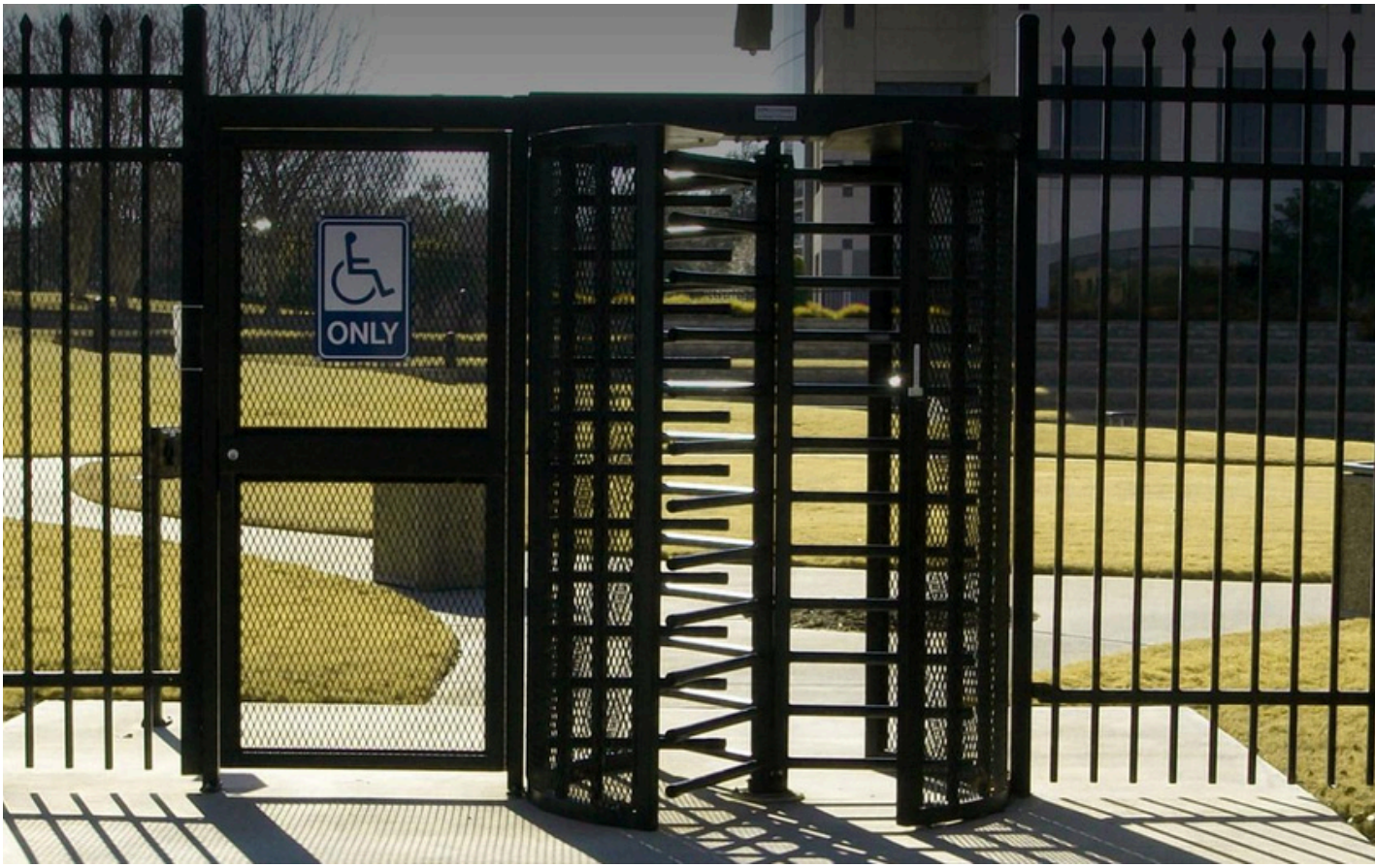
BOON EDAM
YOUR **ENTRY** EXPERTS.

BEYOND THE RACKS:
HOW INTELLIGENT ENTRANCE SOLUTIONS FUTURE-PROOF DATA CENTER SECURITY

TABLE OF CONTENTS

WHY PERIMETER SECURITY IS THE FIRST LINE OF DEFENSE

When securing a building, especially a data center, the entrance is more than just a doorway. It represents the frontline of physical security. While the digital security posture of a facility often garners significant investment and attention, it's the physical envelope that prevents unauthorized access before a breach can even begin.



Security entrances like revolving doors, security portals, and optical turnstiles serve as intelligent guardians of your facility. Full-height turnstiles and barrier systems deter intruders and ensure controlled access. Advanced sensor technology prevents unauthorized entry attempts, such as piggybacking. Sensors monitor each credential swipe, and if more than one person attempts to pass with a single swipe, the system automatically locks the turnstile. This ensures that only authorized individuals gain entry. Additionally, "walk-away" detection locks the turnstile if a user abandons entry after being granted access.

These systems support corporate goals beyond access control, enhancing operational efficiency, streamlining compliance, reducing risk, and maintaining a brand reputation.

HOW AUTOMATED ENTRANCES REDUCE COSTS AND STRENGTHEN SECURITY

The average cost of a breach is $5.5 million, making prevention an invaluable cost-saving tool. Security entrances also offer one of the clearest paths to ROI through automation. By eliminating the need for on-site guards at access points, organizations save significantly on labor while improving consistency and security.

Unlike guards, security portals are always on, enforcing credentials and preventing tailgating 100% of the time. In high-security areas, mantrap portals with multi-factor authentication ensure stringent access control. In public-facing lobbies, optical turnstiles offer sleek aesthetics while quietly deterring detecting unauthorized entry.

By freeing security personnel from manual door duty, these systems allow staff to focus on higher-value tasks like threat monitoring and emergency response. These systems don't simply replace labor, they optimize it.

THE ROI OF PREVENTATIVE MAINTENANCE AND SERVICE AGREEMENTS

Even the most advanced entrance solution can become a liability without regular upkeep. A non-functioning turnstile disrupts business, creates vulnerabilities, and may require costly emergency repairs. When security entrances such as revolving doors, mantrap portals, and turnstiles go offline, they impact more than just physical access. They disrupt access control, workforce management, and even health and safety functions.

Downtime also presents a serious risk. A malfunctioning entrance may leave the organization vulnerable to unauthorized entry, theft, or even liability in the event of an incident. Hiring temporary guards may offset this temporarily, but it still doesn't match the reliability of an automated system. Furthermore, skipping routine maintenance may lead to more expensive repairs or full system replacement, significantly increasing costs in the long run.

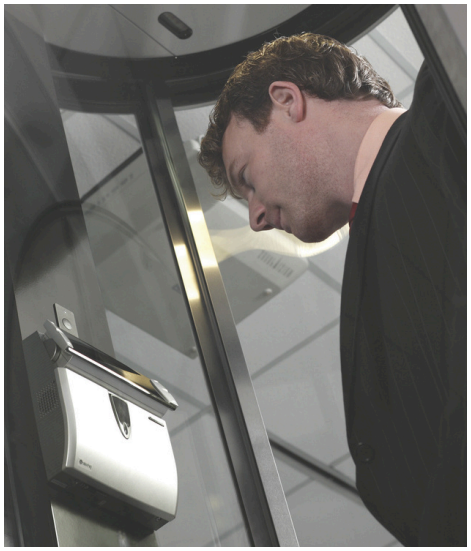
Rather than assigning this workload to internal teams, many organizations enroll in a structured service agreement. These agreements, often offered by the manufacturer or a certified installer, provide peace of mind by assigning highly trained technicians to handle ongoing inspections, diagnostics, and tune-ups. Service agreements also help with budgeting. Knowing your annual maintenance costs up front makes it easier to plan and advocate for funding, rather than dealing with surprise breakdowns and emergency expenses.
.

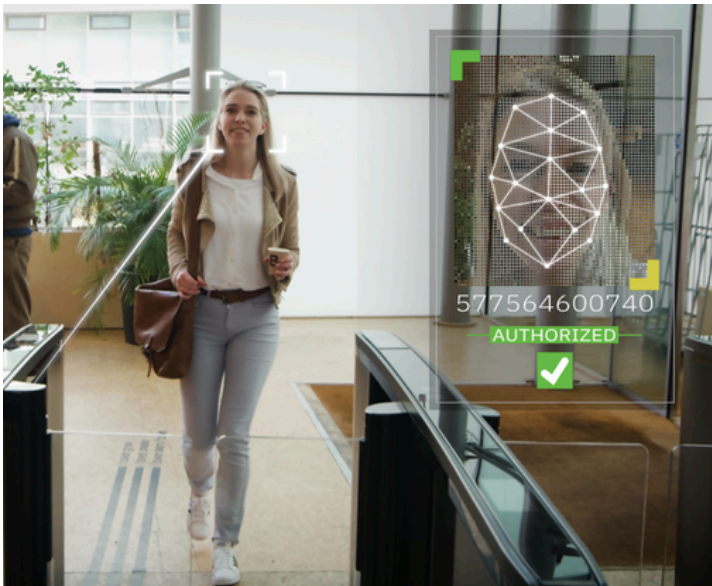
INTEGRATING WITH ACCESS CONTROL AND SECURITY ECOSYSTEMS

Modern security solutions can't exist in silos. Intelligent entrance systems must integrate with broader security ecosystems: access control, video surveillance, biometric ID, and cloud management platforms.

The rise of hybrid cloud deployments allows these systems to function seamlessly across on-premise and cloud environments. Edge and cloud-managed devices simplify integration and help modernize infrastructure without abandoning existing investments.

SaaS platforms built for open, hybrid-cloud environments are redefining the future of security. They enable organizations to unify access control, video, intercom, and intrusion detection into a single command center, managed seamlessly from a single pane of glass.





EMERGING TRENDS: WHAT'S NEXT FOR DATA CENTER PHYSICAL SECURITY

"AS THE THREAT LANDSCAPE EVOLVES AND INFRASTRUCTURE DEMANDS INTENSIFY, DATA CENTERS ARE EMBRACING NEW TECHNOLOGIES AND STRATEGIES THAT **PRIORITIZE PRACTICALITY, RESILIENCE, AND CROSS-FUNCTIONAL VALUE."**

1. Practicality Over Hype: Organizations are moving toward strategic hybrid models that blend on-premise and cloud solutions. Rather than chasing trends, they're adopting technologies that meet operational needs.

2. Responsible AI: AI adoption is growing, but deployment is becoming more outcome-focused. AI can help in many security-related tasks, such as discerning people from objects at a facility's perimeter and interior entrances, detecting attempted piggybacking, spotting and analyzing potentially lethal objects and dangerous people, and more. Intelligent automation helps streamline emergency response, event classification, and system optimization.

3. Privacy and Compliance: The average cost of a data breach reached $4.88 million in 2024. In response, facilities are prioritizing systems with SOC 2, ISO 27001, and GDPR-aligned protections to strengthen compliance and mitigate risk.

"According to IBM, the average cost of a data breach hit $4.88M in 2024, prompting data centers to prioritize SOC 2, ISO 27001, and GDPR-aligned protections."

4. Cross-Team Collaboration: Physical security decisions now involve IT, HR, facilities, and operations. Teams want shared tools that boost communication and performance.

5. Informed Service Expectations: Organizations expect more from integrators and vendors. They are seeking holistic guidance that bridges cybersecurity, physical protection, operations, and business insight.

BEST PRACTICES CHECKLIST: BUILDING A LAYERED DEFENSE STRATEGY

Effective physical security requires more than just hardware. It demands a strategic, layered approach. The following checklist outlines best practices for building a resilient defense that aligns with data center operational goals, regulatory standards, and evolving threat landscapes.

- **Conduct** a perimeter risk assessment and document vulnerabilities
- **Deploy** a mix of security entrances based on traffic flow and risk tolerance
- **Integrate** entrance systems with access control and video platforms
- **Use AI** to automate alerts and reduce data noise
- **Schedule** regular preventive maintenance for all physical systems
- **Align** your entrance security strategy with your business continuity plan
- **Engage** stakeholders from IT, HR, facilities, and legal in your physical security decisions
- **Require** compliance-ready certifications from vendors (SOC 2, ISO 27001, etc.)
- **Invest** in platforms that allow for hybrid-cloud deployments
- **Track ROI** by comparing labor savings, downtime prevention, and compliance outcomes

CASE STUDY HIGHLIGHT: RAGINGWIRE DATA CENTERS TOURLOCK SECURITY PORTALS POWER A HIGH-SECURITY, HIGH-UPTIME ENVIRONMENT

RagingWire, a leading data center provider and subsidiary of NTT Communications, needed a way to secure high-risk zones without slowing operations or compromising uptime. At its Sacramento CA3 and Ashburn VA3 facilities—spanning over 400,000 square feet and delivering 30 megawatts of critical power—RagingWire deployed Boon Edam's Tourlock 180 security revolving doors as a core part of its multi-layer security strategy.

These high-security portals use biometrics, credentials, and weight-based detection to ensure that only one authorized individual enters at a time. Advanced 3D sensors detect and prevent tailgating or piggybacking, eliminating the need for dedicated guard supervision and improving audit readiness.

"Our customers expect our security entrances and anti-tailgating technologies to be extremely fast and accurate," said Eddie Ankers, Director of Corporate Security at RagingWire. "By adding these doors to our defense-in-depth security strategy, we are providing the best possible protection for our customers' mission-critical equipment."

The Tourlock doors integrate seamlessly into RagingWire's broader access control systems and are supported by maintenance agreements that ensure optimal performance and long-term reliability.

Solutions Implemented:

- Tourlock 180 High-Security Revolving Doors
- Integrated biometric and credential authentication
- Maintenance and support agreements

Read more about this case study: RagingWire Data Center Physical Security.

PARTNER WITH BOON EDAM

Future-proofing your data center starts at the door. Boon Edam delivers intelligent, integrated entrance solutions that strengthen physical security, support compliance, and improve operational efficiency, without compromising on design or the user experience.

Our team can help you design a strategy tailored to your facility's unique needs.

READY TO TAKE THE NEXT STEP?

Request a consultation or demo today to see how secure entry solutions can deliver measurable ROI and long-term resilience.

Visit boonedam.us to schedule your consultation.

Boon Edam Inc.
421 N. Harrington St. | Raleigh, NC 27603
M: +1 910 814 3800
E: sales@boonedam.us

BOON EDAM
YOUR **ENTRY** EXPERTS.