AXA VENTURE PARTNERS

Insights

Meet the founder
Sandra Tobler from Futurae

14 February 2023

New York - London - Paris

www.axavp.com

Futurae provides an authentication and transaction platform that combines security and usability. Co-founder Sandra Tobler, shares with us during this interview her journey in cybersecurity, the importance of creating a seamless digital experience to all users profiles, how they constantly follow the way attacks evolve so they can better protect their customers and how Futurae is building systems for the future. Certainly a story that you can't miss.

Sandra Tobler,
Co-founder of Futurae

What initially led you to embark on the world of cybersecurity?

I met my co-founders Claudio and Nikos when they finished their Ph.D. at ETH Zurich as part of the System Security Group. We all shared the common belief that online security needed to be improved for digital products. More and more people use banking, health, or citizen services across different devices and channels online. **The digital journey should be seamless, taking into account that not all people are tech savvy and focusing on including users with different needs,** such as visually impaired people. In our view, robust customer security is a very strategic topic touching on increasing the successful onboarding of new customers to new products, customer satisfaction, operational efficiency, or IT risk that must be taken care of holistically by business owners.

What is Futurae's unique value proposition?

Our cloud-native platform allows us to create unique insights that we gain by analyzing authentications across industries and platforms through cross-correlations. **We can inform customers preemptively of fraud that we expect to happen.** Historically authentication occurred in a very siloed way. We are unique in how we bring out innovation to address new types of fraud by closely aligning with our customers. We did address, for instance, in light speed a module to handle social engineering protection or also have modules to address phishing fraud. Also, the adaptive authentication solution is a unique way to use privacy-preserving contextual data for seamless user experience and to solve typical industry life cycle problems! The Futurae platform offers a lot of flexibility with many authentication methods, and lifecycle configuration options empowering companies with the proper login method and process flow for every customer group.

The Futurae platform allows customers from different industries to benefit from best-of-breed know-how and data from across countries and diverse customer groups. Through that flexibility, Futurae helped customers to reduce support/helpdesk costs from 50 to 90% yearly compared to legacy solutions!

How would you say you built trust when Futurae first started? Not an easy industry, as there is a lot of skepticism.

We were privileged to win important customers in financial services at an early stage, which certainly helped us to gain trust in financial services and other industries. Also, being associated with one of the world's most renowned Computer Science departments, the ETH Zurich system security group allowed us to benefit from credibility through academic vesting. **We always served highly regulated industries because that's where the awareness for our topic is highest.**

How do you keep up to date Futurae's technology with all the cybersecurity attacks we hear nowadays.

We are constantly following how attacks evolve and how operating systems change to support customers addressing those changing environments. A fast go-to market is tremendously important for highly regulated industries we support to serve a large diversity of customers seamlessly and protect them from new types of fraud. For example, when new social engineering attacks emerge, we analyze if we can help address those through technology or fraud alerting modules. We have close ties to some of the best information security research from ETH Zurich. **We constantly put innovation into how authentication can look in the future, what new user interfaces need securing, and how to make digital services more inclusive.** Authentication is a small part of the security infrastructure but is highly exposed to criminals. It's also the first digital touchpoint we have with online services and something we feel every day if it's not done well.

What will you say will be the upcoming trends for customer authentication? What do you foresee as upcoming services?

We strongly believe information security is by nature a non one-size-fit-all market. Depending on the industry, we address other fraud types, and different usability requirements are predominant. Passwordless authentication has yet to mature in deployments in reality, but an exciting trend we are supporting. Analysts predict that by 2025 more than 20% of customer authentication transactions will become passwordless, which is a 10% increase compared to today.

Historically, security and usability have always conflicted, as certain security processes cannot be automated - at least until today. New types of risk-based authentication use algorithms that learn the user context over time to build an accurate profile of a given user's login patterns. The algorithms help differentiate devices, typical user login times, or common work locations, detect anomalies, and more.

We are going one step further, doing this in a privacy-preserving way. We are uniquely positioned in the area of signal-based context authentication we call adaptive authentication. Adaptive authentication allows non-invasive access through the support of signals and contextual data, at no point identifying the signal and the person using the system to preserve privacy.

Systems solely relying on biometric authentication have an expiration date. There is the unsolved problem of non-revocation of biometric information. Once biometric information is leaked on a large scale, there is no way back to “recreate it”. Such a leak will eventually cause a huge societal problem. **At Futurae, we are building systems for the future, considering the limitations of current systems and their impact on people and society.** At the same time, we are striving to make systems more inclusive, also for people with disabilities or those that are less technologically savvy.

Adaptive authentication not only increases security, but also reduces friction for users trying to get work done. Today’s login requirements can be annoying, and users must always enter a username, password, and type or scan a code from an app. Adaptive authentication can ask for less information from users who are recognized and are in expected contexts. It occasionally asks for more details when circumstances suggest a higher security risk. Overall, the result is fewer user interruptions, lower entry barriers, and increased security.