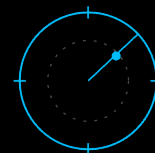


ASF FIELD BRIEF

06 / 06

FREQUENTLY ASKED QUESTIONS



Straight answers.

For the person who answers for the outcome — and for the CFO, CISO, General Counsel, and procurement team reviewing this alongside you. If a question is not answered here, ask it in a briefing: knightscope.com/briefing

What exactly is the Autonomous Security Force?

One managed security operation under a single contract: autonomous machines, AI-driven software, and licensed Security Agents and Executive Protection Agents, operated by Knightscope as one accountable entity. You do not buy robots from one vendor, monitoring from another, and guards from a third. You command a Force, and Knightscope answers for the outcome.

Is this about replacing my people with robots?

No. Machines handle the monotony: patrol, detection, watching everything at once without fatigue. Humans handle what machines cannot: judgment, de-escalation, presence, and response. Autonomy makes the humans more effective; it does not remove them.

What is the ASF-7 Escalation Model?

The operating structure of the Force: seven levels, three layers. Levels 1–3 are autonomous — detection, AI agents, orchestrated autonomy. Levels 4–5 are remote command — Mission Intelligence Analysts and Leads verifying what the machines see, 24/7, against a digital twin of your site. Levels 6–7 are physical response — licensed Security Agents and, where legally required, law enforcement engagement. An accountable human holds escalation authority at every level, every hour of every day.

Who verifies alerts before anything reaches me?

Mission Intelligence — Knightscope's own remote command layer, staffed around the clock. Analysts verify every alert before escalation. You hear about what matters, and nothing else. Every verification, decision, and action is logged, timestamped, and exportable in the Signals orchestration software platform.

Are your agents employees or subcontractors?

Employees. Every security agent is licensed under the laws of the state where they serve, screened beyond industry minimums, and trained on Knightscope protocols. Agents hold equity in Knightscope, Inc., receive full health benefits, and start paid training on day one. The guard industry's 100%+ annual turnover is what happens when a job is treated like a shift; the Force is built as a career.

Who owns Knightscope, and where does my security data live?

Knightscope is American-owned and controlled: publicly traded (NASDAQ: KSCP), U.S.-only operations, no foreign parent company. Your security data — vulnerabilities, patrol patterns, response times — stays under U.S. jurisdiction, with a vendor accountable to U.S. regulators, auditors, and courts. Ask your incumbent who ultimately owns them, and in what country their controlling investors sit.

What is your cybersecurity posture? Will my CISO sign off?

The Knightscope platform holds a FedRAMP Moderate Authority to Operate for federal deployments — and work is underway for the entire stack to be U.S. Federal Government cybersecurity grade for all commercial and government clients: FedRAMP High and Department of Defense Impact Level 5. As a public company, Knightscope operates under audited financials, an independent board, and SEC reporting. We will walk your CISO through the architecture, data handling, and integration posture directly; that conversation is part of every briefing where the CISO wants a seat.

How is it priced?

One managed-service contract scoped to outcomes: the coverage your locations need, not hourly headcount and not a per-device SKU. The architecture — the mix of machines, sensing, remote command, and licensed agents — determines the price, and it is designed per site before anything ships. You see exactly what you are paying for and what it replaces. And planned to improve over time.

Can this consolidate my existing vendors?

That is the point. A typical program splits guards, cameras, monitoring, and executive protection across three or four contracts, each with someone else to blame. The Force replaces that patchwork with one contract, one escalation path, and one accountable entity. In a briefing, we map your current vendor stack against the Force and show you exactly what consolidates.

What happens during an actual incident?

Deter, detect, respond, learn — one loop. Detection is verified by Mission Intelligence before escalation. The response is matched to the situation: talk-down through the machines, dispatch, agents on the ground, law enforcement where legally required. Every step is logged, timestamped, and exportable — and every incident feeds the system, so the Force gets sharper with each one.

How do I prove to my board that it is working?

With data, not anecdotes. Every patrol, alert, verification, escalation, and response is logged and exportable. A Mission Success Specialist is your standing point of contact once the Force goes live. You brief the board with a verifiable record, not an explanation.

Do you cover executive protection?

Yes. Licensed Executive Protection Agents operate under the same command layer as the rest of the Force: the principal, the family, the home, and the assets, protected as one continuous relationship rather than a series of bookings. A capability of the Force — not a separate vendor and a separate contract.

Is everything autonomous on day one?

No, and it should not be. The Force is architected per site: some locations start agent-forward and add machine density over time; others lead with autonomous patrol from the start. The architecture follows your risk profile, not a product catalog. What is constant from day one is the model: one contract, one escalation path, one accountable entity.

What can the Force not do?

The Force is not law enforcement: agents operate under state licensing and the law, and Level 7 exists precisely because some situations belong to the police. Machines do not make judgment calls; humans do, and the system keeps an accountable human in the loop at all times. No security program eliminates risk — the Force is built to detect it earlier, respond faster, and document everything, so nothing lands on your desk unexplained.

What happens in a briefing?

You tell us what you are accountable for, by location. No demo, no pitch. We come back with the architecture: the mix of machines, sensing, remote command, and licensed agents built for your sites, shown in a digital twin before anything ships.

13

YEARS

434

CLIENTS

42

U.S. STATES

4.4M+

AUTONOMOUS HOURS

Ask the rest in person. Tell us what you are accountable for — knightscope.com/briefing