

THE SECURITY PLAYBOOK FOR DATA CENTERS

DESIGNING ENTRANCE SECURITY AROUND THE PEOPLE WHO USE IT

Data center security ecosystems are typically designed around the physical structure of the facility, their location and the need to protect secured areas within, but there's another design parameter that is much less predictable: people.

Employees with time-shifting schedules, contractors working on short term projects, vendors servicing equipment, deliveries, customers and visitors, and auditors reviewing operations all have different reasons for entering a facility at different times with different levels of access.

Applying the same entry process to every individual creates inefficiencies, disruptions to workflows and inadequate security that opens data center operators to liabilities.

A more effective approach is to design and implement entrance security solutions based on who needs access, where they need to go, when they need to be there, and how confidently their identity and authorization need to be verified.

START WITH THE PERSON, NOT THE ENTRANCE

Before selecting a secured entry strategy, consider who and why specific groups of individuals require access across the facility. For each user group, ask:

- Where do they need access?
- How frequently will they enter and exit?
- How long should their access remain active?
- What times or operating conditions should apply?
- How sensitive are the areas they need to enter?
- What level of identity verification is appropriate?
- Should they move independently or require an escort?
- What happens when their role, project, or reason for access ends?

Answering these questions will help determine the appropriate credentialing process, identity authentication method, type of secured entry solution, and level of monitoring for each user group and entry location.



MAKE EMPLOYEE ACCESS SECURE AND EFFICIENT

Employees are the most predictable user group moving through a data center. Their roles, schedules, and access needs are generally well established based on their specific job function, facilitating clear and consistent access policies.

The challenge is balancing security with flow management.

Employees who need to enter a facility every day should not encounter unnecessary delays even when they have the highest levels of security clearance. Basically, very few if any employees will require open access to every secured area within the facility.

Access permissions should reflect specific job responsibilities and the security level appropriate for each area. An employee may be authorized to enter the building and general work areas while requiring additional authorization to access server rooms, executive offices, HVAC areas, or other designated secured locations.

Consequently, as security priorities increase for different secured areas, so should the level of protection. Highly secured areas may require stronger physical entry solutions such as one-person-per-credential enforcement, tailgating protection, and additional identity verification, such as biometric authentication.

Entrance capacity should also account for workflow traffic. Shift changes, breaks, and other predictable peaks can quickly create bottlenecks if entrances are not designed to accommodate daily and peak traffic periods.

The goal is to grant authorized employees access to the areas they need while maintaining stronger controls around the areas they do not.

CONTROL TEMPORARY ACCESS WHILE MINIMIZING RISK

Contractors and temporary workers present a different challenge. Data centers routinely depend on construction crews, technicians, maintenance personnel, and other third parties who may require access for designated periods of time. Establishing access for temporary workers should be treated as temporary from the beginning.

Credentials for temporary personnel can be limited by time, date, area location, project, and expiration date. A technician servicing equipment in one area should not receive broad access simply because it is easier to administer, and credentials issued for a temporary project should not remain active once the work has been completed.

Identity verification is especially important when contractor populations change frequently or when multiple subcontractors are working on site. The entrance strategy should ensure that the individual presenting a credential is the person authorized to use it.

Facilities should also plan ahead for contractor traffic rather than treating it as an exception. Regular facility upkeep and maintenance, expansion, and upgrades can dramatically increase the number of people entering a facility.

The goal is to provide contractors with the access necessary to perform their work without granting access to other areas or leaving permissions in place longer than needed.

VISITORS: MAKE THE PROCESS SECURE AND EASY

Visitors are often unfamiliar with the layout of a facility, its security procedures, and where they are supposed to go.

A well-designed visitor management process should define permissions while maintaining tight control over where visitors can move.

Pre-registration, identity verification, temporary credentials, defined permissions, and escort requirements can all help establish the most appropriate access level based on the reason for the visit.

The physical security entrance deployed to control and manage physical access plays a critical role in any visitor management policy. Access credentials are only as effective as the entry/egress locations where they need to be enforced. Visitors should not be able to tailgate an authorized employee through a security entrance simply because someone politely holds the door open for them.

The process also needs to be practical. If visitor procedures are cumbersome, employees and security personnel may create workarounds that compromise the very controls the visitor management process was intended to provide.

The goal is to create a positive visitor experience that is easy, difficult to bypass, and appropriate to the sensitivity of the areas being accessed.

VENDORS AND SERVICE PROVIDERS: LIMIT ACCESS TO THE JOB AT HAND

Delivery personnel, suppliers and equipment vendors, service technicians, and other support personnel often change, yet visit a facility on a regular basis to perform specific functions. As a result, their access permissions are usually very different.

A plumber may need access to a building's infrastructure but have no reason to enter a server room. A delivery provider may need access to a receiving area but nowhere else in the facility.

Rather than providing broad facility access, access management strategies should establish specific routes and permissions based on the service being provided.

Facilities should also consider when these individuals need access. Vendors and service technicians frequently operate outside traditional business hours, when fewer employees are present and security teams may be managing multiple responsibilities.

The goal is to provide vendors with highly controlled access to the specific locations necessary to complete their work without compromising security.

COMPLIANCE PERSONNEL: PRIORITIZE CONTROL AND ACCOUNTABILITY

Some visitors require access precisely because the facility is highly regulated or sensitive.

Auditors, inspectors, and other authorized third parties involved in maintaining compliance may need to enter areas that ordinary visitors would never need to access.

These users often require a combination of strong identity verification, highly defined permissions, escort policies, and reliable records of where and when access occurred.

Although their visits may be infrequent, a defined entrance process and policy needs to be implemented in advance of their need to access the facility. Any improvisation can create operational delays and unnecessary security exceptions, which can effectively breach compliance.

The goal is to provide controlled access to support compliance audits, inspections, and business requirements while maintaining clear control and visitor accountability.





MATCH THE LEVEL OF SECURITY TO THE LEVEL OF RISK

Designing access processes and policies requires access layers based on who the person is, what they are authorized to do, and the security priority of the location they are entering.

For example, an authorized employee may move efficiently through the facility perimeter and general employee areas using a standard credential. Entering more sensitive areas may require tailgating prevention and higher identity authentication measures. Reaching the most highly secured areas may require one-person-per-credential enforcement combined with biometric verification or another form of higher-assurance authentication.

The result is a layered access approach where security becomes progressively stronger as risk increases and users encounter stricter controls when and where it is warranted.

DON'T RELY ON PEOPLE TO MAINTAIN SECURITY

Even the best policies can weaken when their success depends on people to notice and react to access policy exceptions.

Individuals should not be responsible for determining whether the person behind them belongs in a secured area. Security officers should not have to manually manage routine entrance activity that can be autonomously enforced 24/7.

Effective security entrances should automate routine enforcement and detect and notify personnel when something unusual occurs. This allows security personnel to focus on events that require their immediate attention while continuing to support employees and visitors to a facility.

FIVE QUESTIONS FOR YOUR NEXT SECURITY PLANNING MEETING

As you evaluate how people move through your data center, consider:

1. **Have we clearly defined our different user groups and the areas each needs to access to perform their job function?**
2. **Do access permissions reflect a person's role, schedule, location, and duration of need?**
3. **Do our most highly secured areas require stronger physical security entrances and higher forms of identification and authentication?**
4. **Do our security entrances accommodate workflows, including shift changes, contractor activity, visitors, and maintenance periods, without sacrificing security?**
5. **When someone's role or reason for access changes, can we quickly adjust or remove their permissions?**

If the answer to any of these questions is unclear, it may be time to look more closely at whether your entrance strategy reflects the people using your facility today.

DESIGN FACILITY ACCESS BASED ON YOUR SPECIFIC OPERATIONS

There is no single access process that is right for every user group, entrance, or area of a data center. The best strategies recognize those differences and apply the appropriate access permissions, identity verification, physical protection, and operational efficiency where appropriate.

As your facility grows, personnel and workflows change, and new users require access, your access policies and procedures will also need to evolve.



Need help designing a security entrance strategy around the people who use your data center? Let's talk.
**Boon Edam can help you identify the right secured entry solutions for different users, locations,
and security priorities throughout your facility.**



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


BOON EDAM
YOUR **ENTRY** EXPERTS.