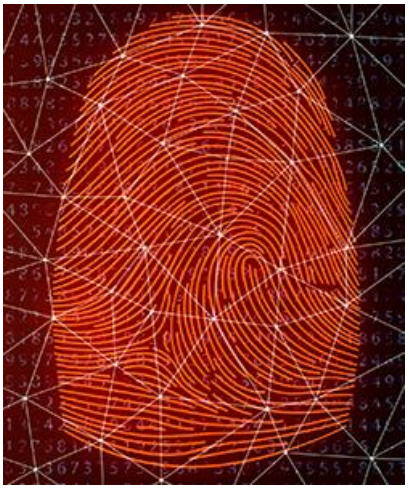
www.pipelinepub.com
Volume 20, Issue 1

Modernize Physical Access Control to Close Data Center Cybersecurity Gaps

By: David Ellis



Over the past few years many businesses, government organizations, and schools have made a massive shift to cloud services. According to Gartner, by 2025, 85% of infrastructure strategies will integrate on-premises, colocation, cloud, and edge delivery options, compared with 20% in 2020. The data center industry is therefore anticipating and preparing for an unprecedented growth of operations and facilities.

As demand for cloud services soars, regulations evolve, and cyber threats increase, data center professionals have a complicated new reality to navigate. Their task is to balance operational efficiency with both regulatory compliance and data security requirements.

Notwithstanding the growing demand for cyber- and physical security measures, many data centers are still using dated access control systems. Systems that date back a decade or more can be especially susceptible to cyber threats. Moreover, assigning and tracking temporary access rights manually is both time-consuming and prone to errors.

Access control technology has advanced significantly. Modernizing access control systems enables automated approaches for managing access rights along with providing stronger cybersecurity protocols. You can streamline the flow of employees and contractors moving in and out of your data center while also ensuring top cyber- and physical security measures are in place.

Open architecture systems lay the foundation for scalability

The pace of technological change has accelerated dramatically. Thirty years ago, new analog technologies entered the market every three to five years. In today's digital world, new options are available more frequently, sometimes every six to 18 months. The decision many companies face is when to adopt these new technologies and when to wait.

This pace of change can be challenging. Many organizations decide to stick with the technologies they know and which seem to work "well enough" rather than rock the boat. Others are reluctant to adopt new technologies simply because they don't want to miss out on the next big and better thing to hit the market.

But it is a manageable dilemma. A good first step is to transition away from proprietary technology and select an open architecture system. Open systems allow for the integration of technologies from different manufacturers and the addition of technology as it evolves and becomes available. An organization can select options that best meet its current needs and implement select new solutions over time.

Open systems also allow for hardware to be upgraded gradually. Entire systems do not have to be replaced every time something new is available on the market. For example, if your team isn't fully confident in adopting a new access control system, you can test and implement it gradually. This may include starting with select doors or certain floors or buildings. You can add on to the system once you've worked out any challenges or obstacles.

A significant change in access control is the evolution away from low-frequency proximity (prox) cards as a credential. Prox cards are easily compromised or cloned, so the market is moving towards new security solutions. If your strategy still involves a hard credential, then moving to higher frequency cards, Bluetooth-capable readers, and encrypted control boards is key. The risk of dated hardware and software solutions in conjunction with bad actors equals the potential for large amounts of lost revenue.

But re-issuing credentials can be easier said than done. The implementation of high frequency and Bluetooth-capable readers allows for the use of mobile credentials. With cardless credentials such as these, access can be issued, changed, or revoked virtually.

Biometric credential systems are taking great leaps forward in security, from simple finger, retina, or palm scans to geometric facial-matching systems using video analytics. For security directors, it may be difficult to decide which biometric credential system to implement. A best practice is to pilot the new technology in specific places. Once tested, the new technology can be integrated with your current system if you decide it's a good fit for your entire data center.

Cybersecurity risks to data centers from legacy access control systems

Access control systems are expensive to replace and can have complex operational impacts when a change is necessary. Security teams are understandably hesitant to adopt new technologies. This hesitancy to upgrade can, however, result in significant gaps in data center cybersecurity. Many older access control systems have known vulnerabilities. Legacy technologies do not always have the needed firmware updates. Some may use passwords that are easily guessed or have been compromised. Many have not been hardened to modern cybersecurity standards. When systems become difficult to use, the likelihood of human error increases proportionately. According to the Uptime Institute's 2022 Outage Analysis, over 85% of major outage incidents reported stemmed from staff failing to follow procedures or from flaws in the processes themselves.

While the data center's servers may be cyber-hardened, they may still be subject to crucial vulnerabilities if the access control system that protects them is not. Edge devices and controllers are often the weakest links in access control systems from a cybersecurity perspective. It is common to see passwords that are easily guessed or rarely changed, or firmware that hasn't been kept up to date.

Now that access control systems have so many ”smart” network-connected devices, it is important to choose a system that allows for centralized monitoring of cybersecurity threats. If your system requires each of your hundreds of readers and boards to be individually checked and manually updated, your team is more likely to fall behind in this work or forget to do it.

Only a small number of access control software companies monitor edge devices. Look for solutions that notify you of the firmware version and if updates are recommended. With a modern, unified system, your software can help you monitor systems. The platform can alert your team when critical updates need to be installed. It can also help you to push those updates to all devices at once. Some software solutions even prompt users to update passwords regularly, indicate when they were last updated, and generate new passwords for each device.

Benefits of a unified approach to security

A unified system is a key component of modern access control systems due to their complexity. Disparate platforms are a struggle to maintain and use. A unified approach streamlines security technologies and enhances operations, physical security, and cybersecurity.

Every layer of perimeter security is linked to the next. Security teams can unify automatic license plate recognition (ALPR), video management systems, access control readers, and other Internet of Things (IoT) devices in one interface and thereby have a complete view of their facilities. This streamlined approach to security improves efficiency, closes cybersecurity gaps, and centralizes data from all systems into data that inform processes and overall operations.

For example, when a forced door alarm is initiated, a system that unifies video monitoring and access control allows your security team to quickly identify and review the related video feed. You may even change an alert to notify different teams based on the combined data from the door sensor and video analytics. A system with workflows may require multiple events to be initiated to trigger an alarm that requires immediate attention. For example, an alarm sounds to the security operations center (SOC) when a door is forced open *and* the camera detects motion. If no motion is detected, then it may be a low-priority alarm instead of a high. Once the cause is determined, your team can follow previously established automated standard operating procedures (SOPs) for the next steps.

A unified system can even combine data from sensors that aren’t traditionally part of a physical security solution, such as temperature sensors. In this case, digitized workflows could alert teams to respond to a potential HVAC unit problem in a data closet where the electronics are kept. The alarm would let the maintenance and IT teams know it is getting too hot prior to the equipment overheating and shutting down. In some organizations, human security guards still check thermostats on their hourly rounds, resulting in extra hours required for validation.

Unifying all aspects of your security within one solution gives your team a complete picture of your facilities and operational status. You can make better, more informed decisions that can improve security, streamline operations, and reduce downtime. The adoption of a modern, multi-site, unified security platform is the natural choice for data centers to meet the challenges they face today.

.