Adding “I AM” to IAM

The presumption of innocence states that the onus for proving guilt belongs to the accuser and not to the defender. However, cybersecurity in the past decade has been more aligned with feudal law.

Most users are innocent. They have a right to say “I am. I exist. I have a right to freedom and to not be under suspicion.” Cybersecurity systems today make them feel the opposite – that “I am NOT. Only hackers are. I must somehow exist within this criminal world.”

The architecture behind most IAM systems is based on proving a user’s innocence. It is becoming increasingly challenging to prove that you are an authorized person with policies such as multi-factor authentication.

The user experience at the front end is no different. What with captchas and frustrating user-lockouts when incorrect credentials are entered, despite ~98% of human customers being legitimate and low fraud-risk, most people are put behind metaphorical bars for crimes they have never committed.

Trust is a two-way street. How can you expect your customers to trust you (and more importantly, end users to trust and adopt your SSO solution), if you have no trust in them?

Users must be given the benefit of the doubt. They must be allowed freedom within their networks.

Ronald Reagan said it well, “trust but verify”. This is the direction in which IAM architecture must now flow. At the moment, the IAM landscape operates not even in verification mode but in an outright ‘prove-your-innocence’ model.

According to industry analyst Gartner, “by 2022, digital businesses with great customer experience during identity corroboration will earn 20% more revenue than comparable businesses with poor customer experience.” This is because in our evolving, networked world, customer experience is becoming one of the single most important reasons to buy from a business. Competition is perpetually increasing, innovation is cut-throat, and people actively educate themselves before making purchases. So, user experience is exponentially more important in products such as Single Sign-On and Password

Management which are targeted at businesses. A poor user experience results in low adoption of the solution .

IAM vendors need to change their mindset and play a different game from here on. Instead of just jailing customers out of their apps until they prove that they are worthy of access, they must use their own intelligence in the form of computer learning and behavioral analytics to determine which login attempts are high risk, while allowing low risk ones a much wider berth to go about their daily operations.

In 2017, Gartner suggested a framework for building IAM systems that treat customers fairly. The framework was as follows:

1. Identify Signs of Legitimate Behavior (Good Customers)
2. Identify Evolving Attack Methods and Patterns (Criminals)
3. Apply Intelligent, Context-Based Adaptive Access to Customer Interactions

The technology that is addressing this challenge is Adaptive Authentication. It revolves around using intelligence to differentiate between genuine and fraudulent access attempts.

It is the basic attitude behind our attempts to protect users that needs to change.

Hacking makes headlines, but statistically it’s just a fraction of what goes in networking. We must assess the reality of security risks and design our solutions accordingly. Simply building as many walls as possible is not the answer – we must create intelligent, responsive gateways if we want IAM adoption to grow.