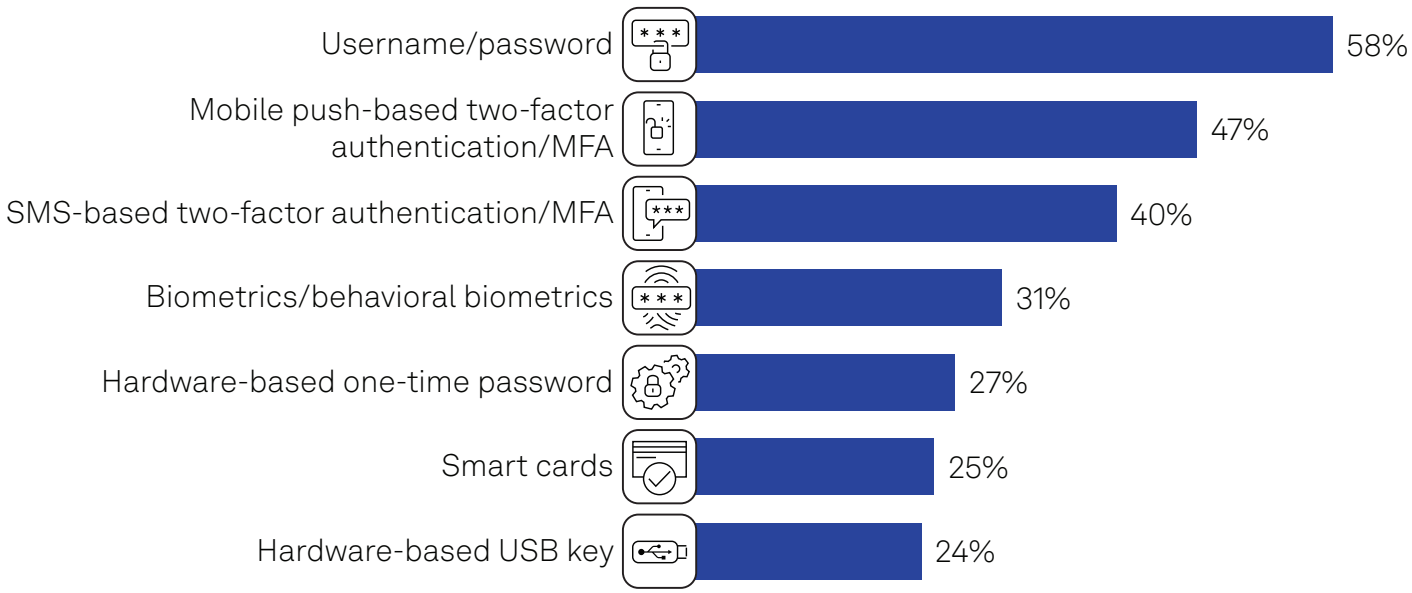
S&P Global
Market Intelligence
Business Impact Brief

Like it or Not, Passwords Are Here to Stay

The Take

The many shortcomings of passwords — the greatest being that they are hard to remember and easy to break — have been well-publicized for years. Yet while passwords can present substantial security risks, they are still common for a variety of reasons (simplicity, cost, flexibility, etc.), and most organizations will likely continue to use them for the foreseeable future. One reason is that other options have their own challenges. Two-factor authentication (2FA) and multi-factor authentication (MFA) methods, such as hardware tokens, biometrics and "passwordless" authentication, are more complex, may have suboptimal user experience and can cost more. Crucially, they also often lack support from many common applications (legacy applications and databases), protocols (RADIUS, LDAP) and resources (VPNs). Perhaps it's no surprise, then, that our survey data shows that the username and password combination (58%) remains the most widely deployed form of authentication by a substantial margin, well ahead of the second choice, mobile push-based authentication (47%).

Username-password combination is still the most widely deployed form of authentication



Q. Which of the following authentication form factors does your organization currently use? Please select all that apply.
Base: All respondents (n=461).
Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2022.

S&P Global
Market Intelligence
Business Impact Brief

Business impact

Passwords aren't all bad. Despite their shortcomings, passwords have some benefits that have made them "sticky." For example, they are relatively inexpensive, and they introduce little friction to user workflows and business processes.

Secure passwords require strong password management. The widespread use of username-password combinations necessitates that organizations have comprehensive password management policies, which can help ensure that employee password practices are as secure as possible. Password managers make it easier for both IT administrators and end users to create, rotate and store passwords, as well as 2FA and MFA codes.

There is no single authenticator to rule them all. There is a continuum of form factors that can be appropriate for different risk and security profiles, compliance mandates, user personas and use cases. Depending on where they are on their authentication journey, organizations are likely to use a broad variety of authentication methods, including passwords, that are appropriate and will work in specific settings. For example, even single sign-on (SSO) tools, while helpful, don't work with all applications and websites. Thus, at this time, it may be more accurate to think of passwordless options, such as passkeys, as a complement to passwords as opposed to a competing alternative.

Breaking up with passwords is hard to do. Despite making passwords more secure by ensuring that even if threat actors get hold of a working password, they won't be able to use it without an additional authentication factor, nearly every "stronger" form of authentication — hardware tokens, software tokens, smart cards, USB fobs, biometrics, etc. — comes with its own baggage, including up-front hardware and software costs, integration challenges and compatibility with applications and other IT resources.

Looking ahead

Initiatives around passwordless authentication have gained a lot of attention recently, in part, thanks to the momentum of the Fast Identity Online (FIDO) Alliance, the introduction of new passwordless authentication standards such as FIDO2, WebAuthN and CTAP, and the support of tech industry giants such as Apple, Google and Microsoft. However, it is still very early in terms of enterprise adoption of passwordless; only 31% have adopted it, according to 451 Research's Voice of the Enterprise data.

Passkeys — multi-device credentials that make it substantially easier for consumers to adopt FIDO-based authenticators — are garnering significant attention in the press and creating excitement. While passkeys hold promise and could be instrumental in the eventual widespread adoption of passwordless authentication, the key word is "eventual." We are very much in a hybrid world where passwords still reign supreme. For passkeys to become the norm, more websites must adopt them, and many sites (outside of the tech industry) have little motivation to change from traditional password-based authentication, particularly at the risk of degrading the user experience and introducing friction that could drive consumers away.

Until issues with passwordless authentication options — such as cost, complexity and user experience — are solved, username-password combos will likely remain a key part of the consumer and enterprise authentication landscape for the foreseeable future. It may take years for passwordless authentication to become dominant, so in the meantime, organizations should ensure that their users are practicing good password hygiene.