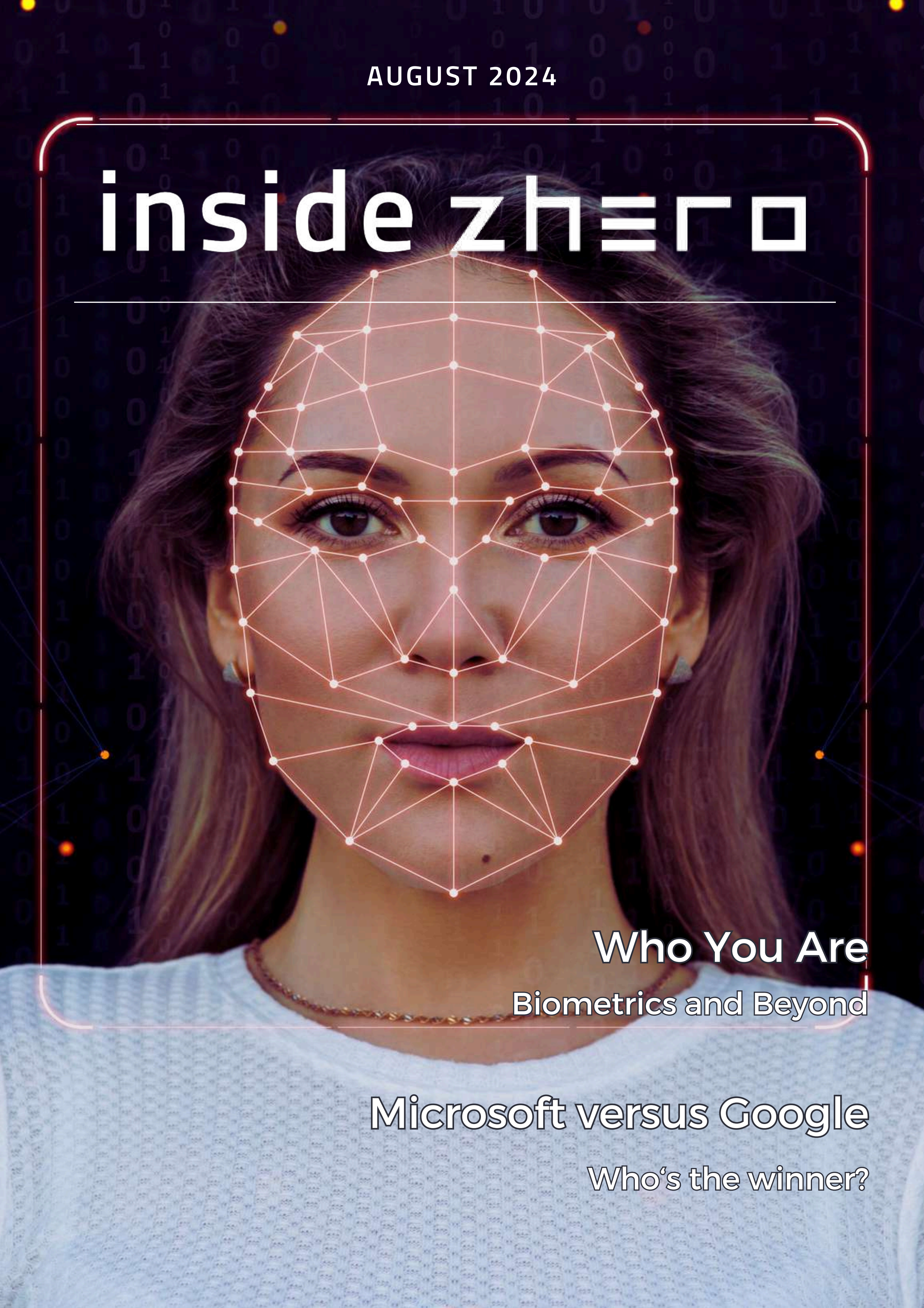


AUGUST 2024

inside zhero

Who You Are

Biometrics and Beyond

Microsoft versus Google

Who‘s the winner?

Message from Izak

Hello again and welcome to a bumper edition of Inside Zhero.

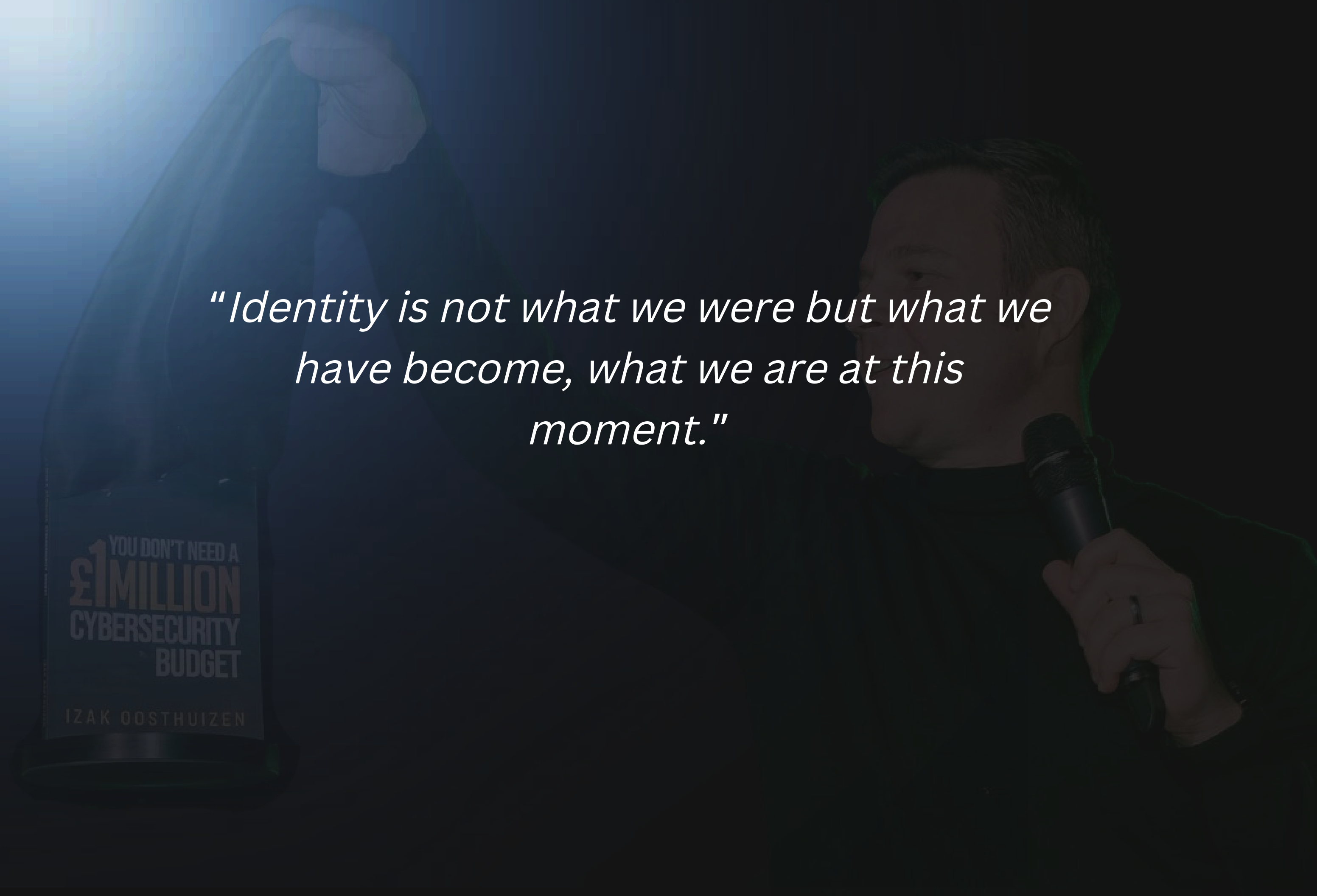
This month we're taking a look at identification - how methods of determining identity have changed over time and what the future holds.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Who Are You" focuses on identification - from the days of the Babylonians to modern biometrics.

2 million Brits were victims of identity theft in 2023.



"Identity is not what we were but what we have become, what we are at this moment."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Book a free 30-minute consulation

WHO YOU **ARE**

The concept of identification dates back to the Babylonian Empire, where censuses recorded population and resources. Over time, data collection evolved, and by the Roman Empire, personalised documents like birth certificates and citizenship records were introduced. The first example of a 'modern ID' appeared in 1414 when King Henry V of England issued the first passport, known as 'safe conduct' papers, to prove identity abroad. This was simply a signed piece of paper. A key development came in 1829 with the reforms of Robert Peel in the UK, which emphasised printed police records. This allowed personal data to be linked to individuals through unique numerical identifiers, laying the foundation for today's ID systems.

Fingerprint ID

Fingerprints have a long history as a form of identification. Ancient Babylonians used them to seal business transactions on clay tablets, and there are even stories of ancient Roman officials solving a murder case by matching a suspect to a bloody fingerprint. In China's Tang Dynasty, fingerprints were used for identification, and around the same period in Japan, thumbprints served as legal signatures. The first official and modern use of fingerprints for identification was in 1859 when a British Colonial magistrate employed them to identify individuals by their prints.

Acceptable ID

What was considered an 'acceptable ID' has varied a lot depending on the era in which an ID document was issued. Since the Roman Empire, birth certificates and land title deeds have consistently been recognised as valid forms of identification for different reasons. Similarly, with the issuance of the first passports in the 1400s, these documents also became accepted as forms of ID. While modern passports are vastly different from the simple slips of paper used in the past, their fundamental purpose has remained unchanged for over 600 years.

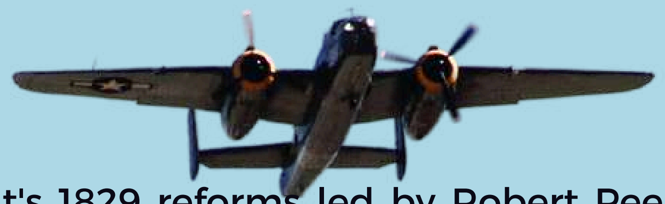
Verifying ID

The methods for verifying different documents have varied greatly over time. Although IDs have been in use for thousands of years, the idea of verifying an ID by checking its information against a centralized database is a relatively recent development. In the past, early passports were personally signed by the issuing monarch, such as those bearing the signature of Charles I, which still exist today. By 1794, the responsibility for issuing passports shifted to the office of the Secretary of State, a role that the Home Office continues to manage. This change brought about the establishment of formal record-keeping, allowing passport information to be cross-referenced with official records for verification when necessary. In the early 20th century, the modern passports we use for international travel were introduced. These passports included new verification features, such as a photograph, a signature, and a personal description. Despite these advancements, verification remained a manual process, involving a physical inspection to compare the individual with the information on the document.

Roman watchword

The Roman army used "watchwords" or passphrases that proved you were a member of the unit. This early authentication system was a fast way to tell if someone was a friend or an enemy.

World War I



After the British Parliament's 1829 reforms led by Robert Peel, the concept of identification cards spread globally. The Netherlands introduced a Personal Number (PN) system in 1849 and started issuing ID cards in 1940. Similarly, the U.S. started distributing Social Security cards in 1936, prompting other nations to adopt ID cards. In the UK, identity documents existed before World War I but were largely unused due to inefficiencies in 18 different personal information registers. During the war, a National Registration was introduced to compile information on all adults and issue identity cards, primarily to assess eligibility for national service. Once the number of eligible men was determined, all 1,413,900 of them, interest in ID cards diminished, and many were lost.

World War II

The Second World War revived the need for ID cards. A comprehensive central register was established at the Central National Register Office, and new folded ID cards with names and addresses were issued. These cards were essential for accessing rations, leading to their regular use. By 1950, ID cards were also integrated into policing. Although the second national register ended in 1952, the National Registration number continued to be used for the National Health Service, voter registration, and National Insurance.

Automated ID

With each iteration of ID design since Henry V's passport, complexity has increased. In 1840, William Henry Fox Talbot's negative-positive photographic system introduced photographs to IDs. By 1858, Sir William Herschel's use of ink fingerprints as signatures marked the beginning of biometric identification. This technology was automated in 1980 in Japan and the U.S. with the development of Automated Fingerprint Identification Systems (AFIS).

Chip and PIN

The introduction of Personal Identification Numbers (PINs) revolutionised how we secure and prove our identities. PINs, which are typically numeric codes chosen by users, were first used with ATMs in the 1960s. They became a crucial method for securing transactions and are now an essential component of security systems, often used in conjunction with physical credit cards, a combination monikered as 'chip and PIN.' In 1967, the first ATM was launched in the UK, requiring a four-digit PIN for cash withdrawals. Since then, PINs have become fundamental in protecting personal information and preventing identity theft.

ID goes digital

The 1970s saw the rise of digital records for ID purposes. In 1977, the U.S. computerised paper records and established a cross-referencing system for banking and government data. This digitisation led to the introduction of smart identity cards in the late 1980s by Germany, Singapore, the Czech Republic, and Spain. These cards incorporated various details such as dates of birth, digital signatures, and biometric data. Today, most ID cards are smart cards with embedded integrated circuits, making them hard to forge. They also often include biometric information, such as photographs, facial measurements, or fingerprints. That brings us to the evolution of online identification.

First digital password

Digital identity through usernames and passwords was first introduced by computer scientist Fernando Corbató at MIT in the 1960s to protect individual files on a shared mainframe used by researchers. This method of establishing an "identity" by securing an account with a password only known to the user became the predominant way to identify people on the internet. However, passwords were weak because if compromised, the account and identity were also compromised. Microsoft later popularised Corbató’s concept, using it to manage access to individual accounts on shared computers. This system evolved into the Microsoft Network (MSN), allowing users to access various services like email and chat rooms with a single login.

Social media revolution

Digital IDs became widely adopted through social media logins, a concept first introduced by Facebook and Google. These platforms pioneered the idea, allowing users to authenticate their identities on other websites by logging in through their social media accounts. This approach streamlined the management of digital identities, offering a convenient alternative to traditional login methods that remain popular today.

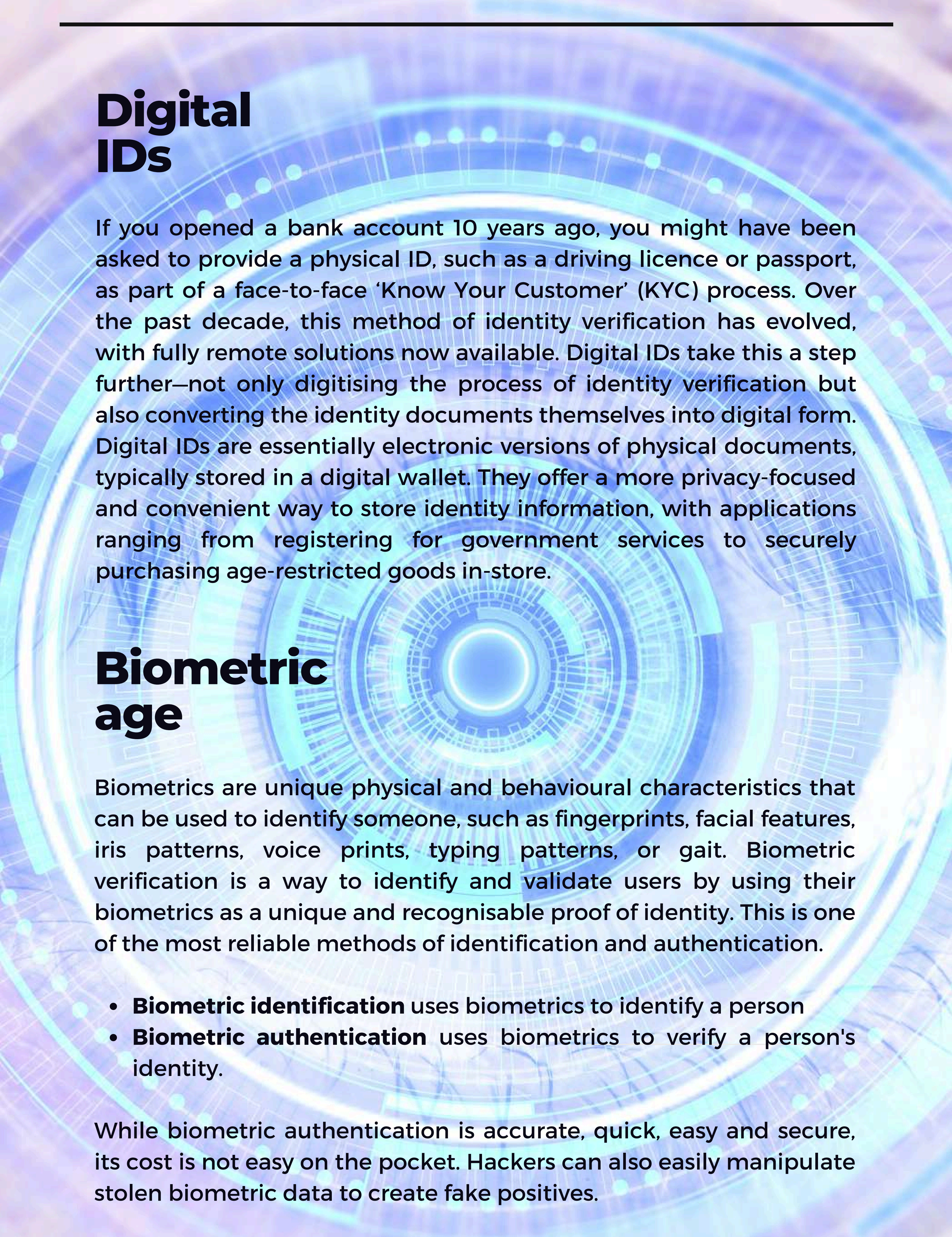
Password evolution

Digital Today, there are passwords for almost everything. Each person has about 100 of them, and they're often shared between family, friends, and coworkers. Netflix, anyone? – although those days are a thing of the past now. Trying to remember all these details daily has led to major password fatigue. Gone are the days when it was okay to store passwords on a sticky note or in a spreadsheet. Now, password managers with autofill and essential security features like two-factor authentication (2FA) and biometrics can help you safely access your accounts—on all your devices—in seconds.

FACT

Prohibition times

In the 1920s, Prohibition led to the rise of "speakeasy" bars where alcohol was sold illegally and on the down-low. Presenting a card, code phrase, or saying a password was your ticket to getting inside.



Digital IDs

If you opened a bank account 10 years ago, you might have been asked to provide a physical ID, such as a driving licence or passport, as part of a face-to-face ‘Know Your Customer’ (KYC) process. Over the past decade, this method of identity verification has evolved, with fully remote solutions now available. Digital IDs take this a step further—not only digitising the process of identity verification but also converting the identity documents themselves into digital form. Digital IDs are essentially electronic versions of physical documents, typically stored in a digital wallet. They offer a more privacy-focused and convenient way to store identity information, with applications ranging from registering for government services to securely purchasing age-restricted goods in-store.

Biometric age

Biometrics are unique physical and behavioural characteristics that can be used to identify someone, such as fingerprints, facial features, iris patterns, voice prints, typing patterns, or gait. Biometric verification is a way to identify and validate users by using their biometrics as a unique and recognisable proof of identity. This is one of the most reliable methods of identification and authentication.

- **Biometric identification** uses biometrics to identify a person
- **Biometric authentication** uses biometrics to verify a person's identity.

While biometric authentication is accurate, quick, easy and secure, its cost is not easy on the pocket. Hackers can also easily manipulate stolen biometric data to create fake positives.

Beef up defence

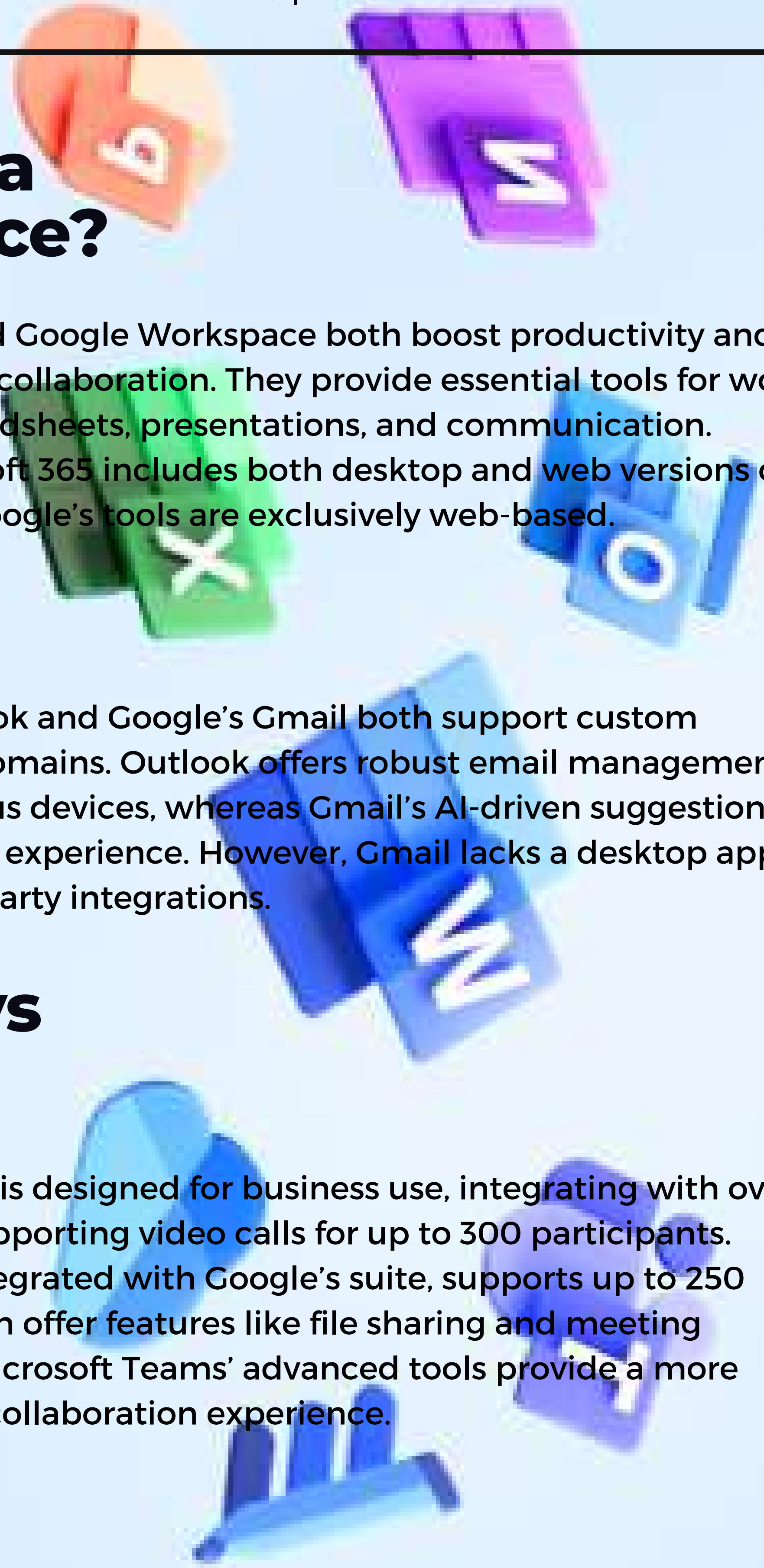
There is no silver bullet to defend against identity theft and other forms of cybercrime and it is no longer possible to stay one step ahead of fraudsters. In today's online world, the best offence is a strong defence, staying abreast of the latest tactics and using data to combat those who seek to exploit it. Multifactor authentication (MFA), a crucial element of any effective security strategy, can now be circumvented by skilled fraudsters.

Beyond MFA

The phone numbers provided during MFA in a fraudulent onboarding attempt can offer more than just proof that the user has access to the phone. These numbers can be analysed across thousands of attributes to identify the person behind them - in milliseconds - preventing the fraudster from executing their scheme before it begins. With fraud and the resulting damage to individuals and brands occurring in an instant, individuals and businesses need to remain vigilant and adopt a nuanced, layered approach to online crime.

PRODUCTIVITY **RULES**

Microsoft 365 and Google Workspace are the leading business productivity suites, with both holding nearly equal global market shares—Microsoft 365 at 46% and Google Workspace at 48%. Microsoft 365 is used by four out of five Fortune 500 companies, including Accenture and PayPal, while Google counts Sony, HSBC, and the US Army among its customers. Both suites offer cloud-based applications that simplify communication and collaboration. While they are similar in many respects, each has unique features. Here you can compare their offerings to help you choose the best fit for your business.



Is there a difference?

Microsoft 365 and Google Workspace both boost productivity and streamline team collaboration. They provide essential tools for word processing, spreadsheets, presentations, and communication. However, Microsoft 365 includes both desktop and web versions of its apps, while Google's tools are exclusively web-based.

Email

Microsoft's Outlook and Google's Gmail both support custom business email domains. Outlook offers robust email management features on various devices, whereas Gmail's AI-driven suggestions enhance the user experience. However, Gmail lacks a desktop app, relying on third-party integrations.

Teams vs Meet

Microsoft Teams is designed for business use, integrating with over 250 apps and supporting video calls for up to 300 participants. Google Meet, integrated with Google's suite, supports up to 250 participants. Both offer features like file sharing and meeting recording, but Microsoft Teams' advanced tools provide a more comprehensive collaboration experience.

Productivity

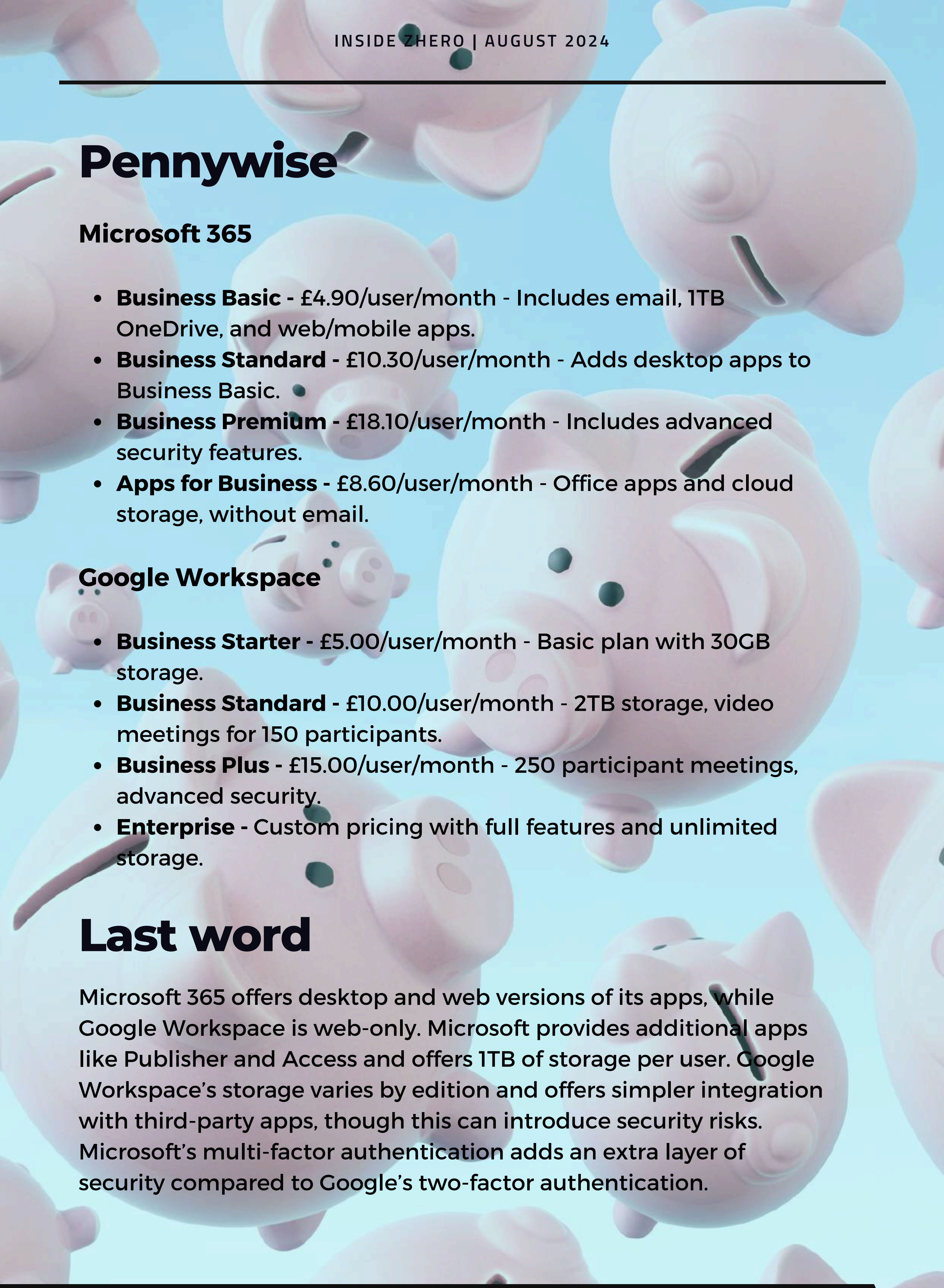
Microsoft 365 and Google Workspace are designed to boost productivity while enabling work from anywhere.

- Both Microsoft 365 and Google Workspace include applications for word processing, spreadsheet calculations, and presentations. Microsoft 365 offers Word, Excel, and PowerPoint. Google Workspace offers Google Docs, Google Sheets, and Google Slides.
- Microsoft's suite can be accessed via PC, mobile, and web applications and includes powerful collaborative features like real-time co-authoring, allowing teams to work on the same document concurrently.
- Unlike Microsoft's productivity tools, which include both desktop and web versions, Google's apps are exclusively web-based.

Google's productivity applications have a cleaner interface and are simple and easy to use. Real-time co-authoring capabilities in these apps allow teams to suggest, comment, make notes, and review changes on the document.

Security

Microsoft's Microsoft 365 and Google Workspace are designed to meet stringent data privacy and security standards and are regularly updated to ensure their security. Both platforms allow administrators to customise security protocols to control user access and permissions. Microsoft 365 offers email protection from spam, malware, and other threats with Exchange Online Protection, It includes security groups and custom permissions to protect business information from unauthorized access and viruses, spyware, and other malware. Google Workspace also provides phishing and spam protection for email, along with two-factor verification, group-based policy controls, the Advanced Protection Program, and endpoint management.



Pennywise

Microsoft 365

- **Business Basic -** £4.90/user/month - Includes email, 1TB OneDrive, and web/mobile apps.
- **Business Standard -** £10.30/user/month - Adds desktop apps to Business Basic.
- **Business Premium -** £18.10/user/month - Includes advanced security features.
- **Apps for Business -** £8.60/user/month - Office apps and cloud storage, without email.

Google Workspace

- **Business Starter -** £5.00/user/month - Basic plan with 30GB storage.
- **Business Standard -** £10.00/user/month - 2TB storage, video meetings for 150 participants.
- **Business Plus -** £15.00/user/month - 250 participant meetings, advanced security.
- **Enterprise -** Custom pricing with full features and unlimited storage.

Last word

Microsoft 365 offers desktop and web versions of its apps, while Google Workspace is web-only. Microsoft provides additional apps like Publisher and Access and offers 1TB of storage per user. Google Workspace's storage varies by edition and offers simpler integration with third-party apps, though this can introduce security risks. Microsoft's multi-factor authentication adds an extra layer of security compared to Google's two-factor authentication.

On 14 October 2025, Windows 10 Home and Pro will reach end of support or end of life (EOL), following Microsoft’s Modern Lifecycle Policy. Ater this date, your Windows 10 PC will no longer receive free security updates and Microsoft will no longer be available to provide Windows 10 technical support. Your PC will continue to work, but all support for Windows 10 is discontinued.

BREAKING NEWS

What you can do

- You could ignore the EOL deadline completely. This is NOT recommended as your PC is no longer receiving updates and security patches from Microsoft. This means your PC is vulnerable to malware infections and other cyber threats. You will also experience performance and compatibility issues.
- You can pay Microsoft for security updates for Windows 10. With the Extended Security Updates package, you can keep your current Windows 10 device fully protected for up to 3 years. According to Microsoft, the first year of protection will cost £50. This increases to £100 in the second year and £150 in the final year of cover.
- You can upgrade your existing PC to Windows 11 or buy a new laptop with this latest OS already installed.

What we recommend

We recommend switching to Windows 11. We will assess whether your existing PC can be upgraded and is capable of running Windows 11 or if you will need a new workstation. While making the change to a new OS may seem daunting, we are here to support and assist you in every way we can.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Lucindi Storme

COMPLIANCE CONSULTANT

Hi Lucindi! What made you realise you want to go into the IT industry?

I didn't pick IT, IT picked me. I was studying Electrical Engineering and in one of the practical classes I set the classroom on fire. So, I went for my second choice.

What's your most-used productivity tool?

My brain and my mood – I rely on my intellect and positive attitude to tackle challenges. As a backup, I use Outlook.

How would you describe yourself?

I see myself as a smiling problem solver. I don't let the little things in life get me down and I'm not afraid of challenges.

What do you enjoy the most about your role?

There is no most – I love everything about my role. I honestly love what I am doing.

Do you have any hidden talents or hobbies?

I don't know about talents but my hobbies include wreck diving and anything to do with speed – bikes, jet skis and horses.

What is your favourite movie or TV show?

My favourite movies are Pulp Fiction and Finding Nemo. My favourite TV show is The Big Bang Theory. It's on repeat!

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975

zhero

crush the chaos