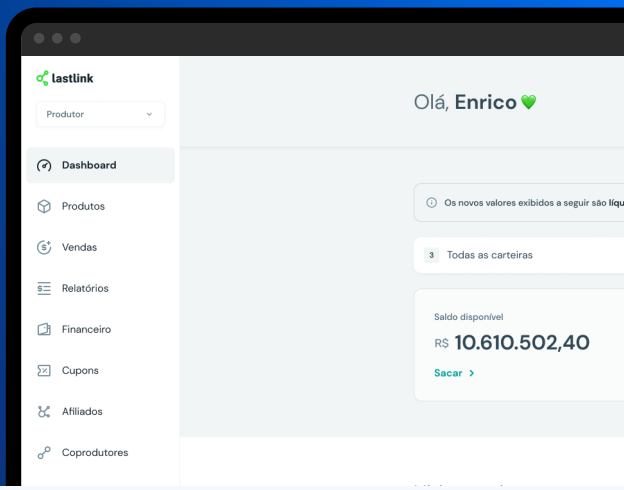
SHIELD | lastlink

Case Study

Lastlink Strengthens Trust and Cuts Fraud Costs with SHIELD's Device Intelligence



"Our partnership with SHIELD is essential to strengthening the trust in our platform. With SHIELD's technology, we're able to block high-risk devices in real time, significantly reducing fake transactions and associated costs. As we continue to grow and support digital creators, this proactive approach to fraud prevention is key to delivering a reliable experience for our users."

Michel Ank
CEO, Lastlink

Key Takeaways

Over 600K transactions protected by SHIELD every month

Decrease operational costs of manual reviews and validation

Trustworthy platform for the long-term growth of info producers

Lastlink's Commitment to a Fraud-Free Ecosystem for Infoproducers

With a user base of over 3 million paying customers and approximately R$400 million in transactions processed in 2024, Lastlink is experiencing rapid growth in Brazil. But with that growth comes an increase in payment fraud challenges.

To stay ahead, Lastlink set out to find an effective solution to proactively detect and prevent fraud—ensuring a safe and trusted environment for both creators and consumers.

Customer Profile
Founded in 2020, Lastlink is an all-in-one platform that empowers digital creators to sell and manage their products—such as live classes, mentorships, courses, workshops, and e-books. In addition to hosting and selling content, the platform also enables monetization through social media, giving creators more autonomy and scalability in growing their business.

Industry
Technology and Digital Economy

Region
LATAM

The Challenge of Tackling Payment Fraud Amid Rapid Growth

Fraudsters exploit platforms like Lastlink by using various techniques and tools to commit payment fraud. Common tactics include using **fake accounts, stolen credit card details**, and malicious tools to conceal their activities.

For example, fraudsters use proxy servers to mask the origin of payments, enabling them to obscure their actual location and making it harder to trace activity across the platform. Fraudsters often use bots to automate transactions at an extremely fast pace, accelerating the checkout process and exploiting system weaknesses. By bypassing payment security measures or using stolen payment details, these bots enable fraudulent transactions to be completed before they are detected.

In addition to these tactics, fraudsters also frequently use multiple email addresses to create numerous fake accounts. If one account gets flagged, they can quickly generate new ones using disposable email addresses. Anti-fingerprinting tools are another method employed to evade detection, as they prevent platforms from identifying the device being used for the transaction, thus making it even harder to flag suspicious activities.

These examples demonstrate how fraudsters employ sophisticated methods to exploit platforms, highlighting the critical need for proactive fraud detection and prevention strategies.

How Lastlink Stopped Fake Transactions and Strengthened Trust with SHIELD

To strengthen its security, Lastlink implemented SHIELD's Device Intelligence to detect and block fraudulent activity before it happens.

The team leveraged the **SHIELD Device ID**, the global standard for device identification, to stop fraud at its root. This technology makes it possible to identify when the same device attempts multiple purchases in a short period or controls several fake accounts—revealing coordinated fraud attempts.

On top of that, SHIELD's **Fraud Intelligence** feature flags when otherwise trustworthy users begin to exhibit suspicious behavior. The technology continuously profiles device sessions and detects the use of tools like anti-fingerprint software, proxies, and other methods commonly linked to payment fraud.

This proactive approach has enabled Lastlink to drastically reduce fraudulent transactions, lower operational costs, and maintain a seamless and secure experience for legitimate users.

With this strategic partnership, Lastlink reaffirms its commitment to security and transparency—creating a trusted ecosystem where digital creators can scale their businesses without worrying about fraud.