
WHAT IS BEHAVIORAL BIOMETRICS?

Authentication is evolving from static one-time user action, to transparent and continuous ways of validating digital identities without imposing frustration on end users.

Behavioral biometrics technologies invisibly and unobtrusively authenticate users by validating the manner in which they physically interact online. Behavioral biometrics technologies learn how individual users hold mobile devices in their hands and press their fingers on the touchscreen. On computers, the system learns how users type on keyboards and move their mouse and cursor.

The BehavioSec solution gathers this behavioral data and analyzes it using advanced techniques, to ensure that the user is who you expect them to be.

PIONEERS IN APPLYING BREAKTHROUGH TECHNIQUES

BehavioSec has over ten years of practical experience applying breakthroughs in the fields of machine learning, big data, and artificial intelligence to the emerging technologies of behavioral biometrics. Early on, BehavioSec worked closely with key customers and government agencies to develop the sophisticated logic and algorithms required to move its behavioral biometrics platform into the mainstream commercial marketplace.

AI AND THE REAL WORLD OF USER AUTHENTICATION

It takes more than scholarly expertise in machine learning and artificial intelligence to make a successful behavioral biometrics product. You need the performance and scalability characteristics required by modern organizations and internet architectures. Unlike academia, in the world of commercial applications you don’t have unlimited time for analysis or unbounded resources for data and bandwidth. To be commercially feasible the underlying machine learning models must be able to learn patterns from smaller sets of data, and do it in real time for millions of users. The BehavioSec solution provides a continuously learning AI subsystem with pre-weighted machine learning models based on prior analysis, using a hybrid of offline and online calculations.

DETECTING NON-HUMAN BEHAVIORS

Behavioral biometrics data can also be leveraged for bot and RAT detection. Because it has built up over time a sophisticated understanding of normal human behavior, BehavioSense can detect behavior that is likely to be non-human in origin.
THE BEST OF BOTH REAL-TIME AND OFFLINE ANALYSIS

In real time, the BehavioSec solution compares the behavioral biometrics of the active user against previously gathered profiles of that user, or others in the user population, for the purposes of continuous authentication. Offline, computationally intensive big data statistics provide additional analysis. Completing the circle, offline calculations feed into existing and new machine learning models for use in online real-time analysis. There are many benefits to this approach:

- Real-time user analysis rapidly adapts and quickly identifies inconsistencies.
- Real-time User Profiles include sub-profiles that are detailed enough so that they are resistant to fraud. This is called a “narrow profile,” versus a “wide profile” that may be so loose as to accommodate fraudulent behaviors and result in false positives, or falsely identifying a fraudster as real.
- Initialized machine learning models make rational assumptions that accelerate the “training” of new User Profiles. By leveraging statistical knowledge, it takes less time to identify the characteristics of a new user and populate their profile.
- The faster that profiles mature, the sooner the system can reliably identify real versus fraudulent users.
- Offline data can be analyzed for trends across disparate user sessions or between different groups of users.
- Offline data can provide a set of characteristics for a population of users, against which to compare brand new users even before they get deeply into a session. Called Population Profiling, this helps to quickly identify possible incidences of new account fraud (NAF).

“BehavioSec machine learning and big data analytics connects end user behavior to a continuous authentication process.”

-Neil Costigan, CEO