The benefits of truly integrated access controls

Whitepaper

Avoid the pitfalls of typical physical access control systems

Why is physical access control important?

Cyber security

PREVENTING DATA BREACHES

It is well understood that data security is of critical importance to protecting your organisation's reputation and your customer's information, but the risk keeps escalating:

→ The number and cost of security beaches continues to rise year over year. The average cost of 'worst single breaches suffered in a year' has risen sharply to between £1.5m and £3m for large organisations, with the number of breaches up by 80%.[1]

For small businesses the typical costs range up to £300k and the number of breaches has increased by 60% in a year.[1]

INSIDER THREAT IS THE BIGGEST CHALLENGE

It's vital to be aware that it's not just the external threat from hackers that has to be tackled:

→ A recent survey of information security professionals, from across Europe, highlighted 'insider threat' (encompassing accidental and malicious acts) as the biggest unresolved information security challenge.[2]

Additional safeguards to IT system access, such as location based log-on, can be enabled by using real-time knowledge of each user's location from their physical access control system interactions; thereby prevent access to some IT resources unless the user in known to be on-site or within a secure area.

→ 36% of desk-based workers in the UK and US are aware of having continued access to a former employer's systems or data"[3]

Procedures for on-boarding and off-boarding staff and contractors need to manage both logical IT data access control and physical access in a unified and consistent way, in order to ensure there are no security gaps between the physical and logical domains.

THE PHYSICAL COMPONENT OF AN ATTACK VECTOR

The first stage in a cyber-attack can depend on gaining physical access:

→ Attacks on bank branches in the UK required criminals to gain entry, by posing as IT staff, in order to install a KVM with 3G dongle on a branch computer terminal.[4]

Secure access-card based entry systems can validate authorised physical access across multiple sites, preventing entry by external individuals and logging the access of staff members.

Why is physical access control important?

Compliance

RESPONSIBILITY AND RISK

Physical data security risks:

→ Physical loss and theft, of records and media, accounts for as many data breaches as hacking.[5]

There are substantial financial penalties for failing to comply with directives and new regulations are being imposed

→ General Data Protection Regulation (GDPR) – New, harmonised, EU Data Protection & Privacy Law:

Replacing European Data Protection Directive 95/46/EC. As a regulation the GDPR will be directly applicable to all EU member states without need for national legislation. It requires prompt compulsory notification of breaches and imposes large financial penalties for non-compliance.

Personal data is to be protected against accidental or malicious actions that could lead to unauthorised disclosure, dissemination or access; with the expectation that solutions implemented provide data protection by default.

REGULATIONS REQUIRING PHYSICAL ACCESS CONTROL

Control over who can enter sites, restricted areas and open server cabinets is a significant component in ensuring data security:

→ PCI-DSS - Payment Card Industry Data Security Standard:

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted.

→ FISMA – US Federal Information Security Management Act:

Organizations must limit physical access to information systems, equipment and the respective operating environments to authorized individuals.

→ Sarbanes-Oxley Act of 2002 – Applicable to U.S. public enterprises:

Physical access to IT infrastructure systems supporting financial reporting should be restricted to authorized personnel only, and that access should be monitored and reviewed on a periodic basis.

→ HIPAA - Health Insurance Portability and Accountability Act passed by US Congress 1996:

Physical measures, policies and procedures must protect a covered entities electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Why is physical access control important?

Best practice

STANDARDS REQUIRING PHYSICAL ACCESS CONTROL

→ ISO 27001 - International standard for information security management system (ISMS) best practice, and ISO/IEC 27002 code of guidelines:

Defined physical perimeters and barriers, with physical entry controls and working procedures, should protect the premises, offices, rooms, delivery/loading areas etc. against unauthorized access. ICT equipment, plus supporting utilities (such as power and air conditioning) should be secured.

→ SSAE 16 and ISAE 3402 - Professional standards for Service Organization Controls (SOC) for financial information:

Logical and physical access controls – processes must manage how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access.

→ ANSI/TIA-942- Data centre infrastructure standard covers many design aspects including physical security

Best practice data centres employ a layered approach to physical access control; starting at the perimeter, segregating access rights between higher and lower security areas within the site and providing time-limited access rights to individual server racks where appropriate. Recommended implementations of these layers incorporate anti-tailgating and anti-passback measures, multi-factor identity authentication and video surveillance.

Access controls for data centres need to allow for the inevitable visits of technicians to maintain equipment, their access needs to be limited to only the appropriate areas and server racks. Access card controlled locks on doors and cabinets provide the flexibility to manage who has access to what and when.

SOURCES

[1]*2015 Information security breaches survey commissioned by the UK Government's Department for Business, Innovation and Skills*

[2]*Infosecurity Europe 2015 attendee feedback: What is the biggest unresolved information security challenge? #1 Insider threat 42%*

[3]*Infosecurity-magazine.com July, 2014*

[4]*The Register 'Bogus IT guys' slurp £1.3m from Barclays' September 2013*

[5]*Information Security and Data Breach Report October 2014 Update*

Typical access control systems

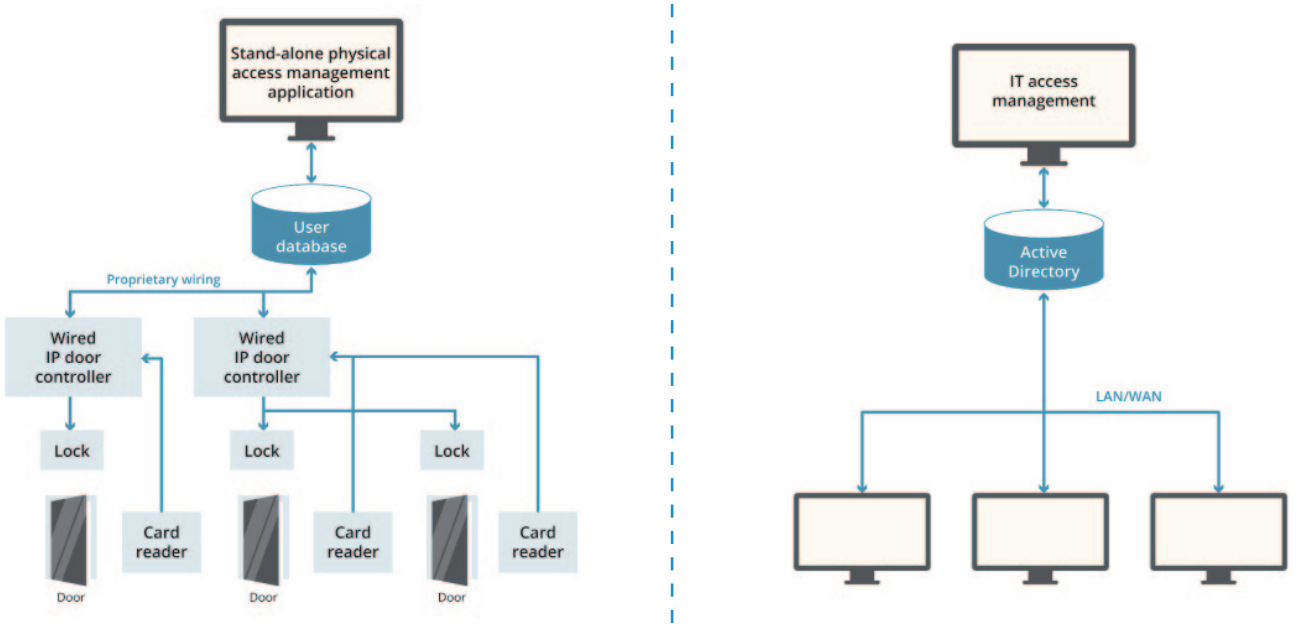
SEPARATE PHYSICAL AND LOGICAL ACCESS CONTROLS

Traditional mechanical locks simply cannot provide scalable solutions that can cost-effectively deal with lost or stolen keys, nor can they provide the flexibility to control where and when people have access, in addition to who has access.

Biometric scanners can be used, although implementations have notoriously been problematic, and new mobile-based keys are becoming available, but, most commonly, RFID cards are used for physical access control. The spectrum of RFID-based technologies used for ID-cards range from basic 'prox' cards to secure encrypted memory cards and on to high-end multi-application and hybrid PKI smartcards, also used for secure PC logon.

The typical access control system is made up of five main components: user ID cards or tags, matching card readers, door locking devices which are driven by door controllers, plus a user access management database application which is separate to the IT-user administration database.

Separate physical (door) & logical (IT) access control systems



Each user of the system is provided with an access card (or tag). The card, which is typically programmed with a unique readable ID at time of manufacture, is normally issued to them when they join the company. The administrator of the access management system will at this point create a new database entry for the user, assign their card number, and then configure the various access rights for that user (i.e. which doors they are entitled to use). At some point after this, usually on a regular schedule, the access management system will upload this information to the door controllers for each of the doors to which the user is allowed access. Traditionally this was performed over serial comms links, although TCP/IP is taking over for uploads on newer systems.

Typical access control systems

When a user approaches a door, they present their card to the card-reader. The reader extracts the ID from the user's card and passes this to the door controller. If the controller recognises the ID it will release the door lock. Log information may later be sent back from the controller to the software, for reporting purposes.

An installation can be more complex than the basic system described above, for example some doors have a card-reader on both sides, and door controllers may have additional logic and sensors to provide alarms or prevent cards being used by multiple people (anti-passback). However, in most cases, all of these additional controls are managed autonomously by the door controller.

DRAWBACKS & WEAKNESSES

This traditional approach has a number of drawbacks and weaknesses. Firstly, the access management software is often installed on an isolated computer or, even if networked, as a stand-alone application. All user data and access rights have to be entered when a new user joins the organisation. When a user's rights change or they leave the organisation, the user database will need to be updated. For a large organisation the initial input of all users into the system can be a significant overhead, as can the ongoing data management.

Larger systems can be connected to other company databases (for example HR systems) using various data export/import and synchronisation techniques. These 'pseudo-integration' approaches tend to be complex, incur significant expense and generate additional points of failure as well as delays. Similarly, the ability to operate across multiple sites usually requires additional software, comms links and data synchronisation processes.

The second major drawback is that door controllers typically operate "off line", that is, they are updated with a list of newly authorised or deactivated users only periodically by the access management application, and make all of their actual door access decisions locally, based on the last list they received. This can mean there is a time lag before any user privilege changes are applied at the door. Also, they cannot take any other information into account, or immediately update other access rights (such as to IT resources) because there is no real-time, combined view of user location (physical) and IT-resource (logical) status.

The benefits of truly integrated physical & logical access control

ENHANCED SECURITY WITHOUT COMPLEXITY

User access to logical IT-resources is typically manged through well-established tools, like Microsoft Active Directory, which support sophisticated and scalable role-based security models. By directly integrating physical access control into an organisation's IT systems, the same logical controls can be extended to physical door access to ensure security by default. Additionally, real-time combined physical and logical access control decision-making can be enabled without complexity. The major benefits of this approach include:

(1) Enhanced security and compliance

→ It avoids security risks from synchronisation gaps or lags between separate physical and logical access control systems.

→ It enables physical location information to be used intelligently and in real-time for controlling access to IT resources. This can be used to limit the access of restricted financial or medical information to secure areas

→ It enables comprehensive audit trail reporting; detailing physical user location at the time of logical system access. This can be used to validate the application of specific regional tax regimes for financial transactions

(2) Simplified management and administration

→ It reduces the administrative overhead of managing totally separate databases for logical and physical access systems

→ It leverages the existing user database's back-up and disaster recovery provision

→ It provides physical access control management across multiple sites seamlessly

→ It brings physical access in-line with IT access controls and enables role-based management across the entire organisation

→ It allows existing and familiar IT access management tools to be used for physical access control

(3) Easier installation

→ It leverages the user information already held in Active Directory, including user-groups & roles, avoiding the need to populate user information in a separate database

→ It automatically extends the reach of physical access control to any site – worldwide - covered by the organizations WAN, without need for site-specific databases and site-to-site synchronisation infrastructure

→ It can use TCP/IP standards to make use of the existing network cabling infrastructure and avoid separate power supply cabling through the use of Power over Ethernet (PoE)

The benefits of truly integrated physical & logical access control

Security & cost benefits summary

	Truly Integrated Solution Real-time unified physical and logical access control	Typical Access Control Separate physical and logical access control systems
Enhanced security and compliance	No delays in adding & removing both physical and logical access permissions	Separate updates or scheduled synchronisations create risk when revoking rights & hamper productivity when granting new permissions
	Supports compliance needs (such as PCI-DSS) to restrict sensitive data access to secure locations Comprehensive real-time alert generation and audit trail reporting Avoidance of 'passback'* and 'tailgating'†	No centralised knowledge of user location and IT resource access, in real-time, fundamentally limits any converged access control capability
Simplified management and administration	No duplication of effort to maintain user information. Able to utilise existing security groups & defined roles consistently	Isolated systems require duplication of user information and maintenance. Pseudo-integrated systems require synchronisations to be managed, adding complexity & increasing points of possible failure
	Leverages Active Directory's multi- server, redundancy and disaster recovery features	Additional databases need extra back-up & management provision
	Unlimited numbers of users and sites worldwide	Increases to numbers of users & sites can require additional software licensing &/or installation of replacement door controllers
Easier installation	Utilise existing MS Active Directory or other LDAP database	Additional database has to be installed, populated and maintained
	Leverage standard network data cabling and Power over Ethernet	Proprietary and complex wiring systems may be required
	Covers all sites on the WAN wherever they are located	Complex site-to-site synchronisation systems need to be added for multi-site operation

** 'passback': an authorised person loans their ID-card to another person to gain access*
†'tailgating': someone follows an authorised person through a door without presenting an ID-card

True integration with EdgeConnector

UNIFIED ACCESS CONTROL WITH ACTIVE DIRECTORY

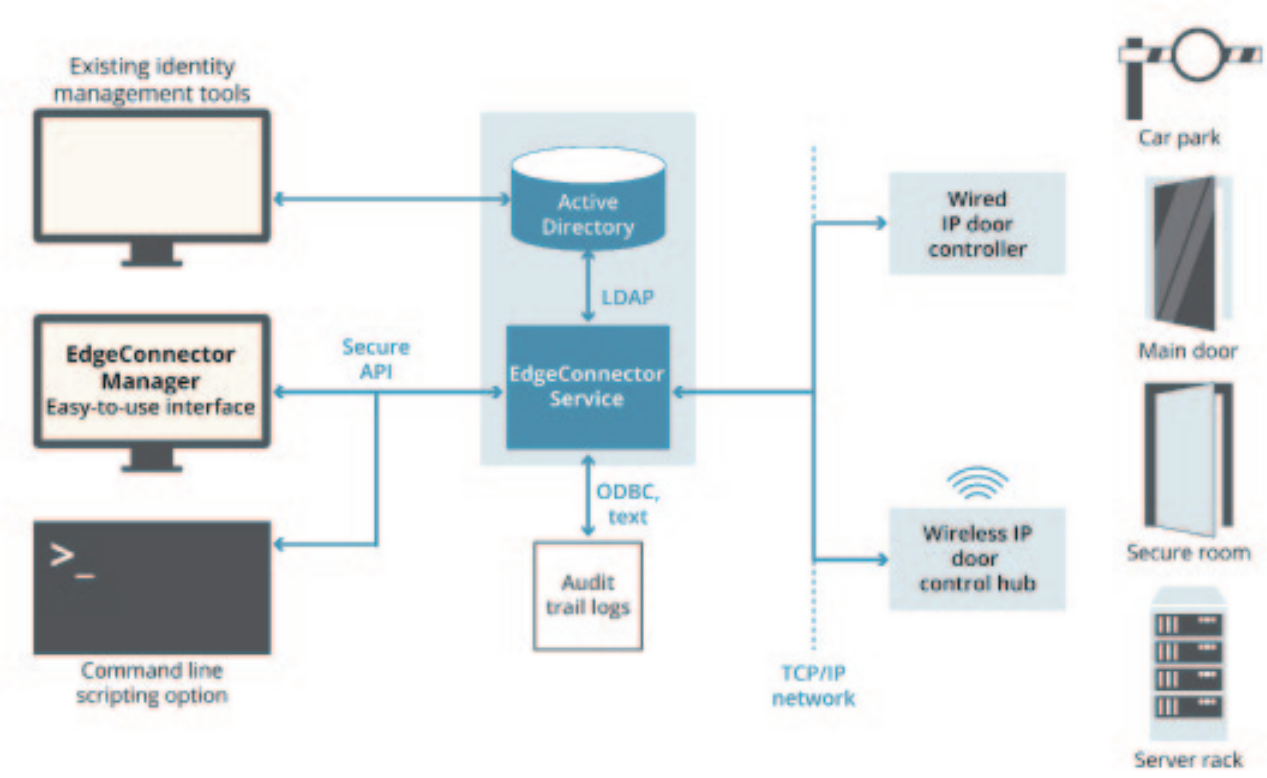
EdgeConnector integrates physical access control in to an organisation's existing Active Directory (or alternative LDAP database). The required user information is already stored in this database and can be used without re-entry or duplication. All door access decisions are made by a centralised Windows Server component, called the EdgeConnector Service, which connects to Active Directory. This has two major advantages:

(1) Access decisions are based on the most recent changes to unified physical and logical access privileges – updated in real-time.

(2) Each user's profile is updated to record their current location based on their physical access control interactions. Users' security group membership may also be changed dynamically, to manage their IT access permissions based on user location.

These features open up a number of different converged access management capabilities, making EdgeConnector far more versatile than other systems. EdgeConnector also benefits from the inherent flexibility of Active Directory when it comes to multiple sites, servers, redundancy and disaster recovery, as well as the ability to run in the cloud if desired.

The EdgeConnector solution architecture



True integration with EdgeConnector

REAL-TIME CENTRALISED DECISION MAKING

From a hardware perspective EdgeConnector is similar to traditional systems, however there are two important features that provide greater power and flexibility:

→ Unlike traditional door controllers that make access decisions locally off-line, when EdgeConnector controllers receive card IDs from readers at the door, they pass these over the network to the EdgeConnector Service. This service validates the user's rights and instructs the local control hardware whether or not to allow access and operate the door.

This centralised real-time processing brings all the benefits of true integration; enabling combined physical and logical access control without complexity.

Any number and combination of wired controllers and wireless control hubs can be manged by the EdgeConnector Service, allowing physical access controls to easily be extended across server cabinets, secure rooms, perimeter entrances and multiple sites worldwide.

→ EdgeConnector is an open, standards based, platform. This allows a wide variety of card technologies and supporting readers to be incorporated, providing a greater choice of cards from different manufacturers and avoiding the potentially significant economic impact of 'card lock-in'.

Additionally, the flexibility to handle multiple card technologies in parallel facilitates the gradual migration from a basic 'prox' technology to more secure standards (which in-turn may be used to integrate other card applications, such as Windows log-on authentication).

EdgeConnector's extensive hardware compatibility makes it easy to run alongside less-flexible legacy systems, providing greater control for a specific location, and can subsequently be extended to replace the entire legacy system in phases.

In addition to the EdgeConnector Service, which can manage door access to any number of doors, geographically located anywhere on the WAN, a secure delegated management console is included. The EdgeConnector Manager client provides an easy-to-use interface for day-to-day management of users, visitors, doors and schedules by non-IT staff, without compromising directory security. Alternatively, other Identity Management applications that integrate with Active Directory can be used for day-to-day management tasks.

EdgeConnector's proven track record

EdgeConnector access control systems manage physical access for many hundreds of thousands of users daily, across North America and Europe. Since its launch in 2008 EdgeConnector has been installed in leading large and medium enterprises; central and regional government departments; universities; police and national health services. In addition, EdgeConnector is used by major companies within the financial sector to meet compliance needs.

Edge Connector is a product of Dot Origin – a leading technology solutions provider specialising in two-factor authentication, public-key cryptography and data encryption. Dot Origin has operated for over 16 years and built up an extensive role of respected customers, as well as establishing partnerships with industry leading vendors (such as ACS, Assa Abloy, Gemalto, HID, Identive and NXP).

www.edgeconnector.com

info@edgeconnector.com

Europe & Asia

+44 (0)1428 685 861

Northern & Latin America

Toll Free: (888) 262-9642 Direct: (562) 262-9642

Dot Origin Ltd.

Coopers Place

Combe Lane

Godalming

Surrey

GU8 5SZ

United Kingdom