

Five Ways Physical AI Is Reshaping Security Deployment



Outside China, the world's installed base of network cameras was on pace to reach 562 million by the end of 2025, climbing to 736 million by 2029. Nearly 80% of the cameras shipped in 2024 arrived with analytics on board. Two-thirds of them did so with deep-learning capability. Cameras have become intelligent sensors.

The market reflects this. Global video surveillance revenue grew 4.3% to **\$27 billion** in 2025, and the growth now tracks AI capability more than unit volume. Whereas previously value was a measurement of coverage and storage, that's now shifted to how intelligent a platform is.

What else changed? The first bullet on the whiteboard: What the platform has to understand, vs. where to mount the cameras. Here are five ways that shift moves decisions to the front of a deployment.

Here are five ways physical AI is reshaping security deployment strategies:

- 1 | **Intelligence Moved to the Edge**
- 2 | **Systems are Specified as Platforms**
- 3 | **Convergence is the Architecture**
- 4 | **Open Ecosystems are the Default**
- 5 | **Cybersecurity and Lifecycle Management are Deployment Prerequisites**



1 Intelligence Moved to the Edge

Decisions now happen at the point of capture.

- Intelligence used to live in the server room. Cameras captured video, streamed it to a central recorder, and analysis happened after the fact, if at all. That model does not scale to hundreds of millions of connected devices.
- Processing has moved onto the device. Purpose-built chipsets run object detection, license-plate recognition, and behavioral analysis where the video is captured, generating insight in the moment. Gartner projected that by the end of 2025, more than 55% of deep-neural-network data analysis would happen at the point of capture.

Edge processing cuts bandwidth and storage by sending only metadata and alerts, and it enables real-time response while keeping sensitive data on-site. According to a [2026 Axis Communications report](#), the U.S. now runs more than 300 real-time crime centers, up from roughly 80 since 2021, each built to act on video intelligence in the moment. Designing an edge-first architecture, with the compute, thermal, and power headroom to run several analytics at once, is a front-end decision.

For the companies building these devices, edge-first is a hardware constraint before it is a software feature. More analytics on the camera means more compute and more heat inside a smaller, cheaper, lower-power enclosure. You engineer that headroom in at the design stage, or the device cannot run the workload the market now expects.

2 | AI Expands the Business Case for Intelligent Cameras

The camera buying decision now spans three departments: security, operations, and business intelligence.

When a camera only recorded, it was a line on the security budget. Now the same device delivers operational and business intelligence, and the budget has changed with it.

Security is still the primary use case, cited by 89% of end customers, but 42% now deploy video for operational efficiency and 38% for business intelligence, up from 38% and 20%, respectively, a year earlier. Genetec's 2026 survey of more than 7,300 professionals finds physical security moving from a protection layer to an enterprise function that contributes to broader business goals. The same camera that secures a loading dock measures throughput, and the one on a production line supports predictive maintenance and quality inspection.

AI monitoring earns its keep quickly. Securitas reports that AI-powered monitoring cut escalated false alarms by 59%, freeing hundreds of guard-hours a year, and an Omdia study commissioned by BriefCam found more than 85% of organizations using video analytics reach a return within 12 months.

A deployment planned for surveillance alone leaves most of the platform's return unclaimed.



3 | Convergence is the Architecture

IT, OT, and physical security are unifying onto one platform that connects video, sensors, and access control.

This is already the norm: Genetec finds more than 70% of organizations running unified or integrated systems, with 60% naming the integration of new capabilities as their main reason to replace legacy technology. Axis survey data points the same way, with 41% of end customers ranking the move to a single unified platform among their top priorities for the next one to three years.

For deployment, convergence pushes decisions upstream. Interoperability, unified governance, and data architecture have to be designed at the outset. Retrofitting integration onto siloed systems is slow and costly, and it leaves the result brittle.





4 Open Ecosystems are the Default

Vendor-neutral, standards-based architecture is the new baseline.

Robust APIs and SDKs and support for open standards give organizations room to build with more than one vendor. Modular design helps this as well. Together they combine the best hardware and analytics along with available applications, then evolve that mix as needs change.

Cloud adoption in physical security is projected to climb from 27% to 44% of customers within two years, and hybrid cloud is the stated preference in Genetec's 2026 findings. The open AV1 codec, backed by the Alliance for Open Media, cuts bandwidth and storage requirements by 30 to 50% while improving quality and AI performance.

For durability, buyers favor architectures that carry that same openness into deployment: hybrid edge-cloud, built to protect today's investment and leave room for tomorrow's analytics.

Open and modular moves the hard part onto the hardware. Combining best-in-class components from several suppliers into one interoperable, manufacturable product is an integration challenge before it is a software one, and it gets solved on the production line.

5

Cybersecurity and Lifecycle Management are Deployment Prerequisites

Securing the security system is now a gating factor.

Every intelligent camera is a connected computer, which makes it part of the attack surface. **Forescout's analysis** of nearly 19 million devices found the share of IoT devices carrying vulnerabilities rose from 14% in 2023 to 33% in 2024, with IP cameras among the most exposed device types. Attackers favor those devices precisely because they sit inside the enterprise network and stay invisible to the security stack watching it.

The global average cost of a successful breach has climbed to a **record \$4.99 million**. Successful intrusions have an intangible cost too, which has driven concerns about cybersecurity and data prevention across a wide swath of those surveyed. These now rank as the #2 concern among end customers, architects and engineers, and system integrators, with 44% agreeing on its importance.

Device hardening, secure boot, end-to-end encryption, and zero-trust integration are baseline. A secure supply chain that guarantees device integrity from production through provisioning prevents tampering and counterfeiting. Lifecycle management determines whether a fleet stays secure across its full service life. Firmware updates, health monitoring, and long-term support are what make that possible. With **global information security spending predicted** to reach \$213 billion in 2025 and \$240 billion in 2026, these have become conditions of deployment.

Securing the security system reaches back to the production line. Device integrity gets built in from the first stage of manufacturing and verified through provisioning, so it rests with whoever fabricates and ships the hardware.



Monitoring Was the Baseline. Intelligence Is the Standard.

The market is completing a decisive move, from systems that document the past to platforms that identify risk, automate response, and deliver operational insight. Security is now an intelligence investment, and it has to be designed for from the first deployment decision.

That promise raises the bar on the companies that build these systems. Intelligent-edge devices have to pack more compute, better optics, and stronger cybersecurity into a form factor that keeps shrinking, using less power and costing less to make. Then it has to scale worldwide without compromising quality or intellectual property.

As the manufacturing and engineering partner behind many of the world's leading security brands, Jabil builds roughly 3 million network cameras and more than 250 security products a year, across cameras, radar, access, and perimeter systems. In-house active alignment, high-level assembly, and design-for-manufacturing turn advanced sensing concepts into producible, scalable products.

Building that future demands as much from the production line as from the lab. Jabil is built for both.

How can Jabil help you build the next generation of intelligent security?

Visit jabil.com/security-ai

About Jabil

At Jabil (NYSE: JBL), we are proud to be a trusted partner for the world's top brands, offering comprehensive engineering, manufacturing, and supply chain solutions. With over 50 years of experience across industries and a vast network of over 100 sites worldwide, Jabil combines global reach with local expertise to deliver both scalable and customized solutions. Our commitment extends beyond business success as we strive to build sustainable processes that minimize environmental impact and foster vibrant and diverse communities around the globe. Discover more at www.jabil.com.