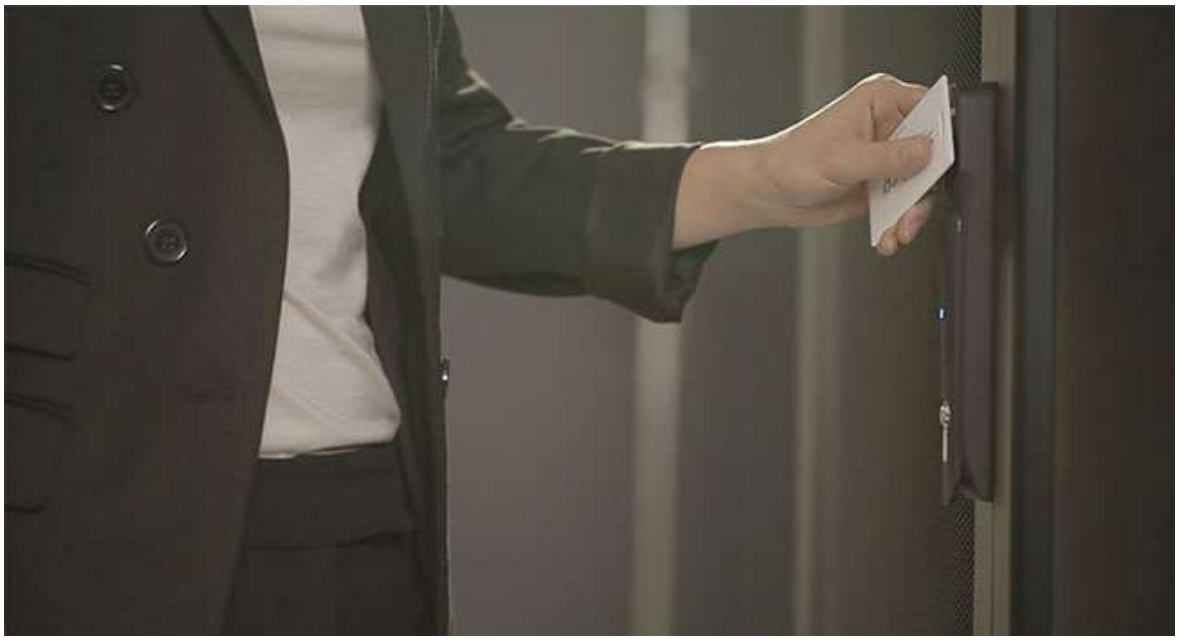


Securing the Physical Safety of Data with Rack-Level Access Control

In our networked and internet-dependent world, securing personal and business data from theft, hacking and other forms of cybercrime has become an issue of paramount importance – and the world's data centers, where data has its physical presence, are key points where multiple layers of security need to be established and sustained.

Consider just two of the many documented costs of cybercrime:

- Database breaches cost global organizations over $3.62 million annually, based on a 2017 industry study
- Recent data from IBM Security Services shows that 71 percent of all attacks on the financial industry and 58% of all attacks in the healthcare industry were carried out by malicious insiders or inadvertent actors (accidental events)

In addition, there are multiple regulatory and compliance requirements creating additional layers of responsibility for data center managers, mandating that organizations must limit physical access to information systems, equipment and the respective operating environments only to authorized individuals.

Data center operators make significant investments in cyber security, erecting firewalls and deploying powerful software programs to prevent electronic cybercrimes. Increasingly, they focus on controlling the physical security of electronics and telecommunications enclosures as well.

The steady, constant stream of service technicians who need access to the server racks, communications hardware, and electrical and environmental systems for maintenance, upgrade and expansion tasks presents many security challenges for the data center manager. In addition to outsiders, inside personnel are just as much of a risk and need to be managed and secured during their time in the facility.

Many data centers focus security efforts on access control to the grounds, the buildings and the secure areas within:

- Access to the building is often gated, with exterior physical protection elements to secure the entire site and requires a guard to verify and document entry through the gate.
- Once an individual enters the facility, they typically sign in with a live guard and receive a credential for access to specific areas.
- In some facilities, access to a specific floor or enclosure area is further controlled by a “man trap” with two sets of doors accessed via an electronic credential, either RFID or biometric.

Extending physical security to the rack level

The server rack is the final point of data vulnerability in the data center, so it makes sense to consider implementing the same level of sophisticated physical security and access control monitoring already established at every other level of entry in the data center.

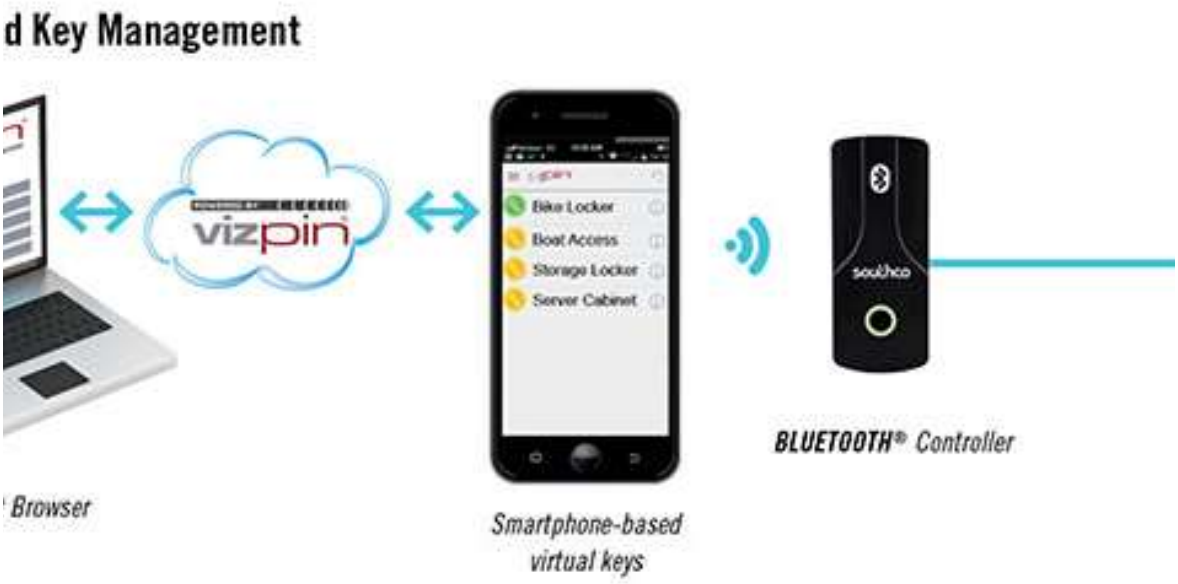
Electronic access solutions, like electronic locks and latches, offer a modular security solution designed for simple integration into Data Center Infrastructure Management (DCIM) systems and existing server rack enclosure designs. Integrating electronic access solutions at the rack level offers the maximum level of physical security, providing peace of mind for the data center operator.

Electronic Access Solutions (EAS) typically consist of four main components:

- **Electromechanical Lock or Latch–** The most critical component of any electronic access system, this mechanism performs the electromechanical locking or unlocking function upon receipt of a valid electronic signal and provides an output of its status to external monitoring systems.
- **Access Control Device –** The access controller acts as the human interface, allowing the electronic lock to be remotely operated through a variety of options, such as digital keypads, biometrics, RFID readers, and other wireless communication devices such as *BLUETOOTH*® enabled smartphones and tablets.
- **Remote Monitoring –** Electronic access solutions have the unique ability to capture an electronic "signature" for each access attempt. This info, together with additional security and environmental data, can be output to a variety of devices, from simple indicator lights to networked, software-based remote monitoring systems.

[redacted] an override system is required to provide access in the event [redacted]. This override system can be mechanical, providing direct mechanical actuation of the lock, or electrical, providing external power in the event of a system power failure.

The key element of effective rack level electronic access systems is the use of intelligent electronic locks that restrict access through the validation of user credentials. Electronic locks can be integrated with a variety of rack level access control devices, such as digital keypads, RFID card readers, biometric readers and electronic key systems.



BLUETOOTH® enabled, wireless smartphones and tablets have enabled a new class of remotely controlled access control solutions. With a *BLUETOOTH*® enabled system, a technician receives a web-generated, time-based electronic key on their smartphone that can be used to access a specific cabinet for a specific time frame. A *BLUETOOTH*® reader installed inside the cabinet can then receive this digital key and output to the connected electronic lock for access. The smartphone can then send audit trail data wirelessly to the cloud via a cellular or Wi-Fi connection for audit trail reporting. This unique solution provides remote access control without the need for a physical network connection.

Integrating rack level EAS into existing data centers

The primary reason data center cabinets and server racks continue to use standard mechanical key locks is in the numbers: While data centers have relatively few access points to get into the building, there are potentially hundreds of cabinet doors that would need intelligent electronic locks – and usually two are required to accommodate the server rack. Traditional building level access control solutions are simple too costly to apply at the rack level and thus a different approach is required for rack access control.

One option is to leverage existing control and monitoring systems such as Data Center Infrastructure Management (DCIM) solutions, power monitoring systems or dedicated rack security systems. Intelligent rack level electronic locks can be retrofitted to server cabinets and integrated with the DCIM or other rack level security system to leverage the existing hardware, software and network connections, and minimize the cost per rack.

Cost-effective rack level security solutions are available, depending on the specific application. For

example

- **Self-contained solutions** that are generally battery-operated and offer simple, drop-in installation and programming to provide integrated access control and electronic locking in a single self-contained device.
- **Standalone solutions** that offer basic plug-and-play access control without the need for software or network administration where remote control and monitoring is not needed.
- **Wireless remote controlled solutions** that leverage *BLUETOOTH*® connectivity with cloud based web portal credential management and monitoring to provide the simplicity of a standalone system with the benefits of a networked control system
- **Integrated solutions** that can be combined with building access control and monitoring systems to incorporate cabinet-level access control into existing security systems.
- **Independent networked solutions** that can be used to monitor and manage rack access across networks from a host computer for remote system configuration, access control and the monitoring of multiple access points.

EAS enables "virtual cages"

Data center operators, particularly those running co-location operations with dozens or even hundreds of customers, seek to maximize return on their expensive real estate. However, certain customers needing a higher level of security, such as government agencies, healthcare operations and financial institutions, require standalone physical cages separating their servers from others in the data center.

Often, this is literally done by erecting chain-link fencing and securing a gate with a padlock – eating up valuable floor space. Electronic access solutions can be used to create "virtual cages" to protect confidential data. By implementing electronic access at the rack level, the more secure data cabinets can be located among the lower security racks since the physical security enhancement is now directly on the rack itself.

Rack level EAS: the final link in data center security

The entire IT and data center industry must continue to apply every tool available to secure personal and corporate data and applications from identity theft, malware, hijacking and other hacking attacks. Using electronic access solutions to secure the server racks is the final component in creating a fully secure data center. Rack level electronic access provides a controlled physical security solution that, when integrated into existing security and monitoring systems, provides a complete end-to-end data center security solution.

Posted by Steve Spatig on Feb 13, 2018

Printable Format E-Mail this page

TSA Breaks Record For Highest Number of Firearms Detected at Airport Checkpoints

Security at 20,000 Feet

A Professional's Guide

Powering Access Control

Most Popular Articles

Enabling Prevention

TSA Breaks Record For Highest Number of Firearms Detected at Airport Checkpoints

Federal Institute Releases Guidelines For How To Respond To Ransomware Attacks

Surveillance Strategies - Camera Positioning to Maximize Coverage and Reduce Project Cost

Security at 20,000 Feet

Whitepapers

The AI (R)Evolution of Enterprise Security

Perimeter and Intruder Security for Educational Establishments

Webinars

A K9 Nose Best

Surveillance Strategies - Camera Positioning to Maximize Coverage and Reduce Project Cost

U.S. Department of Education Releases School Safety Guide