BOON EDAM

DATA CENTER SECURITY
VULNERABILITIES AND SOLUTIONS

Even multiple layers of access security can become vulnerable to unauthorized access over time. Here are a few examples of where vulnerabilities exist and how to eliminate them.

LAYER 1 PERIMETER

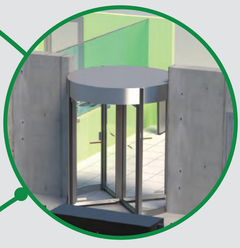
Access Vulnerabilities at the Property Perimeter

Perimeter access controls should both deter and prevent unauthorized individuals from entering a secured property — but shared entry points, weak enforcement, and inconsistent monitoring often result in access breaches. Full height turnstiles outfitted with advanced sensors are ideal for exterior entry/egress points to prevent forced entry and tailgating incidents.

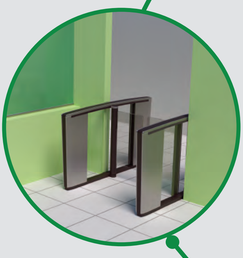
LAYER 2 BUILDING ENTRANCE

Building Entrance Access Challenges

The best way to control and manage access to buildings is with one-person-per-credential access solutions – but high traffic periods like shift changes or special events can slow throughput and create opportunities for tailgating, shared access, and inconsistent enforcement. Security revolving doors can accommodate unsupervised bi-directional traffic of authorized individuals and be integrated with various types of readers and biometrics for multi-factor authorization, as well as sensors to prevent piggybacking.



Properly specified, equipped and installed secured entry solutions virtually eliminate vulnerabilities at every layer of access across data center properties.



LAYER 3 INTERIOR ACCESS

Controlling Access to Interior Secured Areas

Secured interior areas like executive offices, HVAC and utility areas, even employee break rooms should only be accessible to authorized individuals – but lax permissions, temporary and/or contracted workers, and varying workflows can compromise security and safety over time. Optical turnstiles provide a clear visual deterrent against unauthorized access to controlled areas with the ability to detect unauthorized access attempts that trigger alarms to alert security personnel.

LAYER 4 CRITICAL INFRASTRUCTURE

Protecting Your Most Critical Asset – Server Rooms

Gaining access to server rooms demands the highest levels of identity authentication and verification – but reliance on physical credentials and inconsistent enforcement puts your most critical assets at risk, causing high exposure to liabilities. Interlocking mantrap portals equipped with multi-factor access readers and occupancy sensors provide the ultimate defense against unauthorized access. By allowing only one individual at a time to gain access, mantraps virtually unauthorized access without the need for guard supervision.

Consult with one of our secured entry solution specialists to discuss how you can better protect your data center's people, assets and property.

Click here to get the conversation started!

Visit Our Data Center Solutions Site