TechVision RESEARCH

Integration of IAM with Physical Access Control Systems

Published 10 March 2020

Abstract

Physical access control systems (PACS) are becoming more integrated with Logical Access Control Systems (LACS) via Identity and Access Management (IAM) deployments. This direction is further evidence of the trend towards expanding the breadth of IAM services under consistent governance and security models. There have been continued efforts by many vendors to converge these two environments in response to increasing compliance mandates, requirements to better manage alternative user populations such as on-premises visitors and contractors, and an acute emphasis on timely and secure access. In this sense, standard capabilities such as a common authenticator and automated integration with user provisioning are relatively mature. The goal of this integration is to have one service that choreographs access to both facilities and IT resources.

The purpose of this report is to dive into the concepts and conceptual architectures of converged Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS), referred to as PACS-LACS convergence. This insight addresses the typical enterprise objective to migrate their current set of multiple building/facilities access systems to a single PACS and LACS solution that is more secure, easier to maintain and able to be deployed across the entire organization. These solutions, which in many cases are becoming quite mature in the PACS market must also comprise a complete solution that includes video surveillance, high-availability, fault tolerance, and end-to-end administration and monitoring.

Author:

Doug Simmons
Principal Consulting Analyst
dsimmons@techvisionresearch.com

Table of Contents

Executive Summary

Physical access control systems (PACS) are becoming more integrated with Logical Access Control Systems (LACS) via identity and access management deployments. There have been continued efforts by many vendors to converge these two environments in response to increasing compliance mandates, requirements to better manage alternative user populations such as on-premises visitors and contractors, and an acute emphasis on timely and secure access.

In our recent research reports titled "Zero Passwords in a Zero Trust World" and "Multi-Factor Authentication (MFA): Enterprise Strategy and Market Assessment" TechVision Research discusses the need and opportunities to implement better forms of authentication – beyond the password, for accessing IT assets. In this report, we dive into what for many has been the 'holy grail' of authentication capabilities – the convergence of physical access control to buildings, facilities, rooms and so forth with the logical access to IT resources such as the enterprise network(s), applications and systems.

What we mean by converged is that a single medium, such as a form of token (something you have) can be combined with something you know (e.g., a PIN), something you are (e.g., facial recognition) and some form of contextual awareness (e.g., where are you located right now?) *to grant access to both facilities and IT resources* in accordance with an individual's existing affiliation with the enterprise.

Readers who are embracing the emerging Zero Trust security framework should therefore be heartened. Convergence of PACS and LACS instills harmony between the physical identities of the carbon-based world with the IT-centric, logical representation of everyone and everything in the emerging Digital Enterprise. Convergence done properly organically reduces the attack surface. Trust can be established or refuted with fewer lookups, decisions and margin for error.

This report will show you that there are presently a number of options for integrating or converging PACS with LACS. This has been an objective for many enterprises – large and small, over the past decade and more. While the U.S. federal government was able to enforce the deployment of PIV (personal identity verification) cards in the 2005-2010 timeframe for PACS-LACS (and the Department of Defense's Common Access Card (CAC) even before that), the rest of the business world has been watching and waiting for secure-but-economical migration options to emerge. That time appears to have come. The pervasiveness of smartphones, IP networks, cloud services and IAM maturity has brought to bear the opportunity enterprises can embrace.

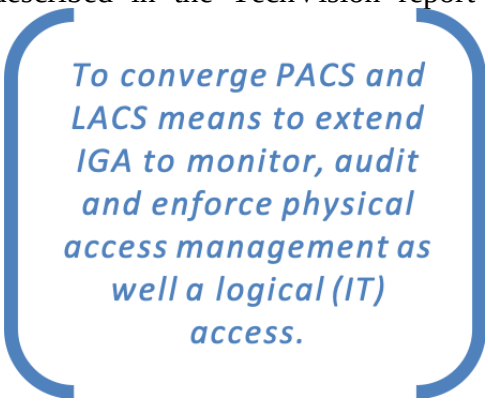
This report illustrates and explains the concepts and conceptual architectures of converged Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS), referred to as PACS-LACS convergence. This insight addresses the typical enterprise objective to migrate their current set of multiple building/facilities access systems to a single PACS and LACS solution that is more secure, easier to maintain and able to be deployed across the entire organization. These solutions, which in many cases are somewhat nascent in the PACS market must also comprise a complete solution that includes video surveillance, high-availability, fault tolerance, and end-to-end administration and monitoring.

From an administration standpoint, the primary integration required for realizing such convergence exists within the Identity and Access Management (IAM) and Identity Governance and Administration (IGA) pillars of the enterprise IT security program. Here is where the journey begins, as the fundamentals of converged PACS and LACS will logically center on these capabilities.

From an IAM point of view, the primary integration point is with the user and account provisioning subsystem. Provisioning (as well as de-provisioning) focuses on automating as much as possible the onboarding of new employees, contractors and possibly other constituencies (i.e., students, faculty, managed service suppliers and so forth). This automation is typically in the form of real-time connectors or agents that interface with authoritative source systems of identities, such as HR, Contractor Management and second-level authoritative sources such as Microsoft Active Directory, enterprise LDAP, Azure AD or other cloud-based identity repositories. We describe this level of automated integration in detail in our document titled "eBook: IAM Reference Architecture".

It is important to understand that PACS-LACS convergence does not focus only on the authenticator, which incorporates the common identity management processes that make the converged card possible. In reality, convergence is very conducive to contextual authorization – making decisions about application access based upon the user's location (either on-premise or off-premise) and security event correlation – the visibility into user activity from when they enter the facility to their subsequent activity in logical applications. Digging deeper, the runtime authorization capabilities of IAM environments are capable of taking contextual awareness into account when deciding (during runtime) whether to let someone or something 'in' via logical access control. These same runtime capabilities can be extended to physical access as well, so that 'time of day', 'last location and time of access' and information of this nature can be used to increase the granularity in runtime physical access control.

IGA is supported by the enhanced provisioning and de-provisioning capabilities as we combine logical and physical access systems. For example, as described in the TechVision report "Designing and Implementing Effective Enterprise Identity Governance and Administration Program" we state that the goal behind IGA is simple: Ensuring appropriate access, when and where it is needed. IGA combines entitlement discovery, decision-making processes, access review and certification with identity lifecycle and role management. IGA operates in the intersection of business process management and access automation allowing people and systems communicate with each other, fulfilling day-to-day operational needs. It focuses on the process and operational components of *identity* and *access management*. IGA is focused on addressing issues related to the mapping of business objectives to policies as well as creating a platform for the execution and administration of these policies. IGA is a bridge between



the business decision makers and those that administer the technology in support of managing all aspects of governing access. To converge PACS and LACS means to extend IGA to monitor, audit and enforce physical access management as well a logical (IT) access.

In this report, we are providing you with the preliminary tools to conduct an assessment of your own enterprise physical and logical security infrastructure and strategy. The desired outcome of this report is to help you develop a more thorough understanding of its infrastructure and process strengths, gaps, areas of concern, and existing "good practices" necessary to develop a realistic PACS-LACS convergence strategy. Therefore, in addition to sharing advancements in convergence technologies, we will help you examine how user identity lifecycles are managed; how information entitlements are assigned, monitored and revoked; and how user identities are audited – across both PACS and LACS environments.

Introduction and Background

Distilling a long market history, there are two main types of access control systems. The first is the traditional method where control panels act as hubs for door readers, door locks, cameras and the system's interface, usually a PC. These door readers and control panels connect with proprietary power and serial (e.g., RS-232) communication wiring.

Newer PACS systems are built on Internet Protocol (IP) networks, including cloud-based systems, in which the facilities access readers are connected the IP network through ethernet or wireless connectivity. Eliminating the need for control panels, IP-based PACS are therefore often less complicated and easier to install via standard IP network hubs.

IP systems have gained popularity as cloud storage becomes more pervasive and they are much simpler to set up - usually with simply an ethernet connections to the enterprise network instead of serial connections to multiple control panels. There is no limit to how many door readers can connect to an IP system, while in a traditional system, control panels can only be connected to a handful of doors. From a scalability and integration standpoint, IP-based PACS are much more economical.

Convergence projects like we are discussing here often require the upgrading of PACS to be able to reduce the number of card authentication techniques or update the PACS to support a specific smart card type (e.g., for the HSPD-12 PIV card in widespread use across the U.S. federal government). Understand that PACS rely upon readers and controllers that in many cases support thousands of doors in the environment and often use proprietary wiring schemes, such as the Weigand interface (developed in the 1970s). While the upgrade of these PACS components can often be a multi-year project for many large organizations, they can today leverage multi-protocol readers, controllers, and cards to ease some of this transition and buy additional time to facilitate the upgrade. However, it bears mentioning that the PACS wiring scheme may need to be converted to an IP-based network and this can increase the cost – sometimes substantially.

It is important to understand that the stability and security of the enterprise IP network is a critical factor when determining whether an enterprise should replace hardwired serial PACS with more

modern IP-based componentry. Just as hackers can wreak havoc on enterprise IT systems protected by LACS, PACS can be just as hackable once they are connected to an IP network. Note that details about overall network security is covered in several dedicated TechVision Research reports, so in discussing PACS-LACS convergence simply understand that IP network security principles apply.

Physical and Logical Access Convergence

For well over the past decade, the use of a common authenticator has been possible through a 'converged access card'. Typically, these access cards have been ID badges combined with traditional PKI-based smart cards. In this way, converged smart cards enable people to access resources protected by physical access control systems (PACS), as well as traditional applications that can leverage X.509 PKI authentication. In addition, the ISO 7816 (credit card sized) badge provides an area to print visual identification and even human readable authentication information. In this way, the user can be visually authenticated by the physical security staff. Combined with the embedded chip, the converged smart card also provides stronger authentication for logical applications. Therefore, the converged badge has two interfaces: the contactless interface that enables authentication to the physical perimeter, and the chip-based contact interface that enables multi-factor authentication to the IT devices, network and applications.

Some of the major changes since this early convergence includes:

- The emergence of the smartphone as a viable token for identification and authentication for both physical and logical security.
- The continued pervasiveness of IP networks as the global communications infrastructure.
- The embracement of cloud-first strategies that compel enterprises to migrate away from on-premise technologies to cloud-centric approaches.

With this as a backdrop, we can now start to drill into the current state of PACS-LACS convergence and share with you the significant advancements that may compel you to begin a long-awaited PACS-LACS convergence program.

Typical Architecture

We'll start with the basic/traditional architecture for PACS and then explore some new architectural approaches for both PACS and the ultimate convergence of the physical and logical access control systems. Components of a typical physical access control system include:

- An access control panel (also known as a controller)
- An access-controlled entry, such as a door, parking gate or other physical barrier
- A reader installed near the entry. (In cases where the exit is also controlled, a second reader is used on the opposite side of the entry.)
- Locking hardware, such as electric door strikes and electromagnetic locks
- A magnetic door switch for monitoring door position
- Request-to-exit (REX) devices for allowing egress.

A high-level look at such and architecture is illustrated below.

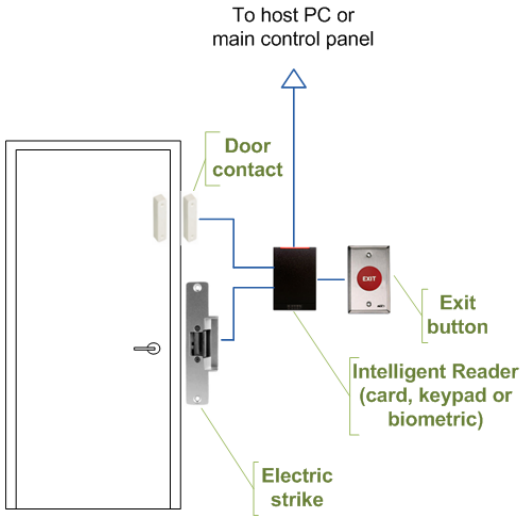


Figure 1: Traditional PACS Architecture

Access control decisions are made by comparing the person's credentials to an access control list. This look-up can be done by a host or server, by an access control panel, or by a reader. While 'legacy' PACS typically conduct the user lookup on a central server, more current systems push the look up to the edge of the system, or the reader instead. The predominant topology for the past decade or so has been 'hub and spoke' with a control panel as the hub, and the readers as the spokes. But things are changing as we'll describe during much of the remainder of the report.

Game Changer: The Smartphone

Today, a growing number of PACS vendors support the use of a smartphone to perform most functions a Physical Access Control System (PACS) can provide, including:

- Badge verification
- Entry/Exit tracking
- Remote opening of doors
- Visitor management

What this provides is support for the use of an application on an NFC or Bluetooth Low Energy (BLE) enabled smartphone to open a door. For most physical access, employees open doors using their badge (RFID, magstripe or other technology), PIN, and/or biometric credential. This advancement in 'token' technology recognizes the pervasiveness of smartphones today, and the PACS industry identified smartphones as a legitimate new medium to store credentials. Without question, this sea change is aided by Apple iOS and Google Android both embracing Bluetooth NFC.

The use of the cell phone to open a door or gate provides some significant advantages, such as:

1. Bluetooth range can be several feet instead of inches.
2. People often have their cell phones in their hands, which is convenient at doors.
3. It does not require another device.

Of additional value of course is that the smartphone can also be used for logical access within the enterprise's multi-factor authentication strategy. In plain sight, this is the convergence we've been looking for. While smart cards embedded in physical access badges have been around for many years – and certainly in widespread use across government agencies, such technology was difficult, cumbersome, complex and expensive for many organizations to deploy effectively, especially globally.

However, as you might expect there are still some challenges for mobile phones within PACS technology. For example, one's cellphone does not work with a dead battery. Furthermore, the PACS market is rather fragmented, with each vendor maintaining their own competing, proprietary infrastructures that require replacement of all the readers at points of access. Mobile credentials also have a significant learning curve and management overhead. Lastly, these credentials are subject to different attack vectors than security personnel see with physical credentials.

All that being said, smartphones are still the 'wave of the future' for PACS (a future that started a few years ago) and in TechVision's opinion they provide the link that brings converged PACS/LACS into a practical reality.

Smartphones are still the 'wave of the future' for PACS (a future that started a few years ago) and in TechVision's opinion they provide the link that brings converged PACS/LACS into a practical reality.

Cloud Based PACS

In addition to locally hosted access control systems - where the server is on-premise in the data center, cloud-based solutions are emerging rapidly. In cloud-based PACS, access permissions are not stored on a local server, but in the cloud. This means that the administrator can manage the permissions from multiple locations by using a (TLS-enabled, secure) browser. This appeals to security managers charged with overseeing multi-location facilities for one, and of even more importance, it radically changes how quickly PACS servers can be deployed across the globe.

As an example, Lenel's OnGuard platform can be optionally configured and tuned to allow PACS server deployment across Amazon Web Services (AWS) cloud infrastructure. For some, this may be of significant value, especially if the enterprise has been waiting for years to upgrade their PACS infrastructure and have dreaded the amount of time, effort and cost it would take to accomplish.

In summary, modern, converged PACS-LACS environments are shaping up like the high-level architecture illustrated below.

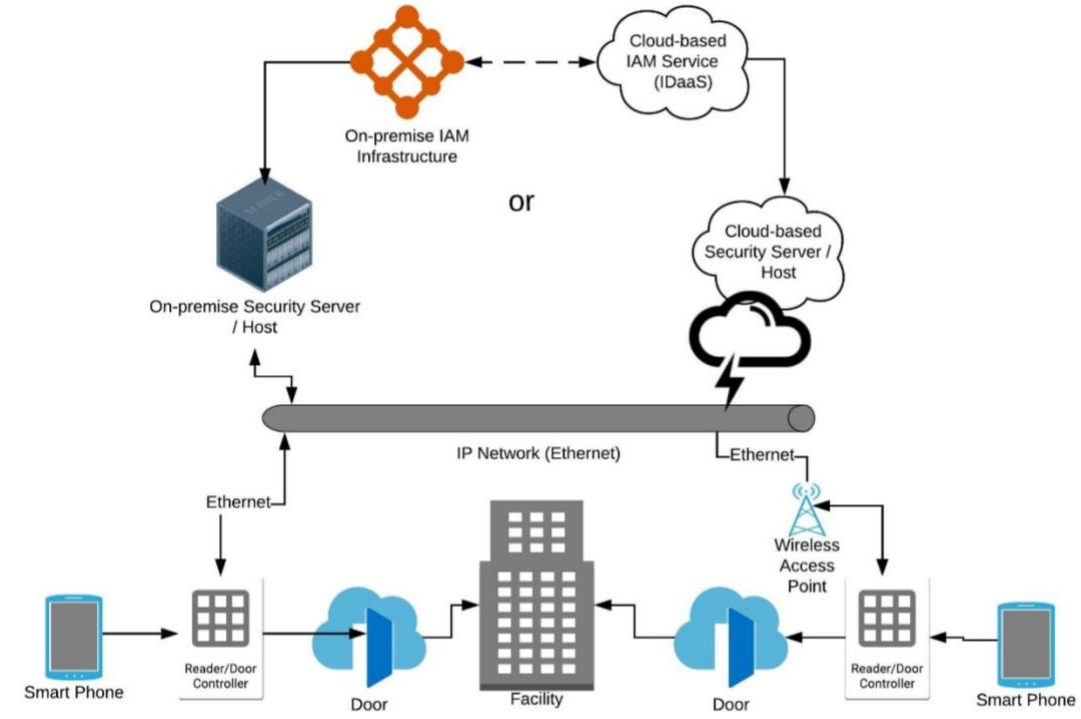


Figure 2: Modern Converged PACS-LACS

Standards

For interfacing with readers, there are many defacto standard card technologies including magnetic stripe, bar code, Wiegand (Wiegand wire is attracted to magnets), 125 kHz proximity, 26-bit card-swipe, contact smart cards, and contactless smart cards. Also available are key fobs, which are more compact than ID cards, and attach to a key ring. Biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry. The built-in biometric technologies found on most smartphones can also be used as credentials in conjunction with access software running on mobile devices. And, as we have said, newer technologies such NFC and Bluetooth can also communicate user credentials to readers for system or building access.

OSDP

The Open Supervised Device Protocol (OSDP) has emerged as a legitimate access control communications standard in the PACS space. It was developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP v2.1.7 is currently in-process to become a standard recognized by the American National Standards Institute (ANSI), and OSDP is regularly reviewed an updated to retain its industry-relevant positioning.

This standard is in wide use by many leading manufacturers like Cypress, HID Global, Mercury and others and the Security Industry Association encourages broad adoption of OSDP and recommends specifying this standard for any access control installations with security requirements. It is particularly valuable for government applications because OSDP meets federal access control requirements like PKI for FICAM (Federal Identity Credentialing and Access Management). Compared to common low-security legacy protocols, the emerging OSDP standard offers:

- Better security than the most common (defacto) access control communications protocols.
- OSDP Secure Channel supports high-end AES-128 encryption (required in federal government applications).
- OSDP monitoring of wiring to mitigate attacks.
- Supports advance smartcard technology applications, including PKI/FICAM and biometrics.
- Supports bi-directional communications among devices.
- OSDP supports a more advanced user interface (than earlier approaches), including welcome messages and text prompts.
- OSDP's use of 2 wires vs. 12+ allows for multi-drop installation, supervised connections to indicate reader malfunctions, and scalability to connect more field devices.
- Audio-visual user feedback mechanisms provide a rich, user-centric access control environment.
- Predefined encryption.
- Multi-vendor communication if all parties are using OSDP.
- The standard applies to peripheral devices (PDs) such as card readers and other devices at secured access doors/gates and their control panels (CPs).
- The OSDP specification is currently recommended when TCP/IP, USB, or other common protocols do not lend themselves to the application.
- The OSDP specification is extensible to IP environments and the OSDP WG is working on deploying OSDP over IP soon.

OATH

Authentication standards are emerging and should be considered as a starting point for an enterprise converged PACS-LACS program. For instance, the Initiative for Open Authentication (OATH) addresses authentication integration challenges with standard, open technology that is freely available to application developers. OATH is a collaborative effort and seeks to provide a reference architecture for universal strong authentication across users, devices and networks. Through an open standard, OATH describes itself as offering more hardware choices, lower cost of ownership, and allow customers to replace existing disparate and proprietary authentication systems whose complexity often leads to higher costs. OATH's framework components are

designed to be interoperable by enabling integration with existing identity and access management platforms and infrastructure (e.g. LDAP directories, web access management and single sign-on servers).

The OATH standard, at a basic level, describes implementation of a core set of authentication credentials. These credentials are:

- One Time Password (OTP) - based authentication
- Public key infrastructure (PKI) - based authentication (using X509.v3 certificate)
- Subscriber identity module (SIM) - based authentication (using GSM/GPRS SIM)

The OATH standard has been ratified in a series of IETF RFCs. Because OATH-based solutions can be compatible, migration between products is intended to become simpler and can leverage a much larger range of devices for OTP generation, such as YubiKey, and even sharing of hardware tokens between vendors. An important architecture goal for universal authentication is to enforce the separation between validation and identity stores. OATH recommends that all identities (user or device identities, as well as device-to-user bindings) be maintained outside the validation server. This separation is important from an integration and cost-control standpoint because it promotes a distributed architecture that favors the reuse of an enterprise's existing infrastructure (e.g., corporate directories). In such architectures, the validation server is a minimal front end. OATH assumes that LDAP (including Active Directory and Azure Active Directory) is used to enable the validation server and the directory to exchange information. The OATH standard is currently being contributed to by a large number of vendors, including Gemalto, HID, Symantec, VASCO, Yubico and many others (please see https://openauthentication.org/members/), and is supported by a number of MFA vendors (discussed in further detail later in this document).

An important architecture goal for universal authentication is to enforce the separation between validation and identity stores.

FIDO

Another important standard in the identification and authentication arena has been developed and promulgated by the FIDO (Fast Identity Online) Alliance, an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices (PayPal and Lenovo were among the founders).

FIDO's aim is to support a full range of authentication technologies, including biometrics, Trusted Platform Modules (TPM), USB security tokens, smart cards, and near field communication (NFC). FIDO specifications provide two categories of user experiences, depending on whether the user interacts with the Universal Second Factor protocol or the Universal Authentication Framework protocol. Both of these FIDO standards define a common interface at the client for the local

authentication method that the user deploys. The client can be pre–installed on the operating system or web browser.

FIDO members total more than 260, including a Board made up of Aetna, Amazon, American Express, Bank of America, Gemalto, Google, Intel, Lenovo, MasterCard, Microsoft, NTT DoCoMo, PayPal, Qualcomm, RSA, Samsung Electronics, USAA, Visa, VMware, Yubico and many others.

Looking to the Future

We have seen over the past 2-3 years a tipping point where the use of mobile credentials with access control systems becoming commonplace. While we anticipated this shift for years, the widespread adoption of mobile phones for more varied uses is now becoming the norm. An example of such usage is Apple's launching of contactless student IDs to over 100,000 students across the United States.

Because the use of mobile and other contactless credentials has proven successful, end users – whether employees, contractors or consumers are becoming more comfortable with the idea (of smartphone-based credentials) and more willing to use these credentials at work and home.

Access control is more sophisticated than ever as we see existing technologies like artificial intelligence acquiring increased capabilities, and technologies like biometrics, becoming more mainstream and accessible to organizations of all shapes, sizes and geographies.

AI is already supporting access control systems by detecting unusual or suspicious activity and sending alerts, recognizing faces, and gathering and analyzing pertinent data. TechVision Research expects advances in AI to continue to identify vulnerabilities, actively monitor facilities and perimeters, diagnose problems, and protect data. As we see growth in the convergence between physical and logical access controls, AI may also be used to alert human employees to security issues in real time, allowing faster responses.

Advances in the integration between PACS and IAM subsystems, such as automated user and device provisioning, workflow approvals and identity governance and administration (IGA) will continue. As PACS vendors continue to move their capabilities to the cloud, leverage mobile phones/devices and so forth, IAM vendors are adding service connectors between the provisioning and access logic from authoritative identity sources such as Active Directory, Azure AD, LDAP and so forth.

For example, Openpath (https://www.openpath.com/solutions/enterprise) is a physical access control vendor that provides administrators with cloud-based access to monitor and manage their environments, and end users with low friction access through e mobile credentials (as well as supporting traditional smart-card-based credentials). The four-year-old CA-based company has connectivity with AD/Azure AD, Okta, Google G-Suite, O-365 and Okta. Openpath can synchronize end users from Okta into Openpath while optionally auto-assigning them access credentials and permissions - and can also authenticate into the Openpath Control Center using

SAML single sign-on from Okta. This is an example of how PACS can be integrated with the enterprise IAM infrastructure.

On the device reader side, ultra-wideband (UWB), is a new wireless, short-range communication protocol that allows devices to "talk" to each other. UWB is expected to be utilized in access control systems by allowing hands-free access to entry and exit points.

What we are seeing is a shift in access control from being strictly a security function to having a more comprehensive, user experience-based focus. These new offerings support not only the workplace, but any environment requiring access security. The key to more ubiquitous offerings lies in the convergence of the logical and physical access approaches and the integration into mainstream IAM services.

What we are seeing is a shift in access control from being strictly a security function to having a more comprehensive, user experience-based focus.

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skillsets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for 10 years and security, and identity management consulting at Gartner for 5 years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.