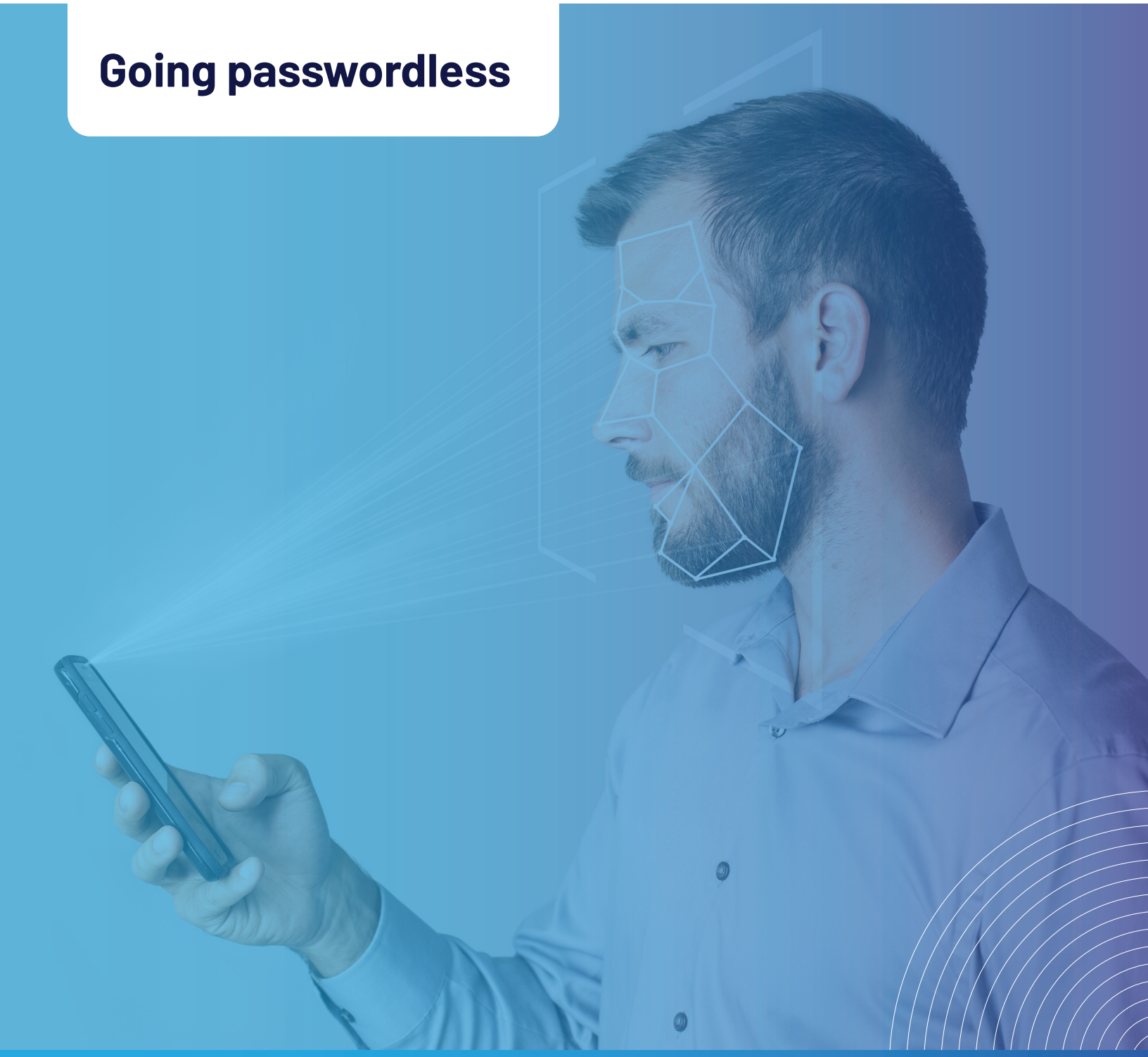
White Paper

Going passwordless



AWARE

781.687.0300 | sales@aware.com | www.aware.com

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.

The COVID-19 pandemic created new challenges for businesses as they were forced to adapt to an operating model where working from home was the new normal. These work from home conditions resulted in greater dependency on technology and without office infrastructure security, many workers have been exposed to an increased number of cyberattack risks. Additionally, workers are experiencing increased password fatigue resulting from the need to constantly update passwords. Given this state of flux, current authentication methods are just not enough to protect company and worker data. The need for stronger authentication is more important than ever before.

Current authentication methods

With the increased threats to cybersecurity, many companies have turned to two-factor authentication. Two-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two pieces of evidence to an authentication mechanism. Factors that grant access include something you know—such as a password, passphrase or personal identification number—and something you have—like a mobile device or a secure USB key.

This level of authentication has become the norm because it allows organizations to continue to use passwords. However, the method is far from perfect. Many users report[1] that the additional hurdles of two-factor authentication are overly inconvenient, which can cause annoyed users to cut corners and take shortcuts that make the system more vulnerable. Though requiring an extra identifier does deter some hackers from attacking systems defended with multi factor authentication, many others are willing to deal with the additional hurdle if they believe that the information stored within their targeted organization is worth the effort. In addition, two factor authentication does not provide identity authentication but rather device authentication. The device possession test is conducted under the assumption that the owner of the particular device will be the only individual using it, not taking into account instances of fraud.

The password problem

As the world continues to increase dependency on digital solutions, society continues to be heavily dependent on passwords and PINs. Unfortunately, passwords have problems. In fact, nearly all IT professionals (~95%) agree that passwords pose real security risks to their organization. This is because people have been using weak passwords, mishandling passwords (writing them on post-its) and reusing the ones users feel comfortable with, among other bad habits. According to Gartner[2], the State of Password and Authentication Security Behaviors Report 2020[3] and Verizon[4]:

- **20-50% of all help desk calls are related to password resets**
- **39-50% of people reuse personal or business passwords for workplace accounts**
- **80% of breaches involved weak or stolen passwords**

Among the top frustrations[5] for employees is changing passwords, remembering the previous 100 passwords and not being able to re-use them. This makes password management a tedious part of the job and surely doesn't add any security if done improperly. As a result, many workers suffer from password fatigue. Password fatigue can be defined as the struggle to for workers to remember all of their passwords. It is estimated that the average business employee keeps track of 191 passwords[6]. This is an obvious burden. Employees become tired of having to remember a host of passwords, so they start repeating passwords and reducing complexity in an effort to relieve the mental burden of how-to login. Unfortunately for

many, the fear of forgetting a password outweighs the fear of a potential data breach. In fact, 91% of people[6] understand the risk of reusing passwords, yet 59% admit to doing it anyway[6]. In short, passwords are the gateway to confidential data, electronic financial transactions, and more, yet we don't treat them as the most critical security risk an organization faces. Password fatigue, then, not only impacts employees but organizational security as well.

It is clear that the enterprise is more at risk if its employees are struggling with password fatigue. According to a survey conducted by the Ponemon Institute, 51% of people[7] rotate the same five passwords across their work and personal accounts. In addition to sharing passwords among their own accounts, employees often share passwords with each other; 69% of people admit to sharing credentials for work account access. Another potential security risk related to password fatigue is susceptibility to phishing since most password reset requests are delivered by email. Phishing is the most common attack vector and present in 36%[4] of data breaches. If an employee experiencing password fatigue was successfully phished, and if they had five passwords in rotation that were shared with another employee, the situation could easily escalate into a serious data breach. As a result, many of the world's worst corporate data breaches originated through password breaches.

COVID-19 impact on workplace technology

The ongoing COVID-19 pandemic has shone a light on the weakness of current authentication methods, making cybersecurity a critical priority as millions of workers and businesses across the world become dependent on digital infrastructure and the internet. According to the 2020 Global Risks Report[8], business leaders say their cybersecurity risks are increasing with cyberattacks and data theft among the top 10 risks CEOs are most likely to face in both short and long term. In the first six months of 2019 alone, data breaches exposed 4.1 billion records[9], often with millions of credentials in a single breach released into the public and dark web. The average cost of a breach is estimated at $3.92 million[10], and in 2021 the global financial loss associated with cybercrime was is $6 trillion[11].

The dependency on technology and the internet, combined with the on-going fear caused by the pandemic, created the perfect environment for cybercriminals to thrive. Workers changed work styles and behaviors. For example, HP Inc.[12] reported that 70% of office workers surveyed admit to using their work devices for personal tasks, while 69% are using personal laptops or printers for work activities. As a result of these factors, home workers were increasingly being targeted by hackers. Cybercriminals were able to ransom millions of dollars from businesses using time-tested tactics like phishing, social engineering and other hacker tools of the trade. For companies, the average cost of a data breach soared to $21,659 per incident during the pandemic, with most incidents ranging from as little as $800 to more than $650,000, according to a new report[4] from Verizon. But 5% of successful attacks cost businesses $1 million or more. KuppingerCole[13] reports that there have been a 238% increase in global cyberattack volume during the pandemic.

Mitigate alarming cybercrime rates with biometric authentication

Passwords were invented in the 1960s and were never intended to protect bank accounts, healthcare records, emails, and a long list of other commandeered usages. They were actually invented for computer time share and worked effectively enough for that use case at the time. The increased threats to cybersecurity and false identification have caused many companies to adopt rigid method like two-factor authentication to combat these issues. However, solving identity and security issues can be made easy with biometrics. This is because biometrics can be streamlined into current multi-factor authentication methods or allow users to go completely forgo passwords.

Biometric multi-factor authentication[14] works like current two factor authentication methods but requires an additional factor in the login sequence. One of the factors that the end user has to provide is a biometric (e.g., face or fingerprint). Biometric technology has become the gold standard for security and identity proofing due to its high accuracy percentages. The addition of biometrics in multi-factor authentication could ultimately render passwords obsolete, strengthening the IT infrastructure of businesses worldwide. At the very least, biometrics could strengthen multi-factor authentication overall.

By the end of 2022, Gartner[15] predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods in more than 50% of use cases — up from 5% in 2018. Passwordless authentication, by its nature, eliminates the problem of using weak passwords. It also offers benefits to users and organizations. For users, it causes the growing problem of password fatigue to also become obsolete.

For organizations, there's no longer a need to store passwords, and as a result enterprises will have:

Better security:

While passwords are vulnerable to phishing attempts, biometrics and hardware tokens aren't. Passwordless authentication[16] removes the problem of duplicate passwords and subpar password management practices like writing codes down on sticky notes.

Fewer breaches:

When companies transition to passwordless solutions, they considerably reduce their exposure to data breaches. When using passwordless solutions to authenticate, there are no passwords for cybercriminals to steal out of a platform server.

Lower support costs:

Passwordless authentication is cheaper in the long run. Passwords require organizations to maintain password management systems so users can perform periodic password refreshes and the occasional password reset. Shifting authentication to biometrics, lightens the load on helpdesks and enables organizations save on costs associated with replacing passwords.

With the increased dependency on technology, new working conditions and an ever-increasing escalation of malicious cyberattacks, this is the ideal time for enterprises to consider upgrading their security products and procedures. Biometrics add convenience and security, allowing companies to protect their data. - their most important asset.

Eliminate your password problem with Aware

Aware is a global leading provider of biometrics software products, solutions, and services that empower users to own and control their identity. Our solutions are a great option for any enterprise considering authentication options that involve biometric technology. Our solutions minimize friction, ensure security, and maximize convenience. We capitalize on our biometric domain expertise and deep customer intimacy to ensure we delight users through a customer experience that leverages the cloud and emphasizes the ease of doing business together for the end consumer. Driven by an understanding of customer and partner business needs and values, we actively strive to maintain our reputation as a service provider trusted to keep identities secure.

Mobile Onboarding: Our solutions provide identity proofing to support mobile onboarding. Advanced security checks can authenticate driver's licenses and passports and ensure spoof-resistant biometric facial matching between live and printed images. The onboarding includes biometric facial matching to identification documents, and verification for over 9,000 documents worldwide. The liveness detection also detects impostors, preventing them from accessing confidential accounts and information

Liveness Detection: Our advanced presentation attack detection algorithms detect not only victim impersonation, but also identity concealment, providing banks and financial companies with the peace of mind that their customers are who they say they are. Our liveness detection is also passive for users, requiring no additional steps (such as prompted head movements) to be effective. Our liveness works for onboarding and authentication.

Mobile Authentication: Our solution provides password-free multifactor authentication using facial and voice biometric recognition and liveness detection and is based on NIST-tested face and voice matching algorithms. With our multimodal biometric capabilities, users can be authenticated with their faces, voices, or a combination of the two for even higher security.

Flexible Configurations: Besides supporting a full range of mobile and server-based operating systems, our solutions can be configured to be available in device-centric, server-centric, or browser-based. Device-based configurations place the biometric functionality onto a person's device and are ideal for situations where network availability is not guaranteed. Server-based configurations, however, place the biometric functionality on the server; a perfect solution for when network availability is strong. Our browser-based configurations serve as a third option, performing biometric capture directly through a browser, and placing additional functionality on the server. Whatever the choice, our solutions will continue to provide the same level of security and convenience.

Interested in learning more about Knomi? Visit www.aware.com/knomi/

AWARE

Sources:

1 https://medium.com/@rezaduty/2fa-security-issue-675a6dec825a
2 https://www.gartner.com/en/documents/3773163
3 https://www.yubico.com/blog/yubico-releases-2020-state-of-password-and-authentication-security-behaviors-report/
4 https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf
5 https://www.comparitech.com/blog/information-security/password-statistics/
6 https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-Enterprise-The-Password-Expose-Ebook-v2.pdf
7 https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Report-Infographic.pdf
8 https://www.weforum.org/reports/the-global-risks-report-2020
9 https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=4e662ce4bd54
10 https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
11 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
12 https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/
13 https://www.kuppingercole.com/research/lc80127/fraud-reduction-intelligence-platforms
14 https://www.aware.com/blog-enhance-multifactor-authentication-enterprise/
15 https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security
16 https://www.aware.com/blog-going-passwordless/