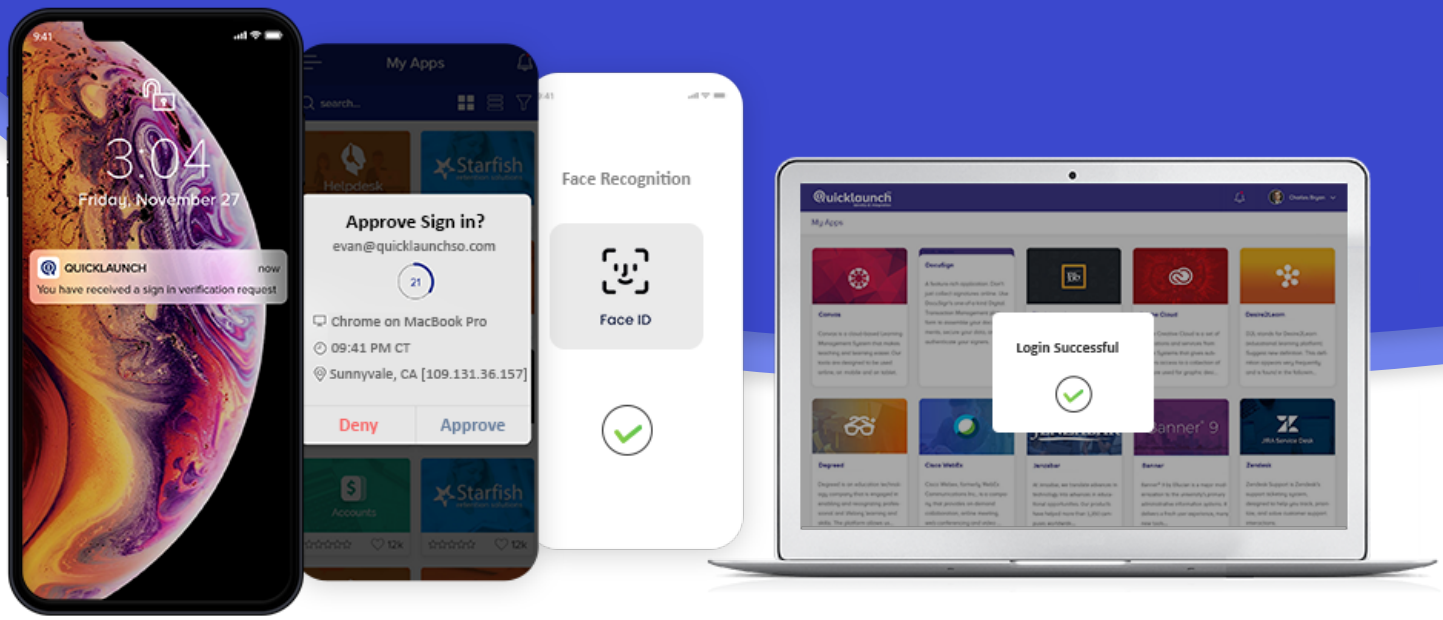
Quicklaunch™
identity & integration



PASSWORDLESS AUTHENTICATION

Introduction

The use of passwords for authentication purposes forces users to create and memorize complex amalgams of letters, numbers, symbols and cases; to change them frequently; and to try not to re-use them across accounts. Users have to manage anywhere from 25 to 45 passwords and their information sources and tools are exploding exponentially. Wanting to sign on to digital tools simply and efficiently, they are increasingly challenged and consequently tend to re-use the same passwords repeatedly.

Passwords are indeed at the heart of the data breach problem. According to the 2019 Varizon Data Breach Investigations Report, 80% of hacking-related breaches involved compromised and weak credentials, and 29% of all breaches, regardless of attack type, involved the use of stolen credentials. Such attacks participate in a thriving underground economy that further exacerbates the problem.

Are Passwords Really Outdated?

Usernames and passwords were invented back in 1964. Despite attempts to make static credentials more secure by adopting 2FA (two-factor authentication), utilizing OTPs, SMSs, or hardware tokens, organizations are still vulnerable to phishing attacks, keylogging and other forms of cyberattacks.

Corporations and institutions of higher education are aware of the security risks associated with shared or stolen passwords and they are looking for solutions to help secure their applications. The perpetual onslaught of breaches over the last decade has clearly shown that passwords have become more vulnerable than ever.

Millions of dollars are spent on authentication, but still, users across different organizations and institutions use passwords to login to their systems/applications. This is because traditional MFA products still rely on passwords, leaving an opportunity for hackers to steal those credentials. Therefore, it has become important for organizations to deploy a powerful login strategy than can fortify security.

Why Passwordless Authentication now?

While it is critical to build out a long-term strategy for authentication, experts concur that the next digital breakthrough will be passwordless authentication, primarily for security reasons but not only. Passwordless authentication offers four key advantages over traditional, knowledge-based authentication. First, it makes sense financially: it increases revenues and lowers costs. Second, it makes sense from a customer perspective, provides a better user experience. Third, from a strategic point of view, it can help redefine competition by unlocking value from interoperability. Fourth, as already mentioned, it greatly improves security.

Higher revenues, lower costs

Cybersecurity has been traditionally perceived as a cost centre, so the financial consideration is perhaps the most notable reason why companies should consider transitioning to passwordless authentication. Not only does it lower costs associated with password management and data breaches, it actually improves revenues through increased productivity and customer ratings.

Password reset overhead savings

Cybersecurity has been traditionally perceived as a cost centre, so the financial consideration is perhaps the most notable reason why companies should consider transitioning to passwordless authentication. Not only does it lower costs associated with password management and data breaches, it actually improves revenues through increased productivity and customer ratings.

Enhanced User Experience

Authenticating users through factors that they already possess, such as their mobile device (mobile authenticator apps, biometrics, SMS OTP) or laptop (Email OTP, Fingerprint, Face Recognition) enhance end user experiences with no lengthy passwords to remember.

Stronger Cybersecurity Posture

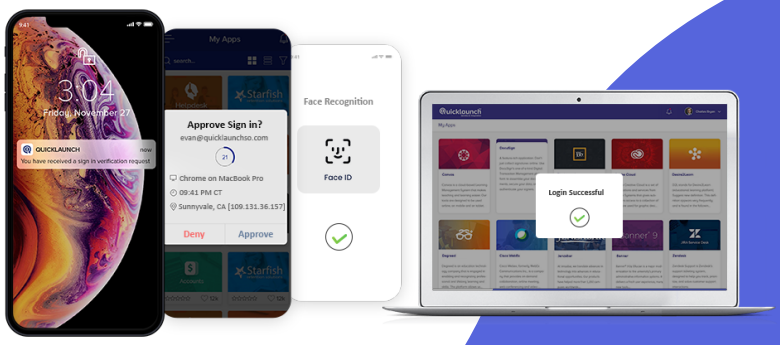
In passwordless authentication, passwords are eliminated altogether, thus offering protection against the two most prevalent cyberattacks: phishing and brute force attacks. In addition, in this authentication method, even when employees receive phishing emails or text messages, there are no credentials for them to offer up.

Quicklaunch™

identity & integration

QuickLaunch is the #1 leader in Identity and Access Management (IAM). More than 500+ organizations trust QuickLaunch's platform to manage over 2,000,000 identities and integrate over 3,000 applications worldwide. CIOs, CTOs, and CISOs use QuickLaunch IAM technologies to engage with IT staff, user groups, and organizations to help them automate their way into digital success. QuickLaunch's technology is vital in protecting the user experience, driving both operational efficiencies and higher productivity for your organization.

Schedule a Demo Today!



quicklaunch.io

+1 (844) 752 8624

QuickLaunch

@QLSSO

@QuickLaunchOfficial