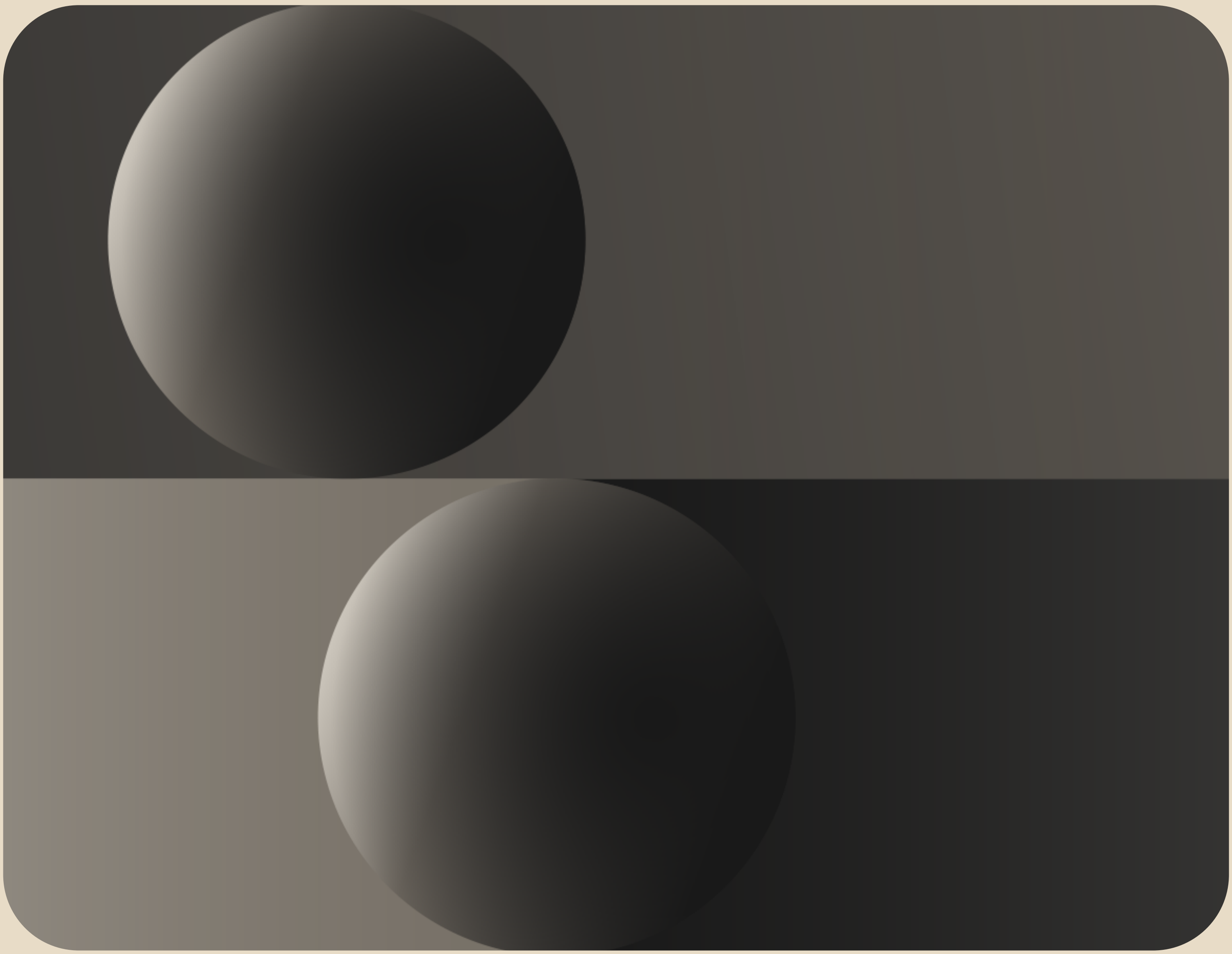
2023 | Insights

Which sign-in methods do customers rely on today and what is the state of MFA Adoption in organisations globally?

The Secure Sign-in Trends Report

Executive Summary



okta

Introduction

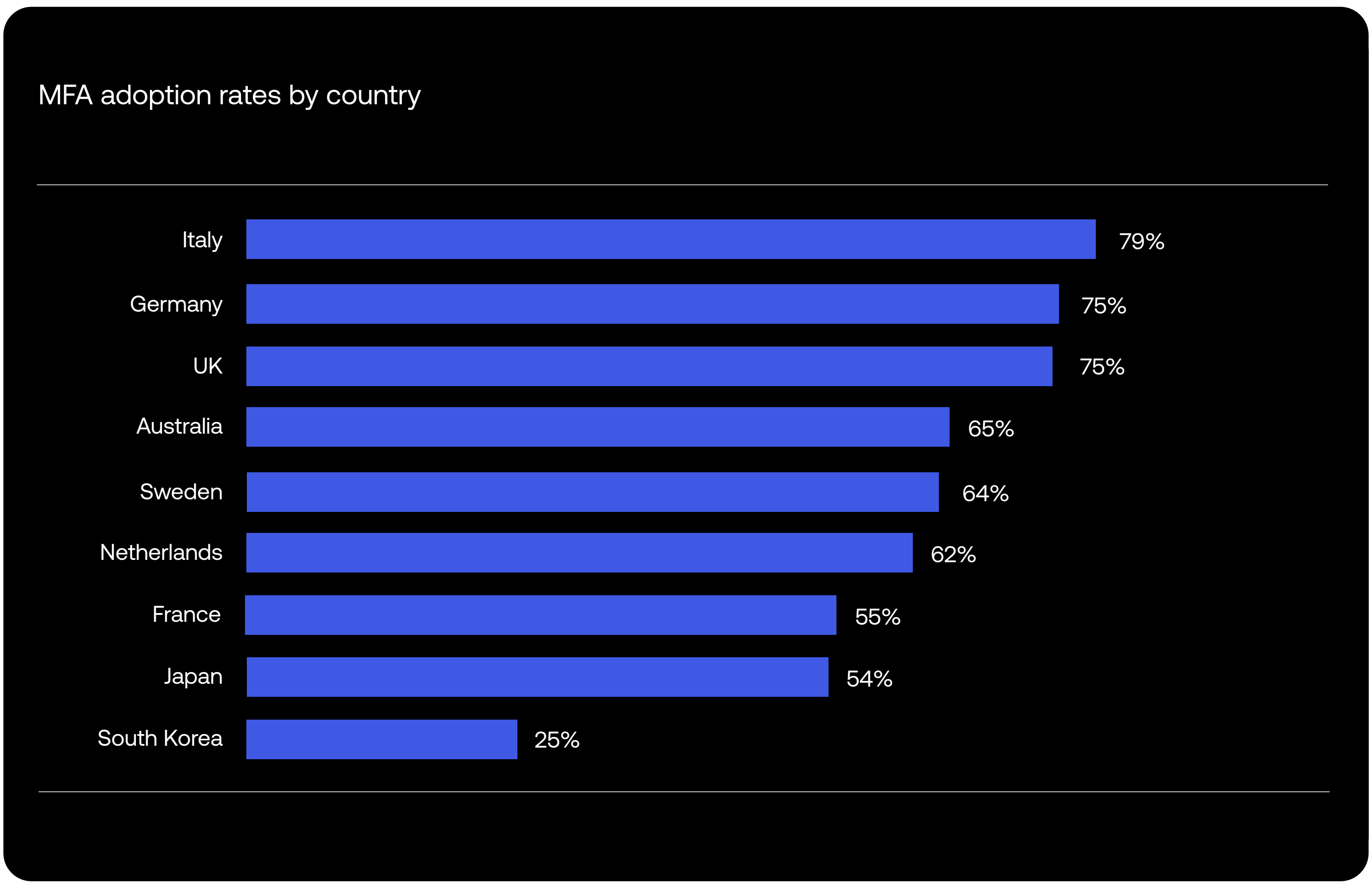
In today's hyper-connected digital world, swift, seamless, and secure authentication has never been so important. It's what helps security leaders better protect customers and employees from cyberthreats that are constantly evolving. It's what empowers customers and employees to access all the apps, tools, and services they need, whenever and wherever they need them. And it's what helps organisations stay compliant, no matter what happens.

Yet, traditional username and password verification is struggling to keep up with the pace of change. It's inefficient, it increases the risk of data breaches through credential-based attacks, and it creates unwanted friction that can damage the customer experience. However, while alternative solutions such as phishing resistant authentication exist to help solve these challenges, many organisations are hesitant to invest, fearing that doing so would damage their customers' experience even further.

In this executive summary, we've summarised the findings from the main report to dispel the myth that phishing resistant authentication leads to extra friction. We also look at key trends that show how Okta customers are choosing to verify their identities online and why Multi-Factor Authentication adoption (MFA) should be a key priority for every security leader pushing forward. ■

MFA adoption continues to grow.

While the initial surge in MFA adoption amongst Okta customers was driven by the need to securely enable remote work and protect employee data during the pandemic, growth has shown no signs of slowing in 2023 — achieving a 6% YOY increase, taking total adoption to 64% overall. As organisations continue to focus on battling sophisticated threat actors and cyberattacks, the need for stronger security measures is critical to protect company resources and sensitive data — and MFA has proven the go-to solution for many organisations across Europe and APAC. ■



MFA adoption rates differ greatly by size and industry.

Though MFA adoption rates remain largely consistent throughout all regions included in the survey, the results differ greatly based on company size and industry. Whereas less regulated sectors like professional services (75%) and media/communications (72%) follow hot on the heels of leaders in the technology space (87%), industries with higher regulatory oversight, such as government (48%), healthcare (56%), financial services (60%), and energy (62%), seem slower off the mark – largely due to their reliance on legacy applications that are limited to basic authentication methods like usernames and passwords.

Company size is also an important factor: with large organisations of 20,000+ employees showing the lowest rates of adoption (54%). Meanwhile, those with fewer than 699 employees tend to have the highest MFA adoption (79%-80%) – again, this gap is most likely due to larger enterprises' dependence on legacy infrastructure and their tendency to use multiple Identity providers rather than one centralised solution provider. ■

Passwords persist, despite their drawbacks.

While passwords remain a popular authentication method for 100% of Okta customers, they're easily compromised and often serve as the first step in the data breach kill chain. Though alternative sign-in methods such as phishing resistant authenticators offer a much higher assurance level, there exists a misconception that implementing them would introduce even more friction for users – but the truth is quite the opposite.

According to data taken from the report, authentication flows that start with username and password verification add at least 13 seconds to the authentication flow – and even longer if the user must retrieve an OTP from an email or voice call. By comparison, authenticators that combine possession and inherence (such as biometric checks) offer the fastest and most efficient challenge times – with FastPass (4 seconds) and WebAuthn (3 seconds) taking the lead. ■

In summary

Transitioning towards passwordless authentication may seem daunting and complex at first, but it is an essential step forward. This is particularly true when considering that username and password combinations consistently score the lowest in terms of both security and usability in the Authenticator and Performance Adoption chart.

Relying solely on passwords puts organisations and individuals at a significant risk, as cyber threats continue to evolve and target this weak link. By embracing passwordless authentication solutions, organisations can improve security, streamline user access, and protect sensitive data more effectively.

To learn more about what approaches global brands are taking to verify their users' identities and prevent unauthorised access – read **The Secure Sign-in Trends Report** in full.

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 customisable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com/uk

okta

EMEA Headquarters
20 Farringdon Road
London EC1M 3HE, UK
info_emea@okta.com
+44 203 389 8779