Tailgating sounds like a simple behavior problem, but in access control it turns into a systems problem. Someone follows an authorized person through a door, gate, or checkpoint, and suddenly your "who should be here" rules lose their meaning. The tricky part is that tailgating is not always malicious. People rush, doors stick, badges fail, and procedures get bent during busy hours. An anti-tailgating system has to catch the unwanted passes without punishing normal human behavior.

Over the years, I have seen the best results come from treating anti-tailgating as a layered design. Hardware that senses presence reliably matters. But so does software logic that knows the difference between a legitimate assistance moment and a true follow-through. Even the most accurate sensor can cause workarounds if the user experience is poor.

This is a practical look at the technologies that can stop tailgating, where they work well, and what trade-offs to plan for before you buy.

The real problem: more than "detect the second person"

Most people picture tailgating as "two people at one card reader." In practice, the event chain varies:

- A valid badge unlock happens, then a second person enters within a short window.
- The second person arrives first, then the authorized person walks up and unlocks the door, and both pass. This is common when teams arrive together.
- Someone holds the door for a coworker, but the coworker's badge fails, and the system thinks it is tailgating.
- A person stops at the threshold for a moment, someone else passes behind them, then the first person exits later. Timing and distance matter.

So an anti-tailgating solution needs more than "detect a face." It needs decision logic tied to your access rules: how long the door remains unlocked, how the reader behaves, whether you have a turnstile or a swinging door, and what assistance policies are allowed.

If you design the system around those rules, you reduce false alarms. If you design around the sensor alone, the result is often either missed events or annoyed staff.

What "works" in anti-tailgating is usually sensing plus context

Anti-tailgating systems fall into a few technology families. Many deployments use one primary method and a supporting layer for resilience.

Video analytics with depth or multi-view cameras

Computer vision has improved a lot, but the key is what the camera can reliably do at your site.

High-performing video-based solutions typically use one or more of these cues:

- Presence detection in a defined zone near the reader
- Person counting or tracking to determine whether a second person is present during an authorized unlock
- Distance estimation, often using depth cameras or stereo setups
- Field-of-view mapping that accounts for where people stand naturally

Where this tends to work best:

- Controlled lanes with consistent approach paths
- Lighting conditions that are manageable, especially if depth sensing is used
- Environments where you can mount cameras at safe, fixed positions and keep them clean

Where it gets harder:

- Highly reflective surfaces or direct glare that confuses segmentation
- Crowded areas where people move in and out of the zone frequently
- Entryways where people approach from multiple angles and the “lane” is not well defined

I remember a retail logistics facility that used a single wide-angle camera to cover several doors. It looked good during the demo, then real traffic patterns appeared. Staff members tended to wait at the side rather than centered in the field of view, and the analytics started treating those waiting positions as “second person near the reader.” The fix was not “turn up sensitivity.” The fix was re-mapping the detection zone and adjusting mounting height to match the actual approach behavior.

The lesson: video systems work, but the installation details and the defined zone matter as much as the algorithm.

Infrared and proximity sensing

Infrared (IR) approaches are common because they can be cost-effective and they behave predictably.

You will see systems using:

- Passive IR presence sensors
- Active IR beams or curtain-like detection
- Proximity sensors placed to cover the entry plane

The upside is clarity. If the system defines a protected zone and detects an additional body passing into that zone, it can trigger an alarm or block the door.

The downside is ambiguity. IR and simple proximity can struggle when:

- People linger close to the sensor without fully entering the lane
- A person bends or leans, changing their apparent presence
- Environmental factors like HVAC drafts, vibration, or dust affect the signal

IR can still be effective when you pair it with timing rules and a clear physical layout. For example, if the door unlocks only long enough for one person to pass, and your sensor placement ensures that a second person will break the zone during that brief window, you can catch most follow-through attempts.

Still, be careful with assist behaviors. If staff are allowed to escort someone with mobility needs, strict beam cutoffs can create constant “violations” that nobody wants to investigate.

Radar and millimeter-wave detection

Radar-based detection has become more practical as hardware costs dropped and processing improved.

Radar can “see” motion and presence through some lighting conditions that make cameras uncomfortable. It can also estimate relative positioning of moving objects.

In anti-tailgating, radar often helps with:

- Detecting additional people entering the protected volume

- Triggering alerts when occupancy exceeds a defined threshold
- Providing presence data for the decision engine

Radar is not magic. It still needs a defined volume and it still has to interpret close-range human motion. People that stand close together naturally can create ambiguous signatures if the system expects larger separation distances.

In one industrial site, radar performed better than camera analytics during shift changes because lighting varied across mornings and nights. But the team had to tune the "two-body at the threshold" timing. A pair of technicians often walked together and arrived at the door within the same second. With the wrong settings, the system started flagging legitimate team arrivals. Once they adjusted the rule to allow a short period for grouped arrivals, the false alerts dropped sharply.

This is the core trade-off with sensing: you either enforce tight rules and risk false positives, or you loosen rules and risk misses. The best systems let you tune that enforcement to your access policy.

UWB and short-range localization (when you can control the environment)

Ultra-wideband (UWB) solutions bring a different approach: instead of identifying people visually, you localize devices or tags with fine time and ranging accuracy. Many deployments use UWB tags inside badges, key fobs, or wearable devices.

In an anti-tailgating context, a common concept is:

- Confirm that an authorized device is within a permitted range of the reader at the moment of access
- Detect whether another person is attempting to pass without an authorized device

UWB can be powerful where:

- You can equip badges or fobs for most users
- The entry area can be planned for consistent signals
- You want robust performance in low lighting and across some weathered surfaces

Where it can be challenging:

- If many users do not have UWB-enabled credentials, you may need bridging methods
- Signal reflections in certain architectural layouts can complicate location thresholds
- Maintenance and charging, if tags are powered devices, become an operational consideration

UWB is also less about "seeing faces" and more about proving proximity relationships. That often aligns well with privacy-conscious deployments, but you still need to plan how you handle exceptions.

Turnstiles and physical barriers with intelligent control logic

Not every anti-tailgating solution has to be "invisible." Turnstiles and controlled gates can prevent follow-through by design, not just by detection.

But the smartest setups still use sensors and logic to avoid punishing legitimate access:

- A turnstile that locks users into one lane is already anti-tailgating by physics.
- The system can still require "one authorization, one passage" and can handle allowed exceptions like authorized assistance.

If your site can support turnstiles, you usually reduce the software complexity because the physical barrier removes most ambiguity. That said, user experience matters. If a turnstile makes it hard for people with mobility aids, or if it adds friction during peak traffic, you will create behavior patterns you did not anticipate.

I have seen organizations install a physical barrier first, then immediately get pushback because deliveries, contractors, and visitors had special cases the barrier did not accommodate. The successful installations planned for those cases from day one, including how staff should escort, how emergency access works, and how to handle badge failures.

What the decision engine should do (and what it should not)

Even with strong sensing, the system has to decide what constitutes a tailgating event. That is where many deployments either succeed or turn into constant alarms.

A good decision engine generally evaluates:

- Door unlock status and the time window during which second-person entry should be flagged
- Occupancy or presence signals in a defined zone
- Tracking consistency, so it does not “double count” the same person if they pause
- A confidence score that supports graceful degradation rather than binary guesses

A system that should be careful:

- Treating any close approach as a violation, without considering legitimate sequencing
- Blocking access too aggressively, especially for first-time users or contractors with badge programming delays
- Ignoring edge cases like door held open during a moment of assistance

The best systems provide operational flexibility. For example, you can alert first and log, or you can block based on a risk threshold. You can also design your workflow so that staff can clear a violation with a supervisor credential rather than having every event become a manual intervention.

Layered architectures that hold up in real life

In the field, the highest reliability usually comes from layering. The exact combination depends on your environment, but common patterns include:

1) Sensing the approach volume (camera, radar, or IR) and validating that it aligns with door unlock timing

2) Correlating the access event (badge reader) with presence signals, not just “someone is near the door” 3) Using a secondary cue to reduce false positives, such as motion direction, a calibrated distance threshold, or a second sensor view

Consider a hospital entry point. People often approach with companions, sometimes because a patient is being helped. A single-sensor system can become hostile quickly. The layered approach lets you require that the companion is present in the violation zone during the authorized unlock, not merely that someone is nearby in the hallway. That nuance dramatically changes the number of false alarms.

Layering also improves failure handling. If the primary camera view is temporarily obscured by dirt or condensation, the system can fall back to another cue. That reduces the “sensor went down, now we cannot enforce policy” failure mode.

Trade-offs you should plan for

When you evaluate anti-tailgating technologies, it is tempting to focus on detection rate. In practice, adoption depends on how the system behaves when it is wrong.

False positives: the operational tax

False positives have a cost. Staff either:

- Start ignoring alerts, which defeats the purpose, or
- Become overwhelmed by investigations, which also defeats the purpose, or
- Create informal workarounds, like letting people enter in groups and hoping nobody triggers the system

If you deploy a camera system in a lane with natural standing positions that look like “two people,” you will get alerts that never get escalated. The best deployments treat tuning as part of the project, not a one-time setting.

False negatives: the compliance gap

False negatives are also a cost, often harder to measure because they only show up when an incident occurs. If your system misses a real tailgating event, you may not find out until later via incident review, badge audit discrepancies, or security reports.

That is why the installation discipline matters. Mount heights, camera angles, and sensor coverage can make the difference between “works in the test room” and “works during rush hour.”

Privacy and policy alignment

Privacy requirements vary widely. Some organizations cannot tolerate facial capture, while others accept video analytics that do not store identity data. Many modern analytics workflows can be configured to perform detection without retaining raw video footage, but you need to verify what is stored, for how long, and who can access it.

If privacy is a concern, systems that rely on proximity, localization, or non-identifying presence counts can be easier to justify. Even then, you should align with your legal and security policies on retention and audit logs.

Practical examples of technology choices

Example 1: Office building lobby, consistent traffic lane

A multi-tenant office lobby often has predictable paths. People approach the reader, pause, and then enter. In that environment, a depth-capable camera or carefully mapped video zone can be effective. Radar can also work, but you will still want to calibrate the expected distance and timing.

If your door remains unlocked for a short period, the system can use that as part of the logic. A tailgater entering after the unlock window will not be flagged, but a true follow-through during the unlock window likely will.

This setup tends to reduce false positives because the approach behavior is consistent.

Example 2: Warehouse dock, mixed lighting and quick movement

Warehouses introduce glare, reflective floors, dust, and dynamic lighting. In these environments, radar or IR can sometimes outperform video analytics because it does not depend as heavily on visual texture.

However, warehouses also create a different challenge: people may pass quickly, cross each other's paths, or approach from slightly different angles depending on staffing. That is where sensor placement and a well-defined protected volume are essential.

A single radar sensor can be effective, but you may also need additional coverage to prevent blind spots.

Example 3: University lab building, high exception volume

Lab buildings usually have frequent visitors, contractors, and researchers who may need assistance. Strict anti-tailgating blocks can become an annoyance machine, so the best deployments focus on alerting and workflow.

In these sites, the technology that works best is often one that can flag violations reliably but can also allow rapid resolution by authorized staff. Layered sensing helps you reduce unnecessary alerts for legitimate escort events.

If you can combine a presence detector with door unlock correlation, you reduce the number of alerts created by normal delays or badge issues.

How to evaluate vendors without getting trapped by demos

Demos are helpful, but they rarely represent your exact traffic patterns. I treat the evaluation like a short proof-of-concept using your own doors, your own badges, and your own movement styles.

Here is a simple way to keep the evaluation grounded.

1) Verify coverage in your lane, not in a generic setting

If the vendor maps a zone on their terms, ask to see how the zone aligns with where people actually stop, stand, and pass. Walk a few real scenarios, including a person pausing to wait for someone and a person trying to enter with a failing badge.

2) Test edge cases, including assistance and grouped arrivals

Invite a couple of legitimate "exceptions" behaviors into the test, like a staff member escorting someone who needs help, or access control companies two authorized users approaching closely together.

3) Ask what gets logged, and what actions you can configure

Do you get an alert only, a block only, or both? How does a supervisor clear an alert? What audit details are available later? If you cannot review and tune behavior after go-live, you will fight the system.

4) Stress the environment you actually have

If your entry area has night shift lighting, reflective floors, seasonal dust, or outdoor glare, test under those conditions. Even a small change in lighting can affect camera-based segmentation.

5) Confirm integration with your access control platform

Anti-tailgating is only as good as the integration with your door control logic. If your access control system triggers unlock in a way that does not align with the anti-tailgating "decision window," you will see either missed tailgates or persistent nuisance alerts.

A key point: ask for the logic model, not just the sensor. You want to know how the system turns signals into a decision.

Designing policies so the technology can succeed

Technology can catch tailgating, but it cannot decide policy by itself. The best results happen when the anti-tailgating enforcement matches how your organization operates.

For instance, if you allow escorts, define when an escort is "allowed" *best access control systems* and how it should be detected. Some organizations issue escort instructions that require a specific badge action or an authorized staff procedure. Others allow escorts but expect staff to intervene when an alert triggers.

You should also consider how your system behaves at peak times. If your doors are used heavily during shift change, the system should be tuned so it does not treat crowding as an automatic violation. That is where layered detection and well-defined timing windows can help.

One practical takeaway: build a feedback loop. After installation, review a weekly sample of events and tune thresholds based on what you see. Many of the worst deployments happen when teams set a threshold once and never revisit it.

Operational considerations that often decide success

Even if the detection is strong, anti-tailgating systems can fail due to operations.

- Maintenance of sensors matters, especially cameras. Dust, fingerprints, and condensation can degrade performance.
- Training matters. If staff do not know how to handle an alert quickly, they will stop responding.
- Commissioning time matters. Calibrating zones and timing windows is not optional if you want low false positives.

Another practical factor is how your credentials behave. If badge readers fail frequently, users will naturally hold the door, wait for help, or enter in groups. Anti-tailgating can only enforce policy if the authorized access workflow is reliable. Fixing badge readability and reader maintenance can reduce tailgating incidents indirectly.

When you should combine anti-tailgating with stronger access patterns

Anti-tailgating is most effective when it does not have to do all the work. In higher security environments, you may also want to rethink how people enter.

For example:

- Add a short controlled vestibule or airlock-like spacing if you can.
- Require two-step verification for certain zones, not for general entry.
- Use controlled lanes with physical guidance so people naturally funnel through the detection zone.

These are not always feasible, but they can reduce the uncertainty that sensors otherwise have to interpret.

Choosing the right technology for your site

No single technology dominates every environment. The best fit depends on your traffic flow, lighting, privacy requirements, and tolerance for false alerts.

Video analytics can be very effective in consistent lanes, especially with depth cues and careful zone mapping. Radar and IR can be strong where lighting and visibility are challenges, but they rely heavily on volume definition and timing logic. UWB localization can provide a robust proximity relationship when credentials are properly

equipped and the environment supports stable signals. Physical barriers can prevent tailgating by design, but they require thoughtful accommodations for accessibility and exceptions.

If you treat it as a full system, not a sensor purchase, you end up with fewer surprises and a better user experience. The most convincing anti-tailgating deployments feel almost boring to users, because they only intervene when something truly does not match policy.

That is the goal. Stop the unauthorized passes, protect your access rules, and let everyone else move through the doorway without friction.

A short checklist to take into your next project meeting

Here is what I would ask in the first technical call, before talking price.

- What exact behaviors count as a tailgating event in our policy, including escorts and grouped arrivals?
- Which sensing method is primary, and what is the fallback?
- How are detection zones and timing windows calibrated to our door mechanics?
- What happens on alerts and how can staff resolve them quickly?
- What integration details exist with our current access control system?

If you can answer those questions clearly, you are far more likely to end up with anti-tailgating that actually works after the installation day.