www.idenprotect.com

idenprotect

Security Simplified.
Productivity Elevated.

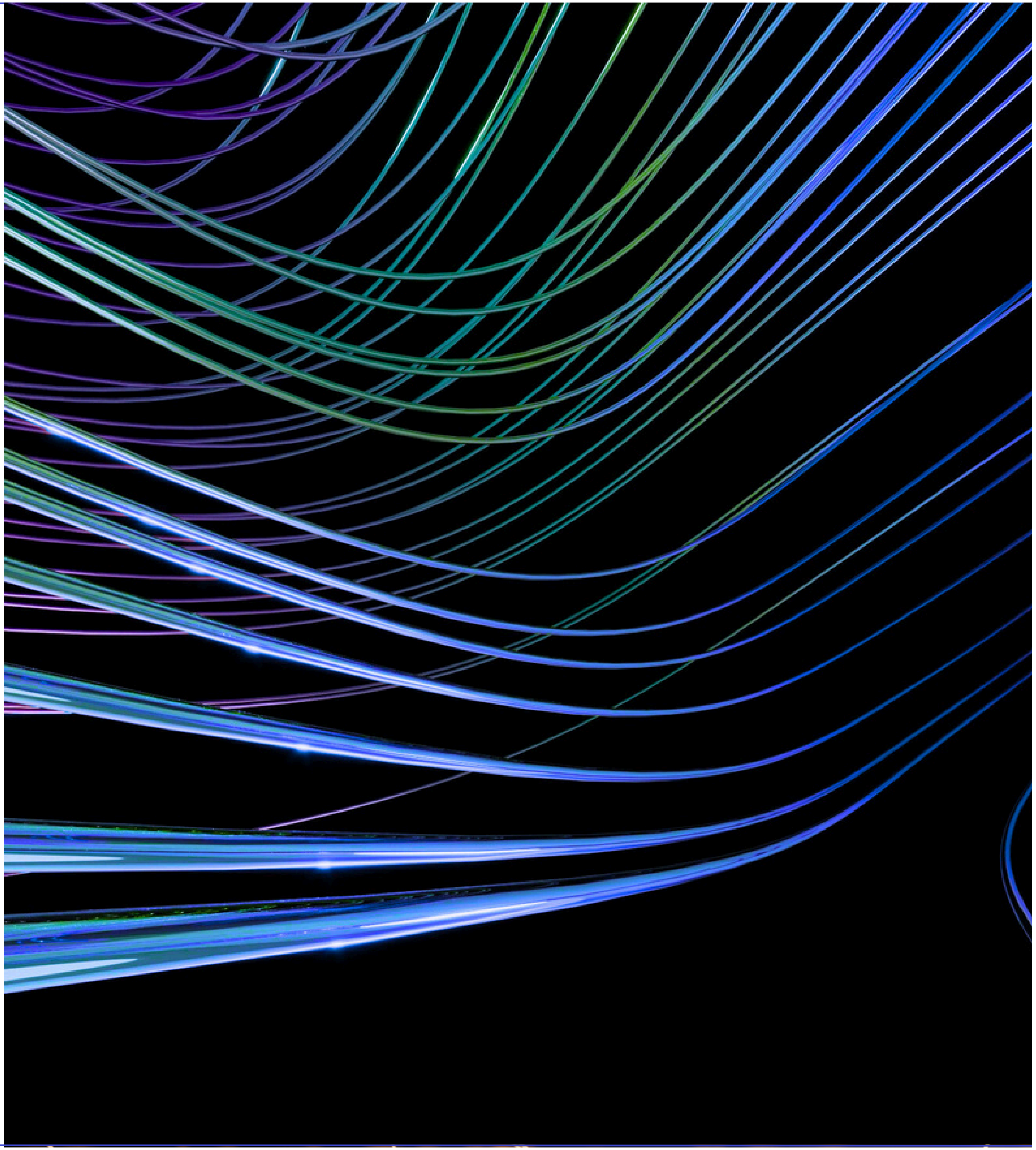
Introduction

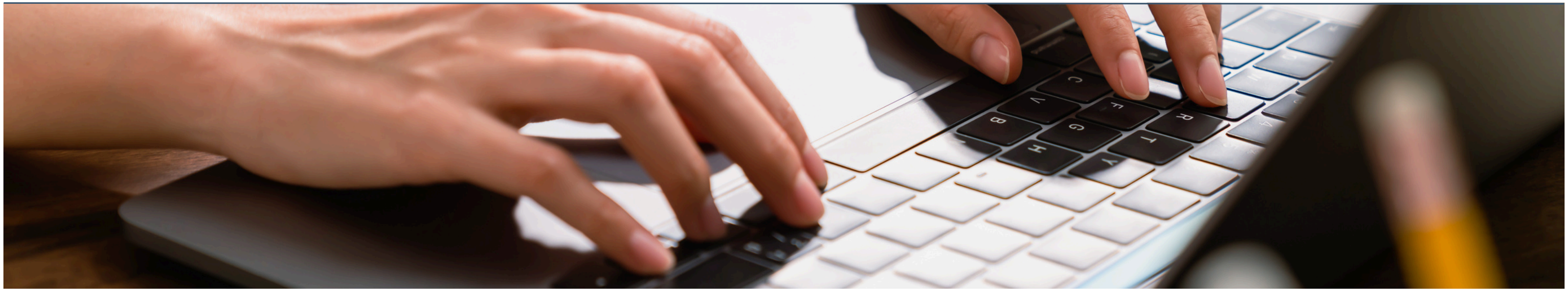
The use of traditional authentication methods that involve humans typing in their usernames and passwords has been a part of daily life since the computer age began.

In the cybersecurity world, it has always been known that the password itself is one of the weak links in securing systems and data. Efforts to improve the security of passwords have led to more complex passwords being implemented that are often impossible to remember.

The introduction of additional tools has created complexity, leaving users confused and frustrated when needing to log into their systems. With increases in user complexity comes increases to support costs.

Technical staff are required to assist frustrated users, either by unlocking or resetting accounts, clocking up hundreds of hours in support time.





The challenge

The greatest challenge is managing the risks posed by passwords. Passwords can be hacked, stolen, or phished – it is a known vulnerability with all shared-secret schemes.

Attackers continue to leverage these shared-secret vulnerabilities to their advantage, and it is clearly evidenced through the significant amount of data breaches that continue to occur, mostly caused by a compromised password.

79%

79% of cyber intrusions in 2024 were malware-free, with attackers increasingly using legitimate remote management and monitoring tools to bypass traditional security measures.

The breakout time for an attacker to move laterally within a compromised network has dropped to a mere 48 minutes in 2024, with some attacks spreading in under one minute.

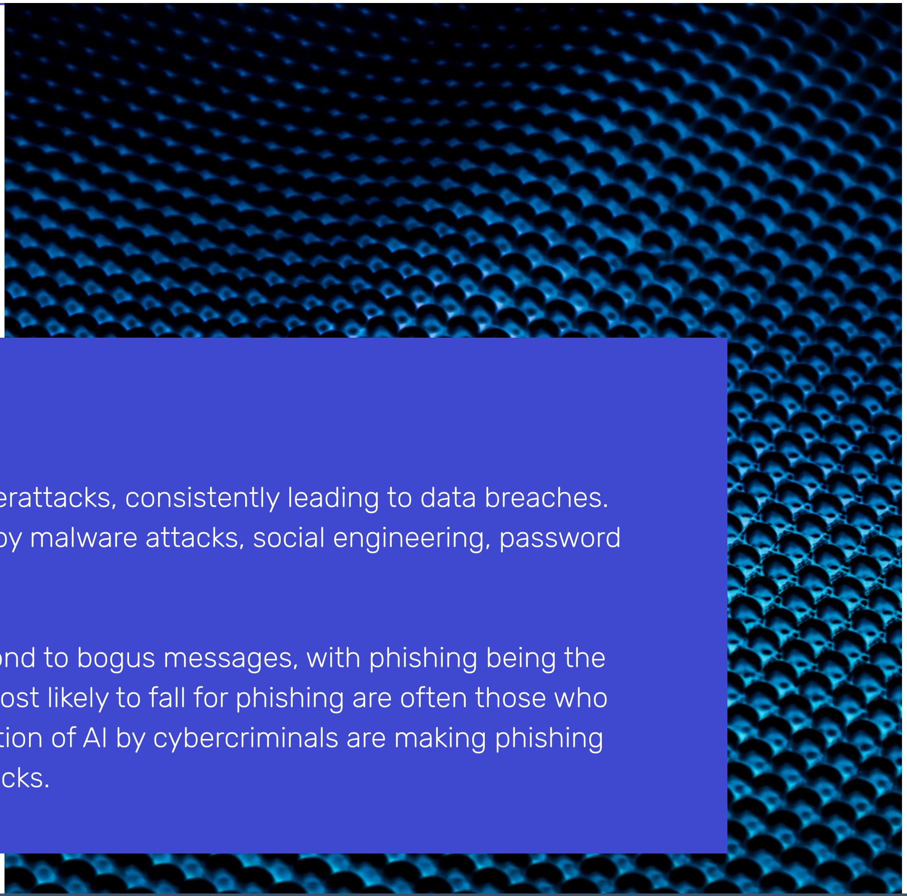
This escalating threat landscape, where identity-based attacks and social engineering are surging, highlights the critical need to move beyond traditional password-based security.

There is no doubt that the case for eliminating passwords from the authentication experience is becoming more and more compelling. How do we ensure that the tools we use provide the adequate controls that all organisations need today in protecting themselves from these types of attacks?

The Information Commissioner's Office (ICO) has warned that a lack of multi-factor authentication (MFA) leading to a preventable data breach could result in substantial financial penalties, urging organisations to deploy MFA across all external connections. With new standards in passwordless technology, greater requirements for a seamless user experience, and the need to reduce complexity and cost, many organisations are now considering the move to passwordless.

This whitepaper explores the compelling case for adopting phishing-resistant and passwordless authentication for corporate environments, outlining a straightforward approach for organisations to make this critical transition.

Why go passwordless anyway?



To appreciate the need for phishing-resistant and passwordless authentication starts with understanding the many challenges that passwords and shared secrets present. The main challenges with passwords can be separated into these distinct elements:

Passwords and shared-secrets are insecure

The continued reliance on passwords and shared-secrets has fostered a multitude of cyberattacks, consistently leading to data breaches. Phishing remains a highly prevalent and successful attack vector, but attackers also employ malware attacks, social engineering, password spraying, and brute force techniques to compromise credentials.

Despite decades of awareness programmes, people continue to fall for phishing and respond to bogus messages, with phishing being the precursor to almost every cyberattack. The Dunning-Kruger effect plays a role, as those most likely to fall for phishing are often those who believe they are immune. Furthermore, the rise of "phishing-as-a-service" and the integration of AI by cybercriminals are making phishing attempts more professional and harder to detect, leading to an increase in successful attacks.

Business email compromise (BEC) is another growing area, where attackers gain access to genuine accounts to send fraudulent requests, often exploiting the trust within an organisation. For instance, a prominent health insurer in Saudi Arabia faced challenges with password complexity and security. Similarly, a Middle East government-backed IT service provider sought to eliminate vulnerabilities posed by traditional authentication methods within their document management system.

To try and reduce the risk of these attacks succeeding, additional layers of security have been implemented, such as 2-Factor (2FA) or Multi-Factor (MFA) authentication. These additional controls, done correctly, can reduce the risk, but it is not as straightforward as one might think. There is now a growing trend in 2FA and MFA attacks that exploit vulnerabilities within those solutions. Software-only authenticators do not provide adequate security protection, and this has been exposed in the past where secret information has been obtained from the authenticator itself. The majority of 2FA and MFA solutions use factors that can be phished, such as SMS codes and One-Time Passwords (OTPs). MFA bypass and MFA fatigue attacks are on the rise to try and confuse computer users in order to gain access. Man-in-the-Middle attacks are now exploiting shared-based vulnerabilities that are present in many "passwordless" MFA solutions – MFA solutions that seem to be passwordless but under the hood are exchanging a password that is still vulnerable to the mentioned attacks.

High costs

The costs associated with using and managing passwords far outweigh any benefits of continuing to use passwords to access systems and data. Password problems are one of the top reasons why corporate users contact their company IT helpdesks. The average employee spends 11 hours per week on password-related tasks, leading to an estimated annual loss of $5.2 million in productivity for businesses. The cost to the company in terms of lost productivity can also be significant, especially when considering all staff over the course of a year.

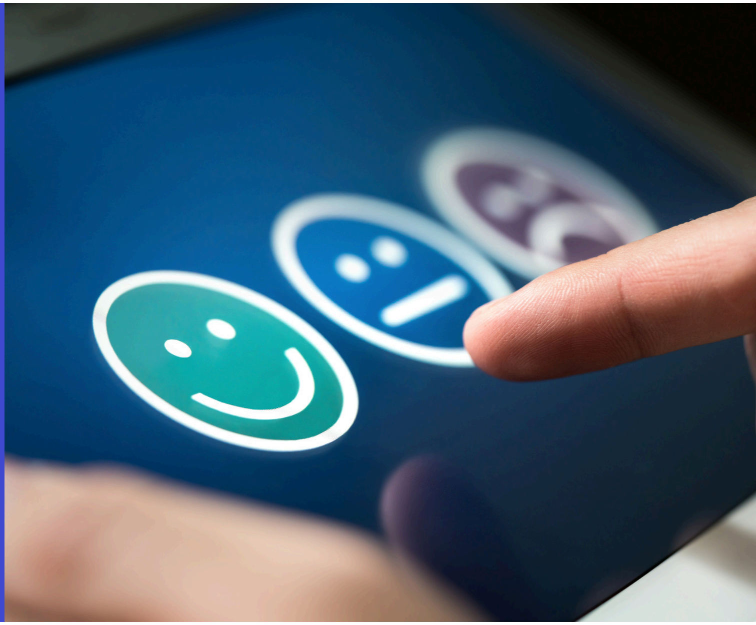
The cost of recovery from a data breach as a result of a password compromise should not be overlooked. The cost of recovery varies based on the severity of the breach, the size of the organisation, and the data exposure. There are five major costs associated with a data breach: investigation and response, remediation and damage control, notification and communication, legal and regulatory costs, and reputation damage. Ultimately, these costs can be substantial and could result in an organisation going out of business completely.

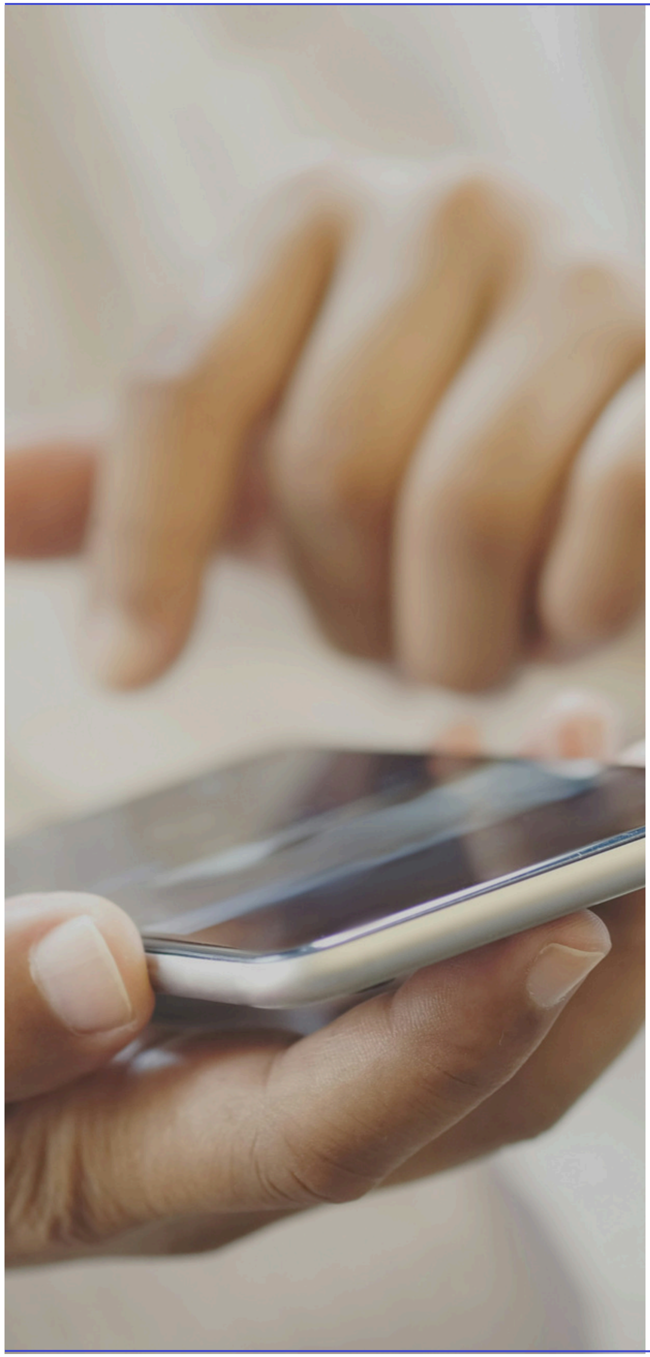
A prominent health insurer in Saudi Arabia, by implementing Idenprotect Passport, realised estimated annual savings of £50,000 from reduced password resets and other administrative tasks.

Poor user experience

Passwords have never been both secure and usable and often lead to a poor user experience. Some of the reasons relate to the difficulty in remembering their passwords. With so many corporate applications, it is common for users to have multiple passwords. This can lead to difficulty in remembering them, resulting in users having to reset passwords or go through a recovery process.

Dealing with corporate password complexity requirements and organisations enforcing frequent password changes all usually result in further support from IT whilst leaving the user frustrated. Participating in difficult password recovery processes can lead to many frustrations and disruptions that could simply be avoided. This constant friction not only impacts employee morale but also significantly hinders productivity, as valuable time is lost on password-related issues.





Evaluation of current authentication methods

Traditional authentication factors that are in use today involve something you know like a password, something you have like a token, and something you are like a fingerprint. Each factor has advantages and disadvantages, so by including two or more factors together, it can help reduce the risk of a credential compromise event.

However, MFA is not foolproof and can still be vulnerable to many different attacks, and unfortunately, nearly all of today's MFA systems have a phishable factor. Only 40% of organisations in the UK, and 35% of charities, had two-factor authentication in place to protect networks and applications in a recent government survey. This figure is alarmingly low, especially when considering that four in ten UK businesses experienced a cyberattack in the last 12 months.

Other newer factors can be delivered through behaviours such as something you do, like a gesture or how you interact with the keyboard, and passive behaviour factors such as location and device type. Combining many factors together can help reduce the odds of an attacker obtaining unauthorised access, but by removing the phishable factor, it would almost eliminate the risk of a successful account compromise attack.

What to evaluate

When evaluating what authentication methods and factors would be most suitable for your organisation, there are a number of key attributes that need to be considered.

Security

- Can the authentication solution ensure that only the authorised user gets access to the account?
- Is the enrolment process secure and tamper-resistant?
- Are there any bypass or recovery processes that could be tampered with by an attacker to obtain unauthorised access?
- Does the solution support hardware-based security for optimised protection?

User experience

- Can the authentication method provide a seamless sign-up and authentication journey?
- Does the authentication method support multiple users, devices, and software types?
- Will the user be required to enter multiple inputs from OTP codes, SMSs, or use multiple authentication applications to access their resources?
- How are account resets and unlocks managed if applicable, or if an authenticator needs to be replaced or recovered?

Ability to eliminate risk

- Is the solution phishing-resistant?
- Can the solution defend against malware attacks, cloning, and credential theft?

Common but flawed approaches to "passwordless"

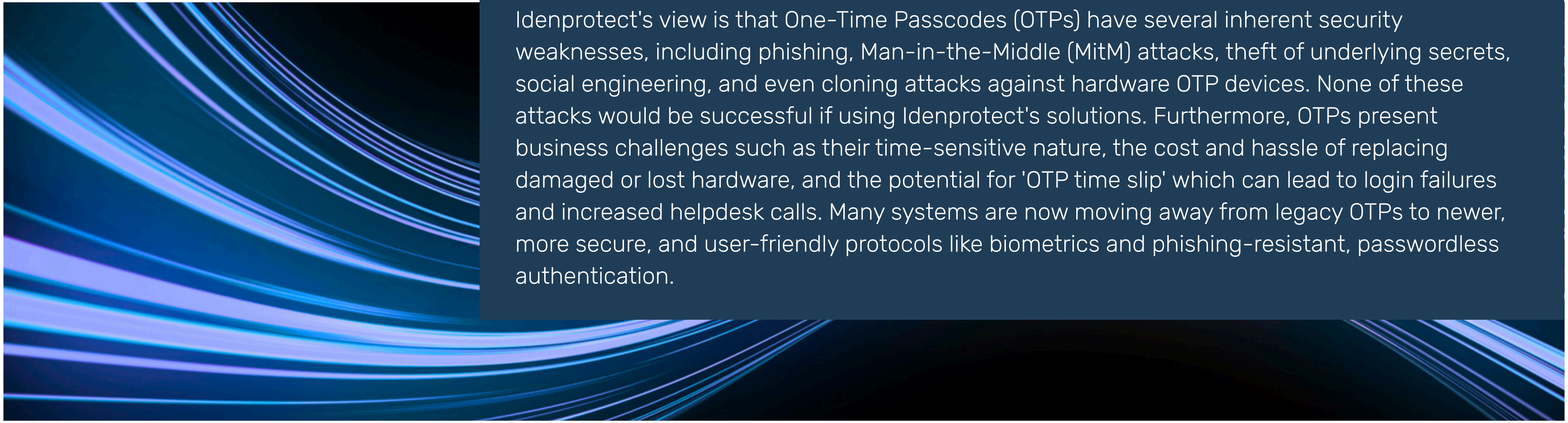
In the current market, many solutions promise better security, better usability, and reductions in cost, but not many can deliver on those promises.

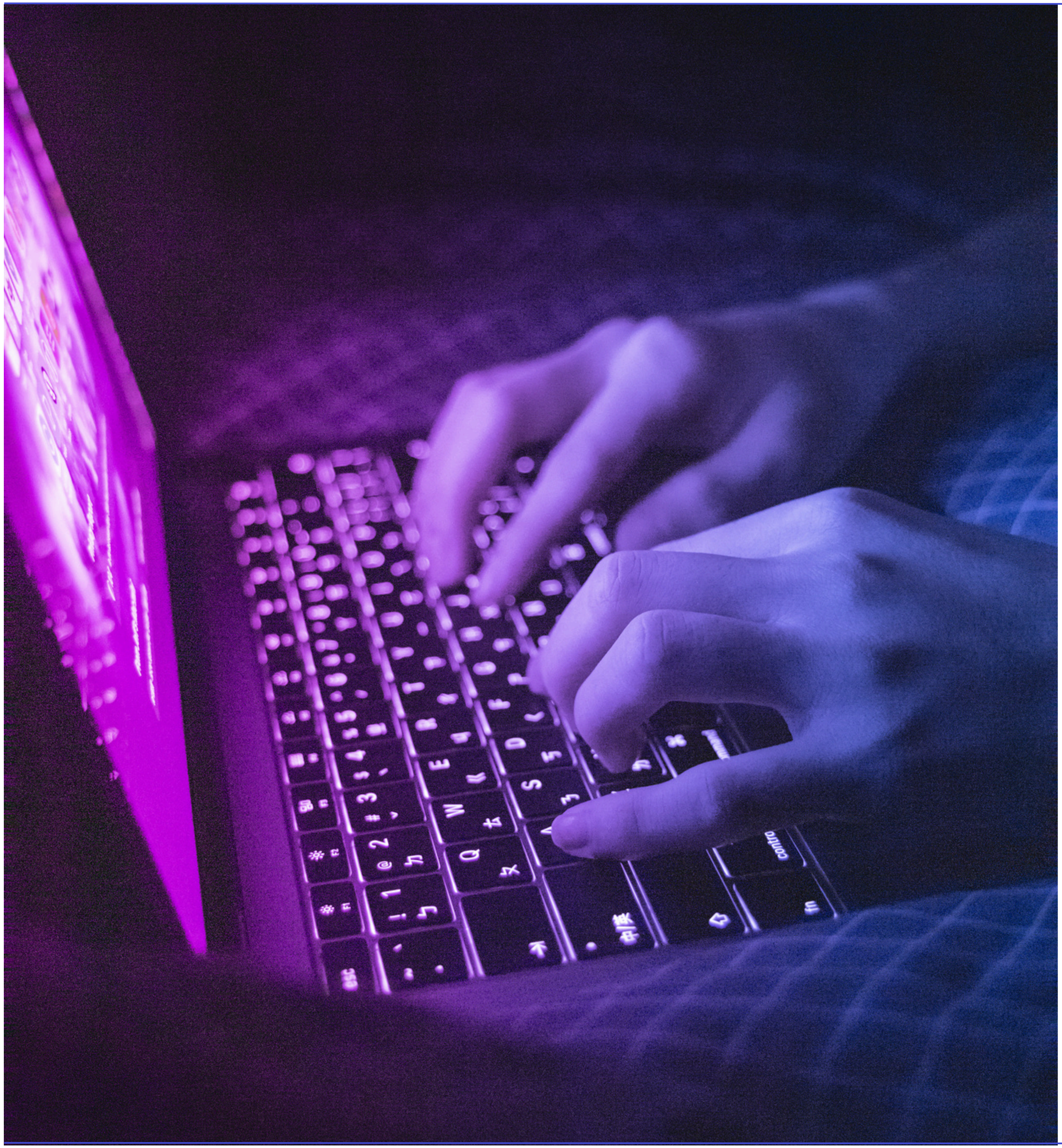
A number of vendors have opted to implement schemes that are just not passwordless in the true sense of completely eradicating the password. Some of these solutions are as follows:

Magic email links | These links have been around for some time and have certainly helped with the user experience. Unfortunately, the security of such a system is wide open to abuse, and while it may appear passwordless to the user, the security weaknesses remain. These links are highly susceptible to phishing, where cybercriminals create fake websites to trick users into divulging sensitive information. They can also be exploited in social engineering attacks, leading users to click on malicious links or download malware. Email security poses further challenges by manipulating fraudulent URLs to look legitimate, attackers intercepting emails, and users inadvertently sharing links with others, allowing unauthorised users access to systems.

Authenticators with OTP and other codes | The use of OTP codes is fundamentally vulnerable to phishing and social engineering attacks. Like passwords, they offer a one-time code that will provide access instead of having to remember a password. Nearly all 2-factor systems use a combination of password and OTP that are both phishable. Some authenticator apps send the OTPs behind the scenes, away from the user's eyes. Although it may defeat the most basic of social engineering attacks, it would not prevent a Man-in-the-Middle phishing attack where the secret can be obtained and used to gain access to the target system.

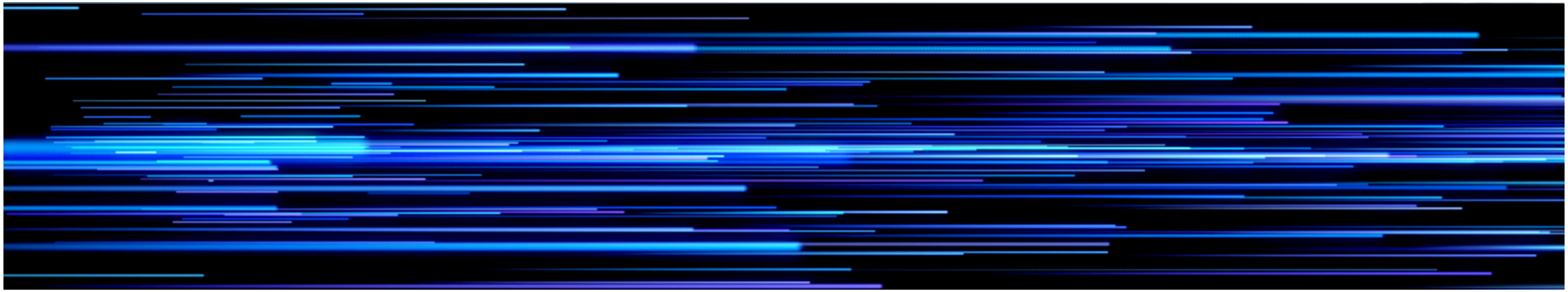
Idenprotect's view is that One-Time Passcodes (OTPs) have several inherent security weaknesses, including phishing, Man-in-the-Middle (MitM) attacks, theft of underlying secrets, social engineering, and even cloning attacks against hardware OTP devices. None of these attacks would be successful if using Idenprotect's solutions. Furthermore, OTPs present business challenges such as their time-sensitive nature, the cost and hassle of replacing damaged or lost hardware, and the potential for 'OTP time slip' which can lead to login failures and increased helpdesk calls. Many systems are now moving away from legacy OTPs to newer, more secure, and user-friendly protocols like biometrics and phishing-resistant, passwordless authentication.





Authenticators that rely on software only

There are a high number of authenticator solutions that solely rely on the software-based operating system for its security. The primary concern with this approach is the reliance on the underlying operating system for security, necessitating constant updates and patches. Another issue is that it is much simpler to copy, back up, or clone software-only solutions that would allow offline attacks against the secure authenticator, potentially resulting in unauthorised access. Many vendors offer additional add-ons and services at a cost to check the health of the device, and although that may address some of the risks, it will not address others. Ultimately, software-based security cannot offer the same robust security controls as hardware-based security.



Move beyond passwords in the enterprise with phishing-resistant passwordless authentication

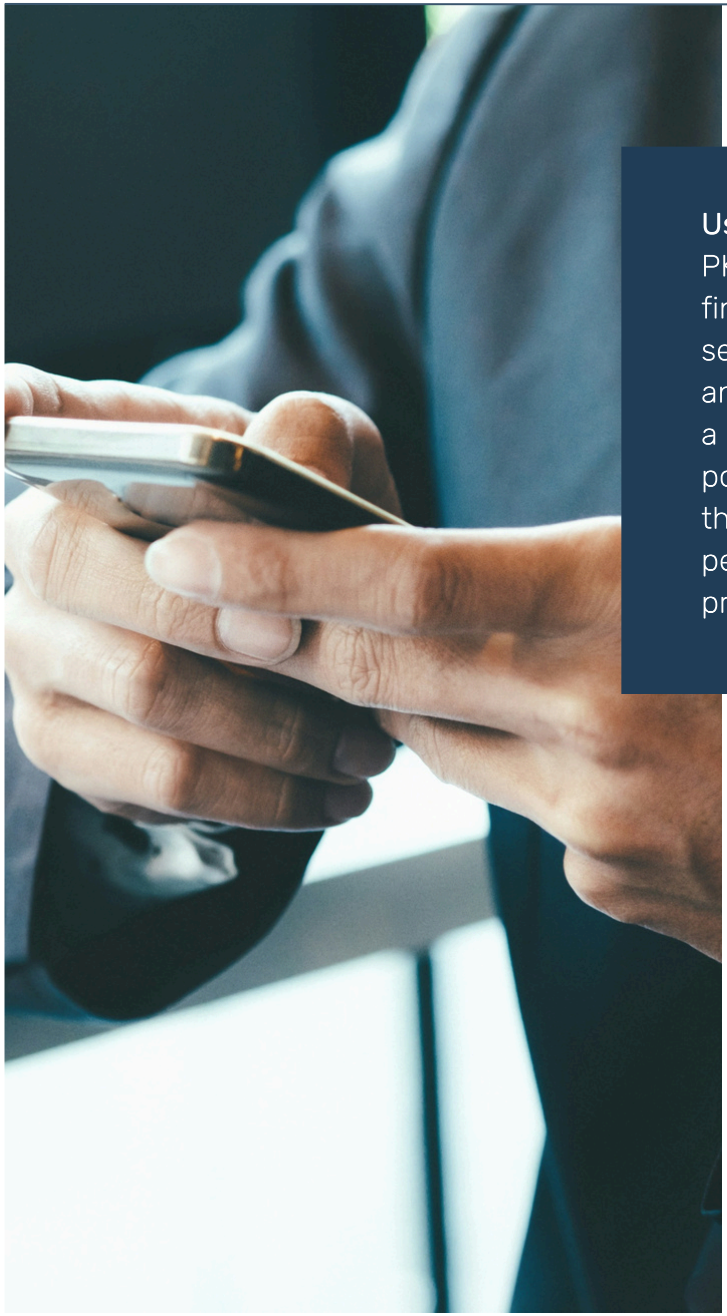
Moving beyond passwords is certainly within reach for all organisations. However, there are certain approaches that will enable success at the first attempt, saving time and money. By understanding the methods of how phishing-resistance and passwordless authentication can be achieved, one should understand the technology concepts and how they would best align with your organisation.

What is phishing-resistant and passwordless authentication?

Phishing-resistant passwordless authentication is a next-generation passwordless authentication solution that decentralises security. In doing so, it eliminates the risk of credentials being obtained and used by unauthorised users to gain access to data. This concept shares similarities with existing MFA solutions, but with one critical differentiator: it removes the human from the central verification process. The human-readable element is the weakest authentication factor in the process. By removing the password, you instantly increase your security posture as there is nothing to phish, and there are no passwords to steal.

Phishing-resistant and passwordless authentication – what are your options?

There are solutions available today that can remove humans from the authentication process. The main two are both based on asymmetric cryptographic keys to authenticate a user's identity, but their deployment, process, and procedures are different. The two you will hear about are Public Key Infrastructure-based (PKI) and Fast Identity Online (FIDO). Both have their strengths and their weaknesses. Importantly, their weaknesses are not based on intrinsic limiting factors but rather on how each works and which deployment scenario it was designed for.



Using PKI as a passwordless authentication method

PKI (Public Key Infrastructure) has been around for many years. In fact, it has underpinned the entire financial services sector for well over three decades. It is now used everywhere, from opening a security door to sending an online payment or using Apple Pay to buy a coffee. Put simply, it is tried and tested. PKI passwordless authentication solutions use cryptographic key pairs (a combination of a public and a user's private key) to authenticate users. It is built on the concept that there is a single point of trust in a hierarchy (the root). If you and others belong in that hierarchy and trust the root, then you will trust each other. PKI is not a technology but part of a collection of elements, including people and process. Within PKI, you are putting trust into the technology, the people, and the process in which the solution is being used.

FIDO — The new kid on the block of passwordless authentication

FIDO is a relatively new method being standardised by the FIDO Alliance. FIDO was built to allow a user to securely access a system without using a password, even when they may not be 100% known by the entity, such as an e-commerce site. Within FIDO, you are putting your trust into the FIDO-approved authenticator rather than a central trust point; this could be something like a YubiKey token or a mobile app. It is important to note that Idenprotect is not FIDO-based.

Choosing the best phishing-resistant passwordless authentication method for enterprise

Organisations seeking phishing-resistant capabilities, which are essential to securing sensitive data, often consider both Public Key Infrastructure (PKI) and FIDO-based solutions. However, the optimal choice fundamentally depends on your deployment strategy and target users. When implementing passwordless authentication in the enterprise, PKI is typically the preferred choice for internal corporate users due to its established trust model and extensive integration capabilities.

PKI operates on a hierarchical trust model, utilising registered authorities and organisations to issue and manage digital certificates. This allows a single certificate or key to authenticate across multiple platforms, making it highly versatile within complex enterprise environments. PKI has a long-standing history as an enterprise solution. In a corporate setting, employees undergo a vetting process, including interviews and HR reviews, providing a strong foundation of trust in their identity. This aligns perfectly with the procedural aspect of PKI, where a known individual with a verifiable background can be issued a credential trusted by others within the organisation. This credential is then owned and managed by the organisation, ensuring compliance with internal policies and regulatory obligations. Furthermore, due to its long-standing presence, PKI is natively supported by many legacy and modern IT systems. This minimises the time required for integration or application rewriting, resulting in faster rollouts to mitigate risk.

In contrast, FIDO (Fast Identity Online) was originally designed with a simpler trust model, primarily for Business-to-Consumer (B2C) applications such as online retail platforms. While major technology companies are now adopting FIDO for enterprise use, this often involves adapting the standard to fit their specific infrastructures, which can dilute its original rigid standards. FIDO keys typically authenticate to a single platform, offering less flexibility for the diverse needs of an enterprise environment compared to PKI's broader application.

Idenprotect's implementation leverages the strengths of PKI, giving it advantages over FIDO solutions. Many organisations already have existing PKI implementations in place, which means they have approved and supported technology without the need to adopt new solutions. Idenprotect can integrate with existing PKI implementations, allowing for adherence to organisational requirements like Hardware Security Modules (HSMs) and can also utilise its built-in Certificate Authority (CA) to be configured as a subordinate or a standalone authority, providing multiple deployment options. This approach means Idenprotect Passport can be used for various enterprise systems, including Windows login, and maintains rigid standards uninfluenced by the evolving approaches of tech giants. This established compatibility means organisations can benefit from faster deployments. For instance, Dubai Airports Group successfully implemented Idenprotect Passport for secure authentication and digital signing, integrating it seamlessly into their existing document workflow.

Starting your enterprise passwordless project

Moving beyond passwords within the enterprise requires some careful planning. Like most projects, understanding what success looks like and building a step-by-step approach is an essential part of a successful project delivery, along with senior stakeholder support and end-user support. Understanding the threats, the technology, user experience, the costs, training and support, as well as the implementation method before selecting a vendor and trying to deliver a project, will save time and money. The attributes to consider are as follows:

What are the threats?

- Phishing attacks
- Credential breaches
- Man-in-the-Middle
- Man-in-the-Browser
- Password spraying
- Brute-force attacks

The user experience

- How enrolment works
- How the authentication process works
- How recovery or replacement processes work

Training and support

- How to train end users?
- How to support users?
- Compliance requirements

Key Performance Indicators (KPIs) for success

- Reduced helpdesk calls for password resets.
- Improved user satisfaction with login processes.
- Decrease in successful phishing attacks.
- Faster onboarding of new users.
- Enhanced compliance audit outcomes.

Costs

- The cost of the solution
- The business case and TCO
- Support and maintenance

Implementation

- Deployment method
- Security and compliance requirements
- Integration with other technology

Technology and security elements

- Technology suitability
- Ability to provide everything needed within one single platform
- Secure hardware-based protection
- Browser support
- Supportability on applications
- Supportability across platforms

Conclusion

This whitepaper has discussed the need for a more secure and user-friendly authentication method to support corporate users today in accessing their resources. Moving beyond passwords and embracing a passwordless approach presents a truly credible way to address security vulnerabilities and user frustrations associated with traditional password-based systems. By leveraging advanced technologies such as biometrics, public-key cryptography, and on-board security chips within modern computing devices, organisations can enhance their security posture while also providing a seamless user experience. Embracing the passwordless approach signifies a proactive step towards safeguarding sensitive information, reducing the risk of data breaches, and ensuring user and senior manager convenience. As we continue to navigate the ever-evolving realm of cybersecurity, it is crucial for organisations to adapt to a passwordless future, as it holds the key to revolutionise the way we authenticate and secure our digital identities.

Idenprotect's phishing-resistant, passwordless authentication offers a tangible path to achieving these benefits, simplifying security while elevating productivity for organisations of all sizes. As demonstrated by successful implementations at a leading Saudi Arabian health insurer and a Middle East government-backed IT service provider, Idenprotect Passport streamlines access, reduces costs, and significantly enhances security.

idenprotect.com | info@idenprotect.com | 020 3900 2704