10 Questions to Ask Before You Upgrade Your Physical Security System

Whether you manage security for a single facility or an entire enterprise network, your access control and monitoring systems are critical to the safety, compliance, and operational flow of your business.

But is your current system actually keeping up with today's risks — and tomorrow's needs?

Use this checklist to evaluate where your current physical security setup may be falling short and what to look for in your next upgrade. These questions apply across industries — from auto dealerships and property management to cannabis facilities, logistics hubs, and airports.

1 Are we still relying on manual processes to detect or respond to security incidents?

In many facilities, monitoring still depends heavily on humans watching live feeds, reviewing logs manually, or responding to alarms without context. While trained staff are invaluable, relying solely on manual processes comes with limitations:

- Human fatigue leads to missed events or slow response times
- Small security teams can't watch dozens of cameras at once
- Reviewing hours of footage after an incident is inefficient
- Most incidents are only discovered after damage is done

Today's physical security environment demands more automation and intelligence. AI and machine learning can now augment human oversight by identifying unusual patterns, detecting policy violations (like propped doors), and surfacing real threats in real time.

🔍 Hakimo Insight: Hakimo's platform uses AI to monitor badge-based access control events and video feeds simultaneously — detecting incidents like tailgating without needing constant human review. This isn't about replacing your team; it's about amplifying their effectiveness.

2 How many false alarms or unnecessary alerts are we dealing with each month?

False alarms are a persistent, often underestimated problem in physical security. Whether it's a door forced open by wind or a misconfigured sensor, false positives can cost teams countless hours and erode trust in the system:

- Security staff waste time investigating non-incidents
- Alarm fatigue sets in, increasing the chance of real threats being ignored
- Response protocols get delayed or bypassed altogether
- Facilities may face fines from authorities for repeat false alarms

Understanding your false alarm volume — and its root causes — is essential before investing in any new system. If you're not tracking false alarm metrics, that's your first red flag.

🔍 Hakimo Insight: Hakimo's AI filters out common false alarms by correlating access data with visual confirmation from video feeds, reducing noise and helping teams focus on what matters. But even if you're not ready for a platform like Hakimo, start by identifying the top three causes of false alerts and whether they stem from hardware, software, or policy.

3 Are we vulnerable to tailgating or unauthorized piggybacking at entry points?

Tailgating — when someone follows an authorized person into a secure area without badging in — is one of the most common and under-monitored risks in physical security. It's also notoriously difficult to detect in real time without dedicated personnel at every door.

Why it matters:

- Tailgating undermines the integrity of access control systems
- It creates challenges for compliance and auditing
- In regulated industries, tailgating can lead to citations or legal issues
- It puts people and assets at risk if unauthorized individuals gain entry

Some organizations attempt to mitigate this with signage or turnstiles, but these measures are often insufficient or ignored. More advanced setups may include mantraps or security guards — but these solutions are expensive and don't scale well.

🔍 Hakimo Insight: Hakimo uses computer vision to automatically detect tailgating events at badge-controlled doors, tagging incidents and correlating them with access logs. But regardless of your tech stack, consider auditing access points for tailgating vulnerabilities and identifying where your risk is highest — such as employee entrances, shipping bays, or visitor-accessible lobbies.

4 Do we have centralized visibility across all our sites and entry points?

Many organizations grow faster than their physical security systems can keep up. It’s common to see a patchwork of camera feeds, access control systems, and security protocols that vary by location or even by door. This lack of centralized oversight causes:

- Inconsistent security standards across sites
- Slow response times when incidents occur
- Difficulty training or scaling security teams
- Redundant tech spend due to disconnected tools

Especially for multi-site businesses — like property managers, airport operations, auto dealership chains, or cannabis cultivation/retail networks — centralization is no longer optional. Your team should be able to log into one dashboard and see real-time security data across all facilities.

🔍 Hakimo Insight: Hakimo offers centralized incident management, reporting, and real-time alerting across multiple facilities. That means a director of security can monitor tailgating events at 20 properties from one interface. If you’re not quite there yet, ask: Can our current system give us a unified view of access and incidents across all our doors and sites?

5 Is our current system giving us usable insights — or just raw video footage?

Video surveillance is essential, but the value is limited if your team is stuck reviewing hours of footage to understand what happened. Many legacy systems record data — they don’t interpret it.
Without context and analysis, video is reactive, not proactive.

Modern security solutions should:

- Flag abnormal behavior proactively (e.g., lingering near access points)
- Highlight policy violations like propped doors or unauthorized access
- Provide summaries or reports your team can act on — not just camera logs
- Help spot trends (e.g., which locations have more incidents)

🔍 Hakimo Insight: Hakimo turns raw video and access events into actionable dashboards — showing you where tailgating is increasing, which doors see the most violations, and when incidents are likely to occur. But even without automation, ask yourself: How long does it take to generate useful security intelligence from your system today? If it’s hours — or days — you’re likely missing opportunities to prevent incidents altogether.

6 How easily can we audit access and generate compliance reports?

In regulated industries — like cannabis, healthcare, and aviation — compliance isn't optional. You may need to prove:

- Who accessed a secure area and when
- Whether dual-authentication protocols were followed
- That unauthorized access was logged, reported, and addressed
- That you have a complete audit trail for inspections or investigations

If you're manually stitching together logs from access control systems and video platforms, you're exposing yourself to errors — and wasting hours of staff time.

🔍 Hakimo Insight: Hakimo auto-generates compliance-friendly incident reports that connect badge data to corresponding video events, making it easy to demonstrate policy enforcement. But whether or not you use an automated platform, ask: Could your team respond to an audit request today, within a few hours, with the proper documentation?

7 Does our physical security system integrate with the rest of our technology stack?

Security doesn't operate in a vacuum. Your access control system, camera infrastructure, identity provider, and building management tools should talk to each other. Without integration, you face:

- Manual data reconciliation
- Higher chance of configuration errors
- Silos between security and operations
- Slower response to incidents or threats

Look for solutions that support open standards, robust APIs, and plug-and-play compatibility with leading platforms.

🔍 Hakimo Insight: Hakimo integrates with top access control platforms (like LenelS2, Genetec, Openpath, and more), helping you get more value from what you already use. Even if you're early in your modernization journey, prioritize tools that won't lock you in or require expensive custom work to integrate down the line.

8 Are alerts timely, actionable — and not overwhelming our team?

A system that notifies you of every door left open or minor policy violation sounds helpful — until your team starts ignoring the alerts because they're overwhelmed. The ideal setup filters and prioritizes:

- High-severity incidents (e.g., repeated tailgating at restricted areas)
- Patterns across time or location (e.g., one facility with more violations)
- Actionable events tied to identities and context
- Real-time alerts only when they require a response

Too much noise? Fatigue. Too little noise? Blind spots.

🔍 Hakimo Insight: Hakimo classifies alerts by severity, provides video context, and notifies only the right people — reducing noise while speeding up response. No matter what system you use, consider: Does your team trust the alerts they receive? Or are they tuning out — possibly missing something important?

9 Can we quickly identify who was responsible for an incident?

When something goes wrong — a restricted door is accessed, a visitor enters a secure area, a package goes missing — you need answers fast. Without the ability to tie badge credentials to physical movement captured on video, investigations can stall or rely on guesswork.
Common pain points:

- Incomplete or missing access logs
- Video footage without time-stamped access context
- Shared credentials or unverified badge use
- Slow cross-referencing across disconnected systems

🔍 Hakimo Insight: Hakimo correlates video with access events, badge credentials, and location data — giving you a full chain of evidence in seconds. Even if your system doesn't offer this today, you should be asking: How long does it take us to investigate a simple security incident from start to finish? If the answer is "more than an hour," your system is slowing you down.

Is our system scalable, flexible, and built for the future?

Finally — it’s not just about solving today's challenges. Your physical security investment should support:

- Growing teams, locations, or compliance requirements
- Remote management and reporting
- Integration with future tools or platforms
- Evolving threats, from insider risk to policy enforcement gaps

Think of your system as infrastructure — not a short-term fix.

🔍 Hakimo Insight: Hakimo was built to scale across multi-site enterprises, adapting to new locations, user roles, and use cases with minimal friction. As AI improves, Hakimo’s detection gets smarter over time. When evaluating vendors, ask: Will this system still meet our needs two or three years from now? Or will we be back at square one?

🧩 Bringing It All Together

Upgrading your physical security system doesn’t have to be overwhelming — but it does require asking the right questions.

This checklist was designed to help you evaluate your current security posture from all angles:
✅ People — Are your teams empowered or overburdened?
✅ Process — Are your policies enforceable, and are alerts actionable?
✅ Technology — Is your stack helping you stay ahead of threats, or just recording them?

As you reflect on your answers, consider grouping your priorities into three tiers:

1. Immediate Gaps – Issues like frequent false alarms or lack of access auditability that are actively costing time, money, or compliance risk.
2. Scalability & Visibility – Gaps in multi-site management, tailgating detection, or fragmented systems that limit your ability to grow securely.
3. Future-Proofing – Consider whether your current tools can adapt to AI-driven automation, tighter compliance needs, or a leaner security team in the future.

Once you’ve identified your must-fix-now items and your nice-to-have improvements, the path forward becomes much clearer.

🚀 Where Hakimo Fits In

Hakimo is built to solve the exact problems outlined in this checklist — not by replacing your entire system, but by making it smarter.

We help companies:

- Reduce false alarms by up to 80% using AI-powered filtering
- Detect tailgating and access violations automatically — without the need for additional hardware
- Correlate badge data with video to streamline investigations and compliance
- Unify incident visibility across multiple locations and doors
- Scale securely with centralized dashboards, role-based access, and audit-ready reporting

Whether you're running a single high-risk facility or a national portfolio of properties, Hakimo gives you the intelligence layer your physical security system needs.

👉 Want to see how it could work for your team?

Schedule a personalized demo or download a sample analytics report to learn more.

www.hakimo.ai

Hakimo