

METRICS THAT MATTER:
ARE YOU GETTING THE MOST OUT OF YOUR DATA CENTER ENTRANCES?

BOON EDAM

Security entrances may appear to be working properly, but it isn't always apparent if they are performing to their fullest potential. Access authorizations may be taking too long, encouraging workarounds that don't adhere to security policies and procedures. Or they may be generating too many nuisance alarms to the point that security personnel simply disregard them. And what about historical data, event forensics, and analysis? Is the data being generated by your security entrances even accurate if access policies and procedures are being violated?

Although your security protocols and supporting metrics may all seem fine, your data center may actually be at risk.

The objective is not simply to collect more data – but to better determine whether each security entrance is delivering the level of security, flow, reliability, and accountability you need to best protect people, property, and assets.

The test: Review and analyze the data from your security entrances and related security systems and correlate it with data from other enterprise systems like employee schedules and attendance records to ensure your security entrances are performing as intended.



START WITH KPI'S FOR YOUR SECURITY ENTRANCE AND ACCESS SOLUTIONS

Performance needs to be measured against key performance indicators (KPIs) established for access, security, and various other facility operations. A full-height turnstile controlling the perimeter, a lobby entrance handling employees and visitors, and a high-security portal protecting a server area all have specifically defined purposes. The following evaluation criteria need to be defined for each security entrance in your facility:

- **Security role:** Is the security entrance intended to deter, detect, or prevent potential threats?
- **Required authorization:** Which employees, contractors, vendors, visitors, and auditors should have access to specific security entrances?
- **Traffic profile:** What normal, peak, after-hours, and project-related traffic volumes are anticipated for each access point?
- **Enforcement policy:** What access credentials, identity authentication requirements, escort requirements, and exceptions apply?
- **Operating status/state:** What constitutes fully-functional, degraded, manual, emergency, and out-of-service operation?
- **Event documentation:** Which access events, alarms, video footage, and operator actions should be retained and/or correlated for each external and internal access point?
- **Response requirement:** Who needs to respond when specific types of alarms and/or events are detected? How quickly must events be addressed, and what actions are required to resolve them?

These seven criteria will create a benchmark for establishing KPIs for each security entrance and access point. Without them, facility security and operations personnel may have a false sense of confidence that access and security protocols are being upheld when they are not.



GET THE BIG PICTURE
BY MEASURING MULTIPLE OUTCOMES

No single KPI or metric can effectively document entrance performance. The ability to correlate multiple data points will provide greater insight to determine whether your security entrances are secure, compliant, dependable, and defensible.

Security Enforcement

Security metrics should indicate whether physical access matches established policies and procedures. Useful indicators include the relationship between valid credentials and completed passages, tailgating and/or piggybacking rejections, access denials, door-held-open or door-forced-open events where applicable, and the frequency of manual overrides.

Alarm volume alone neither validates nor refutes strong or weak security. A low frequency of alarms may reflect good user behavior and effective controls, but it could also indicate incomplete event capture, detection settings that are too permissive, or routine use of an unmonitored emergency bypass. A high frequency of alarms could signal increased risk, confusing procedures, poor credential enrollment, or the need for system maintenance.

What leadership needs to know: Do the facility's security entrances enforce established policies and procedures, and are exceptions investigated rather than merely documented?

Operational Flow

System failures often happen without notice, and during times when a facility may be most vulnerable, such as during times of high-volume traffic. Measure throughput, wait time, queue length, and queue duration during the busiest intervals, such as shift changes, contractor arrivals, maintenance windows, deliveries, and audits.

First-pass credential acceptance is also important. Repeated credential presentations, biometric retries, reversals, and requests for manual assistance can indicate system issues and create friction when authorized individuals are denied access for no reason. Segmenting these events by user group and authentication method helps identify potential problems that require attention.

What leadership needs to know: Are authorized individuals efficiently transiting access points without weakening controls or creating workarounds?

System Reliability

System uptime metrics can mask the loss of important capabilities. A security entrance may maintain power and operate normally without alerting administrators to events that should trigger alerts. Check the availability and operation of specific functions separately from degraded or manual operations and events. Fault frequency, repeated fault patterns, mean time to acknowledge, mean time to restore, preventive maintenance completion, open service items, and emergency-mode tests provide a more accurate view of resilience.

What leadership needs to know: Are security entrances operating with all their intended security functions, and if not, was full performance restored and did any events take place during the specific feature(s) downtime?

Accountability and Compliance

Security policies and procedures are difficult to enforce without detailed records of all events of interest. Event logs need to be complete, time-stamped, retained according to policy, and correlated to access control, video, identity, and incident records.

Measure the percentage of alarms and exceptions that receive a documented disposition, the time required to close them, the number of unresolved or recurring events, and the results of scheduled controlled tests. This will indicate whether the data supports specific actions and if the data will stand up during an audit, customer review, or investigation.

What leadership needs to know: Can the organization demonstrate that security policies and procedures are working, identify exceptions, and determine how to remediate problematic areas?

RAW DATA CAN BE MISLEADING

Busy entrances naturally produce more passages, retries, denials, and alarms than low-volume entrances. Daily traffic metrics can also hide short periods of congestion or degraded operation.

Make traffic metrics comparable and useful by:

- Categorizing event counts by traffic volume and event types such as alarms, denials, or overrides.
- Distinguishing normal traffic from peak intervals instead of relying only on daily averages.
- Segmenting performance by entrance, security layer, user group, shift, and authentication method.
- Comparing each entrance with its own approved baseline before comparing it with entrances that serve different purposes.
- Tracking both the event type and how it was resolved so event activity is not mistaken for completed follow-up.
- Trending results over time so small changes can be investigated before they become operational or security failures.

Context turns data into insightful information. High access denial rates may be a security concern, an expired contractor credential problem, or evidence that a new access and/or identification enrollment process is not working as intended. Traffic volume averages and daily numbers cannot identify specific problems to be addressed.

ANALYZE PATTERNS. NOT JUST NUMBERS.

The best metrics evaluate multiple related data sources to better transform observations into actions.

Signal	What It May Mean	Management Response
Alarms rise while traffic remains stable	A change in user behavior, training, detection settings, or threat activity	Classify the events, correlate them with access and video records, and address the cause before changing thresholds.
Access denials or retries increase	Permissions, expiration dates, enrollment, or onboarding may be out of sync with the work being performed	Review the affected user group(s) and access workflow(s), not just the entrance hardware.
Peak wait times are increasing while first-pass access remains consistent	The process is working, but capacity or scheduling may no longer match demand	Revisit lane allocation, arrival patterns, staffing, and future capacity requirements.
Manual overrides rise along with congestion	Personnel may be bypassing controls to keep people moving	Treat this as a combined security and operations issue, then correct the pressure creating the workaround.
System uptime remains high, but degraded-mode hours increase	The availability metric may be masking reduced enforcement capability	Separate full-function availability from manual, fail-safe, and degraded operation.

LEVERAGE/STRUCTURE METRICS TO TRIGGER ACTION

Metrics reporting should provide greater insight that helps improve overall performance across the enterprise by including the following:

- **Definition:** What exactly is being measured, and which system is the source of record?
- **Baseline:** What did normal performance look like after commissioning or the most recent approved change?
- **Target:** What level of performance is expected for this entrance and its security role?
- **Threshold:** What deviation requires attention, escalation, testing, service, training, or redesign?
- **Owner:** Who is accountable for reviewing the metric and closing the resulting action?
- **Cadence:** Which conditions require real-time review, and which belong in weekly, monthly, or quarterly analysis?

The executive metrics summary should be concise. At minimum, it should include access traffic volume by user group, peak flow periods, first-pass access acceptance, security events normalized by traffic, frequency and reasons for manual overrides, availability of preset features, system time in degraded mode, number and type of recurring faults, open exceptions, control-test status, current trends, and the personnel responsible for remediating issues.

SET DIFFERENT METRICS REVIEWS TO MONITOR DIFFERENT OPERATIONS

Not every metric belongs on the same schedule.

- **Real-time and daily reviews:** Daily monitoring of active alarms, device faults, emergency status, unusual denial patterns, excessive queues, and entrances operating in manual or degraded mode.
- **Weekly and monthly reviews:** Review alarm trends, first-pass access acceptance, peak wait times, override frequency, recurring service issues, exception closure, and changes by user group or shift.
- **Quarterly reviews and reviews after material changes:** Establish baseline validation, review control testing and access workflow, integration system health, capacity assumptions, maintenance needs and schedules, and future investment needs/priorities.

A material change may include a new tenant, expansion project, contractor influx, revised shift schedule, authentication upgrade, software configuration change, new compliance obligation, or renovation. Revisit the baseline after these events so yesterday's standard does not conceal today's risk.





TREAT ENTRANCE PERFORMANCE **AS AN ENTERPRISE ESSENTIAL**

Security entrances play a significant role in maintaining the security and operations of a data center. Like other enterprise systems, they require status monitoring to ensure consistent performance, must accommodate frequent changes in individual access permissions, and need detailed reporting for compliance, investigations, and future planning.

Well-managed access and security entrance solutions can help proactively identify potential threats before they evolve, maintain smooth workflows and throughput, and contribute new sources of data and business intelligence.

Contact Boon Edam to learn more and speak with our team of data center secured entry solution experts.

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

BOON EDAM