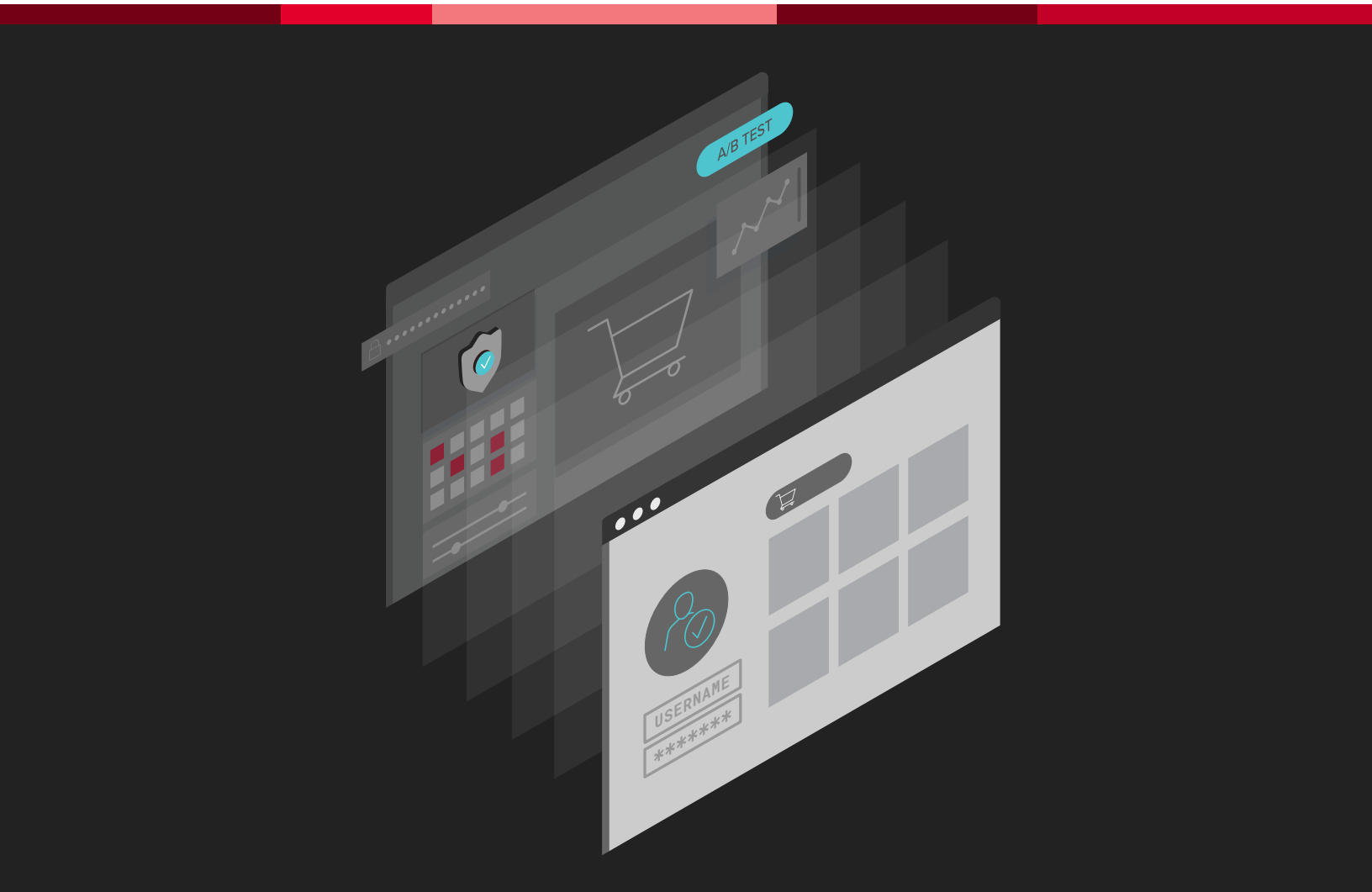
CASE STUDY

Global Multinational Retailer Grows Revenue

By Saving Legitimate Users from Login Distress



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

Safely and silently re-authenticating known legitimate users is driving:

1. Material conversion improvements, supporting sales growth in the tens of millions of dollars per year
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 world's top online beauty retailers—with annual sales in excess of $10 billion–was looking for ways to increase online revenue and improve online customer experience in the hyper competitive beauty industry.

The Opportunity: Rescuing Real Users Lost Due to Log-in Friction

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

Forgotten passwords = login friction for legitimate users. Like many e-commerce platforms, this beauty retailer'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 computer logged into the same merchant session.

Unfortunately, short web sessions can negatively impact revenue and usability for most brands. Here's why: For an average website, among 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 recognizing known good users without increasing fraud. F5 proposed to this beauty retailer that they could safely and silently re-authenticate known good users, 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 beauty retailer 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 beauty retailer 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 retailer'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, online sales of beauty products) and usability for those consumers who were previously experiencing login friction? This was measured by looking at conversion lift and the 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:

Recognizing known good users by leveraging Distributed Cloud Authentication Intelligence safely produced a meaningful improvement in business value. For this beauty retailer, safely and silently re-authenticating known good users produced a measurable improvement in business results. Specifically, the retailer noticed 13,000 fewer manual logins and an increase of 373 additional purchases per day on average. When this capability is extended to all of the retailer's online customers, it is expected to result in 750 additional purchases per day on average. This is expected to increase top-line revenue by approximately $20 million per year.

Recognizing known good users via Distributed Cloud Authentication Intelligence did not increase online fraud. The retailer's key fraud indicators showed no statistically significant increase in fraud when login friction was reduced. F5 Distributed Cloud Authentication Intelligence eliminates the risk of fraud increase by safely and silently re-authenticating only known legitimate returning users. Other categories of users are still subject to the original 30-minute session length.

Recognizing known good users via Distributed Cloud Authentication Intelligence significantly reduced login related user friction. F5 and the retailer'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

By safely and silently re-authenticating known legitimate users, there was approximately a 76% reduction in the number of users who experienced login failure. For this retailer, and in fact, any online business of this size, that represents literally millions of eliminated login failures per year. This, in turn, resulted in a 6.1% increase in conversions—a significant percentage that brings significant additional revenue along with it. Automatically re-authenticating legitimate users who would otherwise experience potential login friction or login failure also produces a number of additional 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 beauty retailer 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 Log-in 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.

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