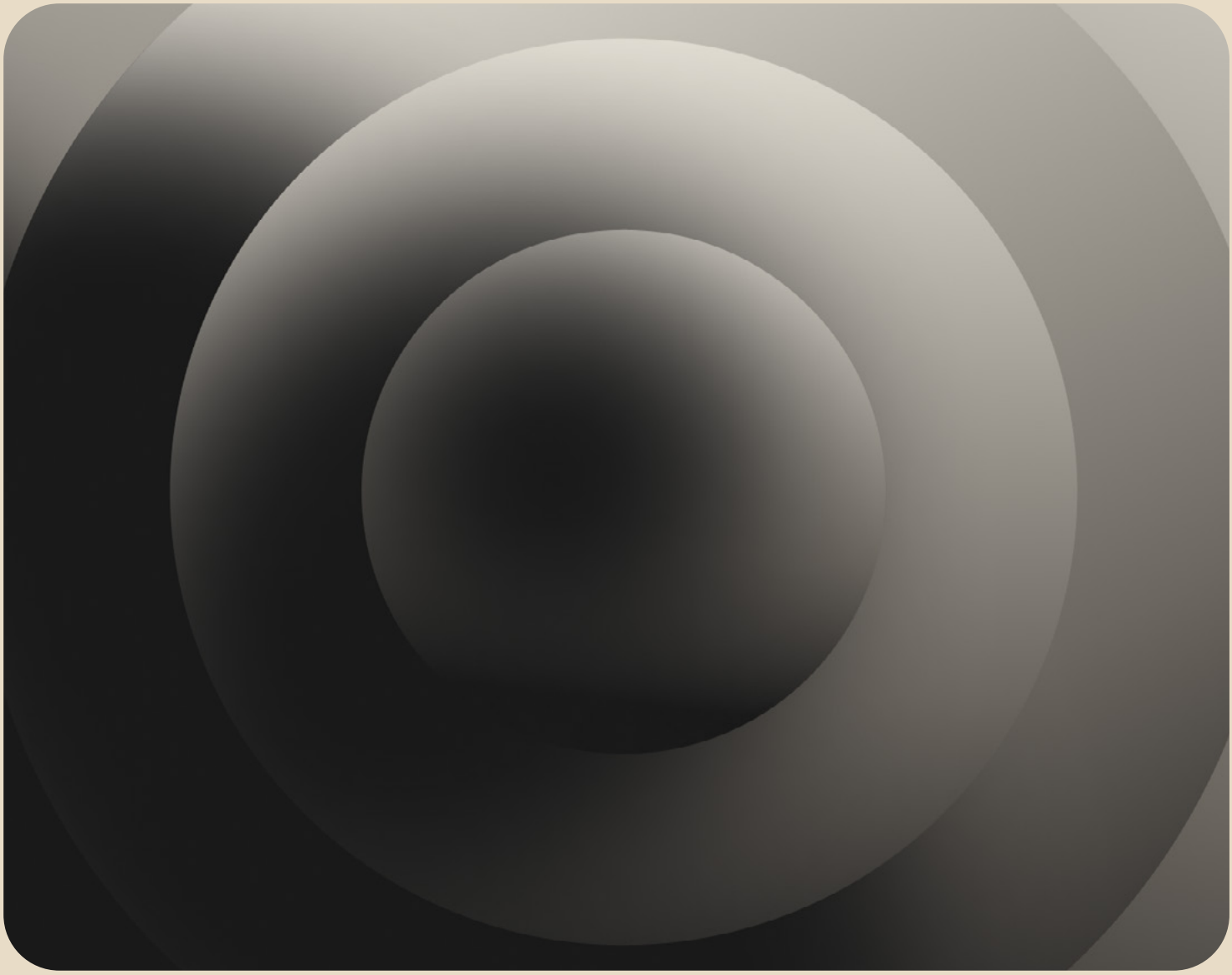
2024

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

The Secure Sign-in Trends Report



okta

It took a little time to convince the world of the virtues of multi-factor authentication (MFA).

From the outset, the consensus in the security community was that MFA was essential to protecting against wave after wave of password-based attacks, but many organizations would only require an MFA challenge for access to their most treasured systems.

During the pandemic, MFA adoption went mainstream. Okta observed a 15% rise in the use of MFA within a few short months, as the world rushed to support remote work. We're now at the point where most Okta admins, and the majority of users, access workplace applications after MFA challenges. And we're seeing regulators and standards bodies across the world demanding that organizations secure access with these stronger sign-in methods.

In this year's Secure Sign-in Trends Report, we find strong growth in the adoption of passwordless, phishing-resistant sign-in methods. In January of this year, 5% of users on our workforce platform didn't sign in once using a password. That small number belies a huge, latent, exciting potential. It's a small number that says that passwordless is here and now. It's possible. If these Okta customers did it, so can you.

So we expect the next wave of MFA adoption won't be driven by security purists, or even by those very sensible policy makers demanding that regulated entities enroll users in MFA. It's going to be driven by a demand for a better user experience and higher security assurance. Once you've experienced passwordless, whether as an employee or a customer, you will never want to go back.

I hope you enjoy geeking out on these numbers. Thanks for reading.

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 an SKU that includes MFA
Tenants-Level Enrollment Rate	% of tenants, Okta 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
Tenants-Level MFA Adoption Rate	% of Okta customer tenants, 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 exclusively 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 orgs/tenants.

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 leveraged Okta Identity Engine (OIE), which provides better-designed and more flexible Identity experiences and flows.

We measured the properties of the following authentication methods: password, email, hardware one-time password (OTP), push, software OTP, security question, SMS, voice OTP, Okta FastPass, FIDO2 WebAuthn, and smart card. Unless otherwise specified, we collected the data during January 2024 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 2024, MFA adoption climbed to 66% among Okta workforce users, and 91% of administrators use MFA.

Adoption rates vary widely by industry and company size

Government and Education, saw above 5% year-over-year growth in adoption, and this may further increase with recent U.S. executive orders (EOs) and regulatory changes.

Phishing-resistant authenticators show great momentum

The adoption of phishing-resistant authenticators increased substantially. The adoption rate for FIDO2 WebAuthn increased from 2% in 2023 to 3% in 2024, while the adoption rate for Okta FastPass leaped from 2% to 6% in the same time period.

Passwordless has arrived

The number of Okta customers who are using passwords is finally starting to decline as organizations adopt modern authentication methods. Just under 5% of users did not use a password during any sign-ins during January 2024.

Security vs. user experience is a false choice

Phishing-resistant authenticators offer a superior user experience. In our authenticator performance and usability assessment, FastPass and FIDO2 WebAuthn came out on top as more secure and user friendly than other options, even under revised, more practical criteria.

Introduction

> "[Multi-Factor Authentication] MFA is widely recognized as one, if not the most, important preventative security controls available today. It provides a strong defense against various adversarial attack techniques such as password spraying, compromised password reuse, and—in some instances— phishing. However, a key challenge is that it is notoriously difficult to deploy and many organizations, small and large, still have not done so even if they recognize the value." [1]

We all understand the assurance Multi-Factor Authentication (MFA) adds to user sign-in events.

One of the most difficult trade-offs in identity and access management is determining what level of friction you're willing to impose on end users in order to secure access to the organization's applications and data. Too little friction creates opportunities for attackers, and too much friction drives employees to use unsanctioned applications, which also creates risk.

As the number of serious security incidents and the costs of these incidents climb, most organizations and employees are coming to accept that strong authentication is a non-negotiable requirement, especially when securing remote access to resources. The challenge now is how to enforce high assurance authentication while minimizing the friction applied to end users.

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 updated our assessment of the state of authentication, identifying trends and analyzing approaches based on considerations such as industry, region, and company size.

Ultimately, this year's report shows that while we are moving in the right direction, we're not moving fast enough. During the COVID pandemic, we saw a 15% spike in MFA adoption as organizations rushed to secure remote working, so it's a little disheartening to see the pace slow: MFA adoption only improved two percentage points year-over-year since 2023, albeit from an already high baseline. As of January 2024, 66% of users authenticated with MFA.

It appears that we are at a turning point. The US Executive Order on Improving the Nation's Cybersecurity is coming into force, and Organizations and Cloud Providers alike are stepping up to drive users toward more secure authentication. Concurrently, technology leaders like Salesforce, GitHub, Okta and Microsoft are all embarking on projects to enforce MFA for privileged users, which will drive interest in the development and adoption of authentication methods that provide high assurance without imposing user friction.

With this report, we aim to provide IT and security professionals with a data-driven perspective on the solutions available today and to dispel the myth that strong authentication must translate to extra friction for users. In fact, the opposite is true: passwordless, phishing-resistant authentication is both more secure and easier to use.

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

[1] https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

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 included:

- 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.

“Okta has enjoyed the benefits of passwordless, phishing-resistant authentication for several years. Over the 12 months since the last Secure Sign-in Trends report, we’ve invested in enforcing phishing resistance throughout the entire user lifecycle: from user enrollment, through to access, and into account recovery. The great news is: it’s possible.”

David Bradbury
Chief Security Officer

okta

Current state: MFA adoption

MFA is 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 user type (whether the user has administrative permissions). The results serve as both a benchmark to gauge organizational and industry progress and to identify areas for improvement.

“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).

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 2024. Each data point represents the MFA adoption during that month.

As we discussed in our 2023 report, 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 corporate network. Since then, year-over-year growth in MFA adoption was at 6% per year from 2020 to 2023, and slowed down to 2% in 2024. As of January 2024, 66% of users sign in using MFA.

This growth rate is not keeping up with the increase in identity-based attacks. In 2024, we saw multiple events where threat actors targeted human and machine accounts that did not have multi-factor authentication enabled. In response, many cloud vendors are now mandating MFA adoption for privileged user accounts, if not all accounts.

Key insight

As enforcement of MFA for privileged accounts becomes a baseline control organizations expect, we expect more service providers to join the list of those already mandating MFA for privileged accounts. IT and Security professionals should leverage this as a driver to accelerate MFA adoption more broadly across their organizations.

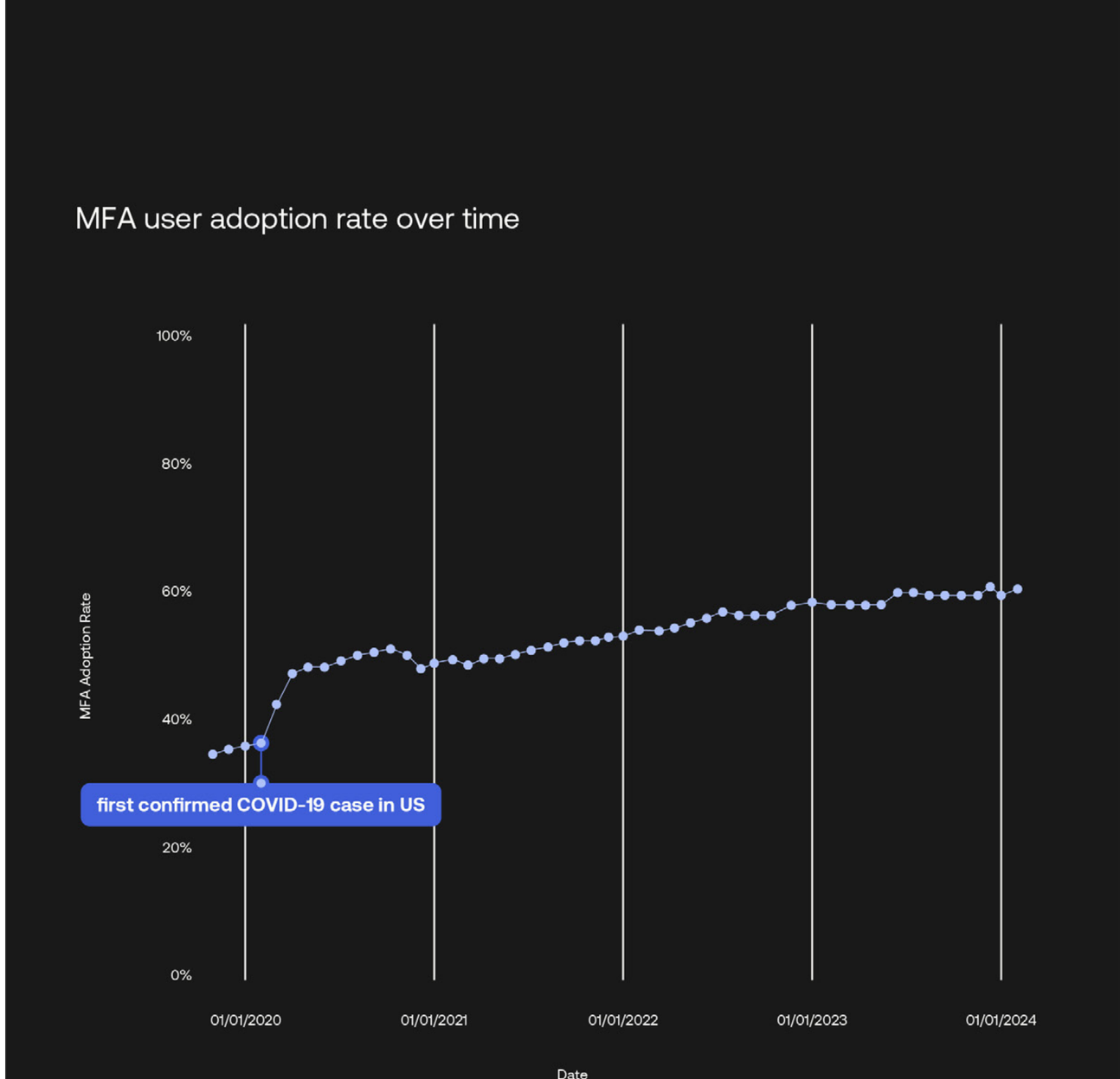


Figure 1: MFA user adoption rates from October 2019 to January 2024. The data reflects workforce use cases for Okta Workforce Identity Cloud and does not include data from Okta Customer Identity Cloud (formerly Auth0) or customer-facing use cases of the Okta platform. The data also excludes data from Okta Federal Risk and Authorization Management Program (FedRAMP) High and DoD Impact Level 4 customers.

Current state: MFA adoption

MFA adoption by region

In the 2023 report, we noted that MFA adoption was relatively consistent across geographic regions, and we expected that to hold true in 2024. Okta customers are more likely to apply MFA to users than any other competing service, irrespective of location.

Our data validated this position: showing MFA adoption rates of between 61 and 68% for the Americas (AMER), Asia Pacific (APAC) and EMEA (Europe, Middle East and Africa). We observed a 3% improvement in adoption rates in AMER and EMEA compared to 2023, and a decrease of 1% in APAC.

Key insight

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

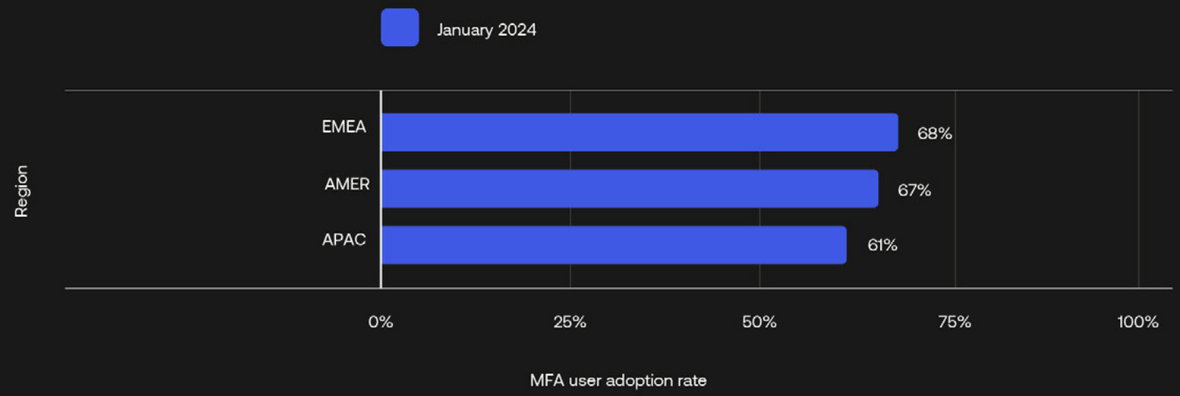


Figure 2: MFA user adoption rates in North, Central, and South America (AMER); Asia-Pacific (APAC); Europe, Middle East, and Africa (EMEA).

Current state: MFA adoption

MFA adoption by industry

In 2024, we continue to observe a wide variation in MFA adoption by industry - increasing to a difference of 50 percentage points between 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 (88%) among Okta Workforce customers.

There was higher MFA adoption across almost all industries during the past year. The Government (up to 55% from 48%)[2] and Education sectors (up to 69% from 64%) saw an increase of above 5% year-over-year in MFA adoption. Both sectors are highly regulated industries that started out with relatively low rates of MFA adoption and are now catching up, and we expect recent U.S. executive orders and regulatory changes to further accelerate the trend. On the flip side, we observed decreases in MFA adoption in the Arts, Entertainment & Recreation sector (down to 53% from 57%) and the Insurance sector (down to 71% from 77%). These industries are among several that compete on user experience when authenticating large networks of business partners (consider insurance brokers, for example). Given the data these small businesses access, however, we find it unlikely that a password alone or a password with SMS MFA will be deemed sufficient by regulators in the longer term. This report outlines several ways to deliver a great user experience without sacrificing security.

Key insight

We wanted to make a special call-out to the progress made in the Government sector. Organizations that provide services to the Government sector, or any other federally regulated sector, should be implementing MFA for privileged accounts, at minimum. In the 2023 report, the MFA adoption rate for government organizations lagged the private sector by more than 16 percentage points. This year, MFA adoption in government organizations increased by 7 points to 55%, one of the largest jumps in our data. With U.S. executive orders coming into force[3] and with the US Cybersecurity and Infrastructure Security Agency (CISA) repeatedly endorsing MFA and phishing-resistant authentication, we are seeing real progress by public service organizations in the United States.

[2] Some 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 55% doesn't include that use case, and may underrepresent the real government MFA adoption rate. Okta introduced smart card as a native authenticator type in 2023. We recommend federal customers migrate from X.509 federation to smart card authenticators so as to take advantage of advanced features such as App-Level Authentication Policies and Okta Device Access.

[3] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028

MFA user adoption rate by industry

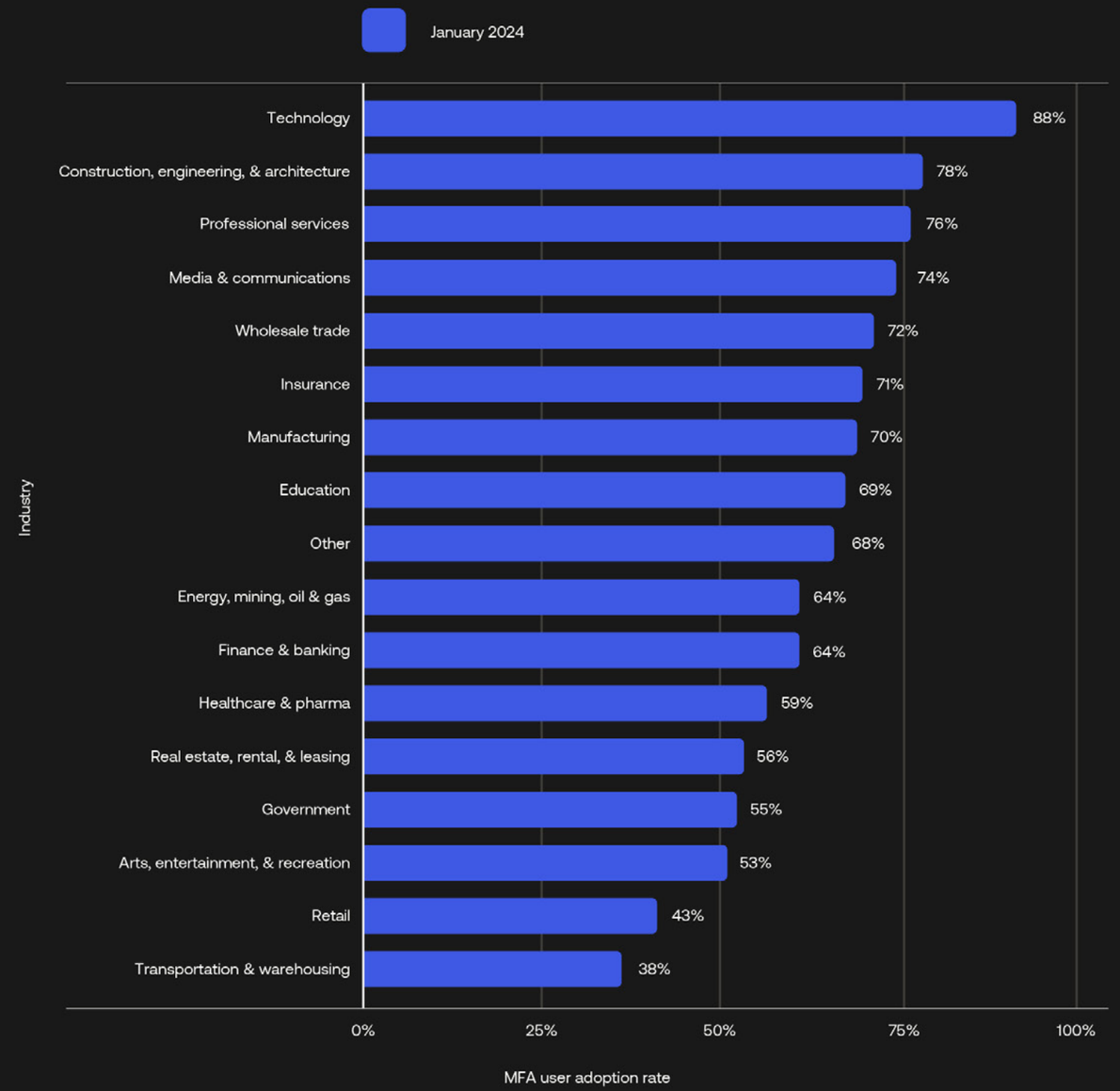


Figure 3: MFA user adoption rates across industries, listed in descending order by rate.

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 adoption rate. Organizations with fewer than 300 employees tend to have the highest MFA adoption (≥82%), while those with more than 20,000 employees have the lowest adoption rate (59%). Despite being the lowest adoption group, the latter organizations have made larger than average improvement (5%) on a year-to-year basis.

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 (our report focuses only on MFA usage using the Okta platform).

Key insight

The lack of a centralized view of Identity and Access Management (IAM) is problematic, whether you're a large or a small company. Large enterprises tend to be more sensitive to trust-eroding security events and should be motivated to pursue broad MFA coverage.

MFA user adoption rate by organization size

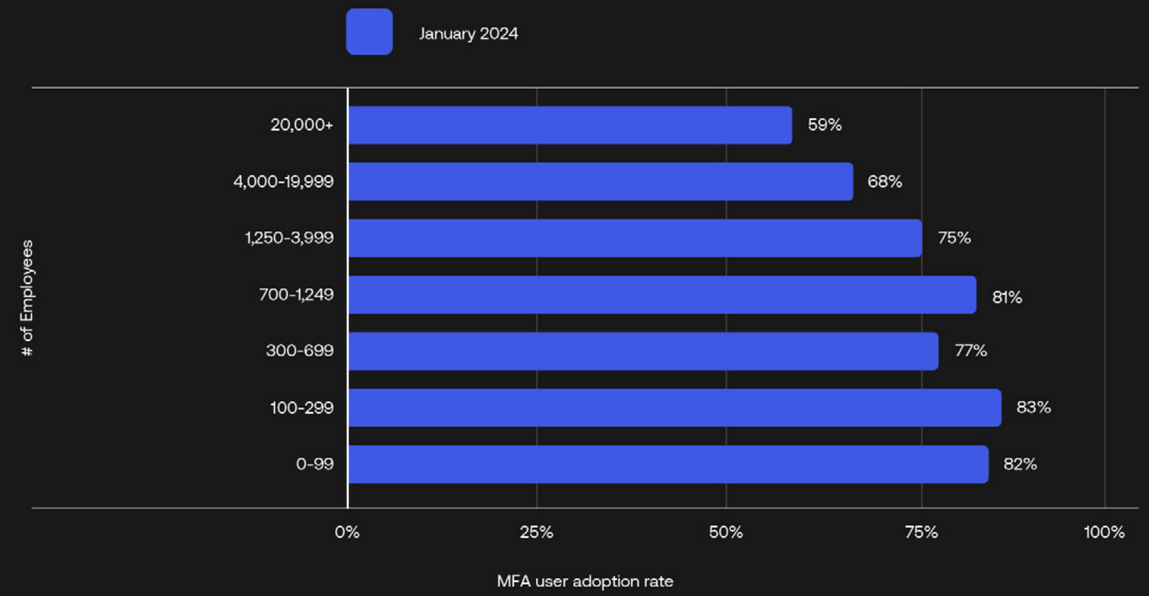


Figure 4: MFA user adoption rates across organizations of different sizes, listed in ascending order by number of employees.

Current state: MFA adoption

MFA adoption by user type

When we assess MFA adoption by Okta administrators, we define an Okta administrator as someone who has at least one administrator role at Okta. This would include everyone from the IT help desk through to IAM and security teams. These MFA adoption numbers are very healthy at 91%, up 1% from last year. Admins also tend to serve as role models for using phishing-resistant MFA. FIDO2 WebAuthn adoption among users with admin permissions grew from 8% to 9% over the past year, while the use of Okta FastPass among administrative users grew from 5% to 13%.

In August 2024, as part of the Okta Secure Identity Commitment, Okta began requiring customers to configure MFA to access administrative and management consoles.[4] Before the MFA enforcement for the WIC Admin Console began we saw high, but not total adoption.[5] Our goal is to achieve full adoption by addressing the remaining long-tail of users with administrative permissions.

To minimize the impact on our customers, this enforcement action is sequenced according to the complexity of existing sign-in flows. Some admins log in directly within Okta WIC, while others use Identity Provider federation or integrations with privileged access management software. Okta now prevents the creation of single factor policies for direct access to the Okta Admin Console and has enforced MFA for access to the Console for 62% of Okta's existing workforce tenants.

We hope that once privileged users experience how easy it is to sign in with passwordless, phishing-resistant authenticators, we will see a broader acceleration in MFA adoption for all users.

Key insight

Okta's enforcement of MFA for access to administrative apps provides IT and security professionals a trigger event to review their organization's broader authentication strategy. We encourage our customers to take this opportunity to thoroughly review sign-in policies for all management consoles and other high-risk or business-critical applications.

Using application-specific authentication policies can help smooth this rollout by requiring strong authentication for high-risk or business critical applications, while allowing employees to use weaker forms of authentication for less risky applications. This strategy allows administrators to improve the security of an organization without impacting business speed.

[4] https://support.okta.com/help/s/blog/a674z000000147HAAQ/mfa-enforcement-for-the-admin-console?language=en_US

[5] Please note that the percentage of admins using MFA to access the Okta Admin Console metric is different from the MFA adoption rate for admins metric. The former metric looks at the access to the Okta Admin Console only, while the latter looks at the access to any applications. Also, the former metric requires admins to use MFA every time they access the Admin Console, while the latter requires at least one MFA authentication in a month.

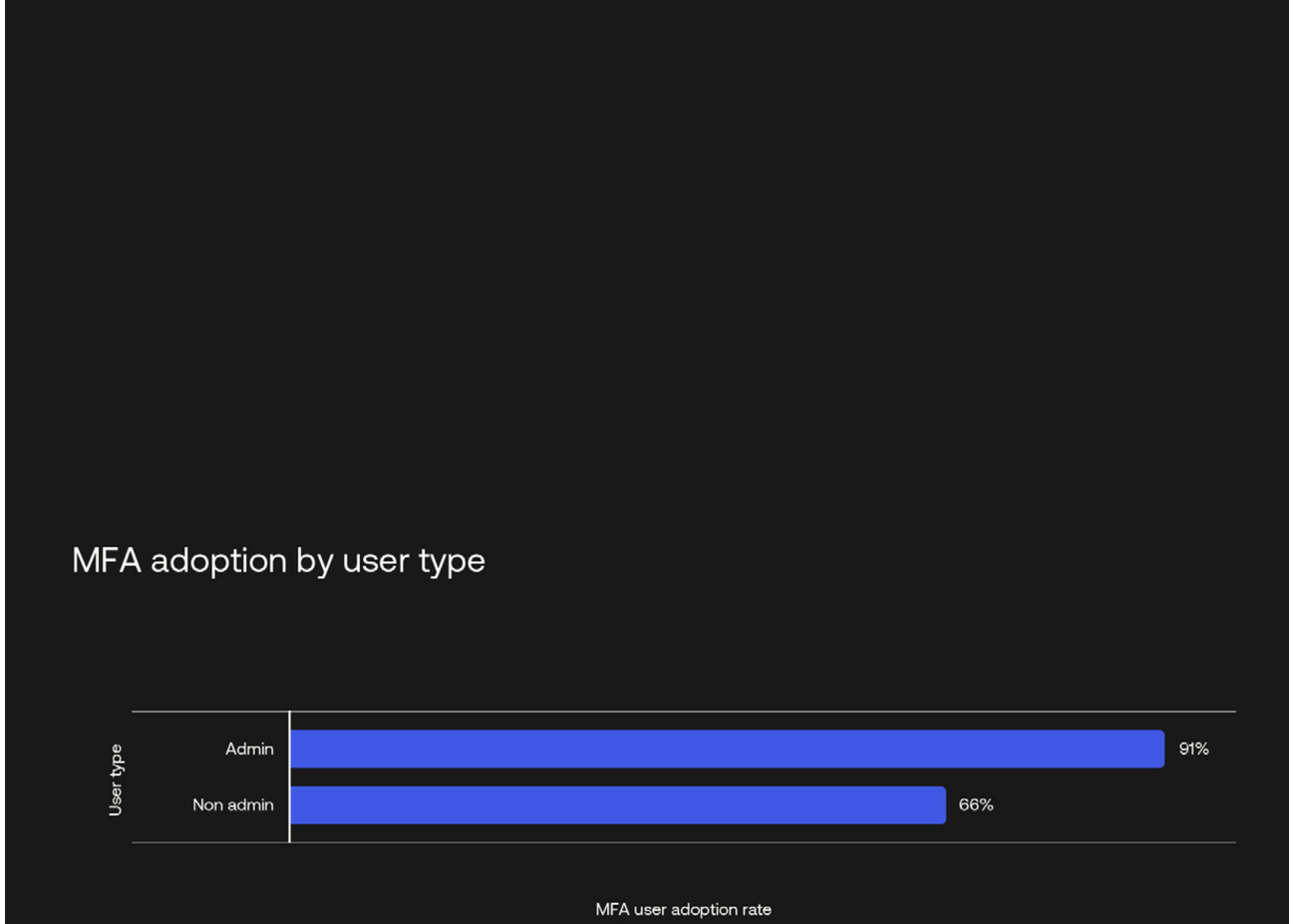


Figure 5: MFA user adoption rate for administrators and non-administrators.

Current state: MFA adoption

MFA adoption rate by authenticator type

The Okta Identity Cloud is built on the idea of being platform-agnostic, and allowing customers to use the technologies that work best for them. Okta offers a wide selection of first-party and third-party MFA authenticators for all use cases. Based on their underlying authentication mechanisms, authenticators can be categorized into three groups: password authenticators, traditional MFA authenticators, and phishing-resistant MFA authenticators.

Traditional MFA authenticators include Email, Hardware Token, Push, Security Question, Short Message Service (SMS) and Soft Token. Phishing-resistant MFA authenticators include Okta FastPass, FIDO2 WebAuthn, and Smart Card. As shown in Table 1, we include as many vendor offerings as possible for each authenticator type. However, if the authentication data couldn't be separated by authenticator types or involved custom options, we placed it in the "other" category and excluded it from further study.

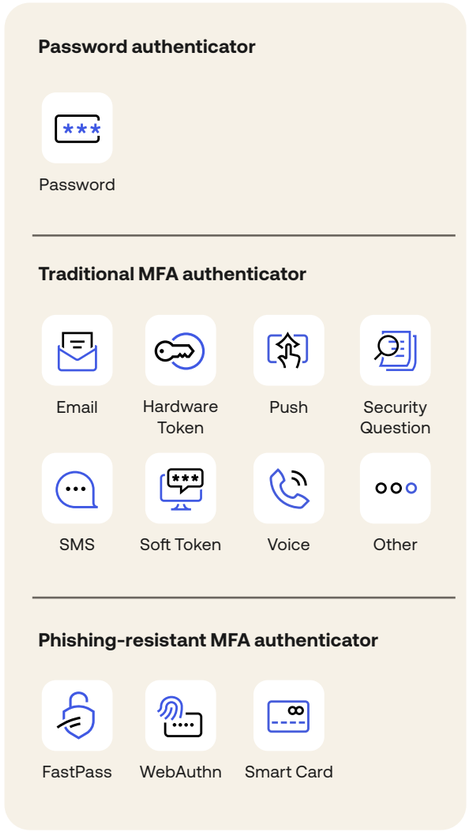


Table 1: Authenticator types and properties

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

Authenticator type	Supported authenticators at Okta, used for Authenticator adoption property study	Authenticator names: types, used for usability and security property study	Factor type	Assurance level
Password	Password	Password	Knowledge	Weak
Email	A combination of Email code and link (aka magic link)	A combination of Email code and link	Possession	Weak
Hardware Token	YubiKey OTP, RSA SecurId, Custom TOTP	YubiKey OTP	Possession	Medium
Push	Okta Verify Authenticator, Push method, Duo Authenticator	Okta Verify push	Possession Possession + Biometric	Medium
Security Question	Security questions	Security questions	Knowledge	Weak
SMS	SMS, Duo Authenticator	SMS	Possession	Weak
Soft Token	Okta Verify OTP, Google Authenticator, RSA SecurId, Custom TOTP, Duo authenticator	Okta Verify OTP, Google Authenticator	Possession	Weak
Voice	Phone authenticator Voice method, Duo authenticator	Phone authenticator Voice method	Possession	Weak
FastPass	Okta Verify authenticator, FastPass method	Okta FastPass	Possession Possession + Biometric	High
WebAuthn	WebAuthn authenticators (a combination of Mac Touch ID, Android fingerprint, Windows Hello, YubiKey, Google Titan, PassKey), Duo Authenticator	WebAuthn authenticators (a combination of Mac Touch ID, Android fingerprint, Windows Hello, YubiKey, Google Titan, PassKey)	Possession Possession + Biometric	High
Smart Card	Smart Card	A combination of PIV, CAC	Possession + Knowledge	High

It is no surprise that passwords persist in the workforce environment. But we also see an increase in passwordless experience, growing from less than 2% in January 2023 to almost 5% in January 2024. Push (29%) is the most popular MFA authenticator, followed by SMS (17%) and Soft token (14%).

The adoption rates of traditional MFA authenticators increased compared to last year, but the changes are small (1.3% in total). We saw a very small SMS MFA adoption rate growth of 1.2% over the last three years, despite the overall MFA adoption rate having grown 14% during the same period. By contrast, we see a substantial increase in the adoption of phishing-resistant authenticators. For example, the WebAuthn adoption rate increased from 2% of users in 2023 to 3% of users in 2024, while the Okta Verify FastPass adoption rate increased from 2% of users to 6% of users in the same time period.

There are three critical drivers for the growth of phishing-resistant adoption. The first is the ever-increasing threat of phishing attacks. For example, the Okta security team observed that the number of organizations that were impersonated by phishing increased by 50% from February 2023 to January 2024 compared to the same period in the previous year. Similarly, Zscaler saw a 58% increase in phishing attacks last year using the data from their network security products.[6]

The second is the availability of phishing-resistant options. Okta offers support for a broad selection of phishing-resistant authenticators, such as Okta FastPass and FIDO2 WebAuthn. Simplifying access to this technology has a direct impact on adoption. Okta made FastPass, the passwordless, phishing-resistant sign-in method built into Okta Verify, available to all customers as part of the free upgrade to Okta Identity Engine. We have observed that 7% of new or migrated OIE tenants who upgraded to OIE between February 2023 and January 2024 tried FastPass within their first 90 days.

Thirdly, we should also expect regulatory compliance to play a role in further driving the adoption of phishing-resistant factors. Government agencies in Australia, for example, must employ phishing-resistant authentication methods to satisfy Maturity Levels 2 and 3 of the Essential Eight controls.

Key insight

OIE offers more flexibility in managing login flows, such as application sign-on policies that allow administrators to configure individual rules for accessing applications, and to offer users a passwordless, phishing-resistant authenticator in Okta FastPass. We advise Okta customers to evaluate and implement stronger authenticators to maximize the benefits to users, not just for the convenience of administrators. For example, SMS authenticator is known to have a low assurance level, is subject to SIM swapping attacks, and has a higher cost to operate. For best results, both IT and Security teams should be involved in the upgrade to rapidly get the most value and evaluate the best authentication strategy for the organization.

[6] https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report

MFA user adoption rate by authenticator

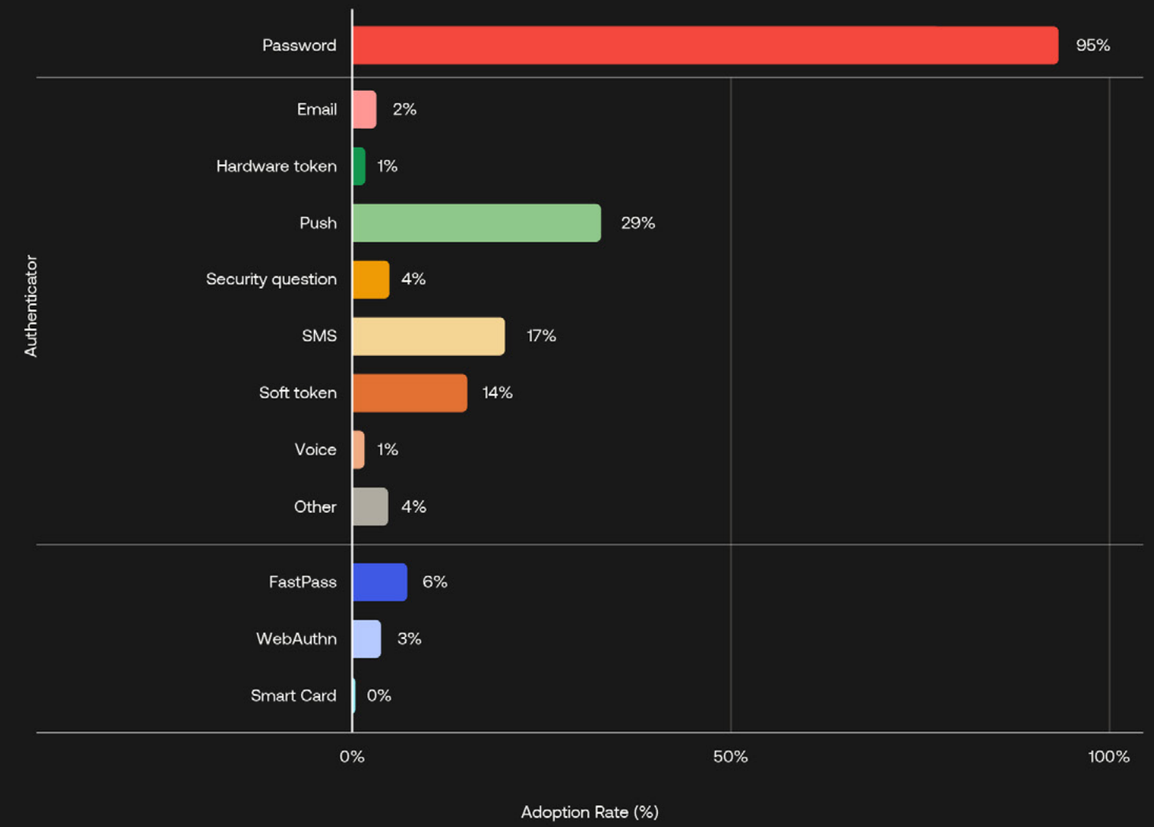


Figure 6: MFA user adoption rates for authenticators available on Okta Workforce Identity Cloud. The summation of the adoption rate for each authenticator is higher than the MFA adoption rate, given that users may authenticate with multiple authenticators.

A data-driven assessment of 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.

If you have read our 2023 Secure Sign-In Trends Report, this section will look very familiar. For the 2024 report, we have updated the metrics, but you won't find many significant changes - the time it takes to type in a password or receive an email code is pretty consistent. However, we included more users and events for this year's study since more organizations have migrated to OIE. Moreover, we improved our methodology using Okta IT and Security practitioners' survey inputs to determine the relative metric weights. Despite the revised, more practical criteria, we arrive at the same benefits of using a phishing-resistant authenticator. Additionally, we added metric data for smart card authenticators. We believe the insights from this session are helpful to anyone evaluating modern authentication methods, such as FastPass or WebAuthn.

Authenticator usability and security properties

Authenticator challenge time

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.

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

The median challenge times are consistent year-over-year for the authenticators. Password authentication continues to show a median challenge time of about six seconds. We assess that the challenge time of passwords is biased towards a shorter value via the assistance of password managers and browser autofill. For authentication flows that start with passwords, entering an OTP adds at least 12 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 (4 seconds). FIDO2 WebAuthn, Okta FastPass (as the name suggests) and smart cards offer a dramatically more efficient user authentication process than any other authenticator. Due to this speed, these authenticators 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.

Key insight

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.

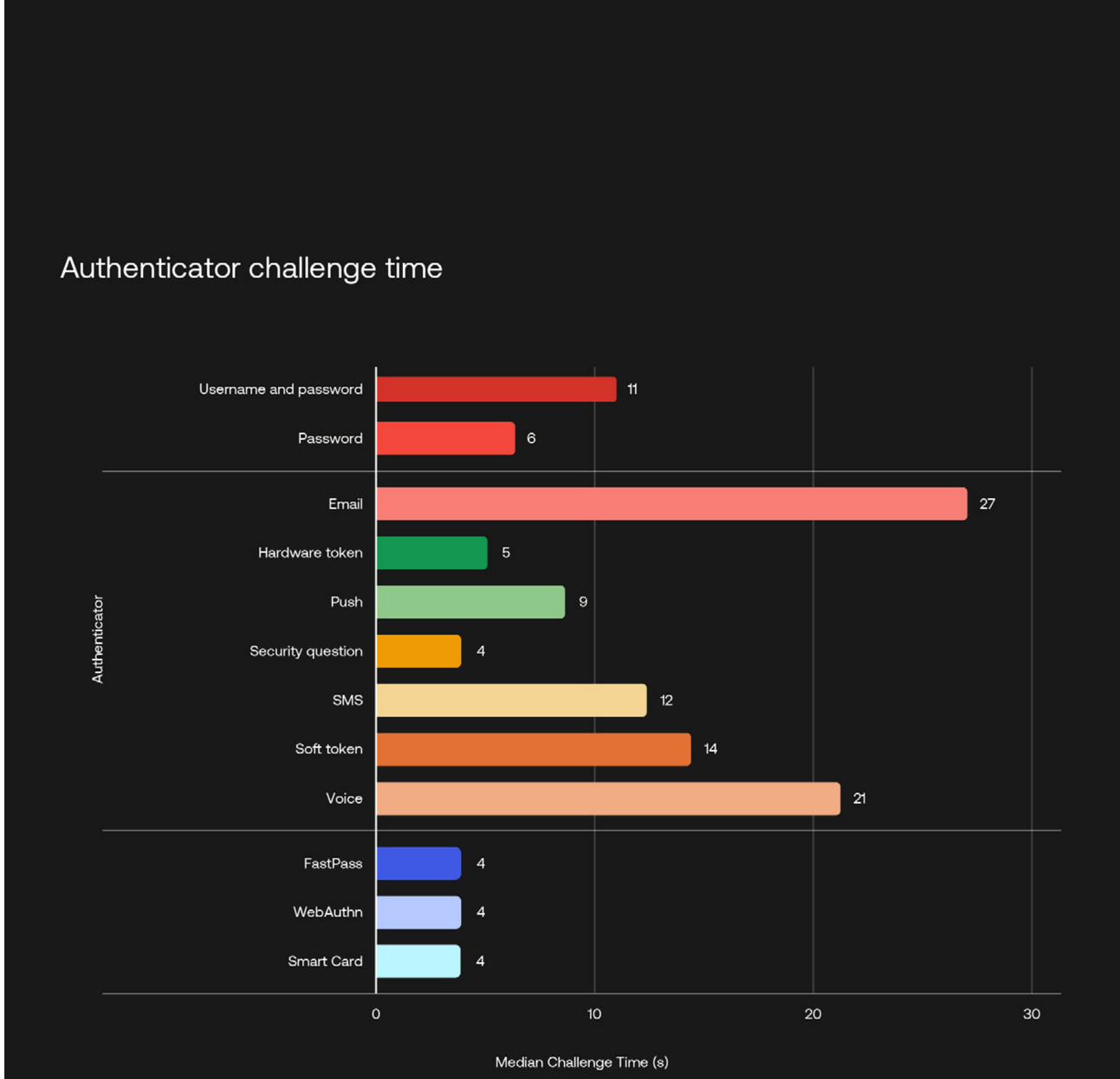


Figure 7: Median challenge times for password (both username-and-password and password-only flows), email, hardware token, push, security question, SMS, soft token, voice, FastPass, WebAuthn, and smart card authenticators.

“

Simple MFA is not enough anymore to defend against bad actors. With Okta FastPass, it's easy to level up and gain not only phishing-resistant MFA, but also gain contextual device posture awareness. You can dramatically shrink the universe of possible attack sources by implementing phishing resistance and by restricting access to highly sensitive applications to only managed devices. With device assurance controls you can also ensure that those devices are patched and intended controls are in force at the time of access.

However, security is not just an ever tightening process. If tighter controls degrade user experience you're just shooting yourself in the foot. That's why we've also implemented passwordless - with phishing resistance, managed devices, biometric-based user verification, and device posture we can achieve AAL2 and then some, while at the same time improving the day to day experience for our end users”

Andrew Meinert
Director of System Operations

HubSpot

Authenticator usability and security properties

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 phishing-resistant authenticators for this purpose.

The median time to register a password is approximately 35 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 or create security questions, and then 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 38 seconds, including the time required for a user to scan a QR code and complete the configuration process for Okta Verify. Hardware OTP, Voice, SMS, and FIDO2 WebAuthn boast the shortest enrollment times at less than 25 seconds. Smart card enrollment processes involve offline user verification, smart card manufacture, and shipment. It can take a few weeks to get a new smart card. Okta Identity platform doesn't have visibility into this process.

Key insight

Interestingly, we observed small increases in enrollment times across the board from 2023. Because enrollment is a manual process, there are many human and technical factors that could have caused this.

Organizations are increasingly turning to automated enrollment processes to help ease this burden. For example, in April 2024, Okta announced a partnership with YubiKey that would allow administrators to drop-ship pre-enrolled YubiKeys to employee's homes. The user experience is then reduced to the time it takes to insert the key and type an initial PIN, allowing employees to be productive almost immediately.

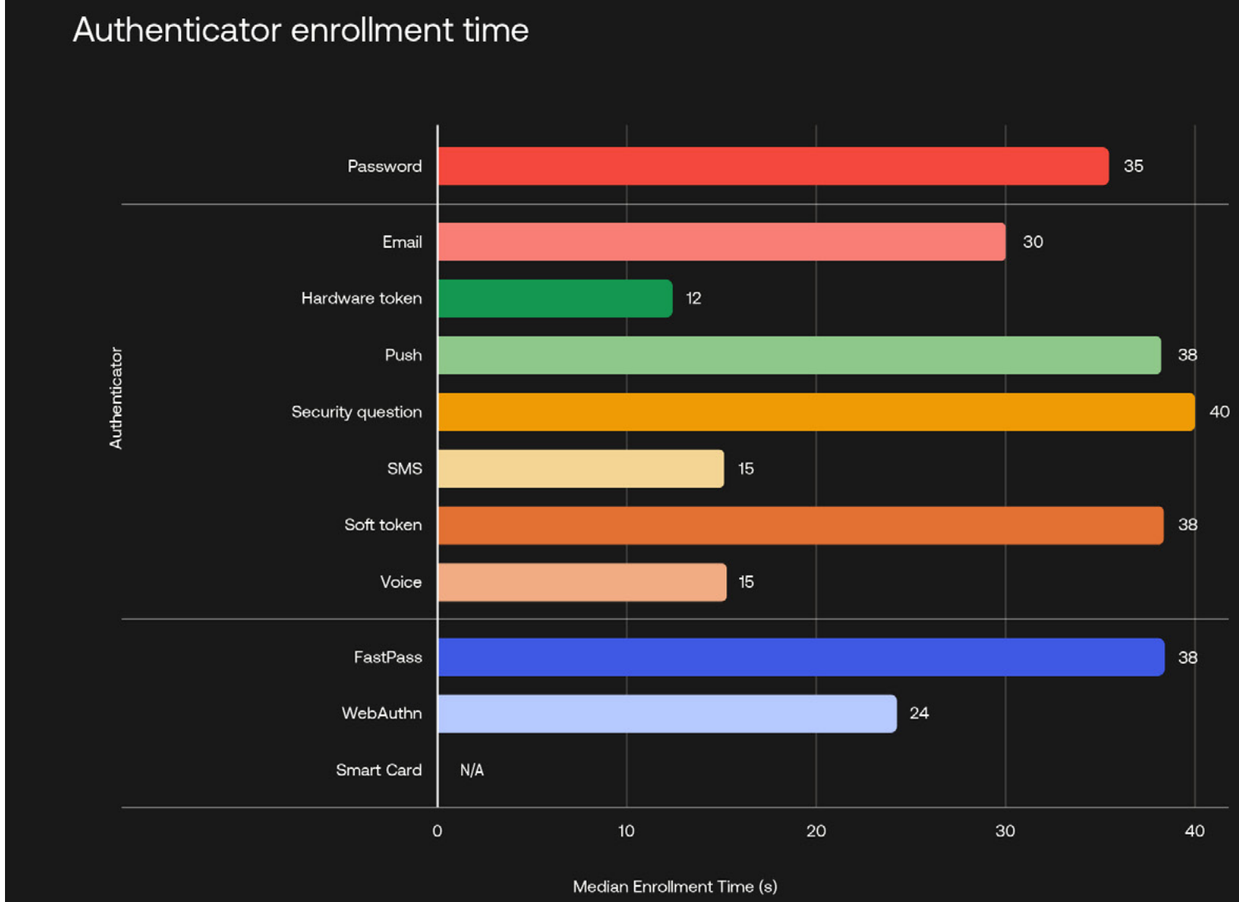


Figure 8: Median enrollment times for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, WebAuthn, and smart card authenticators. Time spent on user verification was excluded from this analysis because it is determined by enrollment and recovery policies, rather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

Authenticator usability and security properties

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 both 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. Unfortunately, determining a benign event from a malicious event requires additional knowledge of usage patterns that are not available in the anonymized data we have for this report. Your security team may be able to develop these reports for your environment.

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 almost 10%), followed by soft tokens, authentication challenges sent over email, and security questions.

FIDO2 WebAuthn and smart card authentication will logically result in fewer unintended user mistakes ("fat finger errors") and fewer suspicious attempts, leading to low failure rates. However, these findings come with one caveat. The implementation of WebAuthn and smart cards isn't entirely consistent with other authentication methods. By design, the authentication action for these methods happens on the user's system, so the Identity Provider (Okta) cannot capture all failed events for these authenticators. For example, if a user uses FIDO2 WebAuthn to attempt to sign in to a phishing proxy and the authenticator detects a domain mismatch, there is no mechanism for sending this information to the back-end servers of the Identity provider. This prevents the administrator from accurately reporting on the number of malicious authentication attempts.

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.

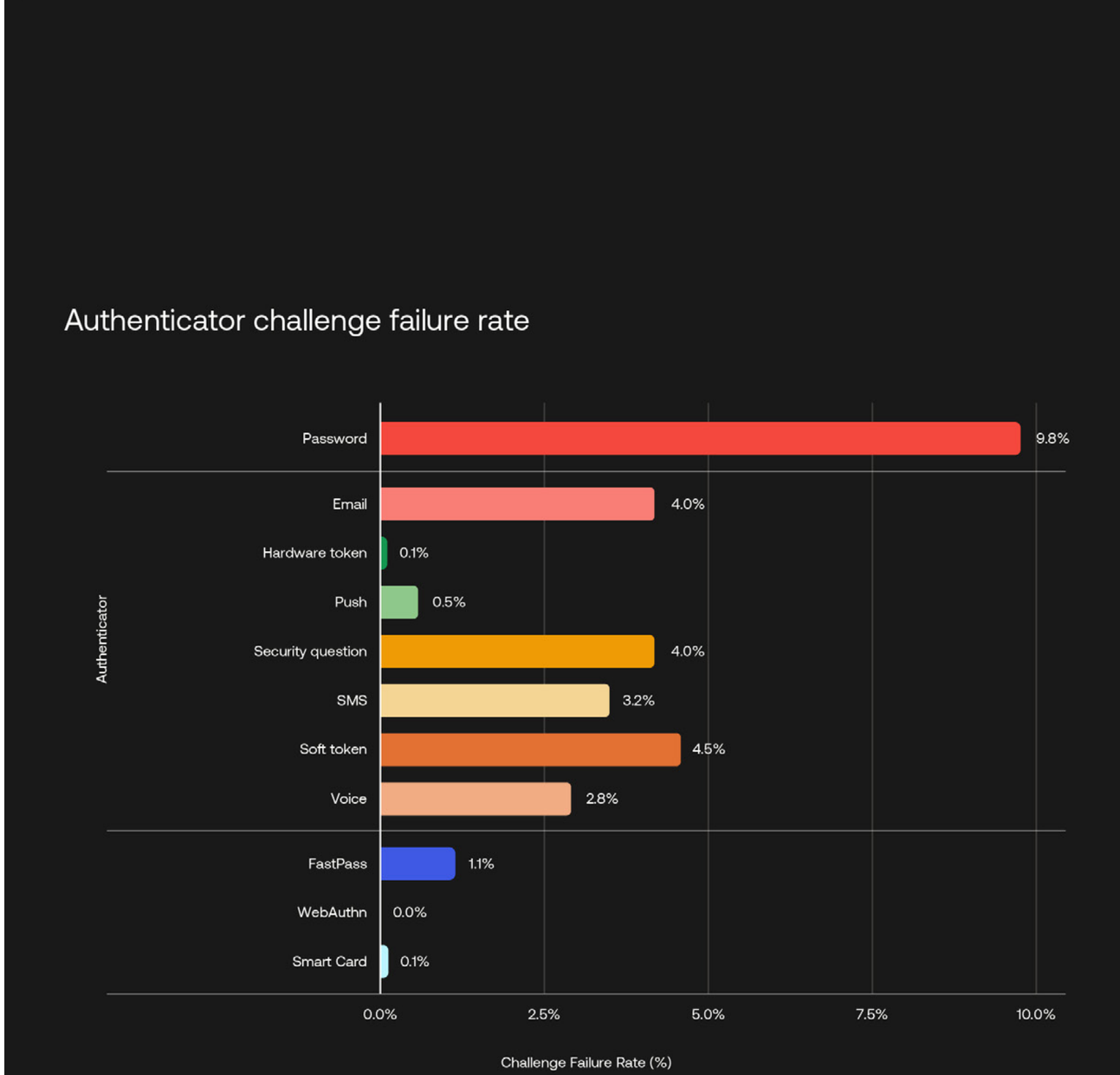


Figure 9: Challenge failure rates for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, WebAuthn, and smart card authenticators.

Authenticator usability and security properties

Phishing-resistant coverage

Phishing-resistant coverage describes the potential percentage of users 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 users whose browsers and operating systems support those capabilities. Based on these criteria, three authenticators have phishing-resistant coverage above zero: Okta FastPass, FIDO WebAuthn, and smart card.

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, 96% 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 95% of users 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. However, not all WebAuthn implementations are the same. These inconsistencies between Windows, MacOS, iOS, and Android, for example, can create confusion and a poor user experience. The introduction of multi-device passkeys represents a significant leap forward for consumer authentication use cases, but can create issues within the Workforce context where the ability to move a passkey between devices can be a violation of company policy. Moreover, some operating system providers recently stopped supporting device-bound WebAuthn in favor of multi-device passkeys, making the user experience unintuitive.[7]

FastPass is also tailored to workforce use cases and security models, providingsuch as strong device binding and device assurance posture checks. It also maintains a consistent look-and-feel across all platforms, including desktop and mobile, encouraging users to use the strongest available authentication methods.

As Smart cards require specialized hardware, deployment of this technology is typically limited to highly regulated industries that can afford to have a homogenious IT infrastructure.

[7] https://passkeys.dev/device-support/

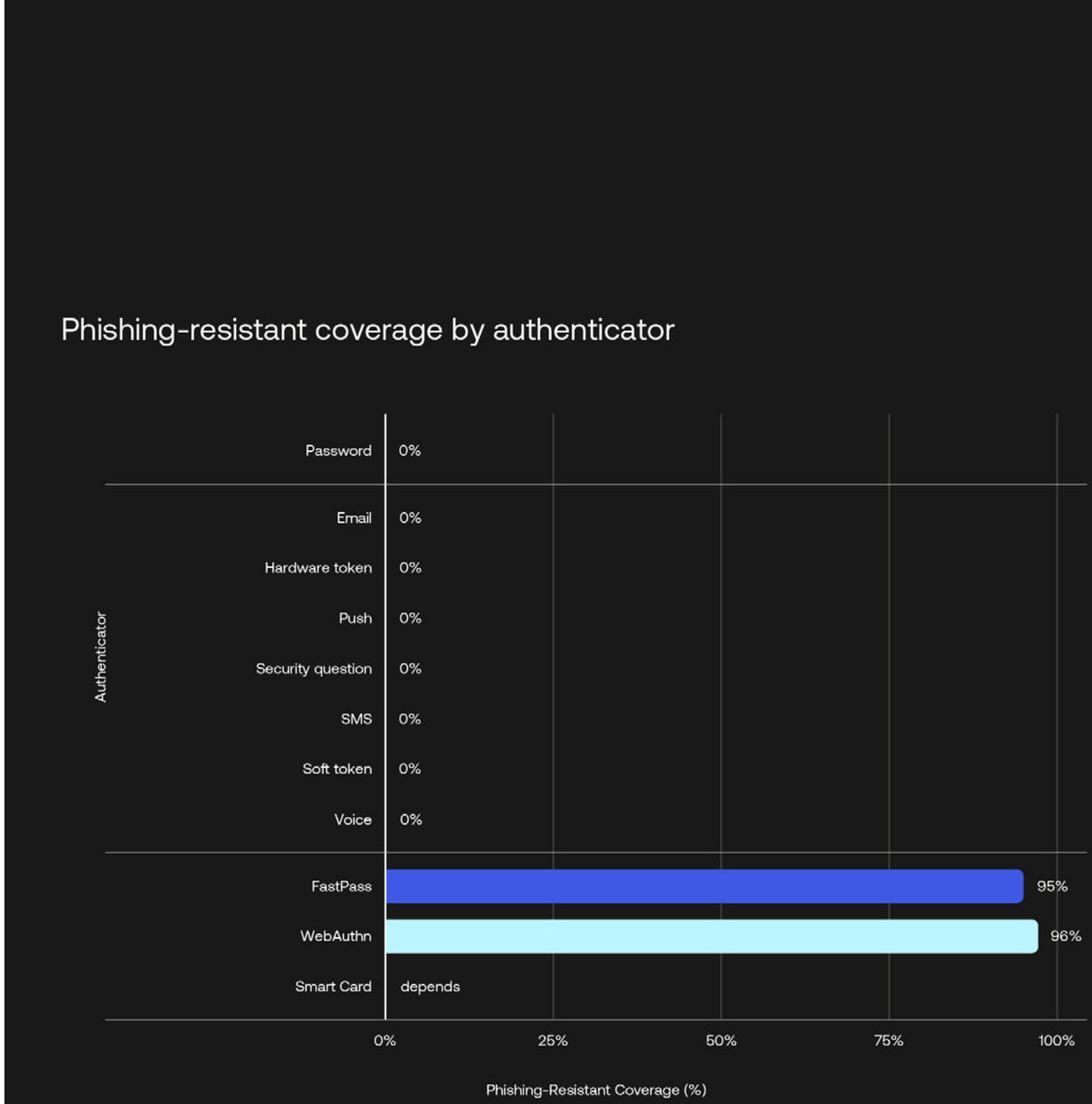


Figure 10: Phishing-resistant coverage for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, WebAuthn, and smart card authenticators.

Authenticator usability and security properties

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 phishing site domain name or cookie mismatch is detected, FastPass rejects the request and alerts the end user and administrators. It also increases user and organizational awareness of threats, improving their ability to detect and respond to malicious activity.

FastPass saves the day

The case study below is based on the experiences of an Okta customer who upgraded to OIE and rolled out FastPass in early 2023.

On a July 2024 evening, one of our employees received a phone call from a widespread social engineering campaign that targeted hundreds of organizations. The caller, who had an American accent and was calling from a spoofed phone number matching one of the actual corporate phone numbers, introduced themselves as the IT team, and instructed the employee to log into a website that was very similar to a company domain. The user was enrolled in Okta FastPass. FastPass denied the login attempt because the domain and certificate didn't match the customer's Okta org. Over the next five minutes, the threat actor convinced the user to make multiple attempts to sign in via the phishing site, and FastPass denied all of them. The security team, already alerted of unsuccessful social engineering attempts by other users, was able to quickly see these failed attempts in the system log and respond, going as far as temporarily removing access for the targeted user. By the next morning, this targeted user was able to regain the necessary access and go back to their work.

In a subsequent investigation, it was clear that FastPass and its alert coverage capability saved the customer from account takeovers by the social engineering actor and minimized the impact on employee productivity.

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 Unified Endpoint Management (UEM) and Endpoint Detection and Response (EDR) vendors. such as Jamf, Microsoft Intune, Workspace One, CrowdStrike, Windows Security Center, and Chrome Device Trust,[8] to ensure an authenticating device is managed and/or demonstrates an appropriate level of security hygiene. This contextual information can further enhance threat detection and authentication policy enforcement.

Key insight

We expect that the ability to proactively detect and alert on social engineering and AiTM phishing campaigns will become more critical as the speed of detection and response becomes a key differentiator in fighting against cyber attacks. Leveraging Okta FastPass alert capability can provide near real-time phishing protection and detection for organizations.

[8] https://support.okta.com/resource/device_context_deployment_guide

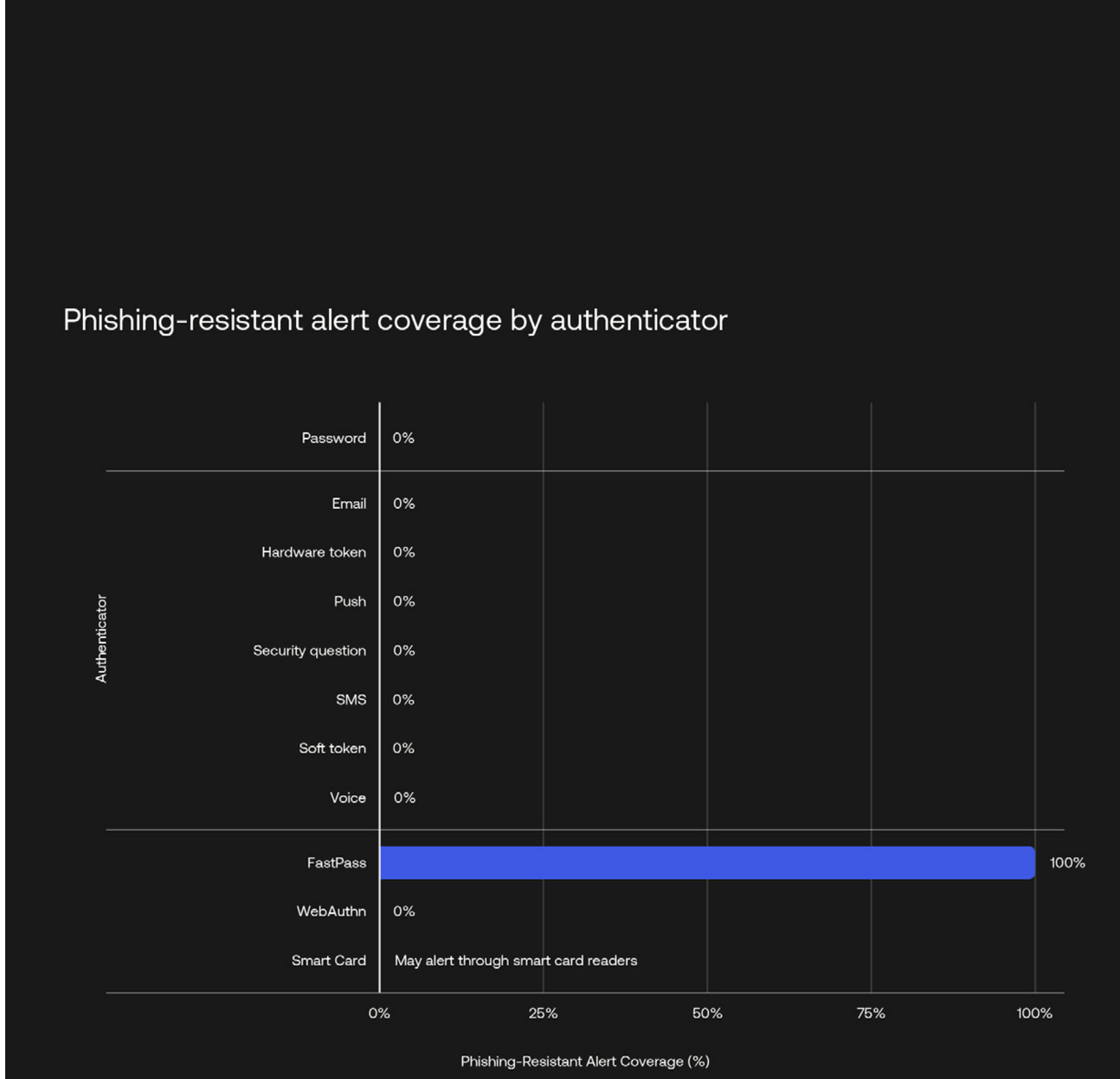


Figure 11: Phishing-resistant alert coverage for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators.

Authenticator usability and security properties

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, where N is a threshold number used to define a possible brute-force failure. For this report, we have used N=10 in the analysis, as it would be highly unlikely that a legitimate user would try so many times. 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 also reflects adversary preferences for conducting brute-force attacks against a given authenticator.

Similar to what we saw in the 2023 report, knowledge-based secrets continue to be targeted by the automated tools of attackers most often or create the most friction for legitimate users who continue login attempts despite multiple failures. FIDO2 WebAuthn has the lowest brute-force failure rate but is subject to the same caveat described previously - due to the implementation of the standard, all failures may not be reported back to Okta resulting in an artificially low score.

FastPass operates differently than other authenticators and has two types of probing schemes. Silent probing or silent authentication allows the Okta Sign-In Widget to automatically check whether FastPass is configured on the device and can be used to authenticate a user with no user interaction. Interactive probing or standard authentication operates more traditionally, and is triggered when a user logs in using a FastPass authenticator. The silent authentication runs in the background, providing frequent device and user checks without extra user friction. As a result, the FastPass challenge happens more frequently than other authenticator types, which is likely to contribute to the relatively large FastPass challenge brute-force failure rate.

Key insight

While MFA bypass events are catching up, 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 account takeover from brute-force attacks.

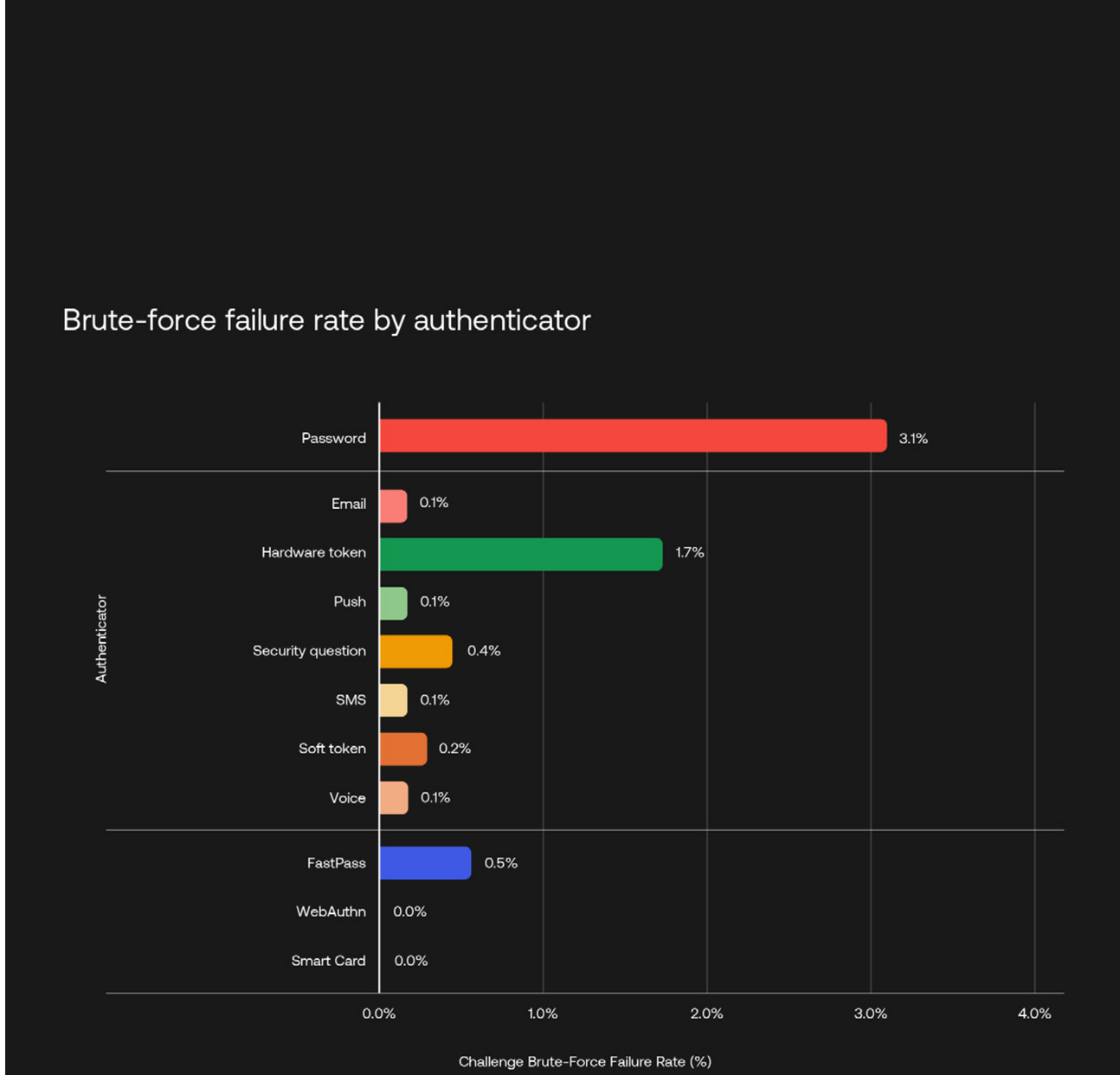


Figure 12: Brute-force failure rates for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators. The data was collected from November 2023 to January 2024.

Authenticator usability and security properties

Authenticator Metric Survey

In last year's report, we used metric weights to describe the relative importance of the authenticator metrics. We came up with the weights using our internal knowledge of authenticator properties, and the degree to which customers reference them.

After publishing the 2023 report, we explored ways to make our metric weights more practical. We decided to conduct a survey of Okta IT and Security practitioners to understand the relative importance of each of the usability and security metrics to an authenticator's usability and security properties. The results of this survey allow us to align the data we collected from our logs with the importance that our administrators place on those metrics, as shown in Table 2, versus the estimations used previously.

Putting it all together, we were able to use the survey results to calculate and plot authenticator usability and security scores. First, we took the maximum and minimum scores in each category to normalize the metrics for each authenticator into the 0 to 1 range. For example, Webauthn gets a challenge failure rate score of 1, while Password gets a score of 0. Then, we weighted those scores according to their impact on authenticator usability and security using the survey result. This gives us the plot of usability and security scores of the authenticators in real-world conditions and priorities. Turn the page to see how your favorite authenticator is stacked up.

Key insight

One critical success factor in strengthening your security infrastructure is gaining full alignment and commitment among security and IT stakeholders. The metric weight survey can serve as an effective way to achieve agreements on key considerations and risks in choosing authentication methods.

Table 2: Authenticator usability and security assessment categories

Adoption		Usability		Security	
Metric	**Weight**	**Metric**	**Weight**	**Metric**	**Weight**
User-level adoption rate	N/A	Challenge time	7.33/10	Challenge failure rate	5.71/10
		Enrollment time	5.14/10	Challenge brute-force failure rate	7.14/10
		Challenge failure rate	6.25/10	Phishing-resistant coverage	8.65/10
				Phishing-resistant alert coverage	7.47/10
Adoption scores of authenticators		**Usability scores of authenticators**		**Security scores of authemticators**	

“Asking individuals to collect and remember unique, strong passwords is a dated approach doomed to failure. The great thing about passwordless MFA options – they’re both convenient and more secure. That’s rare.

Security benefits only matter if they drive business faster and open opportunities for growth. Passwordless sits squarely in this bucket. MFA factors that exclude passwords are faster, simpler, reduce costs and open the door to more integration partnerships.”

Shana Uhlmann
IT Director and CISO

Tattarang

Authenticator usability and security properties

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?

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.

Key insight

Implementing MFA and passwordless at scale is a cultural challenge more so than a technical one. Organizations need choices and flexibility. The Okta Identity platform provides a broad set of options to cater for the unique needs of your organization. You can apply the methodology and framework that best suits you. We hope that our approach to defining the relative weight of authenticator properties, and aligning these metrics with key stakeholders, inspires you to think about new ways to promote stronger authentication in your organization.

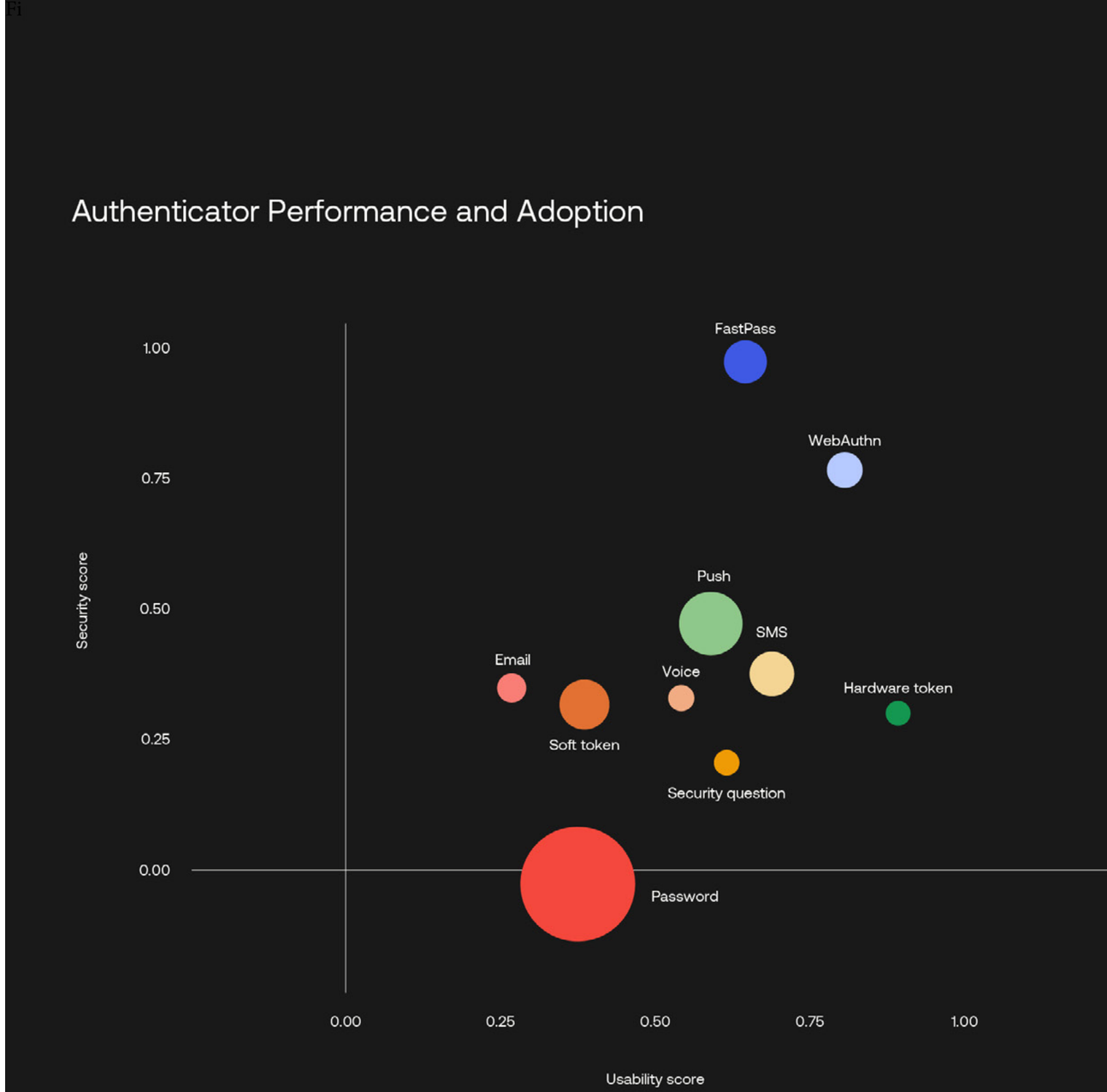


Figure 13: Authenticator performance and adoption for password, email, hardware token, push, security question, SMS, soft token, voice, FastPass, and WebAuthn authenticators. Each authenticator's performance is represented by its usability and security scores as shown in a 2x2 matrix. The size of the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

The way forward

When you consider the degree of success attackers have had over the past 12 months using phishing and social engineering techniques, you would expect to see stronger adoption of phishing-resistant authentication methods. In the months since this data was collected, a number of high profile security events have forced the issue. Salesforce, GitHub, Okta and Microsoft are all committed to mandatory MFA rollouts for portions of their user base. FastPass adoption is accelerating among Okta customers, and concerns about new phishing threats enabled by the AI evolution are hitting the airwaves and the boardrooms. So we are optimistic!

Phishing-resistant MFA is secure, user friendly, and achievable. It's a win-win for administrators and users. It is the leading technology to protect against pervasive threats. We need to help our organizations adopt this technology. At Okta, we hope that this report can help you talk with your executives and users about the journey to stronger, easier authentication by allowing you to compare your position against those of your peers.

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.

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.

Disclaimer

This document and any recommendations about your security practices are not legal, security, or business advice. This document is intended for general informational purposes only and may not reflect the most current security and legal developments nor all relevant security or legal issues. You are responsible for obtaining legal, security, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of the recommendations in this document.

okta

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