The State of Physical Security 2026

Benchmarks, Challenges, and Priorities



CRAM

Contents

2 Executive Summary

6 Key Findings at a Glance

9 Methodology

11 Where Teams Stand Today

14 The Investigation Problem

16 What Teams Are Prioritizing, and Why It Is Hard

19 Getting More From What You Already Own

22 What AI Actually Changes

25 Five Moves the Benchmark Points To

26 Where the Industry Is Headed

Physical security has evolved well beyond video surveillance.



It now spans the technologies organizations rely on to protect people, facilities, and operations: video, access control, guest management, emergency response, and increasingly AI-driven threat detection. Most teams, though, have built that stack one purchase at a time, and this report is a benchmark of where that leaves them, drawn from a survey of 476 security, IT, operations, and facilities leaders and based on the 241 verified responses that passed our quality screening.

The clearest gap is operational, not technological.

46.5%

take more than **30 minutes** to find the right footage after an incident, including **27.4%** who take more than an hour.

Connectedness tracks with speed:

teams running everything in one place find footage within 30 minutes **64.8%** of the time, versus **41.7%** of those whose systems operate separately.

Teams can picture the system they want.
They just can't get the budget to sign off on it.

80.9%

would prefer one connected system

only

22.4%

have a connected system today



At the same time, 84.2% believe they could keep some or all of their existing cameras, and 95.0% find plain-language footage search useful even though only 34.4% consider AI itself a must-have.



95%

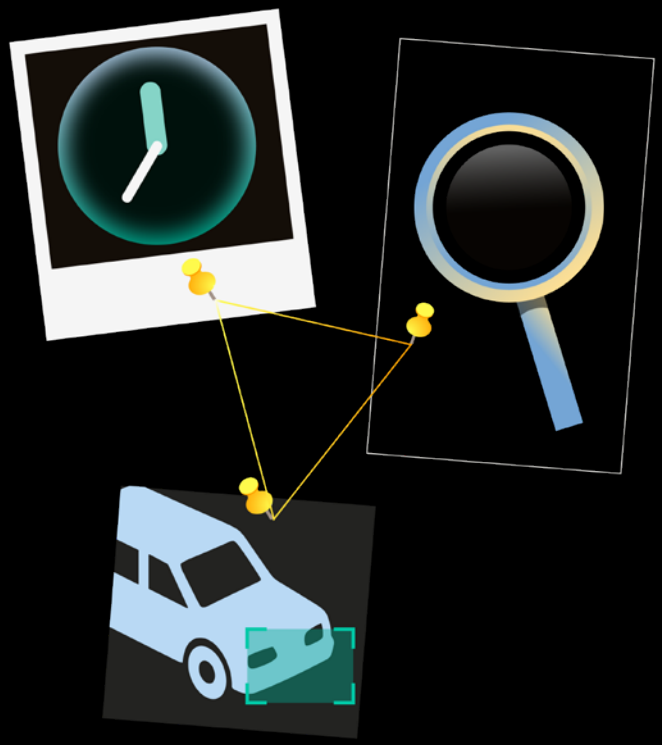
find plain-language footage search useful

34.4%

consider AI itself a must-have.

The opportunity is not to buy more technology. It is to get real connectivity and coordination out of the infrastructure and hardware teams already have.

Key findings



INVESTIGATION TIME

46.5%

Nearly half need more than 30 minutes to find footage

UNIFIED PLATFORM

80.9%

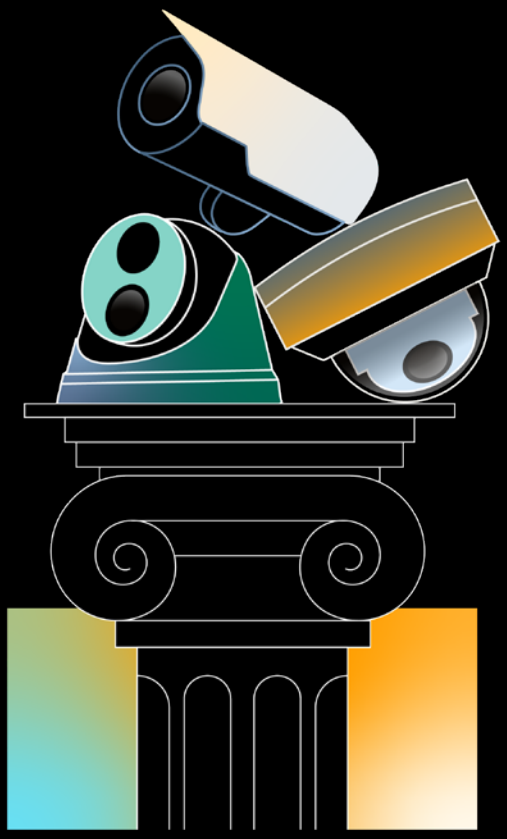
Teams want connected operations



EXISTING INFRASTRUCTURE

84.2%

Most expect to keep their existing cameras

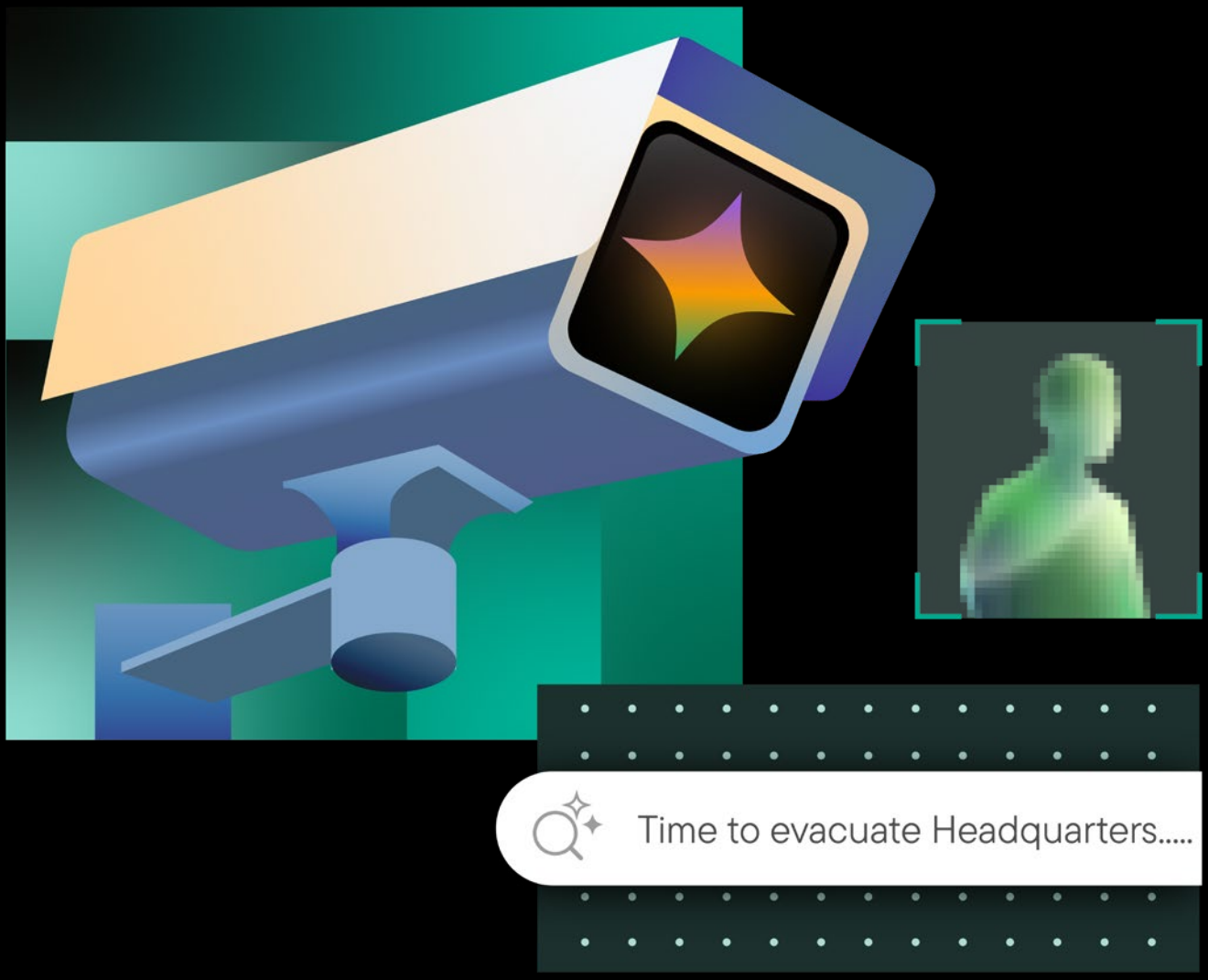




BUDGET & ROI

76.8%

Budget and value-proof compound each other



AI IN PHYSICAL SECURITY

90.5%

Specific AI outcomes outperform the AI label

Methodology

476 responses collected for the survey*

241 included in final analysis. Spanning **seven industries.**

70%

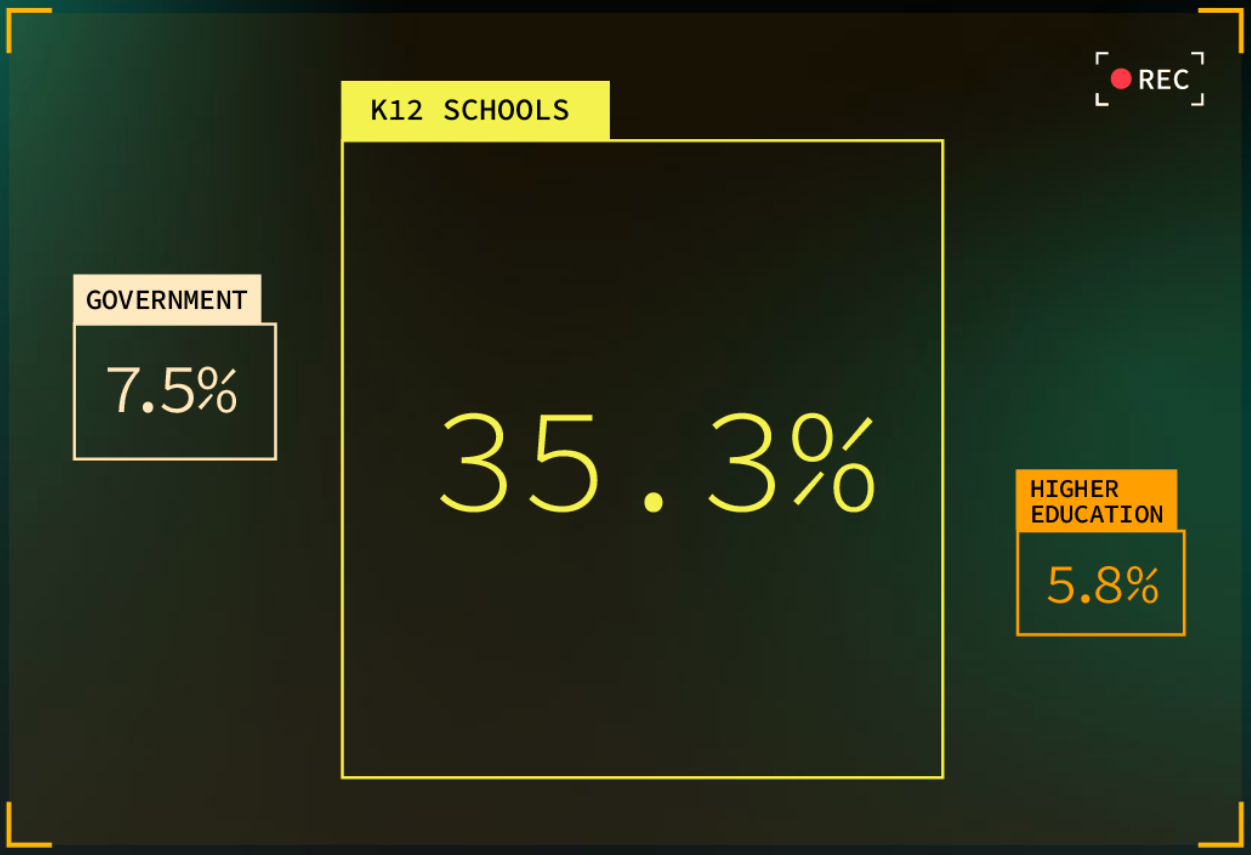
Director-level or higher titles

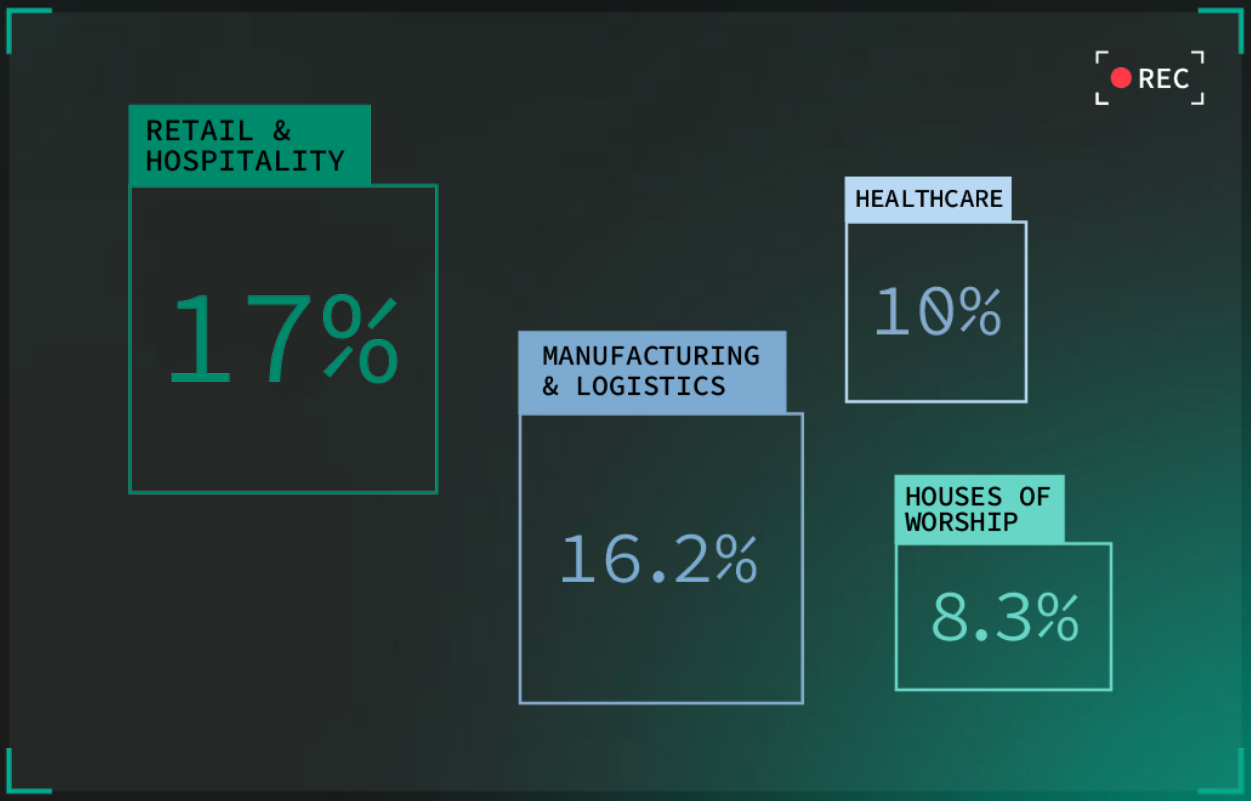
61%

IT respondents

*The survey was fielded from June 23 through July 15, 2026.

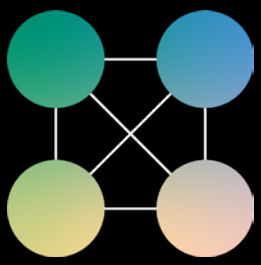
Who responded by Industry





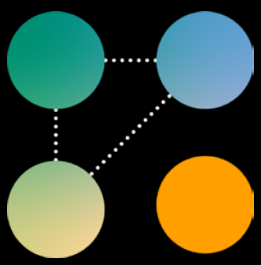
Where Teams Stand Today

Our findings describe an industry at an inflection point. Organizations keep investing in security technology, but those investments have largely been made one solution at a time, so most teams are now running multiple systems that were never designed to work together.



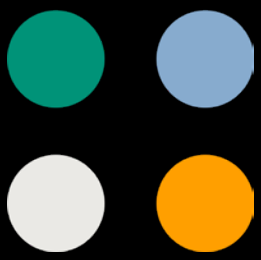
Manage physical security from a fully integrated platform

22.4%



Have a few systems connected and the rest separate

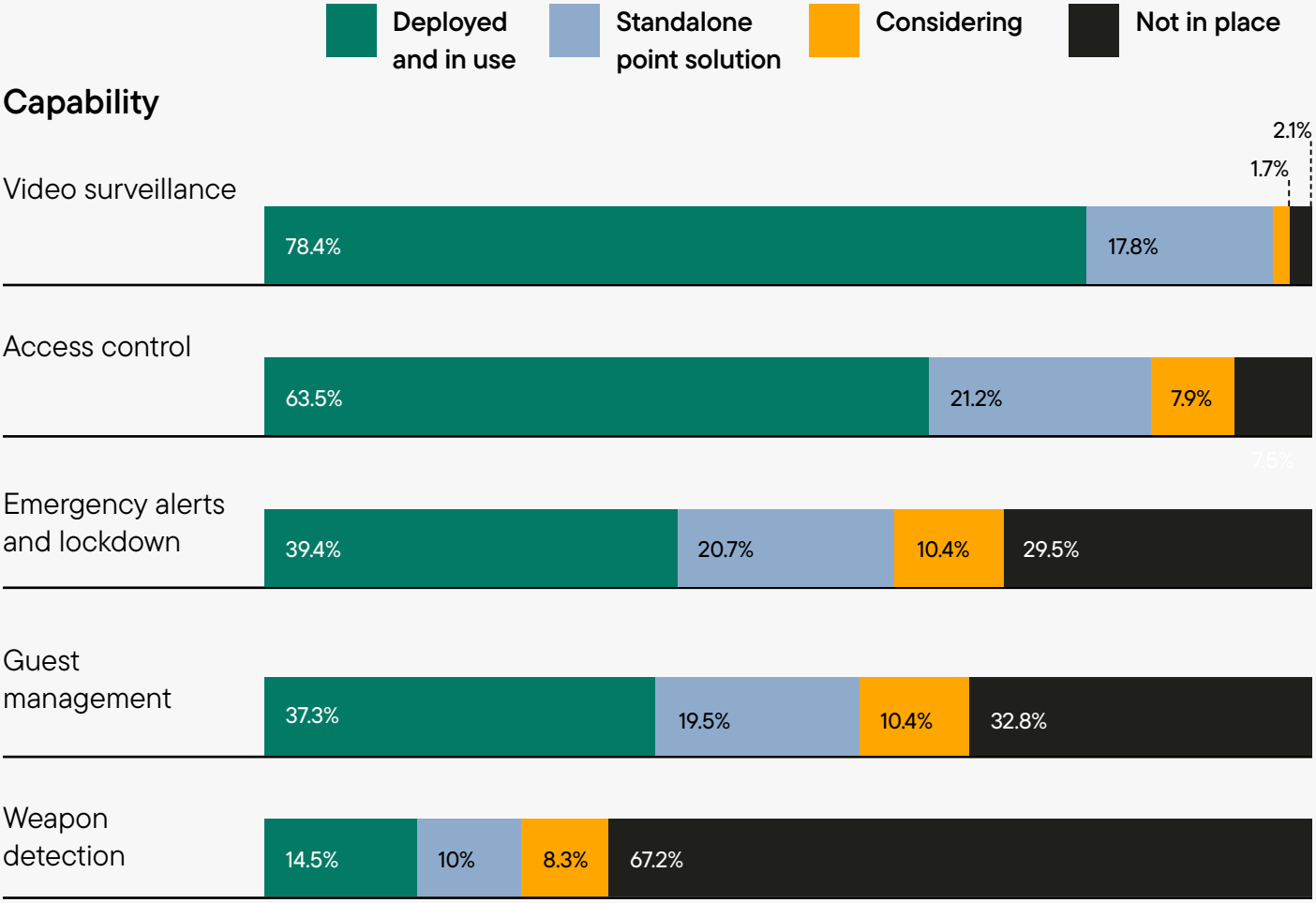
42.7%



All run separately

34.9%

The challenge isn't access to technology. It's fragmentation. Disconnected systems force teams to switch between applications, and they make it harder to investigate incidents, coordinate a response, and keep a complete picture of what is happening. As security becomes more proactive and AI-assisted, those silos matter more, because the value comes from connecting data across every function.



Adoption reinforces the pattern. Most teams already have the core capabilities in place. The issue is how much of it runs in isolation instead of as part of a connected system. Video surveillance is nearly universal and access control is close behind, yet each is run as a standalone point solution by roughly one in five teams (17.8% for video, 21.2% for access). The remaining capabilities are both less common and, where present, still frequently siloed: emergency alerts are in place at 60.2% of organizations, guest management at 56.8%, and weapon detection at just 24.5%. The story is about how little of it works together.

Where teams keep their footage is shifting too.



23.2%

Choose fully on-site



31.1%

On Cloud storage



45.6%

Hybrid storage

Most of these teams also operate at scale: nearly 70% run more than one location, which is exactly where fragmentation starts to become a problem.

The Investigation Problem

Disconnected systems have a cost, and it shows up in the one activity these systems exist for: investigations. When systems don't share data, the context is scattered, and finding out what happened means stitching the evidence together by hand.



46.5%

of teams take more than **30 minutes** to find the right footage after an incident

27.4%

take more than **an hour**

7.9%

take **under two minutes**

That's a long time to be searching mid-incident.

No school office would spend half an hour flipping through files to pull a student's record, and no clinic would accept that to find a patient's chart.

The cost compounds with volume, and the stakes aren't abstract. 18.3% of teams run six or more investigations a month, and the clock is often running on something real: a theft in progress, an injury that needs documentation, a firearm or access alert that needs confirmation. Footage on local storage can age off and vanish before anyone finds it, and the insurance claim or legal case that follows can hinge on whether it still exists.

Coordination is the clearest lever. Teams with everything in one place find footage within 30 minutes 64.8% of the time, versus 41.7% where systems operate separately, a 55% higher hit rate. **That gap widens with scale.** Camera count showed no such pattern, so how footage is organized matters more than how much of it there is.

HITTING THE 30 MIN MARK

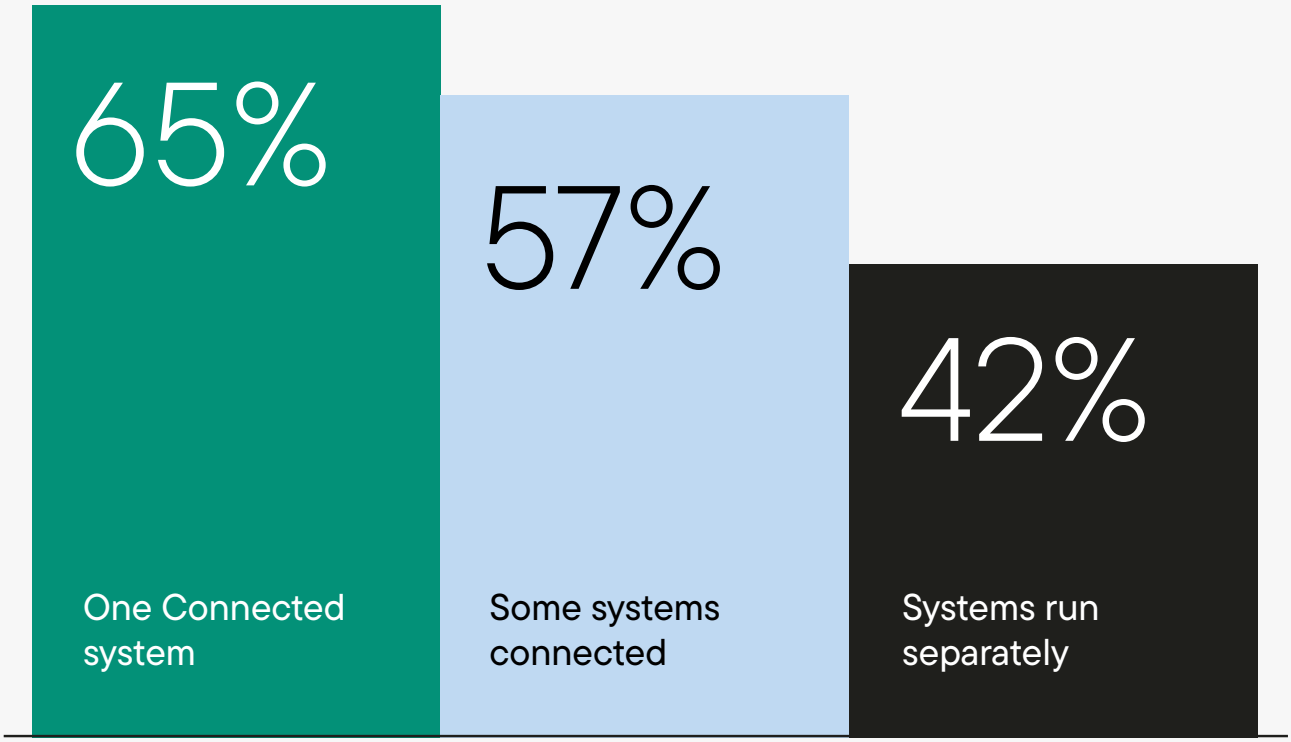
59.5%

single-location teams

30.8%

organizations running 51 or more sites

Teams that connect their systems find footage faster



Connectivity gets a team most of the way there. The real gain comes from being able to describe what you're looking for and go straight to it, which the 7.9% already hitting under two minutes are proving is possible.

What Teams Are Prioritizing, and Why It Is Hard

The priorities teams name are operational outcomes, not technology categories:



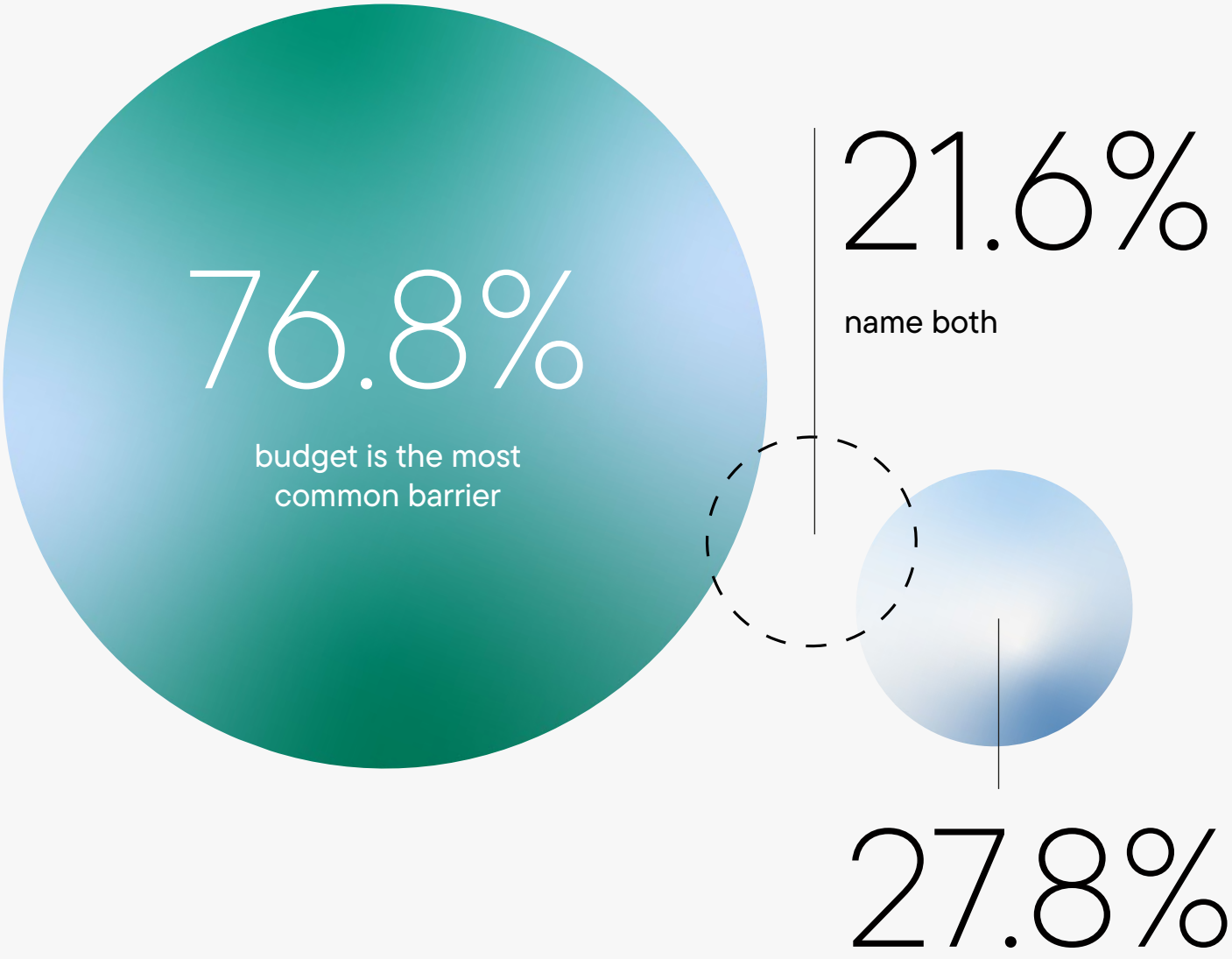
81.3%
want to improve safety and threat response

51.9%
want faster investigations

46.5%
want to expand coverage

None of that requires starting over.

Budget is the most common barrier

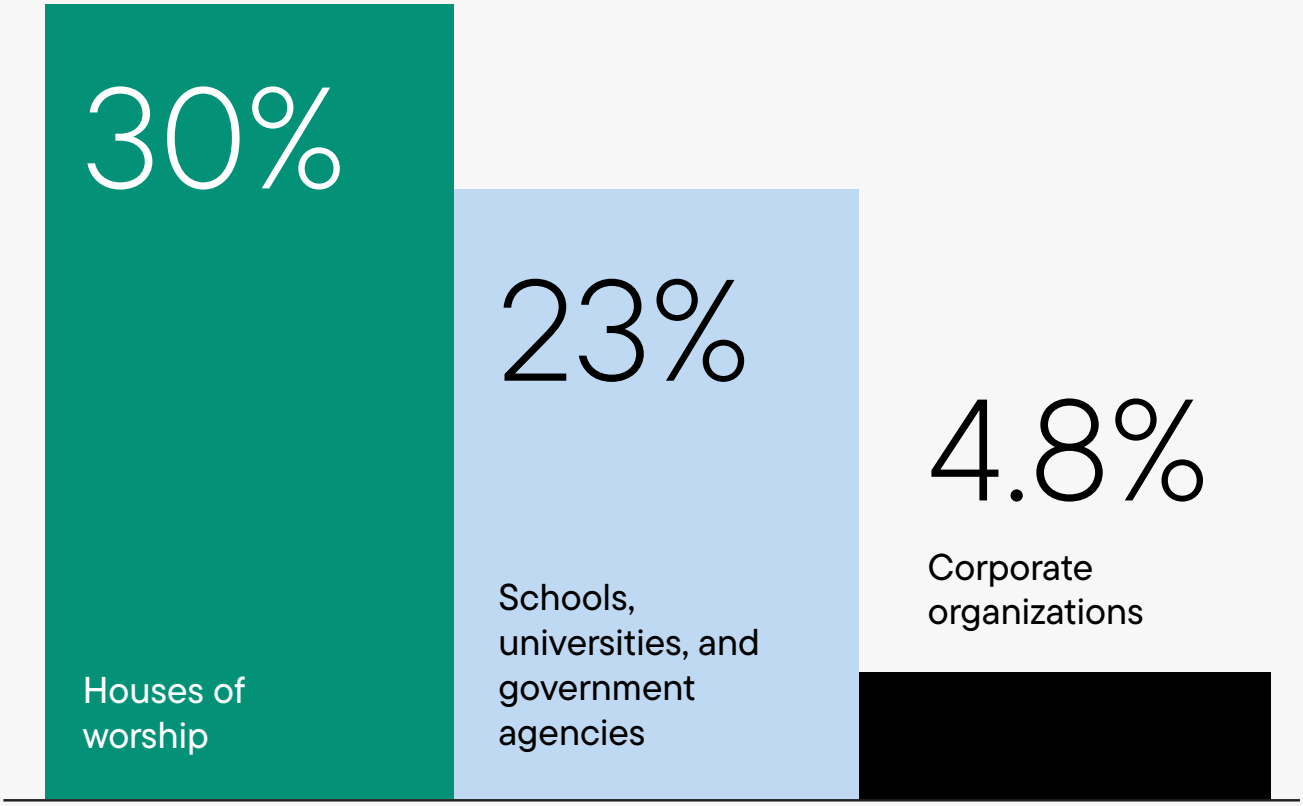


Among those who struggle to prove the value, 77.6% also cite budget. Forced to a single biggest challenge, 29.5% chose the combined answer “limited budget or hard to prove it’s worth it,” ahead of aging cameras (21.6%) and disconnected systems (17.4%).

Here is the deeper issue. Teams want better outcomes, but they often can’t articulate the value of those outcomes well enough to justify the spend. What is improving safety and threat response actually worth? Do the systems in place today even produce the security intelligence needed to quantify it? Security investment used to be tied to hardware refresh, aging equipment, or a compliance mandate.

Now, leaders expect operational impact, which means the case has to connect to outcomes a budget owner recognizes: reduced investigation time, lower operating cost, faster response, and better risk mitigation. Building that case requires data the current stack often doesn't surface, and that gap is a large part of why demand stalls. Who you make that case to depends on where the money comes from, which varies sharply by sector.

GRANTS AS FUNDING SOURCE



Corporate buyers fund almost entirely from operating and capital budget, with grants rarely a factor (4.8%). Schools, universities, and government agencies still lead with operating budget, but lean far more on grants and bond money, with grants reaching 23% for that group and 30% among houses of worship. The practical point holds either way: a grant application, a bond cycle, and an operating-budget request answer to different audiences on different timelines, so the business case has to be built for whichever one applies to you.

Getting More From What You Already Own

51%

of teams believe they could keep every camera they own if they switched platforms

33.2%

could keep some

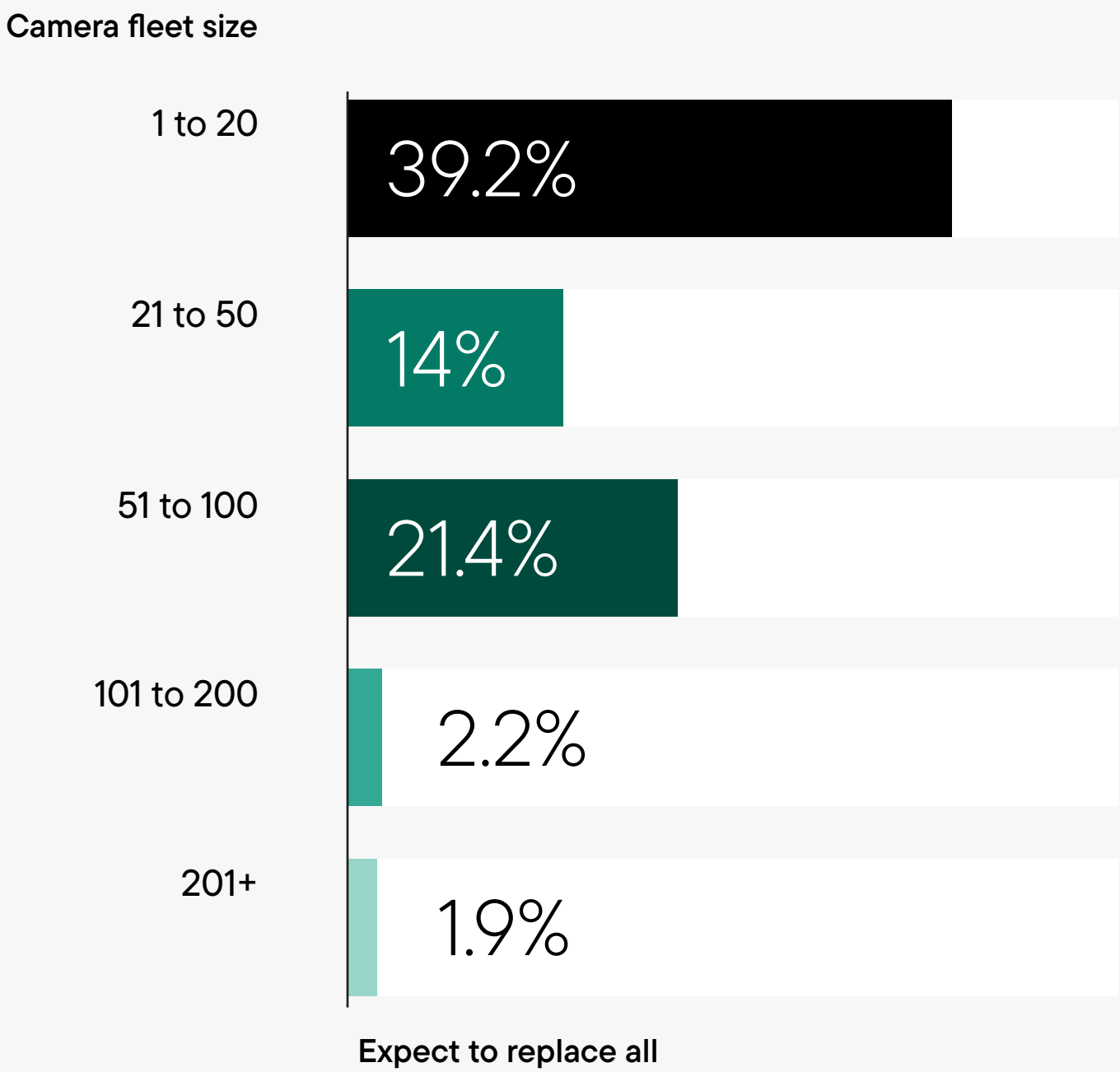
15.8%

expect to replace all cameras

Modernizing rarely means ripping everything out.



Expectations vary by fleet size. 39.2% of teams with 1 to 20 cameras expect a full replacement, dropping to about 2% for fleets over 100. The survey measures expectation rather than a technical audit, but it shows that for most established environments, rip-and-replace is not the default assumption. **“We would have to replace everything”** kills a lot of projects that never needed it.



Before ruling out a change, teams should verify compatibility at the model level, not just take a vendor’s word that it “works with existing cameras.”

A practical compatibility check

01 Inventory camera make, model, age, firmware, recorder, and connection method.

02 Confirm support for the exact models in use, not only the camera brand.

03 Test the capabilities that matter: search, analytics, audio, retention, remote access.

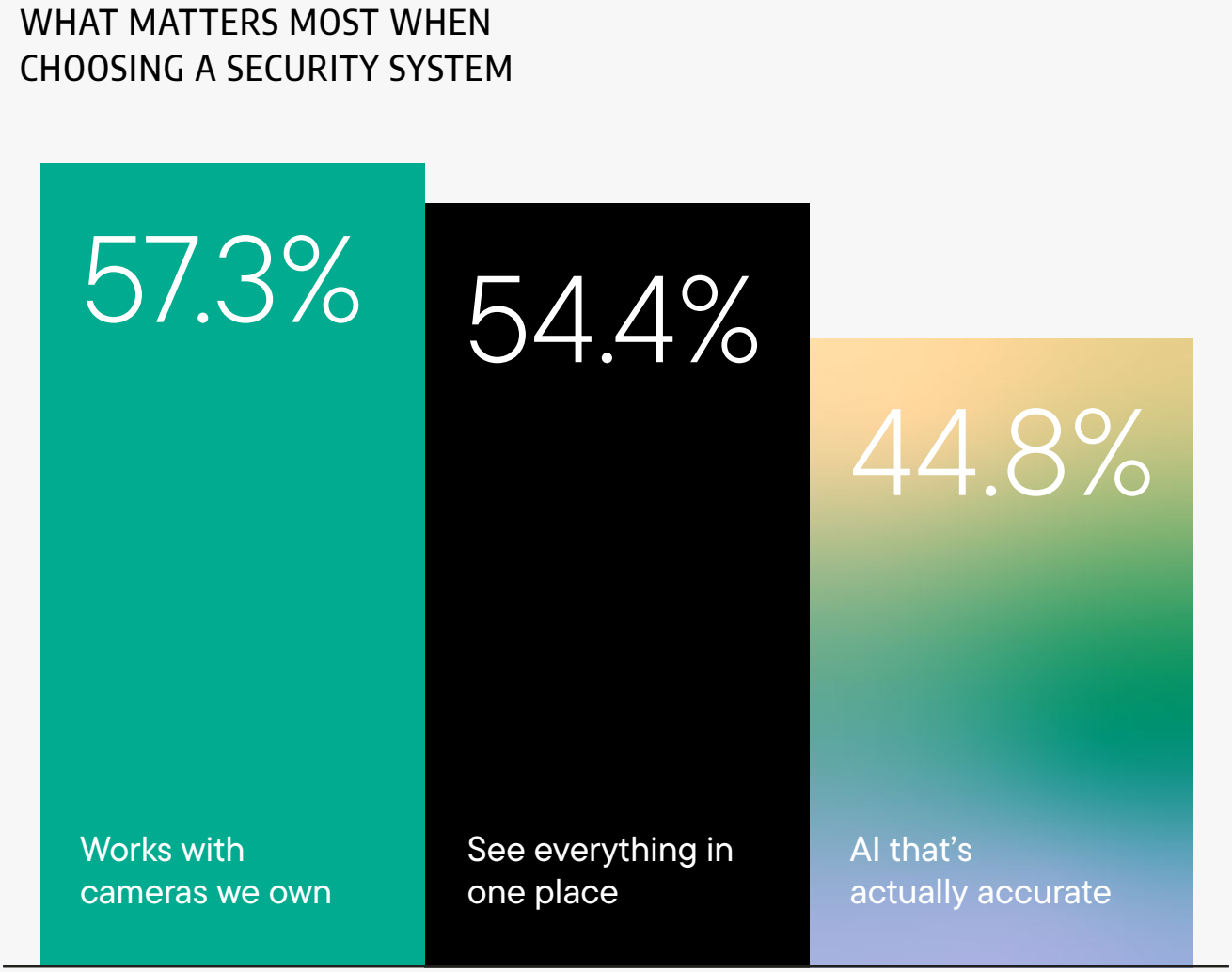
04 Confirm which AI-dependent features (firearm detection, plain-language search, analytics) your existing cameras can actually support. Older hardware is often the real reason those capabilities get left out, not the platform.

05 Model bandwidth, storage, licensing, and support costs across the full environment.

06 Ask whether old and new infrastructure can run together during a phased migration.

What AI Actually Changes

AI is the capability teams are most cautious about as a label and most receptive to as a job.

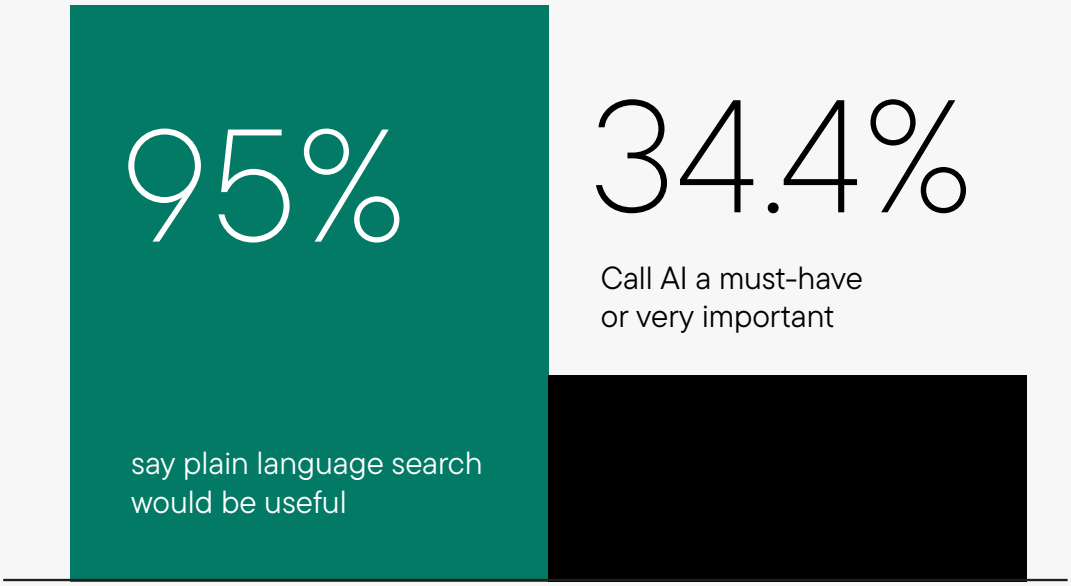


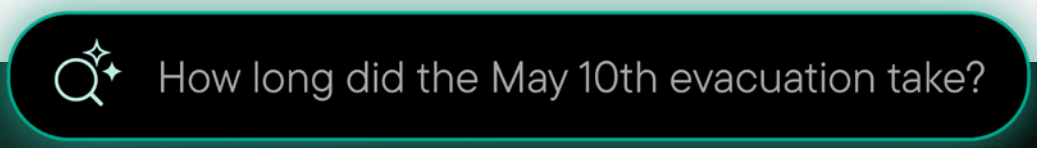
That caution is rational: it is also the priority that ranks last in what buyers say matters, behind clear pricing (71.0%), ease of use (68.5%), reliability (62.7%), hardware compatibility (57.3%), and single-pane visibility (54.4%), with "AI that's actually accurate" last at 44.8%.

AI has to earn its place inside a system that is already affordable, usable, and reliable, which is exactly the business-case bar the budget section describes.

Yet the appetite for what AI does is not in question. Only 34.4% call AI a must-have, but 95.0% say plain-language footage search would be useful, and 62.7% call it very or extremely useful. The gap is the point: teams don't care whether it's labeled AI, they care whether it does the job. Even among the 146 respondents who call AI merely 'nice to have,' 93.8% still want plain-language search.

TEAMS WANT WHAT AI DOES, NOT THE LABEL





In practice, AI means getting answers from your footage on demand: describe an event in plain language and retrieve it in seconds instead of scrubbing timelines, catch high-risk incidents early enough to act instead of just reviewing them after the fact, and let incident reports build themselves.

It can also pull operational answers straight from video nobody had time to watch, like how long an assembly line sat idle or how long an evacuation drill actually took. That's pattern-matching doing work a person would otherwise do by hand, not a black box making decisions.



People still make the call.

24.5%
expect AI to significantly reduce reliance on guards or monitoring staff over the next year or two

40.2%
expect some reduction

35.3%
expect no reduction

The dominant expectation is augmentation: AI absorbs the repetitive review, people keep judgment and response.

So the question isn't whether a system "has AI." It's how accurately the capability performs on your footage, how much time it saves, how often it's wrong, and where a person still needs to decide.

Five Moves the Benchmark Points To

The survey does not define one model of a strong program, but it points to five practical moves.

01

Benchmark investigation time before buying anything.

Track the time from an incident to the correct footage. Use the 30-minute and one-hour thresholds here to see where your team stands, and aim for minutes.

02

Connect the workflows that create the most friction.

Inventory how video, access control, emergency alerts, and guest management interact. Prioritize the handoffs that require duplicate logins, exports, or manual coordination.

03

Build the budget case around measurable outcomes.

Tie the investment to safety and response goals, staff time spent searching, incidents handled, liability or compliance exposure, and the infrastructure you keep. Make sure your systems can actually produce those numbers.

04

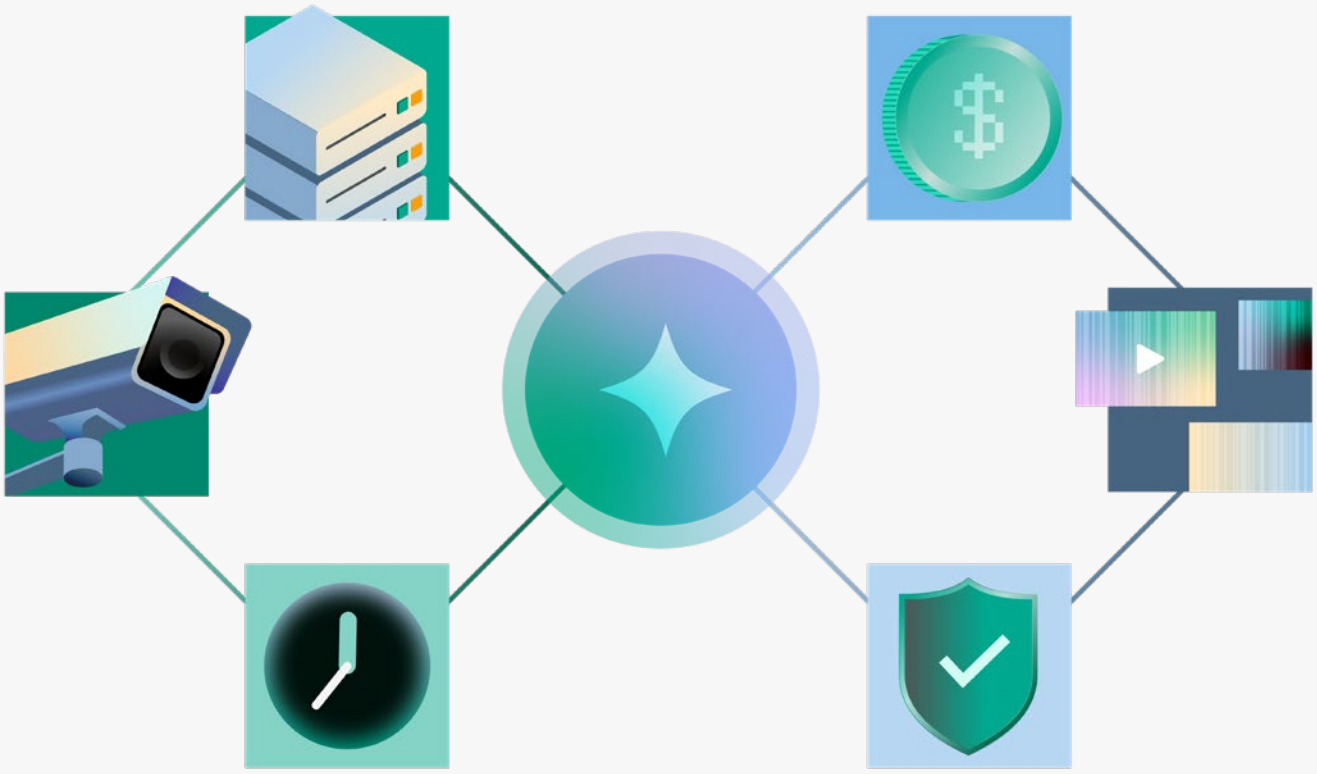
Verify compatibility before assuming a full replacement.

Audit specific camera models, test priority capabilities, and ask vendors to demonstrate a phased migration in your environment.

05

Evaluate AI by the job, not the label.

Test it on the work you actually need done: flagging high-risk incidents early enough to act on them, building incident reports, and pulling operational data from footage, such as how long a line sat idle or how long an evacuation drill took. Measure accuracy, false alerts, time saved, and where a person still needs to review or decide.



Where the Industry Is Headed

This is a snapshot, not a trend line, but the direction is clear. The teams in this survey have the technology. What they lack is coordination, and it shows up everywhere the data looks: systems that don't talk to each other, the half hour spent finding one clip, the budget that stalls because no one can prove what a faster answer is worth.

Those are really the same problem. Connect the systems and a slow investigation becomes a fast one. Make the investigation fast and you finally have a number to bring to a budget owner.

And once footage can answer a question in minutes, the footage becomes useful instead of just stored. AI earns its place here for the same reason: it closes the gap between an event and an answer.

The bar is moving toward speed. The programs that pull ahead will be the ones that get from an incident to an answer fastest, on the infrastructure they already own. The next advantage is not collecting more footage. It is turning footage into an answer, faster.

How Coram Helps

Coram AI is an AI physical security platform that helps organizations investigate incidents faster, improve operational visibility, and coordinate response across video security, access control, guest management, and emergency workflows. Built to work with existing camera infrastructure, Coram enables organizations to modernize physical security operations in one unified system without costly rip-and-replace projects.

Trusted by

1,500+

organizations across North America

Coram serves **school districts, healthcare organizations, manufacturers, government agencies, places of worship, hospitality groups, retailers, and Fortune 500 enterprises.**

The findings in this report map directly to the work Coram is designed to support.

Curious how Coram will integrate with your current environment?

Book a Demo