SIEMENS

DATA CENTER SECURITY

Maximize your reputation by minimizing downtime

siemens.com/datacenters

Introduction

Staying connected has never been more important. As borders closed amid a global pandemic, people around the world turned to the internet for their daily work, entertainment and to stay in touch with family and friends. The internet has become the core foundation through which information is shared and consumed in today's modern society. At the beginning of 2021 there were 4.66 billion people[1], close to 60% of the global population, using the internet. So, it's no surprise that the need for uptime in data centers is crucial as access to data becomes the basis of business continuity.

Yet, according to the Uptime Institute's 10th annual data center survey[2], **a third of survey participants admitted to experiencing a major outage in the previous 12 months, with 31% stating this had led to "substantial financial and reputational" damage.** Among the causes of a hundred of major public outages tracked by the analyst firm during the period of January 2016 to June 2018, security-related outages accounted for 6% of failures, followed by 5% for fire and 1% for cooling or mechanical. Four percent of respondents reported an average cost of an IT outage being higher than $5 million.

According to a study conducted by Ponemon Institute and sponsored by Centrify (2017), the impact of data breaches on reputation and share value is high. **Companies experienced an average stock price decline of 5% immediately following the disclosure of their breach.** Those who declared a high security posture took an average of 7 days to recover. Companies with low security posture that did not respond quickly to the incident experienced a stock price decline that on average lasted more than 90 days.

Organizations with a poor security posture were more likely to lose customers. In contrast, a strong security posture supports customer loyalty and trust. With the extent of potential financial and reputational damage, data center owners and operators need to ensure they leave no stone unturned in their pursuit to minimize downtime.

[1] Global digital population as of January 2021 (in billions)

[2] Uptime Institute's 10th annual data center survey

Table of contents

Physical security in data centers

Standards and norms' landscape for data centers has rapidly reshaped during the last years. Different government' bodies and industry associations have pushed for a physical security standardized approach: European Union norm EN 50600 published in 2016, became International Standard Organization (ISO) norm 22237 in 2018. The Telecommunication Industry Association (TIA) published its standard TIA-942-B in 2017. All of them cover aspects of data center physical infrastructure, including physical security.

A security incident in a data center facility can affect different tenants, with consequent impact on their business continuity. Therefore, access control measures are required to avoid unauthorized people to manipulate data center resources that could compromise the reliability of the physical infrastructure and affect the service availability.

According to the ISO standard, requirements for operational security should be determined by the organization responsible for data center assets. The requirements should be determined following a risk assessment based on the threats posed to the data and the "classification" of that data. The standard applies four protection classes to feature increasing levels of access control. Every protection class is qualified by requirements and recommendations.

Requirements are focused on construction aspects and organization processes, including: segregated routes for employees, visitors, and deliveries; minimum distance between the parking areas and the data center; use of

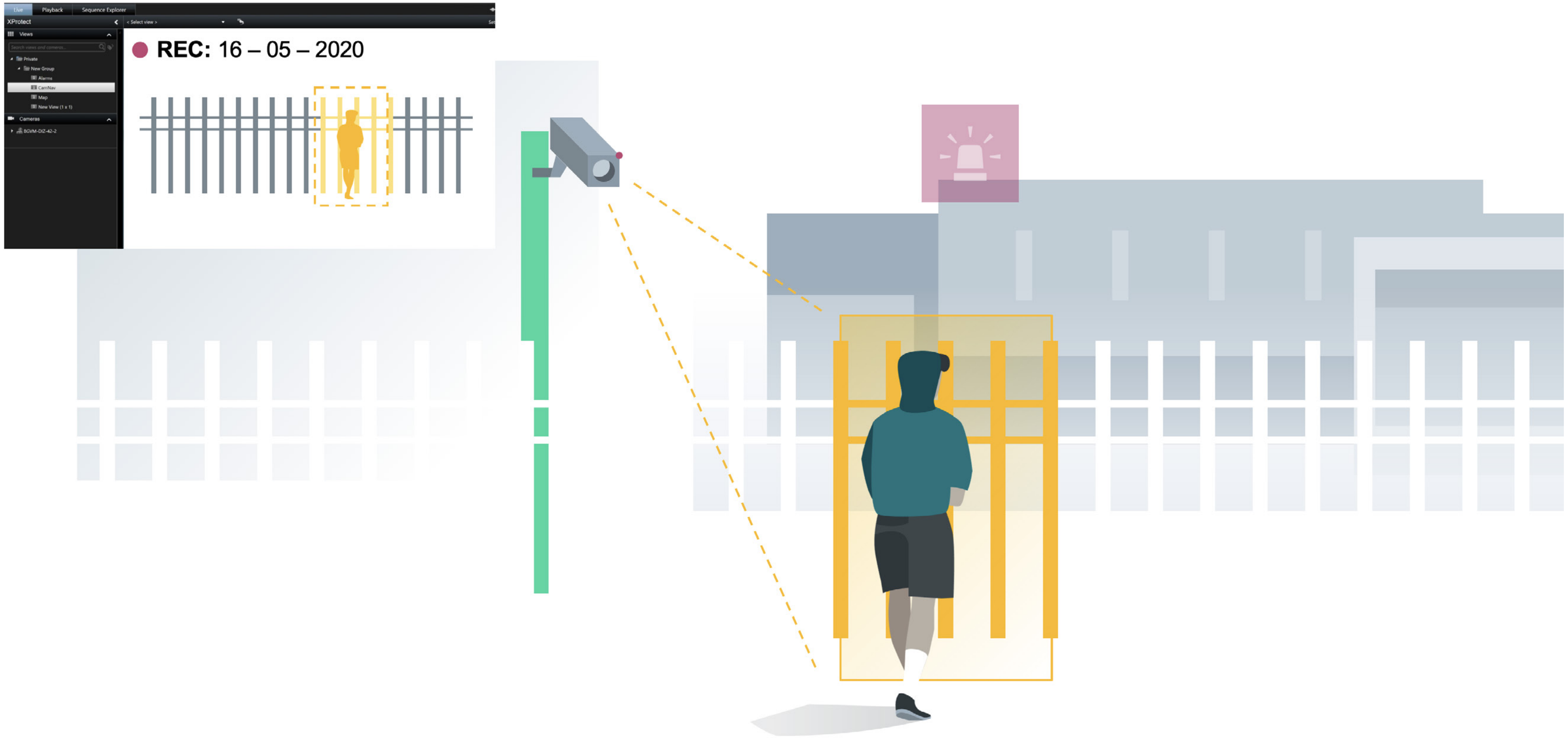
VSS to monitor the loading/unloading areas; detection and prevention of both “undesirable or unnecessary access between areas of the same Protection Class” and “unauthorized access to an area of a higher Protection Class”; monitoring and controlling the number of people and assets entering and leaving any area.

Recommendations include aspects that should be considered to enhance protection, like: enhancement of lighting system and hostile vehicle mitigation on approach routes; fences and boundary controls; secondary access routes as backup routes; parking areas outside the boundaries of the data center with access control for vehicle occupants; perimeter and internal I&HAS; restrictions for general personnel to areas of Protection Class 2, except in emergency situations; use of VSS for areas of Protection Classes 2 to 4; the boundary of Protection Class 4 should not be collocated with boundaries to Protection Classes 1 or 2.

Automation and control of different technologies (e.g. lighting, VSS, I&HAS, access control, alarm monitoring) is key to respond rapidly and effectively to threats. This whitepaper will illustrate security use cases in data centers and will focus on a management platform that can provide data center operators the highest levels of physical security.

Use case 1: **Perimeter security**

When a suspect approaches and touches the fence, an alarm will be triggered. The surveillance camera will track and trace the suspect. Video analytics can be applied to monitor loitering, object detection and combinations of zone detection. Both systems complement each other to strengthen security measures and reduce false alarms around the perimeter of your data center.

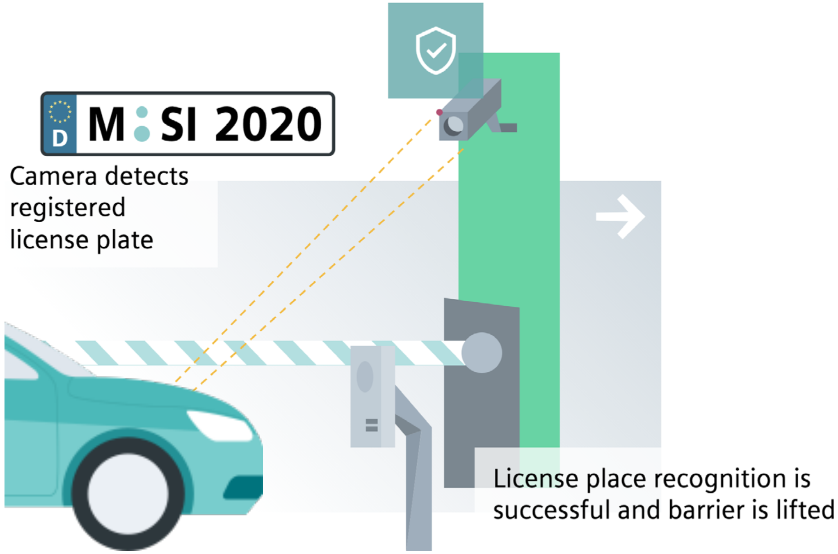


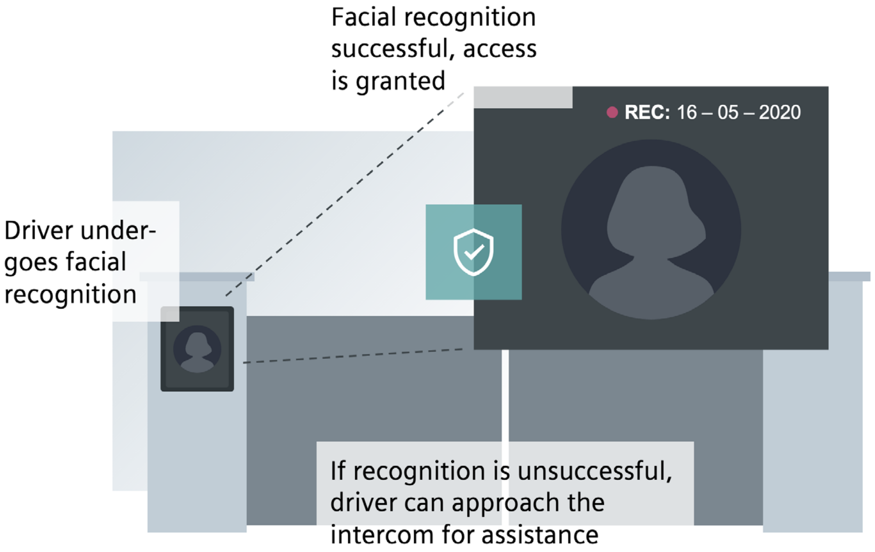
Use case 2: **Gate security (parking area)**

When a vehicle approaches the gate, the security camera will detect the registered license plate. The barrier will be lifted after successful license plate recognition. Moving forward, the driver of the vehicle will undergo facial recognition and when the facial recognition is successful, access is granted to the parking lot automatically. In case facial recognition is not appropriate due to difficult light situations a RFID card or a mobile phone can be used for authorization.

If the access request is unsuccessful, access will be denied and the driver of the vehicle can approach the intercom for assistance.

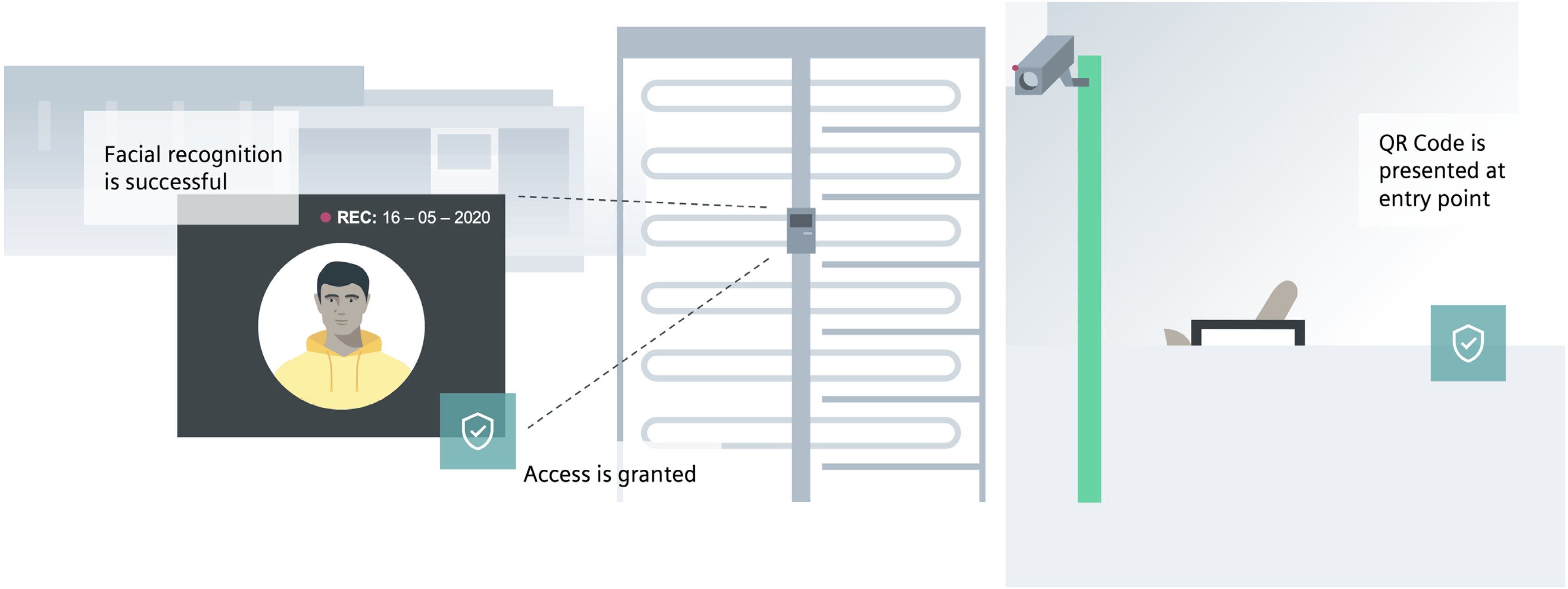
To avoid that a driver of a vehicle forces the entrance despite access denial, the ISO standard recommends hostile vehicle mitigation measures on the data center approach routes.


D
M SI 2020
Camera detects registered license plate
License place recognition is successful and barrier is lifted

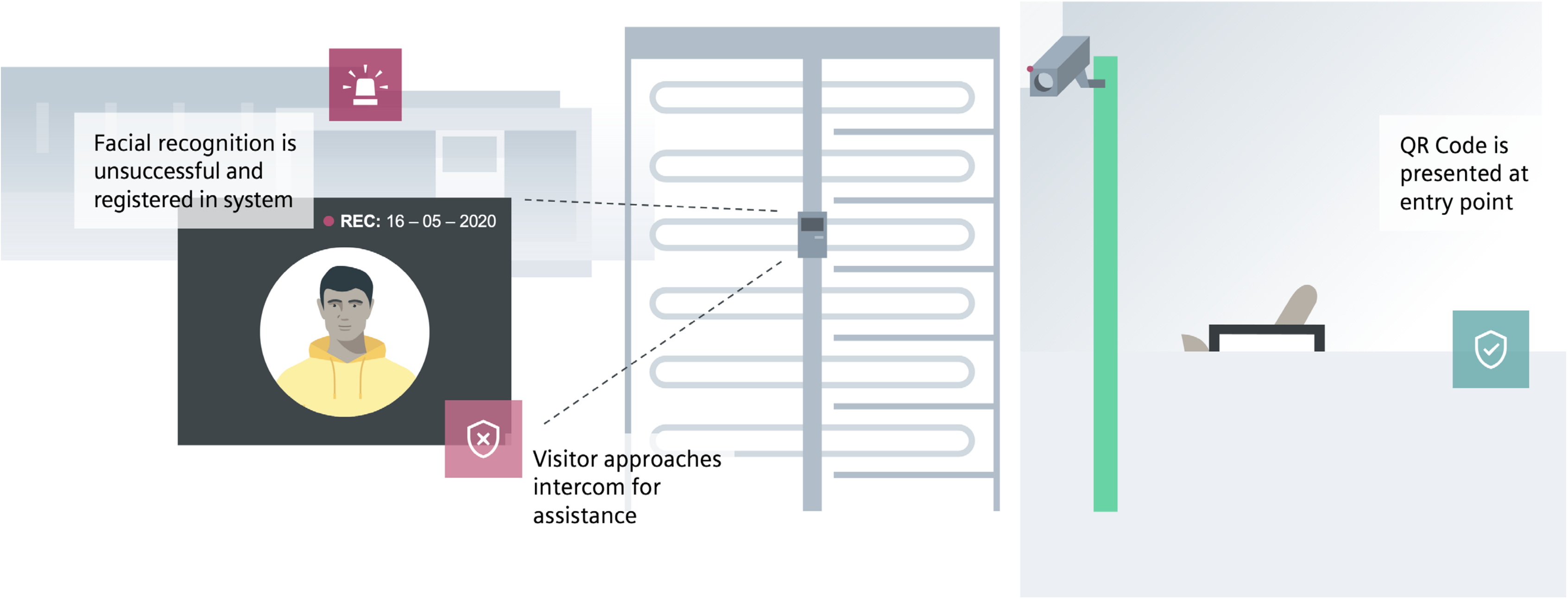

Facial recognition successful, access is granted
REC: 16 – 05 – 2020
Driver undergoes facial recognition
If recognition is unsuccessful, driver can approach the intercom for assistance

Use case 3: **Gate security**

Upon arrival, the visitor will show a QR code to a reader installed at the entry point. If the first authentication will succeed, a security camera will initiate facial recognition. Once the task is completed and the visitor is registered in the system, access will be granted within the data center area.

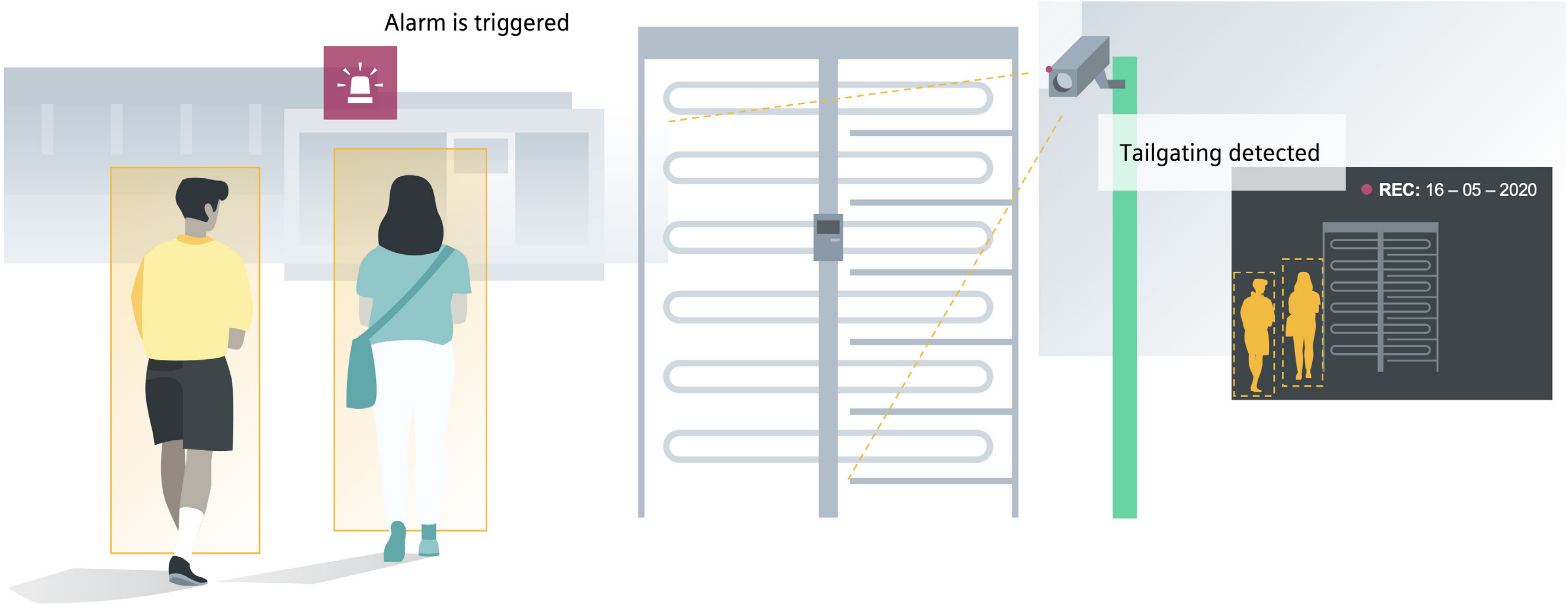

Facial recognition is successful
REC: 16 – 05 – 2020
Access is granted
QR Code is presented at entry point

In case of negative response from the system, access will be denied, and a log will be registered in the system. The visitor can approach the intercom for further assistance.



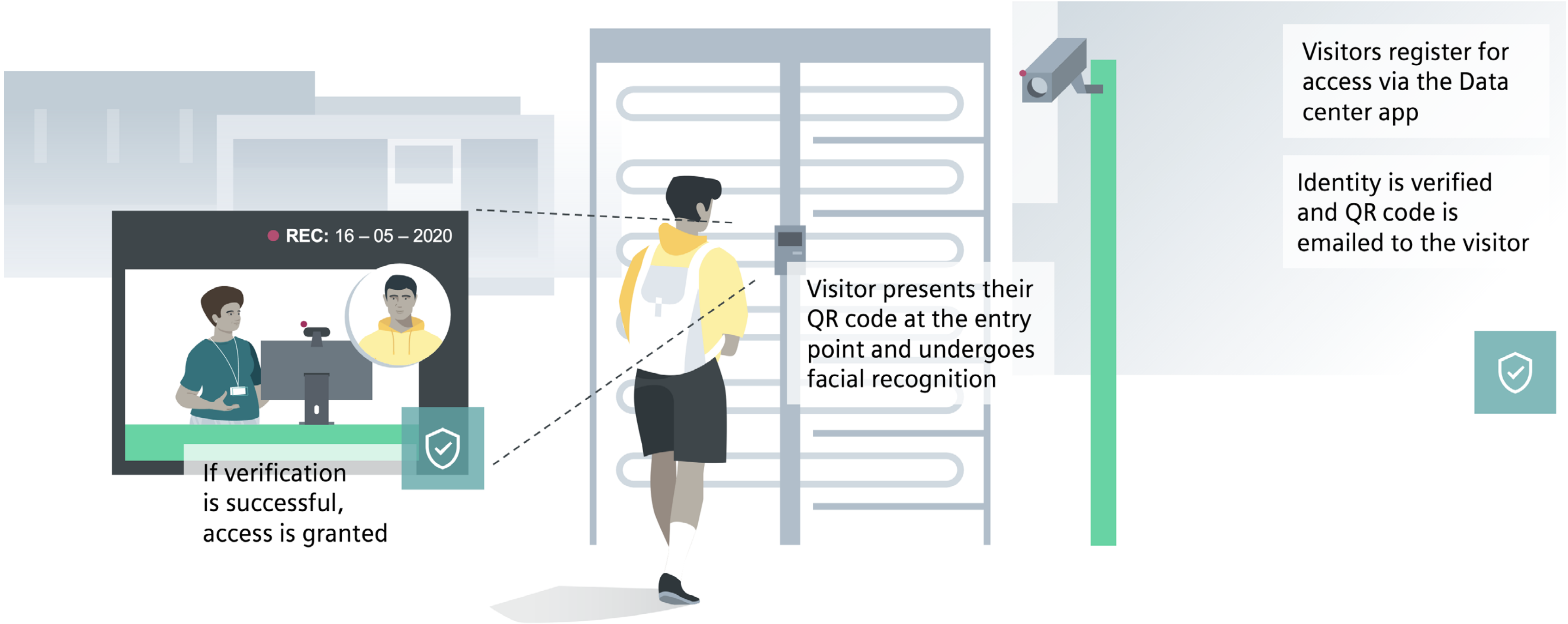
Facial recognition is unsuccessful and registered in system
REC: 16 – 05 – 2020
Visitor approaches intercom for assistance
QR Code is presented at entry point

In case of tailgating (a physical security breach in which an unauthorized person follows an authorized individual to enter a secured premise), an alarm will be triggered by the security cameras and authorities will be informed immediately to assess the situation.



Use case 4: **Data center visitors**

Visitors entering the data center can register for access via the Data Center Identity Management application. A QR Code will be emailed to the visitor after verification of their identity. The visitor can then present their QR Code at the entry point and undergo facial identification. Access will be granted after facial recognition is successful.



Visitors register for access via the Data center app

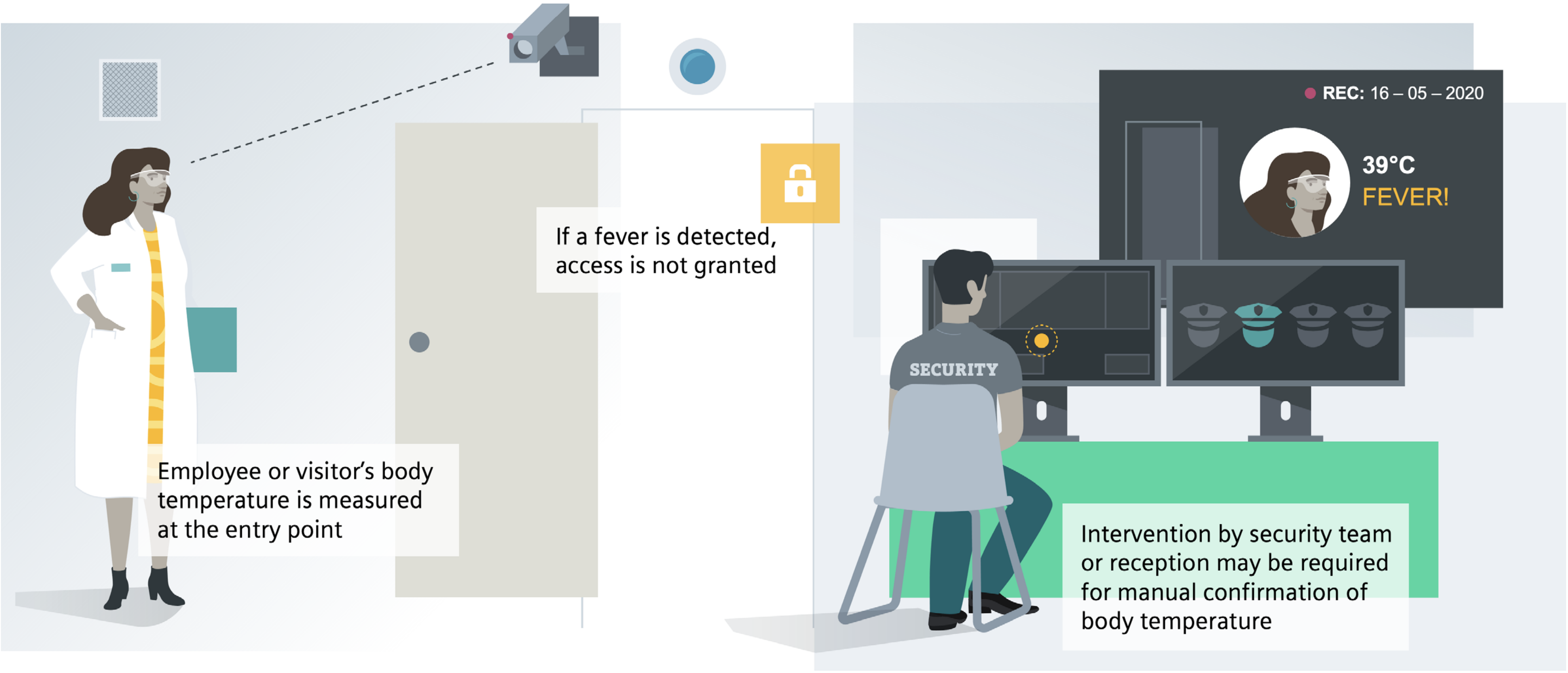
Identity is verified and QR code is emailed to the visitor

Visitor presents their QR code at the entry point and undergoes facial recognition

If verification is successful, access is granted

Use case 5: **Covid-19 mitigation measures**

Before entering the premise, the employee or visitor's body temperature will automatically be measured via thermal imaging camera at the access point. If a fever is detected, access will not be granted. Further intervention and assistance by the security team may be required for manual confirmation of body temperature.



Employee or visitor's body temperature is measured at the entry point

If a fever is detected, access is not granted

Intervention by security team or reception may be required for manual confirmation of body temperature

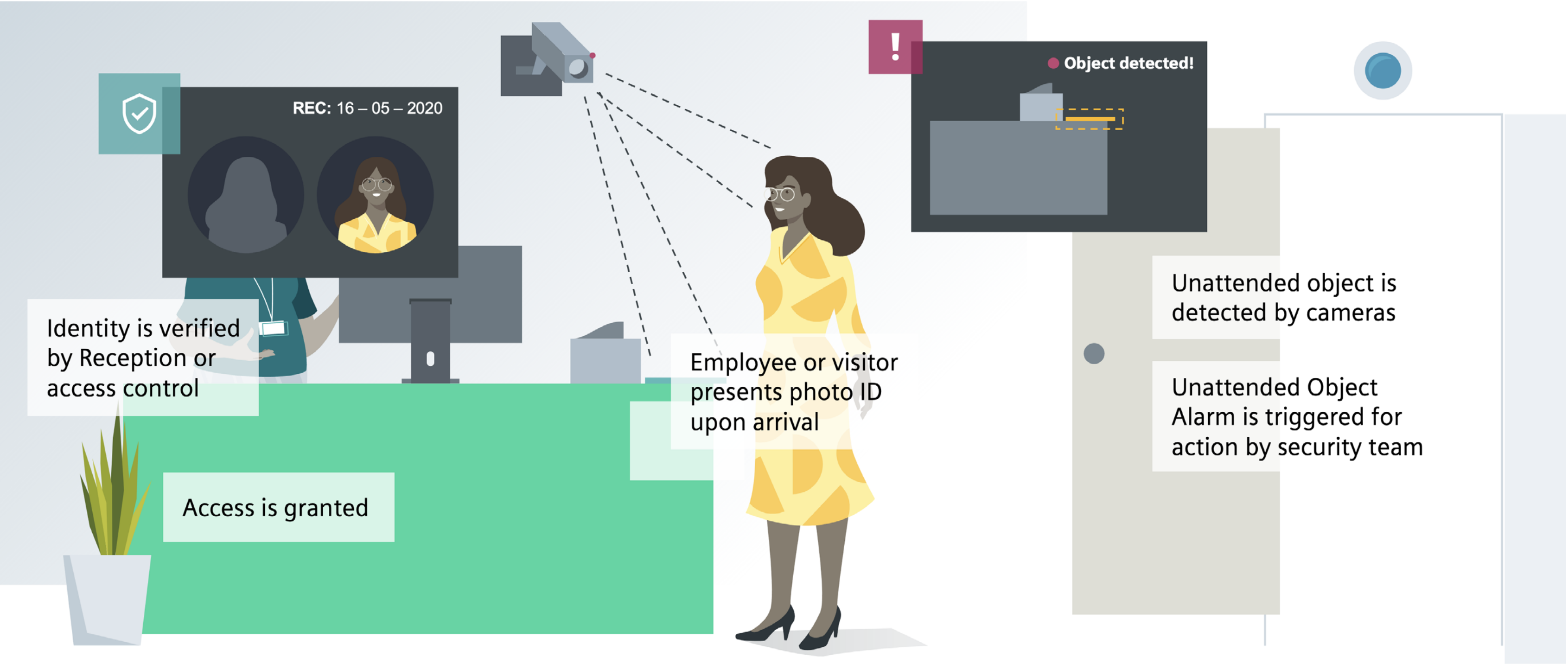
Use case 6: **Reception security in building (Threat)**

If an employee feels under threat by a suspect, the duress button could be activated. Upon activation of the duress button, the security team will immediately be deployed on location to assist and keep the situation under control.

Duress button
is activated
Employee feels under
threat by suspect
SECURITY
Security team is
deployed on location

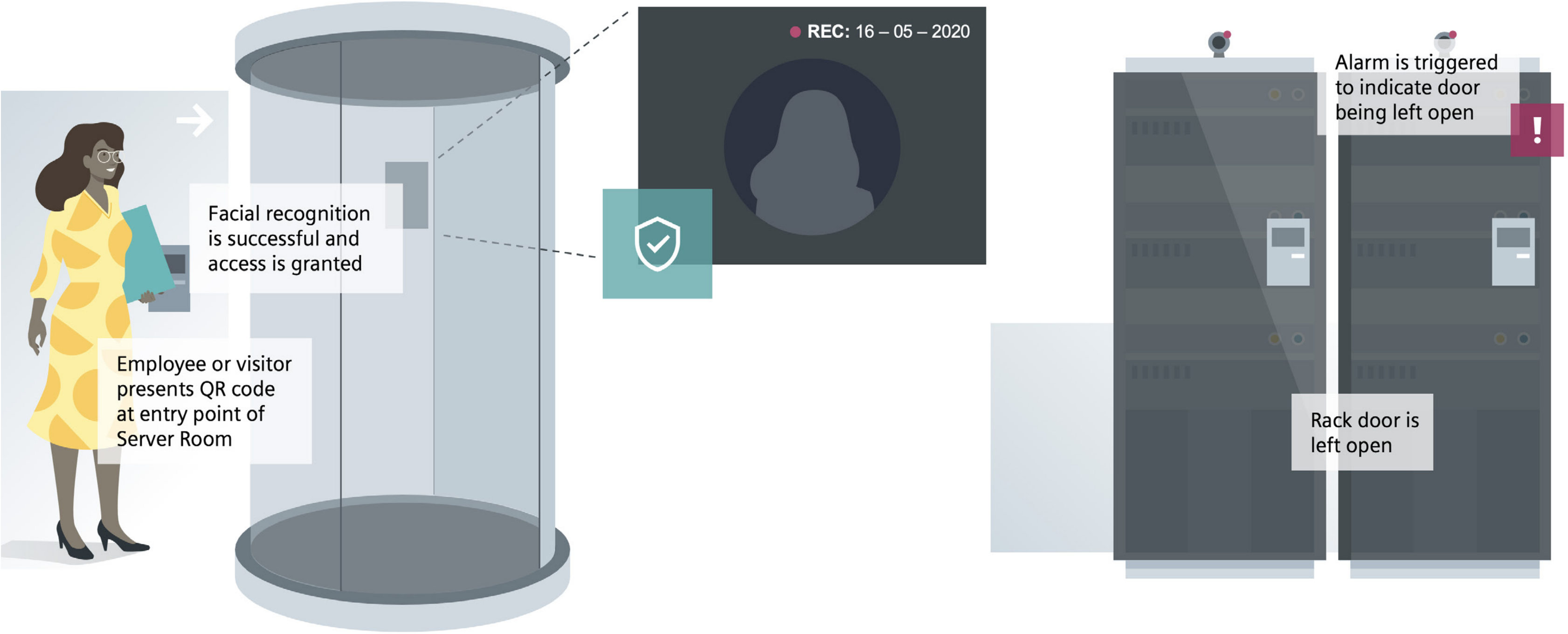
Use case 7: **Reception security in building (Face detection)**

Upon arrival at the entry point, the employee or visitor will present their photo ID for verification of identity. Once verification is done by either reception or access control, access will be granted. If there are any unattended objects at the reception area, it will be detected by cameras and the Unattended Object Alarm will be triggered for action by the security team.


REC: 16 – 05 – 2020
Object detected!
Identity is verified by Reception or access control
Employee or visitor presents photo ID upon arrival
Unattended object is detected by cameras
Unattended Object Alarm is triggered for action by security team
Access is granted

Use case 8: **Entering the white space**

Before entering the server room, a QR code will be required at the entry point. Once facial recognition of the employee or visitor is successful, access will be granted. Access credentials are also required to open the server rack. In addition, an alarm will be triggered when a rack door is left open and authorities will be notified.


REC: 16 – 05 – 2020
Facial recognition is successful and access is granted
Employee or visitor presents QR code at entry point of Server Room
Alarm is triggered to indicate door being left open
Rack door is left open

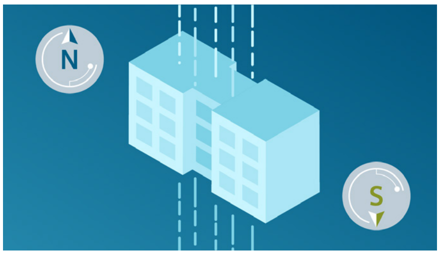
Use case 9: **Access to server racks**

When an alarm is triggered to indicate that a server rack door is left open, the rack door must be closed before accessing another rack. Employees or visitors will need to enter access credentials to access any rack and rack doors will only open upon verification. Any unattended objects in the data center will be detected by cameras and the Unattended Object Alarm will be triggered for further action by the security team.

The role of management platforms

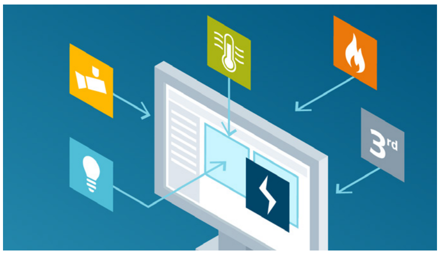
With a security management platform, all different security subsystems installed at a data center are harmonized under one common user interface. Verification actions assure the validity of fire and security alarms. Additionally, site plan information and integrated maps give the operator best possible situational awareness helping to keep track of all events and actions. Therefore, a security management platform is key in a security operations center if incidents need to be resolved in the most efficient manner.

When it comes to people or assets protection, preserving business continuity, compliance or increasing business resiliency and efficiency at data centers, Siemens has the right management platforms to meet your security needs regardless of the size of your business. Developed with an open, modular, and fully scalable architecture, users benefit of an intuitive UI, long term investment protection, maximum flexibility, and satisfaction.



Open platform

Desigo CC supports natively all major protocols to connect to most of building devices and exchange information with other systems, including Cloud applications. Furthermore, it provides SDK and API to build custom solutions to meet any customer requirements.

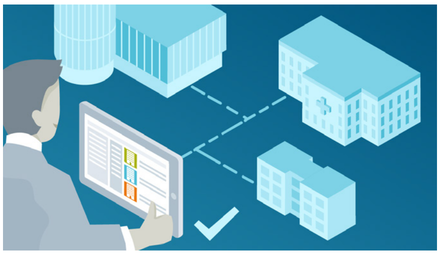


Modular and flexible design

Desigo CC can be configured as a combination of different systems, disciplines or applications to meet any project requirements. The modularity and flexibility of Desigo CC protect your investments and help you plan the future of your operations.

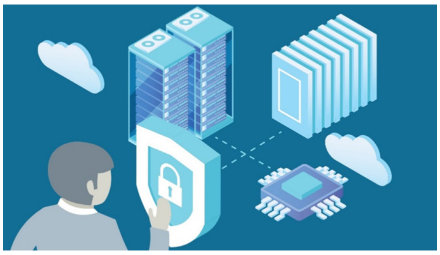
Efficient engineering

Desigo CC minimizes engineering tasks with configuration wizards, comprehensive libraries, automatic graphic generation, and consistent workflow across disciplines. Innovative engineering concepts drastically reduce time for commissioning and training.



Easy operation

Operators are supported in their daily operations with a workflow-oriented UI, assisted event handling and automatic reports of a building’s performance. Desigo CC can also be operated from any device and location by using the touch-responsive Flex Client.



Cybersecurity in mind

Each Desigo CC release provides improved cybersecurity. Penetration tests are done with every new versions to ensure compliance with latest standards. Siemens advising continuous improvement of the cybersecurity with Siemens Product CERT and Siemens CERT.

Facts and figures

According to the Uptime Institute's 10th annual datacentre survey, a third of the survey participants admitted to experiencing a major outage in the previous 12 months, with 31% stating this had led to "substantial financial and reputational" damage. – (2020). Weblink

Combining with the finding that a greater percentage (48%) of outages now cost firms between $100,000 and $1m more than they did in 2019 (28%), the Uptime Institute said the data reinforces the view that outages are becoming increasingly expensive events for firms to overcome. – (2020). Weblink

According to this year's report by Information Technology Intelligence Consulting, an hour of downtime on average costs data center operators $260,000, while a five-minute outage costs just $2,600. – (2018). Weblink

Outages continue to cause significant problems for operators. Just over a third (34%) of all respondents had an outage or severe IT service degradation in the past year, while half (50%) had an outage or severe IT service degradation in the past three years. – (2019). PDF

According to Gartner, downtime costs $5,600 per minute on average. This results in average costs between $140,000 and $540,00 per hour depending on the organization. – (2018). Weblink

According to a 2018 survey by Uptime Institute, 31% of respondents experienced a downtime incident or severe degradation in the last year and 48% reported at least one outage at their site or at a service provider in the last three years. – (2018). PDF

According to a 2018 survey by Uptime Institute, half of the reported incidents cost under $100,000, there were 41 outages that cost more than $1m (15%) and about one-third of outages reported by respondents cost over $250,000. – (2018). PDF

The erosion of consumer trust and confidence may compel customers to reevaluate services and switch to a different vendor to meet their needs, resulting in immediate loss of business. It also dissuades sales leads from choosing the business over its more reliable competitors. The most difficult effect to measure is how many future customers who would have considered a company previously will begin to look elsewhere to meet their business needs. – (2019). Weblink

Unplanned system downtime can incur massive costs that go far beyond "mere" financial concerns, inflicting long-term brand damage and denying future opportunities. – (2019). Weblink

Based on an average reported incident length of 90 minutes, the average cost of a single downtime event was approximately $505,500. These costs are based on a variety of factors, including but not limited to data loss or corruption, productivity losses, equipment damage, root-cause detection and recovery actions, legal and regulatory repercussions, revenue loss and long-term repercussions on reputation and trust among key stakeholders. – (2011). PDF

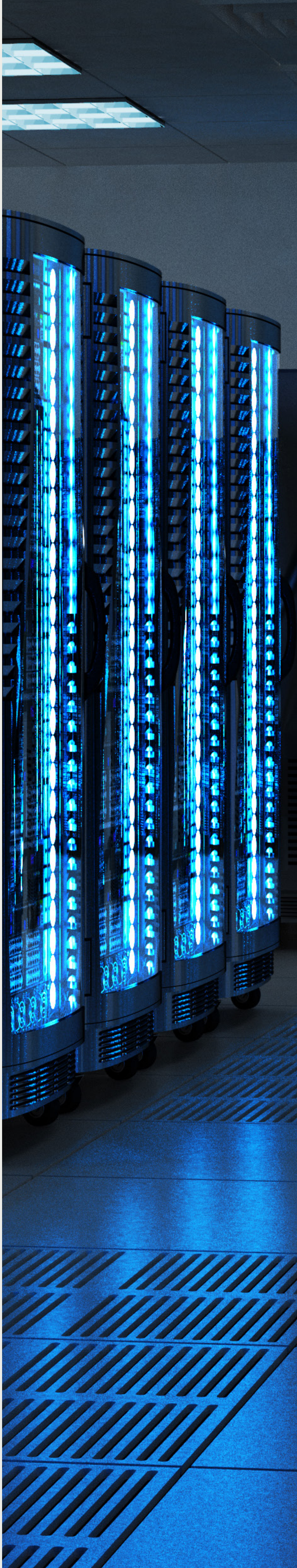
When considering that the typical data center in the United States experiences an average of two downtime events1 over the course of two years, the costs of downtime for an average data center easily can surpass $1 million in less than two years' time. – (2011). PDF

Smart Infrastructure intelligently connects energy systems, buildings and industries, enhancing the way we live and work to significantly improve efficiency and sustainability.

We work together with customers and partners to create an ecosystem that both intuitively responds to the needs of people and helps customers achieve their business goals.

It helps our customers to thrive, communities to progress and supports sustainable development to protect our planet for the next generation.

Creating environments that care.
siemens.com/datacenters



Published by
Siemens Switzerland Ltd

Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.