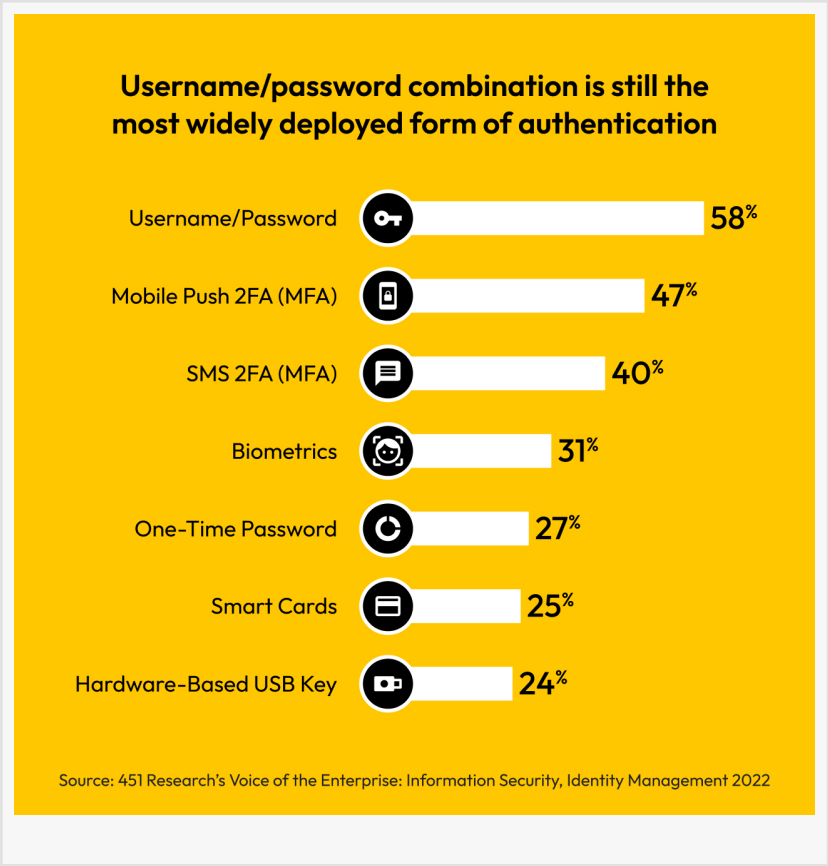
Like It or Not, Passwords Are Here To Stay

S&P Market Intelligence Business Impact Brief Finds Organisations Will Continue To Use Passwords for the Foreseeable Future



LONDON, UNITED KINGDOM, October 12, 2023 /EINPresswire.com/ -- Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords and passkeys, privileged access, secrets and connections, today released a S&P Market Intelligence report that demonstrates username-password combinations are still the most widely deployed form of authentication deployed in organisations (58%). The next most popular forms of authentication are mobile push-based MFA (47%), SMS based MFA (40%) and biometrics (31%).

"Passwords continue to reign supreme as organisations struggle to balance security with simplicity, cost of ownership and flexibility– particularly in hybrid working environments," said Darren Guccione, CEO and Co-Founder of Keeper Security. "SSO and passwordless authentication– although effective– are not universally supported, and therefore, create security holes that leave organisations vulnerable. It is crucial for organisations still relying on the password and username combination, or a hybrid model of passwords and passwordless technologies, to ensure they are managed appropriately and securely."

> It is crucial for organisations still relying on the password and username combination, or a hybrid model of passwords and passwordless technologies, to ensure they are managed appropriately"
>
> *Darren Guccione, CEO and co-founder at Keeper Security*

The S&P Market Intelligence Business Impact Brief indicates that the widespread use of username-password

combinations requires organisations to have comprehensive password management policies in order to ensure 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. In fact, many organisations use a combination of multiple authentication factors to complement password and username combinations, making this integration even more of a necessity.

Largely due to momentum of the Fast Identity Online (FIDO) Alliance, passkeys as a form of passwordless authentication are gaining traction with support from Apple, Microsoft and Google. Passkeys are passwordless credentials that make it substantially easier for consumers to adopt FIDO-based authenticators. However, in terms of enterprise adoption, passkeys are still in the very early stages.

“While passkeys present enticing security benefits, websites have been slow to support them for a variety of reasons. With more than a billion websites in existence, there is a long path ahead for any passwordless option to become ubiquitous,” said Guccione. “As password and username combinations will remain a key part of the enterprise landscape for the foreseeable future, password management solutions that integrate and support a wide range of authentication methods, whilst ensuring security and cyber hygiene, will be important for all organisations to boost cyber resilience.”

The full report can be downloaded here

Bethany Smith
Eskenzi PR
+44 7796 947620
email us here