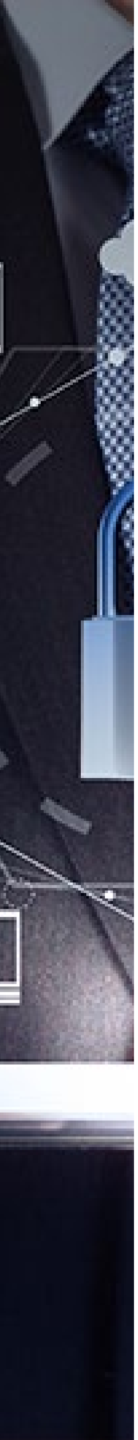
THE STATE OF MULTI-FACTOR AUTHENTICATION

Survey Results eBook

BIO-key®



Contents

Are you looking to:

✓ Reduce the likelihood of being breached and mitigate the consequences that result from breaches

✓ Learn more about the level of security each authentication method has to offer and which is right for your organization

✓ Deploy strong and flexible authentication methods to support both your customers and employees

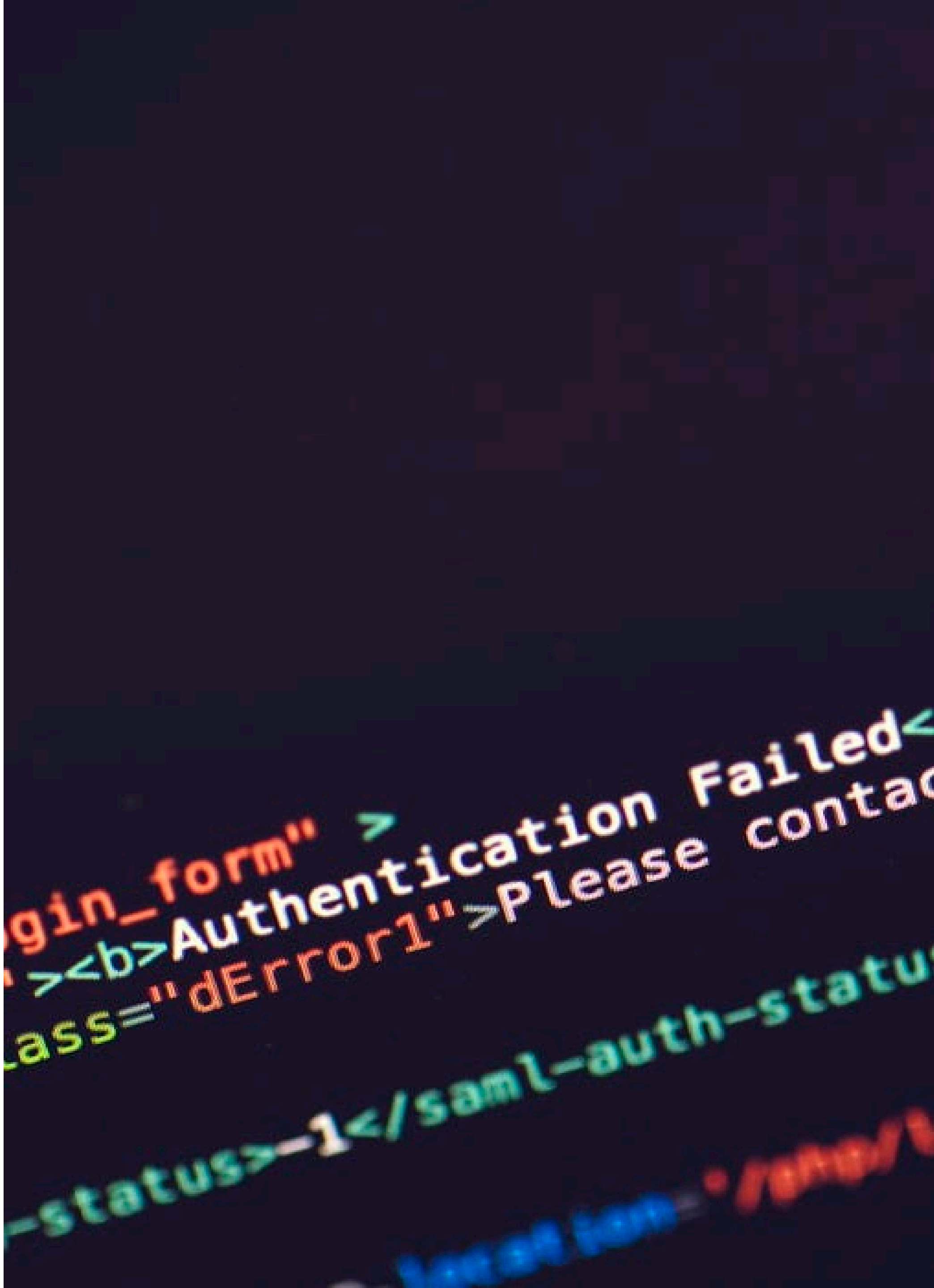
⏱ Estimated reading time: 10 minutes

Summary

Increasing use of cloud-based applications, among other factors, has created an environment in which account takeovers and similar types of incursions are becoming much more common. For example, account takeover fraud increased by about 250% from just 2019 to 2020.[1]

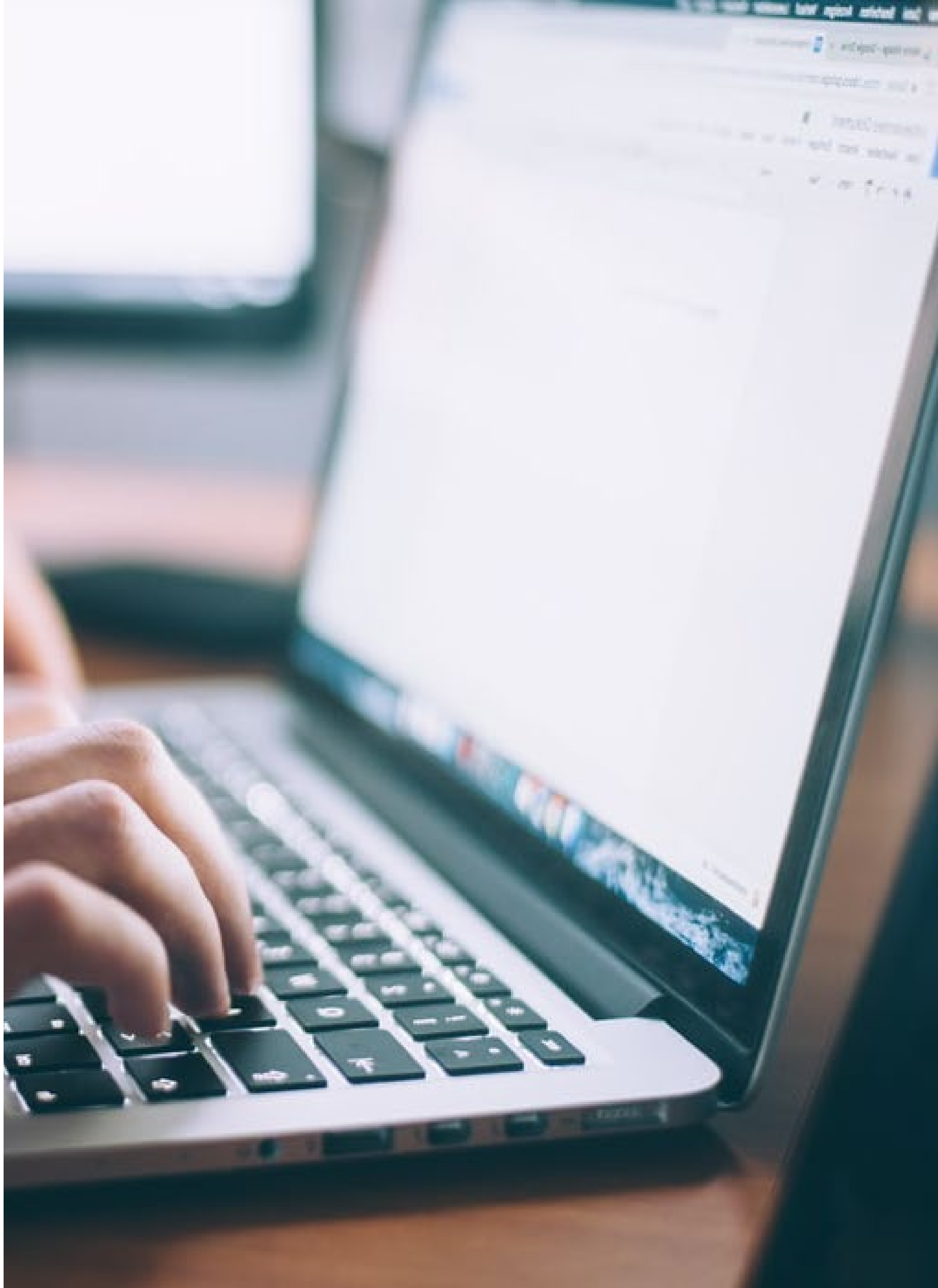
When an account is taken over, it increases the likelihood that bad actors will be successful when sending business email compromise attacks and other phishing emails, or that organizations will fall prey to ransomware, hacking, data loss and a host of other attacks.

[1] https://www.marketwatch.com/story/americans-face-mounting-risk-of-hackers-taking-over-brokerage-accounts-regulators-say-11622826205



Key to addressing the problem is the use of **multi-factor authentication (MFA). MFA** – or more accurately, the lack of it – is becoming an increasingly critical issue that threatens organizations' networks, applications, data, financial security, and reputation. Although MFA has been in use for many years, its use is still not the norm for most organizations.

In short, if organizations employ flexible, robust, and properly managed MFA, they will significantly reduce their likelihood of being breached and the variety of consequences that result from those breaches.



KEY SURVEY RESULTS

Osterman Research conducted an in-depth survey on MFA and related issues for BIO-Key International; here are the key findings from the survey:

Today, only an average of 70% of employees and 40% of customers are required to use MFA to access corporate applications and data.

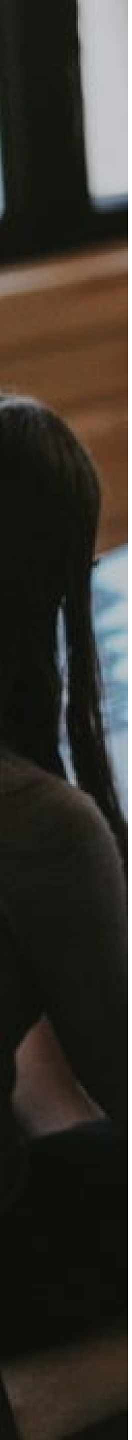
Decision makers perceive hardware tokens, biometrics, and mobile authenticators as the most secure authentication methods.

Only 29% of organizations have implemented passwordless authentication workflows for employees, but another 40% are planning to do so. However, only 9% of organizations have implemented this mode of authentication for customers and only 23% are planning to do so.

The median expenditure per employee for MFA will be $33 in 2021; however, 63% of organizations are planning to increase their investments in MFA over the next five years.

Only one-third of organizations have implemented a Zero Trust Architecture (ZTA), although most others are planning to do so. The leading drivers for implementing a ZTA are preventing data breaches and addressing new attack vectors.

When selecting an Identity and Access Management Solution (IAM), the most important selection criteria are ease of use for end users, the ability to integrate the solution into the existing IT infrastructure, and flexibility to support corporate security policies. Moreover, many respondents cited the lack of MFA and biometrics as key elements missing from their current IAM solutions.



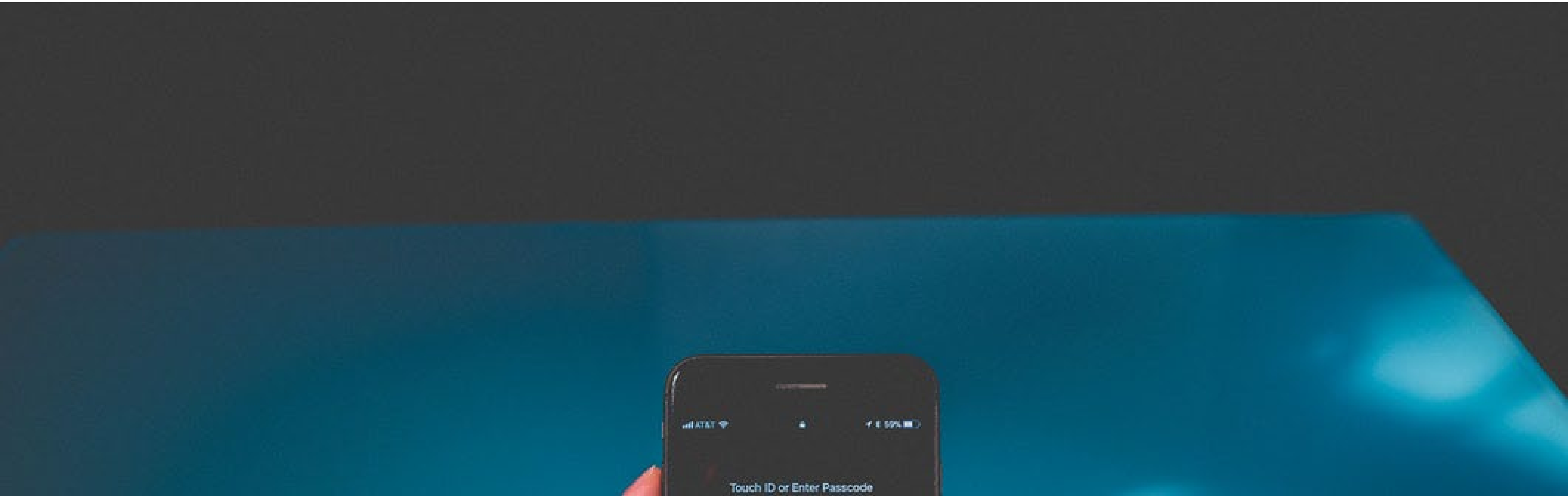
ABOUT THE SURVEY

Osterman Research conducted an in-depth survey of mid-sized and large organizations on behalf of BIO-Key International during May 2021. The goal of the survey was to determine how organizations manage security, authentication, and related issues; and to determine decision makers' attitudes toward various authentication methods including Zero Trust, passwordless approaches, and biometrics.

The online survey was conducted with 169 individuals in organizations that have a median of 1,500 employees. The organizations surveyed represent a wide range of industries. The survey respondents were primarily managers, C-level executives, and directors in IT or IT security teams. Most of the surveys were conducted in North America.

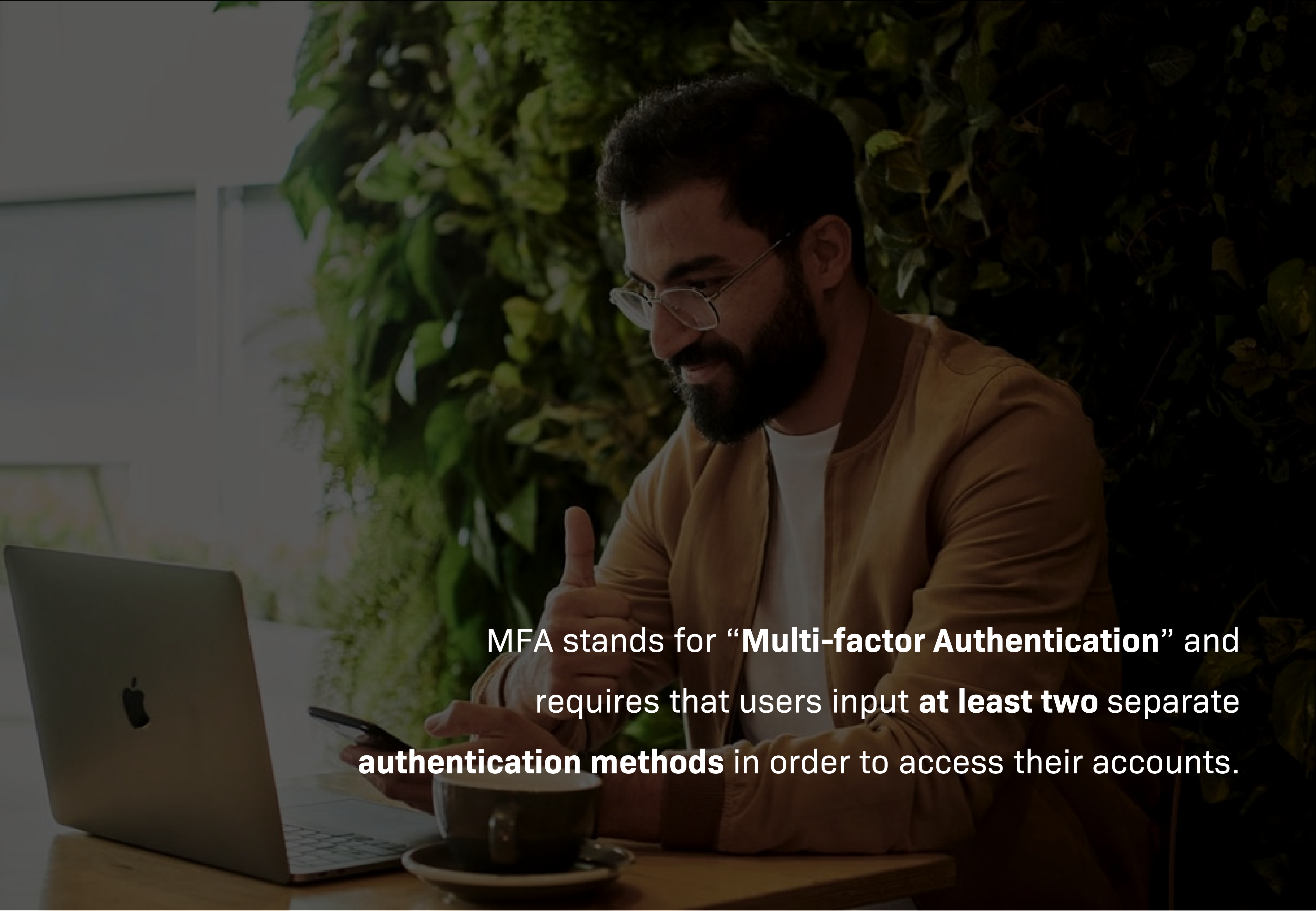
MFA: Broad Usage and Investment

Authentication is the process of informing a system or service about an accessor’s identity. Single-factor authentication, such as using only a username and password to gain access to an email account, is widely used – and highly insecure. Users will often employ their email address as their username making it easy for bad actors to guess; they will choose a simple and easy-to-remember password, again making it easy for bad actors to guess or determine using brute force techniques; and they will use the same password on multiple systems so that they don’t have to remember lots of different passwords.



Re-use of passwords is a particularly serious problem, since if a bad actor can determine the login credentials for one system, they now have access to all the systems for which a user has employed the same credentials.

MFA is a much more secure method of authentication because it requires not just a username/password combination, but something else that proves the accessor's identity. That something else could be something like a palmprint, fingerprint, a hardware token, or a code delivered to the user's mobile phone or via a mobile authenticator.



MFA stands for “**Multi-factor Authentication**” and requires that users input **at least two** separate **authentication methods** in order to access their accounts.

THE IMPORTANCE OF MFA

MFA has been a best practice for many years even though many organizations do not require it for employee or customer access. The survey conducted for this report found that only 70% of employees and only 40% of customers are required to use MFA while accessing corporate applications and data sources.

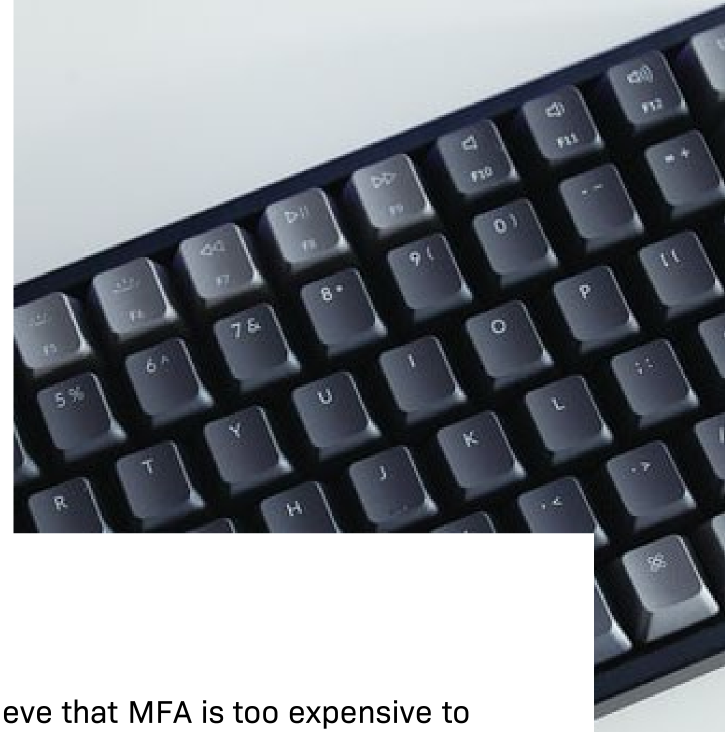
The relatively low use of MFA is a serious problem. It means that access to critical applications and data sources is less secure than it should be. It means that bad actors can more easily gain access to these resources and wreak havoc on organizations via ransomware attacks, the deployment of data-stealing malware, or the theft of financial resources or intellectual property.

If 2020 and 2021 have taught us anything, it's that these types of attacks are on the rise and the non-use of MFA is a major contributing factor.

SOME GOOD NEWS

Despite the relatively low use of MFA, its use is increasing. The survey found that the median expenditure per employee for MFA is $33 in 2021. Moreover, nearly two-thirds of organizations (63%) are planning to increase their investments in MFA over the next five years.

WHY IS MFA NOT MORE POPULAR?



While the use of MFA makes applications and data more secure by increasing the level of difficulty that bad actors face in trying to access them, organizational decision makers have some objections to the use of MFA.
For example:

47% of survey respondents are worried about a lack of user adoption if they opt to implement MFA.

43% are concerned about the impact of MFA on privacy policies and regulations to which the organization is subject.

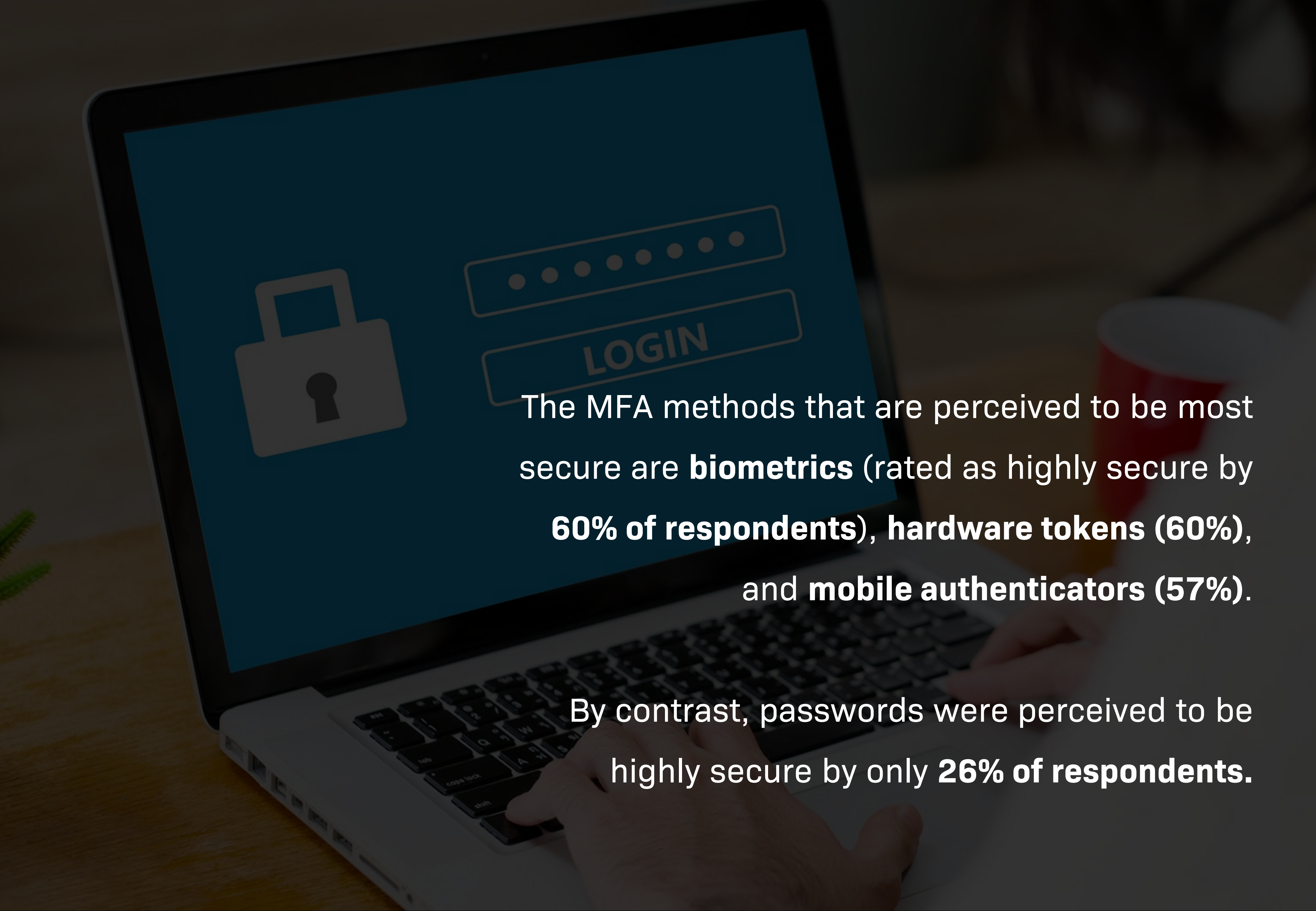
36% believe that MFA is too expensive to implement.

18% just aren’t sure where or how to use MFA.

A Closer Look at Authentication Methods

It's widely understood that single-factor authentication is insecure. But how much more secure are various two-factor authentication methods?

The survey asked respondents to rate the following MFA methods on a scale from "a very low level" to "a very high level" of security: passwords, biometrics, soft/push tokens, hardware tokens, SMS one-time passwords (OTPs), email OTPs, certificates, and mobile authenticators.



The MFA methods that are perceived to be most secure are **biometrics** (rated as highly secure by **60% of respondents**), **hardware tokens (60%)**, and **mobile authenticators (57%)**.

By contrast, passwords were perceived to be highly secure by only **26% of respondents.**

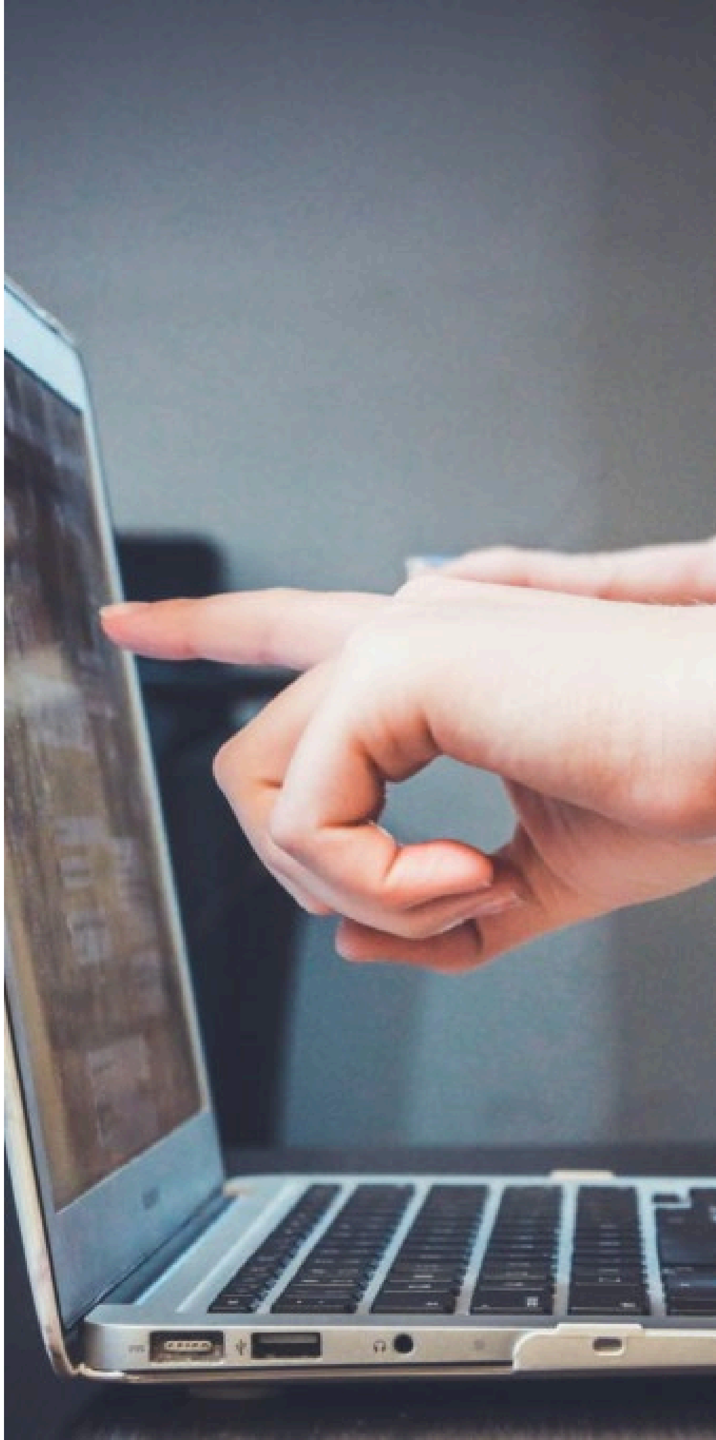
BUT THERE IS A SERIOUS DISCONNECT

We discovered a rather serious disconnect between what IT and security decision makers *perceive* to be highly secure MFA methods and what organizations have actually *implemented* for authentication. For example:

As noted, only 26% of those surveyed believe that passwords are highly secure, but 85% of organizations use them for employee access and 78% do so for access by customers.

On the other hand, biometrics is considered to be highly secure by 60% of respondents but is in use for employees and customers by only 27% and 13% of organizations, respectively.

Similarly, although hardware tokens are perceived to be one of the most secure MFA methods, only 34% of organizations use them for employees and only 12% do so for customers.



There are a variety of reasons that organizations are not deploying more secure methods of authentication. They include perceived barriers to user adoption; difficulties associated with integration across on-premises, cloud, and work-from-home environments; and solutions that are sufficiently flexible to meet user and corporate needs.

CONTEXTUAL/ADAPTIVE AUTHENTICATION WORKFLOWS

We also asked respondents if their organizations have implemented contextual/adaptive authentication workflows or if they planned to do so.

We found that **25% of organizations** have undergone an implementation and **48% are planning** to for their employees; **14% have done** so for customers, while **20% will do so**.

Going Passwordless and Biometrics

Passwordless authentication, as its name implies, does not require a password to authenticate a user – Apple's Face ID and logins using a social media account are examples. Biometrics – a common method for passwordless authentication – includes methods like the use of a fingerprint, palmprint or iris scan.

Currently, only 29% of organizations have implemented passwordless authentication workflows for their employees and only 9% have done so for customers.

However, another 40% of organizations plan implementation of this authentication approach for employees, while 23% plan to do so for customers.

That leaves 31% of organizations with no plans to implement passwordless authentication workflows for employees, and more than twice that number – 69% – for customers.

The large proportion of organizations not planning to implement passwordless authentication is a bit surprising given the push that this mode of authentication has received from market leaders and influencers.

HOW WILL BIOMETRICS BE USED?

Among organizations that are considering the use of biometrics as part of their authentication strategy, there are a variety of approaches that will be adopted:

Nearly **one-half (48%)** will use biometrics only in certain areas, such as specific workgroups or departments.

Only **27% of organizations** plan to use biometrics across the entire organization.

24% plan to use biometric authentication only for critical business applications.

Biometrics will be much more popular for employee access than it will be for access by customers. In fact, **nearly four times** as many organizations (39% vs. 10%) will use biometrics for employees as they will for customers.

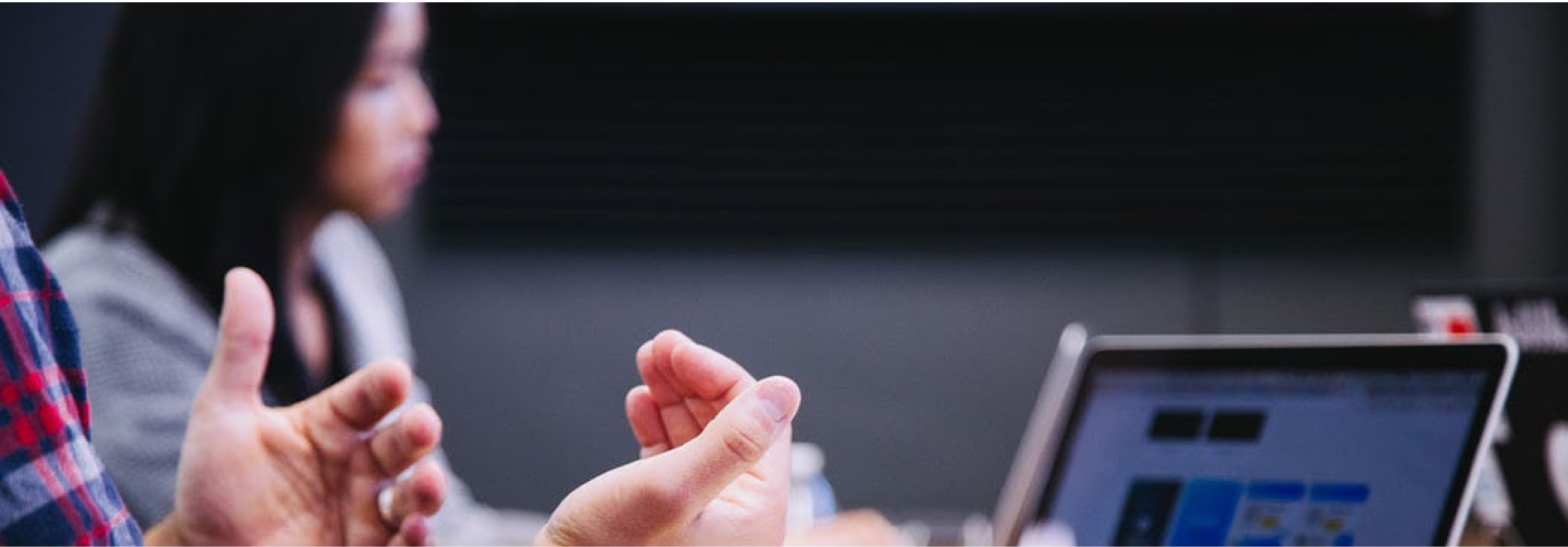
The relatively low planned adoption of biometric authentication is at odds with the fact that it's fast, secure, and convenient. The lack of enthusiasm surrounding its use may be the result of outdated perceptions of early-generation biometric approaches that were relatively poor in comparison to today's.

TOUCH OR TOUCHLESS?

We asked respondents how their employees and customers feel about various modes of delivering biometric authentication:

Respondents believe that **one-third (34%)** of employees and customers prefer touchless biometrics, such as voice-, facial- or palm-based approaches.

However, the majority of respondents indicated that they're either unsure **of employee and customer preferences (28%),** while **27%** indicated that these groups have no preference.



PERCEIVED SECURITY OF BIOMETRIC APPROACHES

We found some level of disparity among respondents in terms of how secure they perceive various biometric approaches to be. For example:

Two-thirds (66%) of respondents believe that iris-based authentication offers a high level of security.

Also, fairly high on the list were fingerprint- and palmprint-based authentication, **considered by 48% and 44%**, respectively, to be highly secure.

Among the biometric authentication approaches perceived to be less secure are device-based biometrics, such as Apple Touch ID and Apple Face ID.

The Growth of Zero-Trust Architecture

What is Zero Trust Architecture?

Zero Trust is what its name implies: no user or resource is automatically trusted based simply on its location or some other parameter. Instead, each user, resource and access request are assumed to be untrustworthy, and so is properly vetted, with the appropriate authentication, authorization and encryption applied before access is granted.

Did you know:

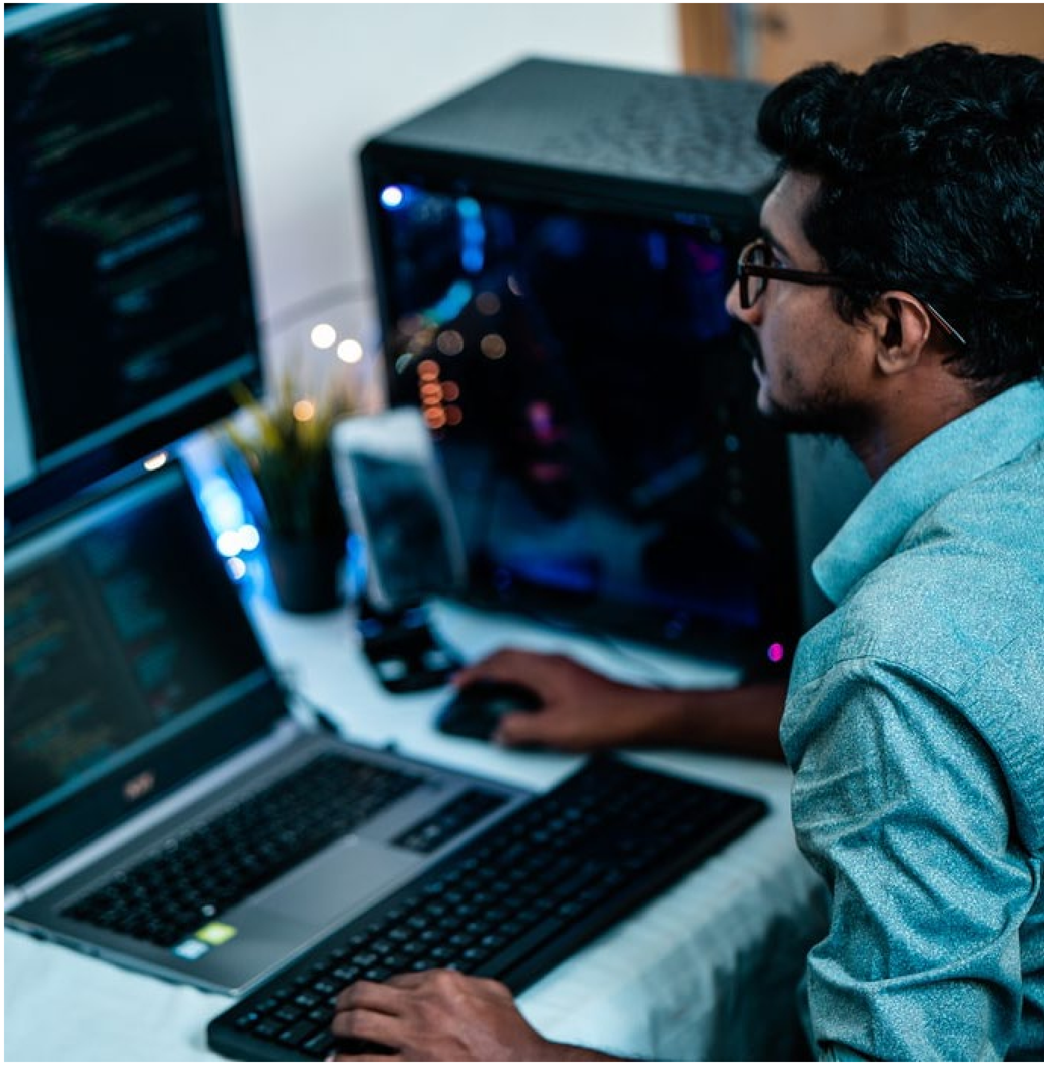
33% of organizations surveyed have implemented a zero-trust architecture

59% plan to do so in the near future

8% have no plans to implement Zero Trust

WHY IS IT IMPORTANT?

As noted by the Center for Internet Security, Zero Trust is important because “it brings us away from the perimeter defense-in-depth models of the past to layers of control closer to what is valued most – the data.”[2]



Zero Trust became even more important in 2020 because of government- and company-imposed lockdowns that required organizations to enable work from home for their employees on a massive scale – and to do so with very little notice.

The sudden shift of employees working behind a “safe” perimeter in an office environment to working in largely unprotected home environments motivated many decision makers to consider Zero Trust in a much more serious way.

[2] https://www.cisecurity.org/blog/where-does-zero-trust-begin-and-why-is-it-important/

THE DRIVERS FOR ZERO TRUST

The leading driver for implementing a zero-trust architecture is to prevent data breaches, cited by 84% of respondents as an important or extremely important reason for doing so.

Sixty-eight percent consider the ability to address new attack vectors and compliance requirements as important or extremely important for implementing Zero Trust.

CHANGES ARISING FROM ZERO TRUST

Organizations will make several changes to their cybersecurity strategies as they adopt and deploy Zero Trust. For example:

69% plan to create and/or update their security policies.

58% plan to implement new technologies and solutions, while an equal number plan to replace various technologies and solutions.

54% plan to implement MFA.

Interestingly, Zero Trust will have comparatively little impact on IT and security labor: only **18% plan** to hire additional headcount and expertise.

This was a surprising finding, since implementing Zero Trust, with the deployment of new technologies and processes, more implementation work, updating security policies, and the like, require more resources, we would have expected labor to increase for a larger proportion of organizations.

WHY WON'T ORGANIZATIONS IMPLEMENT ZERO TRUST?

The leading reason that organizations with no plans to implement Zero Trust won't do so, are focused on two key issues: **54% of these organizations** just don't have the time, budget and/or staff resources to do so; while **41% simply have not made Zero Trust a priority**.

Here again is a conflicting situation. Even while most are planning to implement Zero Trust, most don't plan to increase headcount – yet the reason many won't implement Zero Trust is because they lack the resources to do so.

FINDING THE RIGHT MFA SOLUTION

Identity and access management (IAM) is a set of technologies and processes focused on managing users’ and devices’ roles and access privileges regarding how they access various on-premises and cloud applications and data sources.

MFA is an integral component of any IAM solution: MFA adds in an additional layer of security by enabling access only by authorized users, while other components of an IAM solution, such as single sign-on (SSO) and self-service password reset (SSPR), enable greater convenience and efficiency.

WHAT'S MISSING FROM MANY IAM SOLUTIONS?

Respondents were asked what is missing from their current IAM solutions. **Among the things they cited are:**

- Biometrics
- MFA Methods
- Customer IAM Workflows
- Passwordless Workflows
- SSO options and application integrations
- Governance
- Provisioning
- Cloud-based deployment

Moreover, there are several challenges that organizations have had in implementing their **IAM solutions**. These include user education and adoption, a lack of in-house expertise, and difficulty integrating their IAM solution with the existing IT infrastructure, among other problems.

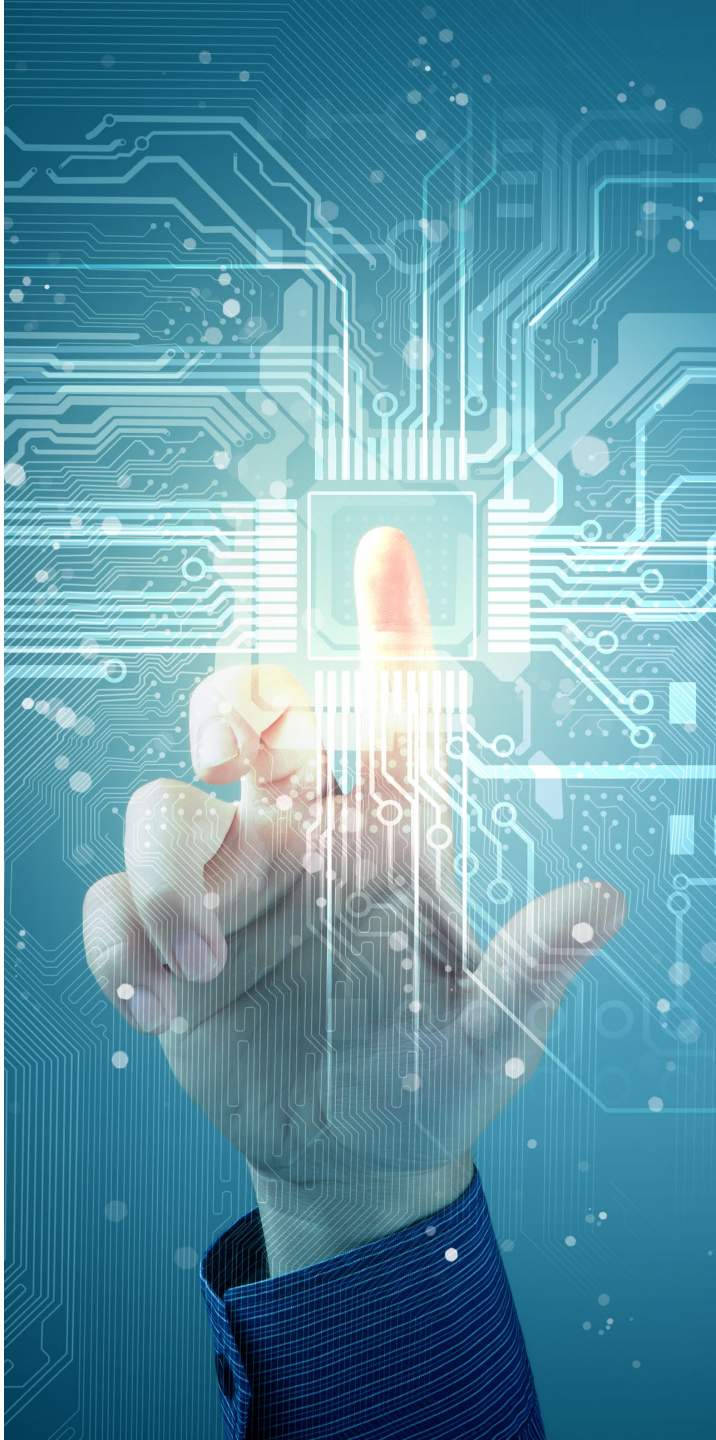
ARE CURRENT IAM SOLUTIONS READY FOR THE FUTURE?

We found that many organizations are not all that satisfied with their current IAM solutions. For example:

Only 35% of respondents agree or strongly agree that their employees and customers like using their current IAM solution.

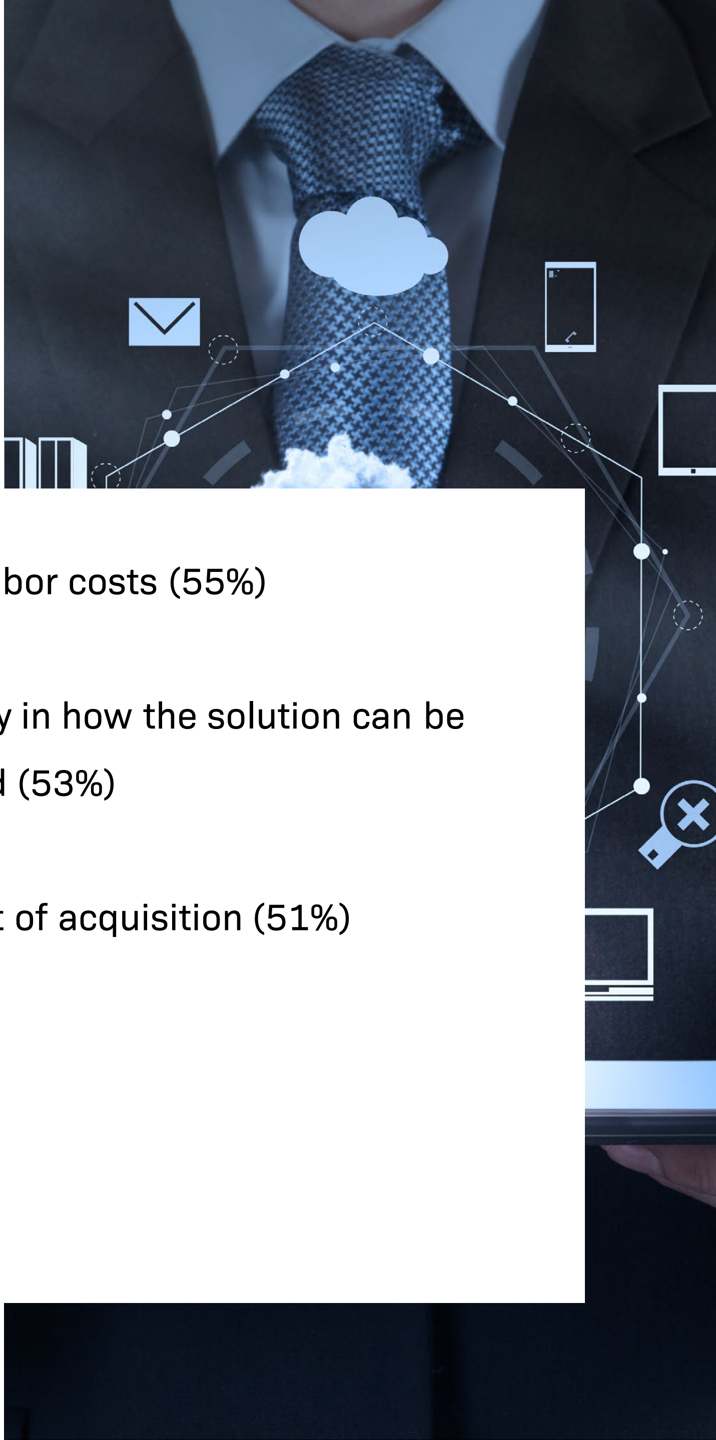
Only 38% agree to this extent that their current IAM solution can support their future security requirements.

Only 44% agree or strongly agree that their current IAM solution can protect their organization from cyberattack.



To address these issues, organizations are looking for various things from an IAM solution:

- Ease of use for end users (cited by 75% of respondents)
- The ability to integrate the solution into the existing IT infrastructure (67%)
- Flexibility to support security policies (60%)
- Ease of administration (59%)
- Low IT labor costs (55%)
- Flexibility in how the solution can be deployed (53%)
- Low cost of acquisition (51%)



Conclusion

MFA is key element of any security architecture because it provides a greater level of protection for corporate application and data resources than traditional authentication methods.

However, it is not as widely used as it should be, although most organizations have plans to expand its use, and most are planning greater MFA investments in the future. As organizations deploy IAM solutions, MFA will be a key element that will enable greater security and efficiency for controlling access to applications and resources.

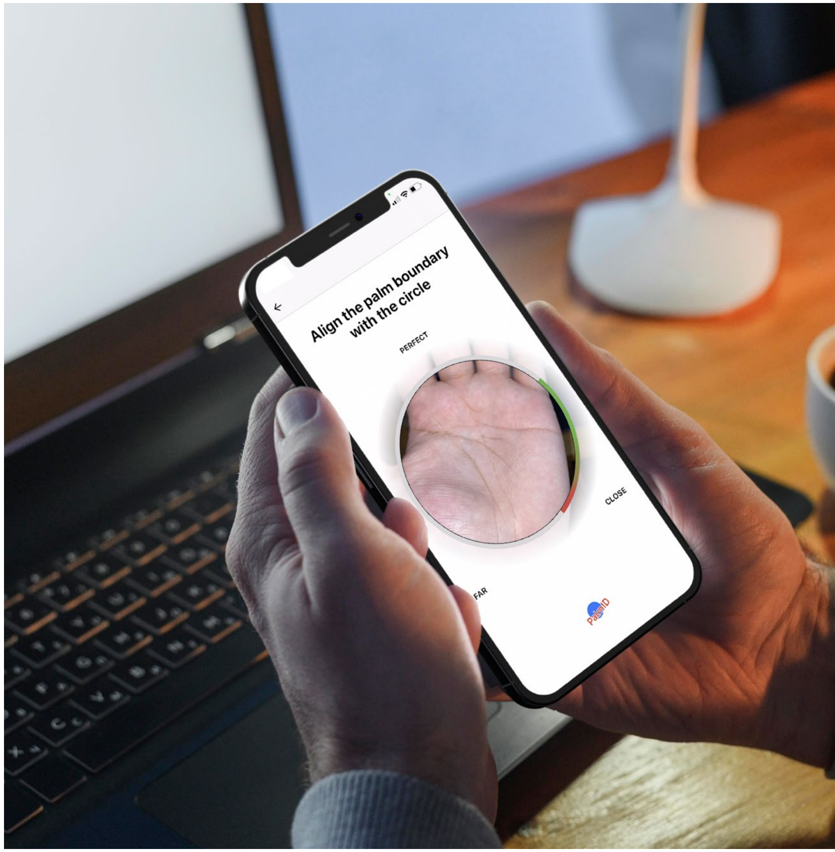
About BIO-key International

BIO-key International is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that enable convenient and secure access to devices, information, applications, and high-value transactions.

BIO-key offers the simplicity and flexibility required to secure the modern digital experience for on-prem and remote users, while easing the burden on IT teams.

BIO-key PortalGuard is a fully unified Identity-as-a-Service (IDaaS) platform with industry-leading biometric identity options, single sign-on, multi-factor authentication, adaptive authentication, and self-service password reset.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery, strong partner relationships, and low TCO.



More information is available at www.BIO-key.com