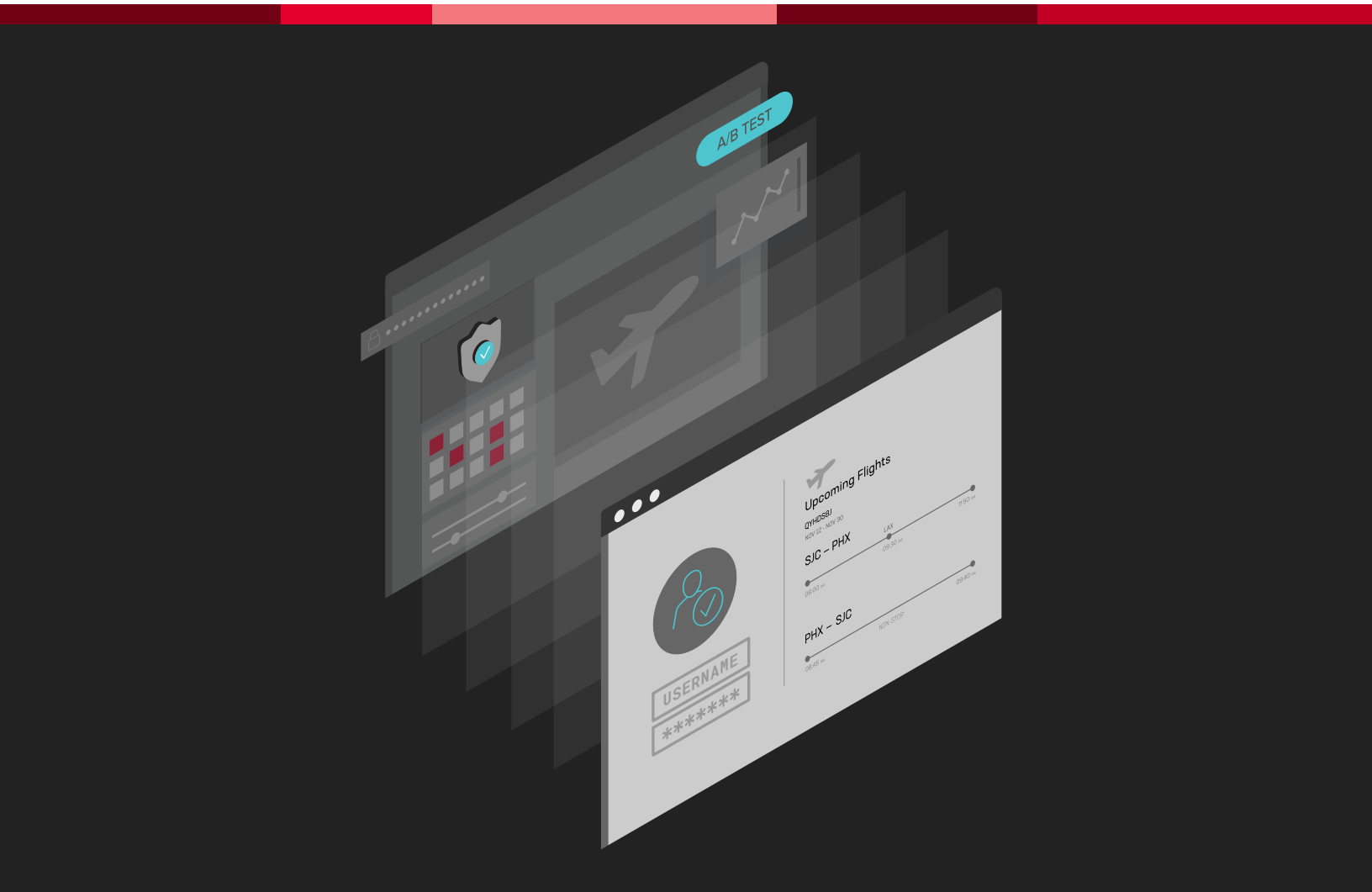
CASE STUDY

Global Top 10 Airline Grows Revenue

By Saving Legitimate Users from Login Distress



HOW ONE OF THE WORLD'S LARGEST AIRLINES IS BENEFITING FROM F5 DISTRIBUTED CLOUD AUTHENTICATION INTELLIGENCE

Safely extending session lengths is driving:

1. Material conversion improvements, supporting sales growth in the tens of millions of dollar
2. Margin improvements by better converting traffic that had already been successfully driven to the website
3. Reduced login friction for millions of users each year

The Customer: One of the Top 10 Airlines in the World. One of the world's leading airlines–ranked among the top ten largest in the world, and with annual sales in excess of $20 billion–was looking for ways to increase online revenue and improve online customer experience in the hyper competitive, travel industry.

The Opportunity: Rescuing Real Users Lost Due to Login Friction

Capturing the attention of consumers and leading them to your website is an expensive proposition for an online business. Once on your site, even seemingly small improvements in the conversion from shoppers to buyers can yield significant revenue and margin improvements.

Short web sessions = login friction for legitimate users. Like many e-commerce platforms, this airline's website automatically logged users out of sessions after 30 minutes of inactivity. Short web sessions are viewed across much of the application security world as a standard security practice, with the intention of preventing fraud that might occur when different consumers use the same PC, logged into the same merchant session.

Unfortunately, short web login sessions can negatively impact revenue and usability for most brands. Here's why; for an average website, among 100 returning, previously logged in users:

- 70% will be able to log in successfully on their first attempt
- 20% will struggle to log in but will eventually get in through multiple attempts or even the friction of a password reset
- 10% will never succeed and will abandon the attempt to log in

Some of the frustrated users who abandon login are known good users, and many of them end up purchasing from other brands whose sites impose less friction.

Safely increasing session length without increasing fraud. F5 proposed to this airline that they could safely increase session length, thereby measurably increasing online sales, without increasing fraud. F5® Distributed Cloud Authentication Intelligence leverages the power of artificial intelligence and F5's network insights to safely and accurately identify legitimate, returning users, so that applications can offer them improved, streamlined experiences that eliminate friction and drive improvements in conversion–and revenue. With Distributed Cloud Authentication Intelligence, F5 offered this airline the ability to have persistent login sessions for legitimate returning users, similar to Amazon, Gmail, and PayPal. This resulted in increased revenue, without an increase in fraud.

The Investigation

During a proof of concept phase, F5 partnered with this leading airline to deploy A/B testing, comparing groups that received extended sessions to control groups using the original default 30-minute web session. Visitors to the airline's website were randomly assigned to the control and test groups based on a mutually agreed upon sample.

The A/B testing was designed to compare fraud indicators and conversion metrics, in order to measure impacts on conversion and revenue as well as potential online fraud.

The A/B testing set out to answer two major questions:

1. Does extending web login session length increase fraud losses? This was measured by looking at three different customer-specific online fraud indicators.
2. Does lengthening web login session length increase business value (in this case, airline ticket sales) and usability for those travelers who were previously experiencing login friction? This was measured by looking at converting lift and reduction in overall user login friction. Conversion lift was measured in the customer's web analytics environment.

WHY F5 DISTRIBUTED CLOUD SERVICES?

F5 is a trusted leader in providing application security. The same AI-powered precision F5 Distributed Cloud Services offer to accurately detect attack traffic in real-time to secure applications can now be offered to safely identify known legitimate users in real-time to improve user experience and increase revenue.

The Solution

After completing the A/B testing, the data pointed to the following conclusions:

Extending session length leveraging Distributed Cloud Authentication Intelligence safely produced a meaningful improvement in business value. For this airline, web application session length extensions produced a measurable improvement in business results. Specifically, the seven-day session extension test produced a 1.3% absolute lift in ticket sales for the test group versus the control group. For any online business of this size, when these impacts are extrapolated across all eligible users over the course of a full year, the positive business impact of session extensions should drive positive sales lift valued in the tens of millions of dollars per year, when controlling for other factors. In addition, the seven-day session extension test group at this airline also saw a 1% increase in additional searches for tickets.

Extending session length using Distributed Cloud Authentication Intelligence did not increase online fraud. At the same time, the airline's key fraud indicators showed no statistically significant increase as session lengths were extended. Distributed Cloud Authentication Intelligence eliminates risks for fraud increases by extending sessions only for known legitimate returning users. Other categories of users are still subject to the original 30-minute session length.

Extending session length using Distributed Cloud Authentication Intelligence significantly reduced login-in related user friction. F5 and the airline's marketing team examined the impacts on login friction in two different ways:

1. How many users continued to experience login failure
2. How many experienced the need to manually re-login

With sessions extended to seven days for known legitimate users, there was just over a 40% reduction in the number of users who had login failure. For this airline–indeed, any online business of this size–that represents literally millions of eliminated login failures per year. In addition, there was a 15% reduction in the number of users who had to attempt manual logins repeatedly. Automatically rescuing legitimate users who would otherwise potentially experience login friction or failure also produces a number of benefits that were not measured in the proof of concept (POC), including reductions in call center traffic, improved customer satisfaction, and improved customer loyalty.

With these POC results, this airline quickly moved from POC into production, and is now enjoying the benefits of improved conversions and reduced user friction without any associated increase in fraud losses.

Safely Reducing Login Friction without Increasing Fraud Risk

F5 Distributed Cloud Authentication Intelligence rescues known good consumers from the frustration of excessive logins and reauthentication, helping brands safely grow top line revenue. Distributed Cloud Authentication Intelligence achieves this by accurately identifying, in real-time, returning consumers and other legitimate consumers through the power of deep analytics and the broader reach of the F5 network. With this insight, web application owners can dramatically reduce or eliminate login friction, capturing increased revenue while delivering frictionless experiences for legitimate customers.

Future Plans

Based on the successful results from the initial session extension A/B testing, this airline plans to work towards 90-day session extensions for greater portions of their web application user population.

To learn more, contact your F5 representative, or visit f5.com.