

Identity Assurance Made Simple

Solution Brief



Secure, contactless, biometric MFA for today's world

Increase the fidelity of user access management with biometrics. Simple to use and easy to deploy, ImageWare Authenticate provides true user assurance across your enterprise applications and end customer base.

SECURITY BREACH IMPACT

Data breaches are expensive, costing small businesses an average of \$3.9 million and publicly traded companies \$116 million per breach.¹

300%
Increase in attacks since COVID-19 as reported by the FBI²

49%
Of people use compromised passwords³

73%
Of passwords have been reused⁴

7.27%
Average decline of share prices after a breach⁵

Passwords are the problem

1. Phishing



30% of phishing emails make it past default security.⁶

2. Stolen Credentials




\$4.77M is the average cost of a data breach due to compromised credentials.⁷

3. Brute Force Attack



80% of all data breaches are the result of stolen credentials or brute force attack.⁸


2FA isn't safe either...



Single-Factor Authentication

Something You **know**


- Usernames and passwords can be forgotten, misplaced or stolen
- Easily hacked



Multi-Factor Authentication

Something You **know**, something you **have**, plus who **you are**

- Cannot be lost, stolen, or forgotten
- Difficult to spoof
- Works across devices



Two-Factor Authentication

Something You **know**, plus something you **have**

- Tokens, smart cards, and mobile devices can be lost or stolen
- Can be counterfeited

1. <https://enterprise.verizon.com/resources/reports/>

2. <https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/>

3. <https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/>

4. <https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/>

5. <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/>

6. <https://www.avanan.com/blog/what-is-a-phishing-scam#:~:text=Phishing%20scams%20are%20so%20prevalent,in%20system%20to%20attack%20>

7. <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>

8. <https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/>

IMAGEWARE AUTHENTICATE SOLUTION

Leveraging Imageware’s award-winning biometric and anti-spoofing technologies, Authenticate ensures the right people access the right resources and prevents fraudulent attackers from accessing systems and data through nefarious means.

- 1 **Everyone is unique**, each of us are our own secure password.
- 2 **Liveness can’t be copied**, replayed, or stored for later use.
- 3 **You can’t** misplace or forget your biometric identity.
- 4 **Enroll once** and use across all your devices.
- 5 **Presentation attack detection** prevents authentication using photographs, videos, and face masks.

Authenticate the person not just the device

Imageware Authenticate provides secure incloud matching and does not store biometric information on the users’ mobile devices to protect individuals’ identities. The solution creates biometric templates using key features of the raw biometric data, which is then destroyed. These templates cannot be reverse-engineered and are encrypted both in transit and at rest.

Powered by the patented Biometric Engine®, designed specifically for fast, efficient, protected storage and processing of biometric information, Imageware Authenticate is vendor neutral, allowing Imageware to build and deliver plugins for nearly all biometric algorithms.



Biometric Authentication is for Everyone



**Downloading
Tickets**



**Sending Money
to Friends or
Businesses**



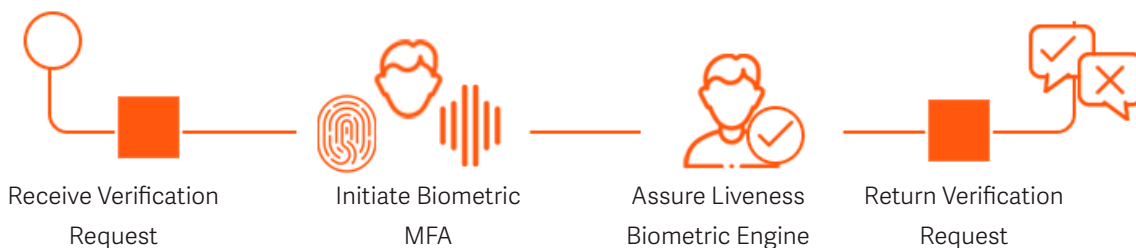
**Logging In
to Critical Work Apps
from Any Device**



Consumer

Enterprise

How it Works



Once installed, users will receive push notification or alert on the Imageware Authenticate mobile app, prompting a seamless two-stage secure identity confirmation:

- Leveraging an advanced AI neural network and ongoing machine learning, Imageware’s Biointellic technology confirms liveness and rules out the possibilities of deep fakes and bad actors.
- Once a valid individual is confirmed, the Imageware Authenticate Platform matches users against their enrolled biometrics. The authentication is complete.

Customer data security is our primary goal. The solution offers step-up MFA access with adjustable factors and authentication, such as policies based on login context, security policies according to risk, a choice of biometrics for end users, and nested requirements for multiple biometrics.

Imageware Authenticate’s self service portal allows businesses to dynamically message users, conduct ad hoc authentications, upload user lists, and view the status of all enrollments with a simple-to-use, intuitive tool.