BEST PRACTICES FOR DATA CENTRE SECURITY AND EFFICIENCY.

A **WHITE PAPER** POWERED BY BOON EDAM

BOON EDAM
YOUR **ENTRY** EXPERTS.

UNDERSTANDING THE STRATEGIC APPLICATION OF SECURED ENTRY SOLUTIONS TO PROTECT DATA, MAINTAIN COMPLIANCE, AND IMPROVE OPERATIONAL EFFICIENCY.

In the world of data centre management, security professionals are guided by three crucial imperatives that influence their strategies and decisions:

1. **Protect Sensitive Assets**: Safeguarding data is just one aspect of protecting data centre assets. It also includes ensuring physical security for people, property, and other critical assets within the data centre environment.

1. **Maintain Regulatory Compliance**: Adhering to industry and government regulations requires a multifaceted approach. Data centres must meet current compliance standards and remain adaptable to evolving regulatory landscapes.

1. **Overcoming Rising Costs**: The rising costs of energy, land, labour, and critical infrastructure supply chain are a challenge for data centres. To ensure the availability of services, competitive pricing, and sustained profitability, data centres must identify and eliminate inefficiencies.

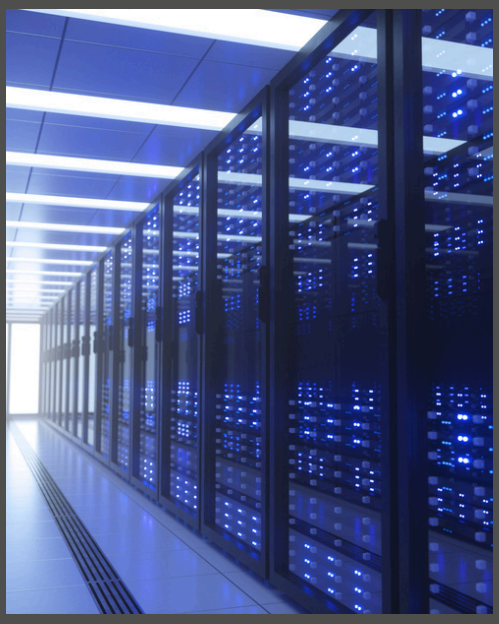
The strategic application of secured entry solutions is invaluable in bringing these imperatives together under a single budget line item.

Understanding the Various Types and Entry Processes for Data Center Security Entrances

As you move towards a facility's critical infrastructure, securing access points becomes increasingly important. Implementing a "layered" strategy with increasing security levels and protecting each step towards the most sensitive areas is the best way to safeguard a data centre's assets, people, and compliance reputation. While each data centre and colocation is unique, the following outline provides a foundation for a robust physical security entry strategy.

Data centre operators know that redundancy comes at a cost, and designing a secured entry process is no different. The objective is to create a seamless experience for authorised users while incorporating multiple layers of physical security that build upon one another.

Let's start by clearly defining where the layers are, what the process entails, and the potential for automation to improve efficiency and lower labour costs.



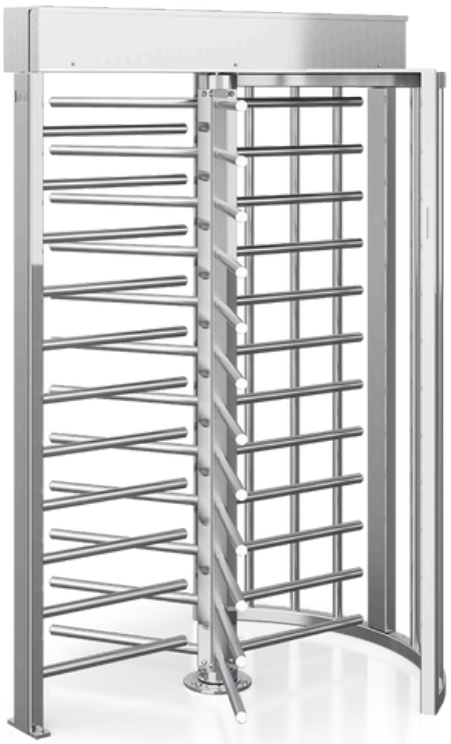
UNDERSTANDING DATA CENTRE ENTRANCES: **THE PERIMETER**

LAYER 1: THE PERIMETER

Physical security is crucial to keep unauthorised pedestrians outside the facility's fence line. Full-height turnstiles provide the first layer of security, which acts as a physical deterrent against infiltration. However, until recently, full-height turnstiles were susceptible to piggybacking, whereby two people could enter the turnstile through the same compartment. But now, new outdoor-rated sensors can detect when two people try to enter a compartment under a single credential, automatically locking the turnstile to prevent access.

The latest sensors also feature "walk-away" detection that locks the turnstile if an individual presents their credentials for access authorisation but does not enter. In conjunction with a completed rotation switch output, this new feature can accurately identify who is and isn't present within the building perimeter, ensuring that everyone is accounted for.

**Full-height turnstiles are only available in the US*



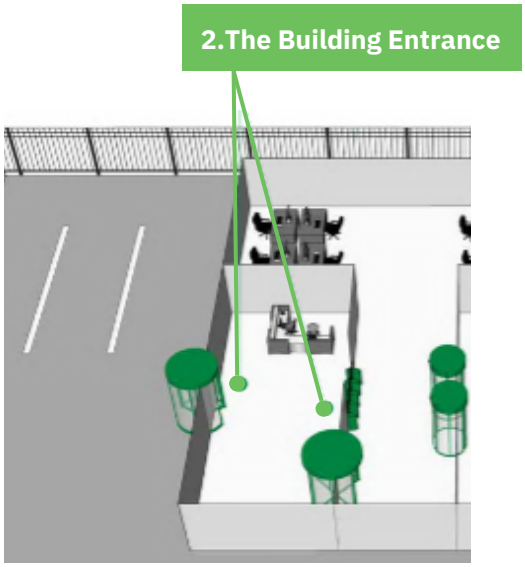
UNDERSTANDING DATA CENTRE ENTRANCES: **THE BUILDING ENTRANCE**

LAYER 2: THE BUILDING ENTRANCE

Upon entering the perimeter of a data centre, there is usually a swing door with a card reader that leads to the reception area. This door is equipped with an intercom, allowing only authorised personnel, such as employees, customers, and confirmed contractors, to enter. If someone is approved but needs to register, they must provide identification such as a driver's license or passport. At this point, you need to decide what kind of customer experience you want to provide. Do you want a detection strategy that utilises speed gates, or do you prefer a piggybacking prevention strategy that uses security revolving doors? Let's examine the advantages and disadvantages of each option.

Security speed gates alone cannot prevent tailgating. Therefore, it is important to rely on governance and manpower to enforce policies. A prevention strategy is critical if governance is tied to compliance and audit requirements. However, if you are a colocation that doesn't cater to regulated industry clientele, then using security speed gates can provide a great customer experience.

On the other hand, if you want to automate compliance and deploy staff to focus more on performing service-level agreement revenue generation, then security revolving doors are preferred. These doors prevent visitors from slipping by the reception desk or colluding while allowing authorised employees and visitors to come and go freely. Additionally, with revolving doors, you can benefit from climate control, dust air filtration and brute force protection.



Products Best Suited for Exterior or Interior Access Points:

- **Tourlock 180 High Security Revolving Door -** The ideal solution when you need to prevent unauthorised entry while supporting high traffic requirements.
- **Lifeline Speedlane Swing Speed Gate** – A slim, feature-rich security barrier that acts as a sleek boundary between public and private environments.

UNDERSTANDING DATA CENTRE ENTRANCES: **THE CRITICAL INFRASTRUCTURE**

LAYER 3: THE CRITICAL INFRASTRUCTURE (SERVER ROOMS)

To protect the most sensitive areas in a data centre, such as server rooms or white space, the one-person rule is enforced. It is critical to verify the identity of the authorised personnel to ensure compliance. Interlocking high-security portals are designed to prevent user substitution. This is achieved through an automated sequence of operations that guarantees the identity verification process does not allow for collusion or substitution. Simply providing access to one person at a time is not enough - it is imperative to verify that the person is authorised to enter.

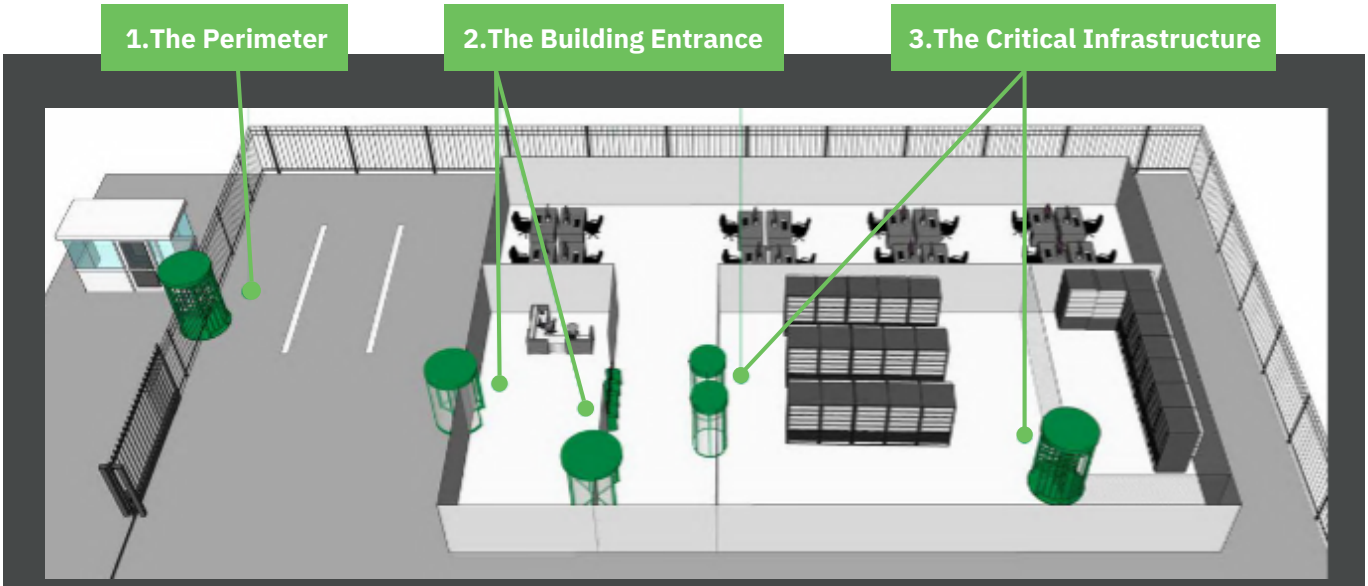
After a user presents their credentials, the first door opens. Upon entering the portal, a sampling process takes place to confirm that only one person is entering. If the samples pass, the first door closes and the portal redundantly re-samples. If the samples pass again, only then the biometric device is activated. This process is used to prevent substitution and ensure that the biometric device is only activated when there is one person in the portal.

An unattended secured interlocking portal utilises the same sophisticated sampling algorithms as the high-security revolving doors to measure risk and reduce the threat surface by layering and measuring at each point. With the help of these algorithms, it becomes possible to measure and predict the level of risk, which many data centre operators do not currently do. The interlocking portal is always closed, even during use, which supports climate control and dust air filtration. For added security, these interlocking portals can be reinforced with vandal-resistant or bulletproof glass.

Many applications require interlocking mantrap portals to be incorporated into fire-rated walls. This can be easily accomplished by securing one directly to a fire-rated swing door. Furthermore, half portals that attach to an existing fire-rated swing door provide a quick and effective means of transforming an ordinary door into a highly secure entrance.

Products Best Suited for Exterior or Interior Access Points:

- **Circlelock Solo Security Portal** - The ultimate single-entry security portal.
- **Circlelock Combi** - A practical half portal that attaches to an existing swing door, transforming an ordinary door into a high-security entrance.



LAYERED SECURITY FOR DATA CENTRES.

THE OPTIMISATION OF STAFF AND LABOUR DEPLOYING UNATTENDED SECURED ENTRY

While deterring, detecting, and preventing unauthorised entry are the primary functions of secured entry solutions, there are a number of other important benefits afforded by security entrances related to cost-savings, operational efficiency, and alarm management.

SECURED ENTRY FOR ENERGY EFFICIENCY

Power usage effectiveness (PUE) isn't the only operational improvement initiative available to data centres. But with rising energy and water resourcing costs, designing a security entrance that is always open and always closed, minimising air make-up and filtration costs, without eating up valuable square footage, is a unique challenge.

Conventional swing and sliding door entrances create a hole in the building envelope every time someone passes through, allowing outside air to rush in to displace the controlled internal atmosphere. In fact, as much as 50% of the total energy loss in a well-insulated building occurs through and around doors and windows. However, air quality is critical, so preventing air loss and filtration is both operationally beneficial and cost and energy-efficient. Security revolving doors and interlocking portals provide energy-efficient entrances that are always closed, thus driving efficiency and assisting with contamination control during everyday use. Boon Edam piggybacking and tailgating prevention solutions utilise 20% to 50% less square footage and provide superior air filtration performance to traditional vestibules.

"On average, eight times less air is exchanged with a revolving door than with a sliding or swinging door, thus driving efficiency and reducing loss and filtration."

SECURED ENTRY FOR COMPLIANCE

Beyond security, secured entry solutions empower staff with the infrastructure and tools they need to meet building requirements and demonstrate absolute customer audit compliance. With a layered secured entry strategy, you can:

1. Automate authorisation at entry/exit points.
2. Better sustain continual operations
3. Protect customer's data, shareholders, and insurance policies.
4. Produce immutable 90-day archived records and alarm retrieval records for customers, shareholders, insurance, and compliance audits.
5. Design entry/exit performance capabilities that utilise segmentation, redundancies, and analytics to build trust.

SECURED ENTRY FOR ALARM MANAGEMENT

Boon Edam full-height turnstiles, security revolving doors and security interlocking portals prevent all of these security violations and, therefore, eliminate all alarms generated by them at conventional swing doors. Compliance benefits include:

1. Automated user notifications are confined locally at the entry / exit and resolve all user interfacing and error issues without alarms.
2. Policies and procedures are enforced automatically without alarms.
3. 100% Elimination of DHOs for compliance reporting.
4. DFO alarms will only occur when the unit is subjected to a brute-force attack.

Most importantly, secured entry solutions consistently force compliance and automate the issue resolution process. As a result, employees do not perform remedial tasks such as false alarm responses and manual entrance checks but can focus on customer-facing objectives that generate revenue.

Boon Edam tailgating and piggybacking secured entry solutions can virtually eliminate 100% of Door Forced Open (DFO) and Door Held Open (DHO) alarms.

SECURED ENTRY FOR EFFICIENT LABOR ALLOCATION

Many data centres employ guards as part of their security strategy. While guards provide a strong physical deterrence, the recent talent shortage has challenged sourcing reliable staff. Like other industries, more is being asked of employed talent to compensate for a reduction in staff. The resulting imbalance between guard supply and demand has effectively changed how data centres leverage their available resources.

Security entrances successfully fill the gap between labour supply and demand by offering solutions that operate independently of or in tandem with security guards. These solutions reduce the current strain on human capital by offering a technology-based alternative. Give your staff the right tools for the job.

Take, for instance, a manned security entrance that requires guard services to check in employees and prevent any possible tailgating attempts. Consider the guards' salary, benefits, etc., then multiply this by all other facility entrances utilising this solution. The costs quickly add up. Now imagine a full-height turnstile, security revolving door, or high security portal installed at the same entryway. These solutions, too, can check in employees and prohibit instances of tailgating and piggybacking with far less associated overhead and risk.

"Instead of employing multiple staff to maintain secure entrances, organisations can now rely on unmanned security entrances that function 24/7/365."

CASE STUDY
RAGINGWIRE DATA CENTRE

Challenge: At RagingWire colocation data centres in Virginia and California, controlling access and preventing unauthorised entry is critical, while allowing unsupervised access to authorised personnel 24/7. RagingWire provides data centre services for some of the most demanding hyper-scale cloud and enterprise companies, and they are recognised as a leader in part because of their commitment to securing their customers' mission-critical equipment and data.

Solution: Boon Edam provided Tourlock security revolving doors to support RagingWire's sophisticated, multi-layer security system. The security revolving doors provide efficient passage for customer change control, while preventing tailgating and piggybacking during both entry and exit. The door systems detect such violation attempts and prevent unauthorised passage, supporting RagingWire's defence-in-depth security strategy.

PHYSICAL SECURITY IS CYBERSECURITY.

Lastly, to protect data centres and their critical data, it is essential to think of cybersecurity and physical security as working hand in hand to protect critical data. Installing security entrances can help ensure that only people entering the building are credentialed employees or authorised visitors, providing the highest levels of security for facilities housing sensitive data.

When mitigating risk in your physical and cyber security planning, remember that security entrances reduce your liability by demonstrating a plausible degree of effort to prevent infiltration. They protect the personal safety and security of staff, visitors, and anyone else in your facility, as well as your organisation's IT and computer systems and data. In addition, security entrances can also help reduce costs related to security personnel and false alarm management while helping to maintain compliance with various government and industry-imposed regulations and internal security policies.

OUR REACH **IS GLOBAL.**

We have been in business for 150 years, manufacturing premium aesthetic and security entrance solutions in The Netherlands, the United States of America and China. We can confidently say that we cover every corner of the globe with subsidiary companies in major cities across the globe. Furthermore our global export division not only partner with our distributors, but also offer direct sales and service to every territory. This wide net allows us to have a strong global footprint and a personal grasp of local markets and their unique entry requirements.

To find your closest Boon Edam expert, please go to:
www.boonedam.co.uk/contact

Boon Edam Limited
T +44 (0) 1233 505 900
E uk.contact@boonedam.com
I www.boonedam.co.uk

V2-1224

BOON EDAM
YOUR **ENTRY** EXPERTS.