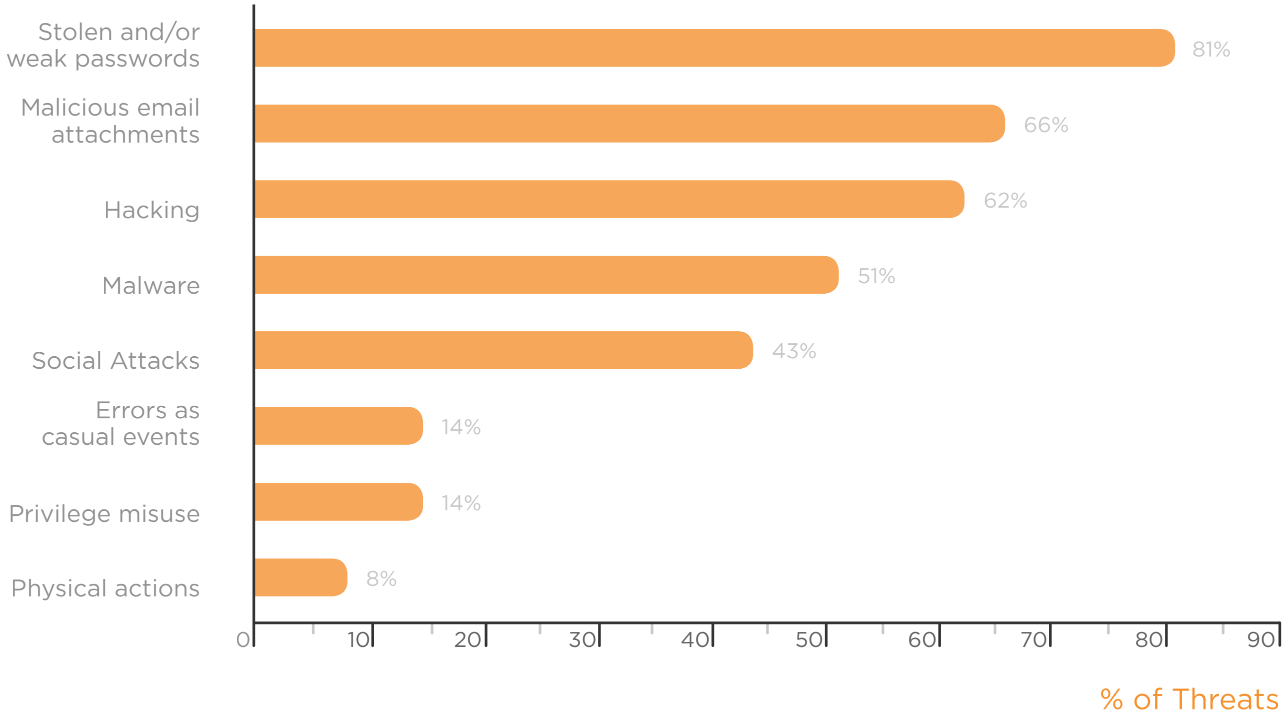
Cipherise Authentication Solution

The Problem

Traditional methods of authentication, such as user name and password, are inherently problematic. Passwords can be brute forced, stolen, shared and often frustrate users with their requirements of length and special characters. On their own, they are not very secure and can represent a significant weakness in your company's defences against cyber threats. How do you know the person logging onto your systems is actually who you think it is?

Companies try to combat this weakness by introducing additional factors, such as tokens or creating strict policies around password creation. This can lead to additional cost for the company and frustration for employees. Additionally, companies are required to maintain and protect a credential store for employees and perhaps even customers. These repositories obviously contain very valuable data, and are always a target for hackers. If this data is exposed through a security breach the result would likely be considerable financial loss and reputational damage.

2016 Threat Vector Frequency [1]



[1] *"Breach Level Index, Data Breach Statistics, 2017 & Verizon, 2017 Data Breach Investigations Report 10th Edition, 2017. Note threats commonly involved multiple vectors."*

How Does Cipherise Solve This Problem?

To solve this problem, a radical shift in thinking was required. Where traditionally authentication methods are centralised, Forticode created a solution that is a decentralised and distributed model.

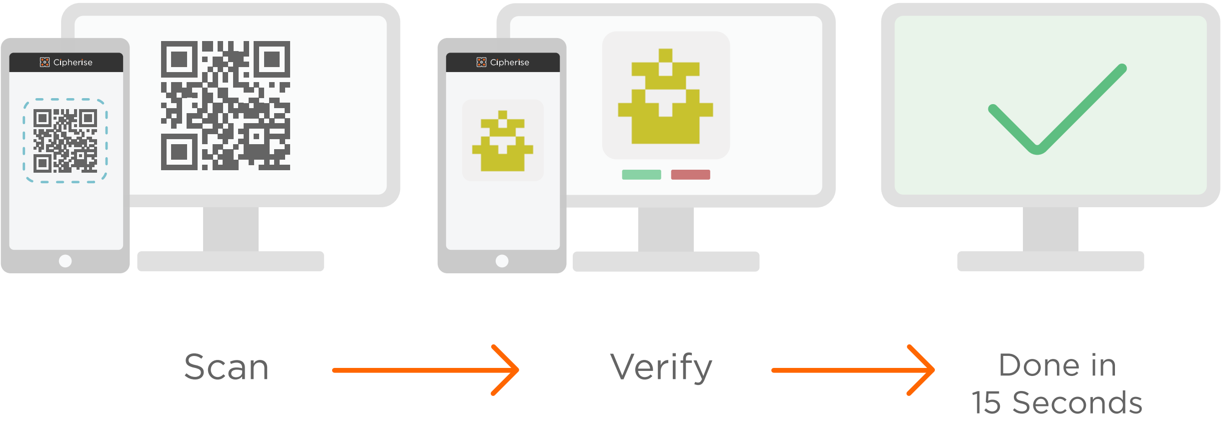
- The authentication process happens when the user interacts consciously with the Cipherise application, allowing the user to be the sole custodian of their credentials
- Cipherise allows users to login safely and securely, even on malware infected devices. Credentials are never typed into or transmitted to the system you are working on
- Bi-directional attribution to ensure true identity assertion. You can be sure the person logging on to your systems is the right person, and that person can trust that the system they are logging into is legitimate
- No need to protect and maintain a credential store, which can be targets for hackers
- Reduce the risk of fraudulent activity
- Stop unauthorised authentication activity before it occurs
- A clear and full audit trail for compliance and auditing purposes
- A levelled approach to security allowing for reduced friction for users and greater security for the business
- Reduced hardware costs. No tokens necessary as users can use their smartphone
- Reduced helpdesk costs associated with password resets

How Does Cipherise Work?

As mentioned previously, Cipherise is a decentralised process, so the actual authentication happens locally, on the user's own device, with the Cipherise app. A service provider does not have to store any credentials for their users.

Enrolment

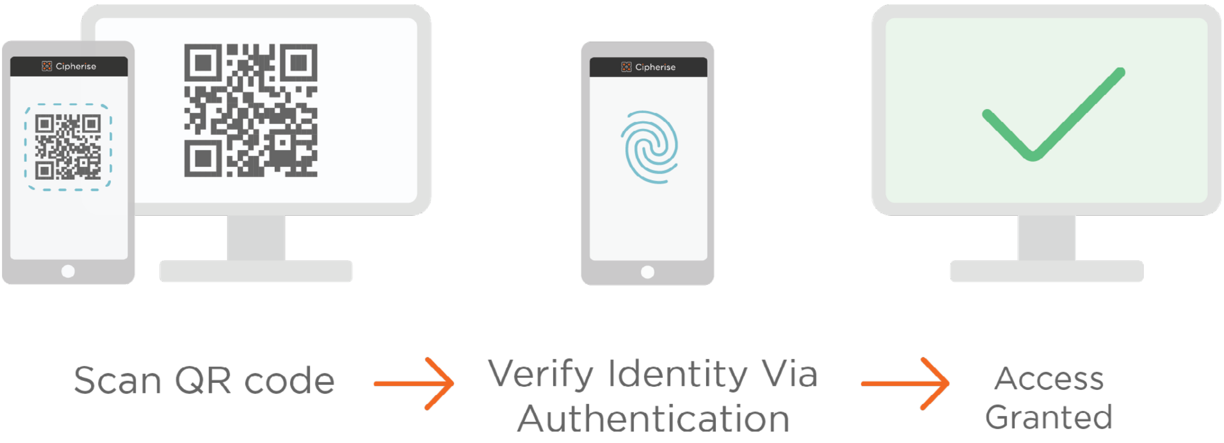
Initially a user would enrol to use a service. This self service process can be done very simply by scanning a QR code with the Cipherise application. During the process, identicons are used as an extra layer of protection. The user can see visually if they match, meaning it is safe to proceed.



Scan → Verify → Done in 15 Seconds

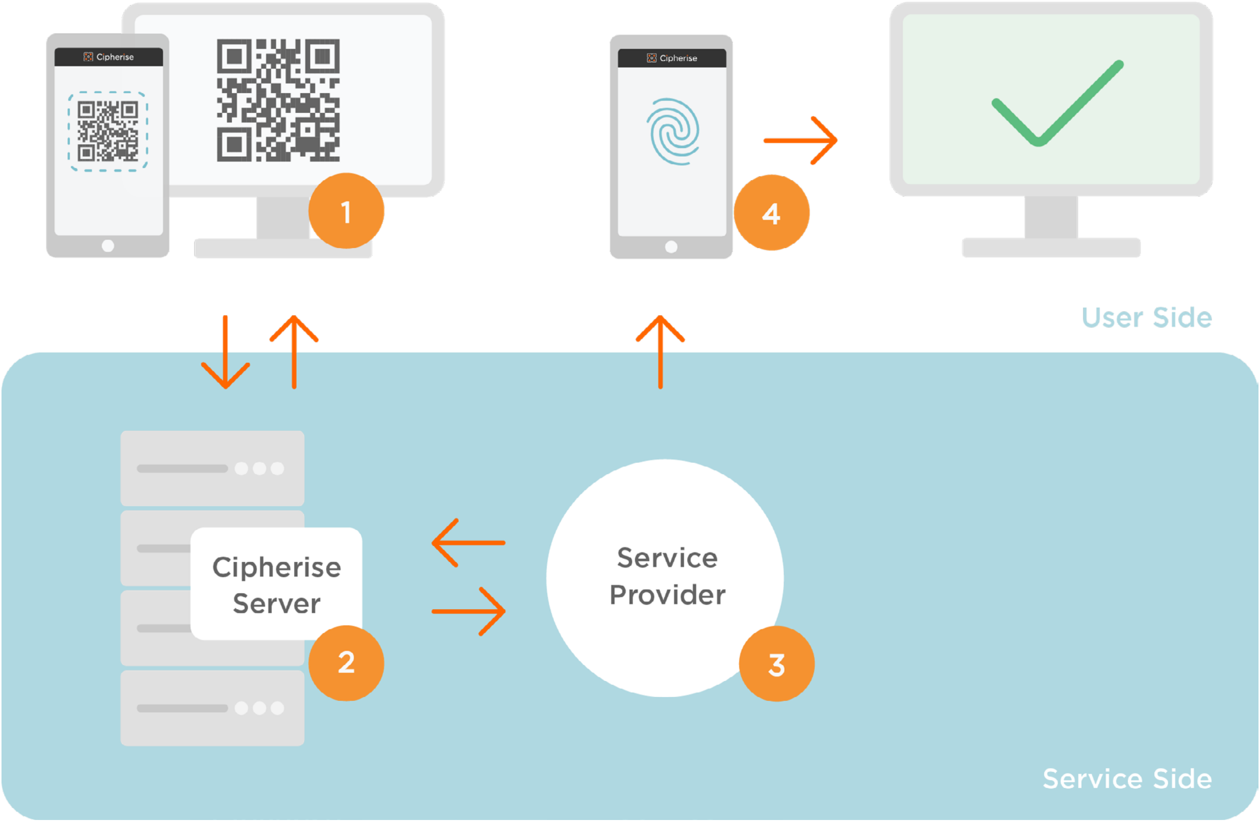
Authentication

Once a user is enrolled to a service, authentication is very simple. A trigger starts the process, in this example a user is presented with a QR code to authenticate. Using their device, they scan the QR code.



Scan QR code → Verify Identity Via Authentication → Access Granted

While this is a simple process for the end user, under the covers Cipherise provides a high level of security by utilising multifactor authentication in a decentralised manner.



1. A user initiates the authentication process by scanning a QR code on the screen.

2. The phone contacts the Cipherise server letting it know that the user intends to authenticate. The Cipherise Server asks the user to authenticate on their device.

3. Once the user has successfully verified their identity, the Cipherise server lets the Service Provider know that the user is verified and would like a session.

4. The Service Provider authorises the session for the user.

It is important to note that the user's credentials are never transmitted, typed in or entered into the browser during this process, greatly reducing risks associated with keyloggers and other malware.

Be in Control With Multi-Factor Authentication

During the authentication process, Cipherise utilises multifactor authentication security measures. The device, (something you have), a secret password (something you know) and biometrics (something you are). This utilisation is almost invisible to the end user, who has a low friction experience, with high level multi-factor security under the covers.

In addition to this, Cipherise has four levels of security, allowing businesses to have greater control over the authentication process.

Organisations simply choose the level of security based on the risk associated with the particular service. If it's a low risk application, a simple notification or approval button may sufice, greatly reducing friction to your end users.

If a higher level of security is required, simply choose a biometric response or OneTiCK™, Forticode's patented cognitive keypad for the highest level of security.

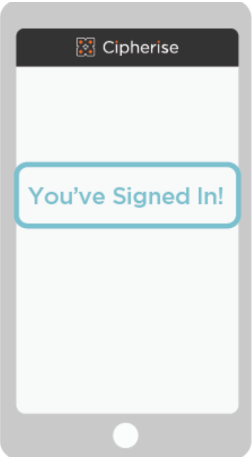
As well as allowing an organisation to have greater control over authentication. Cipherise provides a very clear audit trail for compliance purposes, via the Cipherise Administrator Dashboard.

For more information or to organise a demonstration, please contact us at:

enquiries@forticode.com

Level 7, 22 William
Street,Melbourne, 3000 VIC

@forticode

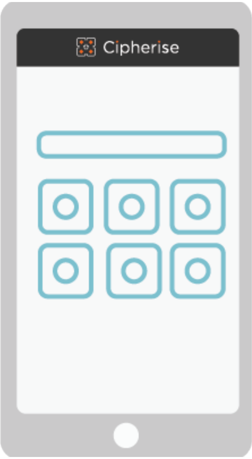


Level 1

Cipherise
Approve

Level 2

Level 3



Level 4