

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

BOON EDAM

Security entrances may appear to be working properly, but that does not necessarily mean they are performing to their fullest potential or being leveraged beyond their inherent security intent.

Employees may be using workarounds to bypass access policies. Long queues during shift changes may be wasting valuable paid labor time. Temporary workers may be exceeding approved credential permissions. Contractors and drivers may be dependent on manual assistance because approved processes are incongruent with their access needs. All of these examples (and more) may also be generating frequent nuisance alarms that distract security personnel from other responsibilities and actual threats.

And what about the data those entrances generate? If employees are routinely bypassing approved processes, using alternate doors, or relying on manual overrides, access data may no longer provide an accurate picture of who entered, when they entered, or how a facility is actually operating.

Access metrics can also support business operations by turning previously underutilized entrance data into another layer of business intelligence.

The objective of analyzing security entrance performance and metrics is to determine if the entrances are providing the highest levels of security, throughput, reliability, and accountability to best protect people, property, inventory, and operations.

The test: Review entrance and access data alongside related operational information such as employee schedules, shift patterns, contractor activity, attendance records, and peak traffic periods. The goal is to determine whether your security entrances are performing as intended at each location where they are deployed throughout your facility.



DEVELOP KPI'S FOR YOUR SECURITY ENTRANCE AND ACCESS SOLUTIONS

Performance needs to be measured against key performance indicators (KPIs) established for security, access, workforce movement, and facility operations.

A full-height turnstile at your primary perimeter entrance, a secured employee access point supporting hundreds of workers during shift changes, and an interior secured area housing high-value inventory all serve different purposes.

KPIs need to be established and revisited periodically for each security entrance in the facility based on the following seven core criteria:

- **What is the entrance's security role?** Is it intended to deter, detect, or prevent unauthorized access, or manage access rates and volume based on occupancy limitations?
- **Who requires authorization to access this specific area?** Which employees, temporary workers, contractors, suppliers, drivers, visitors, and service personnel should be permitted through the entrance? Is their access limited to specific times of day or days of the week, and over what duration of time?
- **What are anticipated traffic volumes?** Estimate the normal, peak, after-hours, seasonal, and project-related traffic volumes for this access point. Are these traffic patterns predictable based on past history, and what fluctuations are anticipated moving forward?
- **What are the credential enforcement policies?** Identify the types of acceptable credentials, identity authentication, escort requirements, schedule restrictions, or exceptions that apply to specific user groups.
- **What are the operational benchmarks?** Establish benchmarks for fully functional, degraded, manual, emergency, and out-of-service status and what course of remediation is required when a performance condition is reported.
- **What form(s) of event documentation are required?** Define different levels/types of access events, alarms, video recordings, operator actions, and overrides that should be retained or correlated with other forms of enterprise data (such as time and attendance records) for each entrance.
- **Who should respond when an alarm sounds?** Define what departments/personnel need to respond to specific alarms, how quickly they need to be addressed, and what action is required to resolve the alarm or event.

These seven criteria establish clearly defined KPI benchmarks for each security entrance and access point. Without them, security and operations teams do not have a clear set of operating procedures and can develop a false sense of confidence that entrance policies are being enforced simply because people are continuing to move in/out of the facility.



GET THE BIG PICTURE
BY MEASURING MULTIPLE OUTCOMES

No single KPI can effectively measure entrance performance. It is critical to correlate multiple data points to ascertain a clear picture of whether warehouse entrances are secure, efficient, reliable, and accountable.

Cyber-Physical Security

Security metrics should show whether physical access matches established policies and procedures. Useful indicators include the relationship between valid credentials and completed passages, tailgating or piggybacking rejections, access denials, held-open or forced-open door events where applicable, use of alternate entrances, and the frequency of manual overrides. Abnormal credential usage is also a good indicator that something is amiss, and requires investigation.

It's also important to note that physical security is also the foundation for cybersecurity as bad actors are increasingly finding it far easier to access critical data through the physical theft of laptops, hard drives and servers, or through the use of USB drives that can be easily plugged into network devices behind your firewall.

Thus, alarm volume alone does not prove strong or weak security. A low number of alarms may reflect good employee behavior and effective controls. It could also indicate that system settings are too permissive, incomplete, or have already been compromised. A high number of alarms may indicate elevated risk, confusing procedures, improperly assigned credentials, or devices requiring service.

What leadership needs to know: Are security entrances consistently enforcing established access policies, and are exceptions being investigated rather than simply recorded and ignored?

Operational Flow Management

Warehouse entrance performance should be evaluated when traffic is at its highest and most chaotic. Measure throughput volume, wait times, queue length, and queue duration during shift changes, breaks, overtime periods, seasonal workforce increases, contractor arrivals, special events, and other high-volume activities.

A delay of only a few seconds per person may appear insignificant when viewed as an isolated event, but when multiplied across hundreds of employees, that small degree of throughput friction can become a measurable source of lost labor time and profits.

First-pass credential acceptance is also important. Repeated credential presentations, biometric fails, reversals, denied entries, and requests for manual assistance typically indicate that there are access issues to be addressed. Segment these events by user group, shift, credential type, and entrance to determine whether the problem is widespread or isolated and to better determine the cause and viable solution.

What leadership needs to know: Are authorized people moving efficiently through secured entrances without compromising controls, creating excessive queues, or generating workarounds?



System Reliability

As previously stated, basic uptime metrics can create a misleading picture of system health, making it important to periodically monitor individual security and operational functions separately. Useful measures include fault frequency, recurring fault patterns, time spent in degraded or manual operation, mean time to acknowledge an issue, mean time to restore full operation, preventative maintenance completion, open service items, and results from emergency-mode testing. Scheduled maintenance of security entrances and related systems is a highly recommended proactive and preventative measure.

What leadership needs to know: Are entrances operating with all intended security and operational functions, and when they are not, how quickly is full performance restored? Equally important is the ability to identify the reasons for disruptions and how to best correct them to avoid future occurrences.

Accountability and Compliance

Warehouse security policies are difficult to enforce without accurate records of access activity and exceptions. Event logs need to be complete, time-stamped, retained according to policy, and correlated when appropriate with access control, video, identity authentication, workforce, and incident records. This becomes especially important in facilities with temporary labor, contractors, high-value inventory, regulated products, or customer-specific security requirements.

Measure the percentage of alarms and exceptions that receive a documented disposition, the time required to close them, unresolved or recurring events, expired or inactive credentials still generating access attempts, and the results of scheduled security tests.

The goal is not simply to prove that an event occurred. The data should help establish what happened, why it happened, how it was resolved, and whether corrective action is required.

What leadership needs to know: Can the organization demonstrate that access policies are working, identify recurring exceptions, and document how security or operational problems were resolved?





ANALYZE PATTERNS. NOT JUST NUMBERS.

The most useful metrics combine related information to turn individual events into patterns that can drive action. For example, an isolated credential retry may be completely inconsequential. Multiple credential retries concentrated at one entrance or during a particular shift may indicate a credential issue, reader problem, enrollment problem, or user behavior that should be investigated. In such instances, a single manual override may be appropriate. Overrides occurring every day during a particular shift change may indicate that entrance capacity, access rules, or operating procedures no longer match actual demand.

Likewise, a single tailgating alarm may reflect an isolated event. A recurring pattern involving the same entrance, shift, or user population may reveal a larger security or process weakness.

Data becomes valuable when it explains where performance is changing, when it is happening, and what may be causing it. Metrics reporting should provide insight that helps improve security and operational performance across the facility. The objective is not to give leadership a dashboard filled with data, but to identify where security, workforce movement, or entrance performance requires attention.

SET DIFFERENT METRICS REVIEW PERIODS FOR DIFFERENT OPERATIONS

Real-time and daily reviews: Monitor active alarms, entrance faults, emergency status, unusual denial patterns, excessive queues, repeated credential failures, and entrances operating in manual or degraded mode.

Weekly and monthly reviews: Examine alarm trends, first-pass credential acceptance, peak wait times, override frequency, recurring service issues, exception closure, temporary credential activity, and changes by user group or shift.

Quarterly reviews and reviews after material changes: Revalidate performance baselines, test controls and access workflows, review system integrations, evaluate capacity assumptions, assess maintenance requirements, and identify potential future investments.

Changes in warehouse metrics can be caused by any of the following:

- Seasonal workers
- Addition of a new shift
- Changes to shift start times
- Facility renovations by contractors
- Addition of new entrances
- Increased throughput or production targets
- A change in credential or authentication technologies
- New access-control software or system configuration
- Changes in high-value inventory or restricted areas
- New customer, regulatory, or compliance requirements

Revisit the performance benchmarks taking any/all of these events into consideration to confirm pre-established standards and detect potential new threats and risks.



TREAT ENTRANCE PERFORMANCE **AS AN OPERATIONAL ESSENTIAL**

Security entrances play an important role in both security and day-to-day operations by managing who enters, when they enter, where they can go, and how reliably access policies are enforced. Like other critical facility systems, entrances require ongoing monitoring to ensure that they continue to perform as intended, support an active workforce, maintain fluid operations, and accommodate evolving security and safety policies and compliance mandates.

The question is not simply whether your security entrances are operating, but whether or not they are performing to their fullest potential across the enterprise.

For more information on assessing your entry/egress systems, please **contact Boon Edam** to speak with our team of warehouse and logistics 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