ISSUE 26: **JUNE 2025**

www.securitymattersmagazine.com

Security MATTERS

The Independent Voice for Security and Risk Professionals

LEAD MEDIA PARTNER THE SECURITY EVENT

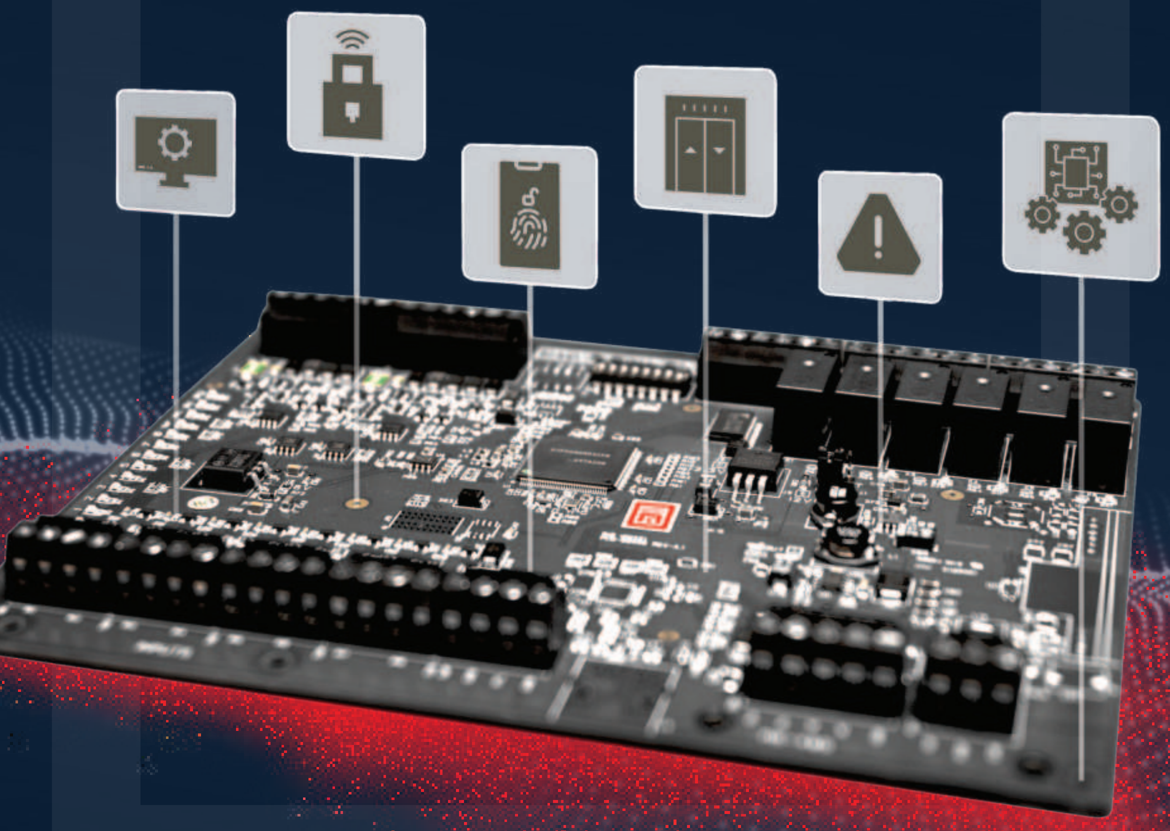
MEDIA PARTNER INTERNATIONAL SECURITY EXPO

Security MATTERS LIVE

CBS ARENA » COVENTRY » 5 JUNE 2025

SHOW PREVIEW

GET ON BOARD



Introducing the app environment that puts you in control.

Mercury™ part of HID

Set controls to neutral

Allan Dickinson explores what true vendor neutrality means within Physical Security Information Management and security software ecosystems, why it matters, the major benefits to be realised and also the key trends driving its adoption

PHYSICAL SECURITY Information Management (PSIM) platforms and broader physical security software solutions seem to offer a sense of being open, while in reality being closed and fragmented, only offering the full feature set when the product is bound to specific hardware vendors or other products they manufacture. However, the industry is undergoing a paradigm shift towards true vendor neutrality.

Vendor neutrality in PSIM and physical security software refers to a platform's ability to interoperate seamlessly with a wide variety of hardware and software systems, regardless of brand or manufacturer.

True vendor neutrality goes beyond supporting limited third party integrations. It means that a platform is hardware-agnostic (it can work with cameras, sensors, access control, alarms and many other devices from different vendors), open architecture-based (it supports open protocols plus inward and outward-bound APIs for integration without paid licensing), free from lock-in (users can switch, add or remove components and retain features without being tied to a single vendor's ecosystem) and scalable (new devices can be integrated with minimal effort and cost).

True vendor neutrality allows organisations to design Best-of-Breed solutions tailored to their specific needs. Whether choosing thermal cameras from Supplier A or video analytics from Supplier C, a neutral platform can tie them together. This 'mix-and-match' capability means better alignment with operational objectives, interoperability between the organisational sub-systems, the cost-effective use of existing infrastructure and, importantly, the rapid adoption of new innovations.

Reduced costs

Although upfront integration might seem complex, vendor-neutral platforms can reduce long-term costs by avoiding rip-and-replace upgrades, allowing gradual system evolution and reducing reliance on proprietary hardware. What's more, maintenance and support can be streamlined when components may be sourced competitively.

Technology evolves at a rapid pace. A vendor-neutral system is better positioned to adopt expansion in scope of the security landscape, new types of sensors or edge devices, emerging Artificial Intelligence (AI)-driven analytics and enhanced cyber security frameworks. Given that integration isn't bound to a single roadmap, organisations can pivot as their needs change.

As organisations grow (whether across facilities, regions or countries), a neutral platform ensures that expansion doesn't require standardising on one brand. It supports localised customisation and centralised management.

Vendor diversity within a platform can create redundancy in case of supply chain disruptions or any vendor failures. It can also serve to improve system uptime and fault tolerance.

An open ecosystem encourages innovation. Developers can build custom apps, dashboards or automations using published APIs in multiple languages. Integrators can also deliver higher-value solutions for unrivalled flexibility.

Key elements

Platforms should have the ability to use widely accepted protocols including ONVIF for video devices, PLAI for access control, BACNET, Modbus and OPC, etc. Alongside these, an open RESTful API for interoperability and allowing third party integrations, while minimising vendor-specific dependencies and opening the door to be fully agnostic.

Accessible APIs allow third party developers and integrators to create custom extensions, apps or services. SDKs can help to facilitate rapid development and integration.

A robust vendor-neutral platform often supports a marketplace or large library of certified plugins and device drivers. This enables the easy addition of new components without rewriting code or altering core systems.

The platform must normalise data from disparate sources, allowing for unified dashboards, event correlation and centralised analytics regardless of data origin. True vendor neutrality also includes governance features. It should support role-based access control, data privacy frameworks and region-specific compliance (all abstracted from the hardware layer).

Emerging trends

Cloud-based PSIM and physical security platforms increasingly support multi-vendor device connections. Hybrid models allow on-premises control while leveraging cloud scalability, further promoting vendor-neutral deployments.

AI-powered analytics are often embedded in edge devices from various manufacturers. Vendor-neutral platforms allow organisations to leverage these decentralised tools, while still feeding data into centralised solutions and populating dashboards for overviews.

With cyber threats targeting physical systems, organisations demand platforms that support end-to-end encryption alongside third party security tools (eg SIEM integration and endpoint protection). Secured by Design policy is another driver of vendor neutrality that's important. This ensures that all software is developed to a high security standard.

Modern software design is shifting towards microservices, thereby making it easier to deploy, scale and update individual features independently. This architecture favours vendor-neutral deployments due to the fact that each service can interact through open APIs.

Several Government-level standards such as CAPSS via the National Protective Security Authority are now encouraged or mandated for interoperability, and notably so in relation to critical sectors. Vendor-neutral solutions are better equipped to meet these evolving requirements.

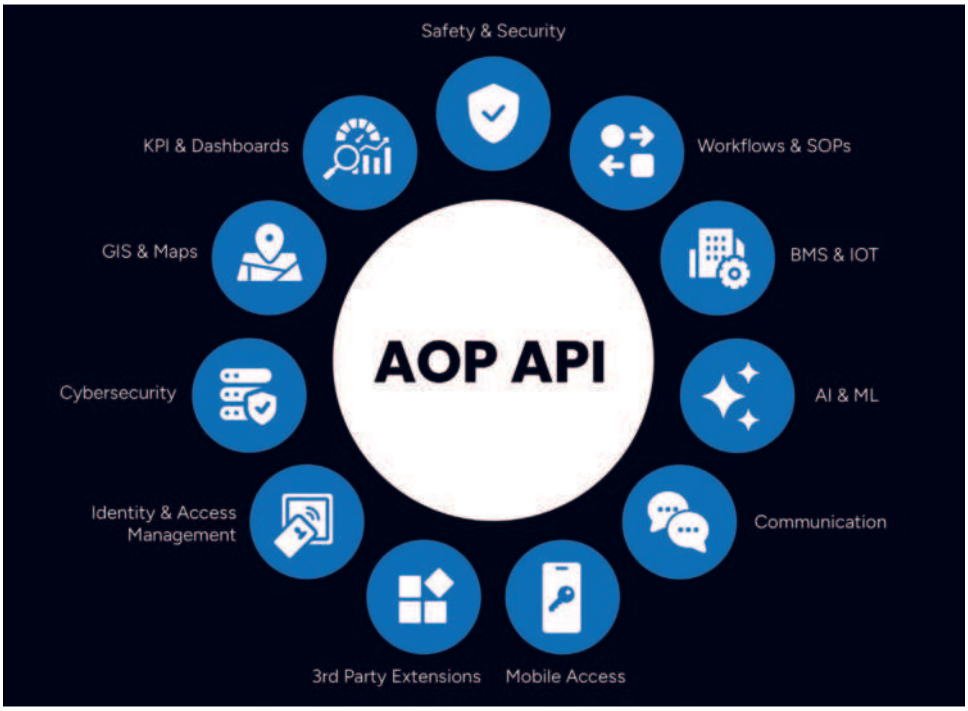
Convergence agenda

For many years, we've been discussing the ever-converging world of PSIM and cyber security, in particular with a focus on how this is re-shaping the security landscape. Recently, it seems that a new convergence theme has emerged.

A growing trend in enterprise security is the convergence of PSIM, cyber security and Physical Identity and Access Management (PIAM). As businesses face increasingly complex threats across both the physical and digital domains, integrating these systems provides a unified approach to risk management.

PIAM plays a critical role in this convergence by managing the full identity lifecycle and ensuring that access, both physical and digital, is granted based on role, context and policy.

With PIAM integrated in PSIM and cyber security platforms, organisations can enforce identity-driven security protocols across all access points. For example, if an employee is dismissed or has a changed role, PIAM ensures immediate withdrawal or modification of both building access and system credentials. This reduces the risk of unauthorised entry or data breaches.



Such convergence enhances real-time situational awareness by correlating identity-based events with physical and cyber activity. It also automates compliance reporting and access governance to improve audit readiness.

Ultimately, the integration of PIAM with broader security ecosystems supports 'Zero Trust' models whereby access is continuously verified and never assumed. This shift creates a more adaptive, proactive and efficient security posture, helping organisations to better protect their assets, data and people in an increasingly hybrid threat landscape.

While vendor neutrality offers flexibility, it can come with integration challenges alongside high costs, notably so when legacy systems use proprietary protocols. Selecting a product/business that allows the organisation to avoid these costs and lengthy integration timescales, while also providing open APIs, is critical. A strong professional services team or experienced integrator is also key in achieving the desired outcome.

Some vendors may resist openness to protect market share. Organisations must negotiate and prioritise platforms that commit to open standards and long-term support to ensure simplicity within their control environments.

When issues do arise, it can be difficult to determine whether the problem resides with the platform or a specific device. Clear Service Level Agreements, IT-focused integrators and centralised monitoring help to mitigate this issue.

The trajectory is clear: vendor neutrality is no longer a 'nice to have'. It's a strategic imperative. Tomorrow's PSIM and security platforms will likely resemble operating systems more than traditional surveillance tools managing a vast ecosystem of apps, devices and services. Those built on vendor-neutral principles will offer unmatched adaptability and resilience.

End users, integrators and consultants should prioritise those platforms with transparent architecture, robust API documentation and a demonstrated track record of third party integrations. By doing so, they not only protect current investments, but also position themselves to innovate faster and smarter.

It seems that convergence will be the order of the day, witnessing Control Rooms adapt and change to the ever-increasing requirements from organisations that could shape the security landscape for the next decade.

True vendor neutrality

True vendor neutrality in PSIM and physical security software solutions represents a shift in power away from closed ecosystems towards open and interoperable environments. It empowers organisations to build systems that reflect their goals and innovation timelines.

As the security landscape becomes more dynamic and technology-centric, only those platforms that embrace open standards and support diverse integrations will stand the test of time.

Allan Dickinson is Director of Advancis Software & Services UK
www.advancis.net