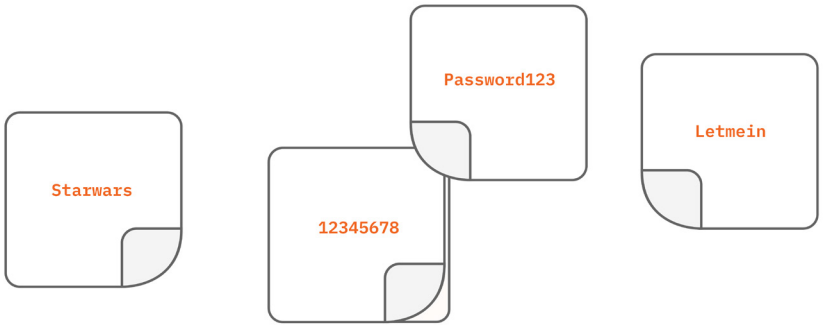
Cipherise



Traditional authentication is broken.

Adding password complexity such as length, special characters or forcing time-bound changes is not working. Over 80% of confirmed data breaches still involve leveraging weak, stolen or default passwords.*

It's time to move on from the traditional method of username and password.

That's why Cipherise exists.

** 2017 Verizon Data Breach Investigation Report.*

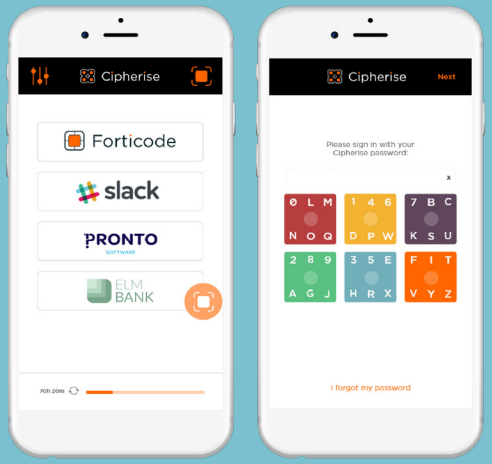
Secure Digital Engagement

Cipherise brings security and awareness to every interaction by providing multi-factor security, simply and invisibly; providing a framework that delivers bi-directional trust and continuous digital engagement in both the digital and physical worlds. Organisations can be sure the right people are engaged and customers can be sure that any communication from their service provider is genuine.

Always be sure that only the right people are logging onto your systems.

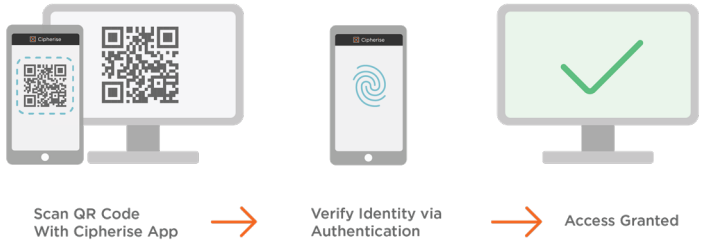
Cipherise provides a highly secure authentication experience across internal or client facing applications, including mobile apps.

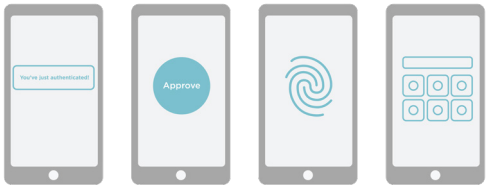
The authentication process is decentralized and happens locally on the user's smart phone. Credentials are never transmitted and with the OneTiCK™ keyboard's unique design, there is no risk of replay.



Be in control with Invisible Multi-factor Authentication

Cipherise provides the end user with a simple, yet highly secure authentication experience.

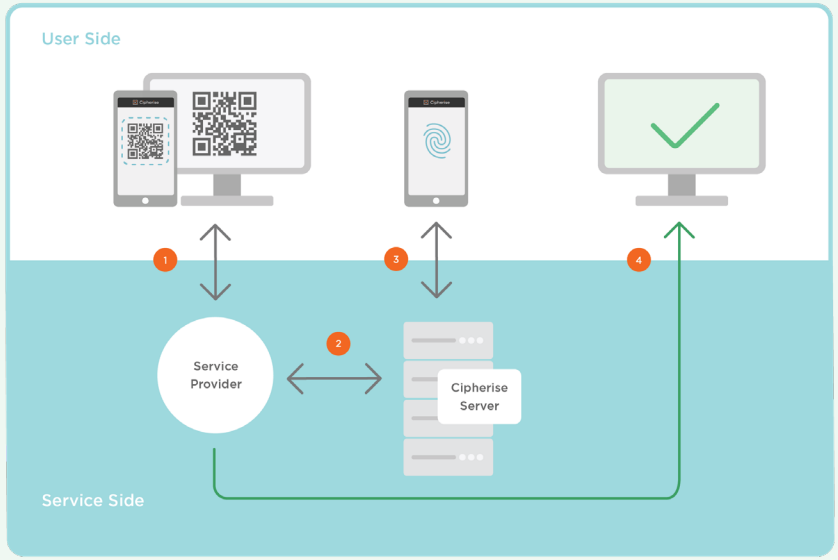




Cipherise has four levels of security, allowing organisations control over the authentication mechanism used. Depending on the level of risk, the organisation can choose from a simple notification, approval button, biometric response or OneTiCK™, for the highest level of security.

All levels are underpinned by the persistence of OneTiCK, a patented one time cognitive keyboard, that dynamically changes every time a user authenticates. This eliminates the risk of keyword replay or over the shoulder observation.

How does it work?



1. User scans QR code and lets the Service Provider know the user wants a session.
2. The Service Provider asks the Cipherise Server to authenticate the user.
3. The Cipherise Server asks the user to authenticate on their Cipherise App.
4. Once verified by the Cipherise Server, it lets the Service Provider know the end user is verified and can provide the user a session.