451 Research® Now a Part of S&P Global Market Intelligence | Business Impact Brief

Love 'em or Hate 'em, Passwords Are Here to Stay

The 451 Take

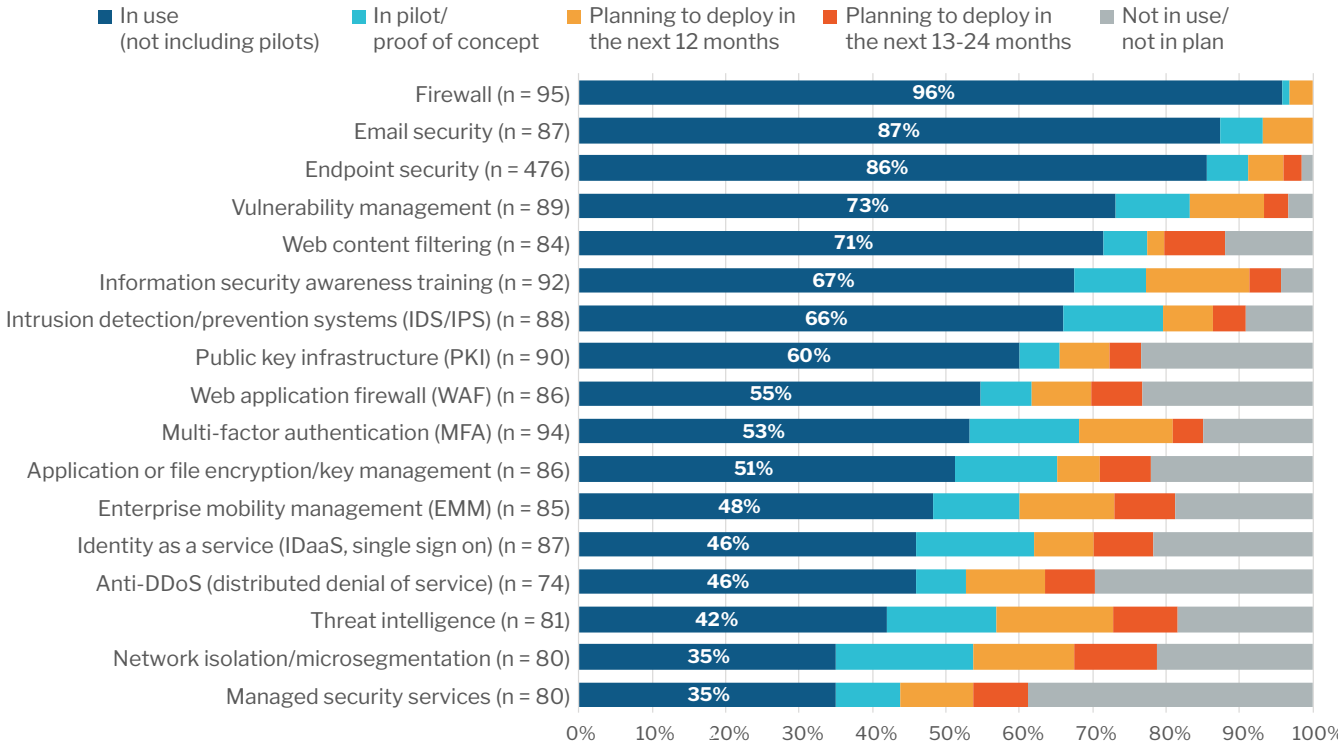
The drawbacks of passwords are well known – simply put, they can be hard to remember and easy to hack, and can be a general nuisance for both end users and security personnel. In recent years, there has been renewed focus on compromised credentials, which have become *the* primary attack vector in the vast majority of data breaches – 80%, according to the most recent Verizon Data Breach Incident Report. However, passwords remain a staple of many firms' security framework, despite the fact that the cybersecurity industry has been calling for the death of passwords for nearly for 20 years now.

Survey data from 451 Research's Voice of the Enterprise: Information Security service, however, shows that just 53% of enterprises have deployed multifactor authentication (MFA) – well below other common security tools like firewalls (96%), email security (87%) and endpoint security (86%). Further, it's likely that of those 53% of firms who do use MFA, deployments are not enterprise-wide, but reserved for just a subset of the total user populations and for specific use cases, like remote access VPNs. And most firms that have deployed MFA are still using passwords in some manner.

Initiatives around 'passwordless' authentication have gained a lot of attention recently, in part thanks to momentum of the Fast Identity Online (FIDO) alliance and the ratification of new passwordless authentication standards such as FIDO2 and WebAuthN and CTAP. However, the passwordless movement is still early on, and passwordless technologies that rely on these protocols can require changes to browsers, applications and devices in order to support public key cryptography.

Enterprise MFA Adoption Lags Popular Security Tools

Source:451 Research Voice of the Enterprise: Information Security, Workloads and Key Projects 2019



451 Research Now a Part of S&P Global Market Intelligence | Business Impact Brief

Business Impact

SOMEDAY PASSWORDS WILL DIE. Despite their shortcomings, there are also some benefits of passwords that have made them so persistent: they are cheap, and they impose little friction to user workflows or business processes. Factor in some of the potential issues around MFA deployment, and it's no wonder, then, that the percentage of enterprises deploying MFA has risen very slowly – from 51% to just 53% over the past three years – despite the growing threat of compromised credentials. In short, passwords are not going away anytime soon.

HORSES FOR COURSES. There's no 'one authenticator to rule them all' – every authentication form factor has its own pluses and minuses, and is more or less suitable for certain circumstances, user preferences and risk profiles. So there is room for multiple types of authenticators, and passwords will likely be a part of the equation.

SOMETHING YOU KNOW. Guidelines from the National Institute for Standards and Technology (NIST) advise organizations to use at least two of the three 'factors' that constitute strong authentication: something you *know* (passwords, PINs); something you *have* (phones, hardware tokens); and something you *are* (fingerprint or facial scan). As phones and biometrics become more common, there's a good chance passwords will be the second factor, and in that sense can be seen as a complement to other authentication form factors.

COMPOSITION RULES DON'T WORK. For years firms have been schooled on the notion of using complex passwords, and also rotating passwords at regular intervals. But adding an exclamation point or two won't decrease risk much, particularly if those passwords have already been compromised and are sitting in a cracking dictionary somewhere.

Looking Ahead

Over time the industry will gradually reduce its reliance on passwords. But the pace of this change thus far has been glacial, and will likely remain so. In the interim, then, there are several strategies or recommendations for firms that aren't ready to go completely passwordless. For starters, if passwords will be around, firms might as well keep them safe by following sound security policies and practices.

Firms should also adhere to current research and standards around password best practices. To that end, password policies should be event-based, not rules-based. Changing passwords based on the number of letters, symbols and numbers is no longer recommended by standards bodies such as NIST, largely because they have proven to be ineffective and cumbersome for users, not to mention creating a flood of helpdesk calls. Also, the complexity of passwords has been shown to have little impact on the effectiveness of credential-based attacks. What's more important is to be able to recognize when passwords become unsafe, and then be able to respond quickly when they do.

Passwords must be checked against up-to-date blacklists that include the latest data breaches and cracking dictionaries to prevent users from creating passwords that may be easy to guess, such as previously used passwords and other obvious and commonly used passwords like 'Admin123!' that would pass typical complexity rules. Passwords also need to be continuously checked – not rotated. Password audits used to happen every few months, but to maximize security, audits should be as frequent as possible – ideally updated every single day to limit the window during which the password is vulnerable.