OCTOBER 2022

IC CONSULT | SECRET DOUBLE OCTOPUS

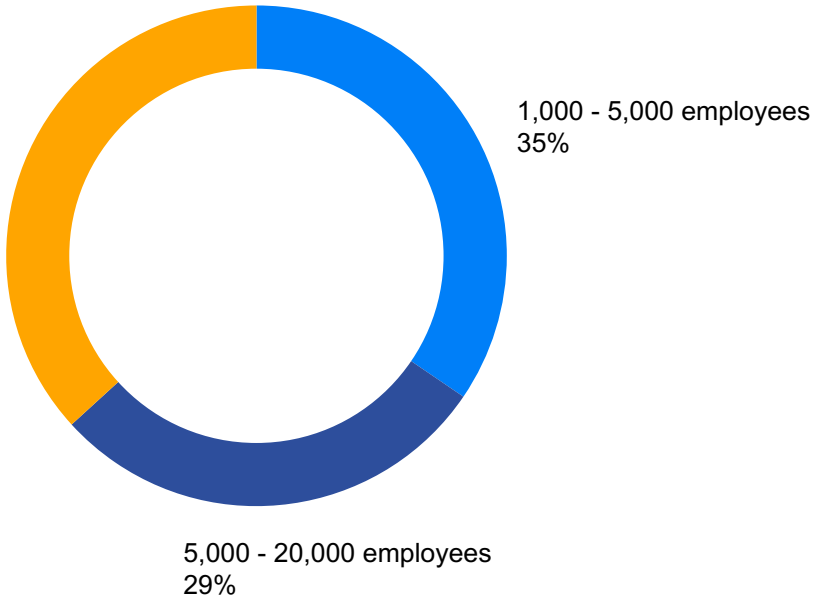
# 2022 State of Workforce Strong Authentication

## E-Book Summary

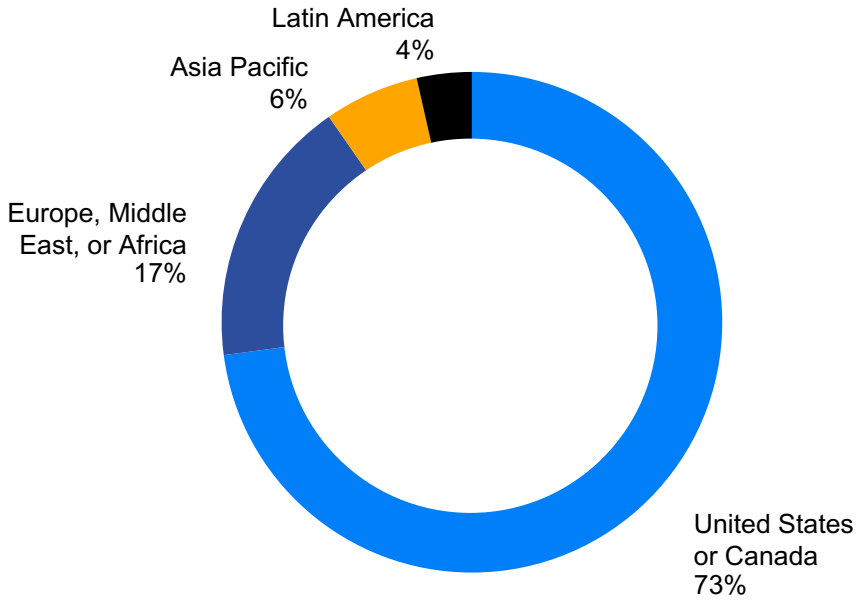
# A Global IT Survey around IAM

Dimensional Research and SDO surveyed 310 IT professionals with responsibility or knowledge of their organizations IAM decisions and strategy to better understand current traction and attitudes for MFA and workforce passwordless authentication solutions. All respondents had to work at organizations with more than 1,000 employees. The following charts show additional demographic data:

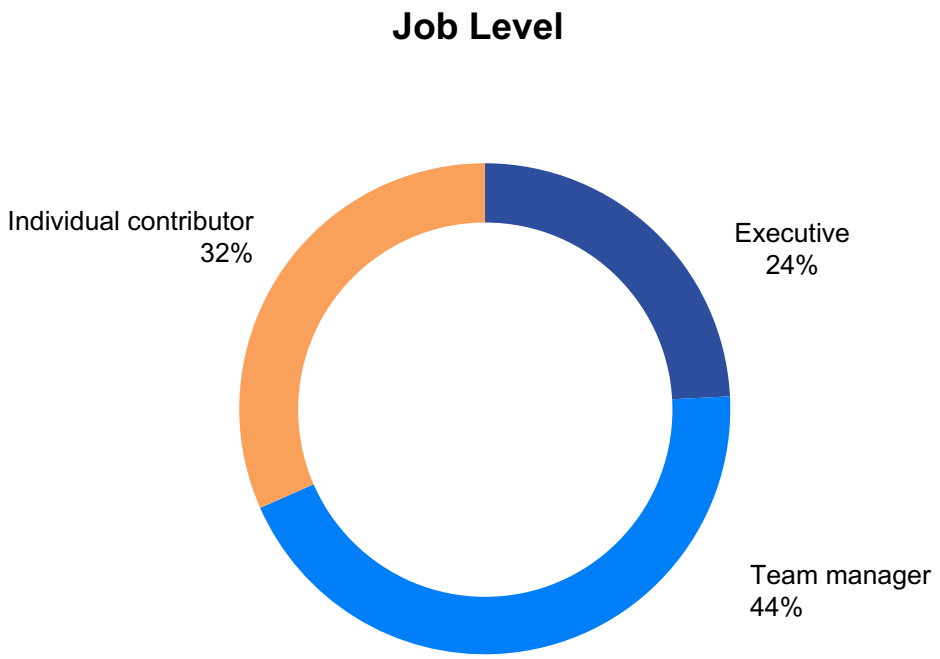
**Company Size**

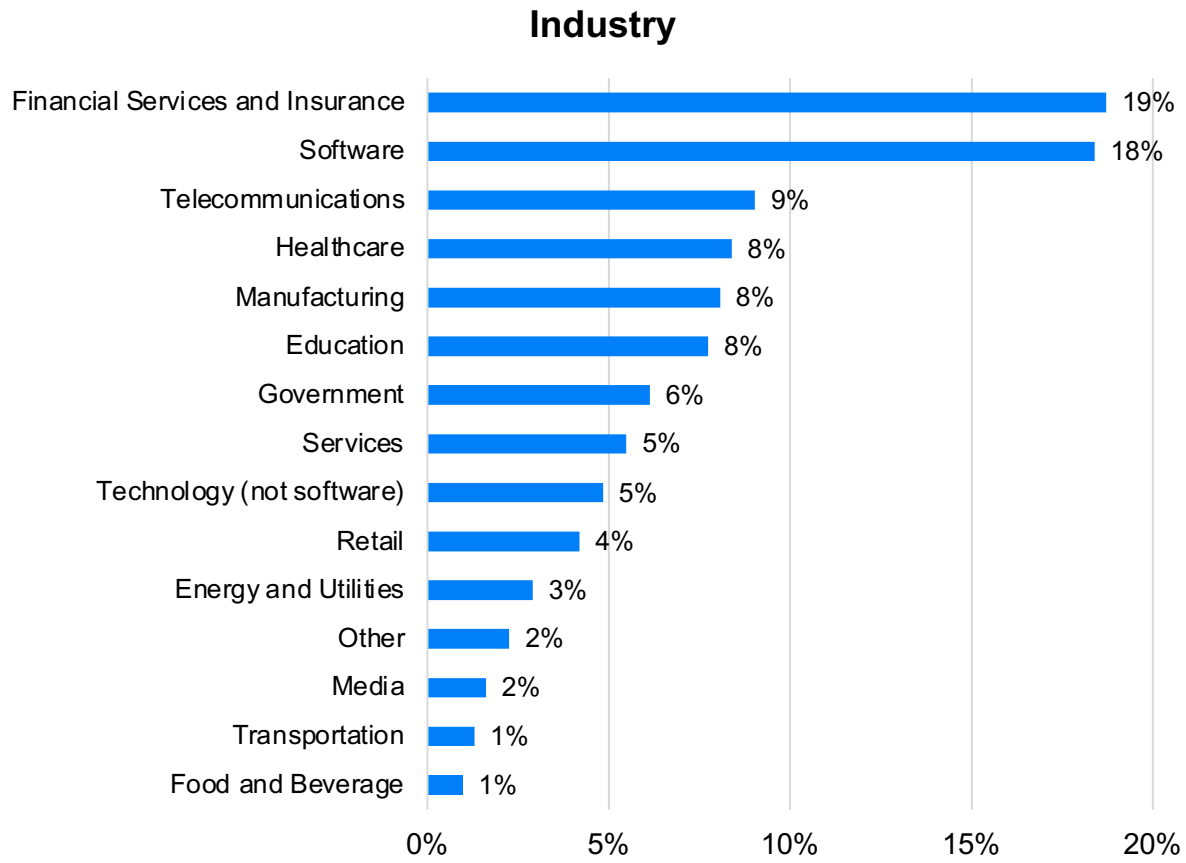



**Region**



# Broadly Diversified Across Level and Industry



# MFA is a work-in-progress for large enterprises

## Only 16% use MFA universally across all use cases

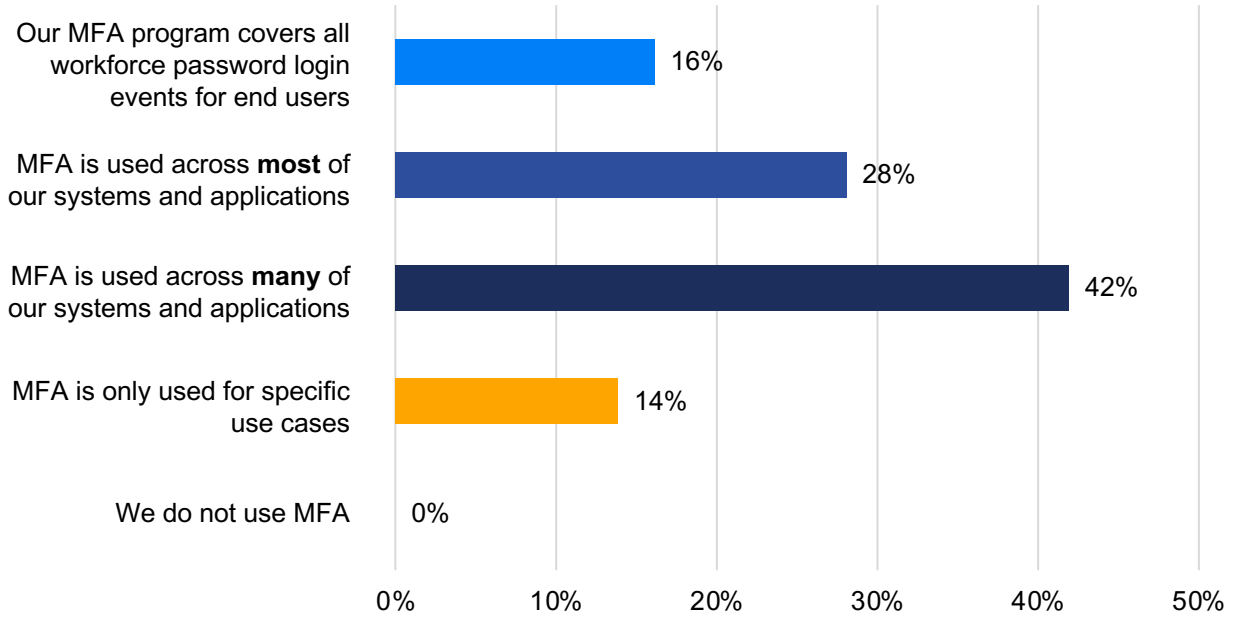
The ability to use MFA universally is important given hackers will find a way to get to the weakest link.

The 2022 survey revealed the same findings as our 2021 research –that enterprises are still using MFA sporadically.

Passwordless promises to be a next-generation investment that provides a universal user experience for authentication across all use cases.

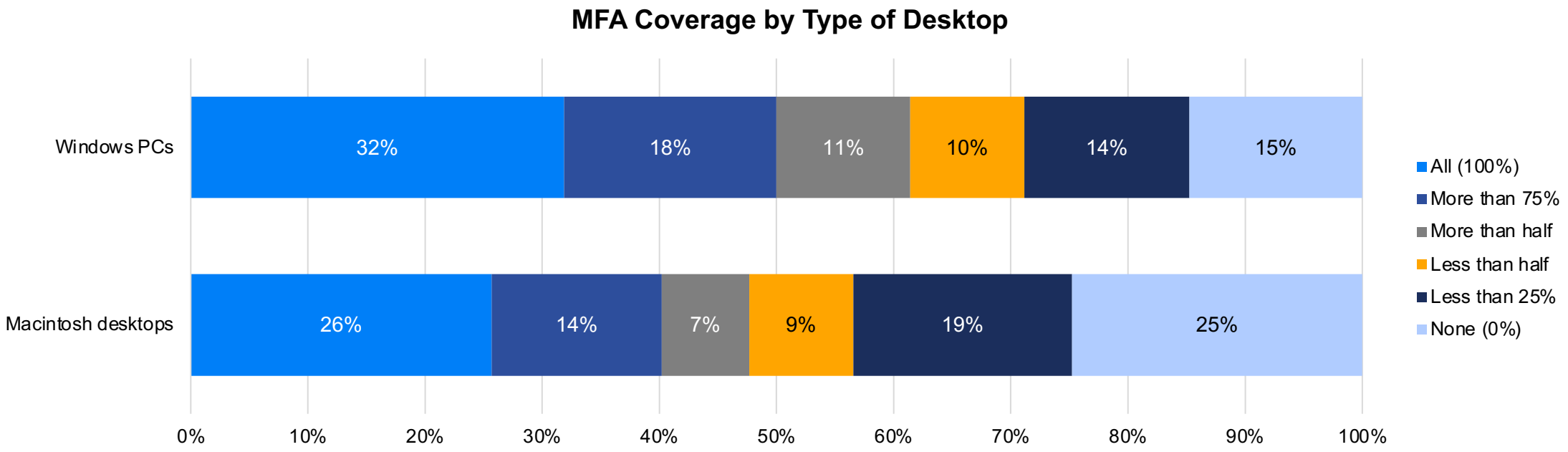
**How would you characterize your organization's adoption of MFA (Multi-Factor Authentication) for workforce passwords?**

Choose the one answer that most closely applies.



# Desktop MFA Use

50% of respondents felt 75% or more of their Windows PCs are protected by MFA while only 40% of them felt 75% or more of their Macs were protected.



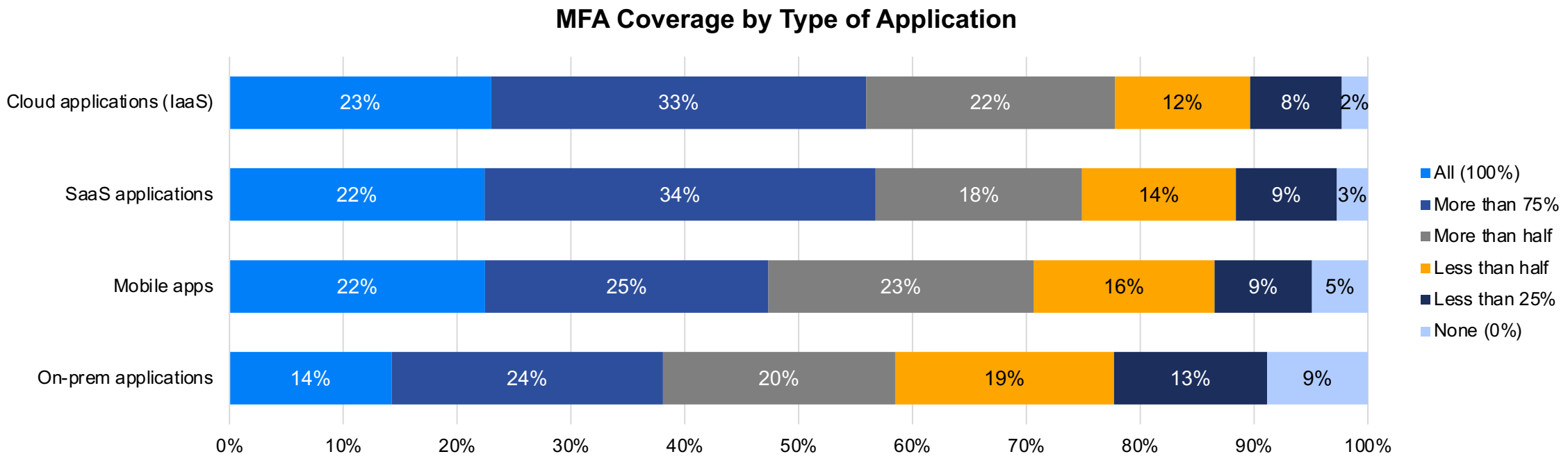

In 2021, desktop MFA was estimated at 41% use in organizations.




iC CONSULT | SECRET DOUBLE OCTOPUS

# Application MFA Use

On-premise applications make up the least MFA protected type of application. Not surprisingly, Cloud and SaaS apps lead in MFA coverage.



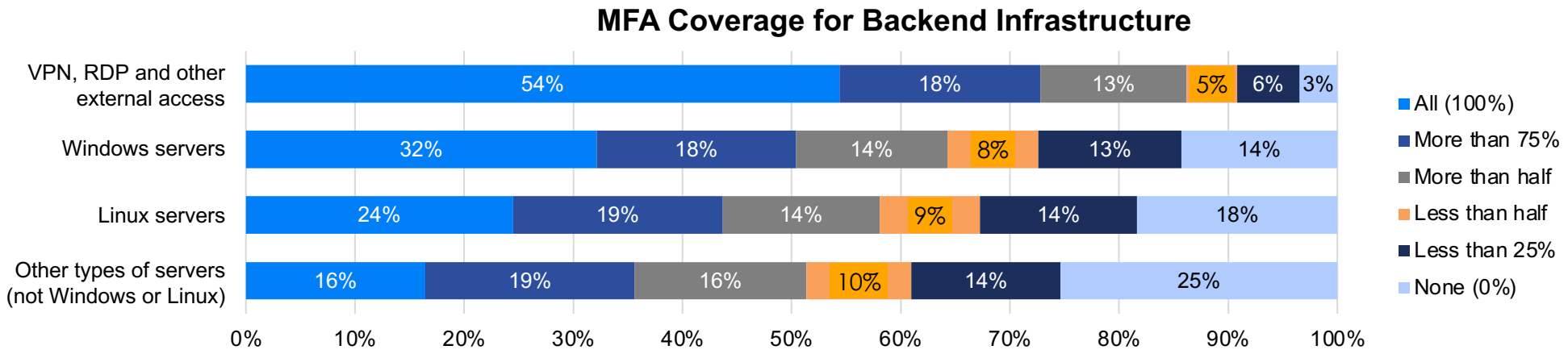


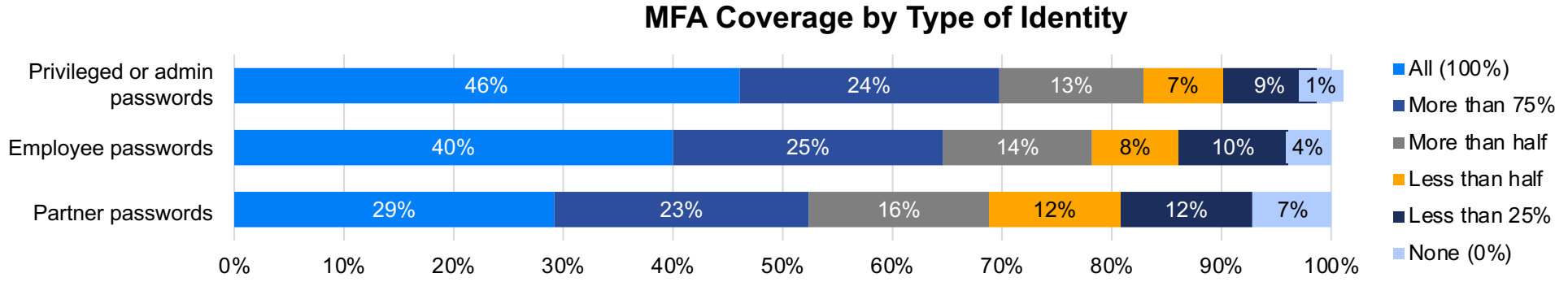


iC CONSULT | SECRET DOUBLE OCTOPUS

# Additional MFA Use

VPN and RDP are heavily covered by MFA, with Linux servers lagging behind Windows Servers. Privileged users/admin MFA use is high relative to partner MFA use.



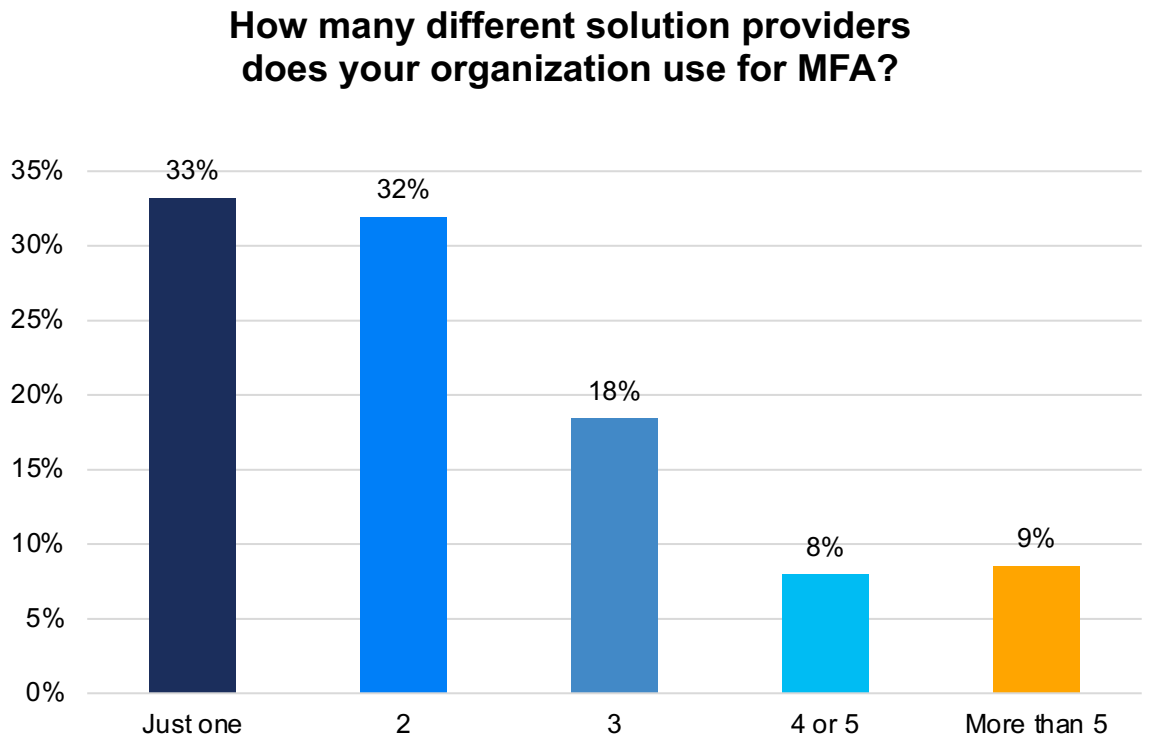



# Most organizations have multiple MFA solutions

67% have 2 or more.

Along with different MFA end user experiences, having multiple MFA solutions burdens IAM and IT security teams.

Yet most organizations have multiple MFA solutions to meet their needs, highlighting the challenge MFA has had in having universal end-to-end coverage.



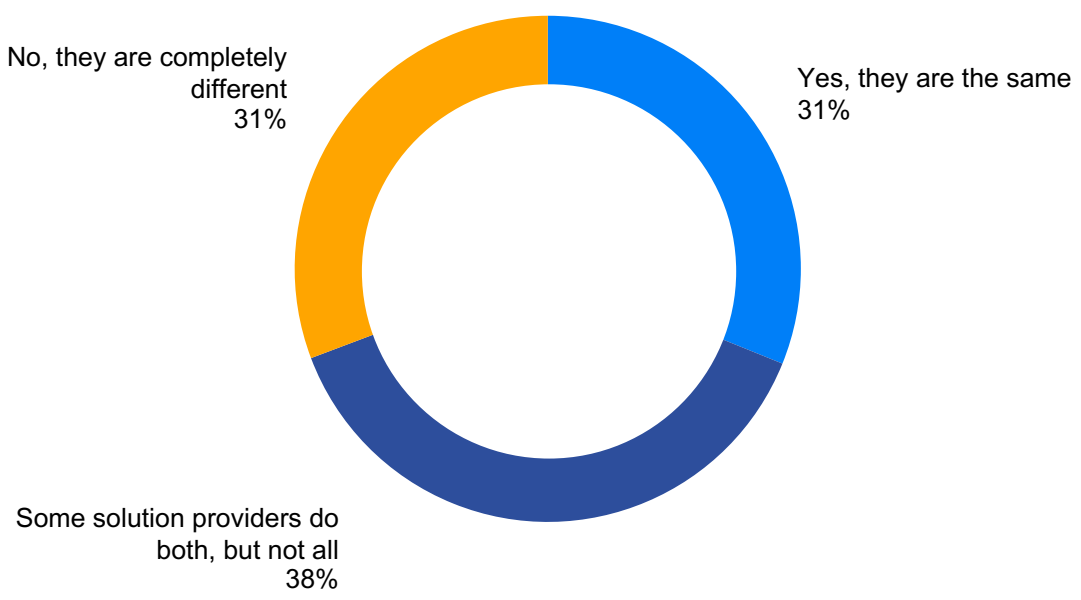
# Most organizations buy MFA solutions from vendors outside their SSO provider

69% of orgs have an MFA solution outside of their SSO providers.

The data here is mixed, because 69% of orgs use an MFA from their SSO provider –with 31% buying exclusively from the SSO provider.

But 69% also use at least one other MFA provider outside of their SSO provider, with 31% not using an MFA from their SSO provider altogether.

**Does your organization use the same solution provider for both MFA and SSO?**







iC CONSULT | SECRET DOUBLE OCTOPUS

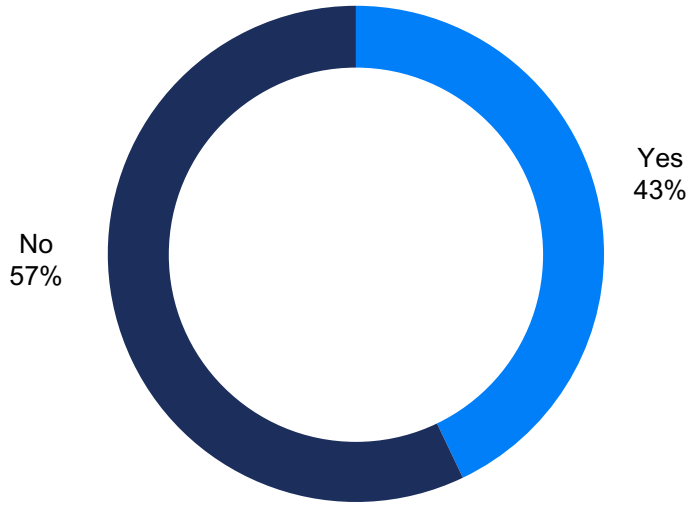
# Adaptive MFA is not mainstream yet in large enterprises

Despite all the talk about adaptive risk decision making with Zero Trust, most organizations have not deployed adaptive MFA today.

Many organizations look to adaptive MFA to improve the user experience and frustration end users feel when using MFA (aka ”MFA fatigue”).

How are end users feeling about MFA these days?

**Does your organization use “adaptive MFA” where risk analysis is used for deciding when to provide an MFA prompt?**







iC CONSULT | SECRET DOUBLE OCTOPUS

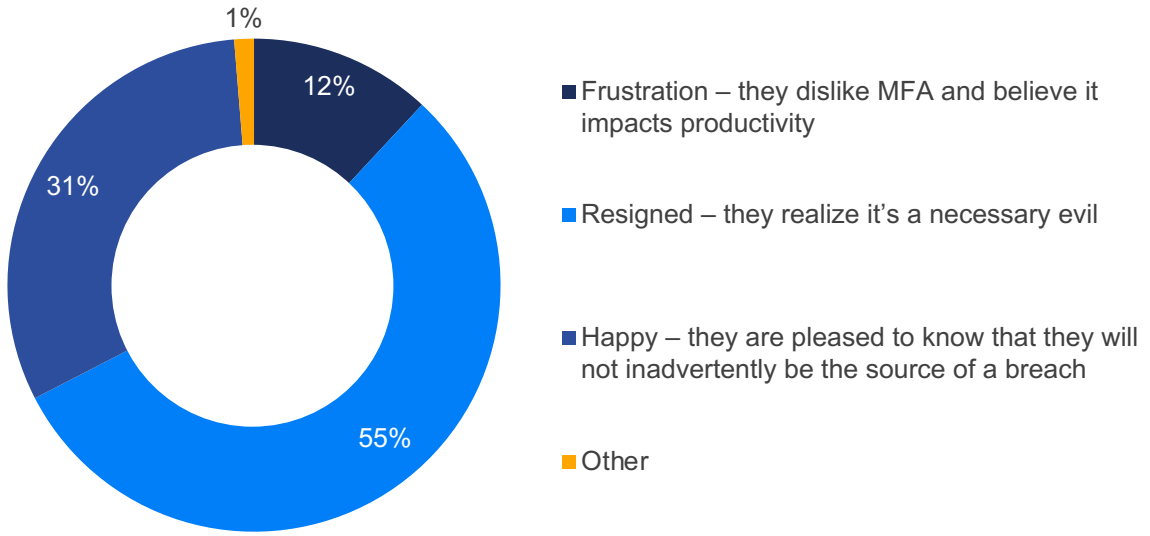
# End user goodwill is not high for MFA

67% are either frustrated or resigned with regards to MFA

The friction that MFA adds to the authentication event continues to irk and frustrate end users. Only 31% of our IT respondents felt that their end users would consider themselves happy with their MFA attitudes.

It is clear there is much room for improvement in delighting end users and IT groups that sponsor the roll out of these technologies to their organizations.

**To the best of your knowledge, which of the following best describes the attitude of a typical employee at your organization towards MFA?**







iC CONSULT | SECRET DOUBLE OCTOPUS

# Addressing Passwordless Confusion in the Market

# Clearing up the confusion

We have found that use of passwordless authentication solutions scores very high for surveys measuring the use of this technology internally, for employees/workers. We wanted to dig into these prior results (from both our own and other vendor surveys) and understand what IT employees actually consider to be ”passwordless”.

At SDO, we make a distinction between technologies that offer a “passwordless experience” versus those that are Full Passwordless. Those solutions that offer a passwordless experience typically do not meet the requirement of an end user never having to type in a password. While most of the time the end user does not need to enter a password, the password still exists and must be remembered at some point in the interaction with the application or resource.

On the other hand, Full Passwordless eliminates the need for an end user to ever need to remember a password. Whilst our competitors would say because SDO rotates a password we are not true passwordless, we do achieve this Holy Grail of passwordless of an end user never needing to set or remember a password. In fact, our Automated Password Rotation approach uniquely enables us to achieve this for the broadest number of use cases encountered in a complex enterprise.



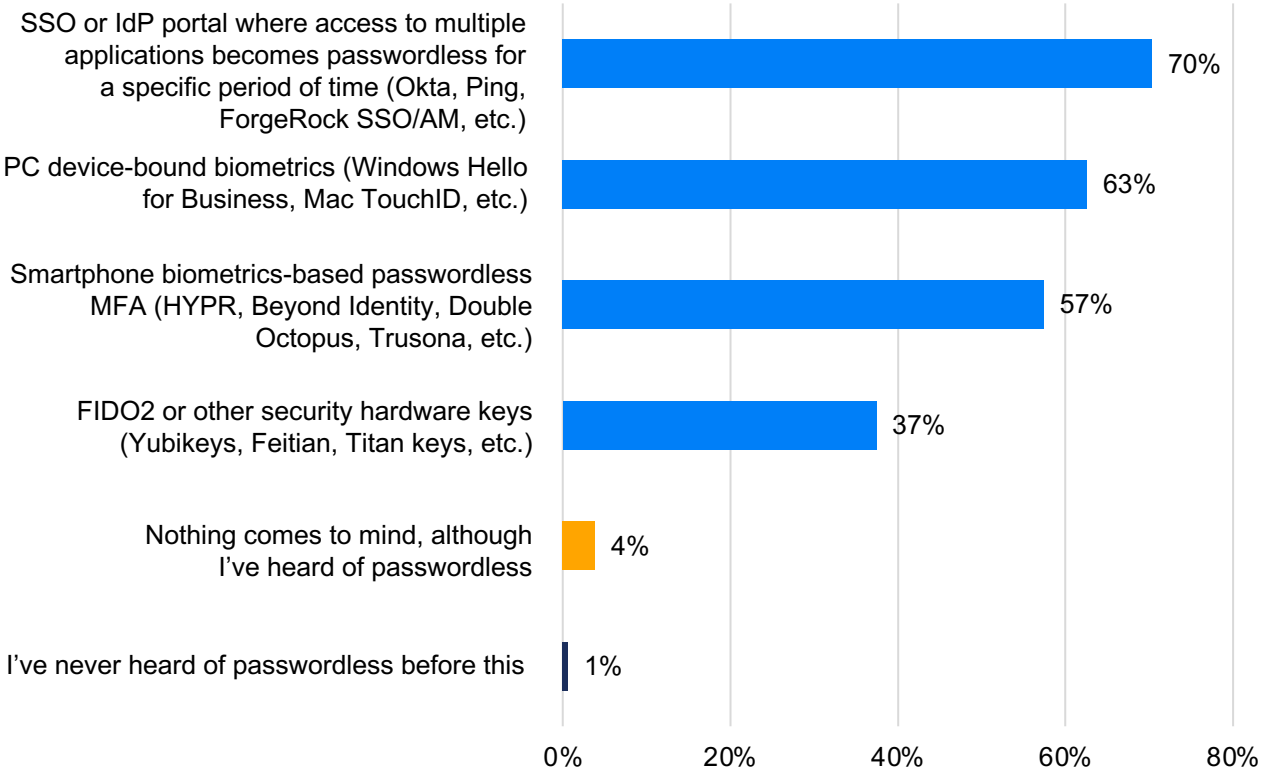

IC CONSULT | SECRET DOUBLE OCTOPUS

# What does passwordless really mean?

IT security and IAM specialists think of several things as ”passwordless” strategies:

- SSO portals that remove the need to authenticate separately to diff apps
- Windows Hello for Business and Mac TouchID which are endpoint device-bound
- Solutions like SDO and others that are modern mobile MFA, FIDO2 certified solutions
- FIDO2 keys such as Yubico and Feitian keys

**When you think of workforce “passwordless” solutions, which of the following technologies come to mind?** Choose all that apply.







iC CONSULT | SECRET DOUBLE OCTOPUS

# Defining “Next-Generation Passwordless”

For this survey, “next generation passwordless” refers to recent innovations in workforce passwordless solutions including:

- FIDO2 or other security hardware keys (Yubikeys, Feitan, Titan keys, etc.)
- Smartphone biometrics-based passwordless MFA (HYPR, Beyond Identity, Double Octopus, Trusona, etc.)

In this survey, “next generation passwordless” does NOT include traditional passwordless technologies such as PC device-bound biometrics (Windows Hello for Business, Mac TouchID, etc.) and SSO or IdP portals where access to multiple applications becomes passwordless for a specific period of time (Okta, Ping, ForgeRock SSO/AM, etc.).



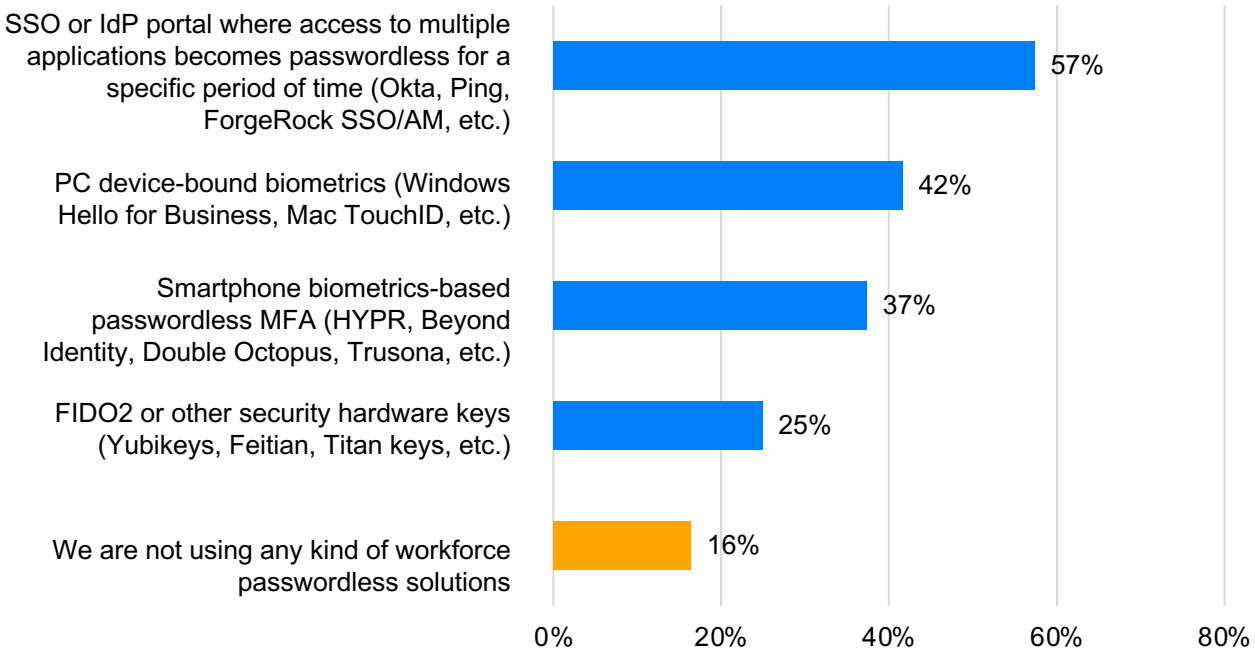

iC CONSULT | SECRET DOUBLE OCTOPUS

# The Current State of Next Generation Passwordless Solutions

By making the distinction of modern, next gen passwordless solutions from prior solutions that are more “passwordless experience” or passwordless such as such as WHfB and SSO portals, we are able to get a clearer view of where market adoption may stand.

A surprising 37% of respondents said they are currently using a next-gen passwordless solution based on our definition.

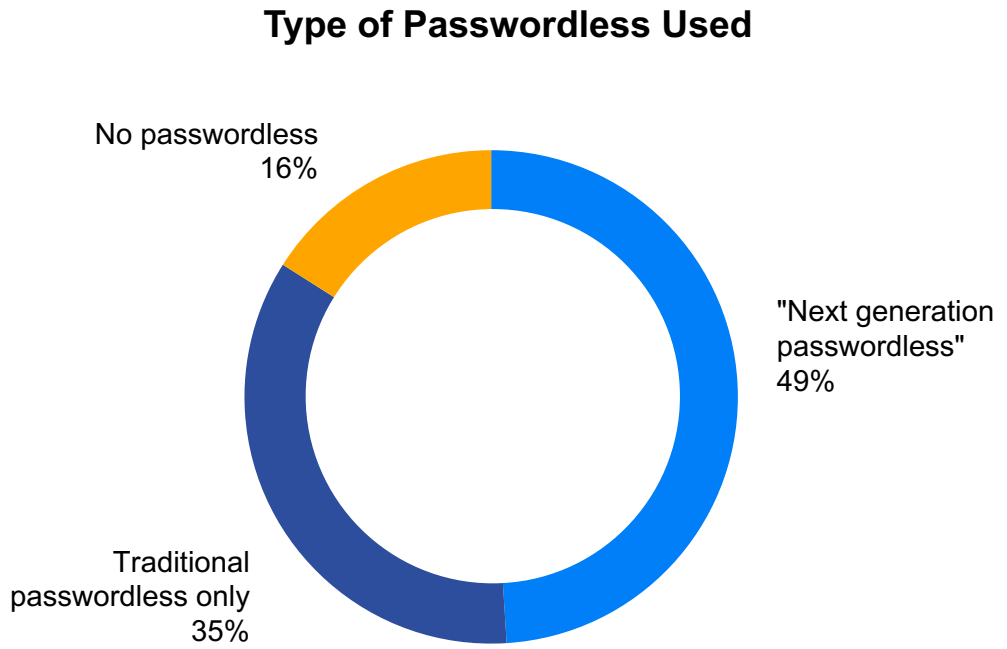
**What types of workforce “passwordless” solutions does your organization currently use?** Choose all that apply.



# Another Take on NG Passwordless Adoption

After explicitly defining “next generation passwordless” to mean FIDO2 keys or smartphone-based biometric solutions for the enterprise, nearly half of IT employees surveyed said they have adopted a NG passwordless solution.

While slightly divergent with the prior slide, it remains in the ballpark for market adoption of software and FIDO2 key solutions that can be considered newer than SSO portals and endpoint device-bound biometrics.



# Next Gen Passwordless is the Future of MFA

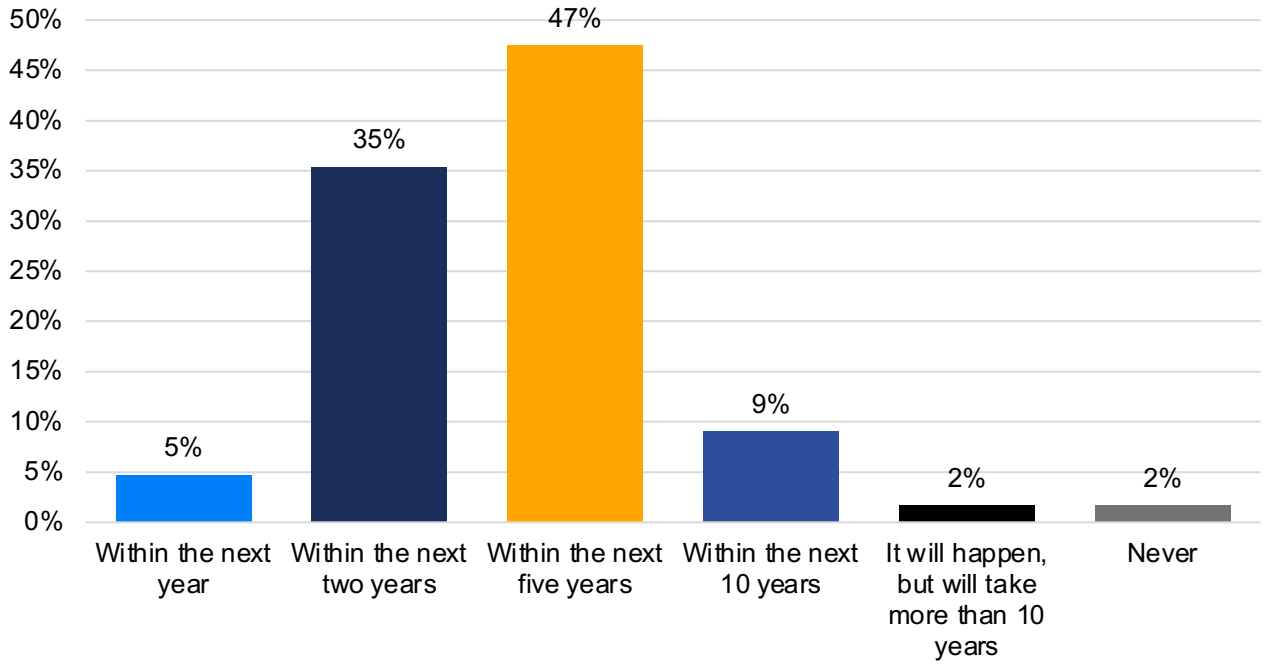
87% see the transition happening within the next 5 years.

Only 2% do not believe FIDO2 keys and smartphone-based biometric passwordless solutions will not become the leading approach for workforce authentication in the next 10 years.

In fact, nearly 90% feel it will happen in the next 5 years and 40% within the next 2 years.

Why is this?

**In your opinion, when will "next generation passwordless" become the leading approach to securing workforce accounts or identities?**



# Perceived Benefits of NG Passwordless Solutions

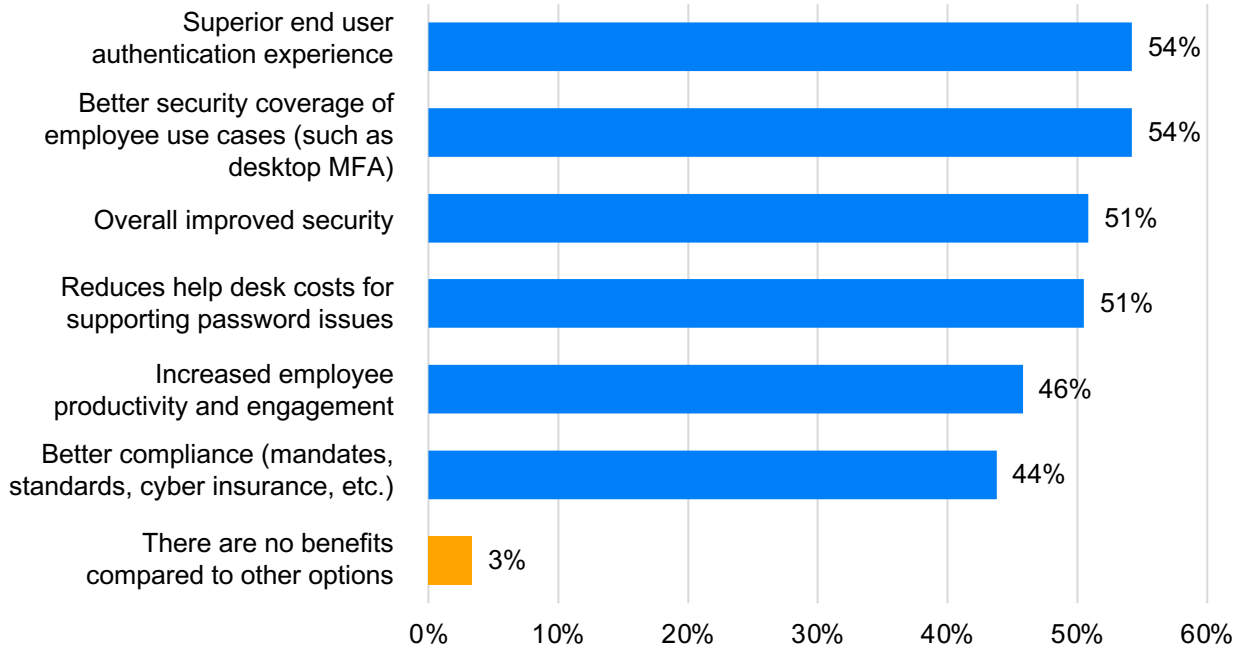
Compliance as a benefit is emerging with the standard 3 motivations for passwordless.

The top 3 reasons for passwordless are:

- Improved security
- Better UX
- Lowers costs, ex help desk costs, etc

The survey found that better compliance has emerged with nearly as strong a showing as those 3 reasons, along with employee engagement

**In your opinion, what benefits do "next generation passwordless" solutions offer compared to other options (i.e. traditional MFA, PC device-bound biometrics, SSO portals)?** Choose all that apply.

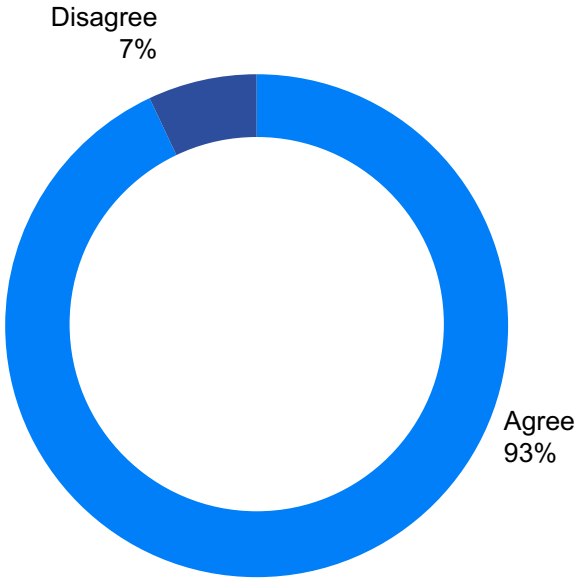


# The view of better security cannot be understated

93% of next gen passwordless solutions deliver stronger security outcomes

Despite anecdotally hearing about market mis-perception that passwordless is actually less secure than traditional MFA, our respondents felt like next generation passwordless solutions would deliver stronger security outcomes.

**Next generation passwordless has the potential to deliver stronger security outcomes.**



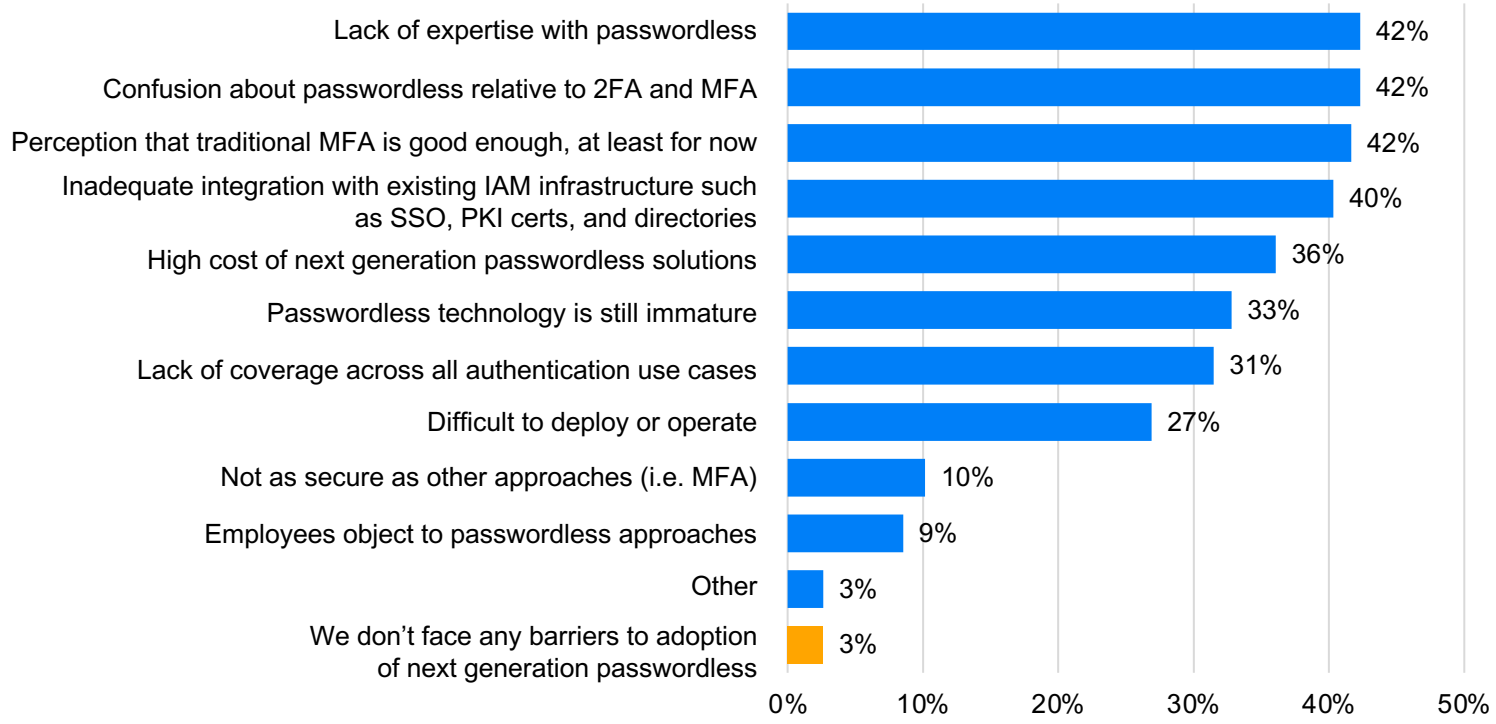
# Top Barriers to Next Gen Passwordless Adoption

## Confusion, MFA being “good enough” and lack of expertise lead the way

There are a plethora of barriers that organizations must battle through to adopt a next gen passwordless solution, not the least of with is the perception that traditional MFA is good enough or that it is not differentiated from basic 2FA.

Cost, immaturity and inadequate integration were also cited.

**What barriers does your organization face that prevent or slow the adoption of “next generation passwordless”?** Choose all that apply.



# MFA Key Takeaways

MFA is widely adopted but not an end user favorite and not universal

- All organizations (100%) have adopted MFA for some type of use
- Only 17% report MFA is used across all workforce passwords
- MFA coverage is more common for cloud (IaaS) and SaaS applications, less for those hosted on-prem
- MFA coverage is wider for privileged or admin passwords, lower for partner passwords
- 67% work with multiple MFA providers and 69% by an MFA solution from their SSO provider (often in addition to other MFA providers)
  - Only 45% are “very” confident that their workforce MFA strategy is effective




iC CONSULT | SECRET DOUBLE OCTOPUS

# Passwordless MFA Key Takeaways

"Next Generation Passwordless" will be the winner in the near future

- 84% have adopted some kind of passwordless technology
- Only 49% have any kind of "next generation passwordless"
- 93% report "next generation passwordless" has potential to deliver strong security outcomes
- 97% report they face barriers to adoption of "next generation passwordless"
  - 87% believe "next generation passwordless" will be the leading workforce security approach within five years




IC CONSULT | SECRET DOUBLE OCTOPUS

## About Secret Double Octopus

Secret Double Octopus is a leader in workforce passwordless and MFA solutions. It's industry-leading Octopus platform offers mid-market to Fortune 100 enterprises the ability to move to a higher security, more frictionless authentication future progressively, from MFA to end-to-end, unified passwordless authentication. From leveraging existing MFA authenticators to supporting legacy on premise applications, no other desktop MFA and enterprise passwordless platform offers as much robustness and flexibility as the Octopus solution. The company has been designated a Gartner "Cool Vendor" and more recently named "Best-in-Class" passwordless solution by AITE Group in 2021.

Learn more at doubleoctopus.com.

Contact Us

Get a Demo

## About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

Contact Us

More Info