SIEMENS

DATA CENTER PHYSICAL SECURITY

# **Inspire trust** by building a unified defense

A multilayer, centrally managed Siemens infrastructure integrates with building management systems, maximizing uptime and data protection to secure your data center's reputation

INTRODUCTION

# **Critical systems** need comprehensive protection

Data centers today play a bigger role than ever in both business and daily life. Whether owned and operated by an enterprise or built to host third-party clients, data centers house systems and data that are critical to commerce, supply chains, government, health care and almost all other functions in our connected world. As a result, these facilities need multiple layers of physical security to protect staff, customers, visitors, systems and data from disruptive attacks.


With so much value concentrated in data centers, protecting them from physical threats is a core responsibility of operators. Intruders can damage a facility, shut off power, steal equipment, trigger lengthy outages and put lives at risk. If they gain access to server racks, they may be able to extract sensitive customer data or disrupt a company's operations. Data center operators that experience either downtime or a breach can lose customers that no longer trust their services. No matter the amount of the compensation to customers, it cannot restore the a data center operator's reputation.

Any amount of downtime — not to mention data loss or corruption — can hurt an organization's finances and reputation. The 2020 Uptime Institute Global Survey of IT and Data Center Managers found that four out of every 10 recent data center outages cost the affected company between $100,000 and $1 million, while about one in six cost more than $1 million. In the same survey, 14 percent of respondents said they had experienced serious outages — ones involving service disruptions, financial losses, compliance breaches and damage to reputation — in the previous three years. [1]

Data breaches can be even more costly than outages. According to a 2021 Ponemon Institute study sponsored by IBM, the average cost of a data breach was $4.24 million, up 10 percent from 2020, with survey respondents in the U.S. reporting the highest costs of any country: an average of $9.05 million. [2]

An effective, unified physical security infrastructure is essential to prevent potentially devastating events and demonstrate a strong security posture that inspires customer loyalty and trust.

**Physical security in data centers**

Data center physical security practices have evolved rapidly in recent years. Official standards and industry best practices now call for multiple tiers or layers of security, from architectural features at the perimeter of a facility to locked cages with identity-based access controls protecting individual customers' systems.

A typical data center has multiple security systems. Managing them separately increases the opportunity for error and the chance of a security lapse. A central management system with a single user interface, integrated with role-based identity management, helps control the components that affect physical security at all layers, such as lighting, video surveillance systems, intrusion and hold-up alarm systems (I&HAS), access control kiosks, gates and doors. This white paper will illustrate security use cases at various layers of a data center and focus on a management platform that allows data center operators to maintain the highest level of physical security.

The recommendations in this paper draw upon both widely accepted standards and successful physical security implementations in large data centers around the world.

Two recent formal standards set guidelines for determining security requirements and ensuring the necessary level of protection. In 2017, the Telecommunications Industry Association published the TIA-942-B standard. In 2018, the International Organization for Standardization adopted ISO 22237. Both specifications provide prescriptions for data center physical infrastructure, including physical security.

ISO 22237 stipulates that organizations responsible for data center assets should determine safety requirements through a risk assessment based on two main factors: the threats posed to each type of data and the classification of that data within four Protection Classes that require different levels of access control.

Each Protection Class has both requirements and recommendations for facility design and organizational practices.

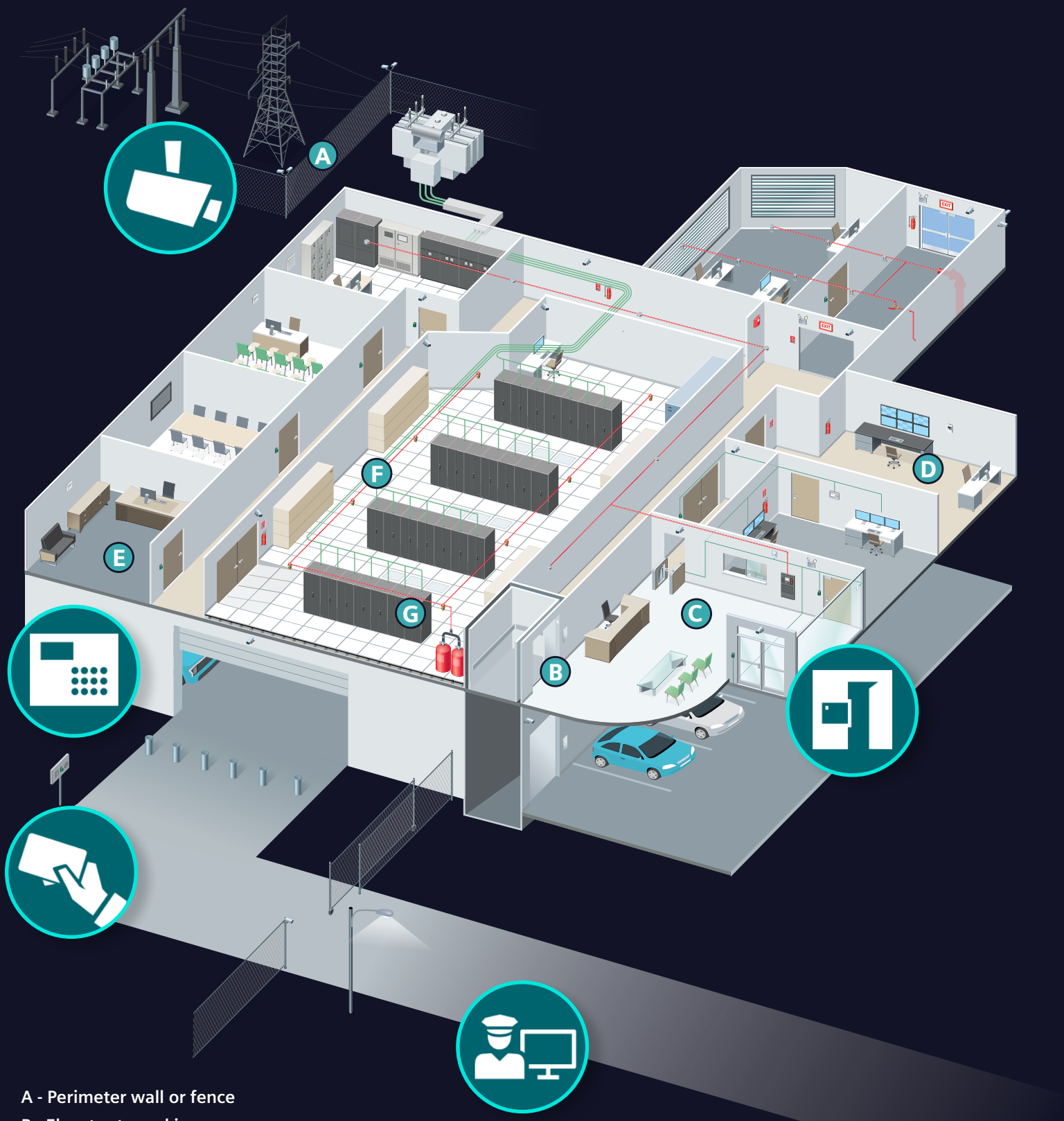
Requirements cover aspects such as:

- a minimum distance between parking areas and the data center
- use of video surveillance systems to monitor loading areas
- monitoring and control of the number of people and assets entering or leaving an area
- the ability to block unauthorized access to an area of a higher Protection Class

Recommendations include other steps that should be considered, such as:

- enhancement of lighting and hostile vehicle mitigation on approach routes
- fences and boundary controls
- perimeter and internal intrusion and hold-up alarm systems (I&HAS)

This paper also draws upon practices and innovations at some of the most advanced data centers in the world, including the Siemens Eagle DataCenter, which hosts 8 petabytes of highly valuable data across its main facility in Munich and three other sites around the world.



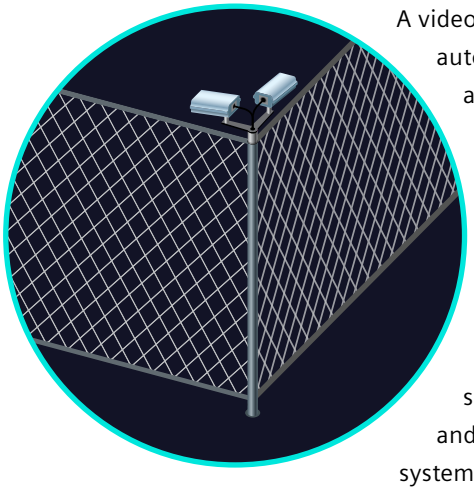

A - Perimeter wall or fence
B - Elevator to parking garage
C - Reception
D - Data center security office with Siveillance Video Monitor Wall
E - Manager's office
F - White and grey space
G - Server rack

# Table of Contents

**DATA CENTER SECURITY LAYERS**

# Layer 1: **Perimeter**

The perimeter of a data center is its first line of defense. In addition to architectural features such as fences, walls, bollards and lighting, it should include systems that allow security forces to detect and respond to threats while minimizing false alarms.



A video management system should allow automated monitoring, recording, analysis and tracking of threats. Wall, fence and ground sensors can trigger alarms and floodlights. Additionally, analytics can trigger defensive alarms for virtual fence line crossings, motion, person detection, or direction of travel. Proper security planning allows the security team to configure, operate and maintain all perimeter defense systems from one interface.

The Siemens portfolio includes many components for data center owners and operators to choose from when designing perimeter defenses, as well as a choice of management systems for administration from one interface.

Siveillance™ Video, available in four versions up to the most advanced, Siveillance Video Pro, allows security teams to manage and operate all cameras around the perimeter. It is available with essential perimeter security features including:

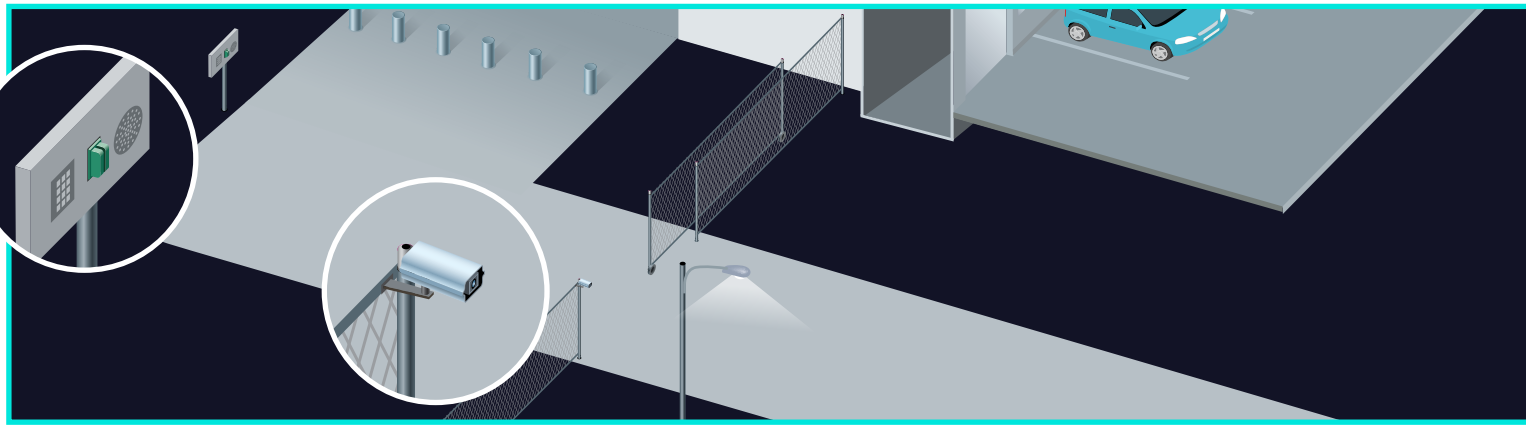
- Camera pan, tilt and zoom control
- Video monitoring wall
- Web and mobile clients for remote monitoring and management
- Automatic incident alarms
- Rule-based bookmarking of suspicious events
- Hardware-accelerated video decoding and motion detection
- Integration with SiPass integrated for access control and Desigo CC for electrical, fire and life safety and building automation management. For those data centers that are adopting the cloud, Siemens also has a cloud video offering, Siemens Video Cloud, that incorporates both access control and video

SiPass integrated, Siemens' flexible access control system, has a broad set of perimeter security capabilities, including:

- Unified management of video surveillance, intrusion detection and access control from one user interface
- Integration with cameras and motion detectors
- Integration with the Desigo CC single-interface building management platform for lighting, power, fire and life safety and mass notification

Siemens security management station, Siveillance Control, enables further integration and automation of perimeter security.

- Incident management across access control, intrusion detection and video surveillance
- Linking of related alarms and messages into a single event and with a proposed response
- Automatically generated action plans sent to users based on their roles, with monitoring of progress
- Computer-aided dispatch with tracking of security officers' locations



**DATA CENTER SECURITY LAYERS**

# Layer 2: **Gate**

The challenge of data center gate security is the need to keep traffic flowing while limiting entry to authorized staff, customers and visitors.

Security may be provided by both perimeter fence gates and parking garage entrances, with active barriers such as automatic bollards in between. In addition to or in place of staffed guard stations, access controls at each entry point may include license plate recognition, access card readers, remote visual verification of a driver's identity and two-way audio communication. Garage security may also require secure access to elevators. Real-time video monitoring is essential throughout.

Entrance security requires an access control system integrated with video management, alarms and a mass notification system. SiPass integrated, the Siemens access control system, plays a central role here and integrates with Siveillance Video. Desigo CC unifies these with building management systems, including gate and elevator controls and Desigo CC Mass Notification, within a single interface. For more automated incident management and decision support, all systems can be integrated with Siveillance Control security management stations.

SiPass integrated and Siveillance Video are available with several key features for data center entrance security.

**SiPass integrated**

- SiPass Identity, integrating SiPass integrated with Microsoft Active Directory
- Large-scale operation and management of card readers and cardholder data
- Watch list to flag security risks
- SiPass Identity self-service portal to automate access requests and streamline approval processes
- Integration with biometrics such as palm scans and facial recognition
- Integration with identity-based elevator control
- Support for multifactor authentication through access card/token, keypad, biometrics and mobile phone near-field communication (NFC)

**Siveillance Video**

- Two-way audio with audio recording
- License plate recognition
- Siveillance Video Monitor Wall
- Alarm configuration, management and handling, with 32,000 alarm priority levels
- Video verification of vehicle and driver against database records

**DATA CENTER SECURITY LAYERS**

# Layer 3: **Reception**

At reception, there can be a variety of systems for screening data center employees, colocation customers and visitors and granting access based on credentials. While keeping foot traffic flowing, these systems must prevent unauthorized entry and monitor who has entered the data center.

With or without staff on site, the reception area needs full-time video surveillance, employee and guest badge reading and physical barriers such as turnstiles. Increasingly, reception also includes health screening for life safety in the facility.

Entry control may involve multifactor authentication including access card reading, biometrics and remote visual verification through video. Several Siemens and partner products support these functions.

**SiPass integrated**

- SiPass Identity for access management through Active Directory
- SiPass integrated visitor management option: a single user interface for management of permanent and visitor access cards, card printing and locating visitors in the facility
- Support for palm or fingerprint scanners and integration with facial recognition systems
- Watch lists to flag individuals who might pose security risks
- Entry and exit logging
- Headcount feature to count all cardholders in emergencies
- Integration with fire safety systems

**Desigo CC**

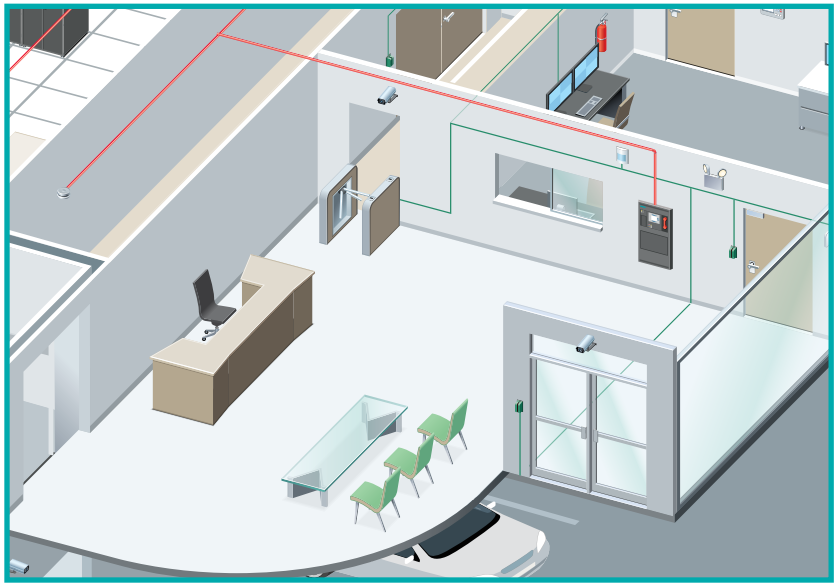
- Management of SiPass intgrated and Siveillance Video along with fire and life safety and building automation systems, including lighting and HVAC, through one interface

**Siveillance Video**

- Live video monitoring of reception unified with SiPass integrated
- Analytics alarming for unattended object detection, loitering, flow of traffic, aggressive behavior, and others
- Alarm management system displaying alarms by priority, with customizable instructions
- Two-way video kiosks for remote visual verification at check-in

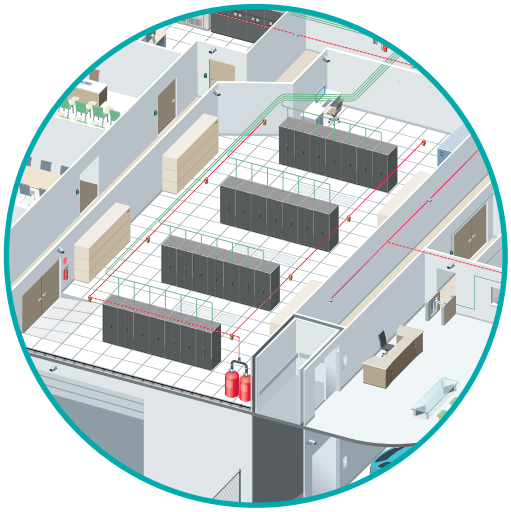
**welloStationX**

- Self-service, no-contact temperature screening kiosk integrated with SiPass integrated access control system and Siveillance Video
- Automated credential issuing: kiosk prints badge or issues pass status to permanent access card. If entrant has an elevated temperature, kiosk denies badge or disables card and alerts staff
- Health condition survey for each entrant at kiosk or via smartphone



**DATA CENTER SECURITY LAYERS**

# Layer 4: **White and grey space**



Data center uptime and integrity depend crucially on the security of the server rooms, or white space, where server, storage and network equipment reside and of the grey space, where the electrical and mechanical infrastructure resides. If intruders breach this area, they can shut down computing or cooling systems, damage or steal equipment or extract sensitive data.

Data center operators need to make white and grey space as available as possible to authorized employees, colocation customers and visitors while controlling access, dividing the space into zones for safety and security and controlling conditions to protect operations.

Defense requires intrusion prevention as well as environmental and life safety systems such as fire suppression and air temperature monitoring. The core products of Siemens data center security and building management provide all the functions needed. They allow operators to build strong protections against intrusions and disruptions while minimizing complexity and cost.

**Siveillance Video**

- Live video monitoring of entrances, exits and white space
- Allows for video verification of alarms from life safety systems
- Monitoring for unattended object and loitering detection
- Alarms displayed based on priority, with customizable instructions
- Recording and analytics for forensic review of incidents

**SiPass integrated**

- Support for role-based access control at doors by two-factor authentication, combining keypads, RFID card or token readers, NFC by mobile phone, and biometrics
- Escort control feature requiring two cards to prevent unaccompanied entry
- Entry and exit logging
- Anti-passback control to prevent two persons from entering with the same card
- Per-room roll call for security and emergency response
- Door interlocking to maintain secure “air locks” between designated doors

**Desigo CC**

- HVAC, fire and life safety, power, lighting and environmental monitoring (temperature, humidity, dust, CO2, fire detection) integrated with SiPass integrated access control and Siveillance Video
- Desigo CC Mass Notification for response to emergencies

**Siveillance Control**

- Automated and advanced incident handling

**DATA CENTER SECURITY LAYERS**

# Layer 5: **Server rack**

Defense against service disruptions and data theft must extend to individual racks within a data center, especially a colocation center where customers own and operate their equipment. Protecting each customer from attack and all data center users from disasters is a major responsibility of owners and operators.

Cabinet access may be controlled through use of RFID card and token readers, keypads and biometrics such as palm and fingerprint readers. In many data centers, cage security also includes wireless locks integrated with access control software. The Siemens data center portfolio includes specific features that can play important roles in server rack protection.

**SiPass integrated**

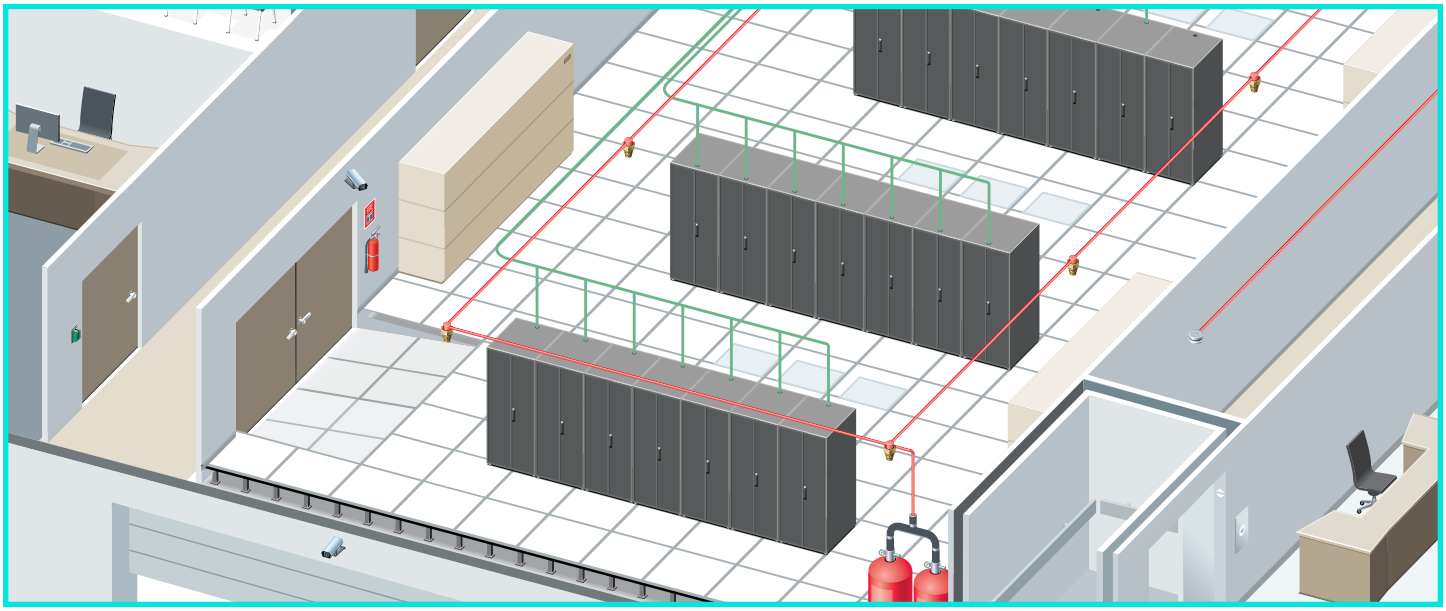
- Tenancy functionality that allows multiple companies to use the access control system independently
- Role-based access control
- Door alarms to warn when a server cabinet is left open, or if multiple cabinets are opened at the same time.
- Integration with wireless cabinet locks
- Integration with Siveillance Video

**Siveillance Video**

- Monitoring and recording of activity at server rack
- Analytics and motion detection with alarms
- Two-way audio communication
- Unattended object detection for equipment left behind

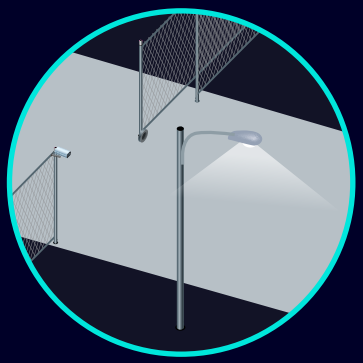
**Desigo CC**

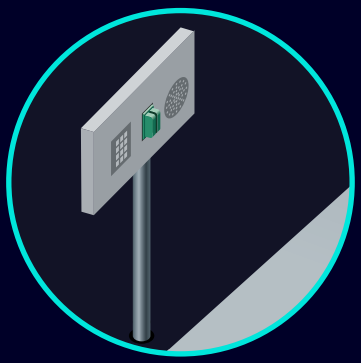
- Server rack temperature, moisture, occupancy and closure sensor monitoring integrated with SiPass integrated access control

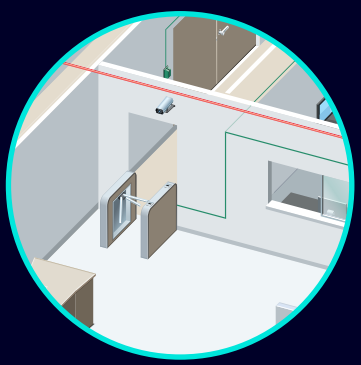


# Use case **scenarios**

To illustrate how the five layers of security in a data center protect operations and assets, the following use cases describe four possible journeys through a data center.







**Data center full-time employee**
A high-level manager for the data center owner-operator arrives at any hour and has full facility access.

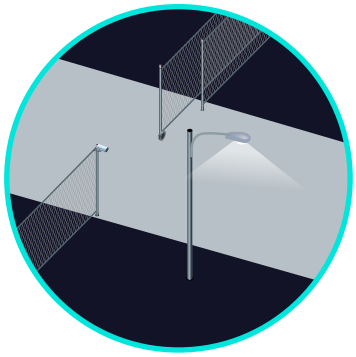
1. The manager drives up to the gate. Her vehicle is tracked by automated cameras at the perimeter fence and detected by Siveillance Video.

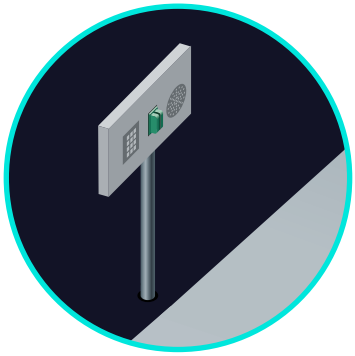
2. At the gate, a camera focuses on her license plate and Siveillance Video recognizes it. SiPass integrated authorizes opening the gate based on her role as defined in SiPass Identity through Active Directory.

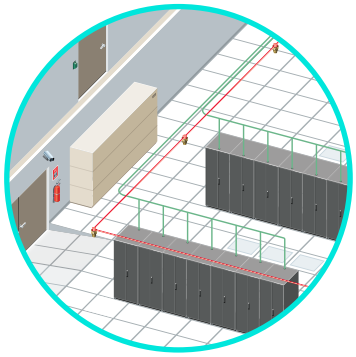
3. The manager drives to the garage door, holds up her mobile phone with an NFC SIM card to an NFC reader and also enters a PIN on a keypad, both unified with SiPass integrated. The garage door automatically opens.

4. After parking in the garage, the manager walks into an elevator, taps her RFID access card on a card reader and holds her hand up to a palm scanner to authenticate her identity. Integration between SiPass integrated and Desigo CC applies access control to the elevator control system.

5. After being admitted at the reception area, she uses a card reader and looks at a facial recognition camera to enter an “air lock” hallway. Once that door has closed behind her, she can use her card to open the door at the end of the hallway and enter her office.







**Customer**

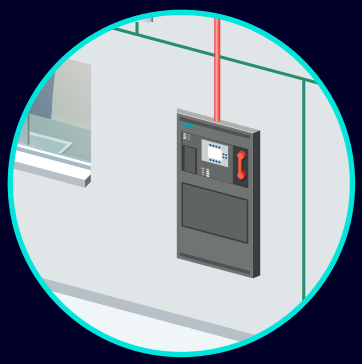
A technician for a company that operates its servers and storage in the data center comes to install new equipment and gets access to the cage assigned to his company.

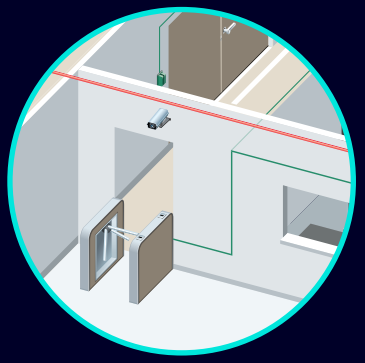
1. The technician drives up to the gate. Siveillance Video recognizes his license plate, which he provided while requesting access through the SiPass Identity Self-Service Portal, and the gate opens.
2. At the garage entrance, he identifies himself to an off-site guard over an intercom and is admitted to the garage.
3. After parking, he takes the elevator to the reception level. He checks in at reception by presenting his access card, which per his request allows him to enter the zone of the data center where his company's server rack is located. The reception area is unstaffed but remotely monitored through Siveillance Video.
4. Next, the technician checks in at a welloStationX temperature screening kiosk integrated with SiPass integrated. After the kiosk determines his temperature is safe, it assigns pass status to his access card.
5. After using his access card and having his palm scanned to enter the data center's white space through two separate doors, the customer goes to his company's server rack. He uses his card and a PIN to open the server cage and installs a server, but he forgets to close the gate before walking away.
6. Siveillance Video detects the open, unattended gate and a tool the customer left on the floor in front of it. Siveillance Video delivers a medium-priority alarm to the data center security office on the same interface used for managing SiPass integrated access control. The security guard correlates the alarm to the customer and alerts him over a two-way audio connection.

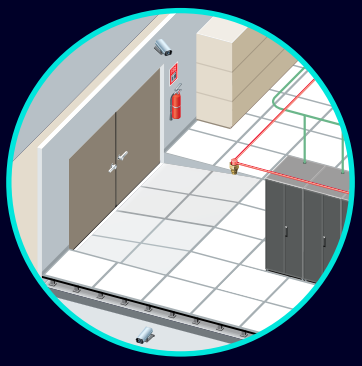
**Authorized visitor**

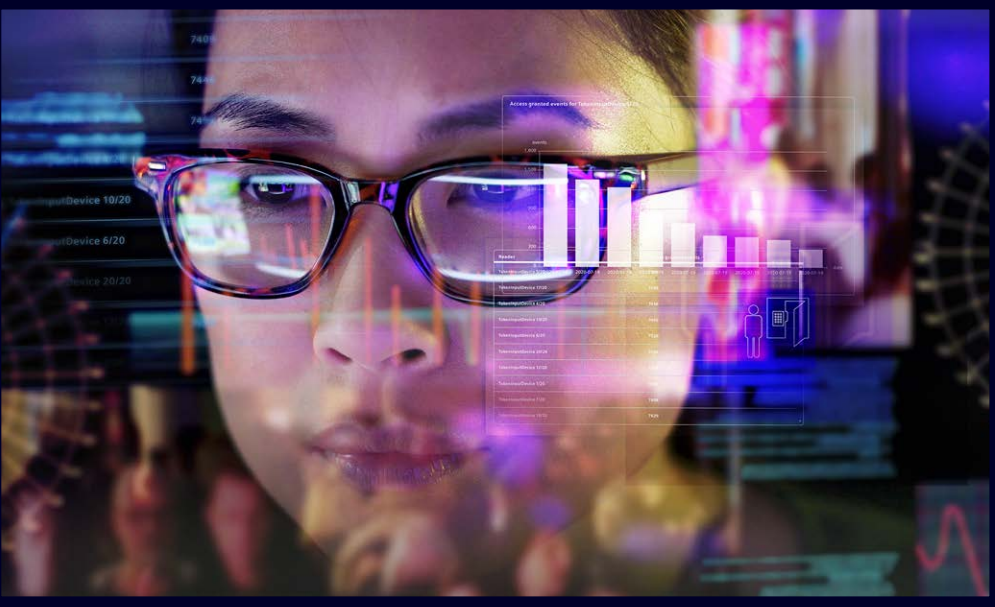
An inspector makes a one-time visit to approve an equipment configuration in the data center and is granted temporary access with an escort.

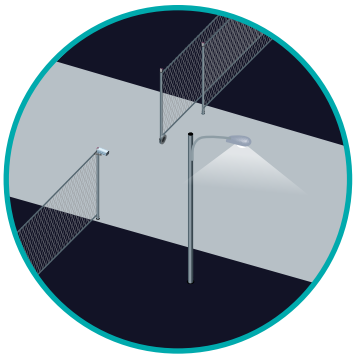
1. Arriving at reception, the inspector speaks to an off-site guard via a two-way video kiosk. The guard prints out a temporary access card at the kiosk and directs her to the welloStationX kiosk, which reads the inspector's temperature as normal and prints out a temporary badge.
2. The off-site guard summons a supervisor to escort the inspector into the server room, an area defined in SiPass integrated as requiring an escort for visitor access. At each door on the way into the server room, both the supervisor and the inspector present their access cards to unlock the door.
3. The inspector completes her work accompanied by the supervisor, who then escorts her out.

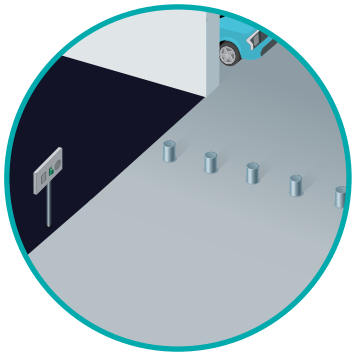


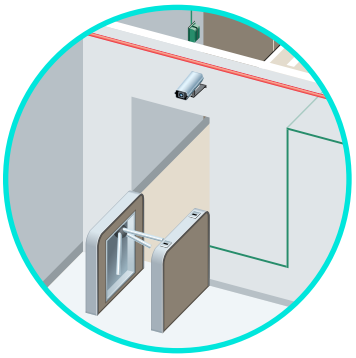












**Unauthorized visitor**

An unapproved visitor arrives after dark without an appointment and is flagged as a potential threat to data center security.

1. A car approaches the perimeter fence and stops at the gate. Siveillance Video reads its license plate, which is not approved for entry, and sends an alarm to security staff. Through integration with Desigo CC, additional floodlights around the gate are turned on. A guard addresses the driver via two-way audio while Siveillance Video cameras show all activity live on a monitor wall in the data center and record it for later analysis.
2. If the car rams the gate, retractable bollards automatically go up in the driveway between the gate and parking garage. Siveillance Video automatically issues a higher-level alarm and Desigo Mass Notification alerts all employees, customers and visitors in the data center. On-site guards respond on the scene.
3. If an unauthorized visitor enters at reception and does not immediately check in, turnstiles remain locked. Siveillance Video detects the activity and issues an alarm, triggering a live response by guards. If there is an on-site receptionist who feels threatened by the visitor, the receptionist can use a duress button to call for a live security response.

Desigo CC centralized command and control

# **Unified management** is critical to data center security

As illustrated in this paper, implementing a comprehensive data center security strategy can mitigate risks, secure customers' data and prevent service interruptions and data breaches caused by intruders. Such a strategy requires many tools to secure the facility at several layers, from the perimeter and outer gate to the cabinets housing servers and storage. Unified management, like that provided by Siemens integrated data center portfolio, is essential for all-encompassing site protection. Having access control, video surveillance, identity management, building automation, alarms and other systems unified under a single user interface increases situational awareness and helps data center operators respond to and track all events and actions. Data center operations secured by integrated management proceed safely and without interruption, ensuring customer trust and user confidence.

The Siemens data center portfolio integrates comprehensive security systems with unified management to meet the challenges of protecting people and assets, increasing efficiency and ensuring business continuity and compliance. Siemens is your trusted partner for end-to-end data center solutions, from security to power management and all other infrastructure and operations requirements. Learn more about Siemens data center solutions at usa.siemens.com/datacenters or contact a Siemens data center specialist to discuss your needs.

**Siemens Industry, Inc.**
1000 Deerfield Parkway
Buffalo Grove, IL
United States of America

usa.siemens.com/datacenters

Order No. 153-SBT-1344