Digital Fingerprints is a continuous authentication system based on behavioural biometrics. Every user protected by the system gets their own set of behavioural models which are trained on their interaction with the computer, such as mouse movement characteristics, keyboard typing cadence or touch screen usage. Then our high-throughput backend system analyses user's behaviour throughout the entire session, notifying Security Operations Centre if user's behaviour does not match their usual one. The analysis is continuous, so even if a session or device gets hijacked, the system will detect the change in behaviour. The analysis begins right before the user logs in, which allows us to quickly detect any ongoing attacks. All of this is done without affecting user experience of the protected system, and no interface changes are needed to integrate with Digital Fingerprints. Collected data is anonymised before it leaves users browser, making sure that no sensitive information can leak.

What differentiates Digital Fingerprints from other providers?

- No data that is considered as Personally Identifiable Information (PII) is collected.
- GDPR Compliance - our product is designed in a way that complies with GDPR.
- Model per user - every user's behaviour is scored against their own personal models, trained with their behaviour.
- Near real-time processing - time from user interaction to scoring is not larger than 5 seconds.
- Continuous authentication - from the moment of logging in up to the moment of the logout.
- Easy integration - with just a single API needed for minimal integration.
- We do not require any specific actions from the end user for the system to work, so user experience is not affected at all.
- All the data that is collected is used only for the sake of security, we do not sell any data to third parties.