451 Research

S&P Global
Market Intelligence **Business Impact Brief**

Overcoming the Hassle of Passwords and MFA with Passwordless Authentication

The 451 Take

The drawbacks of passwords are well known – simply put, they can be hard to remember, easy to hack and a general nuisance for both end users and security personnel. However, passwords remain a staple of many organizations' security frameworks, despite the fact that the cybersecurity industry has been calling for the death of passwords for nearly 20 years now.

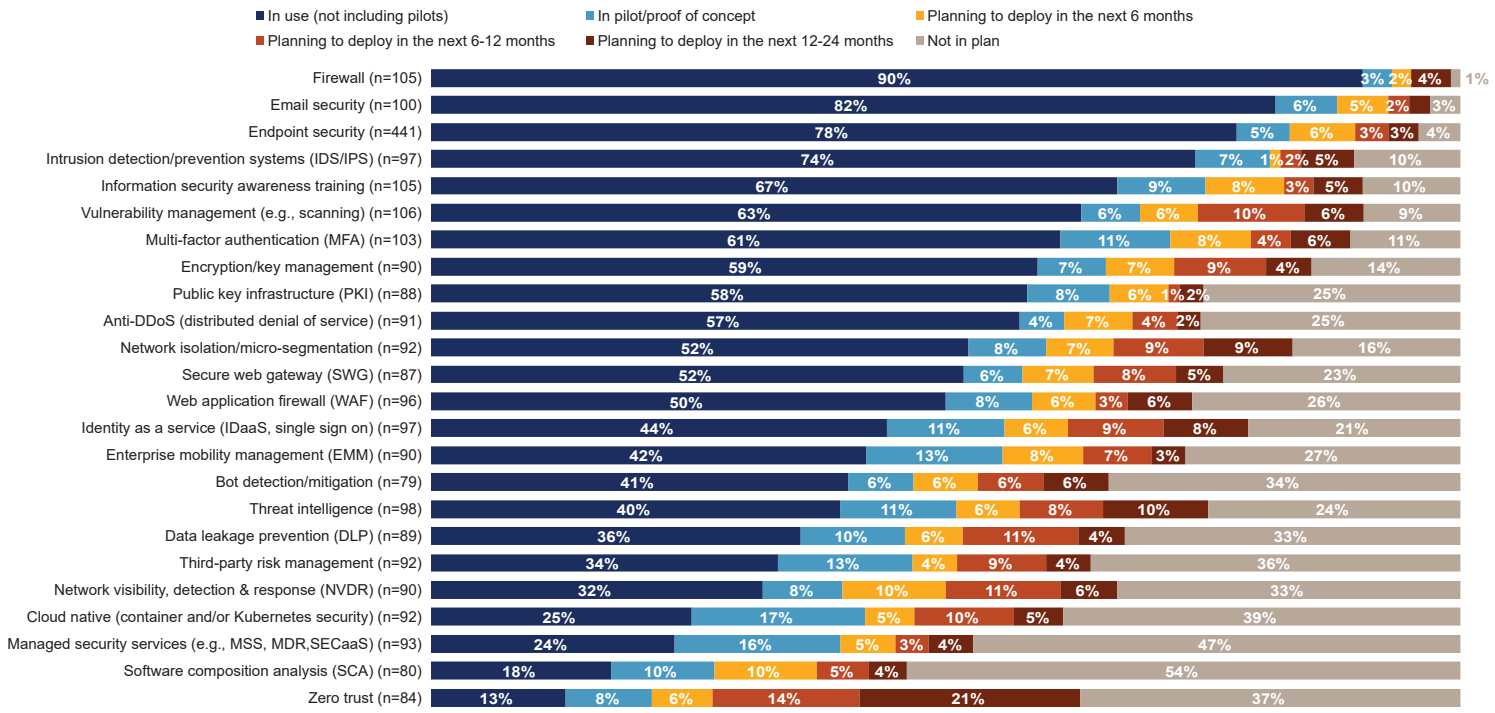
Survey data from 451 Research's Voice of the Enterprise (VotE) service shows that just 61% of enterprises have deployed multi-factor authentication (MFA), well below other common security tools like firewalls (90%), email security (82%) and endpoint security (78%). Furthermore, it's likely that within those 61% of firms that do use MFA, deployments are not enterprise-wide but reserved for a subset of the total user population and also mainly for specific use cases, such as remote access VPNs.

Enterprise MFA Adoption Lags Popular Security Tools

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020

Q. What is your organization's status of implementation for the following information security technologies?

Base: All respondents



451 Research

S&P Global
Market Intelligence **Business Impact Brief**

Business Impact

PASSWORDS ARE A HARD HABIT TO BREAK. Despite their shortcomings, there are also some benefits of passwords that have made them so persistent: passwords are cheap, and they impose little friction to user workflows and business processes. Furthermore, nearly every 'stronger' form of authentication – hardware tokens, software tokens, smart cards, USB fobs, biometrics, etc. – comes with its own baggage, in the form of up-front hardware and software costs, integration challenges, application support and – especially – user inconvenience. It's no wonder, then, that the percentage of enterprises deploying MFA has risen very slowly in recent years compared to other security tools, despite a boost from extended work-from-home (WFH) policies at many enterprises – and despite the growing threat of compromised credentials.

MFA DOESN'T ELIMINATE PASSWORDS. MFA is just a Band-Aid. In fact, most firms that have deployed MFA are still using passwords in some manner, and they often require users to type in a username or PIN, or both. And if you are still using passwords, you still have risk – not to mention the various user-experience issues and potential helpdesk costs for locked-out users or lost authenticators.

MFA CAN BE BYPASSED. MFA can be a helpful tool to provide added security, but it isn't perfect. Like other security tools, MFA is binary – you're either in, or you're out; there's no in-between. In a sense, MFA is like a bouncer at a night club – once you're in, nobody knows what you are doing while on the inside. And if an attacker gets hold of a compromised credential or bypasses the authentication process, a lot of damage can be done before the attacker is ever detected.

PASSWORDLESS IS THE NEXT 'BIG THING' IN AUTHENTICATION. Passwordless authentication aims to improve adoption by making stronger forms of authentication more seamless and allowing for a more positive user experience by completely eliminating passwords or other 'shared secrets' like usernames and PINs. Recent initiatives toward passwordless authentication have attracted a lot of attention in the past year or so, in part thanks to momentum of the Fast Identity Online (FIDO) Alliance and the ratification of new passwordless authentication standards such as FIDO2, WebAuthN and CTAP.

Looking Ahead

Passwordless authentication is the beginning, not the final destination. In other words, passwordless authentication should be viewed as just the first step on the journey toward the 'holy grail' of authentication – eliminating the tradeoff between usability and security. The immediate goal is to provide frictionless authentication that requires no typing or handling of a secondary device.

The ultimate goal, however, is to deliver an access control system that offers continuous, risk-based authentication. Such a system would take into account the identities of the users and their device(s), the users' behavior, the security posture of the device(s), and the risk of the applications and resources that are being accessed to prevent common attacks such as credential stuffing/reuse and password replay attacks.

But the journey won't be effortless, in part because there is tremendous institutional inertia around moving away from passwords. Furthermore, passwordless authentication can present its own challenges: passwordless technologies that rely on the FIDO protocols can require changes to browsers, applications and devices in order to support public key cryptography. As such, passwordless authentication can require an up-front commitment in terms of time and resources, but that commitment should pay off in the long run.