SJUK SECURITY JOURNAL UNITED KINGDOM
Issue 53 | June 2025
SecurityJournalUK.com

Information, Analysis and Insights for Manufacturers, Installers and Senior Security Professionals

Special Report

ARTIFICIAL INTELLIGENCE

Produced in partnership with Western Digital

p43

SJUK LEADERS IN SECURITY
CONFERENCE | MANCHESTER 2025

NetVu
PROTECTING YOUR WORLD

Head to Head Exclusive

FROM PIONEER TO INDUSTRY *leader*

p14

NetVu's Chief Technology Officer and Founder, Mike Newton, tells SJUK about the company's mission to make people safer through continuous innovation

PLUS

Counter **Terror**

Stadium **Security**

Education

ADVANCIS SOFTWARE SOLUTIONS

Streamline your Security.

WinGuard and **AIM** revolutionise the management of physical security and identity systems through seamless integration and real-time situational awareness.

Advancis Software & Services provides advanced software solutions that streamline the complex workflows of modern Security Operations Centers (SOCs). By integrating disparate systems, sensors, and devices into a unified user interface, Advancis simplifies operations and enhances situational awareness. Operators benefit from structured action plans that guide responses to both critical incidents and routine events, with every action and event centrally logged for comprehensive reporting and analysis.

At the core of the Advancis offering is WinGuard, a vendor-neutral physical security management system and building management platform based on the AOP (Advancis Open Platform) architecture. AOP enables seamless customisation through the addition of new functionalities, adapters, and user interface components—empowering integrators and end users to tailor the platform to specific project needs without limitations.

Complementing WinGuard is Advanced Identity Manager (AIM), a centralised solution for managing and synchronising logical and physical access rights across diverse identity, access control, and biometric systems. AIM ensures that user privileges align consistently with roles across both IT and physical security infrastructures.

Get more info about our Solutions.

advancis.net

PROUD PLATINUM SPONSOR OF

SJUK LEADERS IN SECURITY

winguard provides

- Central Event Visualisation
- Vendor-neutral Integration
- Dynamic Workflows
- Dashboards & Reporting
- Modular and scalable

AIM provides

- Integrated Access Control
- Unified Credential Management
- Centralised Authorisation Models
- Seamless Migration Possibilities
- Automated Compliance

advancis

The strategic imperative for security leaders

Oliver Lacey, Head of Sales – Identity Solutions, Advancis Software & Services explores why converged identity management is essential

In today's landscape, enterprise organisations face unprecedented challenges in securing their physical and digital environments. As companies expand across borders, integrate diverse technologies and handle vast amounts of sensitive data, the need for robust, centralised identity and access management becomes critical. Physical Identity and Access Management (PIAM) solutions are emerging as a cornerstone for Chief Information Security Officers and Chief Security Officers seeking to bolster security, ensure compliance and streamline operations.

This article explores the key benefits of implementing an advanced PIAM solution, specifically tailored to the needs of strategic leaders and service providers in enterprise security.

Centralised identity management

For complex, high-secure and multi-national enterprises, managing the physical identities of employees, contractors, visitors and vendors across multiple locations and systems is a monumental task. Each site, whether an office, manufacturing plant or data centre, typically operates its own security infrastructure, creating operational silos and increasing the risk of inconsistencies.

PIAM solutions provide the option to centralise identity and access management across the entire organisation. It offers a unified platform that consolidates identity data, eliminating duplicate entry, minimising administrative burden and improving data hygiene. The traditional saying "you cannot secure what you don't know is there" becomes increasingly challenging in the modern environment. With a global view of assets, authorisation models and access rights, security leaders gain centralised governance and full control of their global estate. This unified approach enables enterprises to apply consistent policies, improve operational oversight and enhance resilience across all physical locations.

Operational efficiency, automating processes, reducing costs

Manual access request and provisioning processes are time-consuming, error-prone and costly, particularly in organisations with high staff turnover or numerous temporary workers. A modern PIAM solution automates physical access requests, approvals, provisioning and de-provisioning, dramatically improving operational efficiency.

By integrating with HR systems, AIM automatically updates access rights when an employee is hired, promoted or leaves the organisation. This automation covers the entire identity lifecycle, from hire to retire, while maintaining organisational control through auditable approval workflows. Research shows PIAM solutions provide up to 40% savings in administration time during the on-boarding processes. Self-service portals empower cardholders to request approvals, renewals or role changes, reducing

"By closing security gaps and maintaining rigorous access controls, enterprises significantly reduce their risk exposure and enhance their overall security posture."

the administrative burden on security teams and accelerating onboarding. Faster processing leads to lower operational costs, fewer manual interventions and a significantly improved user experience.

Hardening your security posture

Effective access control is fundamental to reducing the risk of insider threats, social engineering attacks and unauthorised physical breaches. PIAM solutions allow CISOs and CSOs to enforce the principle of least privilege, ensuring that access to sensitive areas is granted strictly on a business-need basis.

With centralised access models, organisations can swiftly revoke or adjust permissions when roles change or contracts end. Terminating access can be executed promptly and recertification models help maintain a zero-trust framework, ensuring that historical access does not translate to ongoing access without justification. By closing security gaps and enforcing rigorous

access safeguards, enterprises can significantly reduce risk exposure and strengthen their overall security posture.

Policy enforcement

One of the greatest challenges for security leaders is enforcing corporate policies across siloed and diverse platforms, systems and physical locations. Without standardised management, organisations risk policy violations such as breaches of separation of duties or violations of least privilege.

AIM enables organisations to define access policies once and enforce them automatically across all sites and systems. This ensures consistent application of corporate policies, reduces the likelihood of violations and simplifies governance. For CISOs and CSOs, having automated and consistent policy enforcement across the enterprise is essential for maintaining robust internal controls and mitigating organisational risks.

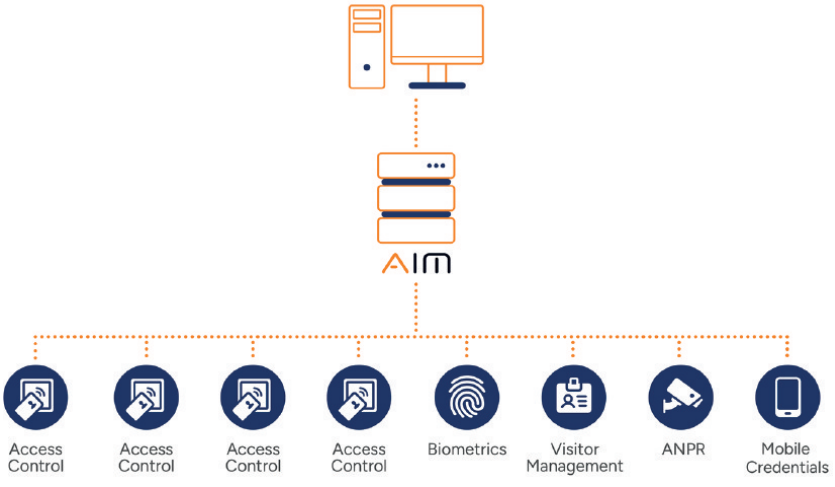
Integration of IT solutions and PACS

The convergence of digital identity management and physical access control is a key component of comprehensive enterprise security. PIAM solutions act as the critical bridge between IT Identity and Access Management (IAM) systems and Physical Access Control Systems (PACS), such as door controllers, biometrics and locker management solutions.

By integrating with IT identity providers (e.g., Active Directory) and broader digital workplace platforms, AIM synchronises logical and physical access based on an individual's role, department or project. This streamlining creates a unified identity governance framework that minimises gaps between digital and physical environments.

> **"PIAM solutions provide the option to centralise identity and access management across the entire organisation."**

The result is consistent, organisation-wide identity lifecycle management that supports a total risk profile and enables a holistic understanding of security posture. Adversaries and threats posed attempt to exploit the gaps and lack of communication between digital and physical solutions and their respective system owners. AIM offers a truly converged and unified identity management across both environments to mitigate these risks and threats posed in traditional IT and security environments with instance alerts, communication and response through one front-end.



Compliance and audit requirements

Enterprise organisations operating in the UK and across Europe must comply with stringent regulatory requirements, including GDPR, NIS2 and ISO standards. Failure to meet these standards exposes organisations to fines, reputational damage and operational disruption.

PIAM solutions ensure that only authorised individuals access sensitive areas, maintaining detailed audit logs and enforcing compliance workflows. AIM simplifies regulatory reporting by centralising all access-related data, reducing the stress and complexity associated with audits. Security leaders can demonstrate full access governance to regulators, supply chain partners, customers and internal auditors, reducing the risk of non-compliance penalties and reinforcing the organisation's reputation for robust governance.

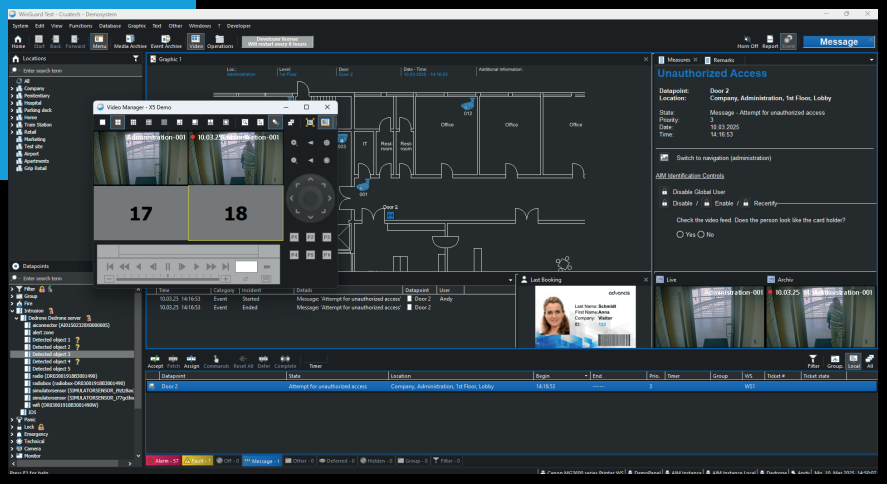
Supporting enterprise growth without disruption

As organisations expand through mergers, acquisitions and new office openings, managing access models across an ever-growing footprint becomes increasingly complex. A PIAM solution must be scalable, supporting the management of thousands of identities across geographically distributed and diverse environments.

AIM delivers standardised policies and processes to onboard new facilities and integrate acquired organisations seamlessly, without overwhelming security teams or requiring wholesale replacement of existing access infrastructure providing a return on investment from the initial financial outlay. By future-proofing the physical security architecture, AIM minimises business disruption and supports enterprise growth with agility and co

Real-time monitoring and incident response

In today's fast-moving threat landscape, real-time monitoring is essential. Integrations of PIAM and



PSIM solutions provide security teams with instant alerts about suspicious activities, such as unauthorised after-hours access or anomalous user journeys. The integrated combination of AIM and WinGuard leverages real-time data to enable automated workflows that guide rapid incident response.

By shortening the window between risk detection and mitigation, AIM empowers physical security teams to act decisively, enhancing the organisation's resilience to both internal and external threats. Actionable intelligence allows security leaders to make informed decisions, improving the organisation's capacity to detect, respond to and recover from incidents.

> **"AIM offers a powerful, scalable platform that centralises identity and access management."**

What we're witnessing is a paradigm shift. Security is no longer about isolated control, it's about unified governance of who can go where, when, and under what circumstances, regardless of the access vector. With AIM AOP embedded directly into WinGuard, we now offer our clients the ability to orchestrate and monitor all identity-based activities in real time, from the Security Operations Centre (SOC).

PIAM benefits for CISOs and CSOs

- **Centralised identity management –** Efficiency and consistency across all locations
- **Compliance and auditing –** Easier audits, reduced legal and regulatory risks
- **Operational efficiency –** Faster onboarding, lower administrative costs
- **Risk reduction and security –** Stronger protection against insider threats and breaches
- **Converged digital and physical access –** Unified identity governance across environments
- **Scalability –** Supports enterprise growth with minimal disruption
- **Policy enforcement –** Stronger internal controls and governance
- **Real-time monitoring –** Faster threat detection and response

For leaders in enterprise security, the challenge is no longer just about managing who has access but about governing how that access is granted, monitored and controlled across the organisation. With growing regulatory demands, increasing security threats, and expanding operational footprints, the need for an integrated PIAM solution has never been clearer.

AIM offers a powerful, scalable platform that centralises identity and access management, integrates seamlessly with IT and PACS systems, and empowers security teams to enhance governance, reduce risks and improve operational efficiency. For CISOs and CSOs, implementing a PIAM solution is a strategic decision that delivers measurable security and business benefits.

By embracing a centralised, automated and policy-driven approach, multi-sited and high-risk organisations can navigate today's complex security landscape with confidence, resilience and choice.

For security leaders

The SJUK Leaders in Security conference, hosted at The Hilton Deansgate, Manchester, UK on 25th June 2025, is a landmark for innovation in the security field. This year's focus on resilience, interoperability and cyber-physical convergence resonates strongly with our strategic vision at Advancis.

During our presentation, we'll showcase the benefits of our market leading PSIM and PIAM platforms. We'll also engage in dialogue with industry leaders about the future of unified identity governance, touching on AI in access and identity management, best practice in automated processes and cross-border compliance challenges. This is more than a product showcase, it's a commitment to thought leadership and co-innovation. As the security landscape continues to evolve, we believe in shaping the conversation, not just following it. ■