FingerprintJS Case Study

How a SaaS Edtech Company Solved Account Sharing

Using **FingerprintJS browser fingerprinting**, a SaaS educational technology company **significantly reduced unauthorized account sharing**, increasing their annual recurring revenue by **$4M+ ARR** while keeping legitimate users happy.

Results

New revenue from sign-ups

The SaaS company was able to grow annual recurring revenue by more than four million USD from spun off accounts within several months of implementing FingerprintJS Pro.

Customers stay satisfied

The company maintained the same level of cancellations and customer support calls after implementation, clearly showing that there were no significant drawbacks for legitimate customers or the business.

Customer satisfaction (CSAT) surveys also remained stable, indicating that additional authentication measures did not have a negative impact on the user experience.

Feedback loop with FingerprintJS

The company continues to work closely with the FingerprintJS technical team to adjust algorithms as user behavior changes over time, maintaining high accuracy and a positive student experience.

Customer Overview

FingerprintJS began working with an education technology company that provides a suite of online services. Their customers are millions of high school and college students in 100+ countries around the world.

Sector:	Education
Use Case:	Account Sharing
Employees:	1,000+

FingerprintJS Features

- ☑ 99.5% Accurate Identification
- ☑ Browser Fingerprinting
- ☑ GDPR and CCPA Compliant
- ☑ Incognito Mode Detection
- ☑ Geolocation

FingerprintJS

The Problem

Account sharing a top business priority

From analyzing login attempts across devices and IP addresses, the company realized that many students were sharing their account credentials with friends and classmates and even selling accounts online. Account sharing prevention became a top priority in 2020 to stop this fraudulent behavior and recoup lost revenue from shared accounts.

Technical challenges to accurate detection

The company found that detecting account sharing was a significant technical challenge that would require a more accurate identifier than using cookies or IP addresses alone.

Students using the platform often had:

- **Shared IP addresses**
  (on university campuses or residences)
- **Multiple devices to access accounts**
  (phone, tablet, laptop, and library computers)
- **VPNs, Adblockers, or clearing cookies**

The customer began building software in-house to prevent account sharing, but it was not accurate enough to catch many shared accounts and risked disturbing too many legitimate users.

The company did not want to build the in-house expertise needed to generate identifiers with sufficiently high accuracy, and instead wanted a provider like FingerprintJS that specialized in visitor identification.

Why FingerprintJS

From their investigation, the company found that the FingerprintJS Pro API provided the most accurate solution out of all the alternatives they considered for account sharing prevention.

Higher accuracy vs. cookies, IP addresses, and other device identification services

FingerprintJS Pro is the most accurate browser fingerprinting service available today, with up to 99.5% visitor identification accuracy. Instead of relying solely on cookies or IP addresses to flag users that are sharing an account, FingerprintJS combines an array of 100+ unique signals that can identify users even when VPNs, incognito browsing or other spoofing techniques are used.

The company also compared FingerprintJS Pro to a competing device identification service and found that the FingerprintJS Pro API caught many additional account sharing instances with a much lower rate of false positives.

Future-proofed account sharing prevention

To ensure that their solution was effective for years to come, the company found it valuable to partner with a team committed to cutting edge identification. As users change their behaviors, browsers change their privacy settings, the FingerprintJS Pro API is regularly updated to provide consistently high accuracy.

GDPR and CCPA compliant

Due to the company's philosophy of putting its customers first, it was essential to maintain users' rights to online privacy. FingerprintJS Pro is compliant with GDPR and CCPA for fraud detection. All customers of FingerprintJS can choose between US and EU hosted data centers to comply with their specific data localization and residency requirements.

Get in Touch

Learn how FingerprintJS Pro can help your business build a custom solution to prevent account sharing.

Contact Sales

sales@fingerprintjs.com

Get Started Today

Create Free Account

FingerprintJS