FINGERPRINTS

ACCESS YOUR SMART WORK PLACE

ACCESS THE RIGHT AREAS

SMART WORKPLACE

The workplace is powered by technology with PCs, smartphones, dongles, cloud applications and more sitting at the heart of today's working world.

While these applications are essential to productivity, securing the office's digital and physical spaces against growing threats while accommodating 'work from anywhere' practices as well as hybrid working models are becoming complex balancing acts.

The balance of convenience and security offered by biometrics makes it perfect to deliver a smarter and more secure workplaces, wherever employees choose to access corporate infromation.

SECTION 01

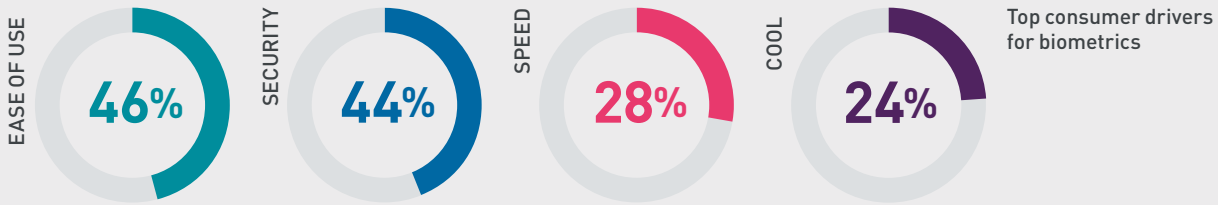
WHY BIOMETRICS?

01

Biometric authentication is putting an end to the frustration, stress and risk of misplaced physical keys, cumbersome and forgettable passwords, and unhygienic PIN codes. With biometric technology, you are the key to everything.

In today's connected workplaces, we are required to prove who we are many times, from office doors to sensitive corporate data, which can be a burden. Smart workplaces striving to be better.

With so many activities needing fast, reliable and convenient authentication, it is no surprise that organizations increasingly demand seamless and secure interactions.



Today there is a broad variety of biometric technologies available to address this need, with fingerprint recognition being the most widely used.

SOURCE: Fingerprints in collaboration with Kantar 2017, 4,000 online consumers in UK, USA, India, China

THE PROBLEM WITH PASSWORDS

Although PINs and password are easy to implement, they can be hacked through data breaches, spyware, algorithms, or even social engineering techniques like shoulder surfing.

As the number of connected systems in our homes grows, we cannot be expected to create, remember and manage a growing list of passwords and PINs.

- ***60% of consumers feel*** they have too many to remember[1]
- Often, we have as many as ***85 passwords and PINs*** to manage across all their personal and professional lives[2]
- ***41% of us*** admit to reusing the same password or injecting minor variations, risking scalable attacks by hackers if just one password is compromised[3]
- ***60% of hacks and data*** breaches are a result of stolen credentials such as PINs and passwords[4]
- ***Gartner predicts that by 2022*** 60% of large and 90% of mid-size enterprises will implement password-less authentication methods in over half of use cases scalable attacks by hackers if just one password

THE BENEFITS OF BIOMETRICS FOR ACCESS CONTROL

Compared to other forms of authentication, biometrics provide choice, security, and an intuitive user experience, bringing a range of benefits to device manufacturers, service providers and end-users alike. In addition, businesses are always sure that only the right person or people are granted access.

SECTION 02

THE SECURITY AND CONVENIENCE BALANCING ACT

02

Biometrics is a unique authentication technology that provides an optimum balance between security and convenience.

Balancing a system's security must take into account how well the biometric identifier can be read and matched with how secure the solution is and how well it prevents unwanted access, hacks and spoofs.

SOURCE: Fingerprints in collaboration with Kantar, 2019, 1,200 online consumers in UK, France, China

ANTI-HACKING MEASURES:

- A mathematical representation of the fingerprint is stored as a template, instead of the image itself.
- Removes the incentive for hacking as it cannot be used to re-create the original fingerprint image.
- The template is stored, and the algorithms involved in the authentication process run in a Trusted Execution Environment (TEE) or Secure Element (SE), keeping data away from threats.

ANTI-SPOOFING MEASURES:

- Increasing the image quality and by using sophisticated matching algorithms.
- Using more than one biometric identifier.
- Increasingly sensitive sensors.

No system can be made totally secure – with unlimited time (and money) it is possible to hack and spoof biometric systems. Advanced biometric techniques however make such malicious attacks extremely expensive and time consuming, and therefore unscalable and unappealing to fradusters.

MEASURING CONVENIENCE AND SECURITY

FALSE REJECTION RATE (FRR)

Often used to gauge the convenience of biometric sensors, this tells you how often the sensor will wrongfully reject the valid biometric in the matching algorithm.

FALSE ACCEPTANCE RATE (FAR)

Frequently used in assessing the security of biometric systems, this tells you how often the sensor will statistically provide a positive match without the right biometric data.

Plotting the FRR versus the FAR for various types of biometric authentication systems gives an insight into the trade-offs between security and convenience. The ideal biometric solution has minimal FAR as well as FRR.

SECTION 03

FINGERPRINT SENSORS: THE STANDARD BEARER FOR BIOMETRICS

Humans have many biometric identifiers, or modalities, that can be captured and analyzed by biometric systems. But what kinds of biometric authentication are there, and **why has fingerprint risen to the top?**

Fingerprint has risen to the top because it is increasingly familiar amongst consumers because of smartphones, and provides an optimum balance between security and convenience, making it ideal for robust and frictionless authentication.

FINGERPRINT TECHNOLOGY FOR SMARTER ACCESS CONTROL

Active capacitive fingerprint sensors provide choice, security and an intuitive user experience, helping device manufacturers in the smart home sector to level up their systems.

EFFICIENCY
Low power consumption – 1,8 volt power

SECURITY
Optimized features to maximize secure authentication

FUNCTIONALITY
High image quality with optimized biometric performance

CONVENIENCE
Enduring speed (<400ms) and minimizing false rejections (FRR 3%)

RELIABILITY
ESD protection: +-15kv

DURABILITY
Waterproof coating IP67, +10M touches

HYGIENE
Enabling a contactless experience for a safer authentication

PRIVACY
Offers enhanced privacy if local storage

Automated processes for biometric recognition have only become possible in the last few decades with the advancements in integrated circuits and computer processing. Today, there is a broad variety of biometric technologies available to businesses, with fingerprint recognition being the most widely used.

FINGERPRINT - Analysis of the unique ridges and patterns of skin on our fingertips

The de facto modality to date and often the first thought in biometrics.

EYE - Examination of the iris, retina or scleral vein patterns of the eye

Previously a preserve of governments, now present in some smartphones

FACE - Scrutiny of the many features of the face

Widely available in many of today's smartphones. Simpler 2D solutions can be easier to spoof and become unreliable with ageing faces.

VOICE - Analysis of a person's voice print

Although cheap, it is easy to spoof and difficult to accommodate changes that come with age, illness or location.

VEIN RECOGNITION - Scrutiny of the vein pattern of fingers or hands

A secure but sometimes slow method with high processor requirements, making scanners large, costly and power hungry.

BEHAVIORAL - Recognition of a person's gait or gestures

Comes with accuracy concerns and is relatively new and expensive as it requires additional complex equipment and analytics to be integrated with a video surveillance camera.

SECTION 04

BUILDING A SMARTER WORKPLACE WITH BIOMETRICS

04

Protecting the workplace and its data is a significant issue for many organizations, and new technologies, growing digital threats and changing working trends have changed office spaces.

GROWING SECURITY THREATS

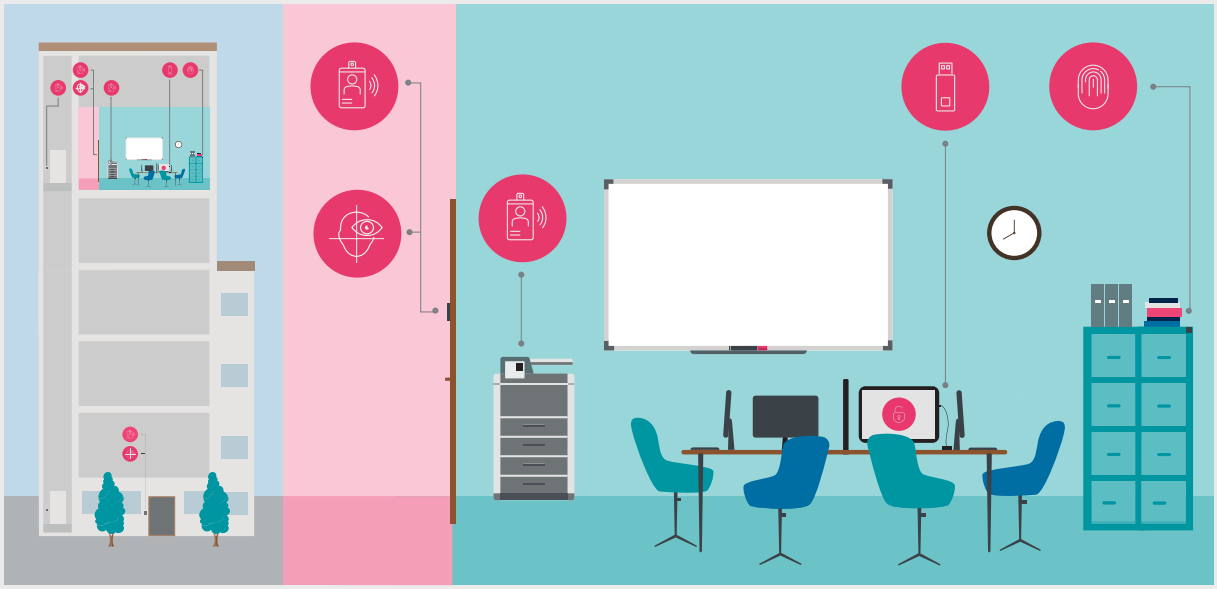
As offices have become more technologically driven, protecting digital spaces from hacks and data breaches has become an acute issue for organizations.

- April 2021 saw *1 billion records* breached for the first time, from 143 known incidents[1]
- A computer hack takes place *every 39 seconds*[2]
- The average business cost of a *breach in 2020 was $3.86 million*[3]
- In 2021, cyber-attacks are set to cost organizations *$6 trillion in losses* – double the amount in 2015[4]

Organizations can never take their eye off the ball when it comes to security, but changes in working patterns have made the challenge more complex for decision-makers.

SOURCES: 1. IT Governance, List of data breaches and cyber attacks in April 2021, 4th May 2021 2. University of Maryland, A. James Clark School of Engineering, Study: Hackers Attack Every 39 Seconds, 2017
3. IBM Security, Cost of a Data Breach Report 2020 4. Cybersecurity Ventures Official Annual Cybercrime Report 2020

Biometrics can bring new levels of protection and convenience for both physical and logical access control, providing a smarter workplace that empowers employees and drives productivity while offering robust protection.



How biometrics makes a workplace smarter

ENTER WORK & ACCESS THE RIGHT AREA

Office doors, alarms & safes – can be accessed and controlled with biometric solutions

KEEP YOUR PC PERSONAL

Biometrics in PCs and peripherals – to access devices, corporate apps and services

ENTER AND UNLOCK DIGITAL SPACES

Access secure data environments – such as the company server, encrypted USB storage devices and ensure seamless connection to VPNs, controlled access servers and applications

WORKPLACE PERSONALIZATION

Your settings – or personal employee accounts can be enabled easily when using shared devices such as printer systems, hot desk PCs and even coffee machines

ON THE CARDS – BIOMETRIC ACCESS CARDS

One of the most direct ways for employers to realize the benefits of biometrics for their workforce and make a smarter workplace is through biometric access cards

Biometric access cards can be thought of as a multi-function key that can be combined with other enterprise use cases such as:

- ID badge
- Physical and logical access
- Time and attendance logging
- Office alarm control

BIOMETRICS... IN AN ACCESS CARD?

1. Privacy Fingerprint data is stored in the card.
Users control their own data. 100% GDPR compliant.

2. Power Ultra-low power consumption, even when active.

3. Flexible Manage access rights and combine access with time tracking, alarm systems, ID badge and more. Works with existing contactless technologies.

4. Performance Small, thin and robust sensor.
Authenticate from any angle in less than half a second.

BIOMETRICS IN ANY WORKPLACE

Hospitals & pharmaceuticals
Convenience and security are vital for staff and patient safety, whether it is in wards, drug cabinets, operating theaters, patient data storage spaces.

Labs and R&D departments
Many organizations pride themselves on innovation, which is often subject to industry espionage and must be protected alongside limiting access to hazardous materials.

Protecting corporate data
Organizations face increasingly severe penalties if data security is poor, and they leak personal, confidential and sensitive information.

WHAT ARE THE OPPORTUNITIES?

CARD MANUFACTURERS

- Bring innovation
- Increase market share
- Add features and functionality to existing card
- Offer a hygienic access solution
- Privacy compliant

ENTERPRISES

- Secure & Convenient physical and digital access
- Hygienic and contactless, no tap on pin pads
- Enhanced privacy as data stored on device, card is personal
- Combine access with ID badge, time and attendance, alarm...
- Works with your existing infrastructure
- Reduce IT, admin and fraud cost
- Reduce concern and stress among staff

Biometrics - providing a worryless, convenient and secure home environment

ABOUT US

Trusted company

- Fingerprints solutions authenticate users billions of times per day
- Hundreds of millions of sensors shipped yearly
- Integrated in over 500 smartphone models

Enhancing design opportunities

- Our small sensors and modules enable brands to be as creative as they like
- Ready for cost-effective, high volume production
- Largest fingerprint biometric supplier to door lock makers globally

Outstanding performance

- Unrivalled low power consumption
- High image quality – optimized biometric performance for small sensors

FINGERPRINTS