Case Study

How One Company Solved Account Sharing with FingerprintJS Pro

Using FingerprintJS' browser fingerprinting service, one customer was able to significantly reduce account sharing, resulting in an immediate increase in new sign-ups while keeping their legitimate users happy.

Results

New revenue from sign-ups

The company noticed increased revenue within weeks of implementing FingerprintJS Pro from new sign-ups spun off from shared accounts.

No impact to customer success

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

Customer satisfaction (CSAT) surveys also remained stable, indicating that additional authentication measures were not negatively impacting the user experience.

Feedback loop with FingerprintJS

The company continues to work closely with the FingerprintJS technical team to adjust algorithms to changes in user behavior to maintain high accuracy and a positive student experience.

Customer Overview

FingerprintJS works with an education technology company that provides a suite of online services. The company's 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

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 accurately 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 customerstarted building software to prevent account sharing, but it was not accurate enough to catch many of their shared accounts and risked disturbing too many legitimate users.

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

Why FingerprintJS

From the company's investigation, they found that FingerprintJS Pro provided the best 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, with up to 99.5% identification accuracy. Instead of relying solely on cookies or IP addresses to flag instances of account sharing, FingerprintJS combines an array of 100+ 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 and other signals change, the FingerprintJS Pro API is regularly updated to provide consistently high identification accuracy.

GDPR and CCPA compliant

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

Get in Touch

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

Contact Sales

sales@fingerprintjs.com

Get Started Today

Start 10-Day Trial

FingerprintJS