BELDEN

Smart Cabinet Access System for Data Center

Denis Blouin
Engineer, Belden Infrastructure Solution Product Manager

Table of Contents

Introduction 1
Why Cabinet-Level Security 2
Deployment Considerations 3, 4
Security Regulations & Initiatives Impact All Markets 5
Belden Has the Experts and the Solutions You Need 5

Our End-to-End Expertise
Your End-to-End Solution

Introduction

With the digital revolution now in full swing, online transactions, mobility, social media and Big Data continue to increase the amount of information being transmitted, stored and accessed by businesses and consumers anytime, anywhere and on any device. And it's all happening through the data center. With virtually every task in every type of business involving the transmission of digital information across networks, data centers have become as integral to today's economy as factories were in the late 1800s and early 1900s.

Much of today's digital information being transmitted and stored via the data center is private, valuable and must remain secure. From personal medical information and financial transactions, to intellectual property and national intelligence, a wide range of mission-critical, private and confidential data that spans multiple industries is required by privacy regulations to be protected from unauthorized access (*see page 4*).

Protecting that data is also imperative to maintaining corporate image and preventing serious financial risk. According to Privacy Rights Clearinghouse, more than 234 million records with sensitive credit card information have been breached within the past decade, and just in the past year, several large retailers and online entities lost millions following security breaches and ultimately experienced reduced customer confidence.

Today's enterprise data centers are at the core of protecting and securing digital information, and external cyber security protocols like antivirus, encryption and firewall technologies have come a long way over the past decade. However, physically securing private and confidential information in the data center is equally important—especially with the biggest cause of security incidents coming from within.

According to a 2011 survey by Gabriel Consulting Group, more than 60% of today's security breaches are at the hands of company insiders or others with legitimate data center access. Consequently, there is a need for better physical security and access control in the data center at the cabinet level where the network equipment that transmits and stores data resides.

Why Cabinet-Level Security

While physical security in the data center is a key part of industry regulations surrounding the protection of data, ensuring appropriate physical security of network equipment within data centers has often gone overlooked.

With advanced external network security like firewalls and encryption, many businesses consider access control at the room level to be sufficient. Many also fail to recognize the potential for internal threats and the need to bring physical security to the cabinet level and deploy methods for accurately identifying culprits when a security breach occurs.

Security breaches at the hands of company insiders can include vendors, contractors, consultants, maintenance personnel and others with legitimate access to the data center. For example, many data centers have areas dedicated to specific systems and outside vendors have access to the data center to install, upgrade and maintain their equipment. This is very common in hospitals, universities and large hospitality venues. Colocation data centers that lease space to customers who are responsible for installing and maintaining their own equipment need to be especially careful due to the number and range of individuals frequenting the facility.

Internal IT staff with authorized access can also be a threat, including employees who are disgruntled, aligned with outside criminals or stealing data for monetary gain or for leverage at another company. For example, a network technician with access to storage devices can easily steal valuable account information or intellectual property using a simple thumb drive. As a result, the need to bring physical security down to the cabinet level in the data center environment has become paramount.

While most privacy regulations recommend or require some level of monitoring, alerting and auditing, they lack details regarding implementation and processes. Consequently, businesses are often left to determine the appropriate physical security methods based on the information they need to protect. A cabinet access system specifically designed for the data center environment with customizable management, administration and reporting can go a long way in providing superior physical security that complies with industry regulations.

Deployment Considerations

When it comes to selecting a cabinet-level access system for the data center, there are several considerations, including:

- **Ease of deployment**—Cabinet access systems should be easy to deploy on any cabinet with components that do not take up valuable rack-unit space allocated for network equipment.
- **Flexibility**—The system should have the flexibility to support a variety of data center environments, including individual cabinet-level access or group-level access for end-of-row (EoR) configurations or pod-based data centers where rows or groups of cabinets are often segregated by function. Another consideration is the ability to support both front and rear cabinet door access separately as some data centers may have different teams responsible for accessing the front and rear of equipment (see Figure 1).
- **Scalability**—Cabinet access systems should be scalable, just as data centers should be scalable. Centralized IP-based access systems with components that reside on the network and are centrally managed from a single software-based platform have virtually no limit to the number of cabinets or groups of cabinets that they can control. This allows the system to grow as the data center grows.
- **Smart Access**—Cabinet access systems should use the latest smart access technology for improved security over keyed locks. Keys can be easily misplaced or passed from one individual to another. Unlike smart access systems, keyed systems can make it impossible to truly identify culprits when a security breach occurs—there is no way to indicate exactly who the person was that used the key. Managing who has keys, when they should have access and immediately retrieving keys following changes to access levels and personnel can also be a difficult task that presents greater opportunity for unauthorized access. Card access systems should also be based on the latest advanced smart card technology such as iClass. Standard low-frequency proximity card systems are vulnerable because their information can be easily copied and used to create duplicate cards. iClass-card based systems allows for encrypted communication between the card and the reader, making card duplicate extremely difficult.

- **Biometric Capabilities**—Cabinet access systems that offer a biometric access option can provide an even greater level of security and help facilities achieve maximum compliance with security regulation auditing requirements. For example, systems that use advanced fingerprint scanning technology to identify user access require the person to be physically present for authorized access. This enables facilities to produce a 100% indisputable audit trail and eliminate the possibility of keys or a smart card being lost or ending up in the wrong hands. In addition to improved security, biometric access is also easier for the user—there is no need to carry a card or remember a password.

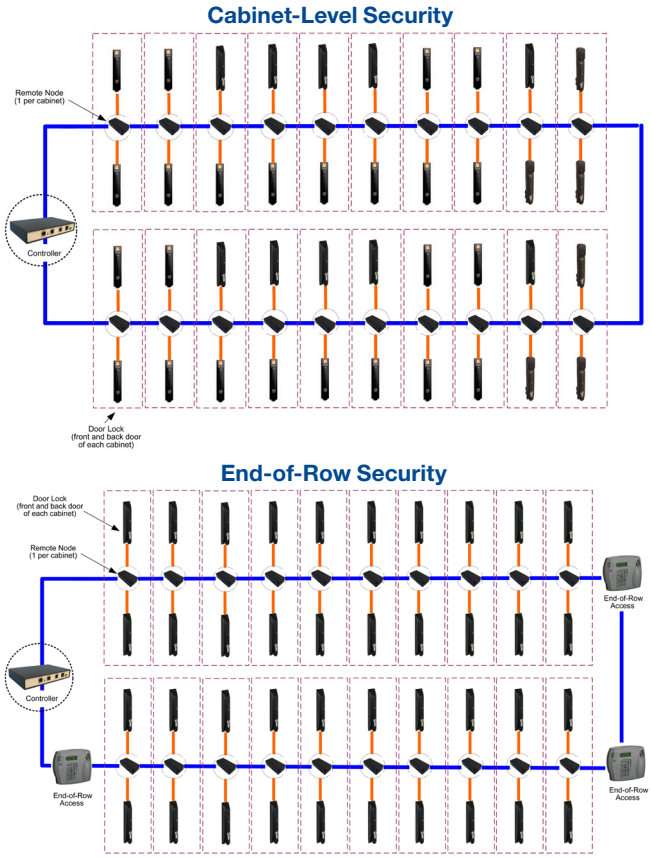

Figure 1: A Cabinet access system with the flexibility to define access by front or rear cabinet door, individual cabinet or row/group of cabinets can support a variety of data center environments.

- **Advanced Security Features**—Another security feature to look for in a cabinet access system is dual custody mode. Commonly used in extremely high security environments, dual custody requires two different users to be present to successfully authenticate access. Three-point latching systems can also offer better security by immobilizing both the top and bottom of the cabinet door rather than just at the lock. The communication between readers and the system should also be encrypted for improved security.
- **Superior Reliability**—When selecting a cabinet access system, redundancy and stand alone capabilities are critical to maintaining system reliability. If the network on which the access system fails the access system should be able to locally records access occurrences and down load information to central data base once network is re establish.

  System using ring typologies allows re-route of signal in case circuit is broken. Systems should also be able to maintain cabinet security in the event of a complete power failure.
- **Centralized Management**—Advanced management software for managing up to thousands of cabinets and users should be a part of any cabinet access system. The software should be easy to set up and configure with the ability to receive and communicate access attempts, alarms and other events from each cabinet in real time for monitoring and alerting to appropriate staff members at workstations or remotely via phones and hand-held devices. Systems features such as the ability to remotely lock and unlock specific doors or place the entire system into full lockdown in case of a system breach add a sophisticated level of management. The system should also have the capability to immediately alert in the event that a connection is cut or a cabinet door has been forced.
- **Reporting Capabilities**—The ability of a cabinet access system to store events and generate detailed audit reports that indicate which users accessed which devices at what time and for how long can be vital for compliance with security regulations that require specific reporting and auditing. The ability to customize and automate reports is also a key benefit for capturing the required information when it is needed.
- **Zoning Capabilities**—A quality cabinet access system should have the ability to group the system's IP-based controllers and their cabinets into smaller zones to facilitate management and reporting based on individual facilities, specific spaces, functions or tenants/customers within a single data center or colocation facility (see Figure 2).
- **User Parameters**—The system should allow for setting up a variety of user parameters and access levels based on a specific environment, including full administrative access, access for monitoring and control, zone access or standard users with access to specific cabinets. The ability to assign users with access for managing individual zones is ideal for allowing tenants to manage their specific zone within a colocation center. Being able to set up and assign users to user groups with access to specific cabinet doors and with parameters such as timebands that allow access during specific times are ideal for data center operations with multiple shifts. User groups and timebands are also ideal for setting up temporary access for maintenance personnel or visiting vendors (see Figure 2).
- **System Integration**—Regardless of which cabinet access system is selected for a data center, the ability and ease of integrating and exchanging information with other systems that reside on the network can make for an overall smarter, more secure computing space. For example, through simple network management protocol (SNMP) traps, queries and syslog files, information can be shared with other security and building automation systems or with data center infrastructure management (DCIM) systems for monitoring, alarm and control. Systems that use iClass-based smart access cards can also integrate with other iClass-based systems—a facility's existing smart cards can be programmed for cabinet access in the data center, which can cut down on deployment costs.

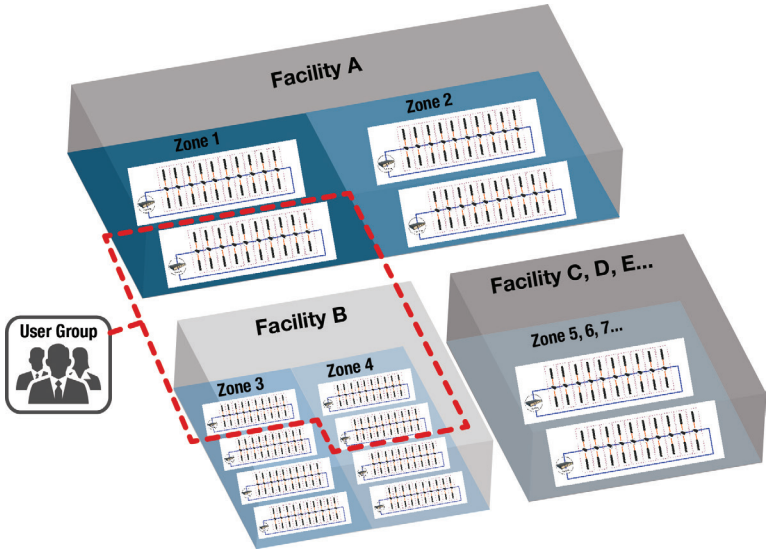

Figure 2: The ability to partition a system's IP-based controllers and their cabinets into zones and create and assign users to specific user groups with access parameters can facilitate managing, administrating and controlling access to cabinets based on facility, spaces, function or users.

Security Regulations & Initiatives Impact All Markets

- Federal directives and protocols to protect classified national security information and intelligence within government entities have been in place since the 1980s, and the digital revolution has given way to several security regulations that impact all markets and industries. The following common privacy regulations affecting a variety of enterprise businesses and data center facilities include requirements for limiting physical access to information systems, equipment and IT operating environments to authorized individuals.
- HIPAA & HITECH—The Health Insurance Portability and Accessibility Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act focus on the protection of personal health information and electronic health records. With violation penalties that can reach $1.5 million, these two acts apply to hospitals and healthcare facilities, as well as companies that need to access or transmit this type of information.
- Sarbanes-Oxley—Mandatory for all organizations, the Sarbanes-Oxley Act of 2002 (often abbreviated as SOX) was enacted in response to financial scandals that occurred in the late 1990s. The act specifies the types of information to be stored by businesses and the amount of time it should be stored. SOX requires businesses to have an auditable trail of information, physical security, and a system for monitoring and reviewing access on a periodic basis.
- PCI-DSS—Established jointly by Visa, MasterCard, Discover and American Express, the Payment Card Industry Data Security Standard (PCI-DSS) relates to all businesses that accept credit card payments—either online or off. Requirement 9 of PCI-DSS states that any physical access to data or systems should be appropriately restricted and entry controls used to limit and monitor physical access to systems that store, process or transmit cardholder data.
- EU General Data Protection Regulation—This regulation unified data protection within the European Union (EU) and within organizations outside of the EU that process any personal data of EU residents. It requires any entity that holds personal data to keep the data safe and security from potential abuse, theft or loss.
- SSAE 16—Issued by the American Institute of Certified Public Accountants, SSAE 16 is an auditing standard that covers data center security, controls, management and operating effectiveness. Geared primarily towards traded enterprises, financial institutions, healthcare organizations and large colocation data centers, SSAE 16-compliant data centers restrict physical access to the data center through a combination of physical security systems and biometric identification.
- Cloud Security Alliance (CSA)—With nearly 50,000 members, this non-profit organization working to promote security within cloud computing providers and facilities heads several research and education initiatives to help companies ensure secure cloud computing services. They also help to assess the security of private and public cloud computing facilities, including physical security and access control.

Belden Has the Experts and the Solutions You Need

Data centers were once viewed as supporters of a business model, but today they are the business model. With virtually all business now accomplished via the data center, enterprise companies need to protect private data from both external and internal security breaches to comply with regulations and to protect their customers and their reputation.

As the overall need for physical security in the data center gains more attention in the aftermath of security breaches, the TIA TR42.1 is even working on a physical network security standard that will provide guidelines for protecting critical network equipment from unauthorized access. The standard is slated to recommend the capability to detect and report unauthorized access to cabinets and device connections or disconnections via DCIM.

To overcome the challenges of physical security at the cabinet level, government and enterprise data centers need enhanced cabinet access systems that ensures indisputable audit trails, integrates with existing facility security systems, offers flexible deployment options and significantly cuts deployment and operating costs—all while maintaining the highest level of regulatory compliance.

Available on all Belden X-Series enclosures for multi-media, servers and networking equipment, the Belden Smart Cabinet Access System is a highly flexible, scalable and reliable IP-based cabinet access system designed specifically for the data center. Field proven and well established via use by leading financial and education institutions, colocation centers and government entities, the Belden Smart Access System is easy to deploy in a variety of configurations with feature-rich security and centralized management for virtually any number of cabinets, zones, users and user groups. With indisputable audit trails and real-time monitoring and alerts, the system can help meet security regulatory requirements.

With physical security for asset protection becoming a vital part of IT operations for data centers and other computing locations, Belden has the experts and solutions to help you cost-effectively protect critical information and avoid the risks of a security breach. Whether it's hospital, financial institution, colocation center or government facility, how a data center is designed can go a long way in ensuring physical security. Before deciding on physical security methods for the data center, Belden experts can help you define the primary objectives of a security plan, determine where security is required within the data center and choose the data center design, configuration and cabinet access system that best suits your needs.