Security Intentions and the Persistence of Passwords

Black & White

May 2022

Commissioned by

bitwarden

451 Research

S&P Global
Market Intelligence

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners — what they are doing, and why they are doing it.

About the Author

Justin Lam

Data Security Research Analyst

Justin Lam is a Research Analyst in the Information Security Channel at 451 Research, a part of S&P Global Market Intelligence, focusing on data security. He has had variety of roles within established and emerging data security vendors over the last 15 years, both in technical and commercial functions. Justin holds a BS in Business from Carnegie Mellon University and is based in the San Francisco Bay Area.

Introduction

Before electronic computing, humans authenticated other humans based on what they had or what they knew. Anyone could have assumed any name, but handwritten signatures, seals from signets or knowledge of lineage were used to verify one's identity. Since shared computing arose, passwords have been used to distinguish users from one another. Passwords were designed to allow computers and networks to authenticate users based on a shared secret that only the human user knew and that the computer could verify.

Automated attacks by bad actors to brute-force-guess a legitimate user's password have pitted a computer's ever-increasing capabilities against a person's limited ability to recall strong, unique passwords. Users' defensive capability to recall strong, unique passwords has not kept up with offensive password-cracking capabilities. While national government guidelines such as NIST SP 800-63B itemize password management best practices, gaps between those best practices and actual user and enterprise behavior persist.

Most enterprise accounts are furnished with a username and secured with the user's password. Enterprise employees may have a large number of accounts provisioned to them – for example, for CRM, supply chain, finance, collaboration, email and messaging. Without enforcement of password uniqueness or password strength, users generally default to weaker passwords and even reuse them. The susceptibility of lost or easily compromised passwords across multiple enterprise accounts can be tremendously damaging to enterprises. Many enterprises and users may even know about these risks but lack the tools to mitigate them.

This report presents key findings and takeaways from a survey conducted by Bitwarden in conjunction with 451 Research (part of S&P Global Market Intelligence) to understand preferences and adoption trends with respect to password management in the enterprise. This study examines use cases, spending patterns and sentiment toward password managers, as well as related standards and their adoption. We uncover and reconcile tensions between security desire and action, priority and spending. The analysis also attempts to capture differences among user personas, industry verticals and firm sizes where possible.

We broadly define password managers as purpose-built programs that safely suggest, store and synchronize usernames, passwords and other authenticators. This may include programs installed in a variety of mobile, desktop and browser locations.

Key Findings

- Due to increased work from home, password managers have become one of the top security technologies.
  - More than half (57%) of all respondents use password management.
  - Another 15% said they would be adopting password management.
- Almost a third (29%) of respondents have had a security incident related to passwords.
  - Of those, 37% had significantly or somewhat impacted internal operations.
- To drive adoption, password manager usage should combine personal and business use cases.
  - Just over half (52%) of U.S. respondents chose password management on their own for personal and work identities.
  - Additionally, 46% of U.S. respondents said password management should be company-provided for employees both at work and home.
  - Similarly, 44% of U.S. respondents use and prefer a tool that enables use for personal and business passwords.

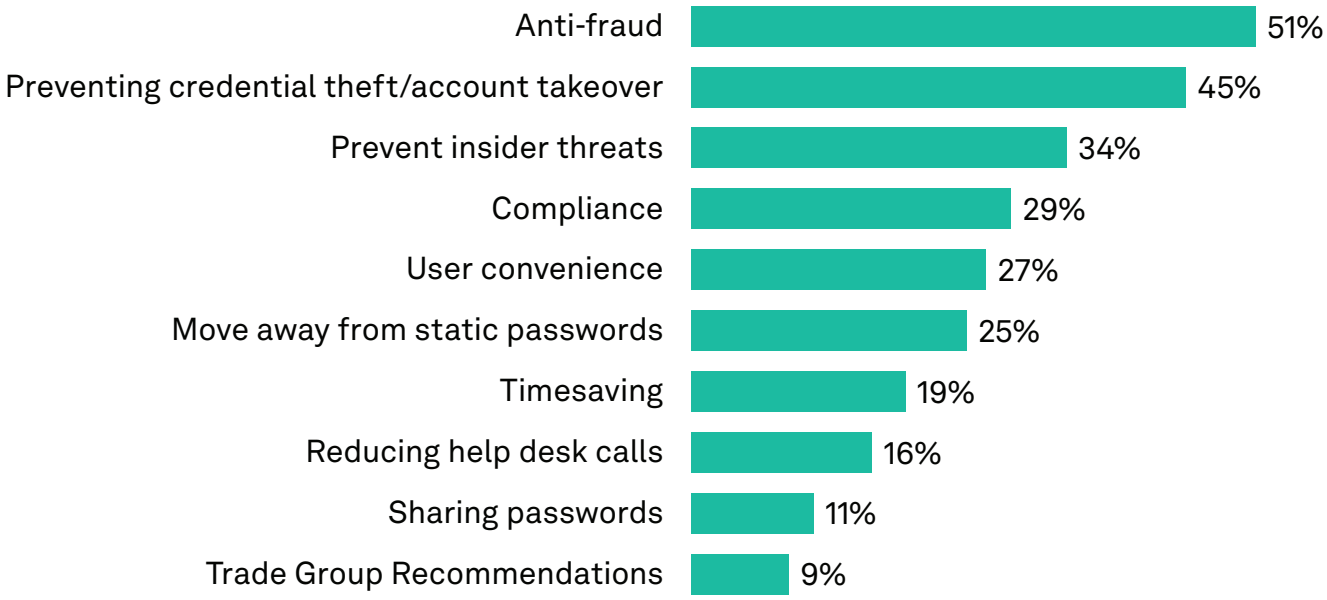
- Hard security costs are more important to justify password managers than soft productivity gains.
  - Account fraud was the top reason for password management, chosen by 51% of respondents.
  - Only 25% said "time saving" and 32% said "user convenience" were reasons to adopt password managers.
- There is misalignment between personnel risk level and adoption among current password manager users.
  - Over half (55%) of U.S. respondents said third-party users are the riskiest users.
  - Yet only 41% of U.S. respondents had deployed password managers to third-party users.
- OS- or browser-based password management comes at the expense of central auditability.
  - Browser- and OS-based password management were the most popular, at 53% and 39%, respectively.
  - Yet there are significant gaps in implementation policy and auditing: 45% of all respondents regularly audit password changes and have a strong password policy in their identity and access management (IAM) systems.
- Passwords are not going away.
  - A majority (55%) of respondents said password ubiquity keeps enterprises using passwords.
  - Meanwhile, 56% of USA respondents said that only 34%-66% of their apps use single sign-on (SSO). Many apps not using SSO means more username and password combinations.
- There is still confusion about what "passwordless" authentication is.
  - Almost two-thirds (61%) of respondents said one-time passcodes (OTP, SMS, email) are a form of passwordless authentication.

Budgets Spent vs. Benefits Perceived

Overall enterprise security spending continues to grow. According to the latest 451 Research Voice of the Enterprise (VoTE): Budgets & Outlook 2021 report, 86% of enterprises expect to increase their annual security budgets, 93% of enterprise respondents said they are maintaining or increasing their password management budgets, and 76% of respondents said they have deployed or plan to deploy password management because of work-from-home concerns. Identity and access management professionals said password managers are the best value for security investment; curiously, these IAM professionals ranked password management ahead of email security (anti-phishing) and user-awareness solutions.

When choosing password management, the impact of security consequences drives decision-making more than the positive usability incentives; the sticks exceed the carrots when justifying password management budget. In ranked choice voting, anti-fraud, preventing account takeover attacks and preventing insider threats were the highest prioritized reasons, chosen by 51%, 45% and 34% of respondents, respectively. In comparison, user convenience, time saving and reducing helpdesk calls were some of the least prioritized reasons, chosen by only 27%, 19% and 16%, respectively.

Figure 1: Main Reasons for Password Manager Adoption



Q: What are the main reasons for adopting password managers?
Base: All respondents (n=400)
Source: 451 Research's 2022 Identity & Access Management custom survey

Enterprises have been negatively impacted, with 29% of all respondents having experienced a security incident resulting from poor password management. Industries that have higher information security spending and higher security capabilities were impacted more. Technology companies, financial services and consulting companies had respective incident rates of 37%, 31% and 38%. Of all the respondents who experienced a security incident, 73% also had further impacts to internal and external operations.

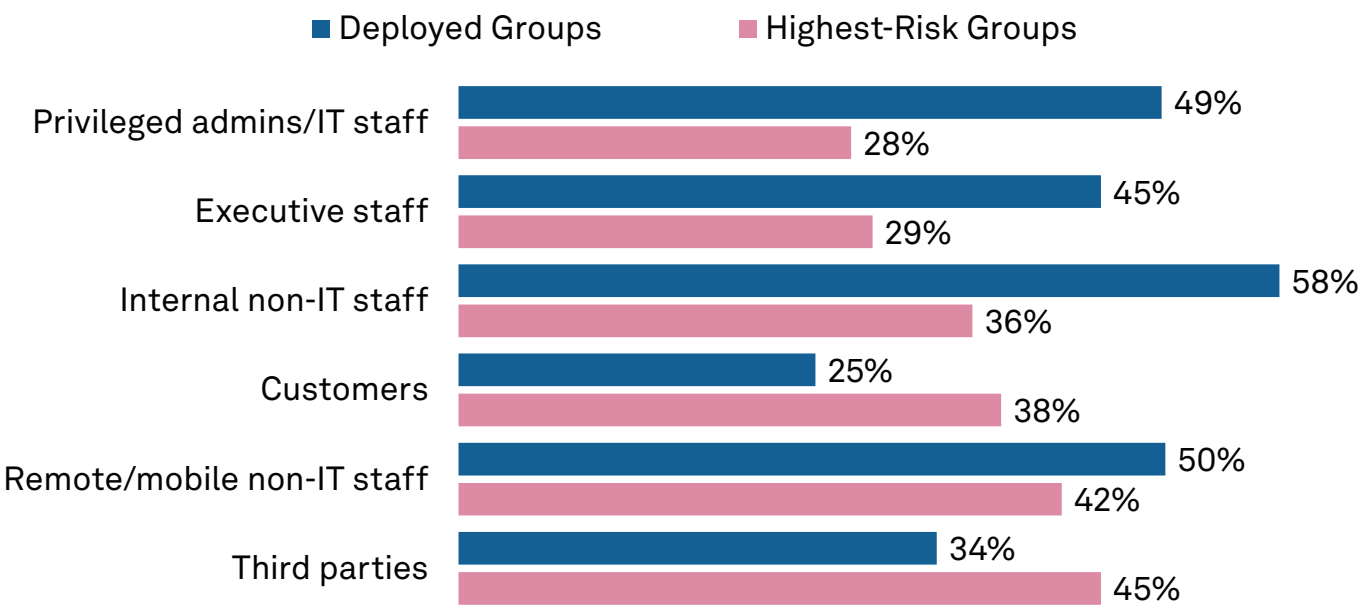
There remain obstacles to realizing value. In another ranked choice vote, respondents respectively selected user experience and management complexity at 29% and 36% as the largest barriers to successful password manager deployment. So, while security consequences justify investments in password managers, implementation is complicated by considerations of end-user experience and operation. In the next sections, the study examines whether this is impacting corporate adoption and keeping enterprises less protected.

Perceived Needs vs. Action

The study focused on midsize to large enterprises with more than 1,000 employees; 27% of respondents work for organizations with more than 10,000 employees. In addition, our study focused solely on employees and did not incorporate temporary, contractor or affiliate personnel who might have access to the same network resources. In general, we observed tension between perceived priorities and actual responses. Our respondents themselves were in roles within IT and security, and when asked which personnel were the riskiest users, they selected third parties (45%) and remote/mobile workers (42%) in ranked choice voting. Curiously, respondents consider administrators (28%) and executive staff (29%) to be the least risky, perhaps showing some confirmation biases because intuitively, IT administrators, IT security and executive staff have unique purview into and the power to affect all departmental and stakeholder activity.

The study asked which personnel have password management already deployed or would have it deployed next. Internal non-IT staff (general employees) were the most common choice in ranked selection, at 58%. The respondents gave lower priority to third parties (34%) and remote personnel (50%) – whom they had cited as 'riskiest' personnel – highlighting a gap between perceived needs and action. Privileged admins and executive staff were selected for password manager deployment at moderate percentages of 49% and 45%, respectively.

Figure 2: Risky Groups – Deployed Groups for Password Management



Q: Which of the following user groups do you consider the highest risk?
Q: Which user groups have you deployed password managers for?
Base: All respondents (n=400)
Source: 451 Research's 2022 Identity & Access Management custom survey

If enterprises are to better manage their risk, they should apply resources such as password managers proportionately to the highest-risk personnel. Acting upon the perceived needs will allow enterprises to reduce or mitigate negative security consequences faster and better. Because it is important to prioritize the security of riskier personnel, it is also important that password security for those personnel be easy to adopt. Successful password manager acceptance among riskier personnel remains critical to filling perceived exposure gaps.

User Productivity (Bottom Up) vs. Enterprise Security (Top Down)

Our study found a clear dichotomy between "top down" enterprise security concerns and "bottom up" usability concerns. When asked about password policies, 80% responded that password policies are sufficient protection for their organization. In the U.S., 88% of respondents said their password policies were sufficient. While standards such as NIST SP 800-63B are the basis for password policy, actual user adherence is an entirely different matter. Over half (57%) of all respondents identified user behavior as the number one barrier to implementing better password management practices.

Enterprises may initially think that they have password management capabilities available, perhaps either through browsers or operating systems. In ranked choice selection, the most popular password managers were part of a browser, such as Safari or Google Chrome, or they were part of the OS, via Windows Credential Manager or MacOS Keychain. Just over half (53%) of respondents identified browsers, while 39% chose OS-based password management. Yet despite the omnipresence of browsers such as Google Chrome and common operating systems such as MacOS, iOS, Android and Windows, 66% of respondents said it would be easier for employees to adopt better password practices if they were provided the appropriate tools. OS- or browser-based password storage may not be the easiest to use, especially in diverse environments. Users may have a mixture of browsers and OS for personal, mobile and professional devices. Passwords stored in iCloud Keychain are not easily available to the Windows or Android user. The inconsistent availability of passwords across platforms creates a negative user experience. With an increasing mix of work from home and further blending of personal and work devices and services, user experience for password management needs to be consistent throughout.

While the belief in password policies is high, the practice of performing password audits is weaker. About two in five (41%) respondents said they do not audit for password strength or reuse. So, while enterprise security ideally promotes healthy password behavior, verifying strong password use lags. Providing tools that safely store credentials and that are auditable and accessible across platforms would enable consistent user experience and consistent security practices. Top-level enterprise security desire should not be traded for better end-user experience. The theoretical top-level desire for enterprise security must address the bottom-up ease of adoption if it is to succeed. Addressing bottom-up user concerns and prioritizing good user behavior can only improve both audit and enterprise security outcomes.

Negative attitudes persist about end-user experience. When considering password manager benefits, just 16% of respondents said "reducing helpdesk calls." Yet there are significant numbers of helpdesk calls, with 56% of enterprises stating that password resets/password management make up 20%-60% of all helpdesk requests.

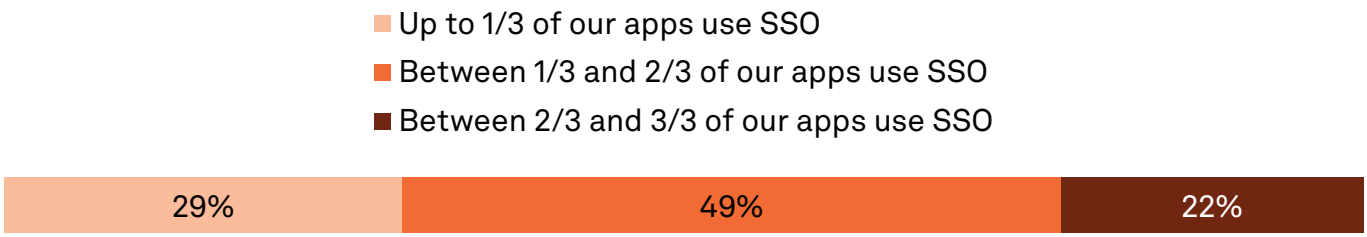
Fortunately, not all requests for improved user experience are being ignored. With work from home becoming more common even as pandemic restrictions subside, respondents acknowledge changing relations between employees and employers with respect to technology. In ranked choice voting, 54% of U.S.-based respondents cited employees' desire to use personally preferred services such as email and video conferencing over corporate standards, and 52% of U.S. respondents said that users preferred choosing a password manager for both work and personal identities. Nearly half (47%) of all respondents said that the company should provide tools for employees both at home and at work, and 59% would prefer a password management tool for personal and business passwords.

The Persistence of Passwords vs. Other Authenticators

This report has covered changing user experience and stricter security objectives. The trends are interrelated and should continue to be a push for greater password management adoption. Due to password theft or compromise, applications continue to adopt multi-factor authentication (MFA) such as one-time password (OTP), emailed codes, SMS, certificate and biometric factors. Almost all respondents (96%) indicated they are familiar with some form of these passwordless authenticators. Yet, 55% of all respondents said that passwords are ubiquitous.

Enterprises have also adopted single sign-on (SSO) solutions to improve both user experience and security. It is not a panacea yet, given that the number of non-SSO-compliant applications being added is increasing faster than ever. Almost half (49%) of respondents said that 34%-66% of their apps and logins were covered by their SSO solution. As work from home and personal application, identity, device and network usage increases, not all services can be covered by SSO. The authentication process for these apps outside of SSO control usually involves a username and password, with the password being the one common authentication factor.

Figure 3: SSO Adoption Approach



Q: How would you characterize your organization's approach to password management/SSO adoption?
Base: All respondents (n=400)
Source: 451 Research's 2022 Identity & Access Management custom survey

Furnishing password managers for personal and work use not only improves user productivity, but password managers also improve security outcomes. As cited in the FBI's Internet Crime report in 2021, aggressive social engineering and phishing/smishing/vishing targeting personal identities, devices and networks enabled more costly business email compromise incidents to transfer funds or make other false financial transactions. User experience and security need not be a tradeoff; the increase in applications, user diversity and work-from-anywhere trends continue to offer password management an opportunity to help users succeed and stay secure.

Looking to the Future

The obsolescence of the password has been predicted for some time. The FIDO Alliance, a broad standards group, is the latest and most significant attempt to move past passwords. FIDO's work with WebAuthn and biometric authentication is to ensure that authentication is easier with biometrics than passwords. There is still much work to be done, including the interoperation of multi-device FIDO credentials. Apple's Keychain system and its biometric usage found on iPhone, Mac and iPad demonstrate what multi-device FIDO credential interoperation might look like. That said, iOS still defaults to asking for a passcode to enable TouchID or FaceID.

Passwords have inertia. With more than 1.5 billion active iPhone users and more than 800 million active iCloud users, the underlying Apple ID account creation still requires a username and password combination. While passwords and passcodes may be used less with biometric or WebAuthn, passwords will continue to be a common means of authentication. Edge cases, such as account lockout, still require passwords. As such, passwords will still be worth stealing, cracking and abusing. The security challenges enterprises face in relation to password use have been around for quite a while, and they are not receding. Users must still have a solution to store these passwords across identities and devices in a work-from-anywhere world.

Conclusion

Enterprises must pay special attention to user experience for security to succeed. They also need to realize that end users are getting savvier in fits and starts. According to the Voice of the Connected User Landscape: Connected Customer, Trust & Privacy – Insight Report, 86% of respondents agree that having a single point of reference to manage their security and privacy preferences would improve their experience with any given online service. In other words, users who experience simple security are more likely to trust and engage with a given service. By making security simple via solutions such as password managers, security leaders can equip and enable users to succeed in their tasks and achieve overall security goals.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence