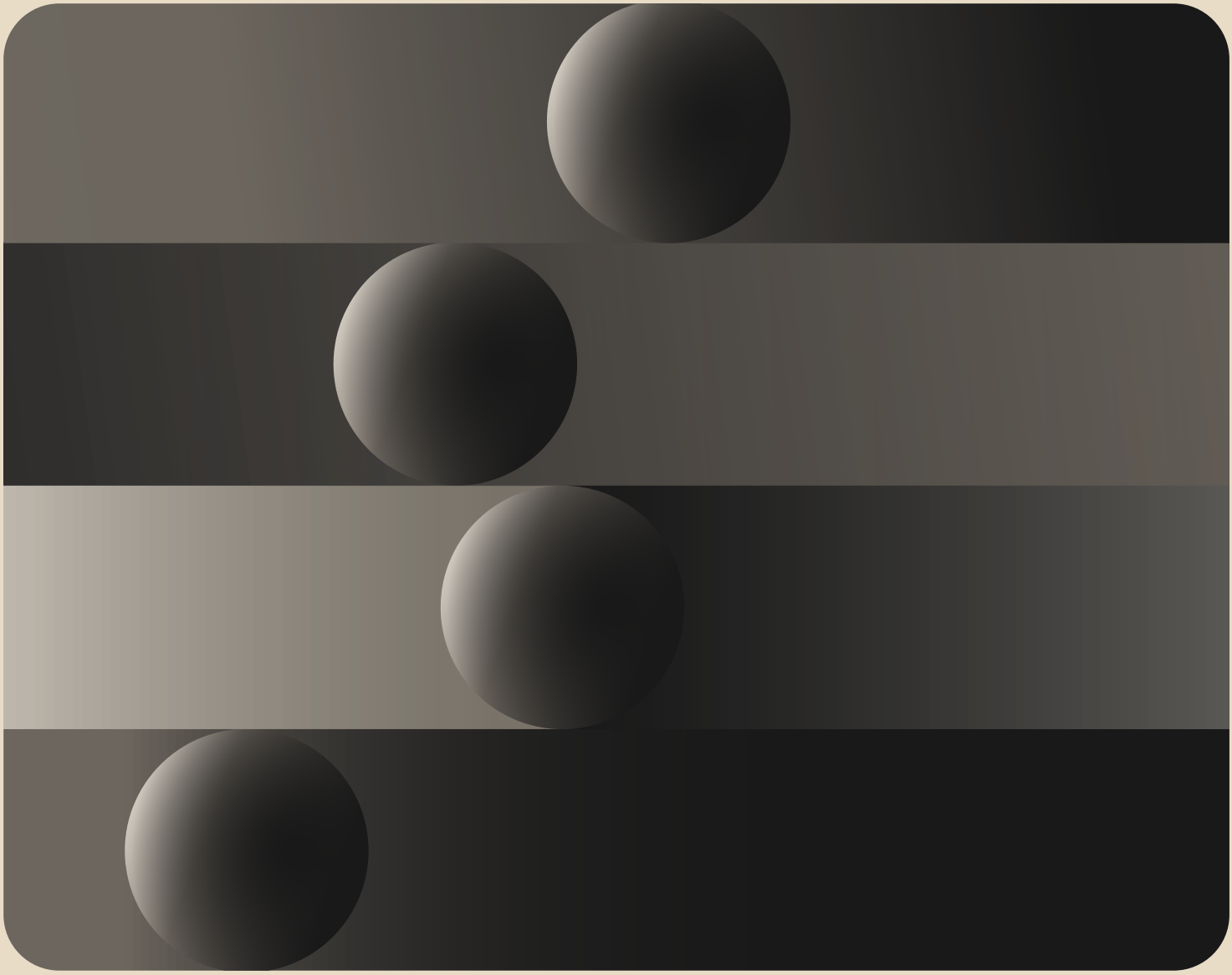
2023

An inside look at MFA adoption and the authenticators that influence it

The Secure Sign-in Trends Report



okta

A few years ago, the Okta team realized that we needed to completely rebuild our platform to better support passwordless, phishing-resistant access to all applications and data. That effort resulted in the Okta Identity Engine. Firing it up on release, it felt like the future had finally arrived.

We're now at the point where a significant number of workforce customers are using this platform, and it felt prudent to take a pulse on how customers were progressing.

Repeatedly, market surveys tell us that everyone is all-in on Zero Trust and passwordless access. I'm confident that Okta is well-positioned to enable that journey. But we can't hope to shape the future without having a firm understanding of the present. It's important to understand what our customers use to sign in today and how that impacts the user experience, hence this report.

We approached the study with scientific curiosity and a commitment to collaboration and transparency, two of the key values we promote at Okta. Through our analysis of normalized and anonymized data, we now have a much clearer understanding of how to evaluate the user experience and security attributes of any given authenticator. This offers vital clues for guiding our customers' journey to passwordless.

I hope you find the insights as valuable as I have.

Todd McKinnon
CEO, Okta

Table of contents

First, a word on measuring MFA adoption

Before you dive in, it's important to understand that the data and conclusions in this report reflect the authentication choices made by organizations, their administrators, and employees. While we frequently refer to users, these users are typically employees in a workplace setting and their authentication options are often limited by organizational policies.

There are multiple ways to measure multi-factor authentication (MFA) adoption, as outlined in the table below. For this study, we measured adoption for actual MFA usage: the percentage of users who signed in using MFA over a given period.

Measurement option	Definition
MFA Attach Rate	% of customers that have purchased a SKU that includes MFA
Org-Level Enrollment Rate	% of organizations that have configured MFA for use
User-Level Enrollment Rate	% of users who have enrolled in MFA authenticators
User-Level MFA Use	% of users who signed in using MFA over a given period

We also chose to aggregate MFA usage data at the user level, given that we are attempting to measure user adoption:

Aggregation option	Definition
Organization-Level MFA Adoption Rate	% of Okta customer organizations with users who signed in using MFA at least once during a month
User-Level MFA Adoption Rate	% of users who signed in using MFA during a month
Event-Level MFA Adoption Rate	% of successful sign-in events that involved an MFA challenge during a month

It's also important to keep in mind that this study only counted direct MFA authentication events in the Okta Workforce Identity Cloud (WIC). If users authenticate using MFA provided by other Identity providers and make use of enterprise federation or social login to connect to Okta, they are not captured by our MFA adoption data. Therefore, it's likely that the reported MFA adoption rate will slightly underestimate the overall rate of MFA use among our customers. We have also excluded test accounts. All adoption and metric data is derived from revenue-linked production organizations.

Authenticator usability and security properties

To best understand the hurdles to MFA adoption, we first must answer some foundational questions: Can we develop a framework and provide a systematic, quantitative view of authenticator properties? Can we use data-driven insights to educate our customers on better protecting their organizations and guiding product development?

For this task, we evaluated authenticators from both usability and security perspectives, as shown in Table 2. Measuring these criteria is a challenging task, given that the logic and user interface (UI) flows of each authenticator vary and can be highly customized. To achieve consistency, we leverage our newly updated Okta Identity Engine (OIE), which provides better-designed and more flexible Identity experiences and flows.

We measured the properties of the following authenticators: password, email, hardware one-time password (OTP), push, security question, SMS, soft token, voice OTP, Okta FastPass, and FIDO2 WebAuthn. Unless otherwise specified, we collected the data during January 2023 from revenue-linked production organizations of workforce customers using the Okta Identity Engine.

We took considerable care to develop data collection methods that allow for apples-to-apples comparisons between authenticators. This report highlights conditions that complicate these comparisons and explains the implications for our results. We also checked for month-to-month variations in the data to ensure the general trends were consistent over time.

Summary of key findings

MFA adoption continues its upward trajectory

As of January 2023, MFA adoption climbed to 64% among Okta workforce users, while at least 90% of administrators use MFA.

Like old habits, passwords die hard

Passwords might offer lower assurance, but they're difficult to shake. For a range of reasons, close to 100% of users still use a password at some stage.

Pandemic lockdowns drive record MFA adoption rates

MFA adoption by Okta's workforce customers jumped from 35% to 50% from February to March 2020, an increase of 15 percentage points. This was a remarkable leap, given the pre-pandemic annual growth rate was just 5%.

Adoption rates vary widely by industry and company size

Highly regulated industries, including government, healthcare, financial services, and energy, lag behind other industries for MFA adoption. Large enterprises also tend to have lower adoption rates than smaller organizations.

Security vs. user experience is a false choice

Phishing-resistant authenticators offer a superior user experience. In our authenticator performance and adoption assessment, Okta FastPass and FIDO2 WebAuthn came out on top as more secure and user friendly than other options.

Phishing-resistant authenticators show promising growth

Less than 4% of workforce users have adopted phishing-resistant authenticators, such as Okta FastPass and FIDO2 WebAuthn. However, the tide is turning. Over the past year, MFA adoption grew by 6%, and phishing-resistant authenticators accounted for over half of this growth at just over 3%.

Introduction

Authentication as a concept existed long before computers. Since at least the days of ancient Rome, when military guards would pass around secret “watchwords” to root out enemies in their ranks, organizations have relied on clever tools and tactics to prevent unauthorized access and protect sensitive information.

That holds true today, although the challenges have evolved. Modern organizations still need to ward off malicious intruders. But rather than enemies at the gate, they must fend off cyber crimes that cost businesses billions of dollars. And they also want to provide a better experience for their employees, contractors, and partners, who expect easy access to critical apps and accounts from any location. In this new reality, passing around watchwords is no longer the ideal authentication strategy. But what is?

In this report, we explore the wide variety of approaches companies today are taking to verify their users’ identities and prevent unauthorized access. Based on anonymized data from Okta customers’ billions of monthly authentications, we've compiled a transparent assessment of the state of authentication today, identifying trends and analyzing approaches based on considerations such as industry, region, and company size.

The report reveals some surprising findings. One example is the rise of multi-factor authentication (MFA), which is now being utilized by 64% of the users we studied. But as the report details, MFA adoption has not been uniform; workers in tech have embraced it, while those in highly regulated industries like healthcare and finance lag behind. Our report goes beyond the numbers, offering possible explanations for the discrepancies. It also introduces phishing-resistant options, such as Okta FastPass and FIDO2 WebAuthn, which prove you can achieve secure authentication and a superior user experience at the same time.

Finally, we recommend that companies look for authenticators that support:

- Frictionless authentication
- Fewer sign-in errors
- Easy user enrollment
- Resistance to phishing attempts

With this report, we aim to give security and IT professionals a data-driven perspective on the solutions available today and to dispel the myth that phishing-resistant authentication must translate to extra friction for users. In fact, the opposite is true. To discover more key takeaways, and to dive into the data behind them, read on.

All data and conclusions in this report are based on our analysis of anonymized Okta data unless otherwise noted.

How to use the data

This report provides a framework for measuring the usability and security properties of a comprehensive list of authenticators. We asked critical questions to help CIOs, CSOs, and policymakers understand the *why* behind the varying rates of MFA adoption. These questions include:

- How has MFA adoption changed over time?
- Does an organization's industry group, location, or size affect MFA adoption rates?
- What observable usability features are relevant to MFA adoption?
  - How long does it usually take for a user to authenticate with any given authenticator?
  - How long does it usually take for a user to set up/enroll in any given authenticator?
  - How often do authentication events fail using any given authenticator?
- What observable security features are relevant to MFA adoption?
  - How much coverage does any given authenticator provide for phishing-resistant authentication flows?
  - How often do adversaries target accounts using any given authenticator in brute-force attacks?

The answers to these questions can help IT and security leaders weigh the costs and benefits of different authenticators to determine the best solution for their organization and users.

“At Okta, we’ve undertaken our own journey to passwordless, phishing-resistant authentication. The benefits have been borne out in multiple failed attacks that have been directed at our own organization.

Our users, meanwhile, have adapted to modern authentication options like FastPass and security keys with ease. Enforcing these stronger, more streamlined authentication flows opened up numerous possibilities, including shorter reauthentication intervals, higher fidelity detection opportunities, and protection against several categories of attack.”

David Bradbury
Chief Security Officer

okta

Current state: MFA adoption

MFA is widely considered to be an essential part of any high-assurance security posture. When signing in using MFA, a user must provide two or more distinct factors to verify their Identity. Those factors include something you know (a “knowledge factor” such as a password), something you have (a “possession factor” such as a registered device), or something you are (an “inherence factor” such as a biometric).

While MFA is generally regarded as table stakes for secure sign-in, multiple internal and external factors influence its adoption. In this section, we examine adoption rates over time as well as by region, industry, organization size, authenticator type, and admin status. The results serve as both a benchmark to gauge organizational and industry progress and to identify areas for improvement.

Current state: MFA adoption

MFA adoption over time

Figure 1 shows MFA user adoption rates for Okta Workforce Identity Cloud customers — those who use Okta to provide employees, contractors, and partners with secure access to corporate resources — from October 2019 to January 2023. Each data point represents the MFA adoption during that month.

Our data reveals that MFA use rose sharply in February 2020, which correlates with the first COVID-19 pandemic lockdowns. From February through March 2020, the MFA adoption rate soared from 35% to 50% as organizations quickly pivoted to remote work and sought to secure a perimeter that now extended well beyond the office.

A jump of 15 percentage points over two months is truly remarkable, especially considering that it would have taken over three years at the pre-pandemic growth rate of 5%.

Moreover, the MFA adoption rate continued to rise at 6% year over year — even after we'd put the worst of the pandemic behind us — reaching 64% in January 2023. ■

Key insight

MFA authentication has steadily gained traction across organizations and industries, largely due to its critical role in mitigating cybersecurity risks. External forces, such as the COVID-19 pandemic and highly publicized cyberattacks, also helped to drive adoption.

MFA user adoption rate over time

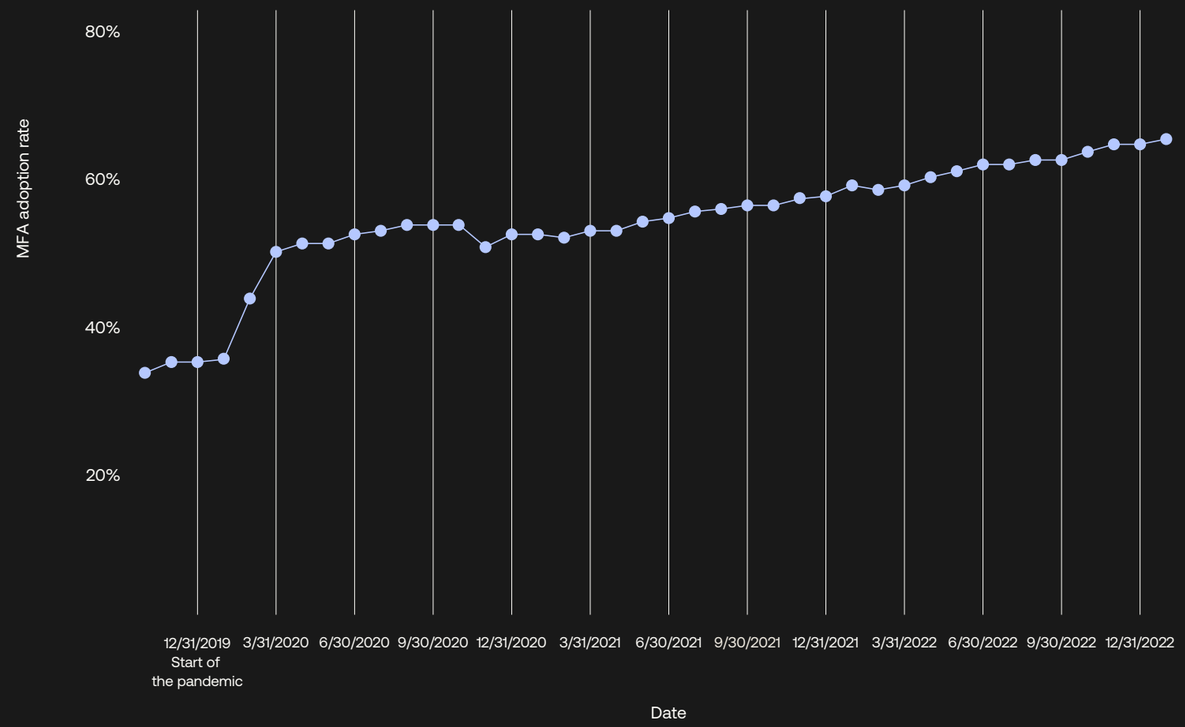


Figure 1: MFA user adoption rates from October 2019 to January 2023. The data reflects workforce use cases for Okta Workforce Identity Cloud and does not include data from Okta Customer Identity Cloud (formerly Auth0) or customer-facing use cases of the Okta platform.

Current state: MFA adoption

MFA adoption by region

This growth does not appear to be isolated to any region. If anything, MFA adoption rates by region are notable in their consistency and hover between 62–65% for AMER, APAC, and EMEA.

We can subsequently conclude that — within the regions we serve — the location of an organization and its users isn't a determining factor in MFA adoption, at least at the aggregated regional level. ■

MFA user adoption rate by region

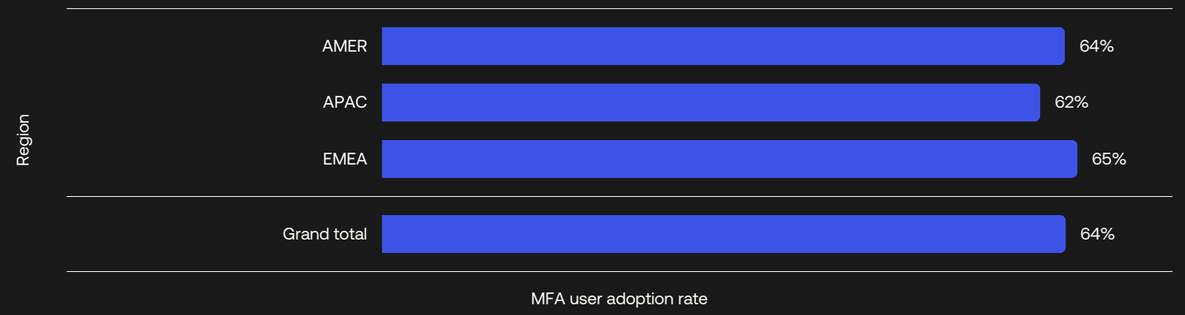


Figure 2: MFA user adoption rates in North, Central, and South America (AMER); Asia-Pacific (APAC); Europe, Middle East, and Africa (EMEA).

Current state: MFA adoption

MFA adoption by industry

MFA adoption varies widely by industry: A difference of 48 percentage points separates the industry with the highest adoption (technology) from that with the lowest adoption (transportation and warehousing). As is often the case, the technology sector plays the role of early adopter and continues to record the highest MFA adoption rate (87%) among Okta Workforce customers.

Where the data gets really interesting is when we travel down to lower adoption rates: Highly regulated industries, including government (48%)[1], healthcare (56%), financial services (60%), and energy (62%), lag behind less regulated industries, such as professional services (75%) and media/communications (72%).

Many organizations within more regulated industries rely on legacy applications that only support basic authentication, such as usernames and passwords, rather than more modern MFA methods. Additionally, the need to meet emerging compliance and regulatory requirements in these industries can often slow adoption.

At 48%, the MFA adoption rate for government organizations lags behind the private sector (64%) by more than 16 percentage points. Despite the low adoption rate, government agencies recognize the need to embrace MFA. Federal agencies must use MFA in the US, Australia, and many other countries. The US Cybersecurity and Infrastructure Security Agency (CISA) has repeatedly endorsed MFA and phishing-resistant authentication. And yet, successive audits of US agencies have unearthed inconsistent MFA implementation, leaving systems vulnerable to credential-based attacks. ■

[1] Government employees may use Personal Identity Verification (PIV) or Smart Card as third-party authentication methods and connect to Okta through enterprise federation. The government MFA adoption rate of 48% doesn't include the use case, and may underrepresent the real government MFA adoption rate.

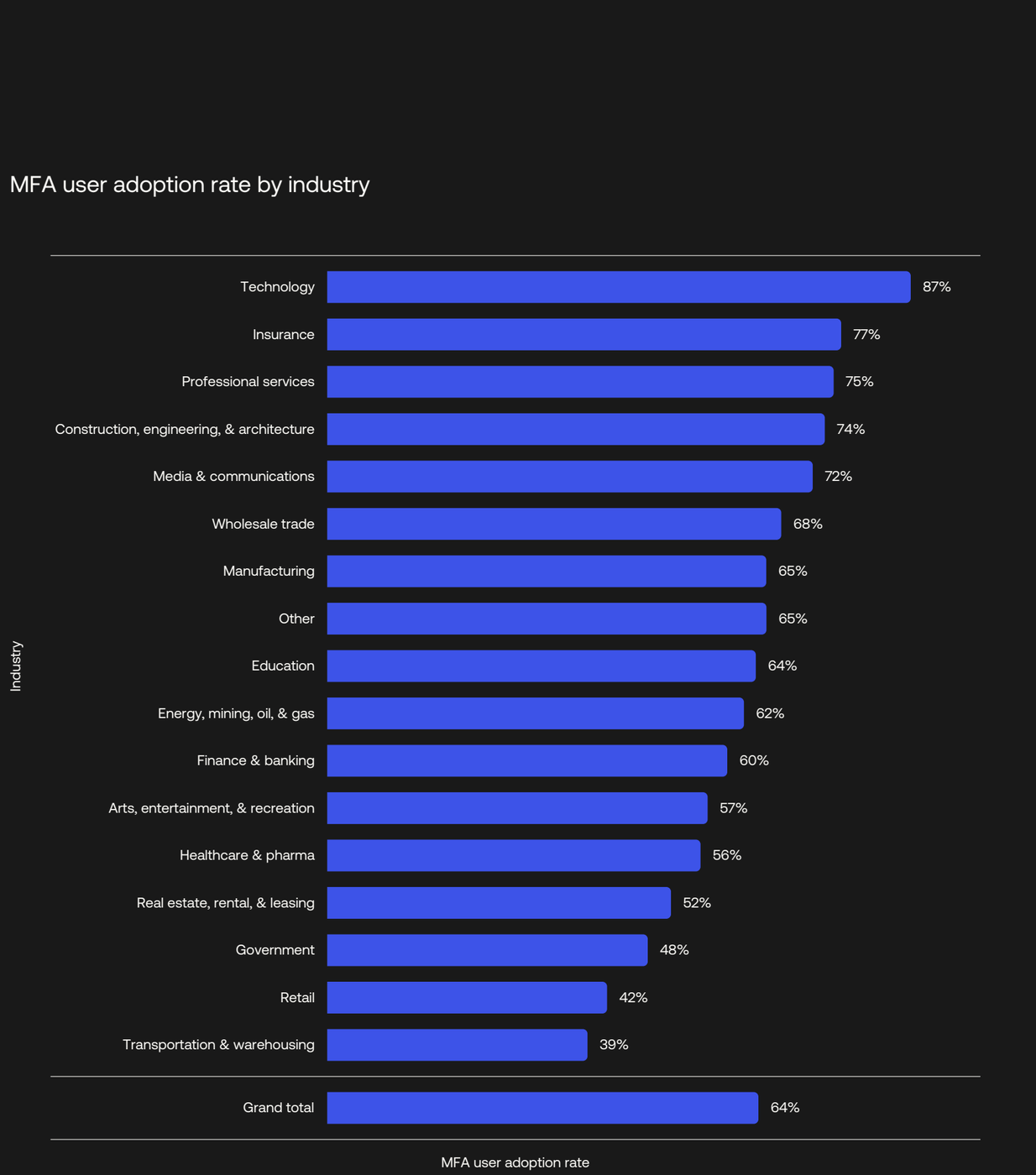


Figure 3: MFA user adoption rates across industries, listed in descending order by rate.

Current state: MFA adoption

MFA adoption by organization size

When we view MFA adoption by organization size, we see a rough inverse correlation between the number of employees and the rate of MFA adoption: The larger the organization, the lower the rate of adoption.

Organizations with more than 20,000 employees have the lowest adoption rate (54%), while those with fewer than 699 employees tend to have the highest MFA adoption (79%-80%).

Several factors may contribute to this adoption delta between large and small organizations: Similar to government and financial institutions, large enterprises may be slow to adopt modern Identity frameworks due to the complexity of replacing legacy infrastructure. Large enterprises are also more likely to use multiple Identity providers and may use MFA solutions other than Okta (again, our report only focuses on MFA usage on the Okta platform).

In either case, the lack of a centralized view of Identity and Access Management (IAM) is problematic. Large enterprises tend to be more sensitive to trust-eroding security events and should be more motivated than other organizations to pursue broad MFA coverage. ■

MFA user adoption rate by organization size

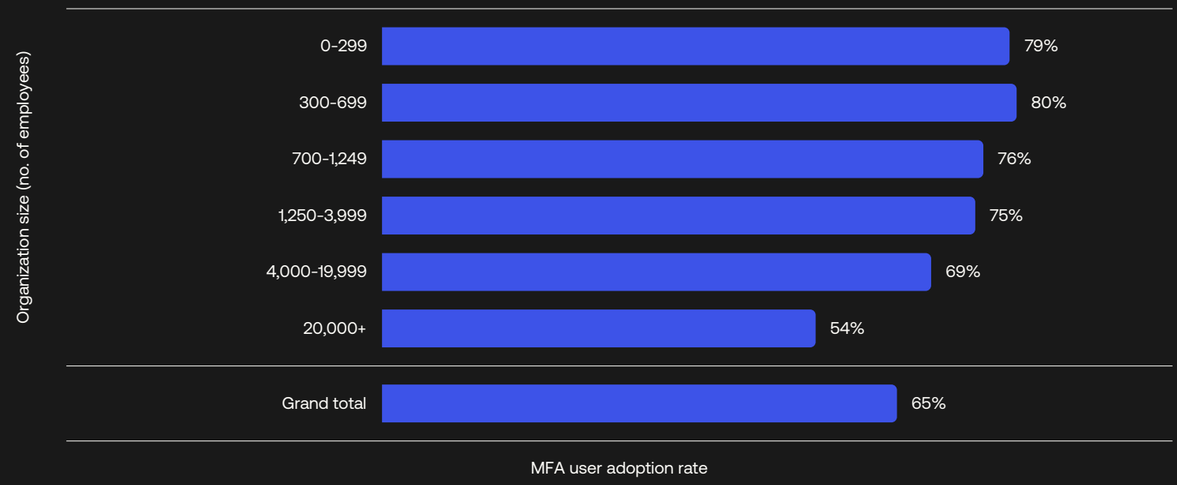


Figure 4: MFA user adoption rates across organizations of different sizes, listed in ascending order by number of employees.

Current state: MFA adoption

MFA adoption rate by authenticator type

We know that authenticators have different assurance levels, and passwords are near the low-assurance end of that scale. But just like old habits, passwords die hard. In fact, passwords continue their reign as users' primary authenticator: Close to 100% of users still use a password at some stage.

When looking at other MFA authenticators, Okta Verify Push (29%) is the most widely used, followed by SMS (17%), and soft token (13%).

Users have historically relied on the weakest forms of authentication due to a combination of platform limitations and admin preferences. The good news is that we're seeing promising growth in phishing-resistant authenticators, such as Okta FastPass and FIDO2 WebAuthn, according to Okta's Businesses at Work report.

Our current analysis shows that Okta FastPass has grown from 0% to 2% of Okta workforce users, an impressive jump considering the authenticator was made generally available in January 2022. FIDO2 WebAuthn adoption has also experienced sizable growth, doubling over the past year (from 1% in January 2022 to 2% in January 2023).

What's more, over half of the overall growth in MFA adoption (6% annually) can be attributed to phishing-resistant authenticators, which grew at a rate of slightly more than 3%. ■

"Factor" vs. "authenticator"

This report uses the terms "authenticator" and "factor" in accordance with the National Institute of Standards and Technology (NIST) definitions:

Authenticator: Something a claimant owns or controls and uses to authenticate their Identity.

Factor: An authentication property, e.g., a knowledge factor (something you know, like a password or security question), a possession factor (something you have, like an enrolled device), or an inherence factor (something you are, like your fingerprint).

Note: Every authenticator has one or more authentication factors. Often the terms are confused when "factor" is used instead of "authenticator," or when an authenticator can satisfy multiple factors. For example, Okta FastPass can provide both a possession factor (a registered device) and an inherence factor (using biometric verification).

MFA user adoption rate by authenticator

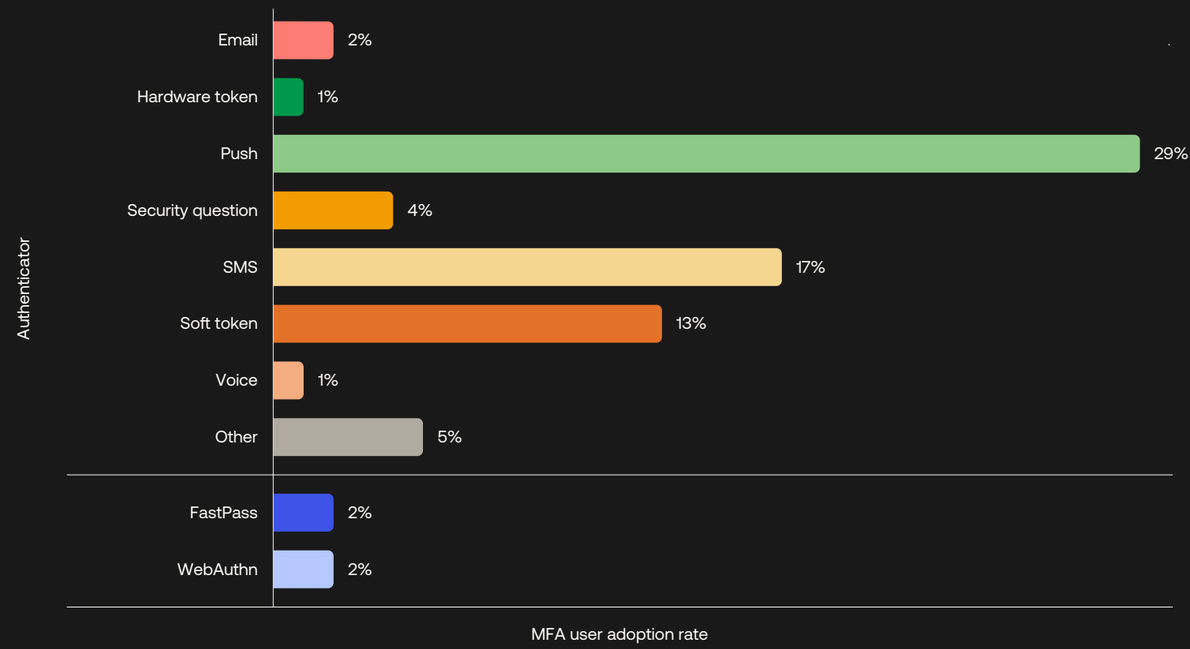


Figure 5: MFA user adoption rates for authenticators available on Okta Workforce Identity Cloud. The summation of the adoption rate for each authenticator is higher than the MFA adoption rate, given that users may authenticate with multiple authenticators.

Table 1: Authenticator types and properties

The table lists the authenticator types used to study MFA adoption, usability and security properties, and key authenticator characteristics.

Authenticator type	Authenticators offered by Okta	Authenticators used in the study	Factor type	Assurance level	Characteristics
Email	Email	Email: A combination of email code and magic link	Possession	Low	User verification
Hardware Token	YubiKey OTP, RSA SecurID, Custom TOTP	YubiKey OTP	Possession	Medium	Hardware protected User presence Device bound
Push	Okta Verify push, Duo	Okta Verify push	Possession Possession + Biometric	Medium	Hardware protected Device bound User presence/ verification
Password	Password	Password	Knowledge	Low	User verification
Security Question	Security questions	Security questions	Knowledge	Low	User verification
SMS	SMS, Duo	SMS	Possession	Low	User presence
Soft Token	Okta Verify OTP, Google Authenticator, RSA SecurID, Custom TOTP, Duo	A combination of Okta Verify OTP and Google Authenticator	Possession	Low	Device bound User presence
Voice	Voice, Duo	Voice	Possession	Low	User presence
Okta FastPass	Okta FastPass	Okta FastPass	Possession Possession + Biometric	High	Hardware protected Phishing resistant User presence/ verification Device bound
WebAuthn	WebAuthn, Duo	WebAuthn: A combination of Mac Touch ID, Android fingerprint, Windows Hello, YubiKey, Google Titan, Passkey	Possession Possession + Biometric	High	Device bound Phishing resistant User presence/ verification

Current state: MFA adoption

MFA adoption by user type

When we assess MFA adoption by Okta administrators, the numbers look healthier. A key contributing factor is that by default, MFA is required to access the Okta Admin Console.

Admins also tend to serve as role models for using phishing-resistant MFA. FIDO2 WebAuthn adoption among users with admin permissions grew from 6% to 8% over the past year alone, while the use of Okta FastPass among admin users grew from 0% to 5%.

But admins still have work to do to improve adoption rates among regular users, whose adoption rate lags 26 percentage points behind. Notably, admins play a key role in configuring which authenticators are available for user enrollment and how those are enforced. ■

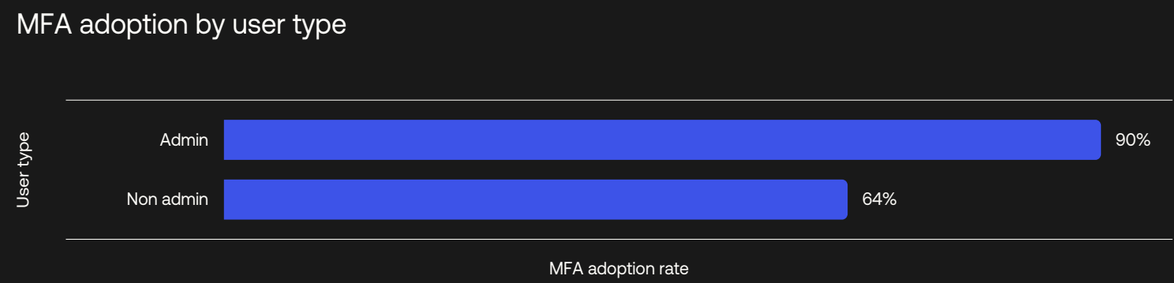


Figure 6: MFA user adoption rate for administrators and non-administrators.

Assessing authenticator usability and security

While MFA adoption is gaining ground, there are still hurdles that must be overcome. To help CIOs, CSOs, and policymakers make informed decisions on which authenticators to adopt, it helps to understand the benefits and drawbacks of each.

To this end, we developed a framework to assess authenticators on both usability and security properties; assessment categories are captured in Table 2. The results give us data-driven insights to help security and IT leaders better protect their organizations and guide product development. ■

Table 2: Authenticator usability and security assessment categories

Usability Properties	Definition	Usability Weight
Authenticator Challenge Duration	A measure of how long it takes users to successfully complete an authenticator prompt. Represented as a median.	10
Authenticator Enrollment Duration	A measure of how long it takes for users to enroll an authenticator, beginning when the authenticator enrollment page appears and ending when a user successfully completes the enrollment after following the instructions provided. Represented as a median.	1
Authenticator Challenge Failure Rate	The number of failed authentication attempts divided by the total number of authentication attempts received by back-end servers.	10

Security Properties	Definition	Security Weight
Authenticator Phishing-Resistant Coverage	The percentage of devices that can be protected by an authenticator that meets the NIST definition of phishing resistance.	10
Authenticator Phishing-Resistant Alert Coverage	The percentage of users who can be protected by an authenticator that is capable of logging authentication requests with failed origin checks and notifying users and admins (a common indicator of adversary-in-the-middle phishing attacks).	1
Authenticator Challenge Failure Rate	The number of failed authentication attempts divided by the total number of authentication attempts received by back-end servers.	1
Authenticator Challenge Brute-Force Failure Rate	The percentage of users with more than N failed authenticator verification events during a single day, expressed as a percentage of users who signed in using the same authenticator.	5

Assessing authenticator usability and security

Authenticator usability properties

Authenticator challenge time

Authenticator challenge time measures the median amount of time it takes users to successfully complete an authenticator prompt.

Password authentication shows a median challenge time of about six seconds. One reason for the short challenge time: Almost everyone is familiar with passwords. Also, due to the wide adoption of password managers and autofill, users can skip password typing altogether. In other words, the challenge time of passwords is biased towards a shorter value via the assistance of password managers.

For authentication flows that start with passwords, entering an OTP adds at least 13 seconds to the authentication flow, longer if the user must retrieve the OTP from an email or voice call.

Our data indicates authenticators that combine possession and inherence (such as biometric checks) offer the fastest challenge times. FIDO2 WebAuthn and Okta FastPass (as the name suggests) offer a dramatically more efficient authentication process than any other authenticator.

Passwordless, phishing-resistant authenticators such as Okta FastPass and FIDO2 WebAuthn also enable organizations to consider re-authentication at a higher frequency or as a step-up for access to sensitive apps. Both are critical defenses against session hijacking attacks. ■

A double take on passwords

We included challenge times for a password authenticator under two optional UI configurations:

- In the **usernames and passwords flow**, a user is presented with a username and password field on the same page at sign-in.
- In the **password-only flow**, a user enters their username on one page and is prompted to enter a password on the next page.

The median challenge time for the password authenticator in the password-only scenario is the best-suited condition to compare with other authenticator challenge times, given that the challenge times for all other MFA authenticators do not require the user to identify their account prior to the challenge. We nonetheless present both flows in the chart.

Key insight

How might this guide your decisions? If access to a workforce application requires two distinct factors (the minimum requirement for NIST AAL2), your best options for user experience (in terms of challenge time) should include FIDO2 WebAuthn or Okta FastPass, which conveniently deliver the best security outcome (phishing resistance) too.

These authenticators typically offer a possession factor and an inherence factor in under four seconds — several times faster than combining passwords with OTP-based challenges.

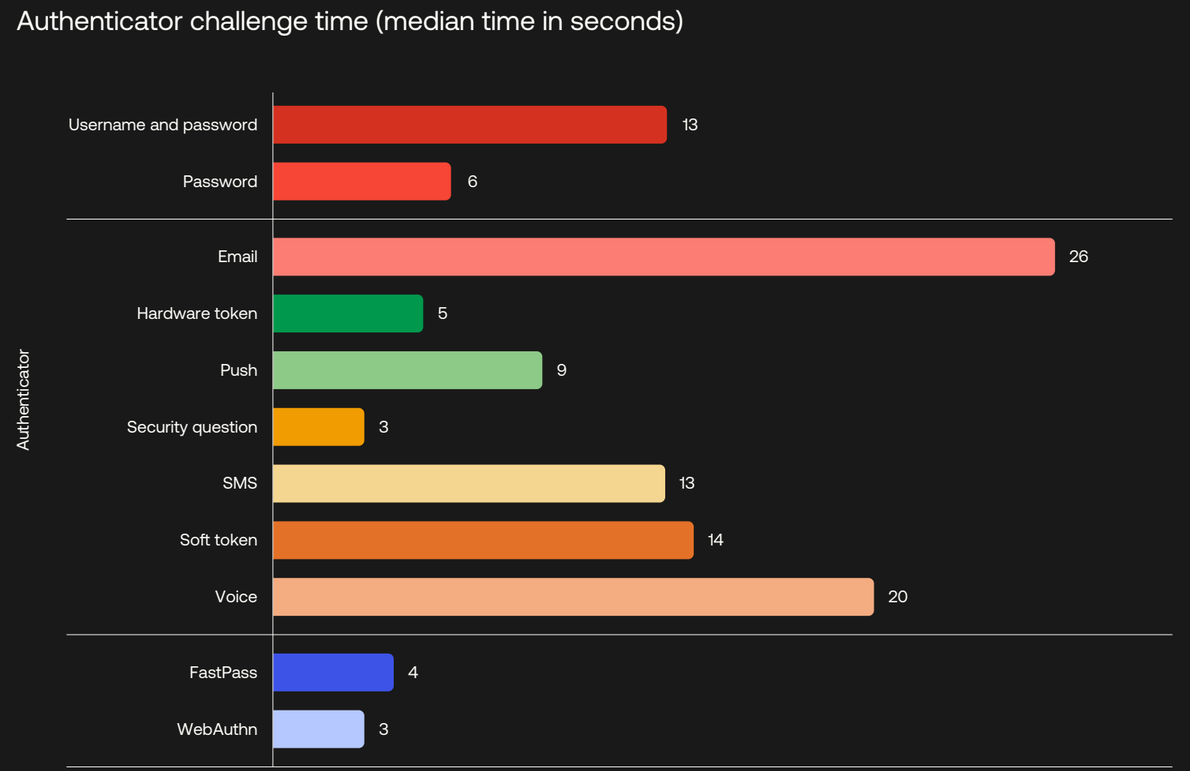


Figure 7: Median challenge times for password (both username-and-password and password-only flows), email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators.

“Enforcing FIDO2 hardware authentication was our most impactful security initiative last year. Okta Workflows gave us the flexibility to manage our risk and create temporary exclusion processes for mobile apps that still don’t support these authentication standards.”

Paul Clarke
Head of Security

Canva

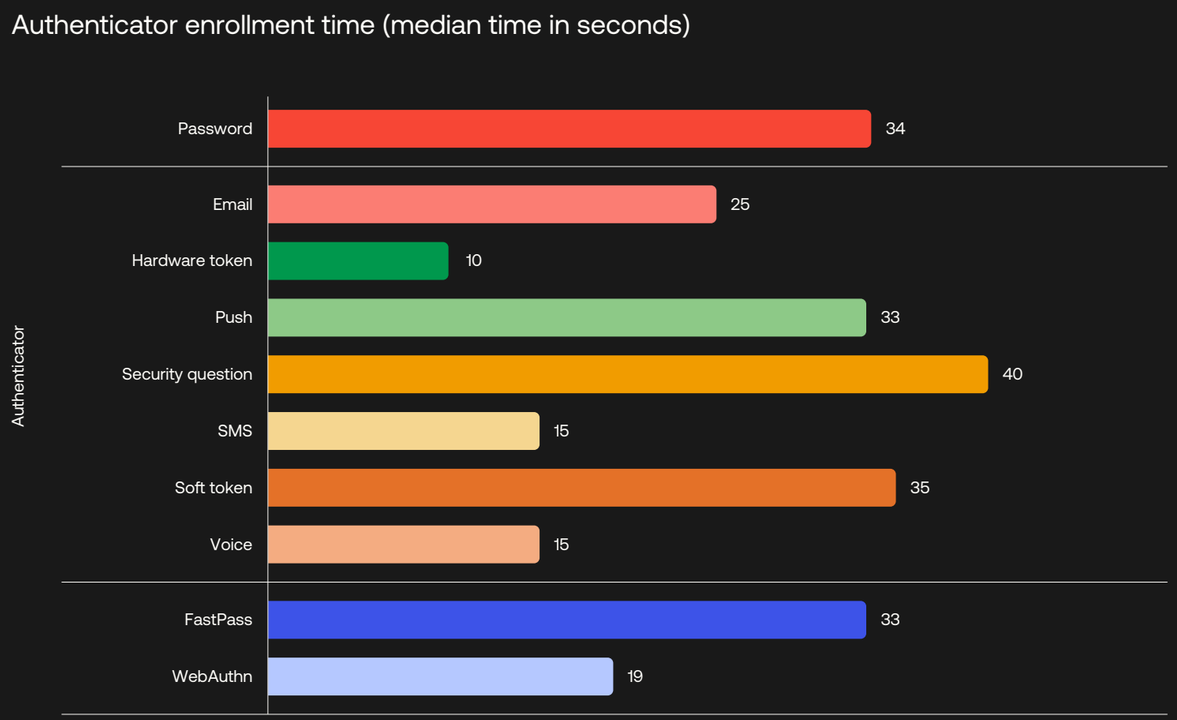


Figure 8: Median enrollment times for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators. Time spent on user verification was excluded from this analysis because it is determined by enrollment and recovery policies, rather than the authenticator itself.

Authenticator enrollment time

Authenticator enrollment time is measured as the median time it takes a user to enroll an authenticator, beginning when the authenticator enrollment page appears and ending when a user successfully completes the enrollment after following the instructions provided.

Authenticator enrollment, reset, and password recovery create temporary periods of elevated risk. For each enrollment or reset event, administrators can (and should) enforce rules on which authenticators are required to initiate and verify user Identity. We recommend configuring authenticators with phishing-resistance for this purpose.

The median time to register a password is approximately 34 seconds, which includes the time for a user to create a new password, confirm (re-enter) the password, and choose whether to sign out of other authenticated devices. A security question records the longest median enrollment time (40 seconds) since it requires users to select security questions or create security questions and type in answers.

Okta's authenticator enrollment flow is designed such that Okta Verify OTP, Okta Verify Push, and Okta FastPass can be enrolled together using the Okta Verify app. Given several authenticator types are enrolled in one motion, the median time to enroll them is approximately 33 seconds, including the time required for a user to scan a QR code and complete the configuration process for Okta Verify. This multifactor enrollment is faster than the median enrollment time for other soft tokens (about 39 seconds). Hardware OTP, Voice, SMS, and FIDO2 WebAuthn boast the shortest enrollment times at less than 20 seconds. ■

Key insight

These figures challenge the misconception that higher assurance authenticators (such as FIDO2 WebAuthn and Okta FastPass) impose a significant burden on users during enrollment.

While some users might initially be unfamiliar with them, the relatively short enrollment time indicates that they find the enrollment and re-enrollment process at least as intuitive as for other authenticators.

“Okta is an integral part of the Identity-centric view of life that we've taken with our security paradigm. Okta FastPass is a great example of how we can empower NTT DATA employees with an intuitive passwordless experience, while still maintaining invisible device policies and security.

When anyone is given a choice between something that’s convenient and something that’s secure, they’re going to choose convenient.”

Steve Williams
Chief Information Security Officer

NTT

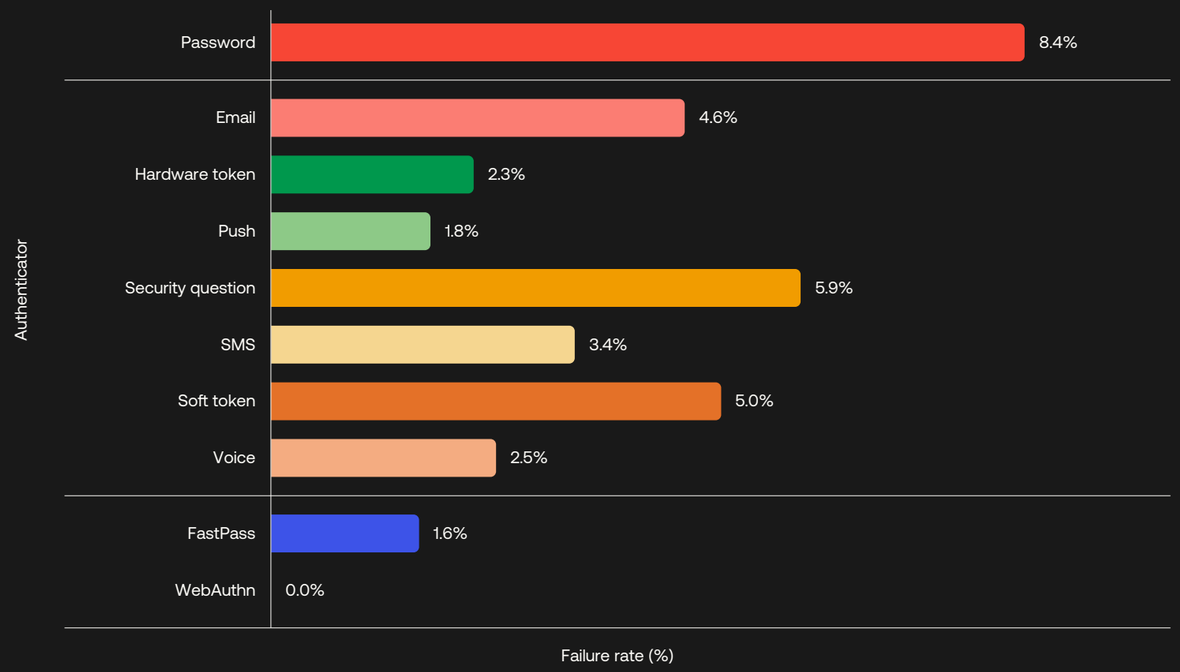


Figure 9: Challenge failure rates for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators.

Authenticator challenge failure rate

Authenticator challenge failure rate measures the number of failed authentication attempts divided by the total number of authentication attempts received by Okta's back-end servers using a given authenticator.

Failed authentication attempts occur more frequently than you might expect. These include events in which a user types the wrong password or an incorrect answer to a security question, enters an incorrect OTP, denies a push request, or provides an invalid authentication response signature using biometric authenticators, such as Okta FastPass or FIDO2 WebAuthn.

Authenticator challenge failure rate is a usability and a security metric, given that a failed authentication event could be benign or malicious. A higher benign failure rate means that users are more likely to make mistakes using a given authenticator during authentication, slowing their productivity. A higher suspicious failure rate typically indicates attackers view those methods as a softer target.

Our data reveals that knowledge-based authenticators impose the most considerable burden on users, followed by various forms of OTP. The humble password has the worst failure rate (at 8.4%), followed by security questions, soft tokens, and authentication challenges sent over email.

Okta FastPass and FIDO2 WebAuthn boast the lowest failure rates, with one caveat: While FIDO2 WebAuthn authentication will logically result in fewer unintended user mistakes ("fat finger errors") and fewer suspicious attempts, the implementation of WebAuthn isn't entirely consistent with other authentications. By design, back-end servers cannot capture all WebAuthn failed events. For example, if a user uses WebAuthn to attempt to sign in to a phishing site and the authenticator detects a domain mismatch, there is no mechanism for sending this information to the back-end servers of Identity providers. All back-end servers can observe is an unresponded challenge since they don't receive the response to the authentication attempt. ■

Key insight

Even accounting for the WebAuthn failure rate caveat, we can see again that the phishing-resistant forms of authentication deliver the best user experience.

Once a device is configured for FastPass or a user has enrolled their device or security key as a FIDO2 authenticator, the possibilities for user error are reduced dramatically.

Assessing authenticator usability and security

Authenticator security properties

Phishing-resistant coverage

Phishing-resistant coverage describes the potential percentage of devices protected by an authenticator that meets the NIST definition of phishing resistance.

If an authenticator is not phishing resistant, its phishing-resistant coverage is zero. A phishing-resistant authenticator has phishing-resistant coverage equal to the percentage of devices whose browsers and operating systems (OS) support those capabilities. Based on this criteria, only two authenticators have phishing-resistant coverage above zero: WebAuthn and Okta FastPass.

FIDO 2 WebAuthn allows websites to update their login pages to add FIDO-based, phishing-resistant authentication on supported browsers and platforms. According to caniuse.com, 95% of devices can use WebAuthn with their browsers and platforms. However, the WebAuthn phishing-resistant coverage is an upper-bound number for any WebAuthn authenticator. For example, WebAuthn platform authenticators may only support certain platforms. Therefore their phishing-resistant coverage could be much lower than the optimal coverage rate represented in the graph.

Okta FastPass is also effective at protecting against credential phishing attacks. It accomplishes this by verifying the origin URL for each authentication attempt. FastPass provides this phishing resistance across Windows, macOS, Android, and iOS platforms. In a workforce context, if we assume the same browser and platform usage mix from caniuse.com, around 94% of devices can access the FastPass phishing-resistant feature. ■

Key insight

Both WebAuthn and FastPass provide phishing-resistant coverage. Traditionally, WebAuthn implementations are single-device credentials in the form of either roaming authenticators, such as physical security keys, or platform authenticators, such as FaceID and Windows Hello. Last year, FIDO and major OS platform vendors introduced multi-device passkeys as WebAuthn credentials that users can synchronize across different devices.

All WebAuthn implementations are phishing-resistant. Multi-device passkeys represent a significant leap forward for consumer authentication use cases. However, in the workforce context, a single-device credential is more secure thanks to its binding with a specific device. FastPass is also tailored to workforce use cases and security models, such as strong device binding and device assurance posture checks.

Phishing-resistant coverage by authenticator

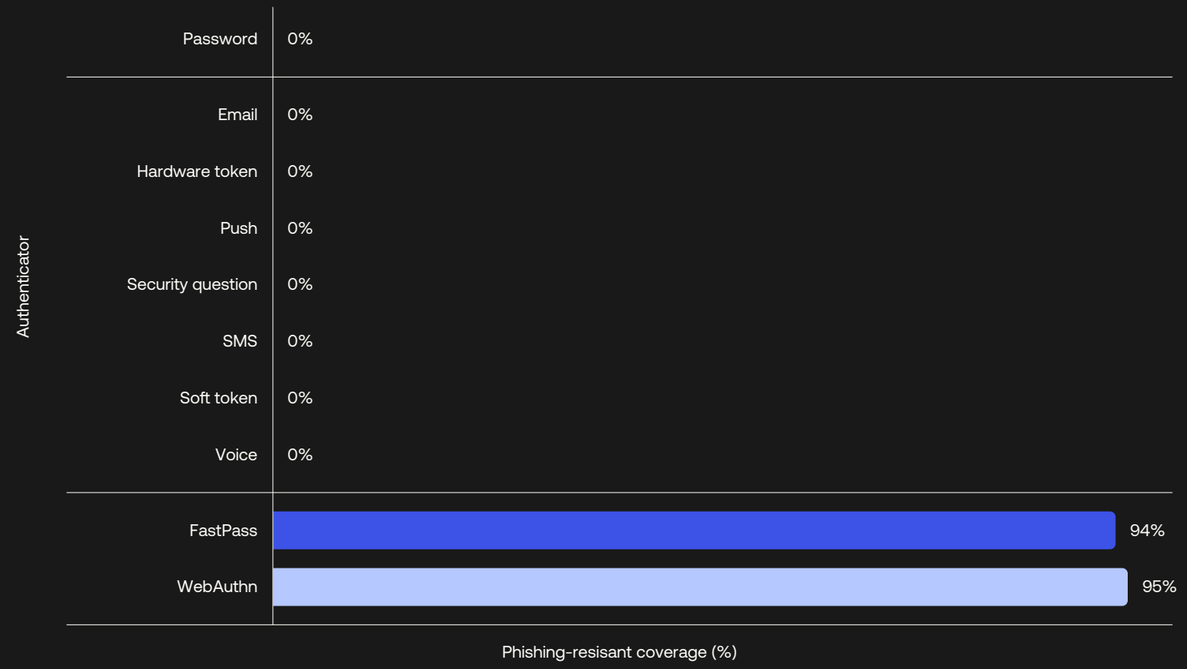


Figure 10: Phishing-resistant coverage for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators.

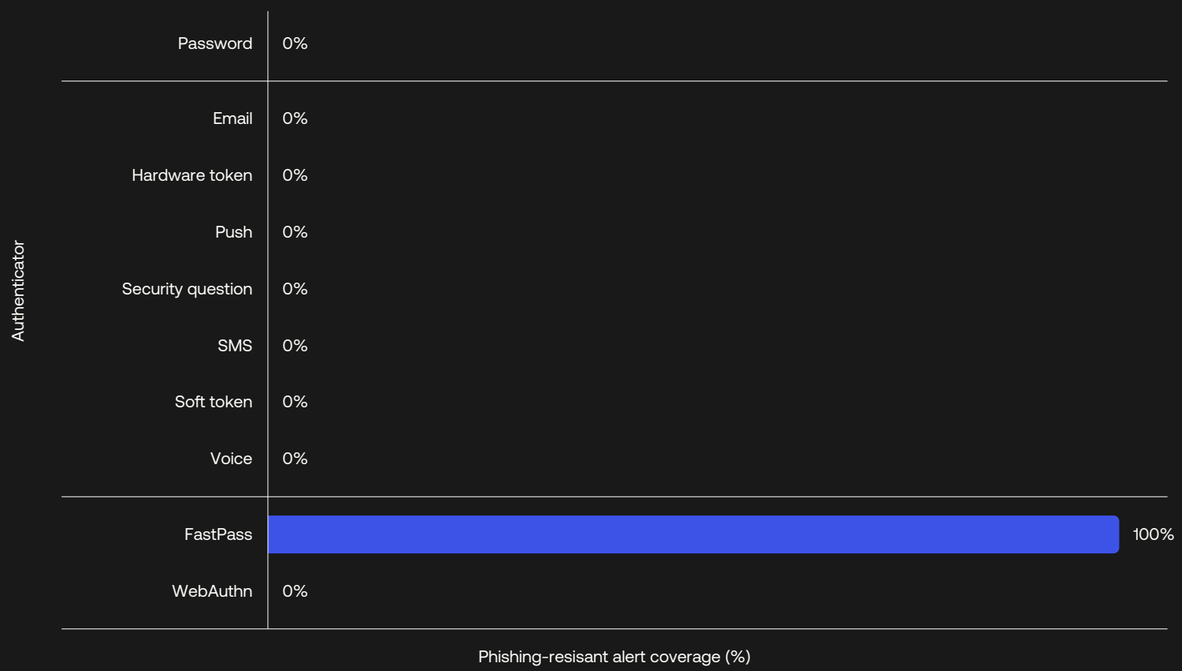


Figure 11: Phishing-resistant alert coverage for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators.

Phishing-resistant alert coverage

Phishing-resistant alert coverage is the percentage of users potentially protected by an authenticator capable of logging requests with failed origin checks, a common indicator of adversary-in-the-middle (AiTM) phishing attacks.

Today, Okta FastPass is the only authenticator capable of creating server-side events when a phishing attempt results in a failed origin check. When a domain name mismatch is detected, FastPass rejects the request and can be configured to alert the end user and administrators.

This ensures that FastPass stops malicious phishing attempts that use AiTM techniques. It also increases user and organizational awareness of threats, improving their ability to detect and respond to malicious activity.

It's worth noting that FastPass is not *just* an authenticator by the traditional definition. It's also capable of collecting device context signals, such as device management state, OS version, device lock, disk encryption, and jailbreak/root detection. FastPass also integrates with top endpoint detection and response vendors, such as CrowdStrike, to ensure the device is secure from an endpoint perspective. This contextual information can further enhance threat detection and authentication policy enforcement. ■

Key insight

We expect that the ability to proactively detect AiTM phishing campaigns will become more critical with the emergence of multiple "phishing-as-a-service" platforms that lease the infrastructure, configuration, and templates required to operate these campaigns at scale. During February and March 2023, Okta identified multiple campaigns that employed these techniques against Microsoft 365 user accounts at several thousand organizations.

Authenticator challenge brute-force failure rate

The brute-force failure rate describes the percentage of users with more than N failed authenticator verification events during a day, expressed as a percentage of users who signed in using the authenticator.

A brute-force failure occurs when a malicious or benign user fails to authenticate more than N times. N is a threshold number used to define a possible brute-force failure. Since threat actors may automate the guessing of a password or OTP, or generate repeated authentication challenges in an attempt to trick or fatigue a user into approving access, a brute-force failure reflects adversary preferences for conducting brute-force attacks against a given authenticator.

We can observe that knowledge-based secrets (passwords and security questions) are targeted by the automated tools of attackers most often, followed by OTP and Push MFA.

FIDO2 WebAuthn has the lowest brute-force failure rate but is subject to the same caveat described in the authenticator challenge failure rate section. ■

Key insight

Despite elevated MFA bypass events, traditional brute-force attacks still focus primarily on knowledge-based authenticators. Using authenticators based on possession or biometric factors can dramatically reduce the likelihood of brute-force attacks.

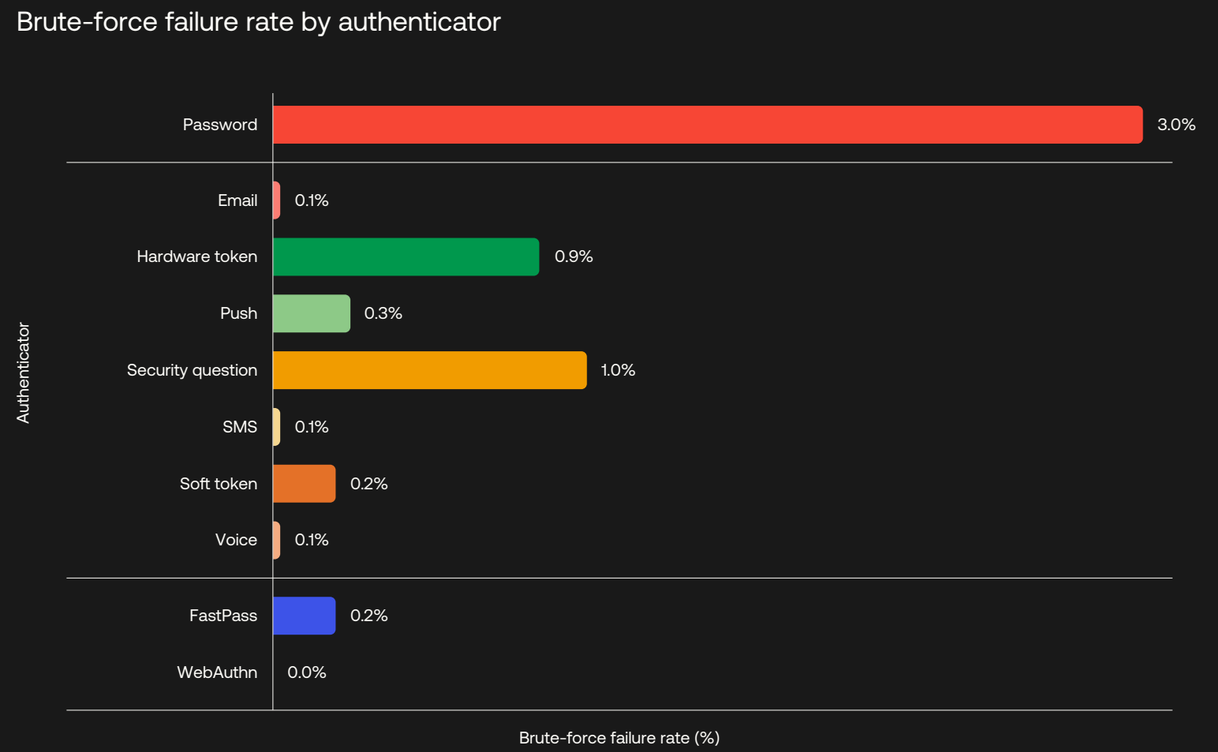
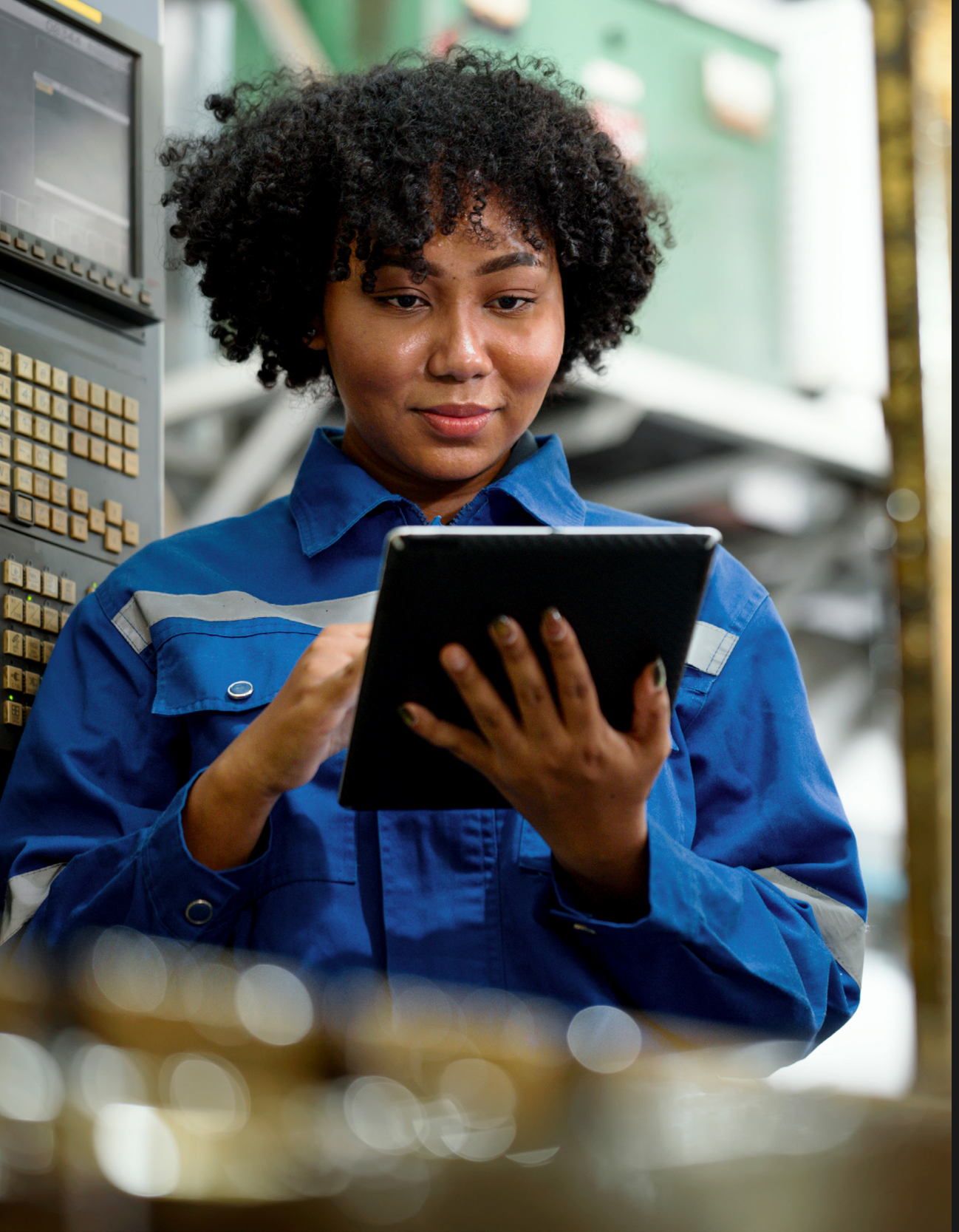


Figure 12: Brute-force failure rates for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators. The data was collected from November 2022 to January 2023.



“Compromised passwords are typically the first step in the data breach kill chain. It’s how an attacker gains initial access before moving laterally across the network, looking to escalate privilege. Passwords alone are no longer defendable or adequate for authenticating FedEx identities and protecting our digital assets.”

Trey Ray
Manager Cyber Security, Network Security

FedEx.

Assessing authenticator usability and security

Assessing authenticator performance and adoption

Phishing-resistant authentication offers a superior user experience

So, what does the sum of these observations mean for an organization's choice of authenticators, and how might security and IT leaders drive the adoption of authenticators that are user friendly and secure?

To find out, we developed a set of composite scores to assess authenticator performance. First, we normalized the metrics for each authenticator to the 0 to 1 range. We then weighted the metrics according to their impact on authenticator usability and security, as shown in Table 2, resulting in usability and security scores for each authenticator. Below, we plotted the authenticator usability and security scores in a 2 x 2 bubble chart, with the size of the bubbles representing the current adoption percentage for each authenticator.

In information security, it's frequently assumed that technology decision-makers must "trade off" security for user experience.

Our analysis finds that this is a false choice. While the study does not attempt to survey users on their preferences, the raw authentication data suggests that phishing-resistant authentication offers a superior user experience. With FastPass or FIDO2 WebAuthn, users are improving the security of accounts without any corresponding decrease in the quality of their experience.

So why is the adoption of these authenticators so much lower than the others we studied? It may be a byproduct of a knowledge gap or lack of familiarity among administrators. Okta FastPass is in a new category of authenticators, and its unique phishing-resistant properties are newer still (announced in late 2022). The FIDO2 WebAuthn standard is also relatively new, and supporting browser and OS coverage have only recently improved.

The dramatic growth of both authenticators over the past 12 months and our quantitative study of their respective qualities bode well for future adoption. ■

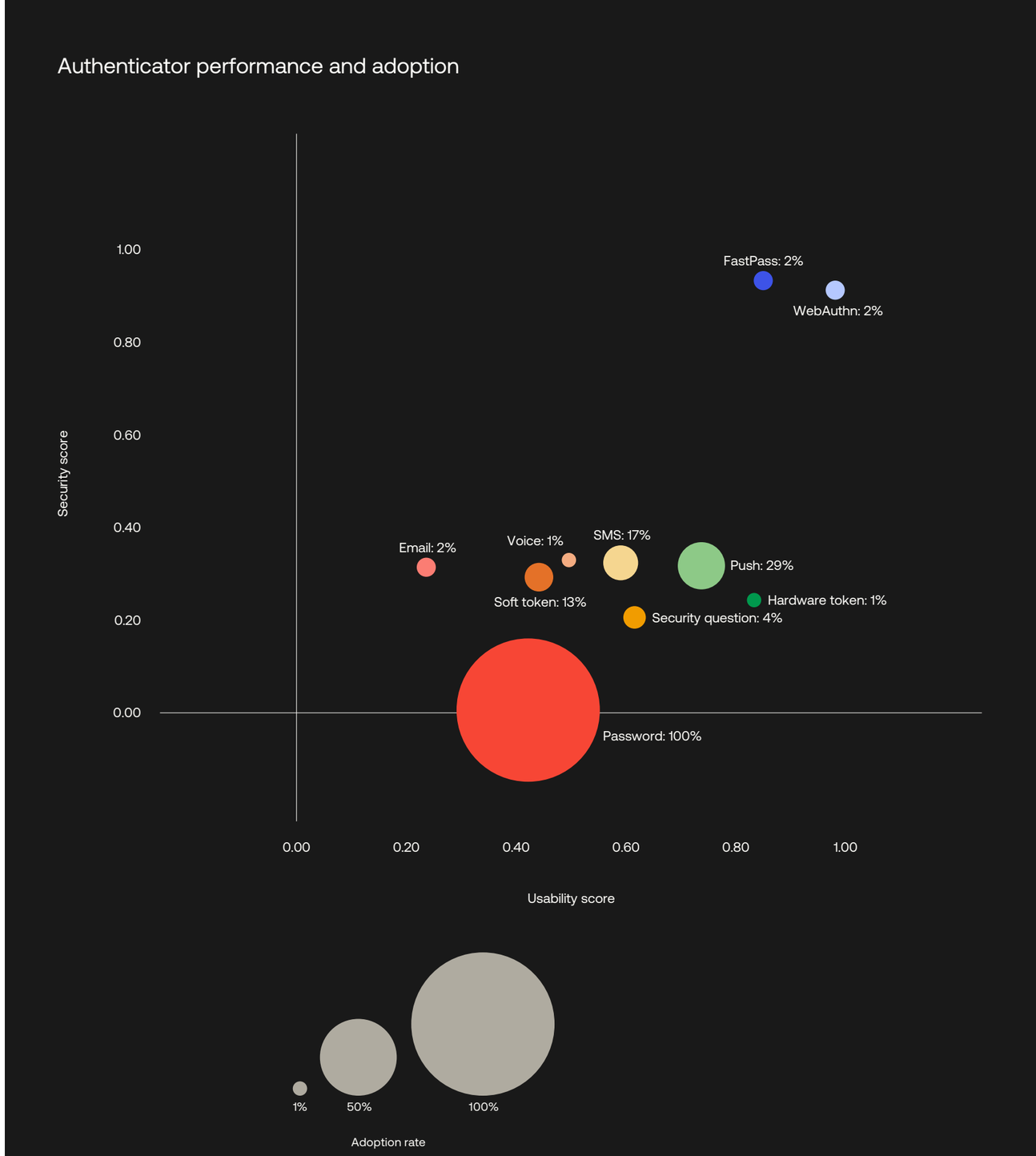


Figure 13: Authenticator performance and adoption for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators. Each authenticator's performance is represented by its usability and security scores as shown in a 2x2 matrix. The size of the bubble reflects the authenticator's adoption rate on a scale of 0% to 100%.

The way forward

Phishing-resistant MFA is secure, user friendly, and achievable. It's a win-win for administrators and users. So why aren't more organizations adopting it? We know that the journey can be complex. IT and security leaders must grapple with user education, legacy technology, and policy or regulatory hurdles — to name just a few challenges.

Fortunately, there are resources to guide your way. For starters, CISA recently released its Zero Trust Maturity Model Version 2.0, which aims to assist agencies and organizations with developing and implementing Zero Trust strategies, including phishing-resistant authentication. Okta has also developed an Identity Maturity Model to help our customers determine where their organization's Identity and security strategy sits now and what's needed to advance.

Looking for more personalized guidance? Get in touch. We're here to help you keep your organization secure and your users happy.

5 tips to improve your authentication strategy

While transitioning to a more robust authentication strategy may seem daunting, organizations can take relatively simple steps to get started.

1. Require MFA in sign-on policies and enforce phishing-resistance for administrative access to sensitive applications and data. We strongly recommend taking advantage of the phishing-resistant properties and device assurance capabilities offered by Okta FastPass, our passwordless authenticator.
2. Make MFA adoption a C-suite and board-level priority. Given its effectiveness for securing an organization's most valuable resources and information, the MFA adoption rate should be visible at the highest levels of the organization.
3. Take a Zero Trust approach to access, in which access is granted according to Identity properties on a per-session and least-privilege basis, and is determined according to the assurance requirements of the requested application or data.
4. Create dynamic access policies that evaluate user attributes, device context (whether the device is known, managed, or exhibiting a strong posture), network attributes (whether the network is trusted), and whether the request is consistent with previous user behaviors.
5. Develop a longer-term plan to minimize or eliminate the use of passwords.

Methodology

To create this report, we relied on data from Okta Workforce Identity Cloud. We anonymized and aggregated data from billions of monthly authentications and verifications from countries around the world. Our customers and their employees, contractors, partners, and customers use Okta to securely log in to devices, websites, apps, and services and to leverage security features to protect their data. They span every major industry and vary in size, from small businesses to some of the world's largest organizations.

Customer company size is defined by the number of full-time employees in the company. Company industry taxonomy aligns with the North American Industry Classification System (NAICS). Customer company size, industry, and geographic region are validated using third-party resources.

Unless otherwise noted, this report focuses exclusively on Okta Workforce Identity Cloud data and workforce use cases. It does not include Okta Customer Identity Cloud data.

Afterword

Lessons learned and thank you

One year ago, Todd and I wanted to understand the state of passwordless. We initially thought about surveying the market or crawling website login pages. After doing some investigation, we realized that the most objective approach is to share how MFA and passwordless solutions are used by Okta's customers.

As we dove deeper into the topic and shared our preliminary findings, a wide range of people expressed interest in our study. Our customers wanted to benchmark their MFA usage against their industry peers and use our analysis of authenticator usability and security properties to champion phishing-resistant authenticators within their organizations. Industry analysts and policymakers wanted access to MFA adoption data to determine where further education, investment, and policy are needed.

Internally, we also learned a lot from the study. Chief among those lessons, we found that the best answers arrive when you set out to answer fundamental questions first.

I also learned that extensive studies like this one require far-reaching collaboration. Fortunately, that's embedded in Okta's culture. Many Oktanauts went the extra mile to contribute to this work. Special thanks to Yi Zhang, Sicong Shan, Andres Aguiar, Sam Sanjabi, Yuming Cao, Gunes Kayacik, and James Fu for helping and coaching me with data collection and analytics. Much gratitude to Shaolin Shen, Yang Chen, Yu Liu, Nao Itoi, Manu Malhotra, Deepti Arora, Glenn Vander Laan, Kristen Shiroma, Leigh Thompson, John Murphy, Moussa Diallo, Robert Lucero, Ed Johns, Dan Post, Shaye Khazaeli, and Greg Fee for helping me better understand our products and interpret the data. I also want to thank Brett Winterford for rewriting the draft to make it engaging and for always reminding me to maintain my scientific approach to the study; to Lauren Everitt, Andrew Dudley, and Jess Bagherpour for editing the report; Katie Ryan O'Connor, Ben Finkenbinder, Michael Clauser, Jennifer Yamamoto, and Kyrk Storer for deciding to publish the report; Lauren Everitt and Kortney Carr for leading the publication process; Rali Vladova, Carmen Yu, Brandon De Jong, Sabrina Barekzai, McKenzie Mayer, Sarah Robertson, and Jourdan McCaffrey for supporting the publication and promotion of the report; Megha Rastogi, Dave Gennarelli, Karl McGuinness, Ashley Tobin, Timothy McIntyre, Yuliya Gorbunova, Jamie Fitz-Gerald, Alyssa Stone, Eila Shargh, Ariel Zommer, Jax Painter, and Tom Malta for reviewing the report. If you appreciate a collaborative culture, you should definitely think about a role at Okta!

Fei Liu
Senior Emerging Tech Researcher

About Okta

Okta is the world's Identity company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871