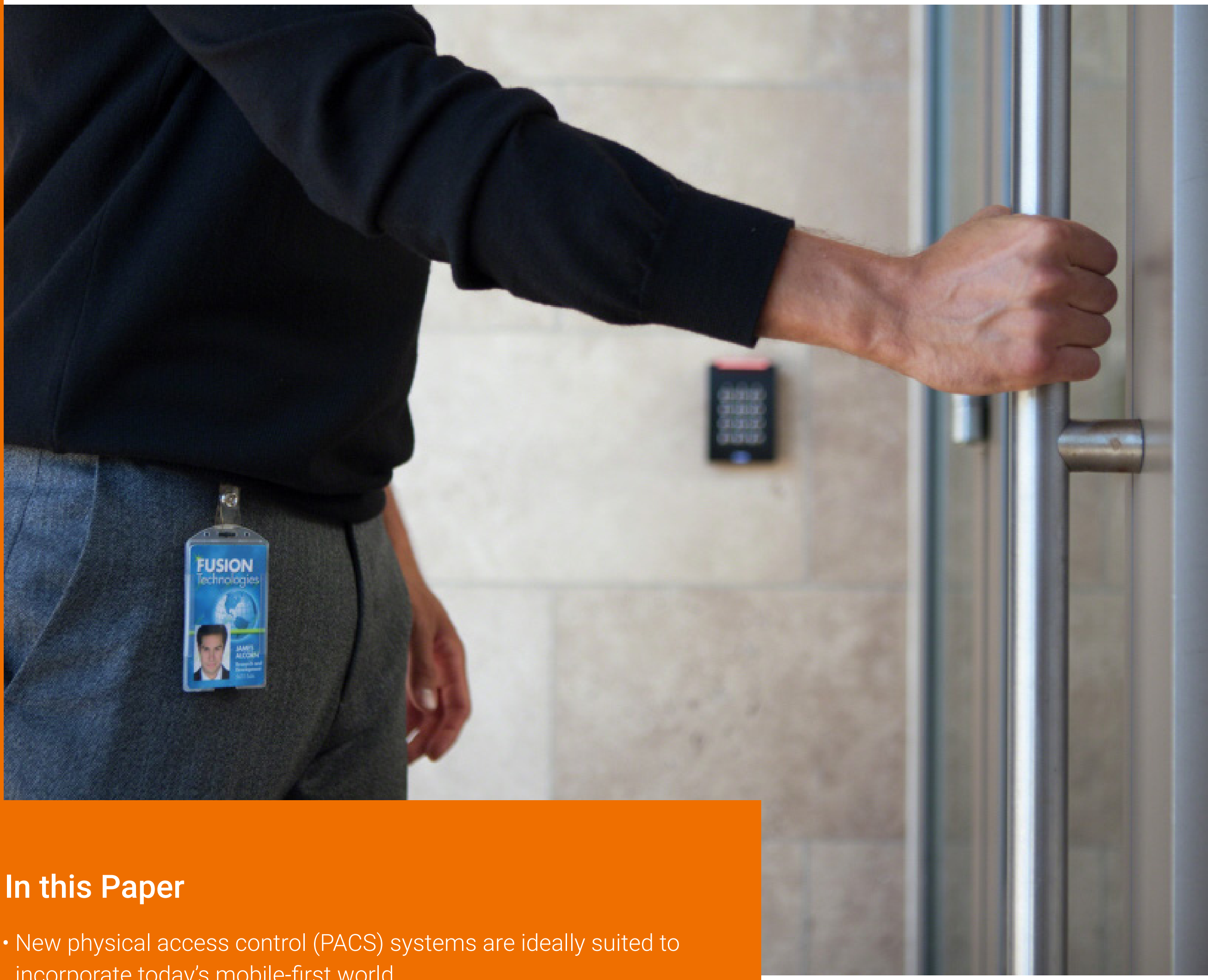
EXECUTIVE BRIEF

Sponsored by

Opening Doors to Streamlined Business Processes with Innovative Access Control Technology



In this Paper

- New physical access control (PACS) systems are ideally suited to incorporate today's mobile-first world
- They offer many advantages including convenience, heightened security, and increased professionalism
- Now is the time to determine if your business should move to a more modern PACS approach

eSecurity Planet

Introduction

Smaller and medium-sized businesses (SMBs) need to leverage technology innovations to operate as efficiently as possible and to compete with larger companies. One area where the use of new technology can immediately deliver benefits is physical access control (PACS). Compared to legacy systems, new PACS systems are ideally suited to incorporate today's mobile-first world. They offer many advantages including convenience, heighted security, and increased professionalism.

Additionally, in several organizations, there is a merging of IT security control and physical access control. Newer PACS systems help bridge the gap and offer efficiencies in both areas in addition to providing much stronger security and resource efficiencies.

To these points, the technologies behind PACS are constantly evolving. Smart card technology still reigns supreme, with good reason, as it meets the needs of many organizations today. But the steady stream of technological advances in access control means SMBs have a number of options available to them in this area.

Some organizations might be intrigued by biometrics or the use of mobile devices as part of their access control strategy. Others might find value and reduced risk when they combine their physical access security with network access security in their organization. Still others may want to incorporate mobile devices into their physical access ecosystem.

> "Modern ID management solutions are needed to ensure appropriate access to resources across increasingly heterogeneous technology environments."

It doesn't make financial or business sense to upgrade access control just because there's a new development in the technology. Rather, your organization needs to choose the technology that fits its needs now and in the foreseeable future, and plan upgrades as part of a coordinated strategy. This strategy should incorporate the needs of different physical locations, as well as any relevant regulations surrounding access and security.

Most organizations will find that several reasons to update their legacy physical access control will present themselves during the normal course of business.

This Executive Brief discusses nine such opportunities for a PACS upgrade.

1. Inefficient ID management: Organizations need more flexible and dynamic access control in today's business environment. In particular there is a need for easier and more refined features, such as managing who has access to certain rooms at certain dates and times. Modern ID management solutions allow a company to provide the right individuals with access to resources while denying access to those who do not have privileges to access those resources. With data theft on the rise and the introduction of new privacy regulations, ID management is becoming much more important. As such, modern ID management solutions are needed to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. A variety of technologies have been used to implement ID management including smartcards and security tokens. PACS solutions that leverage ID management can help address both physical and IT security issues.

2. Unprofessional visitor management: When a prospective customer or long-term client comes to your office, the first engagement carries a lot of weight. A bad impression or a disorganized staff encounter can sour a deal before any meeting begins. Whether you have a lobby reception desk, an employee with a tablet greeting visitors, or a self-serve visitor kiosk, any of these scenarios require a way to quickly register visitors and provide them with a pass to utilize your facilities. The solution must take into account that different visitors will need different levels of physical access, while some will need permission to use corporate WiFi and other IT resources.

3. Facility consolidation: Adding to your current location or moving to a new location presents another great opportunity to replace outdated access control with current technology that offers a better user experience and enhanced security.

4. Card re-issuance process: As new employees join, organizations may manage costs by purchasing additional cards that work with their old technology. Some organizations may also need to change cards due to a new brand image or logo, creating an opportunity to upgrade to newer technology.

5. Need for additional card applications: Organizations that want to add new applications such as time and attendance, secure print management, biometrics, cashless vending, and more will need to issue some type of associated card to users.

"An appropriate approach should allow an organization to automate the entire process of registering a visitor, printing a badge, and capturing detailed information in seconds."

They can use this requirement as an opportunity to migrate to a contactless smart card that combines access control with these or other functions, enabling employees to carry a single card for multiple purposes.

6. Risk management improvement: Either due to insurance requirements or to improve risk management by reducing liabilities, moving from an outdated system to a modern one can dramatically improve security for an organization.

7. Changes to security requirements: As a result of new legislation or regulatory requirements, an organization may be required to increase its security. Similarly, if a company enters a relationship with a client needing a high level of security, there may be requirements to improve access control. New building tenants may also trigger the need for greater building security, either to protect the parent organization or to comply with the tenant's requirements. The organization also might want to add biometrics as an additional authentication factor, and/or new visual card security technologies to prevent counterfeiting.

8. The need for professionalism: Legacy technology can create an undesirable brand impression. In many environments, visitors are still asked to enter their information in a paper log book. Imagine how this makes a modern, tech-forward business look to a job candidate, potential investor, or new partner. An appropriate approach should allow an organization to automate the entire process of registering a visitor, printing a badge, and capturing detailed information in seconds by simply electronically scanning an ID (such as a driver's license, business card or passport). This will give visitors a much better impression and show them that the company is not relying on technology from the last century.

9. Unexpected security event: The unfortunate reality is that sometimes it takes an unexpected event or security breach to prompt an organization to make the investment in a new access control system. Ideally, an organization should migrate before there is a problem. Rather than being reactive to security problems after they occur, a company should invest in modern solutions that can prevent the incidents from happening in the first place.

Is it time to upgrade?

Given these reasons why an SMB should implement new or upgraded forms of physical access control, now is the time to determine if your business should move to a more modern PACS approach.

To determine if your organization can benefit from a PACS upgrade, ask the following questions:

- Has it been more than six years since you last installed or upgraded your PACS system?
- Has ID and credential management become cumbersome for you or your IT team?
- Is there a benefit of expanding smart card capabilities to allow network access or incorporating mobile devices?

> “In most organizations there is a merging of IT security control and physical access control.”

- Does your company now house more or different types of sensitive data than when your initial PACS system was installed?
- Do you want to move to a PACS solution that uses a single device for various forms of entry?
- Would your company benefit by combining elements of IT access control and physical access control?
- Does your organization need to enhance security and beef up data protection to abide with new privacy and data safety standards and regulations?
- Do you need a solution that can be used on a variety of mobile devices?

If you answer yes to any of these questions, it might be time to move to a more modern PACS approach. What you need is a PACS that supports today’s mobile-first way of doing business.

Learn more about how to upgrade your access control system and why HID Global is trusted by millions of companies around the world to safeguard their facilities, assets, networks, and cloud resources by visiting: [*www.hidglobal.com/solutions/dynamic-access-control*]

You can also contact us directly for a personalized overview of how you can upgrade your PACS system. Simply contact us at insidesales@hidglobal.com