5 reasons for IT to get physical with Access Control

White Paper

AVIGILON

A guide to choosing an IT and user-friendly building security system

Network security and building security are equally important. If either system is compromised, the organization is immediately at risk. But while many network security systems are now built to support IT best practices and standards, such as, virtualization, physical access control systems (PACS) have traditionally been designed without IT professionals in mind.

Not only are these legacy systems more difficult for IT departments to deploy, support and maintain, they are also more cumbersome for physical security and facility operations colleagues to manage on a day-to-day basis, often requiring expensive, stand-alone Windows servers, individually licensed software and proprietary door hardware, while only being accessible from a few, isolated office computers.

Fortunately, these limitations are finally changing, as a new breed of affordable, web-based physical access control systems provide several key advantages over traditional PACS. While there are many factors to consider, five of the most important attributes of an IT- and user-friendly physical access control system include platform reliability, system security, mobile access, ease of use and non-proprietary door hardware.

This guide has been written to help IT professionals evaluate the effectiveness of their existing building security system and work with their physical security counterparts to find a physical access control system that meets their organization's overall security, IT and budgetary needs.

5 Reasons for physical security to go virtual

1 Eliminate the cost of stand-alone servers

2 Manage building security in a private cloud

3 Leverage virtual server infrastructure

4 Minimize downtime, maximize reliability

5 Reduce setup and deployment time

1. Reliability

Making sure a door opens or closes in real-time when it is supposed to might seem a little obvious, but taking the time to ensure your physical access control system is trusted and reliable cannot be overlooked. This goes beyond troubleshooting, testing and transitioning your PACS during a trial, pilot or rollover period to the actual design of the software platform and underlying system architecture of the product itself.

Traditional, physical access control systems often require single, stand-alone Windows servers at each and every facility, increasing maintenance and licensing costs while creating single points of failure. When a server goes down, identities, permissions and policies cannot be updated, with door controllers and card readers granting access to those identities stored locally on-site, until the server can be maintenanced or repaired.

A next-generation PACS can simplify system redundancy and provide cost-effective autofailover and hot-standby capabilities, particularly when delivered as an affordable, all-in-one, access control network appliance or solidstate, rack-mounted server. Instead of purchasing expensive stand-alone servers, organizations can deploy two or more network appliances that can synchronize identities, roles and policies across all facilities and door controllers in real-time to reduce costs and increase security.

IT professionals can further reduce costs, enhance scalability and improve reliabillity by deploying a PACS capable of running in a virtual server environment. When the system runs on a virtual server, set-up can be done in record time, hardware costs are minimized and failover processes become even more painless. A failover VM can be automatically provisioned and spunupwhile the existing VM deployment is fixed with no hiccup in service.

2. Security

Traditionally, most building security systems have been purpose-built by manufacturers with a background in the physical security industry. While these developers tend to include all of the important features necessary to keep a building manager sleeping soundly through the night, IT professionals may be the ones losing sleep — unless their physical access control system received a thorough code review. Look for platforms that have some kind of assurance that the PACS received an industry-recognized certification to verify their application was hardened against known software vulnerabilities to reduce or eliminate the risk of network attack.

Not only are software vulnerabilities cause for concern, but operating system and server vulnerabilities need to be taken into consideration as well. For example, many legacy physical access control systems are built to run on a standard Windows application or database server, which often requires consistent vulnerability patching and continuous IT resources to ensure the system is not exposed to the latest security threats making their way across the Internet.

Several manufacturers have begun providing Linux-based PACS platforms which significantly reduce system setup, support and maintenance issues, while eliminating patch management and security headaches. A secure, open-source, Linux-based physical access control system may provide the peace of mind you are looking for in a building security system, controlled by users strictly through a web browser, thin-client, instead of a thick-client application.

Thick vs. thin-client

"With the thick client, you always have to worry about whether an update from Microsoft will break something," says Steve Travis, IT Support Prof Lead, Georgia Tech Police Department. "You have to worry about security, wondering 'Do we have to put this computer on a standalone VLAN and just lock it down and basically it will be used only for card access?' ... That puts a burden on the department ... Whereas if it's a browser-based system, they could be using the same computer they use for day-to-day emails or whatever they use for work."

5 reasons for physical security to go mobile

1 No software to install or servers to maintain

2 Control facility access from anywhere

3 Respond to alarms at anytime

4 Stop being tied to your desk

5 Use your existing mobile devices

3. Mobility

The rise of mobile computing cannot be ignored, with mobile devices, such as smartphones ortablets, now connecting to nearly 89 percent of corporate networks, according to Forbes. Given this increasing mobile demand, selecting a webbased, physical access control platform allows users to manage building security from any web browser, from any location with Internet access.

Traditional, software-based PACS only runs on specific desktop or laptop computers, forcing IT departments to install and/or upgrade individually-licensed software and servers one-at- a-time. Legacy systems also keep facilities managers and security directors tied to their desks, instead of being able to do their job from any building, at any time, from any location.

Managing facilities requires a lot of in-person supervision on a day-to-day basis, which is why it is important to look for a physical access control system that works as well on a variety of mobile devices — as well as a variety of PC and Mac web browsers — as it would on a desktop computer down in the basement of the building.

With a web-based access control system, a facilities manager can carry his iPhone, Android smartphone or tablet to an off-site meeting or to the top floor of the building and still be able to respond to alarms, change door schedules or view video surveillance footage. IT professionals, systems integrators and security vendors can also log into the system from any web browser to change a system configuration or provide ongoing support.

Additionally, in larger organizations with multiple buildings, office locations or off-site campuses, a thinclient system architecture that is delivered via a web browser can significantly reduce costs and increase efficiency when it comes to upgrading, managing and centralizing facility access control, when compared to an old, thick-client model that depends on software alone. Without the added software and individual user license costs, organizations can free up their IT and security budgets to protect additional doors, buildings or facilities.

4. Usability

Ease of use is another important factor to consider when evaluating the effectiveness of a physical access control platform. While IT is comfortable with a wide-range of software, hardware and user interfaces, physical security users may not have as much familiarity with using advanced computers or managing complex operating systems.

A front-desk security guard or back-room facilities manager should easily be able to add, delete or adjust door access schedules and user privileges without feeling intimidated or overwhelmed by the system. Cards, badges and credentials should be easy to update on a regular basis to make sure only the right people have access to the right rooms and resources and that former employees can no longer enter the building. And alarms should be easily accessible and compatible with a variety of video surveillance platforms to provide physical security teams with the information they need to quickly investigate a system alert, security breach or policy violation.

IT professionals, on the other hand, would prefer a system that is built to work the way they work and is designed to integrate with standard IT systems. For example, platforms that support Lightweight Directory Access Protocol (LDAP) are able to bind withan organization's existing HR employee database, Active Directory or Identity Access Management (IAM) system, which eliminates the need to maintain two sets of employee and visitor identities and may even allow organizations to assign building access privileges to the users that exist in their network access control system. Additionally, some physical access control systems are able to easily integrate building security data into a Security Information and Event Management (SIEM) system, so organizations have a unified view of security across the enterprise.

Real-world convergence

If the door to a server room is propped open, a well-integrated system will trip an alert to physical security stakeholders, who can immediately switch to video feed to monitor what's going on in real time. The system can automatically suspend network access in nearby rooms until IT and physical security review the SIEM logs to discover what did or didn't happen, with all activity around the door — including who it was that last swiped in for access — easily accessible. The right access control platform makes it easier for everyone to do their jobs, and ultimately reduces the risk of a small incident snowballing out of control.

5. Flexibility

Having a physical access control system that can grow and scale with the size of your organization is critical, whether you need to protect a handful of doors at a single site or hundreds or thousands of doors across multiple buildings and office locations.

With nearly 80 percent of the cost of a physical access control system attributed to the door hardware — the controllers, switches and card readers that are installed in the walls and ceilings of the building — it is important to choose an access control system that relies on open, nonproprietary door hardware, which provides your organization with the greatest flexibility.

5 reasons to avoid proprietary door hardware

1 Software and vendor lock-in

2 Complacent manufacturers and vendors

3 Costly support and maintenance plans

4 Prohibitively high switching costs

5 Non-future proof investment

Many physical access control systems rely on proprietary door controllers and card readers that only work with a single physical access control system, thereby locking organizations into dealing with a single manufacturer, systems integrator and software platform. If you grow unsatisfied with the system, the cost of upgrades, or level of vendor support, the switching costs are prohibitively higher to deploy a new system.

Open architecture systems allow IT and physical security teams to leverage their investment in reusable, non-proprietary door hardware, giving them the ability to more easily and affordably upgrade their access control system by purchasing a new head-end system, without needing to buy and install all new door hardware and controllers. This allows their IT and security budgets to go further, without being forced into using the software platform that is married to the proprietary door hardware. As the organization expands its footprint or the number of doors increases, IT can simply add more non-proprietary hardware, without worrying about the hardware investment growing outdated.

And because there is still competition for your ongoing access control business, manufacturers and vendors cannot afford to grow complacent.

Summary

IT needs an open-architecture system that offers better scalability, the option to install in a virtual environment and improved options for integration with other IT and physical security systems. Not only do these technologies need to be easy to deploy, for example, in a virtual server environment, they also require the system be hardened to cyberattack while remaining completely reliable.

Meanwhile, the facilities team wants a solution that makes their lives easier. They want it to be easy to change, add or delete users from the system, they need it to allow flexibility to grant access exceptions when the situation arises, and they prefer having the ability to control door access privileges with a smartphone or mobile device, wherever they are in the building, without being tied to their desk.

A system that meet everyone's needs not only improves their workflow, it keeps expenses down, both now and in the future. Organizations that seek out systems that bring together access control with video surveillance, identity management and Security Information ,and Event Management (SIEM) can operate more efficiently and intelligently in all situations.

Perhaps most importantly, though, such a system brings down the barriers that have stalled the convergence of physical and logical access control systems for so long. IT no longer needs to worry about an insecure system that adds more operational overhead. And facilities staff no longer need to spend hours figuring out frustrating and confusing user interfaces. The two parties can finally work together to become more efficient and eliminate security gaps in the process, once an IT- and user-friendly building security system has been acquired.