SpyCloud

Passwords are Dead; Long Live Passwords

Passwordless Authentication and the Fate of Passwords in the Digital Age

Introduction

The State of Passwords Today

Passwordless Does Not Mean More Secure

How to Use Passwords Securely

Conclusion

Introduction

Every couple of years technology pundits claim, "Email is dead," as a new digital communication channel vies to take its place. But the fact of the matter is, as much as users loathe email, it's not going anywhere soon because it serves its purpose. In fact, most channels and platforms that strive to reduce or eliminate email actually use email as a default communication channel – while expanding the attack surface.

We're seeing the same thing happen with passwords. Vendors are trying to solve password challenges by replacing them with alternative authentication methods, most recently passwordless solutions. What these vendors tend to dismiss is that passwords have been used for centuries, and they're here to stay for the foreseeable future for the simple reason that – like email – they serve a purpose. They are a simple, cost-effective, and ubiquitous security measure that is easy to implement.

The hard truth is: replacing passwords doesn't necessarily improve security. Deploying a new authentication mechanism that claims to eliminate passwords invites new and unknown problems while expanding the attack surface. Organizations that adopt passwordless solutions inadvertently trade a set of known challenges (that are completely addressable) with a set that are not.

Rather than deploy a new authentication solution, it may be more prudent to make sure passwords are solid and secure. This whitepaper will show you why and how to do just that, saving you time, money, and the operational headaches of ensuring user adoption.

The State of Passwords Today

Researchers trace the history of computer passwords back to the mid-1960s, but as a simple form of authentication – something the user knows – passwords have been in use for centuries. Case in point: the literary history of passwords includes William Shakespeare's *Hamlet* (when Bernardo exclaims, "Long live the King," which identifies him to a fellow guardsman) and the 18th century tale *Ali Baba and the Forty Thieves* (where "Open Sesame!" was used to open a sealed cave).

Today, passwords are a staple of modern life. People use them countless times a day for work, school, and personal and family business. Research on the average number of passwords per user vary widely from 20-30 to 100 or more – and these are for the accounts survey respondents remember creating! It's safe to assume that the average user has many more passwords they don't recall having since passwords are used not just as a standalone authentication mechanism, but also in tandem with other authentication methods, as we'll explain later.

Passwords remain prevalent because they are convenient and offer ease of use for both developers and users. Security decision makers are familiar with the need to balance security with ease of use. Perhaps the difference between authentication and other security controls is that user friction can extend beyond the workforce itself to include customers and thereby directly impact revenue.

Organizations are increasingly adopting rapid development processes to support and meet the business need for agility and innovation. Passwords offer a low barrier to entry for developers and users alike. It is much easier, less expensive, and less risky to incorporate password-based authentication in an experimental application that may or may not make it to market than it is to incorporate a proprietary solution that users may not trust.

"Most passwordless solutions default to passwords as a backup, which means ***passwordless authentication isn't passwordless after all ."***

Users are also accustomed to passwords. As much as they may complain about passwords, users know how to use them and how to reset them. User friction is minimal and generally accepted.

Unfortunately, passwords also have their challenges, due largely to the "human element." Most notably, rampant password reuse leaves enterprises and their customers at risk of account takeover (ATO). ATO occurs when a bad actor acquires another person's login credentials, most often by leveraging reused or similar passwords from previously breached sites, and uses them to gain access to an existing account. In a successful ATO, an attacker can do anything the legitimate user can do, and in the case of corporate accounts, they can move laterally across the organization in search of higher-level access. A worst-case scenario looks like some of the higher-profile ransomware stories that have been in the news: the attacker acquires an admin password for an account that isn't protected by additional security measures and is able to directly install ransomware onto the company's network. It's a devastating outcome for a relatively simple problem (a compromised password).

Passwordless Does Not Mean More Secure

Security vendors have responded to password risk in a number of ways, from developing new authentication methods (tokens and biometrics, for example) to combining more than one form of authentication (i.e. multi-factor authentication). Most recently, security vendors have offered passwordless authentication as "the answer" to password risk – but it introduces its own risks.

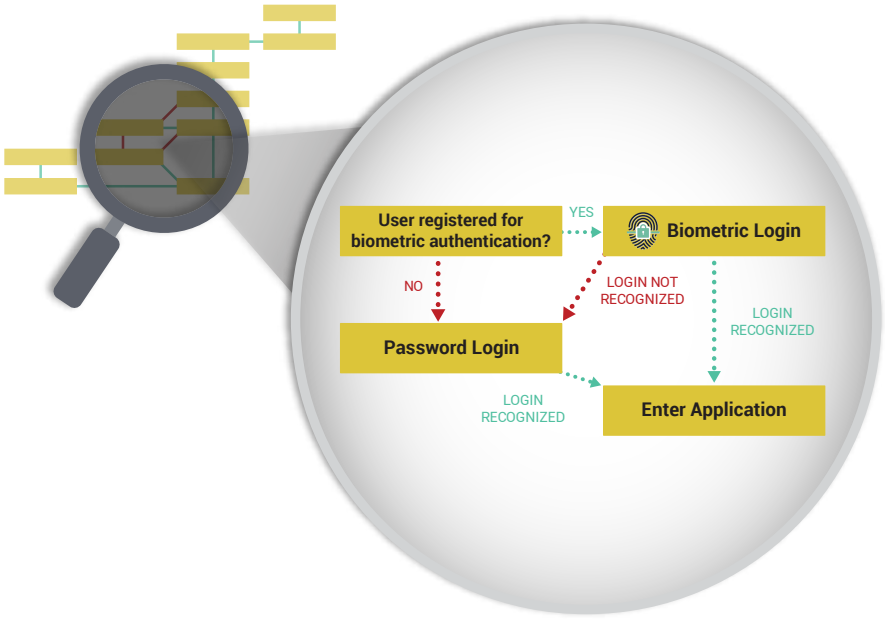
Passwordless authentication is (in theory) just what the name implies. It is a method of authentication that does not require users to enter (and therefore remember) a password. Instead, users are authenticated via a cryptographic key pair. When registering with an application or website, the user is assigned a public key. A private key is stored on the user's device. Most passwordless authentication implementations require users to enter their username and then provide an authentication factor other than something the user knows. This can be something the user has, such as a device, or something the user is, like a biometric identifier.

At first glance, passwordless authentication seems to be a promising alternative to passwords. However, it is not without its own challenges. Like any authentication mechanism, passwordless solutions must have contingencies. For example, what happens if the user's device is lost or stolen? In cases like these, **most passwordless solutions default to passwords as a backup, which means passwordless authentication isn't passwordless after all** – and is ultimately no stronger than a password, as it is still vulnerable to all the risks and threats associated with them.

> ***Gartner analysts stated that 'passwordless' isn't a panacea for every authentication need. For instance, some applications, like a financial account or highly sensitive data, should still require multifactor authentication with one of those being a password.***
>
> - CXOToday.com

43% cited cost, 41% storage of data required, and 40% time to migrate as the main challenges to implement passwordless, ***while 72% think that end users in their organization would prefer to continue using passwords, as it is what they are used to.***

Even in the rare occasion that a passwordless solution is indeed passwordless, organizations still have to contend with the fact that a lot of other services require a password or other knowledge-based factor in the backend. For example, users can bypass the biometrics and use a PIN to access their smartphone, and email systems also require a password.



Passwordless authentication is also a proprietary technology, which itself presents a variety of business risks. Organizations must consider the implications of vendor lock-in, the cost associated with the solution, deployment, management overhead, and additional technological requirements such as open channels, additional operating system resources, and more.

Then there's the additional risk posed by the security posture of the proprietary technology provider, which may introduce new threat opportunities such as an increased risk of a supply chain attack.

Users will also need to be trained on the new system and the proper resources put in place to ensure successful adoption. While users may initially be relieved to be password-free, any new process is likely to create user friction and irritation, especially as IT resolves initial problems.

According to a survey by LastPass: **43% cited cost, 41% storage of data required, and 40% time to migrate as the main challenges to implement passwordless, while 72% think that end users in their organization would prefer to continue using passwords, as it is what they are used to.**

It's important to note that no security technology provides perfect security, and attackers are quick to discover where weaknesses lie. The same goes for passwordless authentication. It won't take long for passwordless systems to become a target. Attackers will evolve their methods as they always do when a new technology or opportunity presents itself. Consider the coronavirus and the Covid-19 vaccine rollout. As early as March 2020, there was an onslaught of activity that leveraged the virus to manipulate users through various threat types,

from phishing campaigns impersonating public health officials to scams promising immunity. Attackers love a new challenge, and that's exactly what passwordless is. There may be a whole new game of "cat and mouse" as attackers poke holes in passwordless solutions and vendors scramble to secure them. Any novel authentication data can still be compromised, and in the case of biometrics, cannot easily be replaced. For example, a major breach in a biometrics system used by banks, UK police, and defense firms resulted in the exposure of fingerprints of over 1 million people, as well as facial recognition information and other personal information.

How to Use Passwords Securely

Fortunately, you don't have to deploy a new passwordless system to improve authentication. Passwords can work securely when you are proactive about protecting them. The key is securing them from day one – from the time of account creation (the start of your relationship with your customer or employee) and constantly from then on. This means that in addition to implementing smart password policies, organizations should continuously monitor for password compromises.

Why is continuous monitoring for password compromises so important? Stolen passwords stay valuable to criminals for years, due largely to the prevalence of password reuse. And because passwords are often reused, your organization doesn't have to experience a data breach to be affected by a cyberattack. It's therefore critical to stop peoples' most predictable behaviors. One way to do so is by monitoring for compromised passwords, quickly remediating them, and preventing users from reusing passwords or variations of passwords that have ever been compromised – regardless of whether it was in association with a particular email address or username.

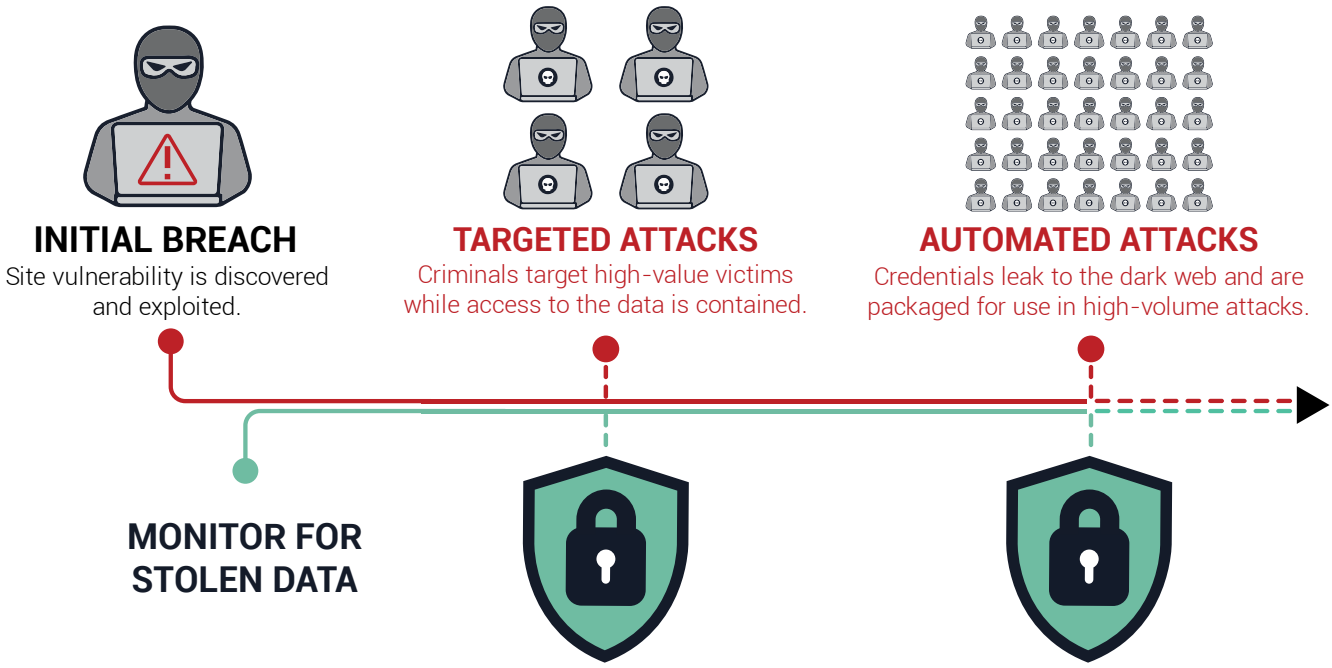
Let's examine how attackers leverage passwords throughout the breach lifecycle to illustrate why continuous monitoring and automated remediation of exposed passwords – which is neither cost-prohibitive nor resource-intensive – is critical:

Immediately following a breach

When a breach exposes passwords, attackers share the stolen data within a very small group of trusted associates who help them monetize it. This period of time can last as long as 18-24 months. Targeted attacks including MFA bypass and ransomware are prevalent. This is the most profitable time for cybercriminals, and the most dangerous for data breach victims, so time is of the essence. It's critical to identify stolen credentials early in the breach timeline, when they are most valuable to criminals and pose the largest risk to the business. Head that off with proactive password checks to negate the value of that stolen data.

After 24 months

At this point, criminals package the old breach data into combo lists to sell on the dark web. This is typically when dark web scanners pick up the data and incorporate it into their credential check databases. Attackers who buy the data use it for automated attacks, like credential stuffing. By feeding stolen credentials into automated tools, attackers can easily test credential pairs against a number of websites to see which additional accounts they can take over. Access to a victim's streaming media service may not prove terribly valuable to an attacker, but when those same credentials provide access to a bank account or sensitive corporate assets, it's a different story altogether. It's therefore critical that your users never reuse exposed passwords and that you prevent users from choosing any breached password (or variations of those passwords).



SpyCloud Tip

Do's and Don'ts of Human-Friendly, Secure Password Policies

In an attempt to mitigate password risks such as ATO, security organizations commonly adopt "strong" password policies, such as forcing password changes every 90 days and requiring long and complex passwords. Unfortunately, instead of improving password security, these password policies have the adverse effect of increasing user friction and encouraging password reuse.

Consider implementing the following password guidelines, as recommended by NIST:

- ✓ Do require a minimum password length of 8 characters.
- ✓ Do allow 64+ character passwords.
- ✓ Do limit failed login attempts.
- ✓ Do ban passwords that are commonly used, expected, or previously compromised.
- ✗ Don't require password complexity.
- ✗ Don't force arbitrary password changes.
- ✗ Don't use password hints or reminders.
- ✗ Don't use knowledge-based authentication.

In 2020 alone, SpyCloud recovered nearly 1.5 billion stolen credentials and operationalized them ***to protect hundreds of enterprises and over 2 billion employees and consumers from account takeover and online fraud.***

Conclusion

Passwords are here to stay – at least for now. They remain familiar, convenient, and prevalent. And while many businesses see passwordless authentication in their future, this technology too can be compromised. Fortunately, you don't have to deploy a proprietary authentication solution to improve password security and prevent credential-based cyber attacks.

About SpyCloud

At SpyCloud, we make it easier for organizations to automate password security in order to prevent account takeover and follow-on attacks like ransomware, business email compromise, and other forms of fraud. We reduce the effort it takes to keep corporate assets and users secure by recovering high volumes of stolen breach data at the earliest stage of the breach lifecycle, and making it easy for businesses to match logins, identify compromises, and remediate them – preventing exposures from becoming account breaches.

In 2020 alone, our team recovered nearly 1.5 billion stolen credentials and operationalized them to protect hundreds of enterprises and over 2 billion employees and consumers from account takeover and online fraud.