

Trafficking-Risk Detection Pilot: Budget-Hotel Retrofit & Acquisition Estimate

Cost to add red-flag detection technology to a budget hotel, plus a plain-language summary of every component.

Prepared for James Polk · August 4, 2026

The concept, in plain terms

Based on what we've discussed previously, the concept is **not** to create a surveillance hotel. Instead, it is to create a technology-enabled budget hotel that **passively aggregates operational data, computes trafficking-risk scores from multiple independent indicators, and routes higher-risk situations to trained personnel for verification before anyone contacts law enforcement.**

The design intentionally avoids intrusive in-room surveillance — no microphones or thermal monitoring inside guest rooms — and relies primarily on operational metadata and common-area information.

Estimated cost to retrofit a budget hotel

Assuming a 50-room economy hotel (Motel 6, Super 8, America's Best Value Inn, or similar):

Component	Estimated Cost
Existing IP camera upgrades (AI-capable where needed)	\$10,000–30,000
Additional hallway / common-area cameras	\$10,000–20,000
Smart-lock integration (if replacing)	\$15,000–40,000
Occupancy / door sensors	\$4,000–8,000
Hallway decibel sensors	\$2,000–5,000
Network upgrades	\$5,000–15,000
Local AI server	\$6,000–15,000
Software development / MVP	\$100,000–300,000
PMS integration	\$20,000–60,000
Dashboard / alert software	\$30,000–80,000

Component	Estimated Cost
Installation / labor	\$15,000–40,000
Total retrofit (MVP)	~\$220,000–600,000

If you buy a hotel that already has modern cameras, electronic locks, a PMS, and reliable networking, the retrofit could drop to roughly **\$150,000–\$300,000**.

Purchasing the hotel

Typical prices (very approximate):

- 40–60 room independent motel in a lower-cost market: **\$2–5 million**
- Older motel needing renovation: **\$1.2–2.5 million**
- Better-performing branded economy hotel: **\$4–8 million**

WHAT A FIRST PILOT COULD REALISTICALLY REQUIRE

Hotel purchase	\$2.5M
Technology retrofit	\$350K
Initial operating reserves	\$400K
Legal / compliance / insurance	\$250K
Approximate first-pilot capital	~\$3.5–4 million

My recommendation for the MVP

Rather than inventing a large amount of new hardware, I'd focus on proving that **software creates the value**. A strong first version could leverage systems many hotels already have: existing security cameras (privacy-conscious analytics in common areas only), PMS data, electronic-lock logs, Wi-Fi metadata, key-card events, and housekeeping / front-desk records.

Those inputs can feed a risk-scoring engine and management dashboard with far less capital than replacing every device. If the software demonstrably reduces trafficking risk or improves detection while respecting privacy and legal requirements, it becomes much easier to justify expanding the hardware footprint and, ultimately, licensing the platform to other operators.

Summary of the items — what each one is

A plain-language glossary of every component in the concept, grouped by category.

Existing hotel systems (data already generated by normal operations)

Property Management System (PMS)

The hotel's core booking/operations software — reservations, check-ins, room status. The main source of stay and turnover data.

Electronic key-card system

Records which card opened which door and when, giving a timeline of room access.

Booking history

Past reservation records used to spot repeat patterns (same guest, room, or behavior over time).

Payment metadata

How a stay was paid for (cash, prepaid, card) — not card numbers, just the pattern of payment.

Wi-Fi network metadata

Counts of devices connected in a room/area — a rough proxy for how many people are present.

Guest registration

Standard check-in information collected at the front desk.

Housekeeping records

Cleaning logs and room-service notes that can flag unusual room conditions.

Physical devices (mostly common-area, privacy-conscious)

Hallway cameras

Common-area cameras that observe foot traffic to and from rooms — not inside them.

Parking-lot cameras

Watch vehicle arrivals/departures; support repeat-vehicle analysis.

Exterior cameras

Cover building entrances and perimeter.

Common-area cameras

Lobby and shared-space coverage.

Door-open sensors

Simple sensors that log when a door opens/closes, showing frequency of comings and goings.

Smart-lock events

Digital record from smart locks of every lock/unlock, including duplicate or repeated key use.

Hallway decibel sensors

Measure noise *level* in hallways (loudness only — **not audio recording or content**).

Stairwell occupancy sensors

Detect movement/presence in stairwells to gauge unusual traffic flow.

Parking occupancy cameras

Track how full the lot is and which vehicles recur.

Operational indicators (the "red flags" the system watches for)

Individually these are ordinary; the system looks for **combinations** that, together, raise a risk score:

- Cash / prepaid payment patterns
- Short stays
- High room turnover
- Multiple duplicate key requests
- Excessive "Do Not Disturb"
- Numerous visitors to one room
- Late-night visitor traffic
- Foot traffic into rooms
- Wi-Fi device counts
- Frequent room changes
- Guest age disparities (where lawful and appropriate)
- Staff complaints
- Maintenance observations
- Housekeeping observations

AI analysis (how the data becomes a risk score)

Weighted red-flag scoring

Each indicator contributes a weighted amount to an overall risk score.

Time-series & cross-day pattern analysis

Looks at how patterns build over hours and days, not just single events.

Repeat guest / vehicle / room analysis

Detects the same people, cars, or rooms recurring in suspicious ways.

Risk prioritization & confidence scoring

Ranks situations so staff attention goes to the highest-confidence, highest-risk cases first.

Human workflow (people, not algorithms, make the calls)

Manager review → Security review

Flagged situations are checked by trained staff before any action.

Welfare check where appropriate

A discreet, appropriate check on guest wellbeing.

NGO notification

Alert an anti-trafficking non-profit, depending on protocol.

Law-enforcement referral

Only after corroboration — never automatically from a score alone.

Intelligence layer (previously discussed integrations)

DeliverFund intelligence sharing

Connect with an anti-trafficking intelligence organization for shared insight.

Docuption Forms workflow automation

Use your forms platform to automate reporting/case paperwork.

Secure encrypted reporting

Protected channels for sensitive reports.

Cross-hotel pattern detection

Spot patterns that span multiple properties.

Historical incident database · Case management · Audit logs

Store past incidents, manage cases end-to-end, and keep tamper-evident records of who did what.

Phase 2 ideas (after the first hotel proves the model)

- Multi-hotel analytics
- Franchise software licensing
- SaaS subscriptions
- Managed monitoring service
- Insurance risk reduction
- Corporate security dashboards
- NGO collaboration
- OSINT integration
- Law-enforcement intelligence portal
- National trafficking-trend mapping

Design principle throughout: intrusive in-room monitoring (microphones, thermal sensing inside guest rooms) is intentionally excluded. The system favors operational metadata and common-area signals, with humans verifying before escalation.