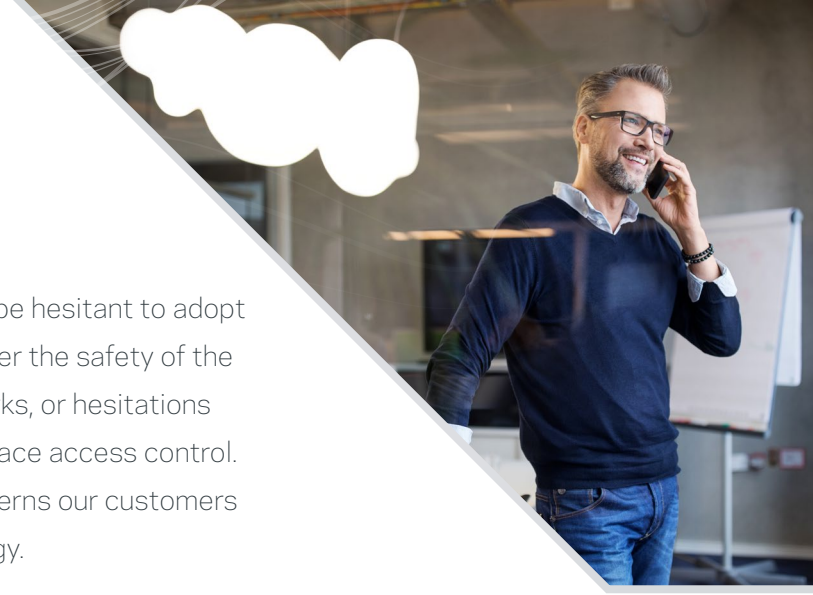
# Five reasons to integrate mobile technology into your security solution

Mobile technology use in everyday life has increased massively in recent years. Most of us now have a mobile device that we use to manage different aspects of our lives – from banking, to accessing public transport, and even paying for a coffee. With approximately half of all web traffic around the globe coming from mobile device users, the move to mobile is having a major impact on industries worldwide.

**So why then is mobile not utilised more within the security industry?**

In this white paper, we highlight five reasons to integrate mobile technology into your security solution. Here, we take an in-depth look at some of the frequently referenced barriers to adopting mobile technology, discuss the benefits mobile technology can bring to an organisation, share the views of industry leaders, and look to what the future holds for mobile within the security industry.



# Barriers to mobile

There are a number of reasons organisations may be hesitant to adopt mobile security solutions; whether it's concerns over the safety of the technology, uncertainty of how the technology works, or hesitations from staff about using personal devices for workplace access control. Here, we address some of the most common concerns our customers raise with us in regard to mobile security technology.

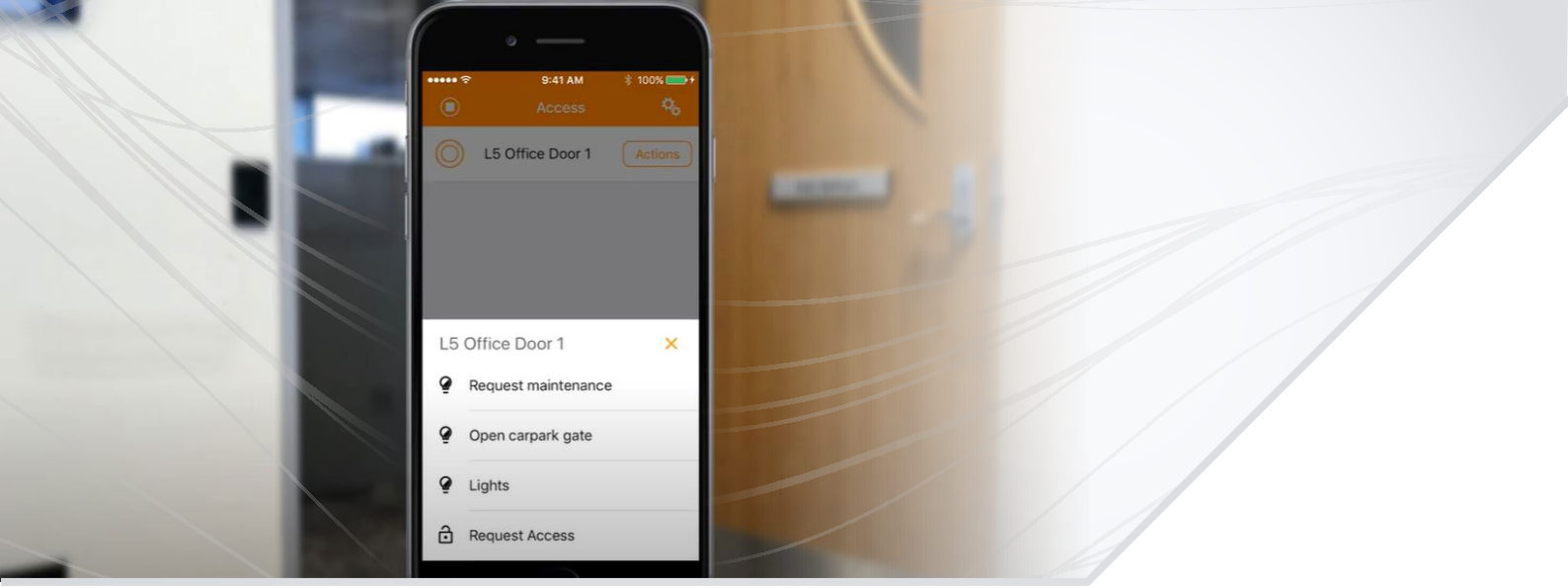
### *How secure is mobile?*

Just like a high security access card, mobile credentials are secure and safe. The nature of a mobile device automatically keeps the credential more secure than an access card, as people tend to care more about their phone than they do an access card, making them less inclined to lend their phone to others and are more likely to notice if their phone has been lost or stolen. If someone were to lose their access card on a Friday afternoon, for example, they may not notice it was missing until the following Monday, but a missing phone would be noticed much sooner.

Mobile credentials are not susceptible to card cloning and some mobile solutions hold the option of adding two -factor authentication using the built-in device security, such as fingerprint, PIN, or facial ID on some phones. This is considered industry best practice and adds an extra layer of security, particularly if using biometrics, to ensure the credential cannot be used by anyone other than the authorised credential holder.

Reviewing the authentication method of a mobile credential solution can provide some assurance as to the safety of the application. FIDO authentication, for example, is trusted by many leading technology organisations around the world. It uses public key cryptography with the private key stored securely on the phone to create strong authentication that is resistant to phishing and other common attacks.

With the current push to contactless methods for carrying out day-to-day activities, mobile credentials can help protect people's health and safety by reducing contact between people and surfaces. With a longer read range between the device and reader than an access card, people are unlikely to make direct contact with the reader, and, as mobile credentials can be set up remotely, face-to-face interactions are reduced, and there is no exchanging of access cards between people. This is especially beneficial for site visitors, where an access card may pass between many different people during the course of a day.




### *Does Bluetooth technology leave you vulnerable?*

Mobile access control utilises Bluetooth Low Energy (BLE) for communication to access control card readers from mobile phones. A mobile access control system utilising a strong authentication method will ensure the communication is secure and cannot be used by anybody 'sniffing' the communications to get access by replay attacks or other methods.

Authentication methods like a public key-based credential will keep communication secure between the reader and device. The reader will send a random string of data to the phone and, using a private key securely stored in the phone's key store, the phone will sign the data and send it back to the reader. The reader will use the public key to validate that the digital signature is correct and, if so, will open the door. As a different random string of data is sent to the phone every time, there is no risk of unauthorised entry via replay attacks.

The risk of a relay attack, or man in the middle attack, can also be mitigated. In a relay attack, an attacker will attempt to impersonate a person's credentials using two devices to 'relay' the messages from the door and a person's phone, using an app they've written on two wirelessly connected devices, like mobile phones. One device will be held near the reader and the other near the phone that is being impersonated; the reader and phone will believe they are talking to each other and perform the authentication.

Choosing an intelligent access control system that uses algorithms to detect this happening can mitigate the risk of these attacks, as can requiring two-factor authentication at the reader.

### *We use our access cards as staff ID. How will we identify people on site?*

A combined staff ID and access card can present security risks. If someone were to misplace their card, it is easy for the person who found it to identify which organisation it belongs to and use it to gain unauthorised access to the building. Separate staff ID and access credentials can mitigate this risk, with mobile credentials negating the need for staff to carry two cards.

Mobile reader technology can also be used to verify whether someone is authorised to be in a particular area on site. Using a mobile reader, a security operator can read an individual's credentials, verify their identity against the staff photo on file, and confirm if they have the authority to be in a certain area.

### *Not all of our staff have a suitable mobile device. Does that mean they can't get into the building?*

Moving to mobile credentials doesn't have to be an all or nothing solution. It's not uncommon for sites operating mobile access technology to offer staff the choice between a mobile or card credential to ensure no one is excluded.


# What are the benefits of mobile technology?

In addition to the security benefits listed in the previous section, utilising mobile technology as part of a security solution offers many benefits to organisations. When implemented as part of one integrated security system, mobile credentials are easy to deploy, simple to operate, and provide administration efficiencies and cost saving opportunities.

Mobile technology removes the need for the operator and cardholder to be present in the same place at the same time to provision and receive credentials. This allows the operator to provision mobile credentials at a time that suits them, and allows for instant access when the cardholder arrives on site. At universities, in particular, this can save huge administrative efforts and time at the beginning of a semester, when large numbers of students are arriving on campus at the same time and require access into lecture theatres and halls of residence.

In addition to time, mobile credentials can also save organisations money. Mobile credentials are more affordable than access cards, when compared to the costs of purchasing, printing, and distributing the cards and, by utilising technology that is already in possession of the users, organisations can reduce plastic waste and emissions associated with creating and shipping access cards throughout the organisation.

Other mobile security solutions allow security operators to manage day-to-day security issues remotely. Tasks such as unlocking doors, managing alarms, and disabling cardholders in the event of a lost credential, can be easily managed on the go via a secure mobile app that communicates directly with the security software.

By freeing security operators from the control room, they can easily respond to security events from anywhere on site, as and when they arise. This technology is critical in an emergency situation where operators need real-time security information but may not have access to the control room.

# Mobile technology for efficient, fast emergency responses

Security emergencies, whether they be evacuations or lockdowns, require access to security information and reliable communication with people on site. With the assistance of mobile technology, organisations can ensure compliance with health and safety requirements and create faster, more efficient evacuations and safer site lockdowns.

In an evacuation, mobile technology can be used to verify that cardholders are safe and reduce the time spent mustering. With wardens operating mobile technology linked directly to their security software, they have full visibility of movement on site, allowing them to move cardholders to safe zones and see which cardholders have not yet reported to the evacuation zone and may need to be followed up with.

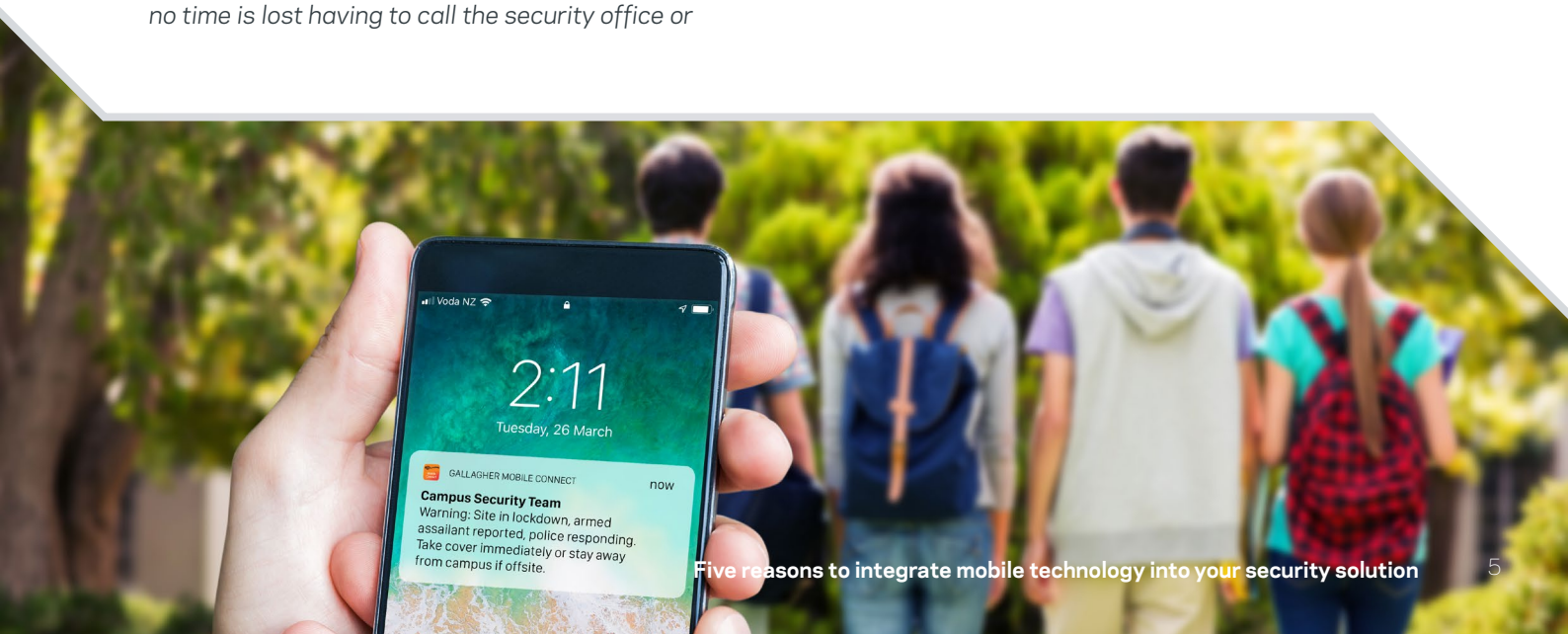
With no need to print physical evacuation lists, mobile technology avoids the manual and lengthy process of accounting for everyone's safety, allowing people to safely return to work sooner.

Emergency lockdown processes can also be improved with mobile technology. Challenges in a lockdown situation include the length of time it can take to initiate the lockdown and providing effective communication to people on site. Mobile security solutions can ensure a secure, fast lockdown process while ensuring people have the information they need to keep themselves safe.

Consider the following example of a lockdown situation at a high school: *A teacher has identified a threat on campus. Instantly, they can activate a campus-wide lockdown from their mobile device; no time is lost having to call the security office or reception to initiate the lockdown. Within seconds, the school is locked down, all external doors are automatically locked, authorities are notified through an automated message, and building access is limited to emergency responders only.*

*Shortly after the lockdown is initiated, security officers send a push notification to staff mobile devices informing them of the situation and advising them to ensure students are safe. A separate notification is sent to students with directions to remain where they are and keep themselves safe. A further notification is also sent to staff and students located off site informing them to stay away until further notice.*

This example demonstrates how mobile technology can enhance a lockdown response, ensuring fast responses and effective communication. Studies have found push notifications on a phone are considerably more likely to be read than an email and receive higher engagement than a text/SMS message. Push notifications are a more affordable option of mass communication than text/SMS messages and, as it's clear where the communication is coming from, people are more likely to view them as a trusted source of information.



# Industry views of mobile technology use in security

According to **Steve Bell, Chief Technology Officer at Gallagher**, choosing a quality security system is vital in ensuring mobile security can provide secure, effective protection that meets the needs of your site.

He describes a secure mobile access solution as one which has algorithms in place to detect potential attacks, holds the option of adding additional authentication requirements such as a fingerprint or PIN, and which utilises a secure authentication method, such as public key credentials.

**Matt Brittle, Head of UK Security, Risk & Resilience at WSP**, believes there are a few key things organisations need to understand as the security industry becomes more mobile, which includes seeking education on how to keep themselves protected against threats. With this knowledge, organisations can ensure they aren't leaving themselves vulnerable to attacks.

As Brittle describes it, we used to lock things away behind a physical door but with mobile, we need to understand what the new virtual door is. The more people understand about their mobile systems, the more secure and seamless the integrations can be.

**Patrick Goudkuil from D J Goode & Associates** believes mobile technology has a part to play in the future of access control across a large number of industries; however, he advises it should be viewed as a piece of the overall security strategy, rather than the sole answer. Goudkuil recommends choosing a recognised partner with a track record of providing robust cyber security, and opting for technology that is secure and compatible with existing systems.

# What does the future hold?

As technology progresses and the world becomes more mobile, it's inevitable mobile technology will become more prevalent in the security industry. While it is difficult to predict exactly what the next big development will be, we anticipate digital IDs will become a feature of mobile security in the near future. In utilising a secure digital ID that can be displayed on a mobile device, organisations can navigate one of the barriers to mobile security – the need for staff to carry a separate ID card in addition to their mobile access credential.

The emergence of IoT and smart technology is accelerating our desire, as consumers, to integrate mobile technology into our everyday lives. From million-dollar smart city projects, to the ability to switch on your washing machine from your mobile phone, we all want to be a part of the technology evolution. With the associated cost efficiencies and environmental benefits, mobile has established an influential role in our future – not only for the security industry, but all aspects of our lives.

# Five reasons to integrate mobile technology into your security solution

1. Ease of deployment
2. Safety
3. Efficiency
4. Cost savings
5. Remote management

**Mobile technology is already an integral part of our everyday lives and there's no doubt it is here to stay. In this ever-changing world, it is now more important than ever for businesses to review their security strategy and consider the extensive efficiency and safety benefits that mobile provides.**


## Want to know more?

Visit **security.gallagher.com** for more information on secure mobile security solutions or email us:
UK / Europe: **info.eu@security.gallagher.com** Global: **security@gallagher.com**