22 people were killed in the 2017 Manchester Arena attack

BEYOND COMPLIANCE

Ardon Anderson *reveals how integrated security systems will define Martyn's Law readiness*

When Martyn's Law takes full effect across the UK in 2027 it will mark one of the most significant overhauls of public venue security in decades. The goal is clear: prevent another tragedy like the Manchester Arena bombing that killed 22 people in 2017. The law mandates that every public venue – from stadiums to theatres to shopping centres – must have formal plans for risk assessment, emergency response, and staff training.

But beyond just plans and training, effectively preparing for Martyn's Law means ensuring staff have technology that actually supports them – systems that are intuitive, integrated and robust enough to guide proactive security and fast decision-making in an emergency.

Martyn's Law – officially the Terrorism (Protection of Premises) Act 2025 – passed Royal Assent in April and represents a fundamental shift in how UK businesses approach venue security. For the first time, security preparedness for terrorist threats becomes mandatory rather than voluntary. Venues with capacity over 800 people must conduct risk assessments, develop detailed emergency response plans, train staff and appoint senior compliance officers. Those between 200-799 face lighter requirements, but still must implement evacuation procedures and staff training. The law is named after one of 22 people killed in the 2017 Manchester Arena bombing – a stark reminder that music venues, stadiums, shopping centres and conference halls face genuine security risks.

According to the government's own impact assessment, security guidance has been voluntary since the early 2000s. A 2019 independent review found that venues consistently deprioritised this guidance compared to actual regulatory requirements, and the result was inconsistent security standards across the UK.

At the same time, the threats facing these venues have fundamentally changed. MI5 Director General Ken McCallum noted in 2022 that self-initiated terrorists: "often don't reveal their plans to anyone and can move quickly and sometimes spontaneously from intent to violence". When attackers operate independently with minimal planning, traditional intelligence-gathering becomes exponentially harder. This reality makes Martyn's Law even more critical: the practical burden of prevention now falls partially to the venues themselves.

Martyn's Law is an opportunity for venues to fundamentally rethink how security infrastructure operates. Cloud-based and hybrid platforms that centralise management and integrate disparate systems are easy to train, use and maintain. This ease of use matters enormously under Martyn's Law, where training is a major requirement and many venues rely on rotating or temporary staff. For-hire workers need tools they can pick up quickly – not systems that require days of onboarding. Centralised platforms that operate from a single, intuitive interface mean staff can become proficient in under an hour, rather than spending weeks learning multiple legacy systems.

When cameras, access control, sensors and alarms operate on a unified platform, operators manage one system instead of many. A single dashboard replaces multiple monitoring stations and updates deploy automatically across hundreds of devices. These improvements are the difference between a security system that becomes more capable at scale and one that becomes more chaotic.

Centralisation also solves the visibility problem. In fragmented systems, operators must manually correlate information from multiple sources to understand what's happening. For instance, without seeing associated camera footage instantly when someone triggers an access denial at a door, operators can lose critical seconds pulling up separate systems to investigate.

Integration eliminates this friction. When access control and video management operate on the same platform, an access denial automatically surfaces the relevant camera feed. Operators see context immediately: the person is holding the wrong credential, appears to be tailgating or matches a person of interest flagged earlier. Response becomes faster because the system eliminates the manual steps that slow operators down.

Beyond central integration, modern security platforms can detect specific behaviours without streaming every second of footage to a central server for processing. This 'edge' intelligence fundamentally changes what's possible for venue safety.

With an AI-powered camera, security teams can set up analytics and alerts to count people, identify crowd density patterns, detect loitering, flag unattended objects, or recognise when someone enters a restricted area. The camera does this processing locally and alerts operators when those anomalous conditions occur. This enables even small, lean teams to ensure that they never miss a critical moment when they are busy juggling an expansive set of priorities.

This approach directly addresses Martyn's Law requirements around risk assessment and emergency response. Understanding crowd flow patterns helps identify bottlenecks that could impede evacuation. Recognising abnormal behaviours in real-time supports faster threat detection. Automatic alerts ensure the right people know about developing situations immediately rather than discovering them during post-incident review. The shift from reactive to proactive security changes how the entire security system works. Instead of just recording what happened, modern systems can spot patterns, flag unusual activity, and send alerts in real-time – giving security teams a chance to step in before situations escalate.

Proactive security is only one piece of the puzzle. Martyn's Law also requires organisations to conduct ongoing risk assessments, review procedures and demonstrate continuous improvement. This means learning from near-misses, identifying patterns in security incidents and refining response protocols based on evidence.

This forensic analysis has been difficult in the past. Finding specific footage requires knowing exactly when and where an incident occurred, then manually reviewing hours of video. Security teams can spend days or even weeks reconstructing events.

TERRORISTS OFTEN DON'T REVEAL THEIR PLANS AND CAN QUICKLY MOVE FROM INTENT TO VIOLENCE

Modern platforms with searchable video and natural language queries transform this process. An operator can search: "person in red jacket near Gate 7 between 2-3pm" and surface relevant footage in seconds. They can track an individual's movement across multiple cameras to understand how a situation developed. AI-enabled cameras can also collate valuable insights and analytics, including heatmaps to show movement and high-traffic areas throughout a venue, as well as people counting tools to measure occupancy.

Meeting the requirements of Martyn's Law requires infrastructure that provides genuine operational capability rather than checkbox compliance. Risk assessment requires understanding traffic patterns, identifying vulnerable areas and recognising how threats can materialise in your specific environment. Emergency planning requires knowing how quickly areas can be evacuated and which exits remain functional under various scenarios. Staff training requires practicing with actual tools and real-world scenarios. Compliance oversight requires demonstrating continuous improvement and evidence-based decision-making.

For example, when inspectors ask how a venue identified and mitigated a specific risk, answers shouldn't require weeks of manual investigation. Organisations need to demonstrate not just that they have security measures in place, but that they actively use security data to improve those measures. None of this happens with fragmented systems that create more work than insight. It happens when security infrastructure provides the visibility, integration and intelligence that turn security from a cost centre into an operational advantage.

Given these operational demands, the temptation for many businesses will be to treat Martyn's Law as a 2027 problem and continue operating with existing systems until the deadline forces action. However, this approach fails because building effective security requires time to understand

Picture credit: Tomaz Kozlowski

new technology, implement it properly, train staff and refine procedures.

Organisations that defer investment could put themselves in a position where they are scrambling to achieve compliance through rapid deployment of disconnected solutions that create more complexity than capability. They'll add cameras that nobody has time to monitor, implement procedures that staff haven't practiced and generate documentation that doesn't reflect operational reality.

MARTYN'S LAW NOW MEANS THE BURDEN OF PREVENTION FALLS PARTIALLY ON VENUES

The alternative is treating the compliance deadline as a forcing function to build infrastructure that venues should have regardless of regulatory requirements. Security systems that scale effectively, integrate comprehensively and provide real-time operational intelligence aren't just compliance tools. They're what serious protection of large public spaces requires in an era when threats are less predictable and attacks can materialise rapidly.

Martyn's Law makes that burden explicit and mandatory. The question isn't whether venues will comply, but whether they'll comply effectively or merely adequately and build infrastructure that genuinely protects the thousands of people moving through their spaces or infrastructure that satisfies inspectors while leaving actual vulnerabilities unaddressed.

The challenge ahead will be to ensure building systems work in concert. The venues that embody Martyn's Law won't just expand their existing infrastructure, they'll use intelligent tools that detect threats, connect operations and enable swift, coordinated responses ●

MARTYN'S LAW EXPLAINED

Formally known as Martyn's Law, the Protect Duty is proposed UK legislation designed to improve public safety and security at publicly accessible locations. The law is named after Martyn Hett, one of the 22 victims of the 2017 Manchester Arena terrorist attack, and reflects the campaigning efforts of his mother, Figen Murray. Its central aim is to ensure that organisations responsible for public venues take proportionate and preventative steps to protect people from terrorism.

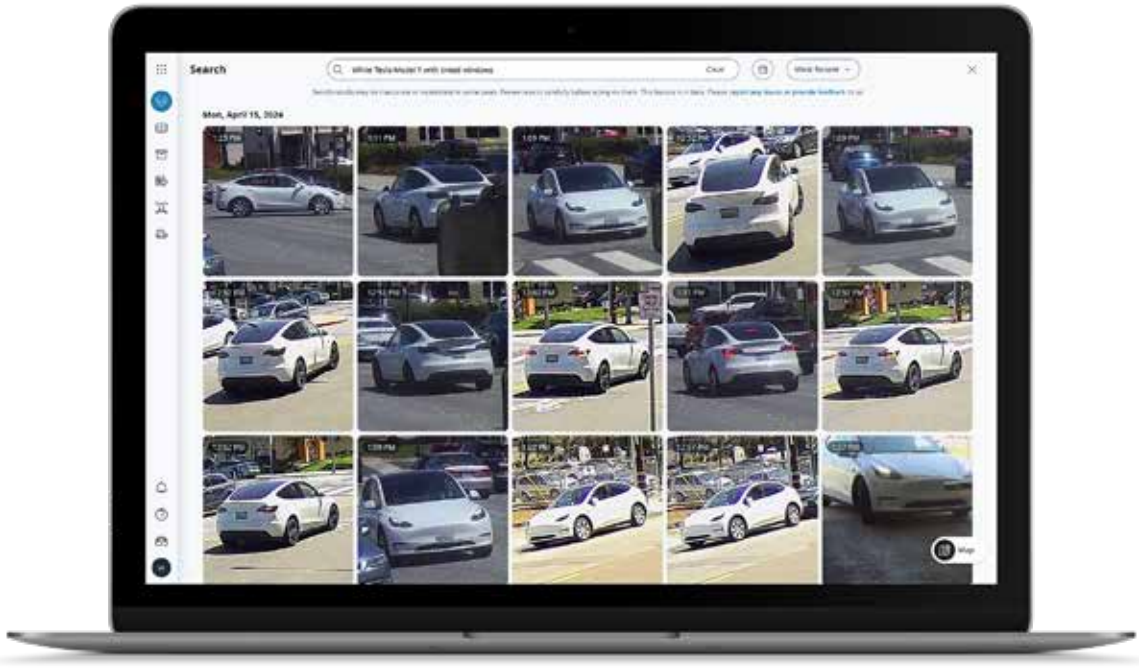
Martyn's Law introduces a legal duty on those who own or operate qualifying premises and events to consider the risk of terrorist attacks and implement appropriate mitigation measures. The duty is intended to be proportionate, meaning requirements vary depending on the size, capacity and nature of the venue or event. Smaller premises will face simpler obligations, while larger or higher-risk locations will be expected to adopt more robust security arrangements.

Key elements of the proposed law include risk assessment, staff training and preparedness planning. Responsible persons will be required to assess potential terrorist threats, put in place reasonable protective measures and ensure staff are trained to recognise and respond to incidents. This may include awareness of suspicious behaviour, clear evacuation procedures and effective communication during emergencies. Importantly, the law focuses on preparedness rather than imposing excessive physical security measures on all venues.

Oversight and enforcement will be carried out by a regulator, with an emphasis on support and guidance rather than punishment, particularly during initial implementation. Sanctions will be available for serious or persistent non-compliance, but the overarching objective is cultural change rather than enforcement alone. The law is due to come into force in 2027.

Ardon Anderson is the Vice President for EMEA at Verkada, a leader in AI-powered physical security technology.

Instead of just recording what happens, modern systems can spot patterns, flag unusual activity and send alerts in real-time



Picture credit: Verkada