# //AXUR

# Stori strengthens digital security and protects over 1 million applicants with Axur

## stori

Stori is a Mexican unicorn expanding access to credit cards. With more than 1 million applicants, the company stands out in Mexico and operates offices in Mexico, the United States, and China.

## ⊚ Problem

With over 55,000 online mentions of Stori, the company faced a fertile environment for the spread of threats and reputational attacks. Manually reviewing these mentions became a monumental—and often impractical—task for a human team. Stori was in a constant effort to safeguard its brand and protect customers from digital threats that could compromise financial security and reputation. Growing activity across the Deep & Dark Web posed an even more critical risk, where stolen information such as customer credentials could be sold on the black market.

## ᄋ Solution

Axur's platform provided Stori with expanded visibility and proactive cyber defense capabilities. Axur supported the company by managing external threats such as phishing, data leaks, and other incidents—ensuring protection even beyond traditional perimeter boundaries. With Axur's advanced capabilities, Stori experienced a major transformation in detecting and mitigating digital threats.
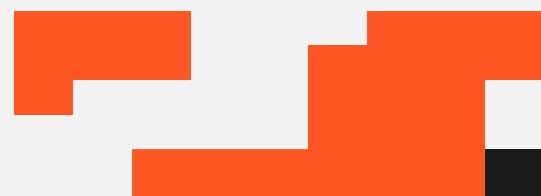
## Impact at a glance

⚠️ **566 threats identified and neutralized**

🌐 **55,000+ brand mentions monitored across the internet**

🕐 **Most threats resolved in under 24 hours**

📅 **100% of threats mitigated within 10 days**

🛡️ **1M+ applicants protected**

👁️ **24/7 monitoring across Surface, Deep & Dark Web**

> "We know that as the company grows, threats will grow as well. Greater exposure helps us scale, but it also puts us in the sights of more attackers."
>
> 💬
>
> **Cybersecurity Team**
> Stori

### Detecting fraud across multiple layers of the web

Axur helped Stori identify and neutralize digital fraud impacting its reputation across both the Deep & Dark Web and the Surface Web. Most threats were resolved in under 24 hours and fully mitigated within 10 days. As the company continued to grow, managing these threats became essential to maintaining customer trust.

### Deep & Dark Web threats

Deep & Dark Web activity represented an increasing risk, with customer credentials and personal data being sold on underground marketplaces. Information such as card data, emails, and passwords could be leveraged for identity theft and financial fraud. Threat actors relied on techniques such as phishing, malware, and credential stuffing.

> "Phishing was one of the threats that raised the most concern for our team. Customer information is extremely important, and we are always committed to protecting it."
>
> **Cybersecurity Team**
> Stori

### Phishing and Surface Web threats

Phishing was one of the team's top concerns, as it directly put customer data at risk. On the Surface Web, attackers used social engineering, fake social media profiles, and fraudulent applications to deceive users, steal information, or deploy malware.

### Greater control and expanded visibility

Axur gave Stori greater control and visibility into external threats targeting its brand and users. By monitoring over 55,000 online mentions, the platform enabled efficient threat management and ensured the company could scale with its digital presence protected.

### Strategic partnership strengthens the customer experience

Close collaboration with Axur's Customer Success and Support teams made a significant difference in Stori's experience. Personalized attention, fast response times, and professional engagement strengthened the relationship between both companies. In a world where trust and security are fundamental to financial growth, the partnership between Stori and Axur stands out as a model to follow. Stori proved that through technology and strategic collaboration, it is possible to strengthen cybersecurity and safeguard online reputation.

## Discover how to elevate the digital financial experience with security

BOOK A DEMO

Gartner
Peer Insights™

👍 4.9
★★★★★

Discover all our solutions: **axur.com**

///AXUR