Verkada

2026 Verkada industry report

State of Cloud Physical Security

Europe edition



How European security teams adopt and govern AI under a shifting regulatory regime.

What 759 IT and security leaders across the United Kingdom, Ireland, Germany, France, and the Netherlands told us about where physical security is heading, and what it means for the people running it.

© 2026 Verkada Inc. All rights reserved. Findings from a 2026 study conducted by Dynata on behalf of Verkada.

© Copyright 2026 Verkada Inc. All rights reserved.

Verkada and the Verkada logo are registered trademarks or service marks of Verkada Inc. (“Verkada”). All other trademarks are the property of their respective owners.

Verkada may make changes to this document at any time without notice. The information presented herein may be inaccurate or outdated, and Verkada is under no obligation to maintain it. ALL INFORMATION IS PROVIDED “AS-IS” AND WITHOUT ANY WARRANTIES, IMPLIED, EXPRESS, OR OTHERWISE. VERKADA DISCLAIMS LIABILITY FOR ALL DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, ARISING OUT OF USE OF THIS DOCUMENT.

Any intellectual property rights relating to Verkada products are and shall remain Verkada’s exclusive property. Use of any Verkada product is subject to Verkada’s end user agreement or other executed agreement with Verkada. No license, either expressed or implied, to use or distribute any Verkada product is granted under this document.

No part of this document may be sold, licensed or sublicensed, copied, modified, transmitted, or transferred without Verkada’s prior written consent.

Table of contents

01 Executive summary 4

02 The global backdrop 6

03 Methodology 7

04 AI maturity 8

05 Regulation as the distinguishing force 11

06 The governance–regulation gap 14

07 Trust and the autonomy line 16

08 The operational picture 17

09 The foundation: cloud, part-finished 20

10 Four markets, four plays 23

11 What to do next 26

12 Appendix: data tables 27

Executive summary

European AI adoption is real, and conviction is strong: three quarters of organisations are using or piloting AI (75%), and 94% expect a moderate or major impact. But two findings sit in tension. Regulation weighs on most purchases here — more than four in five organisations (84%) say it influences their buying — yet governance coverage is strikingly low: just 37% have comprehensive AI governance covering physical security. Another 42% have general AI guidelines, but not the physical-security-specific kind the obligations call for, and only 32% have formal, quantified ROI — which counts whether organisations quantify their return, not what that return is. That gap, between the rules pressing in and the controls in place, is the region's core problem.

Four barriers cluster closely here — privacy (36%), regulatory uncertainty (31%), cost (30%), and cybersecurity (29%) — and most organisations have already pulled back from at least one AI feature on legal or regulatory grounds. The EU AI Act[1] sets a consequential regulatory window, its high-risk provisions for biometrics and critical infrastructure arriving in stages over the next few years, though it binds only the EU members in the sample: Germany, France, the Netherlands, and Ireland. The United Kingdom sits outside that regime, regulating AI through existing data-protection law and a lighter-touch, principles-based approach.

Both governance and proof are concentrated among the organisations already actively using AI; most of the region sits in the middle of adoption, where the governance and measurement that active users carry are far less common. Closing that gap is the central call to action — and in a market this regulated, the documentation it requires is also what will prove compliance when the rules tighten.



1 EU AI Act — Regulation (EU) 2024/1689 — Annex III high-risk (biometrics). EUR-Lex — Official Journal of the EU: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Key findings

1. **Three quarters are using or piloting AI.**
   40% of organisations actively use AI and another 35% are piloting it, totalling three quarters (75%) engaged, and belief in AI's impact is broad: 94% expect a moderate or major impact, and nearly half (48%) expect a major one.

2. **Regulation is the distinguishing force.**
   84% say regulation influences purchasing (40% significantly), and four barriers cluster within seven points: privacy (36%), regulatory uncertainty (31%), cost (30%), and cybersecurity (29%).

3. **Most organisations restrict at least one AI feature.**
   Only 17% restrict nothing, and the restrictions land consistently across feature types: 39% restrict real-time biometric identification, 38% facial recognition, and 38% automated decision-making.

4. **Governance and proof trail adoption.**
   Three quarters of organisations are engaged with AI (75%), but only 37% have comprehensive governance covering physical security and 32% measure formal ROI.

5. **A fifth of European organisations have not settled whether to trust AI (19%).**
   72% agree AI can make accurate decisions without human oversight, and 19% neither agree nor disagree — the largest neutral share on any question in this report.

6. **Transparency is widely demanded.**
   95% rate vendor transparency about how AI models work important, and 45% treat it as a hard purchasing requirement — near-universal across every European market.

7. **AI's value reaches beyond security.**
   88% of organisations use or plan to use camera data beyond security — most often for safety and compliance monitoring (58%) — and operational insight is a notable primary value in Europe (18%).

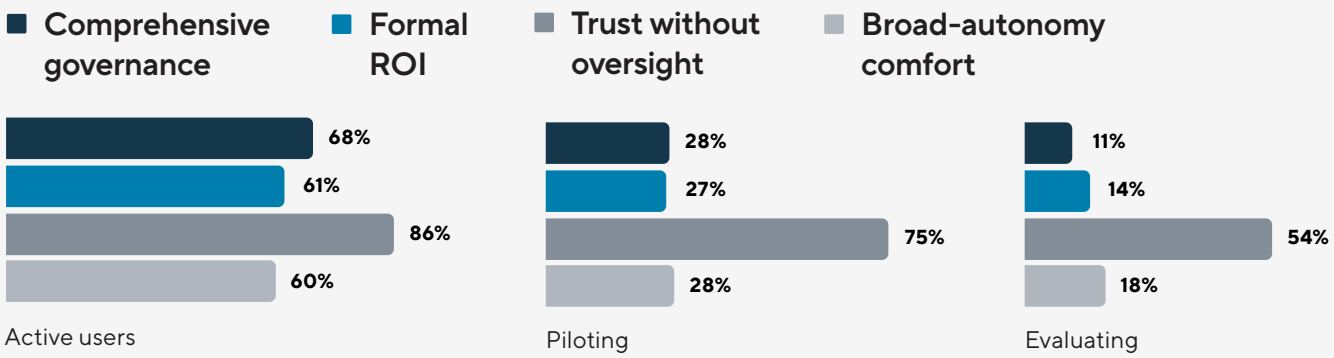
8. **The cloud question is settled.**
   19% are fully cloud, 72% hybrid, and 9% on-premise; 86% say the future is cloud-based and 91% are transitioning.

The global backdrop

Europe sits within a fast-moving global market. The worldwide picture below sets the context for the regional deep-dive that follows; the Global edition covers it in full.

1. **Four in five organisations worldwide are using or piloting AI.**
   41% are actively using AI and another 39% are piloting it, totalling 80% engaged; nine in ten (92%) agree AI will move security from reactive to proactive within three years.
2. **The most mature adopters lead on every measure.**
   Worldwide, those actively using AI lead together on governance (68%), formal ROI (61%), trust (86%), and comfort with broad autonomy (60%); pilots and evaluators lag on all four.
3. **Governance and proof lag adoption.**
   Worldwide, four in five are engaged with AI (80%), but only 41% have governance covering physical security and 38% measure formal ROI.
4. **Cloud is the infrastructure most associated with AI use.**
   Worldwide, 22% of organisations run fully cloud-managed physical security, 70% are hybrid, and 8% fully on-premise; 94% of hybrid and on-premise organisations are transitioning towards cloud, and fully-cloud organisations actively use AI 2.6 times as often as on-premise ones, an association the survey cannot show is causal.

A two-speed market: most measures jump at active use



Active users lead on governance, ROI, and broad-autonomy comfort; trust is high at every stage.
Base: global (n=2,741); active users (n=1,125), piloting (n=1,062), evaluating (n=404).

Survey question: Current AI use (Q12) cross-tabulated with governance (Q24), ROI measurement (Q27), trust (Q26), and autonomy comfort (Q20).

Methodology

Europe comprises the United Kingdom and Ireland, Germany (n=200), France (n=200), and the Netherlands (n=156), for a combined n=759. Fieldwork ran 30 March to 17 April 2026. Respondents are IT and physical security leaders at organisations with 100 or more employees, all involved in determining, influencing, or making decisions about physical security infrastructure. Percentages are rounded to the nearest whole number. All figures are self-reported: they reflect what respondents told us about their own organisations, not independently measured outcomes. Regional aggregates (the Europe figure, and the Global, North America, Asia, and ANZ summary columns shown in the appendix) are computed across the combined respondent pool for the markets they cover — base-weighted, not a simple average of market percentages. 'Active use' (Q12) means an organisation reports using AI features in physical security today; the survey does not measure how broadly those features are deployed, so active use should not be read as full-scale deployment. Because the study is a single snapshot, where organisations at different maturity stages differ, the data cannot establish whether the stages are sequential phases an organisation moves through or distinct populations that differ from the outset. Findings are reported as differences between groups; where the report's recommendations imply a progression from one stage to the next, that progression is an assumption the cross-sectional data cannot confirm. NET figures are computed on unrounded data and may differ from the sum of the rounded component percentages by a point. The ROI questions (Q27 and Q27a) record which metrics organisations track, not the size of any return: the study captures no payback periods or financial figures.

Many findings are shown by stage of AI maturity (Q12): actively using AI, piloting it, evaluating it, or not yet engaged. Ireland (n=52) is too small a sample to profile on its own and appears only within the Europe aggregate and this methodology. There is no year-over-year comparison in this edition, because there is no 2024 European baseline. Differences between markets are not adjusted for organisation or estate size; because active AI use rises with the number of sites monitored, some of the variation between markets may reflect estate-size composition rather than regional attitude.

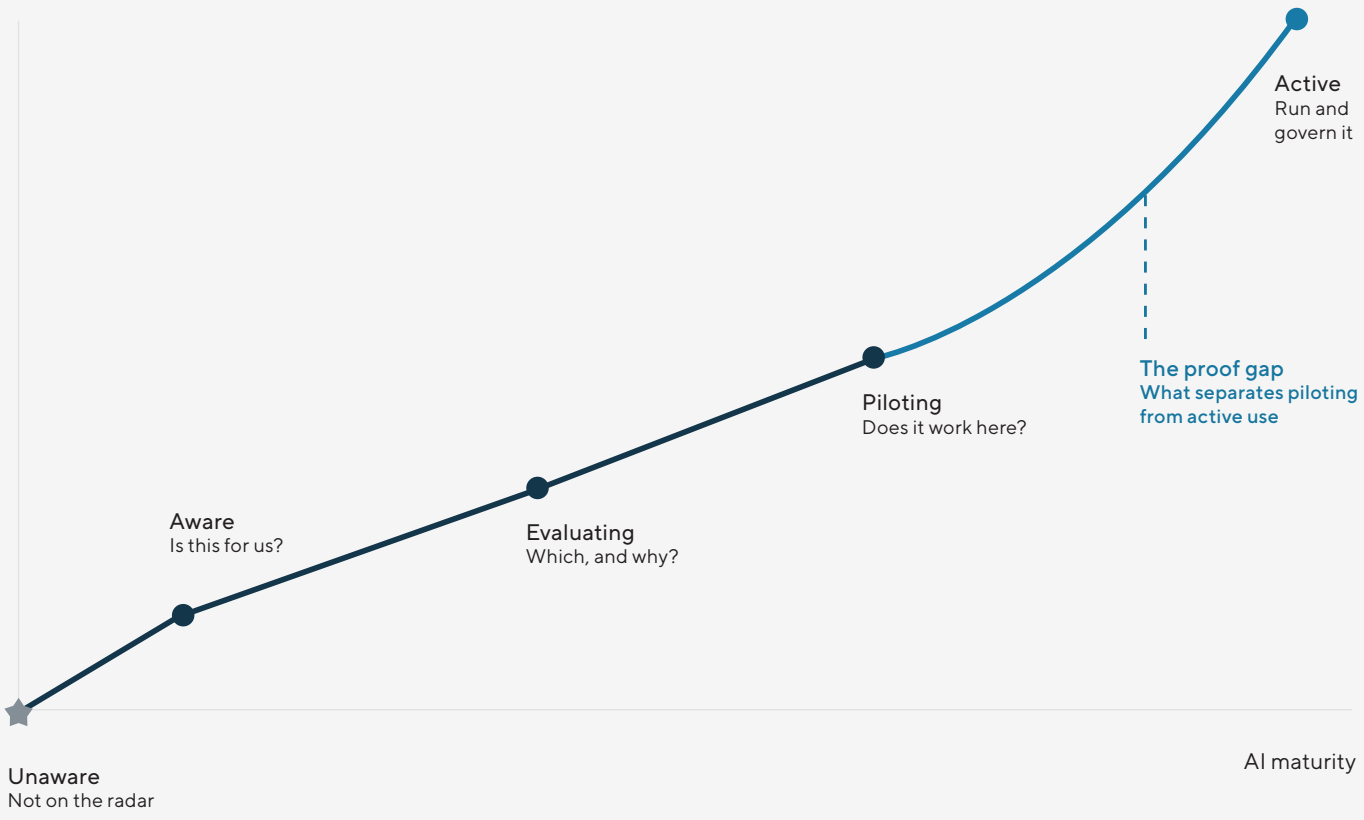


AI maturity

AI maturity is often described as a sequence of questions: whether AI belongs in the security operation at all, which tools to back and why, whether those tools hold up in a real environment, and how to run and govern them in active use, past the pilot stage. Those questions correspond to four stages, from aware to evaluating to piloting to active use. One caution travels with that framing: this survey is a single snapshot, so it shows how organisations at each stage look today, not a path any single organisation has been tracked along — the stages may be sequential phases or simply distinct populations, and the data cannot tell the two apart. What separates the stages is evidence that the technology works, and the widest difference sits between those piloting and those already in active use. Across these stages, 40% of European organisations are actively using AI, 35% are piloting it, 17% are evaluating it without having started, and 8% remain aware or unfamiliar with no current plans. Three quarters of the region is already engaged, and the work ahead is concentrated in the middle, among the large piloting cohort. Europe's active-use base is substantial; the difference here is a regulation-aware approach to how AI is put into active use, not a slower pace.

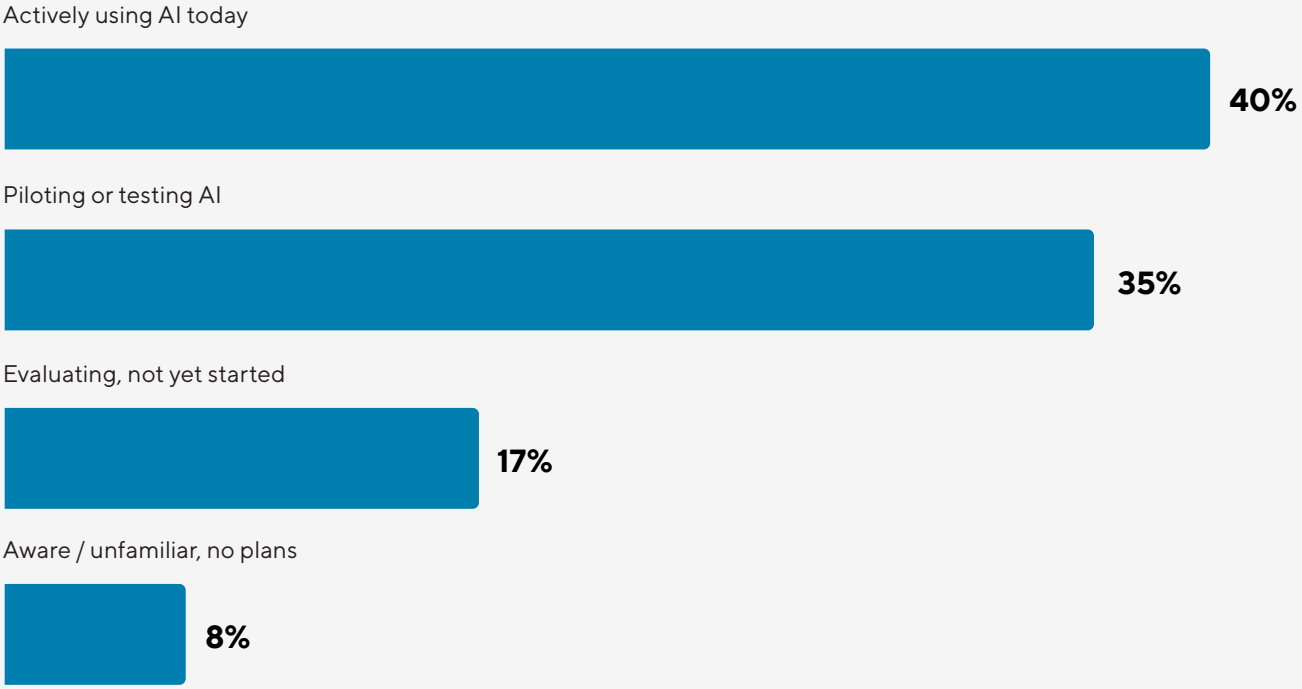
The AI maturity curve

Each stage is a question; the climb from piloting to active use is the steepest.



How far Europe has deployed AI

40% active | 35% piloting | 17% evaluating



NET active + piloting = 75% engaged. Base: Europe (n=759)

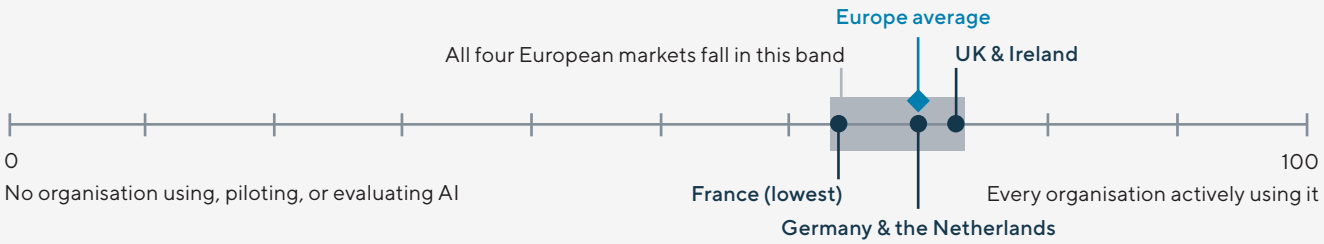
Survey question: Which best describes your organisation's current use of AI in your physical security system? (Q12).

Among the organisations already actively using or piloting AI, the features in heaviest use are the dependable ones: AI-verified alarm monitoring (54%), AI-generated incident reports (52%), real-time alerts (43%), facial recognition (40%), and proactive deterrence (40%). Belief in AI's impact is broad and strong: nearly all expect a moderate or major impact (94%), and nearly half (48%) a major one. Reported satisfaction is high: 94% are satisfied and 40% very satisfied — though as a self-report from the teams that chose and run these systems, it reads as a positive signal rather than an independent verdict on whether the deployments worked.

Looking two years ahead, the capability agenda favours the proven over the frontier: real-time alerts are named by 32% of organisations and AI-generated incident reports by 28%, while predictive threat modelling, the most speculative capability in the set, is named by 19%. Facial recognition (26%) and anomaly detection (24%) sit between.

The four European markets cluster in a narrow maturity band

On a 0-100 index, no market is near either extreme; France sits lowest, and the other three sit within a few points of one another.



Index = (active x 3 + piloting x 2 + evaluating x 1) ÷ 3, rebased to 0-100, from current AI use (Q12).
The United Kingdom and Ireland are reported as one market. Single-market bases ~156-203, so the ordering within the band is within sampling noise; read the band and its ends, not a rank. Base: Europe (n=759).

Survey question: Which best describes your organisation's current use of AI in your physical security system? (Q12).

Broken out by market, the four European markets span a wide range, from 49% actively using AI in the combined UK–Ireland market (a blend of two regulatory regimes the survey cannot separate) down to 30% in France, with Germany (40%) and the Netherlands (41%) in between.

What the maturity picture hides is how much of the value is already perceived rather than promised. Alarm verification, incident reporting, and real-time alerts — the three features most widely in use — carry satisfaction levels that point to working deployments rather than experiments. The opportunity now is less about discovering new use cases than about widening the ones that already work, and about converting the large piloting cohort to active use.

What this means

Most of the region has already decided to use AI; the harder question is converting a pilot to active use with evidence behind it. In Europe, the evidence that convinces leadership and the records a regulator will later ask for overlap heavily, so building them during the pilot serves both.

Regulation as the distinguishing force

More than four in five European organisations (84%) say regulation influences their physical security purchasing, and 40% say it influences it significantly. Four barriers sit within seven points of one another: privacy (36%), regulatory uncertainty (31%), cost (30%), and cybersecurity (29%). None of them separates from the others, so regulation is best read as the most distinctive brake on European deployment rather than a runaway one. Cost sits third here, not first: the brakes are weighted towards how AI handles data and how the rules will settle. The influence question points the same way. 84% say regulation shapes their purchasing, but the plurality (44%) call that influence moderate, against 40% who call it significant.

The barriers European organisations name most often

All four sit within seven points and do not separate

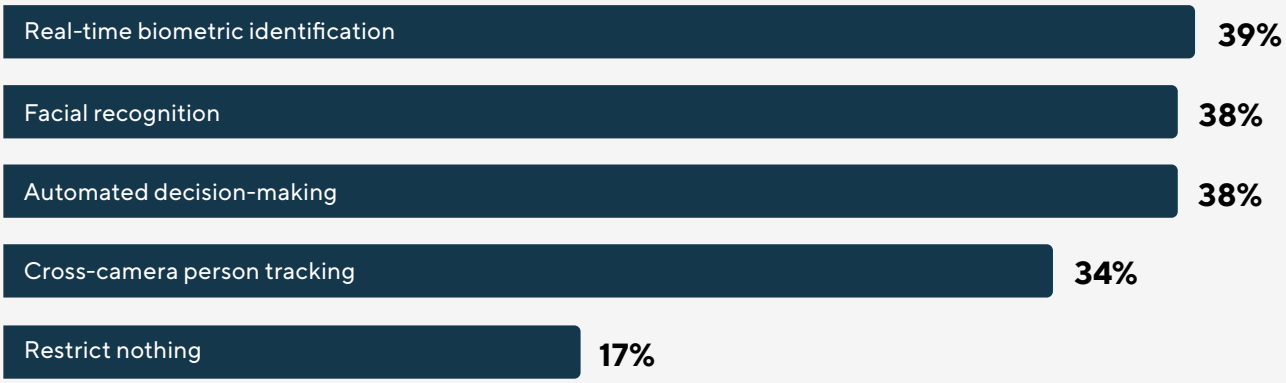


No one barrier leads: privacy (36%) does not separate from regulatory uncertainty (31%) at 95% confidence, at any of the three ranking levels the survey reports. Base: Europe (n=759).

Survey question: What are the top barriers preventing your organisation from adopting or expanding AI in physical security? Select up to three (Q23).

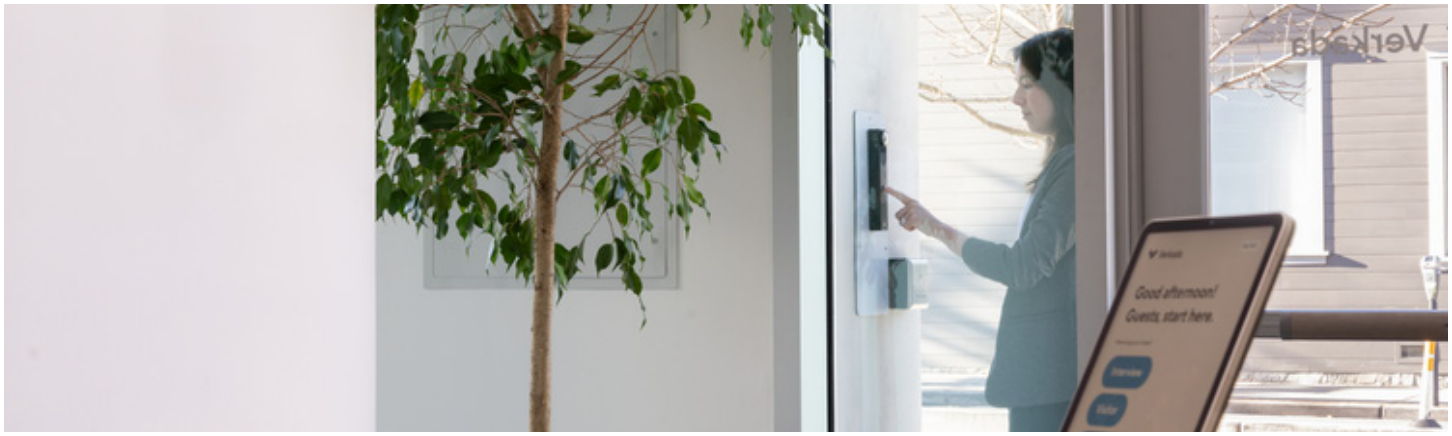
Restriction follows directly from that weight. 39% have restricted or avoided real-time biometric identification, 38% facial recognition, 38% automated decision-making, and 34% cross-camera tracking; only 17% report restricting nothing. For most organisations, pulling back from at least one AI feature on legal or regulatory grounds is already part of how they operate. Yet the restriction rates stop well short of total: even under this regulatory weight, most organisations have not pulled back the marquee biometric features, because the GDPR and the EU AI Act offer a compliant path — a documented necessity case and the right records — that makes deploying with controls a real alternative to avoiding the capability outright. The question counts capabilities held back for regulatory or legal reasons, but avoidance can also reflect a feature an organisation never wanted, so the figures mix active restriction with plain non-adoption.

Restriction is mainstream: only 17% restrict nothing



Base: Europe (n=759).

Survey question: Has your organisation restricted or avoided deploying any of the following AI features due to regulatory or legal concerns? Select all that apply. (Q32)



Regulation weighs most on the organisations actively using AI: 54% of active users report that regulation significantly influences their purchasing, against around 31% at the piloting and evaluating stages alike, because the teams actively using AI are the ones meeting the obligations in practice. The window ahead is not uniform, because it depends on whether a market sits inside the EU. For the EU members in the sample (Germany, France, the Netherlands, and Ireland), the EU AI Act sets the terms: systems that identify people by biometric characteristics, categorise them, or infer emotion count as high-risk and must clear conformity assessment, a fundamental-rights impact assessment, and EU-database registration, while non-biometric analytics such as perimeter or crowd monitoring sit in a lighter tier. Under the EU's Digital Omnibus simplification package,[2] those high-risk obligations are deferred to 2 December 2027 for stand-alone systems and 2 August 2028 for product-integrated ones, provisional pending formal adoption — the regulatory position as of June 2026.

The United Kingdom is the exception. Outside the EU AI Act, it takes a deliberately pro-innovation, principles-based approach, regulating AI through the Information Commissioner's Office (ICO) under the UK GDPR[3] and the Data Protection Act 2018,[4] recently extended by the Data (Use and Access) Act that received Royal Assent in June 2025.[5] That is lighter on AI-specific statute, but not a free pass: the ICO still treats facial recognition as high-risk to people's rights and expects a documented necessity-and-proportionality case and a data-protection impact assessment before deployment, with a dedicated police biometrics framework under Home Office consultation. Either way, organisations deploying biometric features now are deploying into rules that are still settling. The organisations already actively using AI are the ones who hold comprehensive governance and documentation, and because the EU AI Act's high-risk obligations and the UK's necessity-and-proportionality test both demand essentially the same record — what the system does, why it is necessary, and how its use is controlled — building that documentation now is the move that holds up whichever way the rules land. Waiting for the final text mainly delays that preparation.



What this means

Regulatory readiness functions as a deployment requirement here, not an afterthought. Whether obligations run through the EU AI Act, arriving in stages through 2027 and 2028, or through the UK's data-protection and biometrics regime, the certifications and documentation for biometric and critical-infrastructure features matter most when secured before active use rather than after.

2 EU Digital Omnibus (AI) — Commission proposal, 19 Nov 2025; provisional agreement 7 May 2026. European Commission — Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

3 UK GDPR (retained Reg (EU) 2016/679) — Retained EU law as amended by DPA 2018 / DUAA 2025. legislation.gov.uk — The National Archives: https://www.legislation.gov.uk/eur/2016/679/contents

4 UK Data Protection Act 2018 — 2018 c. 12. legislation.gov.uk — The National Archives: https://www.legislation.gov.uk/ukpga/2018/12/contents

5 UK Data (Use and Access) Act 2025 — 2025 c. 18 — Royal Assent 19 June 2025. legislation.gov.uk — The National Archives: https://www.legislation.gov.uk/ukpga/2025/18

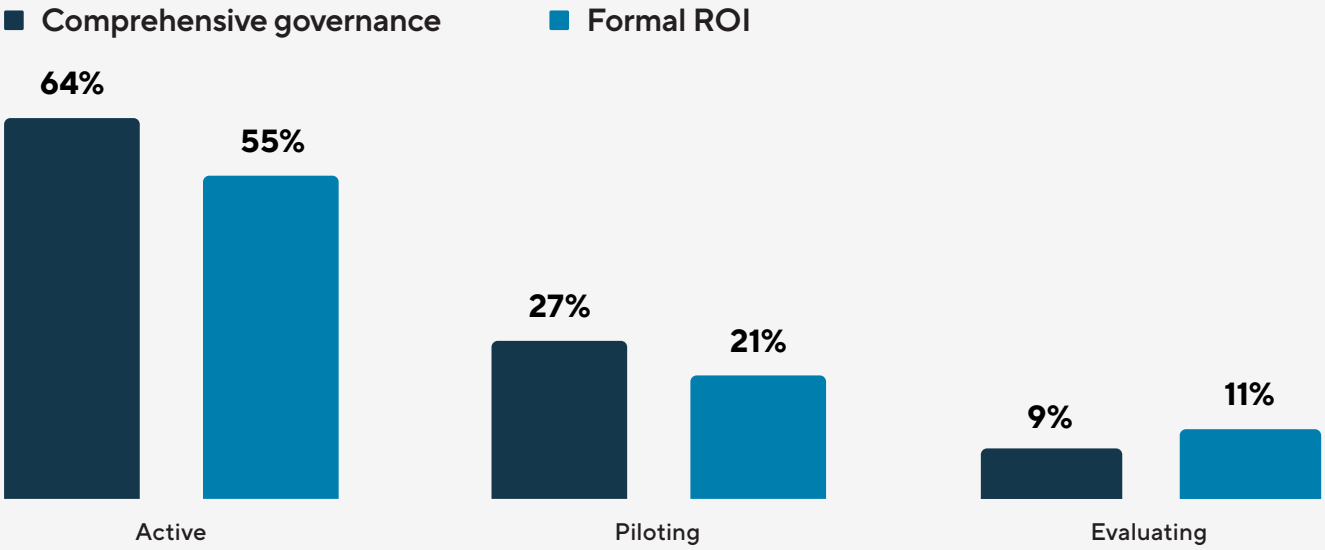
The governance–regulation gap

Just over a third of European organisations (37%) have comprehensive AI governance covering physical security, and under a third (32%) have formal, quantified ROI. For a market where regulation influences more than four in five purchases (84%), the distance between obligation and formal structure is the central problem. These governance figures are self-described — there is no external rubric for what counts as comprehensive — as are the conviction figures (94% expecting impact, 75% engaged). Like the satisfaction numbers, they are best read as how organisations characterise themselves, not as independently verified fact.

Comprehensive governance stands at 64% of active users, 27% of those piloting, and 9% of those still evaluating — formal ROI follows the same staircase, at 55%, 21%, and 11%. Active users have built the structure that active use demands; those still piloting have not. That matters because 35% are piloting and 17% are evaluating, placing most of the region in exactly the middle, adopting AI faster than it is building the governance to support it.

Governance and proof are higher among active users

Comprehensive governance: 64% of active users, 27% piloting, 9% evaluating



Comprehensive governance and formal ROI are both far higher among active users than among pilots or evaluators.
Base: Europe (n=759); active users (n=303), piloting (n=269), evaluating (n=126).

Survey question: AI governance framework (Q24) and AI ROI measurement (Q27), by stage of AI use (Q12).

A general AI policy is not always enough to close the gap. Physical security carries obligations that a broad, organisation-wide policy may not address — how biometric data is handled, how automated decisions are documented, how camera footage is retained and reused — and the teams pairing a specific physical-security governance framework with their deployments are the ones best positioned for the regulatory window ahead.

What this means

Active users carry comprehensive governance at more than twice the rate of those still piloting — 64% against 27%. That gap is between the two groups as the survey observed them, not a change it could watch happen; building governance during the pilot is the recommendation, and the same documentation also makes the regulatory obligations easier to meet.



Trust and the autonomy line

European organisations are willing to let AI act within limits, but many have not settled how far it should go. Four in five (81%) say they would be comfortable with autonomous AI deterrence, yet 36% would deploy it broadly and 14% are neutral on the question. Agreement that AI can make accurate decisions without human oversight stands at 72%, with 19% neither agreeing nor disagreeing. The two questions are not strictly comparable — Q20 asks about one specific action, an automated deterrence response, while Q26 is a broad statement about AI judgement — so part of the gap reflects that difference in scope. For most, the hesitation is an open question about where to draw the autonomy line rather than outright scepticism: only a small share are actively uncomfortable.

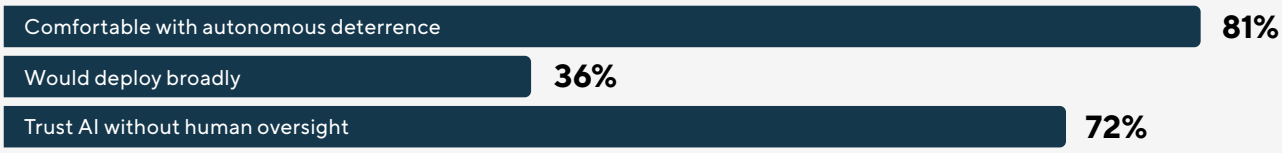
Transparency is the one place where the answer is settled: 95% rate it important that vendors are transparent about how their AI models work, and 45% treat it as a hard requirement. Whatever an organisation decides about autonomy, it wants to understand the system it is trusting.

Experience is the steepest gradient on the autonomy question. 63% of active AI users would deploy autonomy broadly, against 23% of those piloting and 14% of those evaluating, so willingness to hand AI more independence rises step for step with hands-on experience. The same pattern holds by seniority across the global sample, where the C-suite is far readier than managers to grant broad autonomy (53% against 31%).

What this means

19% of European respondents neither agree nor disagree that AI can be trusted to make accurate decisions without human oversight. The cases that travel furthest here pair a clear autonomy line with transparency about how the system works, rather than assuming the question is already answered.

Comfort runs ahead of unsupervised trust



Comfort and trust are top-two-box agreement; "would deploy broadly" is the top-box share. Base: Europe (n=759).

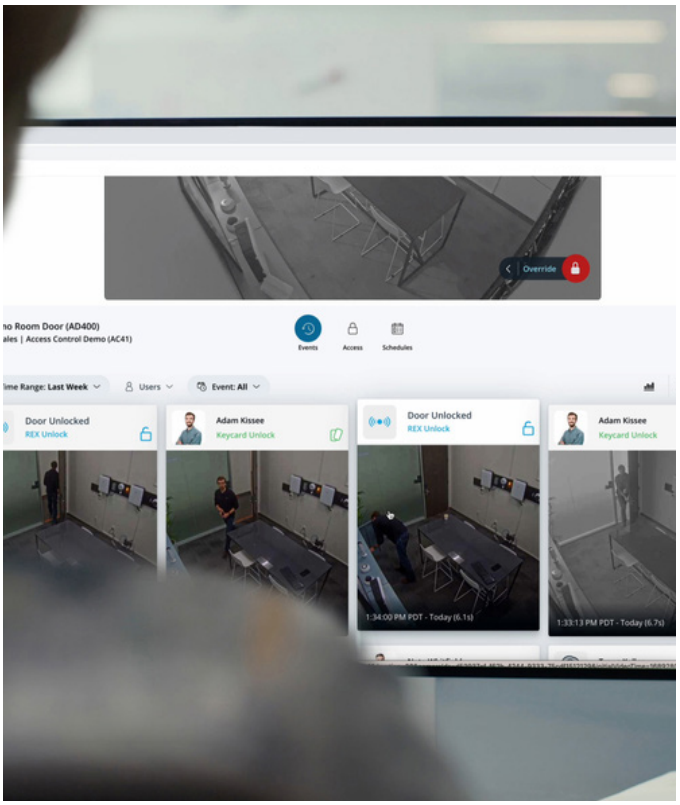
Survey question: Comfort deploying autonomous AI deterrence (Q20) and trust in AI without human oversight (Q26).

The operational picture

Europe's value case reaches well beyond security, and the breadth of reuse shows it: 88% of organisations use or plan to use camera data for purposes beyond security (current reuse is about 85%). Investigation cycles are quick — 60% of organisations resolve incidents within four hours, including 17% in under an hour. On what AI is primarily valued for, among active users, the security mandate still leads, with real-time threat detection (28%) and faster investigations (26%) close enough that the survey cannot rank them, and operational insight beyond security at 18%. AI here is valued not only for catching threats but for what it reveals about how a building and an organisation actually run.

Even with Europe's careful approach to data, the camera estate has become operational infrastructure, and only 12% of organisations use none of it beyond security — a data-minimising stance that shapes how the rest is reused: where data does go beyond security, safety and compliance monitoring leads (58%).

What organisations measure AI against, among those that track ROI formally, clusters around system efficiency (58%), with response time (25%) and false-alarm reduction (13%) the next most cited. The study captures which metrics organisations track, not the size of the return: it records no payback periods or financial figures. When asked in their own words what will change most about physical security over the next three years, 52% named AI spontaneously, so the direction is widely shared even where the formal measurement behind it is still being built.

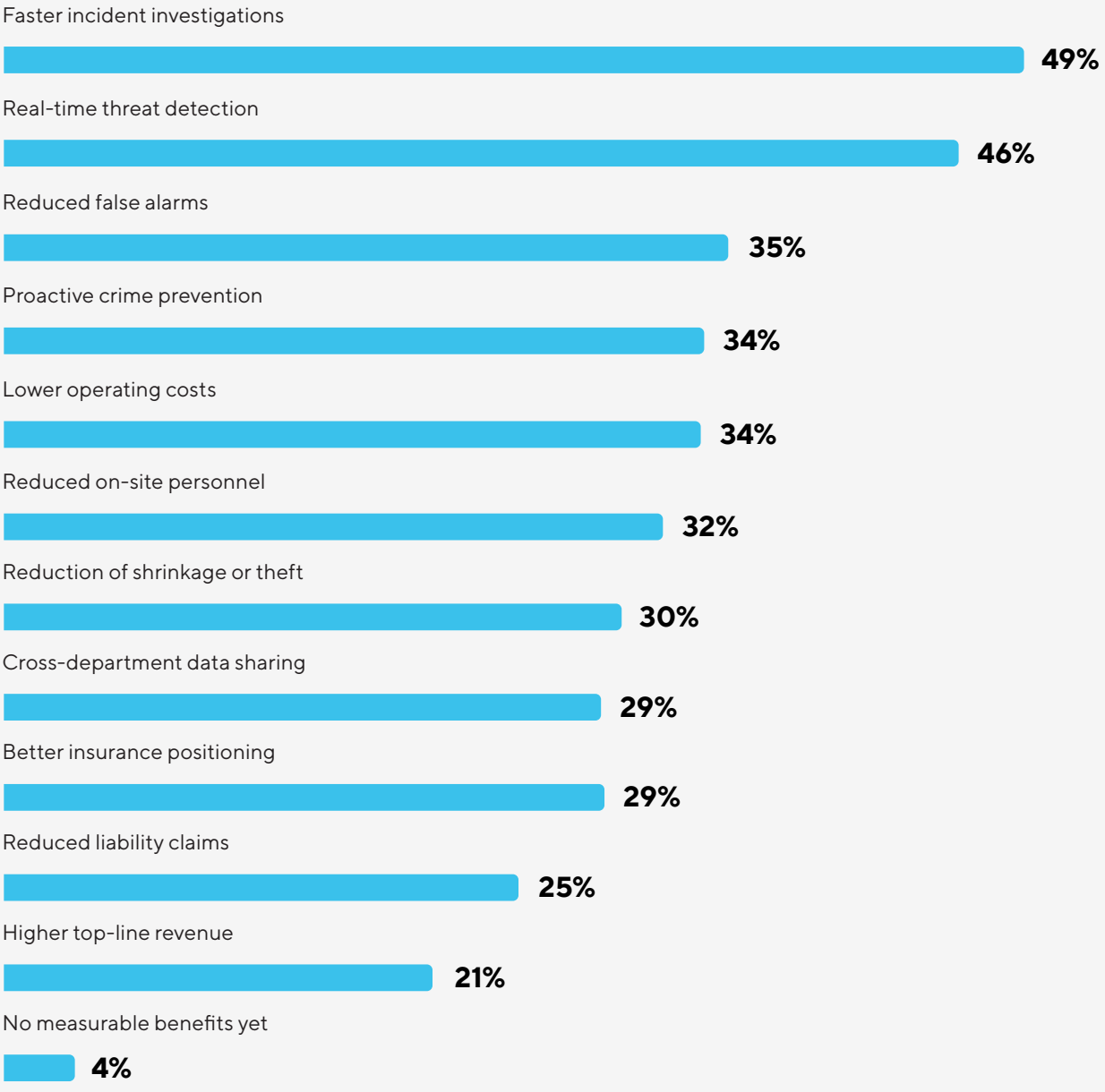


What this means

Most European organisations use or plan to use camera data beyond security (88%), most often for safety and compliance monitoring (58%). Operational insight is a notable part of that picture, named as the single primary value by 18% of active users. The breadth of value the estate already delivers is the foundation of the case here, and deliberate restraint on which camera data is reused is part of how teams earn trust internally.

The benefits European organisations most often name

Investigation speed and threat detection sit level at the top; only 4% report no benefit

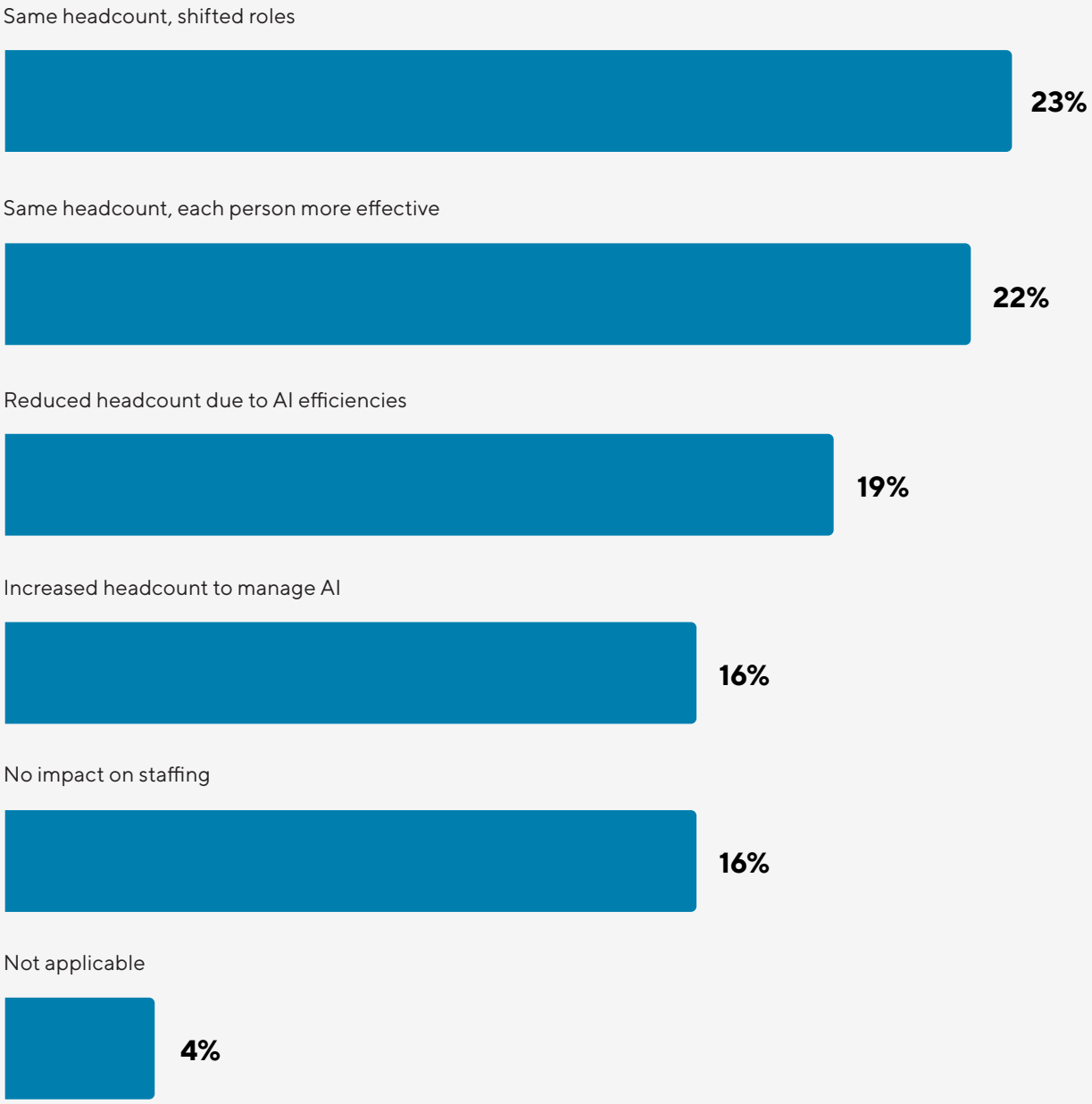


Faster investigations (49%) and real-time threat detection (46%) do not separate at 95% confidence, so neither leads the list. Q28 asks which benefits an organisation has experienced or expects to experience, so these figures blend realised and anticipated benefit. Base: Europe (n=759).

Survey question: Which benefits has your organisation experienced (or expects to experience) from AI in physical security? Select all that apply. (Q28)

How respondents say AI has changed their security staffing

The two largest responses both describe the same headcount working differently



Reported effect on staffing, as described by respondents. Roughly as many organisations have added headcount to run AI systems (16%) as have cut it (19%) — the two do not separate at 95% confidence. Base: Europe (n=759).

Survey question: How has AI in physical security affected your organisation's security staffing? (Q29)

The foundation: cloud, part-finished

The cloud question is settled, even though the migration is only part-finished. 19% of organisations are fully cloud-managed, 72% are hybrid, and 9% remain on-premise; more than four in five (86%) agree the future of physical security is cloud-based, and 91% of those not yet fully cloud are planning or in progress on the transition. AI is being layered onto a base that is already deep in hybrid cloud, with the shift to full cloud management still under way. Cloud concentrates footage and identity data off-premise and widens the attack surface, and cybersecurity concerns rank among the top barriers to AI adoption (29%), so the case for cloud rests on operational value weighed against that exposure rather than on security alone.

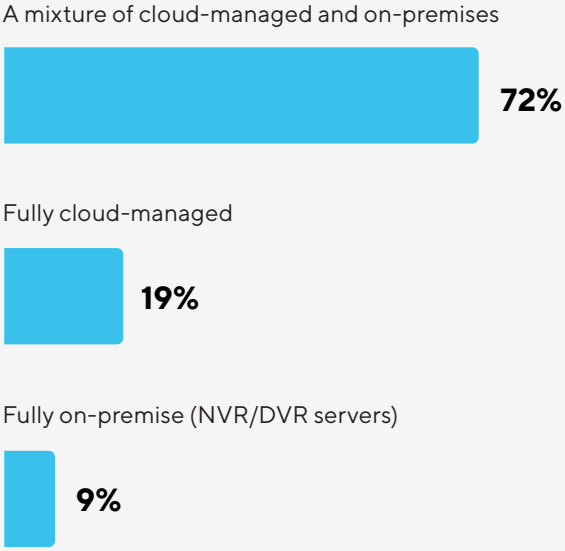
Budgets concentrate with the leaders. 79% expect their physical security budget to grow, and 20% expect growth of 20% or more, but the appetite is uneven by maturity: 32% of AI-active organisations expect significant growth, against 6% of those still evaluating. The organisations already actively using AI are the ones funding the next stage of it.

Most European organisations run hybrid infrastructure

72% hybrid

19% fully cloud

9% fully on-premise



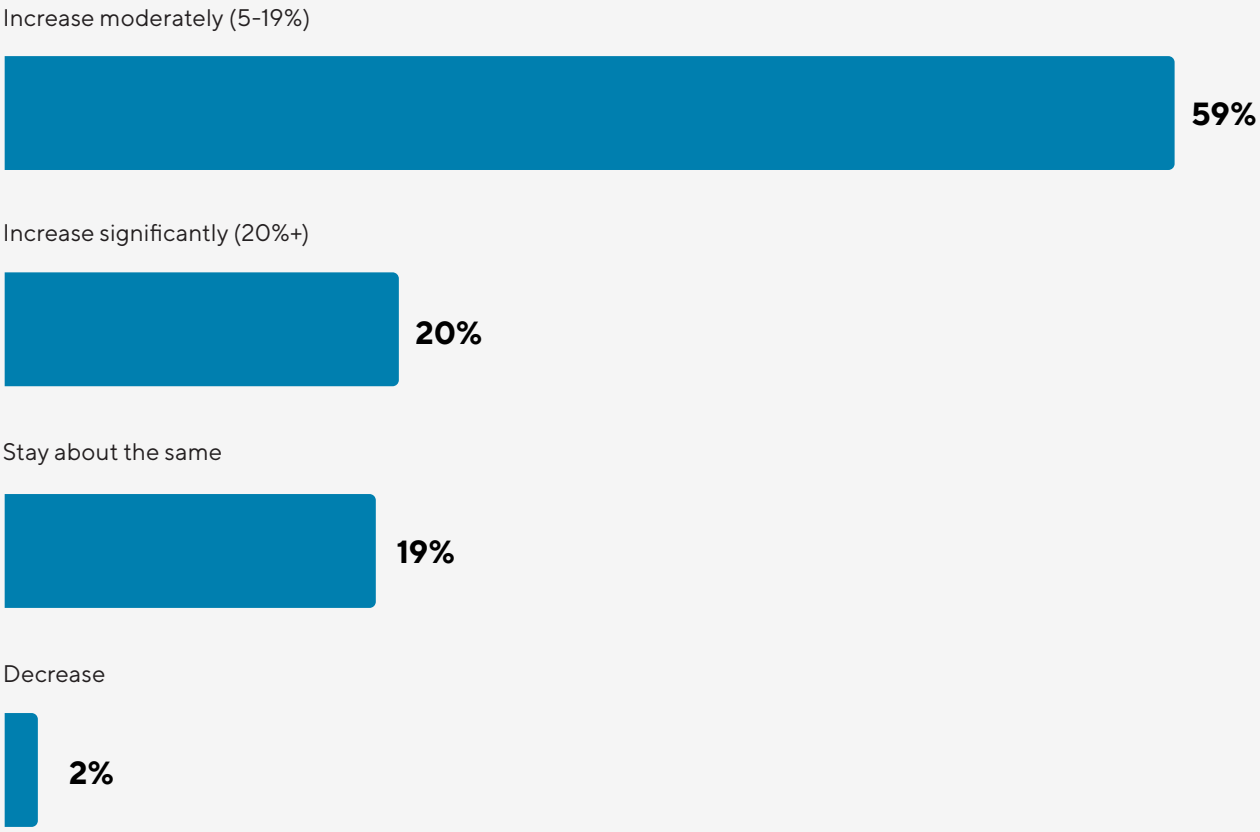
81% of European organisations run hybrid or fully on-premise infrastructure, so the cloud transition is under way rather than finished. Base: Europe (n=759).

Survey question: Which of the following best describes your organisation's physical security infrastructure deployment across your sites? (Q4)



79% of European organisations expect security budgets to rise

79% expect an increase; most of that is moderate rather than significant



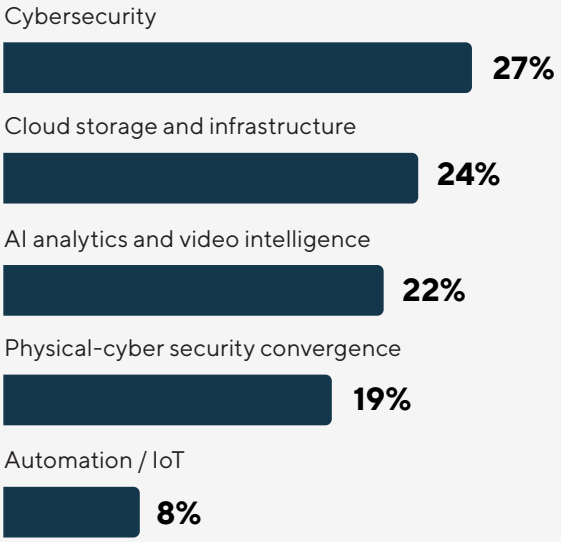
Stated budget expectation for the next 12 months, not committed spend. Base: Europe (n=759).

Survey question: Thinking ahead to the next 12 months, do you expect your budget for physical security investments to... (Q8)

Investment priorities are tightly clustered. Cybersecurity (27%), cloud storage and infrastructure (24%), and AI analytics (22%) sit within five points of one another, with physical-cyber convergence at 19%. Infrastructure and AI are funded together rather than in sequence. That link shows up directly in adoption: 59% of fully-cloud organisations are actively using AI, against 22% of on-premise ones (a small, directional on-premise base), so the infrastructure decision and the AI decision move together.

Investment priorities cluster within five points

Cybersecurity (27%) and cloud storage (24%) do not separate from one another

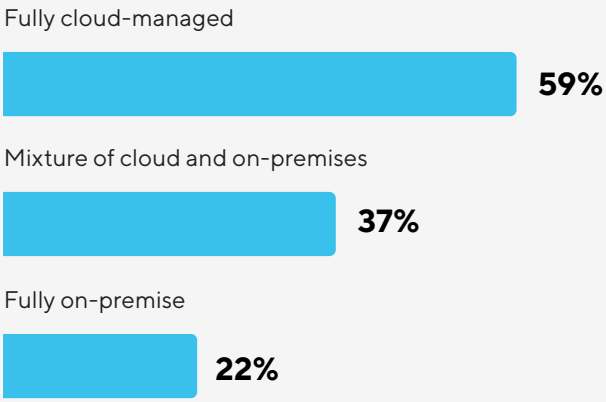


Cybersecurity (27%) and cloud storage (24%) do not separate at 95% confidence, so the list has no single leader. Base: Europe (n=759)

Survey question: When considering investments in your physical security system, which would you consider top priority? Please select one. (Q9)

Active AI use tracks how far an organisation has moved to cloud

59% of fully-cloud organisations are actively using AI, against 22% fully on-premise



Base: fully cloud (n=143), hybrid (n=545), fully on-premise (n=71). The fully on-premise figure rests on a small base and should be read directionally. This is an association, not a causal claim; organisations that have moved to cloud differ from those that have not in ways this survey does not hold constant — notably the number of sites they monitor and their expected budget growth. Source: Europe regional banner.

Survey question: Actively using AI features today (Q12) by physical security infrastructure deployment model (Q4).

What this means

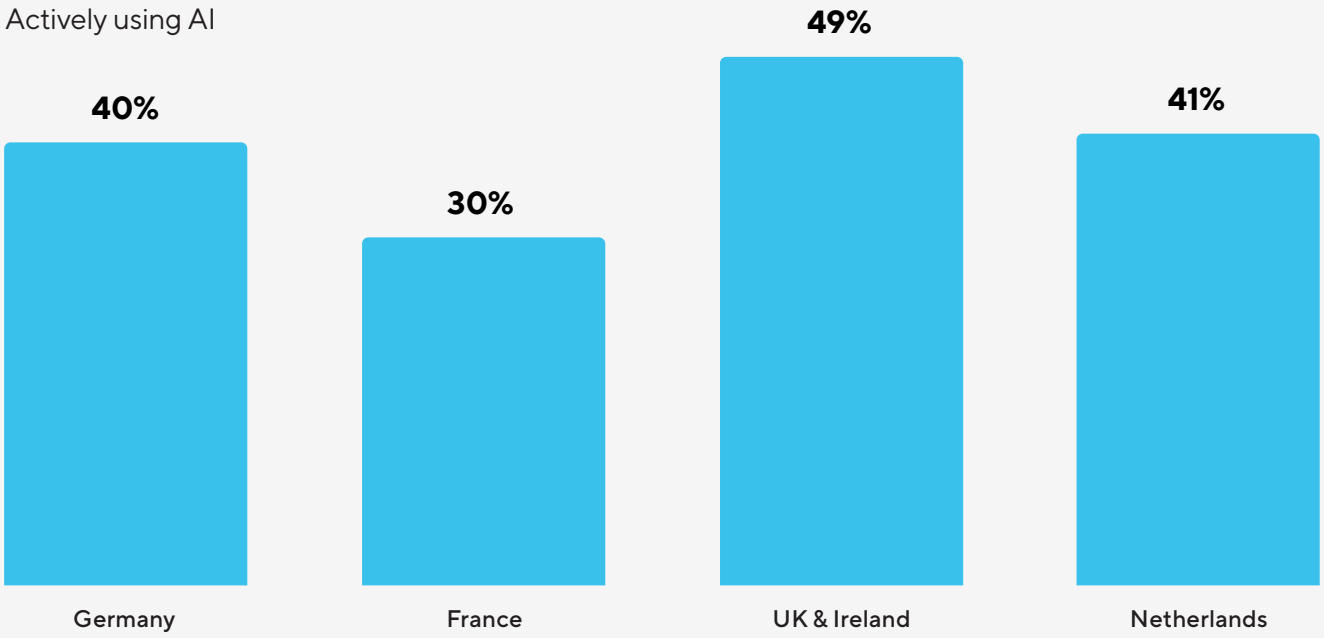
Active AI use runs close to three times higher on fully-cloud infrastructure than on-premise (59% versus 22%, though the on-premise base is small enough to read as directional), and the consistent break is between cloud and on-premise rather than between fully-cloud and hybrid. The migration off on-premise-only travels with AI adoption rather than standing apart from it, though the survey cannot show that one drives the other. The foundation-first sequence — cloud and cybersecurity, then AI, then convergence — matches both the budget pattern and where adoption is happening.

Four markets, four plays

The four reporting markets sit under four different legal regimes, and that is what warrants a different conversation in each — more than any ranking of adoption rates. France sits genuinely lower on active use; the other three are too close together to rank. Germany, France, the United Kingdom and Ireland, and the Netherlands each present a distinct regulatory profile.

Germany combines comprehensive governance (43%) with the region's near-universal demand for vendor transparency. German organisations name privacy (42%) and regulatory uncertainty (35%) among their top barriers, but where AI meets the standard German teams expect, trust runs high (80%). That posture has a legal backbone: a workplace camera or AI monitoring tool cannot go live without the works council's agreement under the Works Constitution Act[6] — the route that, after a 2023 EU Court of Justice ruling narrowed Germany's stand-alone employee-data provision under the Federal Data Protection Act (Section 26)[7], now also carries the lawful basis for the monitoring — and biometric systems carry EU AI Act high-risk obligations on top of that.

Active AI use across the four reporting markets



Base by market: Germany (n=200), France (n=200), UK & Ireland (n=203), Netherlands (n=156)

Survey question: Actively using AI today by market (Q12).

6 Works Constitution Act (BetrVG) – Betriebsverfassungsgesetz, §87(1) No. 6. Federal Ministry of Justice – gesetze-im-internet.de: https://www.gesetze-im-internet.de/englisch_betrvg/

7 Federal Data Protection Act (BDSG) – Bundesdatenschutzgesetz, §26. Federal Ministry of Justice – gesetze-im-internet.de: https://www.gesetze-im-internet.de/englisch_bdsg/

France sits lowest of the four European markets on AI adoption, with 30% actively using AI and 12% fully cloud-managed (though with roughly 200 respondents in the market, the survey cannot tell whether that reflects regulation, culture, or the sample itself). The piloting cohort is large; the conversation that matters most is about getting the cloud and infrastructure base in place so they can convert to active use. Advanced biometric features meet an additional brake: the CNIL, France's data protection authority, runs one of the strictest biometric regimes in Europe, having ruled most employer biometric access and attendance systems unlawful and allowing facial recognition only where a high-reliability authentication need is established and no less-intrusive option exists.

In the combined UK–Ireland market, facial recognition is already in use at 43% of organisations using or piloting AI — but that single figure spans two regulatory regimes the survey cannot separate, because the two are reported as one market (n=203). The United Kingdom sits outside the EU AI Act; the ICO holds facial recognition to a necessity-and-proportionality bar under data-protection law, so the appetite here meets evidence requirements. Ireland, as an EU member, falls under the Act and an active Data Protection Commission, which has fined a public body €550,000 for facial recognition used without a valid legal basis — so the Irish organisations inside this combined figure answer to a different regulator than their UK counterparts.

In the Netherlands, 41% actively use AI and 35% would deploy autonomous deterrence broadly — both close to the European average. A further 19% are still developing a formal AI governance policy. The regulatory line here is firm regardless: the Dutch data protection authority, the Autoriteit Persoonsgegevens, treats camera-based facial recognition as almost always prohibited and has named mass and camera surveillance a headline supervisory priority for 2026, while high-risk AI deployers must complete a fundamental-rights impact assessment and register in the EU database.

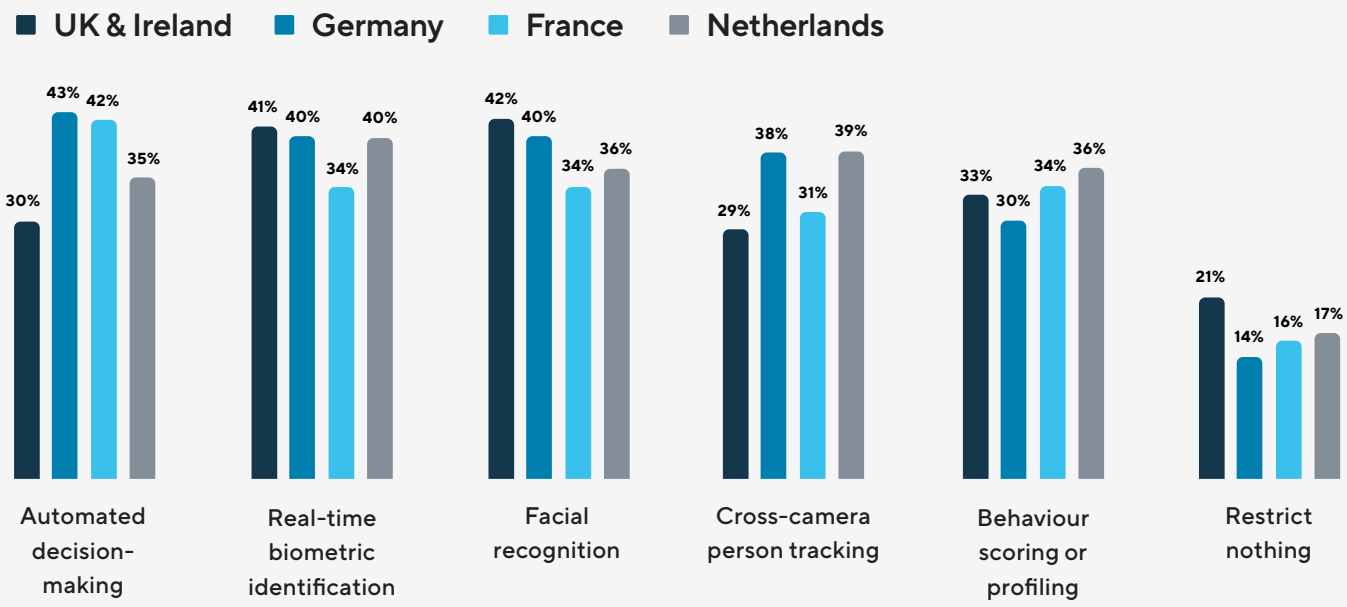


What this means

Each market sits under a distinct regime: Germany's works-council route and high reported trust, France's strict CNIL biometric rules, the UK–Ireland split across two jurisdictions, and the Netherlands' regulator treating facial recognition as almost always prohibited. Those legal contexts are real whichever way the adoption figures fall: France sits genuinely lower on active use, and the other three are too close together to rank. The regime an organisation sits under shapes the conversation more than a single regional playbook would.

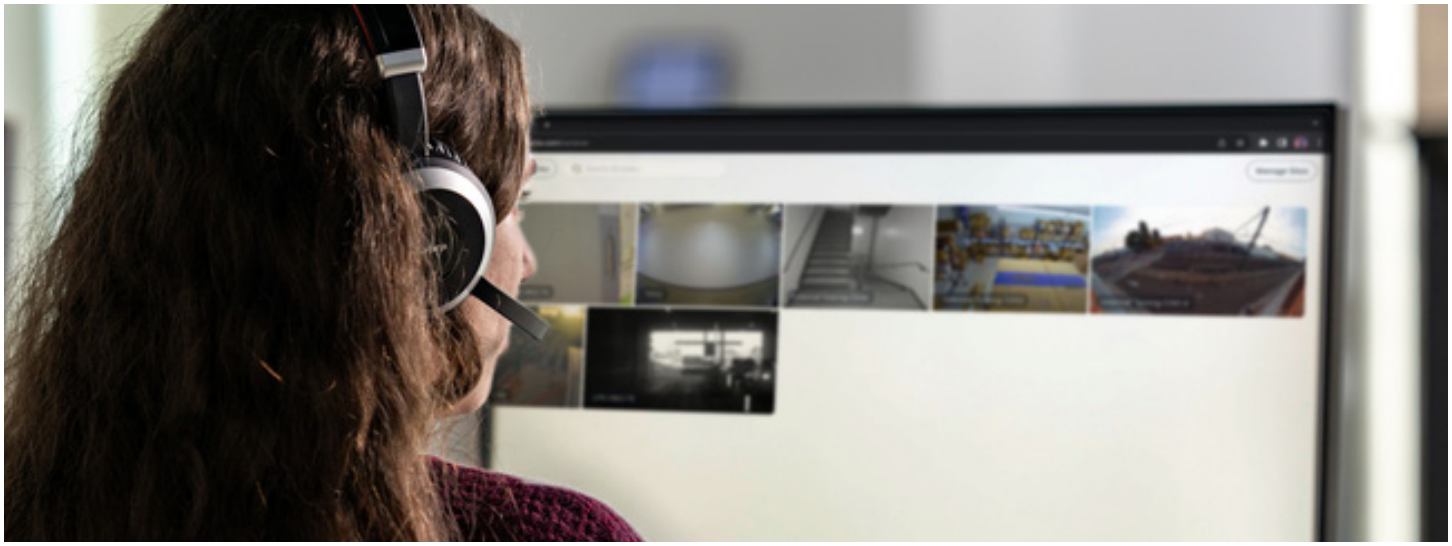
Which AI capabilities each European market holds back

In every market, 38-42% say regulation significantly shapes purchasing



Only two differences clear the workbook's significance test at 5% risk: Germany and France restrict automated decision-making more than the UK & Ireland, and Germany and the Netherlands restrict cross-camera person tracking more than the UK & Ireland. Every other gap sits within sampling noise. Restriction figures mix active restriction with plain non-adoption. Base by market: UK & Ireland (n=203), Germany (n=200), France (n=200), Netherlands (n=156). Ireland is reported with the United Kingdom because its own base (n=52) is too small to report separately.

Survey question: Has your organisation restricted or avoided deploying any of the following AI features due to regulatory or legal concerns? Select all that apply, by market (Q32)



What to do next

Five moves the data points to for the leaders running these decisions in Europe.

1 **Deploy AI analytics within an integrated risk stack.**

The features your peers trust most are the dependable ones, and they sit on a foundation of cloud and cybersecurity. Bring AI analytics in as part of an integrated approach to risk rather than as a standalone tool, so that what you deploy fits the base you already run.

2 **Pursue operational value, deployed carefully.**

The value teams here describe reaches beyond security into operational insight, safety, and compliance. Build your case on that broader read, and be deliberate about which camera data you reuse, because the restraint other organisations show on data is part of how they earn trust internally.

3 **Sequence cloud or hybrid ahead of AI rollout.**

Adoption tracks infrastructure closely: the organisations getting the most from AI are the ones already on cloud, whether fully cloud-managed or hybrid. The meaningful step is leaving an on-premise-only footprint, not necessarily reaching full cloud management; sequence that move with cybersecurity, then AI. If your fundamentals are not yet in place, as in many French organisations, that is the conversation to have before the AI one.

4 **Take the compliance case to your committee.**

More than nine in ten (95%) organisations here rate vendor transparency about how AI models work important, and 45% treat it as a hard requirement. The regulatory load is rising under both regimes: the EU AI Act's high-risk provisions arrive in stages through 2027 and 2028 for the EU markets, while the United Kingdom tightens its data-protection and biometrics rules. The organisations best positioned for that load treat vendor certifications and audit-ready model documentation as procurement requirements, brought to the governance committee early rather than chased later.

5 **Build governance and measurement in during the pilot.**

Comprehensive governance runs 27% of teams still piloting and 64% of those actively using AI, and formal ROI 21% against 55% — active users carry both far more often than pilots. Build them into your plan during the pilot rather than retrofitting them later, so your structure and evidence are in place rather than resting on enthusiasm alone.

Appendix: data tables

Consolidated results for every survey question referenced in this report, from the 2026 Dynata study. Each table opens with the global aggregate (GLOBAL, bold) and four regional aggregates — NA (United States and Canada), Europe (France, Germany, the Netherlands, and United Kingdom and Ireland), Asia (Japan, Malaysia, Singapore, and South Korea), and ANZ (Australia and New Zealand, n=214, the smallest regional unit). The individual European markets follow: France (FR), Germany (DE), Netherlands (NL), and United Kingdom and Ireland (UK+IE). Canada, Ireland, and New Zealand are reported only within their combined units.

The base sample size (n) for each column is shown in the table header. Most questions are asked of all respondents; five carry smaller subsample bases, reflected in their headers: Q10 (organisations not yet fully cloud-managed), Q13 and Q16 (organisations actively using or piloting AI), Q17 (organisations actively using AI), and Q27a (organisations with formal, quantified ROI metrics). An asterisk on a base (for example, n=80*) marks a small base that should be read as directional. Percentages are rounded to the nearest whole number; "—" indicates no responses, and "<1" indicates less than half a percent.

Q4 — Which of the following best describes your organisation's physical security infrastructure deployment across your sites?

Base: all respondents (n=2,741).

Deployment model (%)	GLOBAL n=2,741	NA n=1,001	Europe n=759	Asia n=767	ANZ n=214	FR n=200	DE n=200	NL n=156	UK+IE n=203
Fully cloud-managed	22	25	19	22	18	12	24	17	22
A mixture of both cloud-managed and on-premises	70	68	72	68	78	76	67	75	70
Fully on-premise (servers such as NVR/DVR)	8	6	9	10	4	11	10	8	8
NET: Hybrid or Fully on-premise	78	75	81	78	82	88	76	83	78

Q5 — How many sites does your team monitor?

Base: all respondents (n=2,741).

Sites monitored (%)	GLOBAL n=2,741	NA n=1,001	Europe n=759	Asia n=767	ANZ n=214	FR n=200	DE n=200	NL n=156	UK+IE n=203
1-5	16	15	24	10	14	22	21	33	22
6-20	24	24	24	26	22	20	26	22	29
21-50	25	25	22	27	26	26	25	14	19
51-100	18	16	17	22	22	20	14	23	13
101-500	11	13	10	10	13	6	10	7	14
More than 500	6	7	4	6	4	5	4	1	4

Q7 — To what extent do you agree or disagree with each of the following statements? (% agreeing)

Base: all respondents (n=2,741).

% agreeing with statement	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
The cloud makes security system maintenance easier	91	95	87	90	92	86	86	86	92
The future of physical security is cloud-based	89	92	86	87	91	78	91	86	90
The cloud makes it easier to manage security systems across multiple sites	92	95	91	91	89	88	92	90	94
The cloud makes it easier to scale the security system when adding more devices	93	96	92	90	87	93	92	92	93

Q8 — Thinking ahead to the next 12 months, do you expect your budget for physical security investments to...?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Increase significantly (20%+) (4)	22	28	20	14	26	11	24	23	23
Increase moderately (5–19%) (3)	59	56	59	64	58	66	60	56	54
Stay about the same (2)	17	13	19	21	14	22	15	19	18
Decrease (1)	2	2	2	1	2	2	2	1	5
Don't know/ Can't say	<1	<1	<1	<1	-	-	<1	1	-
NET: Top Box (4)	22	28	20	14	26	11	24	23	23
NET: Top 2 Box (3–4)	81	84	79	78	84	76	83	80	76
NET: Bottom 2 Box (1–2)	19	15	21	22	16	24	16	20	24

Q9 — When considering investments in your physical security system, which would you consider top priority? (select one)

Base: all respondents (n=2,741).

Priority (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Cybersecurity	26	27	27	23	28	26	24	31	30
Cloud storage and infrastructure	25	28	24	20	32	20	24	16	32
AI analytics and video intelligence	23	23	22	24	25	20	22	23	22
Physical-cyber security convergence	18	14	19	24	11	28	20	18	10
Automation / IoT	8	8	8	10	4	5	8	12	6

Q10 — Are you considering either a partial or full transition to a cloud-managed solution?

Base: organisations running hybrid or fully on-premise deployments.

Response (%)	GLOBAL (n=2,138)	NA (n=747)	Europe (n=616)	Asia (n=599)	ANZ (n=176)	FR n=175	DE n=153	NL n=130	UK+IE n=158
Yes - started planning around transition/ currently in progress	72	68	72	77	66	74	74	73	69
Yes - just started to plan about it	22	27	18	16	31	14	18	20	23
No – not considering any transition	5	3	8	5	3	11	7	5	7
Not sure	1	1	1	2	1	1	1	2	1
NET: Yes - just started / Yes - currently in progress	94	96	91	93	97	88	92	93	92
NET: No / Not Sure	6	4	9	7	3	12	8	7	8

Q11 — How important is it to have different physical security products integrated into one centralized system?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Extremely important (5)	45	54	43	36	40	35	44	38	53
Very important (4)	46	41	47	49	56	53	49	50	38
Somewhat important (3)	8	4	9	14	3	11	7	12	7
Not too important (2)	<1	<1	1	1	<1	1	-	-	2
Not at all important (1)	<1	-	-	<!	-	-	-	-	-
NET: Top Box (5)	45	54	43	36	40	35	44	38	53
NET: Top 2 Box (4–5)	91	95	90	85	97	88	93	88	92
NET: Bottom 2 Box (1–2)	1	<1	1	1	<1	1	-	-	2

Q12 — Which best describes your organisation's current use of AI in your physical security system?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
We actively use AI features today	41	47	40	37	31	30	40	41	49
We are currently piloting or testing AI features	39	38	35	41	46	42	37	36	27
We are evaluating AI features but haven't started yet	15	12	17	17	16	20	17	14	16
We are aware of AI features but have no current plans to adopt	4	3	6	4	4	4	5	7	6
We are not familiar with AI features available for physical security	1	1	2	1	1	4	1	2	2
I'm not sure whether our current system includes AI features	<1	-	<1	<1	1	<1	-	1	1
NET: Active / Piloting	80	85	75	78	77	72	77	77	76
NET: Active/ Piloting/ Evaluating	94	96	92	95	94	92	94	90	92
NET: Evaluating / Aware but no plans	19	14	22	20	21	24	22	20	22
NET: Unfamiliar with AI / Unsure	2	1	2	1	2	4	1	3	2
NET: Evaluating/Aware but no plans/Unfamiliar/Unsure	20	15	25	22	23	28	23	23	24
NET: Aware but no plans/ Unfamiliar/Unsure	6	4	8	5	6	8	6	10	8

Q13 — Which of the following AI-powered features does your organisation currently use? (select all that apply)

Base: organisations actively using or piloting AI features.

Feature (%)	GLOBAL (n=2,187)	NA (n=850)	Europe (n=572)	Asia (n=600)	ANZ (n=165)	FR n=144	DE n=154	NL n=120	UK+IE n=154
AI-verified alarm monitoring (reducing false alarms)	55	54	54	57	53	54	64	43	52
AI-generated incident summaries or reports	53	53	52	59	43	59	55	49	44
Real-time motion, loitering, or line-crossing alerts	47	50	43	48	41	38	47	38	47
Facial recognition	43	39	40	50	46	33	41	41	43
AI-powered proactive deterrence (automated voice warnings)	42	39	40	48	42	33	44	38	43
AI-generated timelines	42	42	38	48	31	38	36	35	41
Smart search by attributes (clothing color, vehicle type, etc.)	37	43	34	34	34	25	33	40	38
Object detection (weapons, packages, etc.)	35	39	32	33	37	37	32	29	30
People or vehicle counting / occupancy monitoring	35	38	32	34	31	38	32	32	29
Behaviour detection (tailgating, running, fighting, etc.)	35	34	34	36	34	33	29	41	36
License plate recognition (ALPR/ ANPR)	31	30	31	34	31	28	32	32	31
Natural language video search (describe what you're looking for in words)	29	27	28	34	22	22	28	31	33
Heatmaps for traffic flow and space utilization	23	20	22	26	23	24	19	23	21

Q14 — Which AI capabilities do you believe will have the greatest impact over the next two years? (% ranking in top three)

Base: all respondents (n=2,741).

Capability (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Real-time alerts (motion, loitering, line-crossing, tampering)	31	34	32	28	24	29	32	34	35
AI-generated incident reports and summaries	28	28	28	28	25	27	27	28	30
Anomaly detection (unusual patterns or activity)	27	29	24	30	21	32	20	18	23
Facial recognition	26	25	26	27	31	20	24	24	33
AI-powered proactive deterrence (automated voice warnings)	24	22	22	28	21	22	25	14	24
Automated target tracking (person or vehicle across cameras)	22	22	22	21	25	19	24	26	23
Activity detection (tailgating, running, fighting)	21	23	21	19	22	22	24	17	22
AI live-alerting (ex: a person not wearing a hardhat who should be)	21	20	21	23	22	25	24	24	12
Predictive threat modeling	20	20	19	22	16	15	18	24	19
Person detection by physical characteristics (clothing, appearance)	18	18	18	17	22	16	22	20	15
Object detection (weapons, backpacks)	18	22	17	13	20	16	19	19	15
License plate recognition	12	10	15	12	17	18	11	12	18
People or vehicle counting / heatmaps	12	11	13	13	13	15	12	13	11
Natural language video search	11	11	12	9	13	12	8	14	12

Q15 — How much of an impact do you think AI-based video analytics will have on how you approach physical security?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Major impact — it will fundamentally change our approach (4)	50	56	48	48	42	44	46	53	49
Moderate impact — meaningful improvement to operations (3)	45	40	47	48	53	49	50	42	46
Slight impact — incremental improvement only (2)	4	3	5	4	5	6	5	3	4
No impact (1)	<1	<1	1	<1	<1	<1	-	1	1
NET: Top Box (4)	50	56	48	48	42	44	46	53	49
NET: Top 2 Box (3–4)	96	96	94	96	94	93	95	96	95
NET: Bottom 2 Box (1–2)	4	4	6	4	6	7	5	4	5

Q16 — How satisfied are you with the AI features in your current physical security system?

Base: organisations actively using or piloting AI features.

Response (%)	GLOBAL (n=2,187)	NA (n=850)	Europe (n=572)	Asia (n=600)	ANZ (n=165)	FR n=144	DE n=154	NL n=120	UK+IE n=154
Very satisfied — they deliver clear value (5)	42	52	40	30	43	31	42	40	48
Somewhat satisfied — useful but room for improvement (4)	51	43	54	58	52	65	55	50	46
Neutral — too early to tell (3)	6	4	6	11	5	4	4	10	5
Somewhat dissatisfied — haven't met expectations (2)	<1	1	<1	1	1	-	-	-	1
Very dissatisfied — cause more problems than they solve (1)	-	-	-	-	-	-	-	-	-
NET: Top Box (5)	42	52	40	30	43	31	42	40	48
NET: Top 2 Box (4–5)	93	95	94	88	94	96	96	90	94
NET: Bottom 2 Box (1–2)	<1	1	<1	1	1	-	-	-	1

Q17 — What is the primary way AI adds value to your physical security operations? (select one)

Base: organisations actively using AI features.

Primary value (%)	GLOBAL (n=1,125)	NA (n=469)	Europe (n=303)	Asia (n=286)	ANZ (n=67*)	FR n=59*	DE n=80*	NL n=64*	UK+IE n=100
Real-time threat detection and alerts	31	32	28	32	37	36	20	27	32
Faster investigations (searching footage, finding incidents)	26	29	26	20	30	20	28	23	30
Operational insights beyond security (occupancy, traffic, space utilization)	15	12	18	18	10	15	24	22	13
Proactive deterrence (preventing incidents before they happen)	15	15	12	18	10	17	9	8	13
Compliance and audit support	8	8	9	9	8	7	8	11	9
Reducing false alarms	4	3	7	4	4	5	12	9	3

Q18 — How familiar are you with generative AI capabilities being applied to physical security systems?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Very familiar — I've seen demos or used them (4)	57	64	53	53	52	50	57	47	57
Somewhat familiar — I've heard about them but haven't experienced them (3)	38	33	39	42	42	40	37	44	34
Not very familiar — I've heard the term but don't know the applications (2)	4	3	6	5	4	6	6	6	7
Not at all familiar (1)	1	<1	2	<1	1	3	-	2	2
NET: Top Box (4)	57	64	53	53	52	50	57	47	57
NET: Top 2 Box (3–4)	95	97	92	95	95	91	94	92	91
NET: Bottom 2 Box (1–2)	5	3	8	5	5	9	6	8	9

Q19 — How valuable would each of the following AI-powered features be for your organisation? (% extremely or very valuable)

Base: all respondents (n=2,741).

Feature (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
AI-generated incident reports (automatic written summaries of security events)	84	89	81	81	79	77	84	78	83
AI-generated custom alerts (describe a scenario; the system monitors for it across all cameras)	83	87	78	82	82	76	82	79	77
AI-powered proactive deterrence (system issues contextual voice warnings automatically)	83	87	78	83	80	78	78	72	81
Natural language video search (describe what you're looking for in plain language)	77	84	73	74	74	69	76	69	76

Q20 — If your physical security system could automatically detect unauthorized behaviour and issue contextual voice warnings without human intervention, how comfortable would you be deploying it?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Very comfortable — we would deploy broadly (5)	39	49	36	30	37	29	40	35	42
Somewhat comfortable — we would start with limited deployment (4)	48	44	44	55	52	50	44	44	39
Neutral — would need to evaluate further (3)	10	6	14	13	8	14	14	16	14
Somewhat uncomfortable — concerned about liability or accuracy (2)	2	1	3	3	1	5	2	2	3
Very uncomfortable — we would not want automated interventions (1)	1	<1	2	<1	1	1	1	3	2
NET: Top Box (5)	39	49	36	30	37	29	40	35	42
NET: Top 2 Box (4–5)	87	93	81	84	89	80	84	79	81
NET: Bottom 2 Box (1–2)	3	2	5	3	2	6	2	5	5

Q21 — To what extent do you agree: "In the next 3 years, AI will move physical security from mainly reactive to proactive."

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Strongly agree (5)	38	45	33	33	37	30	31	35	38
Agree (4)	54	50	54	60	56	58	56	51	48
Neither agree nor disagree (3)	7	5	10	6	7	11	11	10	9
Disagree (2)	1	1	2	<1	-	1	2	3	4
Strongly disagree (1)	<1	<1	<1	<1	-	-	<1	1	<1
NET: Top Box (5)	38	45	33	33	37	30	31	35	38
NET: Top 2 Box (4–5)	92	94	87	93	93	88	87	86	86
NET: Bottom 2 Box (1–2)	1	1	3	1	-	1	2	4	5

Q22 — Beyond security, does your organisation use (or plan to use) data from your physical security cameras for any of the following? (select all that apply)

Base: all respondents (n=2,741).

Use of camera data (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Workplace safety and compliance monitoring	66	72	58	67	68	56	52	58	65
Operational efficiency (loading dock throughput, queue management)	58	61	48	64	59	48	46	47	53
Space utilization and occupancy planning	40	45	33	41	44	34	30	35	32
Insurance documentation and claims support	40	44	41	32	42	34	44	42	44
Retail analytics (foot traffic, customer behaviour)	37	39	32	36	44	30	26	30	43
We do not use camera data for non-security purposes	8	5	12	8	5	13	16	8	9
Interested but haven't started yet	2	3	3	2	1	2	3	3	3

Q23 — Top barriers preventing your organisation from adopting or expanding AI in physical security (% ranking in top three)

Base: all respondents (n=2,741).

Barrier (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Privacy concerns (facial recognition, biometric data)	35	33	36	37	34	32	42	36	34
Cybersecurity concerns about AI systems	34	34	29	40	28	32	26	35	26
Cost of AI-enabled systems or features	33	37	30	34	23	33	30	27	30
Concerns about accuracy and false positives	30	33	27	32	24	20	30	26	30
Difficulty integrating AI with existing infrastructure	27	30	24	27	25	20	25	28	23
Regulatory uncertainty (EU AI Act, national AI laws, data privacy regulations)	26	24	31	23	29	30	35	28	29
Concerns about bias or fairness in AI detection	25	25	24	26	27	28	16	22	29
Lack of confidence that AI will deliver measurable ROI	21	19	19	24	28	20	22	19	16
Lack of understanding of what AI features actually do	18	17	17	20	27	14	21	14	18
No executive buy-in for AI investment	12	8	14	13	15	14	18	16	9
We don't see significant barriers — we're actively adopting	8	10	11	4	9	12	8	9	14

Q24 — Does your organisation have a formal policy or governance framework for using AI in physical security?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Yes — comprehensive AI governance policy covering physical security	41	47	37	38	42	34	43	35	37
Partially — general AI guidelines but nothing specific to physical security	41	38	42	42	44	43	44	40	40
In development — currently creating one	14	13	15	15	10	14	11	19	16
No — we do not have any AI governance policy	4	3	5	4	4	7	2	6	6
I'm not sure	<1	<1	1	<1	1	2	-	1	<1
NET: Yes & Partially	82	84	79	80	86	78	86	75	77
NET: Partially & In development	54	50	56	57	54	57	55	59	56
NET: No & I'm not sure	4	3	6	5	5	8	2	6	7
NET: Partially & In-Development' & No & I'm not sure	59	53	63	62	58	66	57	65	63

Q25 — How important is it that your physical security vendor provides transparency about how their AI models work?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Extremely important — it's a requirement for purchasing (4)	47	54	45	40	42	43	46	39	49
Very important — strongly influences our decision (3)	47	42	50	50	50	50	50	54	47
Somewhat important — we consider it but it's not decisive (2)	6	4	4	9	7	7	3	4	3
Not important — we trust established vendors (1)	<1	<1	1	<1	1	-	-	3	<1
NET: Top Box (4)	47	54	45	40	42	43	46	39	49
NET: Top 2 Box (3–4)	94	96	95	90	92	93	97	93	97
NET: Bottom 2 Box (1–2)	6	4	5	10	8	7	3	7	3

Q26 — To what extent do you agree: "I trust AI-powered physical security systems to make accurate decisions without human oversight."

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Strongly agree (5)	26	32	23	20	29	18	25	24	26
Agree (4)	48	43	49	52	51	50	55	47	45
Neither agree nor disagree (3)	16	11	19	20	11	22	16	20	17
Disagree (2)	9	12	7	7	8	8	4	7	9
Strongly disagree (1)	1	1	2	1	1	2	-	1	3
NET: Top Box (5)	26	32	23	20	29	18	25	24	26
NET: Top 2 Box (4–5)	74	76	72	73	80	68	80	71	70
NET: Bottom 2 Box (1–2)	10	13	9	7	8	10	4	8	13

Q27 — Has your organisation measured the ROI of AI features in your physical security system?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Partially — we track some metrics informally	48	46	51	48	52	55	53	49	46
Yes — we have formal metrics and quantified ROI	38	45	32	36	41	26	32	35	34
No — we haven't attempted to measure ROI	11	8	13	15	4	15	11	12	15
Not applicable — we don't use AI features	2	1	4	2	3	4	4	4	4

Q27a — What specific metrics or indicators does your organisation use to measure the ROI of AI features? (among organisations with formal, quantified metrics)

Base: organisations with formal, quantified ROI metrics.

Metric (%)	GLOBAL (n=1,050)	NA (n=447)	Europe (n=243)	Asia (n=272)	ANZ (n=88*)	FR n=53*	DE n=65*	NL n=55*	UK+IE n=70*
System efficiency	62	64	58	61	72	51	48	64	67
Response time	28	32	25	26	26	26	18	34	23
Incident management	24	27	17	19	40	11	18	16	21
Service improvement	20	21	15	20	25	19	8	14	19
AI-driven / less manual processing	11	12	13	8	9	9	18	14	9
Verification methods	3	3	3	3	1	-	5	4	4
Systematic measures	2	1	3	4	-	4	3	-	4
Organisational metrics	42	48	35	37	51	21	37	40	40
False-alarm-rate reduction	19	27	13	10	26	6	9	18	17
Safety and compliance	8	8	7	8	10	4	6	7	11
Business impact / success rate	4	2	4	4	4	6	6	-	6
Reliability and stability	3	3	3	4	1	4	3	7	-
Operational costs	23	28	18	18	26	9	14	11	33
Cost efficiency	18	23	13	14	19	8	6	9	27
Electronic devices and software	16	16	21	15	8	30	22	14	17
Profitability	11	10	13	10	18	11	11	16	13
Customer satisfaction	5	5	6	4	3	11	9	2	1
Employee and staffing	3	2	3	3	6	6	-	4	3
General positive mentions	2	2	2	2	1	2	2	-	4

Q28 — Which benefits has your organisation experienced (or expects to experience) from AI in physical security? (select all that apply)

Base: all respondents (n=2,741).

Benefit (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Improved real-time threat detection	53	58	46	53	49	50	38	40	56
Faster incident investigations	51	54	49	51	44	53	40	42	58
Proactive crime prevention	39	42	34	40	46	29	30	35	40
Reduced false alarms	38	44	35	34	33	34	30	35	39
Lower overall security operating costs	38	34	34	46	35	34	29	35	36
Improved cross-department data sharing (operations, facilities, HR)	37	40	29	42	33	30	30	31	28
Reduced need for on-site security personnel	32	28	32	40	29	34	28	28	36
Reduction of shrinkage or theft	30	30	30	29	35	36	27	31	28
Better insurance positioning or reduced premiums	27	29	29	22	31	30	32	24	28
Reduction of liability and/or lawsuit claims	25	27	25	22	31	24	24	26	26
Increase in top-line revenue	25	26	21	28	28	16	24	18	25
None — no measurable benefits yet	3	3	4	2	<1	2	6	4	5

Q29 — How has AI in physical security affected your organisation's security staffing?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Same headcount but shifted roles (more analysis, less manual review)	23	22	23	25	20	24	21	28	19
Same headcount but each person is more effective	22	22	22	23	23	20	22	24	22
Increased headcount to manage AI systems	20	17	16	16	22	17	17	10	17
Reduced headcount due to AI efficiencies	18	14	19	22	14	20	22	15	19
No impact on staffing	14	13	16	11	17	17	14	18	17
Not applicable	3	2	4	2	3	4	3	4	6

Q30 — How long does it typically take your team to investigate a security incident (from alert to resolution)?

Base: all respondents (n=2,741).

Duration (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Less than 1 hour	14	14	17	10	14	17	16	20	16
1 – 4 hours	44	47	43	40	41	37	42	46	48
4 – 24 hours	34	31	33	40	35	41	36	29	25
1 – 3 days	7	6	6	9	9	4	4	5	10
More than 3 days	1	2	1	1	1	<1	2	1	2

Q31 — How much do government regulations around AI influence your organisation's physical security purchasing decisions?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Significant influence — regulations directly determine what we can deploy (4)	37	40	40	34	29	38	42	40	39
Moderate influence — we factor them in but they're not the primary driver (3)	49	48	44	50	57	45	47	43	43
Slight influence — we're aware but they don't change our behaviour much (2)	9	7	11	11	8	12	7	13	13
No influence (1)	3	3	3	3	4	2	4	2	3
I'm not sure what regulations apply to our AI-powered security systems	2	2	2	2	1	3	-	2	2
NET: Top Box (4)	37	40	40	34	29	38	42	40	39
NET: Top 2 Box (3–4)	86	88	84	85	86	82	88	83	82
NET: Bottom 2 Box (1–2)	12	10	14	13	12	14	12	15	16

Q32 — Has your organisation restricted or avoided deploying any of the following AI features due to regulatory or legal concerns? (select all that apply)

Base: all respondents (n=2,741).

Feature (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Automated decision-making (AI triggering actions without human review)	44	45	38	49	49	42	43	35	30
Real-time biometric identification	43	49	39	38	46	34	40	40	41
Facial recognition	42	48	38	36	45	34	40	36	42
Behaviour scoring or profiling	36	39	33	32	41	34	30	36	33
Cross-camera person tracking	32	28	34	31	41	31	38	39	29
None — regulations have not restricted our AI adoption	18	19	17	18	13	16	14	17	21
Not applicable — we don't use AI features	4	2	6	4	3	6	4	6	6

Q33 — When evaluating physical security vendors, how important is it that products comply with international regulations and standards (e.g., NDAA, EU AI Act, GDPR, SOC 2)?

Base: all respondents (n=2,741).

Response (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Extremely important — hard requirement (4)	45	51	48	36	44	42	48	48	52
Very important — strong preference (3)	46	43	44	52	50	47	46	42	41
Somewhat important (2)	7	4	7	11	5	10	4	8	5
Not important (1)	1	2	1	1	1	1	1	2	1
NET: Top Box (4)	45	51	48	36	44	42	48	48	52
NET: Top 2 Box (3–4)	92	94	92	88	94	89	94	90	94
NET: Bottom 2 Box (1–2)	8	6	8	12	6	11	6	10	6

Q36 — Thinking about the next three years, what is the single biggest change you expect to see in physical security? (unprompted; coded responses)

Base: all respondents (n=2,741).

Expected change (%)	GLOBAL (n=2,741)	NA (n=1,001)	Europe (n=759)	Asia (n=767)	ANZ (n=214)	FR n=200	DE n=200	NL n=156	UK+IE n=203
Artificial intelligence	54	62	52	44	57	44	58	55	49
Wider AI adoption	26	31	27	18	26	22	32	34	23
Automation and robotics	15	20	11	13	19	9	12	8	13
Proactive response and prevention	12	16	10	8	14	6	7	12	14
Detection and prediction of risks	11	14	8	9	18	6	10	6	9
Organisational system improvements	46	46	44	45	55	41	40	47	48
System integrations	18	23	15	12	25	6	18	19	18
Convenience, efficiency, accuracy	12	10	11	14	12	12	10	10	11
Safety and security outcomes	11	9	10	14	11	13	6	9	10
Reputation, growth, service quality	1	1	1	1	<1	-	1	2	2
Workforce changes	10	9	8	15	7	7	8	6	8
Profit and cost structure	5	4	4	8	4	2	3	4	5
General positive mentions	2	4	1	2	<1	<1	<1	1	2
External and sustainability factors	<1	1	1	<1	<1	1	1	1	<1

Theme totals (bold parent rows) count each respondent once, even when an open-ended response was coded to several sub-themes, and a respondent may be counted under a parent theme without matching any listed sub-theme; a parent total therefore need not equal the sum of the sub-themes beneath it. Responses to Q36 were unprompted and coded after collection.

Key measures by AI-maturity stage

Base: Europe (n=759). Columns are AI-maturity stages (Q12): organisations actively using AI, piloting it, or evaluating it.

Measure (%)	Active (n=303)	Piloting (n=269)	Evaluating (n=126)
Comprehensive AI governance covering physical security	64	27	9
Formal, quantified ROI metrics	55	21	11
Trust AI to act without human oversight (top-2-box)	84	79	52
Comfortable deploying broad AI autonomy (top box)	63	23	14
Expect significant budget growth (20%+ over next 12 months)	32	15	6
Regulation significantly influences purchasing	55	31	32

Active AI use by cloud deployment

Base: Europe (n=759). Share of organisations that actively use AI features today (Q12), by physical-security deployment model.

	Fully cloud-managed (n=143)	Hybrid (n=545)	Fully on-premise (n=71*)
Actively use AI features today	59	37	22

Active AI use by number of sites

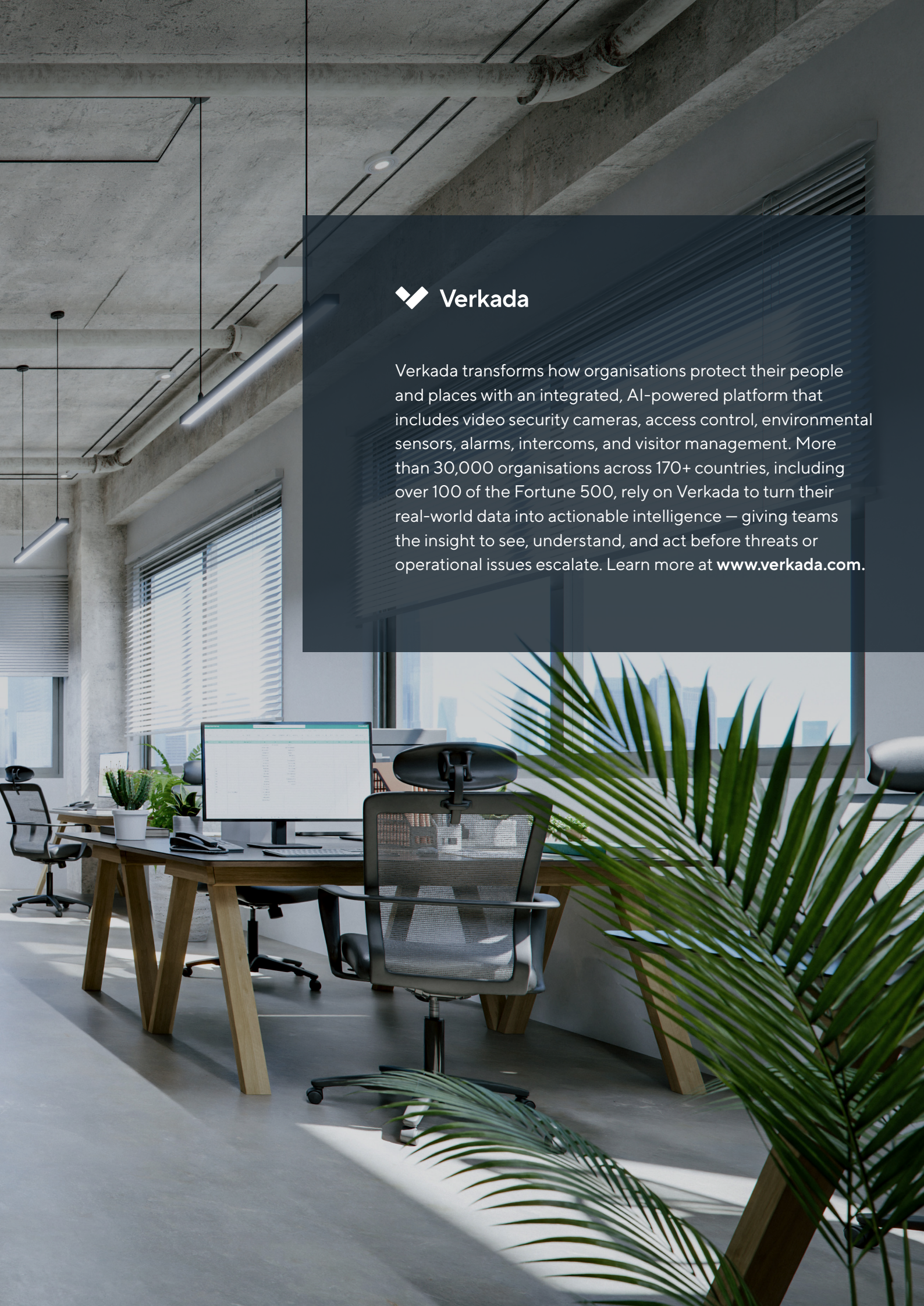
Base: Europe (n=759). Share of organisations that actively use AI features today (Q12), by number of sites monitored.

	1-5 (n=181)	6-20 (n=183)	21-50 (n=164)	51-100 (n=131)	101-500 (n=72*)	More than 500 (n=28*)
Actively use AI features today	27	35	46	51	47	46

AI autonomy comfort by seniority

Base: global respondents by job-title level (Q3). Comfort deploying autonomous AI deterrence (Q20). A global cut; the survey does not provide a region-specific seniority breakdown.

Comfort with autonomous AI deterrence	Manager (n=967)	Director/Senior Manager (n=1,018)	C-suite (n=557)
Would deploy autonomy broadly	31	39	53
Would start with limited deployment	51	49	39
Neutral — would evaluate further	14	9	6
Somewhat uncomfortable	3	2	1
Very uncomfortable	1	1	1



Verkada

Verkada transforms how organisations protect their people and places with an integrated, AI-powered platform that includes video security cameras, access control, environmental sensors, alarms, intercoms, and visitor management. More than 30,000 organisations across 170+ countries, including over 100 of the Fortune 500, rely on Verkada to turn their real-world data into actionable intelligence — giving teams the insight to see, understand, and act before threats or operational issues escalate. Learn more at **www.verkada.com.**