SECURITY

The new standard in facility protection: Enhancing perimeter security

By Kurt J. Measom | February 28, 2025

Perimeter protection is essential for organizations across all sectors, serving as the first line of defense against potential threats. Whether it's a single room or a multi-structure campus, the perimeter marks where security efforts begin. When an intruder crosses this boundary, the risks of theft and damage increase significantly.

Organizations are investing in reinforced barriers and controlled entry points to address rising security concerns. These measures can effectively deter unauthorized access and protect people, assets, and operations. Understanding the importance of perimeter security and implementing proactive, layered strategies can enhance its effectiveness as a crucial defense line.

Layer 1: The perimeter
Physical security begins with keeping unauthorized pedestrians and vehicles outside the inner fence line. Full-height turnstiles are an ideal first layer, providing a strong physical barrier against infiltration. Traditionally, full-height turnstiles were vulnerable to piggybacking, where two people squeeze through a compartment using one credential. However, advanced outdoor-rated sensor technology now detects such attempts and locks the turnstile, preventing unauthorized entry. These sensors also include “walk-away” detection, which locks the turnstile if an individual, after being granted access, backs out before completing their entry. Combined with a completed rotation switch output, these enhancements ensure precise tracking of who is or isn't on the premises.

Layer 2: The building entrance
Once inside the facility perimeter, only authorized staff, customers, verified contractors or visitors should have access. Installing a security revolving door at the building entrance streamlines access for badge holders while maintaining robust security. Approved individuals without a badge must be escorted and issued a temporary credential, typically exchanged for a driver's license or passport. Security revolving doors use advanced sampling algorithms to ensure that only one person enters per approval, similar to the technology found in full-height turnstiles.

These doors also provide environmental and security benefits. They remain closed during operation, aiding air makeup, humidity control, and dust filtration systems. For added protection, the doors can be reinforced with vandal-resistant or bulletproof glass, offering critical defense during brute-force attacks.

Layer 3: The building interior
In some designs, a traditional swing door with a card reader is used to enter the facility's reception area. This is acceptable when the proper measures are in place for vehicles and pedestrians at the perimeter. When this design is used, the next layer is installed between the entrance lobby and the rest of the building interior. This layer, often implemented with a security revolving door or optical turnstiles, prevents visitors from slipping past the reception desk while allowing customers and contractors to come and go freely.

Layer 4: Critical infrastructure

Protecting highly sensitive areas, such as server rooms or other critical infrastructure, requires interlocking mantrap portals to enforce the one-person rule and ensure only authorized individuals gain access. These portals are designed to prevent user substitution through a precise, automated sequence of operations.

Once a user presents their credentials, the first door opens. After entry, the portal samples to confirm compliance with the one-person rule. If verified, the first door closes and resamples before activating the biometric device. This delay eliminates the possibility of collusion or substitution.

Unattended secured entry interlocking portals, equipped with the same advanced algorithms used in security revolving doors, allow organizations to measure and predict risk levels at each access point. These portals also support building air makeup and environmental controls, and they can be reinforced with vandal-resistant or bulletproof glass for added protection. Many configurations include fire-rated walls and doors, making them easily adaptable for interlocking mantrap portal systems.

The six key risks of perimeter breaches

Unauthorized access to a facility poses significant risks. To ensure a robust layered security strategy, organizations must address six critical areas where threats escalate sharply if the perimeter is compromised:

1. **Security of personnel and visitors:** Balancing security with a welcoming atmosphere at the perimeter is challenging. Security measures like barriers, turnstiles, or biometric-controlled entrances protect everyone within the facility without compromising a welcoming environment.
2. **Safety of high-risk areas:** Hazardous facility zones require defined perimeters to prevent unauthorized entry. Controlling access in these zones mitigates potential safety risks and reduces liability, helping organizations meet compliance standards and protect lives.
3. **Protection against theft and loss:** Unauthorized access can lead to financial loss, intellectual property theft, and operational disruptions. Robust perimeter security prevents damage before it occurs.
4. **Compliance with industry regulations:** Regulated industries require controlled perimeters and strict access protocols. Investing in secure perimeters ensures compliance with HIPAA, PCI, and NERC standards.
5. **Ensuring business continuity:** Fortified perimeters minimize incidents that disrupt workflow and impact morale, ensuring smooth operations.
6. **Mitigating legal liability:** Effective perimeter security demonstrates proactive risk management, reducing liability risks.

Achieving an impenetrable perimeter

As the importance of perimeter security gains recognition, identity-based systems have emerged as a critical component of effective strategies. Integrating identity verification with proactive access control establishes a strong defense against potential threats. Although perimeter security investments may be difficult to justify in budget-conscious environments, the long-term benefits far outweigh the initial costs. By fortifying the perimeter with advanced solutions, organizations can create a secure environment that supports operational success.

Article link: https://www.securitymagazine.com/articles/101425-the-new-standard-in-facility-protection-enhancing-perimeter-security

Used with permission from Securitymagazine.com
By: Kurt J. Measom