HAVENTEC AUTHENTICATE

Stronger account fraud prevention with decentralised authentication

haventec

SIMPLY POWERFUL SECURITY

NEXT GENERATION IDENTITY MANAGEMENT

Haventec Authenticate protects against common identity theft attacks:

- Phishing
- Social Engineering
- Shoulder Surfing
- Password Cracking
- Mass Account Breaches

Authenticate employs two main security methods to block unauthorised access to accounts:

1. **DECENTRALISATION** – breaking credentials into multiple parts and distributing them across multiple locations.

   Benefit: No more passwords, no more vulnerable central stores of identity.

2. **SINGLE-USE ENCRYPTION KEYS** – changing keys and re-encrypting data for every transaction.

   Benefit: even if some parts of a user's credentials are stolen they cannot be reused.

Authenticate demands the following conditions are true to authorise access:

- ✓ User is on an Authenticated device
- ✓ User enters their PIN, which is only known to them (not stored or saved anywhere)
- ✓ The device has a valid single-use authentication secret
- ✓ User is connecting to an authenticated domain

FRAUD PREVENTION

The following common attacks are prevented because even if access details are stolen during a single interaction they cannot be reused.

PHISHING

DESCRIPTION

Tricking a user into clicking on a fake website link to capture credentials and secrets then reusing that information for fraudulent activity.

PROTECTION

The fake website does not have, and will not have, access to the single-use authentication secret.

SOCIAL ENGINEERING

DESCRIPTION

Manipulating a user to capture credentials and security question answers then using that information to fraudulently reset credentials.

PROTECTION

The attacker does not have access to the authenticated device.

SHOULDER SURFING

DESCRIPTION

Observing a user entering credentials, including secrets, then reusing that information for fraudulent access attempts.

PROTECTION

Even if the attacker accurately captures the user's credentials they will not have access to the authenticated device nor the single-use authentication secret.

PASSWORD CRACKING

DESCRIPTION

Computer code that tries password variations and harvested usernames to find a match – the weaker the password, the faster it can be cracked.

PROTECTION

Even if the attacker discovers the user's credentials they will not have access to the authenticated device.

HAVENTEC IS DECENTRALISING CYBER SECURITY

Haventec was founded in Australia by a highly experienced team of business leaders, technologists and inventors committed to making cyber security better for everyone.

We have extensive experience in commercialising technologies that solve real world challenges, and know how to tame complexity while mitigating risk.

We believe you can build trust by giving people back control of their identity and other sensitive information, including financial data.

Our internationally patented technologies are based on a simple, powerful idea: decentralise data access security and everyone's data is safer.

When you remove the need for central stores of user credentials or other valuable data you remove a lot of the motivation for hackers to attack your systems.

KEY BENEFITS

1 / **Decentralise** critical information to protect privacy

2 / **Reduce** risk for organisations online

3 / **Simplify** user experience and remove friction

4 / **Offer** solutions that are easy to configure and scale

PROTECT PRIVACY & PREVENT FRAUD WITH HAVENTEC'S SIMPLY POWERFUL SECURITY.
ASK US HOW.

+61 2 8320 9488 | info@haventec.com

haventec.com