ACTIVE WITNESS

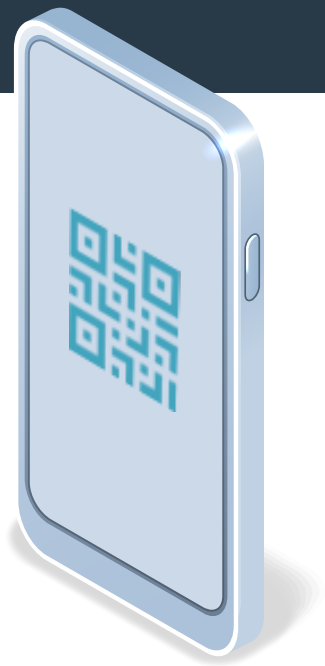
Mobile Credentials & Cloud-Based Systems

What's all the Buzz About?

The access control industry is replacing physical key cards with mobile credentials, and they are using the cloud to do it. Employees, visitors, students – everyone almost always has a smartphone with them. And since people are less likely to lose their phone than they are a key card, it only makes sense to incorporate mobile access into any security solution.

There are a number of benefits to moving to the cloud to support an access control system including almost unlimited – and less expensive – scalability and remote management and troubleshooting. It might be tempting to try and hold onto that legacy access control system for just a little longer, but existing legacy technology can be more susceptible to threats which can render the security system useless.

Those looking to install or improve access control need to consider a solution with mobile access and with cloud-based management as it's more economical, is easier to use and manage, and improves user satisfaction.

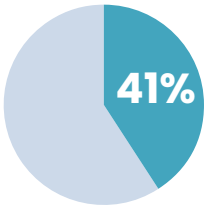


The access control industry is
- Moving to cloud-based systems from server based
- Replacing physical key cards with mobile credentials

Cloud based systems support
- Scalability with limitless number of users and access points at minimal cost
- Highly customizable solutions
- Remote troubleshooting
- Simplified user enrolment with digital streamlining of administration processes
- Minimal time spent on system administration
- Low cost of maintaining the infrastructure
- Nimbler for ongoing product development

Mobile credentials support

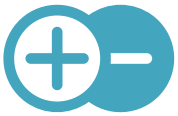
• While physical credentials may cause problems for users, they also cause headaches for building management. A study explored common pain points and inconveniences related to access control card purchasing and usage and found:



41% of office workers use key cards to enter their office. Yet the same amount of people said smartphones or smartwatches would be their first-choice credential.

3 out of 4 people use keys, key cards or fobs. 41% had their keys, key cards and fobs lost or stolen while 34% let someone borrow them.

The survey found that **over 50%** of the respondents identified the cost of proximity cards as the most crucial issue, followed by 14% that indicated the shipping/lead times of new cards was the main pain point.



In all, over **75%** of survey respondents reported that dealing with proximity cards – from paying for new cards to waiting for them to arrive – was a part of their day they could do without.

• Minimizing the environmental impact of plastic waste associated with lost, stolen or damaged key cards.

• Eliminating the cost of issuing new physical key cards and going digital saves both the cost of purchasing key cards and employee hours spent reissuing cards.

• Lower administrative burden

• Touchless access

• Increased security: Mobile credentials are difficult to fraudulently replicate as mobile access is protected by PIN or biometric credentials.

Existing legacy technology –which is still very much out there – is susceptible to ongoing security threats such as theft or fraudulent replication of cards.

What are the Risks of Inadequate Security?

80% of company leadership would agree that the burden of keeping their staff safe from physical harm is greater than ever before.

71% state that the potential for physical threats has exponentially increased vs. early 2020.

69% feel that leadership would agree that if there were a fatality resulting from an unaddressed physical threat that it would be impossible to recover, both financially and in the public eye.

65% see increased potential for financial losses.

87% agree that developing physical security technologies is necessary to mitigate violent threats and is necessary to the future of the company.

44% feel access control is more important after the coronavirus pandemic.