PHYSICAL SECURITY TRENDS FOR 2026

Nicholas Smith *explains why organisations will focus on flexibility, responsible AI and unified connected systems to strengthen security and operational performance*

In 2026, the conversation around cloud adoption will continue to mature. Organisations will prioritise solutions that offer deployment flexibility and scalability. Rather than committing to a single deployment model, enterprises will evaluate each workload based on performance, cost and data residency requirements. They will then choose the environment that best supports their operational needs, whether it's on-premises, in the cloud or a hybrid approach.

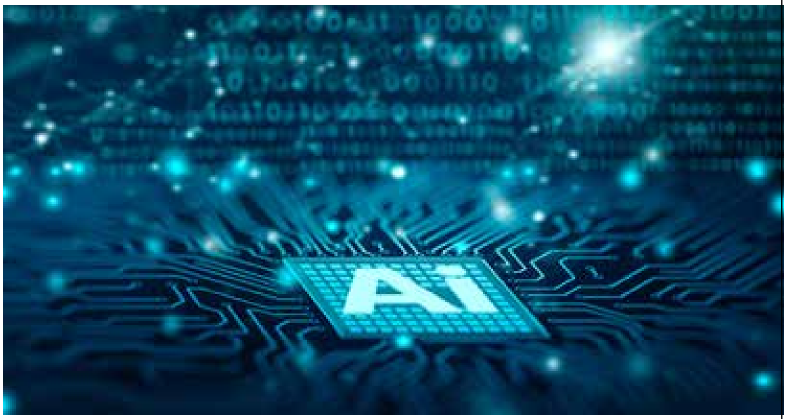
Open architecture solutions will give end users the freedom to choose the devices and applications that best support their operations. This approach will extend the life of existing infrastructure while allowing teams to adopt cloud services where they add the most value. Vendors that offer full-range deployment options and strong interoperability across environments will be best positioned to meet these expectations. In contrast to proprietary systems that limit choice and create lock-in, open solutions provide a more adaptable path that supports long-term flexibility and control.

In 2026, the conversation will shift from AI and LLM hype to practical, outcome-driven Intelligent Automation (IA) solutions that streamline workflows, improve accuracy and enable faster, smarter decisions. IA will increasingly automate repetitive tasks, enhance monitoring precision, support predictive maintenance and extract meaningful insights from growing data volumes.

Rather than adopting technology for its own sake, users will focus on features that genuinely improve daily operations, such as intelligent search to accelerate investigations, reduce false alarms and strengthen situational awareness. By optimising response and reducing manual overhead, IA allows operators to focus their time and energy on important work and decision-making that requires human judgment.

As the market matures, expectations around transparency and responsible implementation will rise. Users will demand clarity on how AI is used, how systems are built and how data is collected, processed and protected. They will also expect vendors to prioritise cyber security and ensure that IA features are deployed in a safe, controlled and accountable way. Organisations will move away from innovation for its own sake to delivering measurable, trustworthy and meaningful outcomes powered by intelligent automation.

Access control will remain a top priority as organisations modernise legacy systems and focus on maximizing ROI. The value of access control is expanding well beyond locking and unlocking doors to deliver measurable business outcomes, such as energy efficiency, occupancy management and operational insights.



Picture credit: AdobeStock

Access Control as a Service (ACaaS) adoption will accelerate as organisations prioritise easier maintenance, greater scalability and predictable operating costs. Enterprises will favour hybrid deployments that combine on-premises and cloud capabilities. Unifying ACaaS and Video Surveillance as a Service (VSaaS) will further enhance visibility and streamline management across sites.

Mobile credentials and biometrics will continue to transform identity management, offering greater convenience and security while decentralising ownership of identity data. As mobile wallets and ultra-wideband technologies become mainstream, users will gain more ease and flexibility in how they authenticate and interact with secured environments and facilities.

Over the next year, the number of connected devices will continue to surge as organisations integrate IoT sensors, building systems and smart devices into unified security and operations platforms. Bringing this information together in one place will give teams a clearer view of what is happening across their facilities and help them respond faster and with greater confidence.

The convergence of IT, operational technology and physical security will accelerate, enabling real-time data sharing and smarter decision-making across facilities. End users will expect open, scalable platforms that connect diverse devices securely and deliver both operational and security value.

As the landscape grows more complex, organisations will seek guidance on how to deploy the right technologies and manage them effectively. The leaders in this space will be those who unify diverse devices securely, offer cloud-native and hybrid options, and embed cyber security and data residency into their design ●

Intelligent Automation will allow operators to focus on decision-making that requires human judgment

Nicholas Smith is the Regional Sales Director for Genetec UK and Ireland.