Over the past five years B-Secur has grown from being a deep R&D focused company with six employees to having a strong commercial framework and around 40 full-time employees, working across technology, science, commercial and operations. This growth has been driven by developing a world leading, next generation, biometric product called 'HeartKey' (HK). Ben Carter, CCO explains more…

"ECG technology is moving into the mainstream. We believe we are on a precipice of seeing ECG technology coming out of the hospital and into the home, within everyday devices. We see it in vehicles monitoring driver and passenger wellbeing and we see it being a crucial aspect of the human/machine interface allowing simple and seamless interpretation of people's needs by devices. Everyday life throws up challenges, the fast pace and pressures people put themselves under are challenges enough, without the unexpected happening. Biometrics can help by providing constant, detailed and relevant feedback personalised for the individual. This provides a mechanism to help people manage the stresses and strains of modern life. The benefits don't stop there though as the potential to authenticate users and protect sensitive data opens a wealth of use cases.

"We see a growing and significant ecosystem where all devices have IoT connectivity and consumers will be able to access ECG health and wellness information all day, every day. We believe this will be a fundamental development in how individuals manage their health.

"At B-Secur, we take physiological data from humans across multiple diverse devices, secure and encrypt that data, taking it all the way through to the cloud via our HK analytics platform. This solution provides real time and trended information to the uniquely identified user, fundamentally changing and enhancing the end customer experience."

So how can biometrics support the increased usage of digital identity and the importance of protecting this?

"Digital identity and wide scale identity fraud is one of the greatest challenges brought by our increasingly digitalised world. On device authentication means that the data transfer of sensitive information can be reduced. However just this year the UK's National Cyber Security Centre revealed more than 23 million people use the password '123456' – a reminder of how vulnerable our personal data is. The need and time for change is now. Biometrics have the potential to offer a convenient and secure method of verifying a user's identity. With ECG (B-Secur's HeartKey), biometrics can also provide more than just trusted verification (and inherent liveness detection) – there is potential for your health and wellness to become part of your digital you. The Health and wellness data gathered offers many additional use cases; e.g. Insurance, Healthcare, Wellness trending for Enterprise etc.

"Liveness detection is essential for true mainstream adoption. Essentially this is the confirmation of 'live' human presence. Unlike some other biometrics, ECG has the ability to prove such a vital credential.

"In the age of big data, consumers are rightly concerned about how their personal data is protected."

“It is key for detecting spoofing attacks, or synthesised data. For example, researchers from Michigan State University claim to have created a set of master fingerprints that could fool a scanner up to 65 percent of the time. ECG can eliminate this risk – not only assisting in the unique identification of a user but confirming the ‘live source’ of a signal.

“In the age of big data, consumers are rightly concerned about how their personal data is protected. We have reached a time where traditional methods for securing data, such as usernames and passwords, are simply not strong enough to be considered secure. The design and widespread adoption of new multi-factor authentication is required to satisfy the increasing demand for security and trust e.g. end users want their data to be secure, but there are limits on how much time and effort people will tolerate to provide credentials to authenticate. Therefore, the factors chosen for any authentication task must be carefully balanced with the usability of the system, depending on the level of security required. Regulators also have a part to play to ensure companies that provide services to require multi-factor authentication where appropriate.

"Looking to the future, standardisation of these systems will play a large role in the overall adoption of the technology. End users do not want to have to work with multiple authentication systems across different services, as this only increases the complexity for them. This has been recognised in the market already, with the World Wide Web Consortium (W3C) working on a new WebAuthn standard which aims to standardise an interface for authenticating users to web-based applications.”