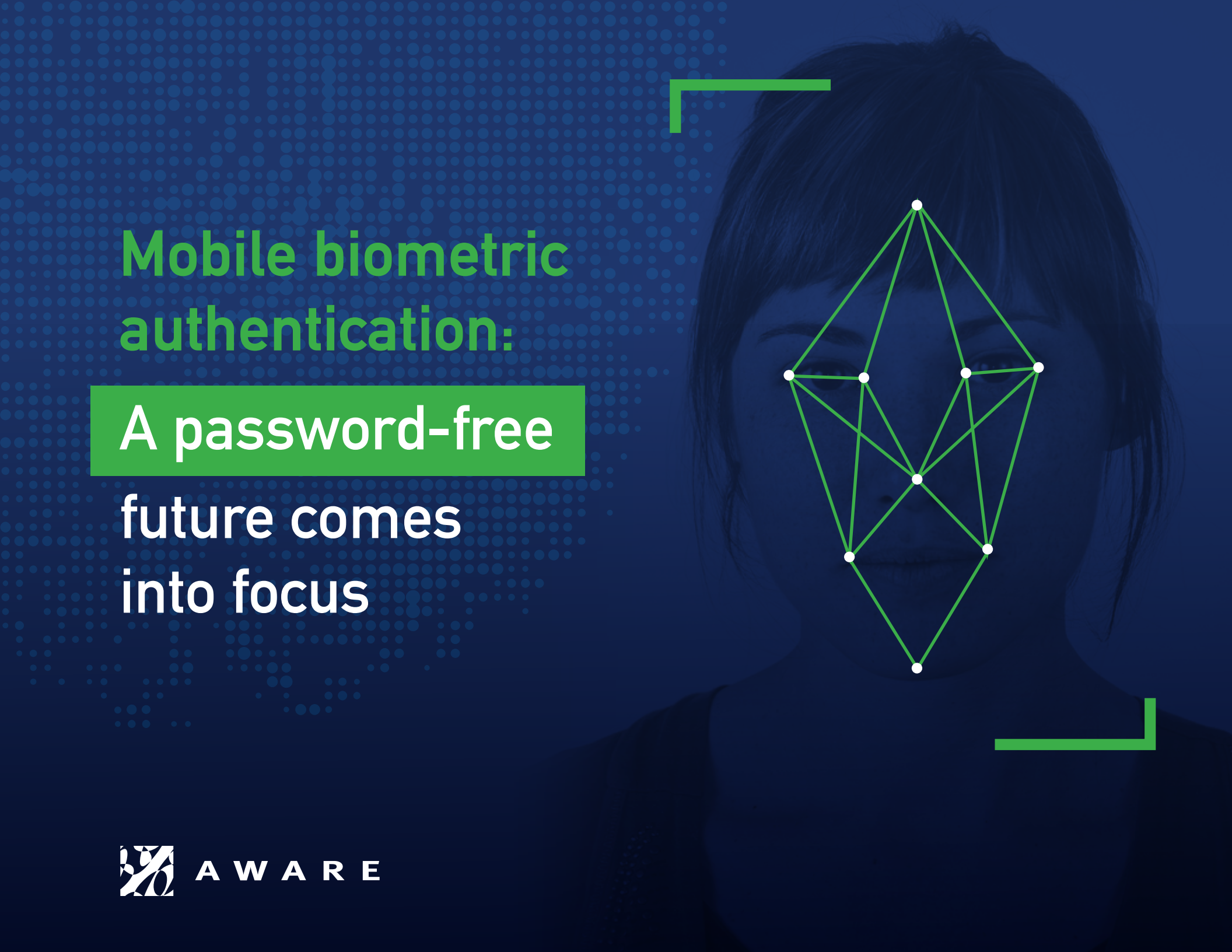
Mobile biometric authentication:

A password-free future comes into focus



AWARE

Table of Contents

Introduction

If you looked into your Magic 8-Ball and asked, "Will I ever be able to stop using passwords for authentication?" it would certainly reply:

"OUTLOOK GOOD."

And the outlook is good considering biometrics are making authentication simpler and more secure than ever. Passwords have never looked so retro. But if you asked us the same question, we would say you don't need a Magic 8-Ball to know that the future of authentication is already here.

Expect to see the following authentication advancements in action sooner than later.

Facial Recognition

When rumors were first heard that Apple's iPhone X would not have a fingerprint sensor, aspiring fraudsters could be forgiven for a moment of encouragement. Alas, that hope was short-lived, as we now know that facial recognition is used in its place.

"Magic 8-Ball, does this mean that facial biometrics are here to stay for mobile authentication?"

"IT IS DECIDEDLY SO."

Apple Face ID is here. The trendsetting device maker has opted for 3-D facial recognition technology in place of fingerprints for the newest iPhone.

Facial recognition for authentication has existed for several years. However, Apple's seal of approval further confirms not only its ease-of-use, but also the powerful security features of the underlying biometric technology that make it possible. As with fingerprints before it, Apple promises to usher in broad market adoption of facial recognition for mobile authentication.

Liveness Detection and Multimodal Biometrics

Why stop at face recognition? Fraudsters will undoubtedly try to spoof biometric authentication security measures.

Fortunately, modern biometrics are equipped with technologies that assess the "liveness" of the user. They make it difficult for a fraudster to use a video or audio recording of a victim to impersonate them.

A multimodal approach applies different biometric modalities such as face, voice, and keystroke dynamics to increase security. The additional biometric data not only improves biometric performance in terms of fewer false matches and non-matches. It also contributes to liveness detection.

Face + voice + keystroke = Multimodal biometric authentication.

Facial recognition can be added to other modalities for improved performance and liveness detection. For example, a user can type in a passphrase while looking into the camera. The authentication engine simultaneously analyzes keying cadence and facial geometry, making it more biometrically accurate as well as more difficult to spoof. Or, the app may request a random spoken series of numbers while capturing the facial image. The two can be matched and analyzed for liveness in concert. The chances of spoofing that, according to the Magic 8-Ball, are...

"VERY DOUBTFUL."

FIDO: Standards-Based, Password-Free Authentication

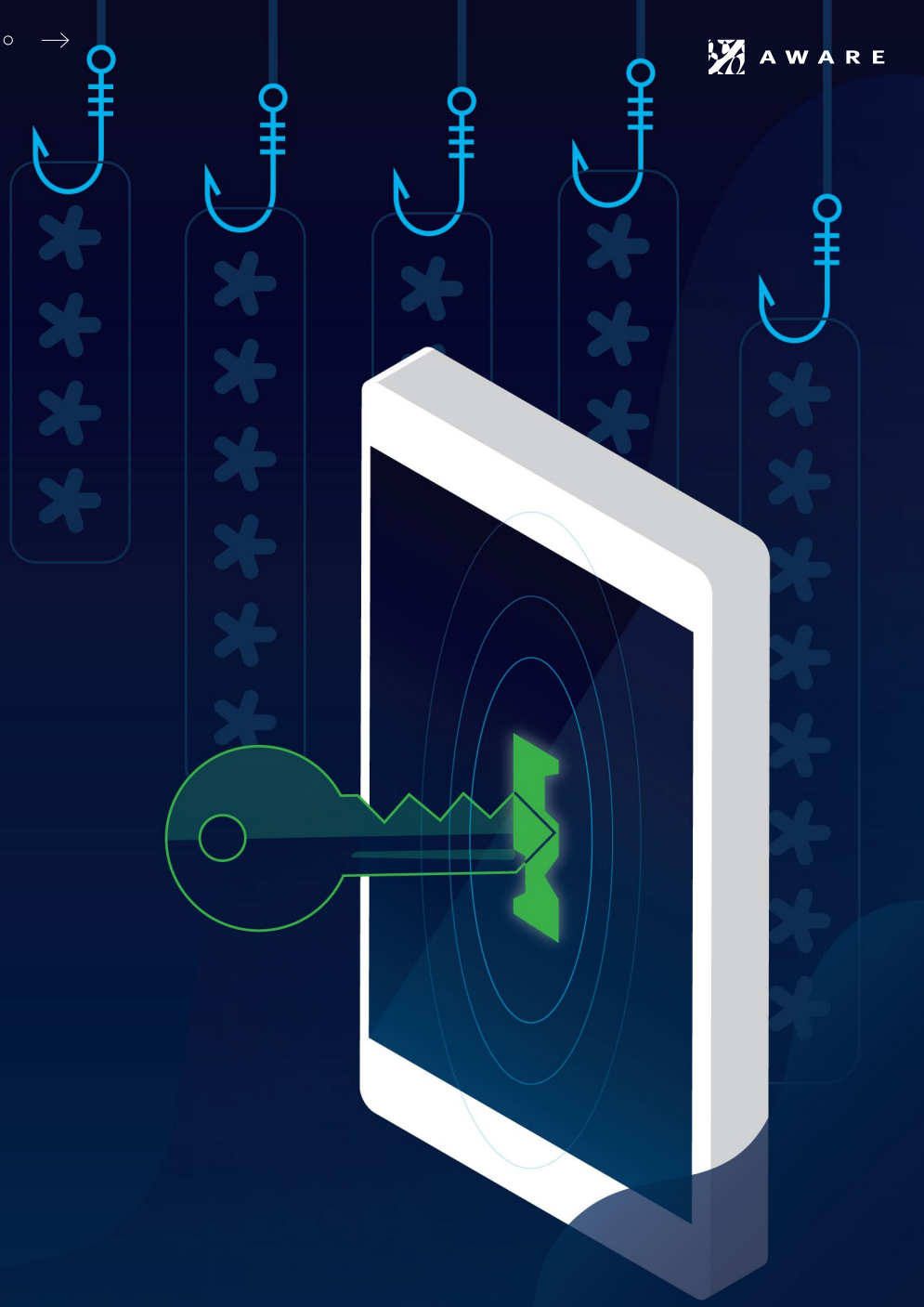
Even though they were invented back in the 1960s, passwords are still the most commonly used authentication mechanism. With the vastness of today's internet and the power of our smartphones, passwords have become intolerably inconvenient and vulnerable to compromise through phishing, breaches of password storage servers, brute-force guessing, and social engineering.

FIDO aims to get rid of the password and enhance authentication in a standards-based way, using biometrics and public key (asymmetric) cryptography. Under FIDO, a unique private/public key pair is created on a device, such as by a mobile banking app. Importantly, the biometrics and private keys never leave the mobile device; only the public key is stored centrally. Upon authentication, a successful biometric match makes the local private key available for a challenge response to the server.

FIDO 2.0 standards are being adopted to build authentication right into the browser, effectively filling the missing identity layer of the internet. Imagine authenticating a transaction through a bank's website using a combination of facial recognition and keystroke analysis without needing to memorize complex passwords. It would be easier for customers to bank online securely and harder for fraudsters to exploit stolen account data.

Does this approach make a large scale theft of passwords virtually impossible?

"SIGNS POINT TO YES."



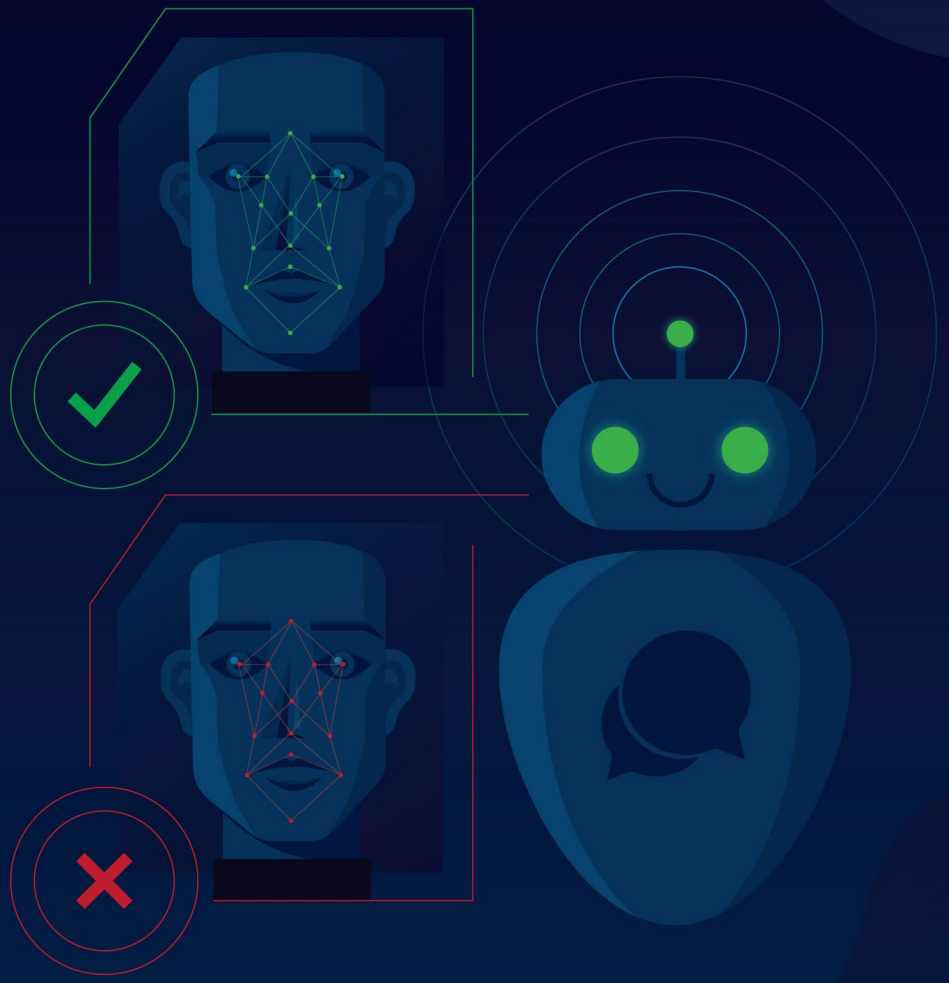
Biometric Authentication with Chatbots

A chatbot is a computer program that can communicate in written form in a way that simulates human conversation. Thanks to rapid advancements in machine learning, they're harder than ever to distinguish from humans, prompting many organizations to use them for certain types of customer interaction. They can be extremely useful and easy to work with, but can they be used for applications where security is needed, as in "Bankbot, can you please pay my electric bill on Thursday?"

Authenticating during a text chat, such as by using keystroke dynamics and even face biometrics, can make bot-chatting useful for applications where security is required. Soon, they'll be able to not only understand what you're saying but also to verify that you are who you claim to be.

Chatbots with built-in, continuous security?

"WITHOUT A DOUBT."



Out-of-Band Biometrics

An "out-of-band" approach to authentication involves using multiple channels to ensure that a transaction originates with the user. For example, using a mobile device to log in to a website through a browser on a PC. In this way, a mobile device can serve as an additional authentication factor like a token, representing possession (something a user has) to demonstrate authenticity.

But what if the device is compromised? The possession factor is largely rendered useless and actually becomes a liability. By adding biometrics as an authentication factor, possession is enhanced with inherence (something the user is). This time, when logging into a website via browser, the user still receives an out-of-band authentication challenge, but it will include a requirement to perform a biometric authentication on the device, making it much harder for a lost or stolen device to be used to fraudulently access the owner's online accounts.

Our prediction for out-of-band mobile biometric authentication?

"YOU MAY RELY ON IT."

Continuous Authentication

People tend to think of authentication as a gateway; complete your biometric capture or enter your password and "Open Sesame."

However, biometric modalities such as keystroke dynamics and facial recognition analysis have introduced the possibility of continuous authentication. This always-on, real-time method is more *process* than event.

For example, while typing information into a website, keying cadence can be analyzed in real time to detect anomalies that indicate a fraudulent user. If there is a deviation that indicates a change in identity, your session may be terminated. Other biometric modalities such as face and voice could also be used in this way to ensure the security of a session or phone call.

Continuous authentication is definitely in its infancy, but according to Mark Diodati, research vice president at Gartner, adoption is "inevitable."

In Magic 8-Ball speak, that's as good as a:

"YES, DEFINITELY."

The Ultimate Objective: Invisible Authentication

Security measures are a means to an end, and authentication is no exception. We'd prefer it to be in the background, even completely invisible.

In fact, invisibility is the ultimate objective of authentication, and it's nearer to reality than ever before. As biometric modalities like face, voice, and keystroke rapidly advance, identity verification will come closer to happening without any active participation from the user, while improving resistance to fraud at the same time. Authentication has always strived for security with convenience. Invisible biometric authentication makes it a reality.

Is there finally an end in sight for the 50-year-old password? Can biometrics deliver on the ultimate objective of invisible authentication?

This time, we don't need a Magic 8-Ball to know that the answer to both is a resounding, "Yes."

AWARE

WWW.AWARE.COM/CONTACT