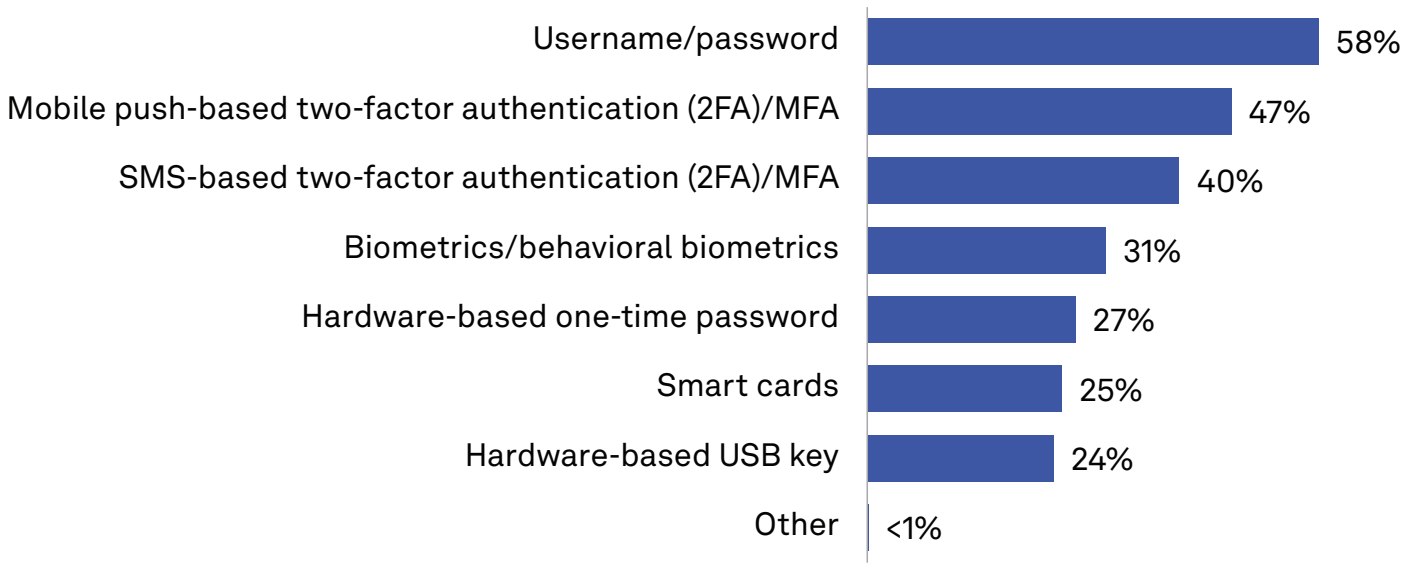
Secure Passwords Require a Stronger Password Policy

The Take

For years, passwords have been viewed as the bane of security, and their shortcomings — mainly that passwords are hard to remember and easy to defeat — have been well publicized. For sure, passwords can present substantial security risks if certain security measures are not followed. Yet for a variety of reasons (simplicity, cost, etc.), passwords are still common, and most organizations will continue to use them for the foreseeable future. In part, this is because the primary alternative to passwords — multi-factor authentication (MFA) — has its own hurdles to overcome, including complexity, user experience and lack of support by many common applications (e.g., some databases), protocols (RADIUS, LDAP, etc.) and resources (VPNs). Perhaps most importantly, however, passwords are often one of the multiple "factors" in MFA, namely "something you know." Thus, it may be more accurate to think of passwords as a complement to MFA as opposed to an alternative.

It is no surprise, then, that our survey data shows that username and password (58%) remain the most widely deployed form of authentication by a substantial margin, well ahead of mobile push-based two-factor authentication (47%), which likely relies on a password as the first factor anyway.

Passwords are still the most prevalent authentication method



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.

Business impact

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, user personas and use cases. Depending on where they are on their authentication journey, organizations are likely to use a variety of authentication methods, including passwords.

Secure passwords require a strong password policy. For most firms, the omnipresence of passwords in turn necessitates the creation and use of a strong password policy, which can help ensure that passwords are as secure as possible. When creating password policies, organizations should take various measures: They should obtain a list of compromised passwords from data breaches as the National Institute of Standards and Technology (NIST) has suggested, continuously monitor to detect when a "good" password is compromised and becomes "bad," and eliminate password management practices that have shown to be ineffective, such as requiring periodic password resets.

Privilege escalation is a big security challenge. As many recent studies have shown, most successful breaches involve stolen or compromised credentials and the escalation of privileges via lateral movement. While lateral movement and privilege escalation is frequently viewed as a privileged access management (PAM) problem, there are other ways to address this issue. One way is to provide more secure credentials up front and do more to secure them directly so lateral movement and privilege escalation becomes more difficult.

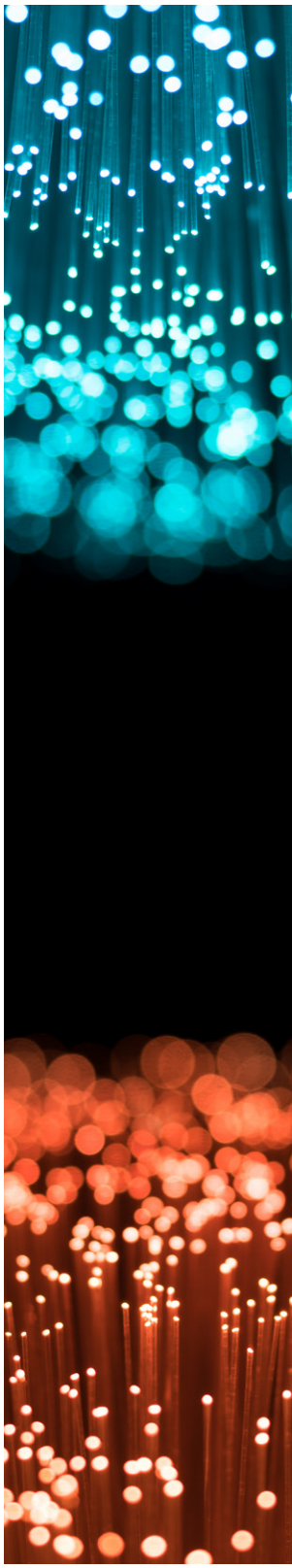
Securing Active Directory (AD) is one of the most crucial pieces of an organization's password policies. AD typically contains the "crown jewels" of an organization; thus, AD is one of the most common and effective targets for attackers. As such, companies need to pay more attention to AD security now than they ever have, partly due to the increase in ransomware attacks.

Looking ahead

Securing AD has become one of the top objectives for firms and a way to improve security quickly by addressing privilege escalation. Additional data from 451 Research's Voice of the Enterprise surveys shows that about a quarter of respondents use some form of third-party AD security tools. However, some AD password security features and tools are limited. They typically offer basic functionality such as prohibiting a user's name in a password ("Sarah123") or rudimentary risk scoring for passwords, but don't offer capabilities such as checking to see whether passwords have previously been compromised in a data breach or the ability to reevaluate passwords after they have been set.

Ransomware and other forms of malware are often introduced into the network via a single compromised password. Therefore, organizations that prevent compromised passwords are increasing their protection against ransomware and other forms of malware, ultimately stopping them from gaining a foothold as a precursor to moving laterally or escalating privileges.

Some organizations are enhancing what comes natively with AD or other tools to both meet compliance and regulatory guidance, such as NIST, and prevent password-related attacks. An AD password security offering may provide additional helpful features, some of which are required by NIST guidelines. These include the ability to detect passwords that have been compromised in breaches and continuous monitoring.



ENZOIC

Enzoic is a cybersecurity company committed to protecting accounts in Active Directory through compromised password detection. Organizations use the Enzoic for Active Directory tool to automate password policy enforcement and to comply with NIST password guidelines. The plugin also includes continuous exposed password monitoring, which detects if a password is compromised when it is created and on a daily basis thereafter.