Three Essential Reasons to Upgrade Your Access Control Technology

A changing world calls for more secure, feature-rich access control technology

EBOOK

Introduction

The security landscape continues to evolve in new and complex ways, with security leaders under increasing pressure to meet a range of emerging requirements. But technology is changing too, and organizations today have an unprecedented opportunity to drive improvements in access control. Those who can seize this moment by embracing new technologies will be able to address escalating security threats while supporting the need to offer touchless experiences and derive greater value from their access control investments.

In addition to adopting updated standards in support of touchless and mobile implementations, access control overall is moving to more integrated systems with multi-layered security that can include multiple facilities. **These integrated solutions allow organizations to deliver new levels of convenience and enhanced flexibility going forward.**

With so many recent advances, there is no better time to upgrade from older, legacy technologies to new access control standards offering new capabilities. Organizations today can leverage solutions to move toward more dynamic access control technologies that provide greater value, offer enhanced functionality, and deliver a higher level of security.

Future-ready

Technology enhancements today put security in a future-ready posture, with the ability to support the requirements of today while also looking ahead to the needs of tomorrow.

In the immediate moment, adopting a new standard of access control can improve security and help to consolidate multiple locations under a single, secure technology standard. At the same time, moving to more advanced access control solutions will build a foundation for addressing unanticipated change and evolving security threats. Organizations thus can mitigate against both present and future risk by upgrading to a more modern solution.

New technology standards support a wide range of high-value applications from touchless mobile access and cashless vending to time and attendance, secure print management and network login.

Three Reasons to Upgrade

① Security & Data Privacy

Organizations increasingly are pivoting toward a Security First mentality, putting security at the center of every business decision.

In this regard, the industry is trending toward more secure access control technologies that simultaneously increase security, prioritize user experience, and increase efficient credential management. HID Global research found that in 2020, 58 percent of organizations had deployed at least one form of more secure credentialing technology, with mobile as the leading advanced credentialing solution.

While a majority of companies have deployed or plan to deploy new secure solutions, the work is not complete. Threats continue to evolve, and unprecedented events during the pandemic revealed new vulnerabilities. To achieve a Security First posture, organizations need to improve their secure access control infrastructure in order to add multi-application capabilities. They need to introduce easier-to-manage credential options, and more user-friendly technology, always with an eye toward ensuring those systems and people's personally identifiable information are secure.

SUPPORTING DATA PRIVACY

Modern solutions that ensure the security of personally identifiable information are both a good business practice, and safeguard compliance with emerging regulations.

HID's Seos® credential technology, for example, leverages widely reviewed open standards and best-in-class cryptography for unrivaled privacy protection. Supported by a software-based infrastructure, Seos secures trusted identities on any form factor, and can be extended for applications beyond physical access control. Organizations thus get the flexibility to support privacy across their unique mix of form factors and applications.

Seos uses a layered security approach that includes Secure Identity Object, or SIO® — a cryptographically protected data model for the storage of secure identity data. Defining characteristics include:

- Assigned unique digital identity information for the user
- Bound to the device cryptographically
- Signed at the time of creation and validated each time the credential is used
- Encrypted to prevent an unauthorized party from reading the embedded User ID

LEGACY CHALLENGES REMAIN

Within access control systems, security gaps are not always visible to the naked eye, and therefore they aren't often considered as the top priority. **Some hold the perspective that their current access control ecosystem is "good enough" because "we've not yet had a breach," yet there is a growing understanding of the significant security risks that an outdated access control system can bring.**

Continued use of magnetic stripe cards, barcode technology, and 125 kHz Prox cards expose organizations to the risk of credential spoofing and cloning, which has been demonstrated widely and is accessible for even the least sophisticated of bad actors to implement. Additionally, there are risks associated with reader to controller communication with the commonly used Wiegand protocol as compared to the more recent Open Supervised Device Protocol (OSDP) standard. While Wiegand leaves organizations vulnerable to man-in-the-middle attacks, OSDP is an evolving standard with AES-128 encryption and wire monitoring, making it a safer, more robust, future-proof option for governing physical access control communications.

INHERENT SECURITY

Modern access control solutions, especially mobile, are inherently more secure. When a card is lost, for example, delays in reporting the loss invite the possibility of misuse. With mobile credentials, on the other hand, it's far easier to mitigate risk since a lost mobile phone will be reported almost immediately.

Modernization also supports emerging data privacy requirements. HID Origo™, HID Global's physical access control cloud platform, for example, is ISO 27001 certified. A widely known and accepted international security standard, ISO 27001 serves as an information security management systems framework that specifies security best practices, establishes controls to manage risk, and protects data. Additionally, HID Global's Seos is the industry's first credential certified to the highest IT security level established by the independent testing service provider TÜV Informationstechnik GmbH.

Accredited certification provides independent, expert validation that HID maintains the confidentiality, integrity, and availability of customer data in accordance with international, industry-leading security practices.

By adapting to modern standards, security can meet legislative and regulatory calls for increased security. Modernization also means that organizations are well-situated to meet that call for improved access control.

② User Convenience

Users increasingly expect a high level of convenience in their access control experience. To achieve this end, mobile access is key — phones, tablets, watches, and other mobile devices offer choice and ease-of-use to end users, along with new and more convenient ways to open access points.

With mobile devices, which today are always on hand, users don't have to maintain and carry multiple cards or keys. **And the longer reach of the Bluetooth Smart communications standard, for example, makes it possible to communicate with readers from greater distances, supporting health and safety initiatives**. In addition, some smart device sensors enable gesture detection, offering the ability to unlock doors by performing intuitive gestures, providing both convenience and an extra layer of authentication through the mobile device.

Overall, it is predicted that there will be nearly 235 million smart wearable devices in use by 2024. With their ready-to-use convenience, these "always-on" devices are natural candidates for access control applications.

TOWARD TOUCHLESS

Touchless access controls came to the fore during the COVID-19 pandemic, as people sought to minimize interpersonal and surface contact. But security professionals see advantages of these solutions that extend beyond health and safety, especially in the promise of improved user convenience.

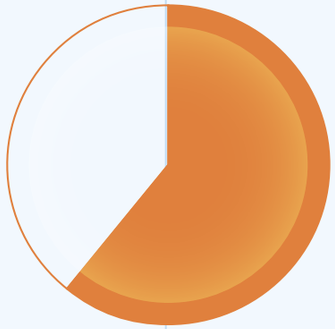
When HID asked about the top drivers to upgrade physical access control, touchless solutions topped the list, with 41 percent of security directors citing it as a major motivator. With heightened awareness around the health and security benefits of touchless technologies, security professionals increasingly recognize these as a key driver of user convenience going forward.

INTEGRATED SOLUTIONS

Security leaders also see a benefit to users in the integration of third-party building management and engagement applications. When integrated with building management apps and cloud-based access control management, mobile access delivers increased data capture, added convenience, advanced security, and flexibility.

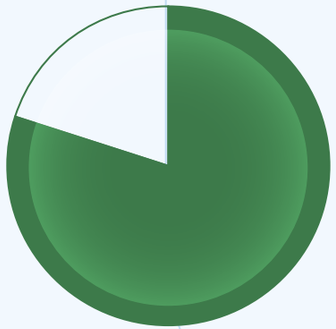
Building managers gain new opportunities to engage with tenants and gain the insight required to control core systems more efficiently like lighting and HVAC, while security professionals can easily provision and revoke credentials for staff, contractors, and visitors over the air, for a quick and convenient experience.

61%



61% of security professionals surveyed view contactless solutions as the future for the access control industry[1]

80%



80% of respondents still utilize a username and password to access network applications[2]

1. HID Global, The 2021 State of Physical Access Control Report
2. IDC, Worldwide Quarterly Wearable Device Tracker, September 2020

③ Flexibility

The ability to remotely issue and revoke credentials doesn't just support the end-user experience, it also drives added flexibility for security professionals as they seek to manage the evolving modern workplace, which may include remote and hybrid working arrangements. In this environment, security professionals can leverage the flexibility of remote credentialing to drive greater operational efficiency.

Security teams also gain added flexibility through the adoption of more modern reader technology, such as HID Signo™ Readers and a highly secure credential platforms like Seos. These solutions make it possible to easily adapt and expand physical access control systems as new technologies emerge.

FLEXIBLE BY DESIGN

HID Signo Readers are flexible by design, capable of interoperability with over 15 credential technologies, including Seos, HID Mobile Access®, MIFARE® DESFire® EV1/EV2/EV3, iCLASS®, and many more. This unparalleled credential support also extends beyond just today's technologies. A single HID Signo Reader is also capable of supporting legacy credential technologies including HID Proximity, Indala Proximity, AWID Proximity, and EM Proximity. Thus, this capability not only provides choice - it actually simplifies migration to modern credential technologies like HID Mobile Access, which supports over 250 mobile devices and IOS/Android capabilities.

Security teams in turn gain the added flexibility of managing firmware upgrades and servicing readers remotely, without having an engineer physically touch or even be on location at each reader.

A PLATFORM APPROACH

To drive business value, organizations need a platform that is flexible enough to support multiple applications for managing not only physical access (e.g. buildings) but also logical access (e.g. computer/software login, time and attendance, etc.).

Moments of change offer an opportunity to pivot in this direction. For example, an organization may want to add new integrations such as visitor management or location services, or applications like time and attendance, secure print management, biometrics, cashless vending and more. This is an opportune moment to migrate to a platform that supports smart card technology (Seos) and contactless wearable or smartphone solutions, combining access control with extended applications so that employees can carry a single card or device for many purposes.

A platform approach enables administration to be centralized into one efficient and cost-effective system. In this way, organizations can create a fully interoperable, multi-layered security solution across company networks, systems and facilities. Such a move positions security strategies for future success, enabling organizations to migrate to modern reader and credential technologies.

SECURITY, DATA PRIVACY, USER CONVENIENCE AND FLEXIBILITY GO HAND-IN-HAND

Organizations need modernized access control solutions to support simultaneous demands for greater security, data privacy, convenience, and flexibility.

With the pressure of constant refresh cycles and a growing “Bring Your Own Device” (BYOD) environment—along with increased network access via mobile devices—security must deliver a new and higher level of responsiveness. Modernization drives success.

BEYOND LEGACY SOLUTIONS

Legacy security solutions that use proprietary technology are often too static, providing little or no possibility for functional enhancement. Unable to adapt, organizations are easy targets for attack. Often, too, these legacy technologies are anchored to obsolete software, devices, protocols, and products, making it difficult to drive change in the access control infrastructure.

Modernization shifts the dynamic. Adopting interoperable technologies with the latest high frequency credentials and modern encryption standards ensures security is flexible and secure, making it much easier for organizations to support new functionality and higher levels of data privacy.

Such solutions enable the provisioning of secure identity credentials to smart devices, offering organizations the flexibility to use smart cards, mobile devices or both. And they deliver added business benefits, with functionality for access control beyond the door.

UPGRADING YOUR ACCESS CONTROL TECHNOLOGY: A SOLID INVESTMENT

Organizations that continue to invest in outdated technology will never be able to progress to best-in-class access control security and data privacy management, with all its convenience and functionality. By replacing older systems with the new technology standards, even gradually over time, security leaders can minimize the risk of a serious breach in the future. The best approach is to be proactive.

There are always reasons to avoid or delay change, including budget limitations and concerns about the impact of change on productivity and workflow. But delaying change can be especially dangerous in the access control infrastructure, where a combination of technology obsolescence and escalating security threats can cripple an organization's ability to protect its people, facilities, and data assets.

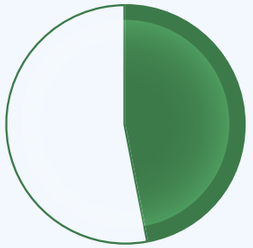
Access control solutions should enable organizations to easily adopt future capabilities without disrupting ongoing business operations. While investment is required for change, there is also positive return on that budget commitment, realized through improved security operations, more efficient workflows and/or reduced insurance premiums due to better risk management. Additionally, cost efficiencies can be realized by migrating from 125 kHz Prox cards to a highly secure credential technology like Seos, while also integrating HID Mobile Access, which offers better predictability of mobile ID licensing costs with subscription billing.

By taking steps to avoid a security event impacting the organization's workforce or customer data, security leaders can prevent costly long-term legal issues or brand impacts that may take years to overcome.

57%

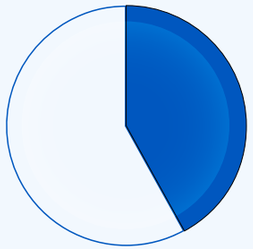
57% of respondents stated "return to work" protocols were the greatest challenge[1]

47%



47% stated "ease of use" as an important advantage required in a new system

42%



42% of installations are using insecure credentials, such as 125 kHz Prox, magnetic stripe and barcode

1. HID Global, The 2021 State of Physical Access Control Report

Conclusion

Too often, it takes an unexpected event or security breach to prompt an organization to upgrade their access control system. The time is now for security managers to take steps to move toward a more reliable, upgraded access control standard, enabling their organizations to meet the need for security and privacy with confidence, with an investment that will carry them well into the future.

Embracing the positive aspects of change requires an access control platform that meets today's requirements and is flexible enough to respond to future needs, all while meeting the highest levels of data privacy, user convenience, and flexibility. To that end, HID physical access control systems are difficult to compromise, but easy to implement: easy to install, use, manage and upgrade.

If you would like to find out how HID Global can help you upgrade your existing system, request a consultation from one of our Sales Advisors. Please visit our website, leave your details, and we will be in touch.

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-12-09-pacs-three-reasons-to-upgrade-eb-en
PLT-03113

Part of ASSA ABLOY