Shooter Detection Systems™

AN ALARM.COM COMPANY

A SPECIAL REPORT

The State of Active Shooter Security at U.S. Sports & Entertainment Venues

Published by Shooter Detection Systems | November 2026



trust their venue to protect them against an active shooter.

The data reveals important gaps remain.

Contents

The State of Active Shooter Security at U.S. Sports & Entertainment Venues

Executive Summary

01 The Evolving Threat Landscape

02 The Preparedness Gap — Fear vs. Readiness

The Business Case for Preparedness — What a Security Incident Really Costs

03 The Outdoor and Perimeter Problem

04 The Response Time Problem

05 The Staffing Crisis as a Force Multiplier for Risk

06 The Security Technology Stack — What's in Place and What's Missing

The SAFETY Act Framework — What It Is and Why It Matters

07 What Best-in-Class Looks Like

08 Recommendations for Venue Security Leaders

The Path Forward

Methodology and Sources

About Shooter Detection Systems

Executive Summary

Every game, concert and live event begins with the same expectation: that the organization hosting it has invested in the people, processes and technology needed to keep attendees safe.

According to the NCS4's 2025 Spectator Safety and Security Survey, approximately 80% trust their venue to have measures in place to protect them against an active shooter.[7] But the data reveals a significant gap between what fans expect and how prepared venues are to respond. Drawing on primary FBI data, peer-reviewed academic research, and IRB-approved survey data from venue security directors and fans across MLB, MLS, NBA, NFL, and NHL, this report evaluates the current state of active shooter preparedness across sports and entertainment venues.

The findings reveal that while the industry has made substantial progress, important gaps remain. Those gaps are measurable, increasingly consequential, and, importantly, within the control of venue leaders to address.

The Threat Landscape Has Changed

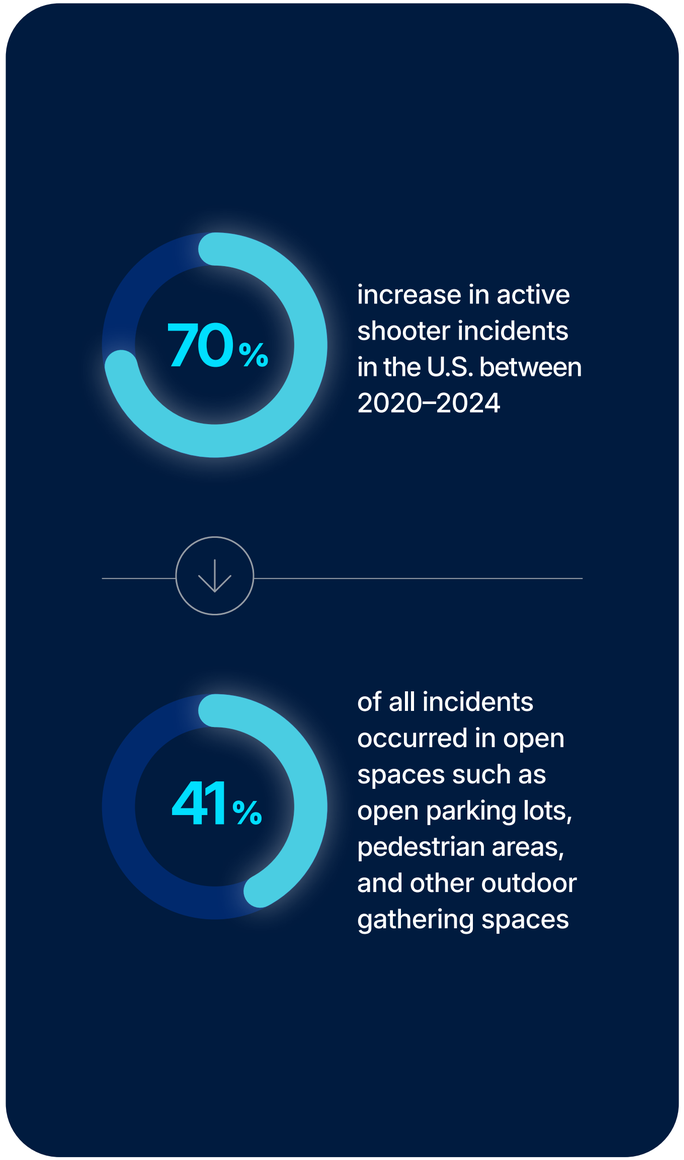
Between 2020 and 2024 the FBI identified 223 active shooter incidents in the United States, a 70% increase over the previous five-year period. Those incidents resulted in 1,070 casualties, an average of 4.8 casualties per incident, while 48 met the federal definition of a mass killing. Open spaces represented the largest location category, accounting for 41% of all incidents. The FBI's definition of open space explicitly includes open parking lots, pedestrian areas, and other outdoor gathering spaces — the same environments where spectators congregate before games, concerts and other live events.[3]

The Preparedness Gap

The data reveals a consistent and consequential pattern across multiple dimensions of venue security.

ON TECHNOLOGY

Security technology adoption varies considerably depending on the function it serves. Communication, surveillance, and access control technologies are nearly universal among surveyed venues. Two-way radios and surveillance cameras are deployed at 96% of venues, while walk-through magnetometers are used at 94%. By comparison, advanced gunshot detection systems,



which provide automated confirmation of a live fire event, are deployed at 13% of venues, despite 30% of security directors identifying them as a priority investment if additional funding were available.[6,9]

ON THE OUTDOOR ENVIRONMENT

Approximately 50% of fans tailgate before events[8], and 76% arrive within 30 minutes of game time.[7] Together, these patterns create predictable periods of high crowd concentration in parking lots, tailgate areas, and other open spaces surrounding venues.

ON STAFFING

65% of venue security directors reported experiencing staff shortages within the last two years, while 74% use contracted security staff in some capacity on game days.[17] Among contracted staff, active shooter response ranks last among reported training priorities, despite the risk.[6]

ON RESPONSE

Many active shooter incidents conclude within minutes, often before law enforcement arrives.[5] In that compressed response window, relying solely on human observation to identify and report suspected gunfire can delay the flow of critical information to security personnel and first responders.

PROFESSIONAL VS COLLEGIATE

The 2026 NCS4 Venue Security Director Survey — the first to include both professional and collegiate venues — reveals a consistent and significant security gap between the two segments across nearly every dimension: table-top exercises (95% professional vs. lower collegiate rates), AI adoption, SAFETY Act certification (64% professional vs. 50% collegiate), staff screening practices, and use of industry research to inform security policy (95% professional vs. 71% collegiate).[17]

The Business and Legal Dimension

The preparedness gap extends beyond immediate safety concerns to potential legal, financial, and reputational risks. Venue operators have a legal duty of care to attendees, and security practices designed around past threats may not keep pace with the threats that exist today. The DHS SAFETY Act framework provides certain liability protections for venues and technologies that have pursued certification, with three levels of status that offer different protections. 64% of professional sports venues have obtained or are in the process of obtaining SAFETY Act Certification for their security programs.[17] The technologies they deploy within those programs should meet the same standard.

What Best-in-Class Looks Like

A best-in-class approach to venue security uses a layered security model that extends detection capability beyond the entry point and integrates that detection with automated response. Walk-through magnetometers remain the primary weapons detection tool at venue entrances, screening attendees as they enter the facility. A layered approach extends that coverage to the environments magnetometers cannot reach: the parking lots, tailgate areas, and pedestrian plazas where crowds gather before passing through entry screening, and the concourses, seating bowls, and back-of-house spaces inside the venue where a threat may originate after entry. Integration with video management, access control, and mass notification systems activates automatically at the moment of detection. When those layers work together, the response chain compresses from minutes to seconds, with verified location data reaching security personnel and first responders simultaneously, without depending on a human observer to initiate it.

The Path Forward

Professional sports venues are among the most visible, most attended, and most trusted public gathering spaces in American life. The fans who fill them deserve a security posture that matches that trust. The data, frameworks, and technologies needed to strengthen preparedness already exist. The challenge now is putting them into practice.

This report concludes with seven actionable recommendations to help venue security leaders identify vulnerabilities, strengthen preparedness, and close the gap between threat and response.

01 The Evolving Threat Landscape

Key Takeaways

The FBI designated 223 active shooter incidents from 2020 to 2024, **a 70% increase from the prior five-year period**.[3] In 2025, incidents rebounded 42% from 2024's historic low, confirming the long-term upward trajectory.[4]

Open space, including parking lots and outdoor gathering areas, was the single largest active shooter location category over the five-year period, accounting for **41% of all incidents**.[3]

Active shooter situations are tied with fan behavior as the top concern among venue security directors, alongside vehicle ramming, IEDs, and unauthorized drones.[6]

The threat does not stop at the turnstile. High-profile incidents at Guaranteed Rate Field and Nationals Park both **originated at or beyond the venue's security perimeter.**

The security landscape facing sports and entertainment venues has fundamentally changed. For decades, venue security focused primarily on fan behavior, alcohol management, crowd control, and emergency medical response. Those responsibilities remain essential, but they now exist alongside another challenge: the sustained rise of active shooter incidents across American public life. The FBI defines an active shooter incident as one or more individuals actively engaged in killing or attempting to kill people in a populated area. As active shooter incidents have increased, so too has the recognition that sports and entertainment venues share many of the same characteristics as the locations where these attacks occur. Large crowds, predictable gathering patterns and expansive outdoor spaces have become defining features of both the live event experience and the modern threat landscape.

The data underscores how the threat has evolved. Between 2020 and 2024, the FBI identified 223 active shooter incidents in the United States — a 70% increase over the previous five-year period. Those incidents resulted in 1,070 casualties, including 369 fatalities and 701 injuries. The risk remains high. In 2025, the FBI identified 34 active shooter incidents, a 42% increase over 2024, reinforcing that short-term fluctuations have not altered the long-term trajectory.[4] A broader measure reinforces the risk: according to the Gun Violence Archive, there were 407 mass shootings in the U.S. in 2025, defined as an incident in which a minimum of four victims are shot (injured or killed), not including the shooter, in a single event at the same general time and location.[11]

These incidents are not confined to isolated or remote locations. They are happening in the places where Americans gather: in commercial areas, in open public spaces, in parking lots and parks and outdoor gathering areas. Over the five-year period, open space was the single largest active shooter location category, accounting for 92 incidents, or 41% of the total. Commerce locations accounted for another 88 incidents, or 39%. Open space and commerce environments accounted for a combined 81% of all active shooter incidents from 2020 to 2024, two categories that together describe the environment surrounding every major sports venue in the country on game day.[3]

The FBI's definition of open space is precise and worth noting. It includes incidents that take place "primarily in an open-air location rather than beginning or ending inside a building," with named examples that include "open parking lots" and "public streets."[1] That definition maps directly onto the pre-game and post-game environment at every professional sports venue in the United States, and that is where the security posture at most venues is most likely to be tested.

The Threat Does Not Stop at the Turnstile

Several high-profile incidents have reinforced an important lesson for venue security professionals: the threat does not stop at the turnstile.

In July 2021, a shootout between two vehicles outside Nationals Park in Washington, D.C. forced the suspension of a live game and sent fans scrambling for cover.[13] The incident caused immediate and significant crowd panic throughout the stadium, despite the fact that no one inside was harmed.

In August 2023, two women were struck by gunfire during a game at Guaranteed Rate Field in Chicago. Investigators were initially unable to determine whether the shots originated either from within the stands or from outside the venue, and the game was suspended while law enforcement responded.[14]

The threat environment has also expanded beyond the immediate venue footprint. The 2015 Stade de France bombings, the 2017 Manchester Arena attack[15], and the 2017 Las Vegas Route 91 Harvest festival massacre, in which a shooter firing from an elevated position into an open-air crowd killed 60 people and wounded more than 400, each demonstrated a clear and consequential shift.[16] Threats do not stop at the property line. The areas of greatest vulnerability are often the areas least covered by traditional security infrastructure.

What Venue Security Directors Are Telling Us

The FBI data reflects a national trend. Survey findings from the professionals responsible for protecting sports venues show how those trends are being experienced on the ground.

In a 2025 peer-reviewed study of venue security directors across MLB, MLS, NBA, NFL, and NHL, active shooter situations were cited among the top concerns by 65% of respondents, tied with fan behavior as the single most frequently named threat.[6] The broader list of concerns — including alcohol abuse, weapons, vehicle ramming, vehicle-borne improvised explosive devices (VBIEDs), improvised explosive devices (IEDs), and unauthorized drones — reflects how significantly the venue security landscape has evolved.[9] Security leaders today are balancing many of the traditional operational challenges of managing large crowds while preparing for an increasingly diverse range of emerging threats.

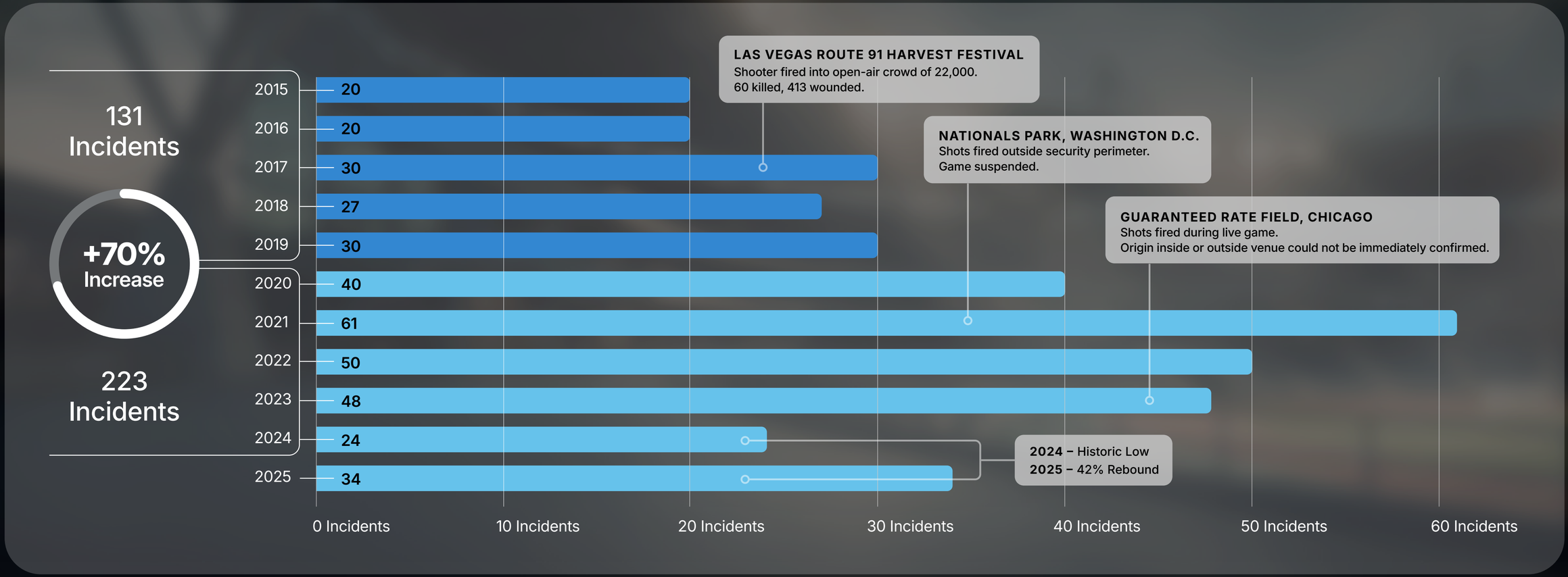
The research also found that 88% of venue security directors reported that fan behavior is about the same or worse than it was three years ago, while 61% of venues detected unauthorized drones on event days.[17]

Collectively, the findings suggest that venue security is no longer defined by any single threat. Instead, security leaders are managing an increasingly diverse risk environment that requires a layered and adaptable approach to preparedness.

In a 2025 peer-reviewed study of venue security directors across MLB, MLS, NBA, NFL, and NHL, active shooter situations were cited among the top concerns by 65% of respondents, tied with fan behavior as the single most frequently named threat.

Active Shooter Incidents in the United States, 2015–2025

FBI-Designated Incidents by Year

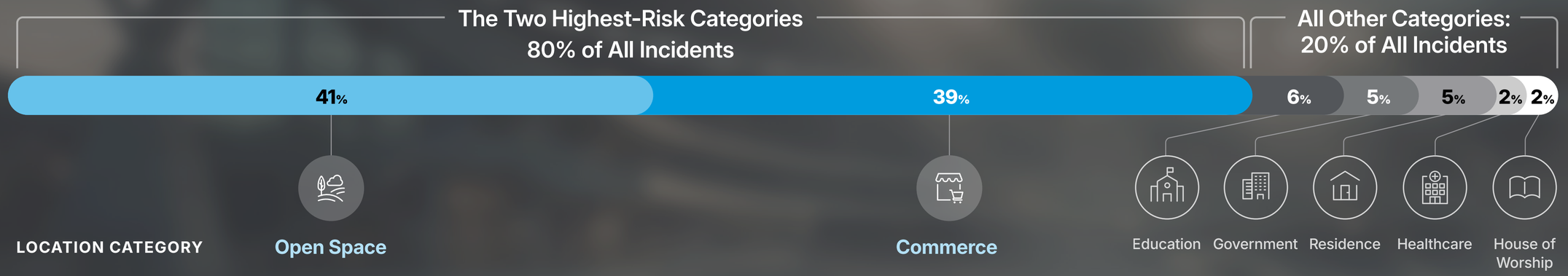


1,070 casualties across 223 incidents, 2020–2024. Average: 4.8 casualties per incident.

Source: FBI Active Shooter Incidents in the United States, 2022, 2023, 2024, and 2025; FBI and ALERRT Center at Texas State University

Where Active Shooter Incidents Occur: 2020–2024

FBI-Designated Incidents by Location Category, Five-Year Period



LOCATION CATEGORY	Open Space	Commerce	Education	Government	Residence	Healthcare	House of Worship
INCIDENTS – 223 TOTAL	92	88	13	11	11	4	4

The FBI's definition of open space explicitly includes open parking lots, public streets, and other outdoor gathering areas—environments that closely resemble the spaces surrounding sports and entertainment venues before and after events.

Open space and commerce are the only two location categories with active shooter incidents in every year of the five-year period from 2020 to 2024.

Source: FBI Active Shooter Incidents in the United States, 2024; FBI and ALERRT Center at Texas State University.

02 The Preparedness Gap — Fear vs. Readiness

Key Takeaways

96% of venues conduct annual tabletop exercises[6], reflecting strong planning commitment. But planning tools alone do not compress detection-to-response time when an incident occurs.

Gunshot detection systems, which provide the only automated confirmation of a live fire event, are **deployed at just 13% of venues**, despite 30% of security directors identifying them as a priority investment.[6,9]

80% of fans trust venues to protect them against active shooters.[7] Active shooter response policy ranks among the lowest in fan familiarity across all venue policies.

The security technology stack at most venues is wide but shallow: strong on access management and communication, **thin on automated threat detection after the entry point**.

The threat data is clear. The question is whether today's security programs are equipped to respond to it. The research reveals an important distinction between recognizing the threat and being prepared to respond. Venue security directors are clear-eyed about today's security environment and have made significant investments in planning, communications, and emergency preparedness. At the same time, the findings suggest that awareness alone does not always translate into operational readiness.

95% of professional venues conduct annual tabletop exercises[17], reflecting a strong commitment to emergency planning. At the same time, 30% of venue security directors identified gunshot detection systems as a priority investment if additional funding were available.[9]

Tabletop exercises play an important role in preparedness, but they are only one component of an effective response. Technology, staffing, communications, and clearly defined operational protocols all influence how quickly and effectively a venue can respond when an incident occurs.

What Fans Believe

Preparedness is not only an operational issue — it also shapes the spectator experience.

According to the NCS4's 2025 Spectator Safety and Security Survey, 74% consider safety and security precautions before deciding to attend a sporting event. Approximately 80% trust the venue to have measures in place to protect them against active shooters.[7] That confidence reflects a reasonable expectation that organizations hosting tens of thousands of people have invested in the people, processes, and technology needed to protect attendees.

The survey findings from venue security directors, however, suggest there are opportunities to further strengthen preparedness. While venues have made significant investments in security infrastructure, security leaders also identified areas where additional capabilities and resources could enhance active shooter preparedness.

The NCS4 data also surfaces something worth noting about how fans experience security at the venue level. Active shooter response policy ranked among the lowest in fan familiarity across all venue policies and procedures, with a mean familiarity score of 3.53 out of 5, lower than prohibited items policy, fan code of conduct, alcohol policy, emergency medical procedures, and drug policy.[8]

Fans trust venues to have a plan. What the data suggests is that clearer communication about the security measures that are visible — entry screening, camera coverage, and trained personnel — can reinforce that trust and make fans feel more confident in the environment they are entering.

Where the Investments Are Going

Understanding the preparedness gap requires looking at where venue security investments are being made. The most widely deployed technologies at professional sports venues are communication and access tools: two-way radios (96%), surveillance cameras (96%), walk-through magnetometers (94%), and access control and credentialing systems (94%).[6] These are foundational investments, and they reflect a security posture built primarily around access management and communication. They are the right tools for the threats venues have historically managed most frequently, such as fan behavior, unauthorized access, and crowd control.

What is largely absent from the current security technology stack is automated threat detection capability that functions after a weapon has passed the entry point. When venue directors were asked what they would purchase with additional funding, gunshot detection systems ranked fifth on the list at 30%, behind facial recognition, facial validation/authentication, retractable bollards, and video analytics.[9] That ranking is not evidence of indifference to the active shooter threat. It reflects a budget environment in which the most visible and politically legible technologies tend to win the allocation conversation.

The result is a security stack that is wide but shallow: many tools, few integrations, and significant gaps in the highest-stakes scenarios.

The AI Uncertainty Factor

One finding from the venue director research deserves specific attention because it points to a structural challenge that will shape security investment decisions for the next several years. Only 31% of venue security directors are currently using AI in any security application, and 51% say they are uncertain how AI could assist their operations.[6]

That uncertainty reflects a broader challenge facing the industry. The AI security technology landscape has evolved rapidly, making it increasingly difficult for venue operators to evaluate emerging capabilities, distinguish between different categories of technology, and determine which solutions best align with their operational needs.

One area where this distinction is particularly important is gunshot detection. AI-based video analytics, which attempt to identify visible firearms using camera footage before a weapon is discharged, serve a fundamentally different purpose than acoustic and infrared gunshot detection systems, which are designed to detect and confirm a live gunshot event. While both technologies may play a role within a layered security strategy, they address different operational challenges and should be evaluated independently.

As AI continues to mature, venue security leaders will face increasing pressure to separate marketing claims from operational performance, making investment decisions based on demonstrated capabilities, operational requirements, and integration with their broader security strategy.

What is largely absent from the current security technology stack is automated threat detection capability that functions after a weapon has passed the entry point.

02B The Business Case for Preparedness — What a Security Incident Really Costs

Key Takeaways

The costs of a security incident extend well beyond the immediate response: legal liability, reputational damage, lost revenue, insurance consequences, and long-term erosion of public confidence.

Venue operators have a legal duty of care to attendees. **A security posture built around historical threats may not be adequate** when an incident originates in the parking lot or after the screening window closes.

Nearly three-quarters of fans consider safety and security precautions before deciding to attend an event.[7] **Fan trust is directly connected to revenue.**

Formal cost-benefit analysis of security investments is not yet common practice in the industry. Organizations that make the business case explicitly are **better positioned to act before an incident forces the decision.**

Preparedness is often evaluated through the lens of cost. The challenge is that the costs of preparedness are immediate and measurable, while the costs of an incident are uncertain — until they become real. For venue security leaders, every investment competes with a wide range of operational priorities. New technologies, staffing, training, maintenance, and capital improvements all require finite resources, making security investment decisions an exercise in balancing competing risks.

The financial impact of a security incident, however, extends well beyond the immediate response. Legal liability, operational disruption, reputational damage, lost event revenue, increased insurance costs, and long-term impacts on public confidence can continue long after the incident itself has ended.

Unlike security investments, these costs rarely appear in a budget or business case before an incident occurs. As a result, organizations are often asked to evaluate preparedness against costs that are tangible today rather than risks whose financial consequences may not be realized until much later.

Legal Exposure and Duty of Care

The legal implications of venue security in the United States extend beyond emergency response and into an organization's broader duty of care. Venue operators are expected to take reasonable steps to protect attendees, and what is considered reasonable continues to shift with evolving industry standards of preparedness. Aligning with best practices for detecting, communicating, and responding to threats is increasingly viewed as a core part of that responsibility. The consequences of a security failure extend beyond physical injury to include reputational and financial harm.

Research published in the Global Sport Business Journal describes the current approach to venue security as primarily "property-centered and liability-limiting," focused on avoiding negligence claims rather than on patron safety as an affirmative goal.[9]

As the threat landscape evolves, security strategies must evolve with it. A security program designed around historical risks may not fully address the threats venues face today. Evolving industry standards of preparedness increasingly look beyond entry-gate screening, such as walk-through magnetometers. Best practices point to layered capabilities that can detect and respond to threats originating outside the screening perimeter or emerging after the screening window has closed.

For sports and entertainment venues, that includes considering not only security at points of entry, but also how threats occurring in parking lots, pedestrian plazas, tailgate areas, and other public gathering spaces are detected, communicated, and managed.

One framework designed to support both preparedness and risk management is the U.S. Department of Homeland Security's SAFETY Act. Venues that have pursued SAFETY Act Certification, and that deploy SAFETY Act-certified technologies, have a documented legal protection that uncertified venues do not. That distinction has direct implications for civil litigation outcomes, and the SAFETY Act framework is covered in detail later in this report.

Reputational Damage and Attendance Impact

Security incidents can have consequences that extend well beyond the immediate response. As established earlier in this report, nearly three-quarters (74%) of fans consider safety and security precautions before deciding to attend a sporting event.[7] That figure suggests a link between a venue's security posture and its revenue. When a high-profile security incident occurs, the impact is rarely limited to the day of the event. Public attention often extends beyond the incident itself to include how the venue responded, how information was communicated, and whether attendees felt protected throughout the event.

The reputational consequences extend beyond individual fans. Sponsorship relationships, broadcast partnerships, and league standing are all downstream of public confidence in venue safety. Research conducted through the Department of Homeland Security's Best Practices in Anti-Terrorism Security (BPATS) program found that many venue operators view security investments as an important component of brand protection and long-term business resilience.[12] For these organizations, preparedness is not solely a security consideration — it is also a business decision intended to protect public confidence and support the long-term success of the venue.

One of the challenges, however, is that the benefits of preparedness are difficult to quantify before an incident occurs, while the costs of security investments are immediate and visible. That dynamic can make it difficult to evaluate investments whose greatest value lies in preventing or mitigating events that may never happen.

Insurance Considerations

A venue's security posture can be a factor in how insurers evaluate risk and set premiums for event liability coverage. Venues that can demonstrate a documented, layered security program, including certified technologies and formal preparedness protocols, may be viewed more favorably by underwriters than those that cannot. The inverse is also true. An incident that reveals gaps in detection or response capability can affect coverage terms, premium levels, and in some cases insurability for future events.

The Department of Homeland Security's SAFETY Act also plays an important role in this broader risk management framework. Established to encourage the adoption of qualified anti-terrorism technologies, the program provides liability protections for organizations that deploy designated or certified technologies as part of their security programs.

For venue operators, the SAFETY Act can complement a broader security strategy by recognizing technologies and security programs that have undergone federal review. Beyond the legal protections it offers, the framework provides an additional benchmark that organizations may consider as part of their overall approach to preparedness, risk management, and resilience.

The reputational consequences extend beyond individual fans. Sponsorship relationships, broadcast partnerships, and league standing are all downstream of public confidence in venue safety.

Event Disruption and Operational Costs

The operational impact of a security incident extends well beyond the immediate threat itself. The Nationals Park incident in July 2021 resulted in game suspension, mass fan evacuation, and significant crowd panic, all without a single person inside the stadium being struck.[13] The disruption to that event, and the operational response it required, represented a real cost to the organization independent of any legal or reputational consequence.

Evacuation and lockdown procedures at a venue hosting 40,000 to 80,000 people are not simple or inexpensive to execute. They require coordination across security, operations, law enforcement, and communications teams under conditions of maximum stress and minimum information.

Venues that have invested in automated detection and integrated response systems are better positioned to manage that coordination effectively. Venues that have not are managing it manually, in real time, with incomplete intelligence.

The Business Case for Proactive Investment

Research from the Department of Homeland Security's BPATS program suggests that formal cost-benefit analyses of security initiatives are not yet common practice across the sports and entertainment venue industry.[12] Many venue operators describe the value of security investments in qualitative terms, while the financial consequences of avoided incidents remain difficult to quantify.

This creates a challenge for decision makers. The costs of new technologies, staffing, and preparedness initiatives are immediate and measurable, while the benefits of preventing or mitigating a security incident are inherently harder to capture in traditional budgeting processes.

Organizations that take a broader view of preparedness often evaluate security investments across multiple dimensions, including legal liability, operational continuity, reputational resilience, insurance considerations, and public confidence. Looking at preparedness through this broader business lens can provide a more comprehensive understanding of both the costs of investment and the potential costs of inaction.

Organizations that take a broader view of preparedness often evaluate security investments across multiple dimensions, including legal liability, operational continuity, reputational resilience, insurance considerations, and public confidence.

03 The Outdoor and Perimeter Problem

Key Takeaways

Open space accounted for 41% of active shooter incidents from 2020 to 2024.[3] The FBI's definition of open space explicitly includes parking lots.

Approximately 50% of fans tailgate before events, and 76% arrive within 30 minutes of game time[7], creating predictable windows of high outdoor crowd concentration with minimal detection coverage.

Traditional security tools, magnetometers, cameras, access control, are designed for the interior environment. **None provide detection capability in the parking lot or tailgate area.**

Security at sports and entertainment venues has traditionally focused on protecting the venue itself. Walk-through magnetometers at entry gates, credentialed access points, and surveillance cameras covering concourses and concession areas are now standard infrastructure. The event experience, however, extends well beyond the venue entrance.

Long before spectators pass through security screening, they gather in parking lots, tailgate areas, pedestrian plazas, rideshare drop-off zones, and other outdoor spaces surrounding the venue. Those same areas remain heavily occupied after events as attendees return to vehicles, wait for transportation, or continue social activities.

The importance of these spaces is reinforced by where active shooter incidents are occurring. Between 2020 and 2024, the FBI identified open space as the single largest active shooter location category, accounting for 41% of all incidents.[3] That proportion increased to 58% in 2023[2] and remained high at 50% in 2024.[3] The FBI's definition of open space explicitly includes parking lots, public streets, and other outdoor gathering areas — locations that closely resemble the environments surrounding sports and entertainment venues before and after events.

These findings reinforce that venue security cannot begin and end at the entrance. As spectators spend a significant portion of their event experience in outdoor spaces, those environments have become an increasingly important part of comprehensive security planning.

The Outdoor Crowd Problem Is Structural

The challenges of securing outdoor environments are shaped not only by the physical layout of sports and entertainment venues, but also by how spectators use those spaces before and after events.

According to the NCS4's 2023 Spectator Safety and Security Survey, approximately 50% of sports fans engage in tailgating activities when attending an event.[8] The NCS4's 2025 survey found that 76% of fans enter the venue 30 minutes or less before start time, with 23% arriving at or after the start time.[7] That means the outdoor environment surrounding a major sports and entertainment venue is not just large and open; it is predictably, densely populated during a defined window before every event, and it clears out in a similarly compressed window after the final whistle.

The research also suggests there may be opportunities to better manage these crowd patterns. Nearly 65% of spectators said they would consider entering the venue earlier if incentives were offered[8], highlighting one potential strategy for reducing crowd concentrations outside the venue immediately before events.

Parking was cited as the top point of difficulty by 59% of spectators in the NCS4 2025 survey.[7] Fan violence outside the venue and tailgating incidents are among the most commonly witnessed or experienced incidents at sporting events, according to the NCS4 2023 survey.[8]

Together, these findings reinforce the importance of the outdoor environment within overall venue security planning. Because large crowds routinely gather in these spaces before and after events, parking lots, tailgate areas, and pedestrian approaches should be considered an integral part of the broader security environment rather than simply the areas surrounding it.

What Security Directors Are Saying

The professionals responsible for securing these environments recognize the unique challenges posed by outdoor spaces. In a 2025 peer-reviewed study of professional sport venue security directors, one director described the scenario directly: "An active shooter scenario in a professional sports facility parking lot would be difficult to deal with due to vehicles, open space, panicking fans, and reaction time from security."[9]

That assessment captures the operational reality with precision. Parking lots are not controlled environments. Vehicles create visual obstructions and unpredictable movement patterns. Crowd behavior in an open space under threat is fundamentally different from crowd behavior inside a building, where exits are defined and shelter-in-place protocols can be communicated. In an open parking lot, there is no shelter. There is no defined perimeter to lock down. There is only the time between when a shot is fired and when security has verified, actionable intelligence about where it came from.

The Incidents That Defined the Challenge

Several high-profile incidents in recent years illustrate the unique challenges associated with responding to threats in and around sports and entertainment venues.

The July 2021 shooting outside Nationals Park in Washington, D.C., originated entirely outside the venue's security screening perimeter. Although no one inside the stadium was injured, the incident prompted the suspension of the game and sent spectators scrambling for cover as law enforcement and venue security worked to determine what had occurred.[14]

Similarly, during a game at Guaranteed Rate Field in Chicago in August 2023, two women were struck by gunfire. Investigators were initially unable to determine whether the shots originated from inside the stadium or from outside the venue, creating uncertainty during the early stages of the response while officials worked to assess the situation.[15]

Although the circumstances differed, both incidents highlight a common operational challenge: security incidents occurring outside—or at the edge of—the venue can be difficult to quickly locate, verify, and assess. In those situations, security personnel must rapidly gather information, coordinate with law enforcement, communicate with spectators, and make operational decisions while the situation continues to evolve.

The 2017 Las Vegas Route 91 Harvest festival massacre made the same point at a catastrophic scale. A shooter firing from an elevated position into an open-air crowd of 22,000 people killed 60 and wounded more than 400.[16] The incident fundamentally changed how the security industry thinks about outdoor perimeter threats at large-scale public events, and it remains the most cited example of what the outdoor coverage gap looks like when it is exploited at full scale.

The Coverage Gap in Practice

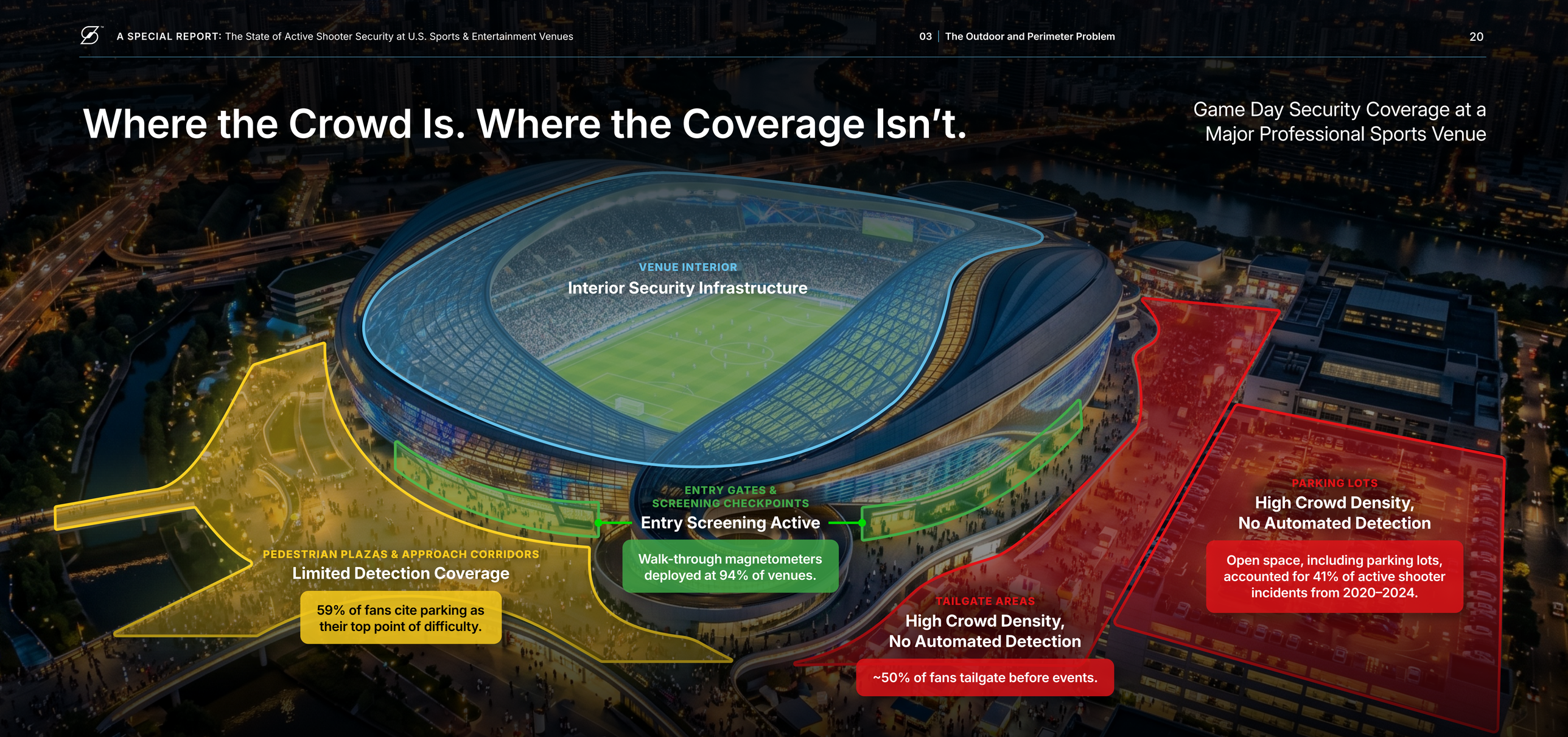
Traditional security tools are designed for the environment inside the building. Walk-through magnetometers screen at entry. Surveillance cameras cover concourses and seating areas. Access control manages credentialed entry points. None of these tools provide detection capability in the parking lot, the tailgate area, or the pedestrian plaza where the pre-game crowd is concentrated.

The result is a security posture that is strongest at the point of entry and weakest in the environment where the crowd spends the most time before passing through it.

An active shooter scenario in a professional sports facility parking lot would be difficult to deal with due to vehicles, open space, panicking fans, and reaction time from security.

Where the Crowd Is. Where the Coverage Isn't.

Game Day Security Coverage at a Major Professional Sports Venue



Color zones indicate crowd density and automated detection coverage during the peak pre-game window. Red zones represent areas of highest fan concentration and lowest detection capability.

Source: NCS4 2023 and 2025 Spectator Safety and Security Surveys; FBI Active Shooter Incidents in the United States, 2024; Global Sport Business Journal, 2025.

04 The Response Time Problem

Key Takeaways

Many active shooter incidents conclude within minutes, often before law enforcement arrives. In **77% of incidents from 2020 to 2024, the situation resolved before law enforcement exchanged gunfire**.[3]

Saturday is the highest active shooter incident day across the five-year period, and **incidents are most likely to occur between noon and midnight**, aligning directly with peak entertainment and sports event scheduling.[3]

A manual notification chain, witness reports to staff, staff to supervisor, supervisor to escalation, introduces **dangerous delay at the moment when seconds matter most**.

Automated detection compresses the notification chain from minutes to seconds, delivering verified location data to security personnel and first responders simultaneously without human initiation.

When an active shooter incident begins, every minute matters. Research from the foundational ALERRT Center and FBI study of active shooter incidents (2000-2013) found that many active shooter incidents conclude within minutes, often before law enforcement arrives on scene.[5] That finding has shaped emergency response doctrine for more than a decade and remains the central operational reality that every venue security plan must be built around.

More recent FBI data reinforces this pattern. Between 2020 and 2024, only 23% of active shooter incidents involved an exchange of gunfire with responding law enforcement. In the remaining 77% of incidents, the event had already concluded before that occurred — whether because the shooter fled, was apprehended, died by suicide, or was stopped through civilian intervention.[3]

These findings underscore an important operational reality for venue security leaders: the earliest moments of an incident are often the most consequential. While law enforcement plays a critical role in the response, venue personnel are frequently responsible for recognizing the incident, initiating emergency procedures, communicating with attendees, and coordinating the initial response before outside assistance arrives.

The Challenge of Identifying Gunfire

Sports and entertainment venues present a uniquely complex environment for identifying and responding to gunfire. On event days, crowd noise, announcements, music, pyrotechnics, fireworks, and the sounds of tens of thousands of spectators create an environment where unusual noises may not be immediately recognized or interpreted consistently. Witnesses may describe the same sound in different ways — as a bang, a pop, or fireworks — and not everyone who hears it will immediately recognize it as a gunshot.

During an active shooting, 911 centers are routinely overwhelmed with calls providing incomplete or conflicting information. At a venue with 50,000 people, the volume of simultaneous calls can delay the point at which dispatchers have a coherent picture of the incident. Every minute spent resolving ambiguity is a minute in which the response has not yet been coordinated.

For venue operators, this creates an important operational challenge. The speed at which an incident is recognized, verified, and communicated can influence how quickly emergency procedures are initiated, how accurately information is shared with first responders, and how effectively attendees are directed to safety.

The Outdoor Amplification Effect

The challenges associated with responding to an active shooter incident are often amplified in outdoor environments. Inside a venue, security operations centers can often draw on multiple sources of information, including surveillance cameras, access control systems, radio communications, and detailed facility maps, to help assess an incident and coordinate a response.

Outdoor environments present a different set of operational challenges. Parking lots, pedestrian plazas, tailgate areas, and approach corridors are larger, less structured spaces where spectators move freely before and after events. Camera coverage may be less comprehensive than inside the venue, visibility can be affected by vehicles and other physical obstructions, and responding personnel may need to assess a much broader area while managing large, mobile crowds.

These conditions can make it more difficult to quickly determine where an incident occurred, what has happened, and how best to coordinate an effective response. As a result, preparedness for outdoor environments requires security strategies that account for the unique characteristics of these spaces rather than relying solely on approaches designed for the interior of the venue.

When Timing Matters

The FBI's active shooter data reveals not only where incidents occur, but also clear patterns in when they occur. Those patterns provide important context for venue security leaders responsible for preparedness, staffing, and event-day operations.

Between 2020 and 2024, Saturday recorded more active shooter incidents than any other day of the week, with 46 incidents over the five-year period (an average of 9.2 incidents annually).[3] The FBI's updated dataset through 2025 identifies Monday as the highest-incidence day overall, though weekend days — including Saturday — remain consistently represented across both reporting periods.[4]

The FBI also found that active shooter incidents were most likely to occur between noon and midnight, with 57% of incidents occurring during afternoon and evening hours between 2020 and 2024.[3]

For sports and entertainment venues, these findings align closely with periods of peak attendance and event activity. Professional and collegiate sporting events, concerts, festivals, and other large public gatherings are frequently scheduled during weekends and during the afternoon and evening hours identified in the FBI's analysis. While this overlap does not suggest a causal relationship, it reinforces the importance of ensuring that staffing, communication systems, and emergency response protocols are fully operational during periods when venues are busiest.

Rather than changing the nature of the threat, these scheduling patterns provide additional context for preparedness planning, helping venue operators align security resources with the times when both attendance and historical incident frequency are highest.

The Manual Notification Gap

Response time is influenced not only by how quickly an incident is detected, but also by how quickly accurate information reaches the people responsible for coordinating the response.

Under current conditions at most venues, the notification chain following a suspected shooting event depends on a human being initiating it. A witness calls 911 or reports to a security staff member. That staff member radios a supervisor. The supervisor attempts to verify the report before escalating. Each step in that chain introduces delay, and each delay occurs during the window in which the incident is most likely still active.

The challenge becomes more complex during large public events, where thousands of attendees may witness the same incident from different locations and report conflicting or incomplete information. Security personnel and emergency dispatchers must quickly assess those reports, establish situational awareness, and coordinate an appropriate response under rapidly evolving conditions.

Automated detection removes that dependency. A system that detects a confirmed ballistic event and simultaneously notifies security personnel, building occupants, and 911 dispatch does not hesitate, and does not wait for a supervisor to confirm before escalating. It compresses the notification chain to seconds rather than minutes, and it does so with verified information rather than witness accounts.

In an environment where most incidents conclude within minutes, the difference between a sub-one-second automated alert and the minutes it takes for the manual notification chain can be significant. The staffing picture at most professional sports venues makes that dependency more consequential than it might appear.

05 The Staffing Crisis as a Force Multiplier for Risk

Key Takeaways

65% of venue security directors experienced staff shortages in the last two years. **74% rely on contracted security staff** for game day coverage.[17]

Active shooter response training ranks last among contracted staff training priorities, the workforce most likely to be the first observer of an outdoor incident.[6]

The contracted security workforce is trained primarily for routine functions: entry screening, crowd management, fan code of conduct. **It is not trained or positioned to be the primary detection mechanism for a live fire event**.

Technology deployed as a force multiplier, not a replacement for people, **addresses the structural gaps** that staffing investment alone cannot close.

Effective security at sports and entertainment venues depends not only on technology and planning, but also on having the right people in the right place at the right time. Large venues require hundreds of personnel to support entry screening, crowd management, traffic control, parking operations, guest services, and emergency response, and often within a concentrated window before, during, and after an event. The operational demands are significant, and the staffing reality at most venues is not keeping pace with them.

The research suggests that maintaining those staffing levels has become increasingly difficult. According to NCS4's 2026 Venue Security Director Survey, 65% of venue security directors reported experiencing staff shortages within the previous two years. The most frequently cited causes were staff no-shows, a lack of qualified applicants, lack of interest, and budget constraints.[17]

In the 2024 edition of the NCS4 Venue Security Director Survey, venue operators have responded in a variety of ways. Nearly 97% reported implementing measures to improve recruitment and retention, including wage increases, complimentary meals, employee recognition programs, and parking incentives.[6] Despite these efforts, staffing shortages remain a common operational challenge across the industry.

The survey also found that 74% of professional sports venues rely on contracted security personnel to some extent on event days.[17] Approximately 36% reported relying entirely on third-party security providers, while more than 75% outsource the majority of their event security staffing.[6]

These findings highlight an important characteristic of venue security operations. Security teams are often assembled from a combination of full-time personnel and contracted staff who may work at multiple venues or events throughout the year. Maintaining consistent staffing levels, communication, and preparedness across that workforce has become an increasingly important consideration for venue security leaders.

The Training Challenge

Staffing is only one part of the equation. The effectiveness of a security program also depends on ensuring personnel receive training that reflects the environments and risks they are expected to manage.

The NCS4 2024 survey documents a significant divergence between the training priorities for full-time in-house security staff and those for contracted security staff. Among full-time security personnel, the most common training requirements included de-escalation and conflict resolution (89%), incident reporting (87%), venue and event familiarization (87%), operation of security technology (83%), and standard operating procedures (81%). Active shooter response training was provided by 72% of venues, ranking 11 out of 12 training categories.[6]

Among contracted security personnel, training priorities were more heavily focused on event operations, including prohibited items (85%), crowd management (83%), venue and event familiarization (83%), fan code of conduct (79%), and standard operating procedures (77%). Active shooter response training was provided by 63% of venues, ranking last among the 13 training categories included in the survey.[6]

These differences likely reflect the distinct responsibilities assigned to each group. Contracted personnel are frequently responsible for entry screening, crowd management, parking operations, and guest interactions during events, while full-time security teams often assume broader operational and incident management responsibilities.

At the same time, the survey findings highlight an important consideration for venue operators. Because contracted personnel are often deployed throughout parking areas, entry gates, and other public-facing locations, they may be among the first to observe unusual activity or receive reports of an incident. Ensuring that all members of the security workforce understand emergency procedures, communication protocols, and their role during a critical incident remains an important component of overall preparedness.

Technology as a Force Multiplier

Many venues are already using technology to help address staffing challenges. According to the NCS4 survey, technology investments are increasingly being considered alongside recruitment, retention, and training efforts as part of a broader strategy to strengthen operational readiness.

Rather than replacing personnel, technology is most effective when it supports the people responsible for managing security operations. Communication platforms, access control systems, surveillance technologies, mass notification tools, and other security technologies can help improve situational awareness, streamline information sharing, and support more coordinated decision-making during routine operations and emergency incidents alike.

This is particularly important in environments where staffing levels fluctuate or where venues rely heavily on contracted personnel. In these settings, technology can help promote greater consistency in communication, provide timely information to security teams, and support established emergency procedures without replacing the judgment and experience of trained personnel.

Ultimately, preparedness depends on the combined strength of people, processes, and technology. As staffing challenges continue across the sports and entertainment industry, many venue operators are evaluating how technology can complement existing security programs by supporting faster communication, improving situational awareness, and helping security teams respond more effectively when every second matters.

Ultimately, preparedness depends on the combined strength of people, processes, and technology. As staffing challenges continue across the sports and entertainment industry, many venue operators are evaluating how technology can complement existing security programs.

06 The Security Technology Stack — What's in Place and What's Missing

Key Takeaways

The most widely deployed security technologies at professional sports venues are built for access management and communication. Two-way radios and cameras are at 96% adoption. **Shooter detection systems are at 13%.**[6]

Walk-through magnetometers, deployed at 94% of venues, are effective during the entry window only.[6] **They provide no coverage in parking lots, tailgate areas, or for weapons introduced after screening.**

Millimeter wave screeners, deployed at 10% of venues, detect non-metallic threats that standard magnetometers miss[6], but **carry throughput and cost constraints that limit broad deployment**.

Handguns accounted for 63% of firearms used in active shooter incidents from 2020 to 2024[3], making them the weapon most likely to be concealed, passed through a staffing gap, or introduced through a non-screened access point.

The tools at most venues operate in isolation. The integration gap is where the response either accelerates or stalls in an active incident.

Professional sports and entertainment venues have made significant investments in security technology over the past two decades. The question is no longer whether venues are investing in security, but how those investments are distributed across different aspects of the security environment.

The NCS4's 2024 Venue Security Director Survey documents the current technology landscape across professional sports venues with considerable specificity. The most widely deployed tools are two-way radios and surveillance cameras, each at 96% adoption, followed by access control and credentialing systems and walk-through magnetometers, each at 94%. Social media monitoring (90%), public address systems (90%), mobile ticketing apps (90%), and handheld magnetometers (79%) round out the upper tier.[6] They share a common characteristic: they are built for access management, communication, and crowd control.

At the other end of the adoption spectrum, the picture shifts significantly. Gunshot detection systems are currently deployed at 13% of venues. Millimeter wave screeners are at 10%. Facial recognition systems are at 8%. Robots in security roles are at 2%.[6]

These findings suggest that while foundational security technologies have achieved widespread adoption, emerging technologies remain in earlier stages of implementation. As venue operators continue to evaluate evolving threats, staffing challenges, and operational priorities, decisions about future technology investments will likely be shaped by a combination of risk, operational fit, cost, and organizational priorities.

The Entry Screening Layer

Entry screening remains one of the foundational components of security at entertainment and sports venues.

According to the NCS4 2024 Venue Security Director Survey, walk-through magnetometers are deployed at 94% of professional sports venues, making them the industry's primary weapons screening technology.[6] During spectator ingress, they provide an effective means of screening attendees for metallic weapons before they enter the venue. Unfortunately, 51% of professional venues and 27% of collegiate venues report having appropriate screening measures to protect against privately made firearms, such as 3D-printed weapons.[17]

Like all security technologies, however, walk-through magnetometers are designed for a specific purpose. Their role is to screen spectators as they enter the venue through designated access points. Once screening has concluded, their function is complete, and other security measures assume responsibility for monitoring the venue and its surrounding environment.

Handheld magnetometers, deployed at 79% of venues, extend the screening layer but carry the same temporal and spatial limitations. Both are entry-layer solutions in an environment where the threat does not confine itself to the entry window.

The survey also found that millimeter wave screening systems have been adopted by 10% of venues.[6] Unlike traditional magnetometers, these systems can identify both metallic and certain non-metallic threats, expanding the range of items that may be detected during entry screening. At the same time, they typically require additional space, involve higher implementation costs, and can affect throughput at entry points — important operational considerations for venues managing large numbers of spectators within relatively short arrival windows.

Together, these findings highlight an important characteristic of entry screening technologies: they are designed to secure the point of entry. They represent a critical layer within a broader security strategy, while other technologies, personnel, and operational procedures address the security needs of the venue before, during, and after spectators enter the facility.

What Happens After Entry Screening

The technology adoption data reveals a consistent pattern: the tools deployed at the highest rates operate at or before the entry point, while the tools that provide detection capability after a weapon has entered the venue are deployed at the lowest rates.

Video analytics, which can support post-entry surveillance, are deployed at 50% of venues. Mass notification systems, which are critical to coordinated response once an incident is confirmed, are at 71%. Gunshot detection systems, which provide automated confirmation of a live fire event, are at 13% as of the NCS4 2024 Venue Security Director Survey,[6] despite 30% of venue security directors identifying them as a priority investment if additional funding were available.[9] That figure, however, reflects a moment in time. Adoption of gunshot detection technology at professional sports venues appears to be growing, reflecting greater awareness of the outdoor threat gap, and a broader recognition that entry screening alone is not sufficient for the threat environment venues now face. The trajectory is encouraging. The gap between current adoption and the scale of the threat remains significant.

Handguns accounted for 63% of firearms used in active shooter incidents from 2020 to 2024, making them the weapon most likely to be concealed, passed through a staffing gap at entry screening, or introduced through a non-screened access point.[3] A security stack that is strongest at the entry point and thinnest in post-entry detection is optimized for the wrong end of the threat timeline.

The Integration Gap

The adoption data alone does not capture the degree to which the tools deployed at most venues operate in isolation from one another. Surveillance cameras, access control systems, mass notification platforms, and incident management tools are typically managed through separate interfaces, by separate teams, with little or no automated connection between them.

The consequence of that fragmentation is most acute in an active incident. A confirmed gunshot event requires simultaneous action across multiple systems. Cameras need to be directed to the incident location. Access control needs to initiate lockdown or controlled egress at the right doors. Mass notification needs to reach building occupants, security personnel, and first responders with accurate location data, not a general alarm. Under current conditions at most venues, that coordination happens manually, sequentially, and under conditions of maximum stress and minimum information. Each system works. The connections between them do not, and in an active shooter scenario, those connections are where the response either accelerates or stalls.

Before examining what an integrated detection system looks like in practice, it is worth understanding the legal and procurement framework that should govern how venues evaluate the technologies they deploy.

06B The SAFETY Act Framework — What It Is and Why It Matters

Key Takeaways

DHS administers the SAFETY Act program at three distinct levels: green seal DT&E Designation (provisional), blue seal Designation (broader liability cap), and red seal Certification (full Government Contractor Defense). **They are not equivalent protections.**

Over 60% of professional sports venues have obtained or are pursuing SAFETY Act Certification for their security programs.[9] The technologies they deploy should meet the same standard.

Shooter Detection Systems is the only gunshot detection manufacturer to hold the highest level of SAFETY Act Certification, first achieved in 2017 and renewed in 2023.

Most venue security directors have encountered the term ‘SAFETY Act certified’ in vendor presentations and procurement conversations. Fewer have a working understanding of what the program actually is, how its award levels differ from one another, and why those distinctions carry real operational and legal weight. For a venue evaluating security technology investments, that understanding is not optional.

The Origin and Purpose of the Program

In the aftermath of the September 11, 2001 terrorist attacks, the private sector expressed considerable reluctance to deploy security technologies and services in civilian settings. The reason was straightforward: the potential liability exposure in the event that a deployed technology was involved in, or failed to prevent, an act of terrorism was enormous.

Congress responded by enacting the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, known as the SAFETY Act. The program’s purpose was to mitigate liability risk for private sector operators and technology vendors, and in doing so, to encourage the widespread deployment of effective anti-terrorism technologies and services that could save lives. The SAFETY Act Program is administered by the Office of SAFETY Act Implementation within the Science and Technology Directorate of the U.S. Department of Homeland Security. The program is voluntary, but for venues and technology vendors that pursue it, it provides a documented framework of legal protection that has direct implications for how liability is assessed in the event of a terrorism-related incident.[12]

The Three Levels of SAFETY Act Status

The SAFETY Act framework[12] includes three distinct levels of designation, each providing a different level of liability protection. Understanding these distinctions is important when evaluating security technologies and the protections they offer.

The first level is Developmental Testing and Evaluation Designation, commonly referred to as DT&E Designation, represented by a green DHS seal. This is a temporary status, typically lasting three years, granted to technologies in early development or limited deployment. It provides a limited liability cap and signals that the technology has not yet demonstrated the effectiveness required for a full Designation.

The second level is SAFETY Act Designation, represented by a blue DHS seal. This provides a broader liability cap than DT&E Designation and applies to technologies that have demonstrated a meaningful level of effectiveness. It does not, however, confer the Government Contractor Defense, which is the program’s most significant legal protection.

The third and highest level is SAFETY Act Certification, represented by the red DHS seal, which is the most recognizable marker of the program’s highest standard. It confers all of the benefits of Designation plus the Government Contractor Defense, which can remove liability for claims arising from an act of terrorism when

a certified technology is deployed. Achieving Certification requires DHS to have high confidence in the technology's ongoing effectiveness. It is not awarded to systems with unresolved performance concerns, and it is not a one-time achievement. Certification must be renewed, and renewal requires demonstrating sustained performance over time, not a single point-in-time result.[12]

A vendor holding active SAFETY Act Certification has passed that bar more than once. Shooter Detection Systems achieved SAFETY Act Certification for its indoor gunshot detection system on its first application in 2017 and successfully renewed that Certification in 2023, reflecting more than six years of demonstrated performance in real-world deployments across a wide range of environments. As of the publishing of this report, Shooter Detection Systems is the only gunshot detection manufacturer to hold SAFETY Act Certification status[10], the red DHS seal.

Why This Matters for Venues Specifically

The SAFETY Act framework has two important implications for sports and entertainment venues: one at the organizational level and another at the technology level.

The first is organizational. Venues themselves can apply for and obtain SAFETY Act Certification for their security programs. The certification process requires venues to have comprehensive and robust security measures that deter and defend against terrorist attacks. According to the NCS4 2026 Venue Security Director Survey, 64% of venues and 50% of collegiate venues have obtained or are in the process of obtaining DHS SAFETY Act Certification.[17]

The NCS4's 2024 Venue Security Director Survey also found that nearly all venues (96%) also support the DHS "If you see something, say something" initiative, reflecting a broad alignment with the DHS security framework at the operational level.[6]

The second relevance is procurement-based. The technologies a venue deploys within its security program carry their own SAFETY Act status, independent of the venue's organizational certification. As a result, venue operators evaluating security technologies may wish to consider both the venue's own SAFETY Act status and the status of the technologies incorporated into their broader security program. Venues are encouraged to apply the same certification standard to the technologies they procure as they do to their own security programs. Understanding what meeting that standard looks like in practice, across both detection performance and system integration, is what separates a security posture that is certified on paper from one that performs when it matters.

Shooter Detection Systems achieved SAFETY Act Certification for its indoor gunshot detection system on its first application in 2017 and successfully renewed that Certification in 2023, reflecting more than six years of demonstrated performance in real-world deployments across a wide range of environments.

Understanding SAFETY Act Status: Not All Certifications Are Equal

DHS administers the SAFETY Act program at three distinct levels. The protections they provide are materially different.



SAFETY Act Certification

Full Government Contractor Defense.
Complete Liability Protection.

The highest level of SAFETY Act status. Requires the most rigorous DHS review and demonstrated sustained field performance over time. Must be renewed every 5 years.

Shooter Detection Systems is the only gunshot detection manufacturer to hold SAFETY Act Certification, the highest level of DHS SAFETY Act status. First achieved in 2017 and renewed in 2023.



SAFETY Act Designation

Broader Liability Cap.
Blocks Punitive Damages.

A step forward from provisional DT&E status, but does not include the Government Contractor Defense, the program's most significant legal protection.



Developmental Testing and Evaluation Designation

Limited Liability Cap

Provisional status for technologies in early development or limited deployment. Temporary, typically lasting three years. Signals the technology has not yet demonstrated the effectiveness required for full Designation.

What to Ask Every Vendor

+ What level of SAFETY Act status does the product hold?
+ Is the status current and active?
+ Can you provide your signed DHS certificate in writing?

A green seal, a blue seal, and a red seal are not equivalent protections. Search for technology status on SafetyAct.gov.

Source: U.S. Department of Homeland Security SAFETY Act Program; DHS Best Practices in Anti-Terrorism Security (BPATS).

07 What Best-in-Class Looks Like

Key Takeaways

Best-in-class venue security is defined by six integrated layers: **entry screening, perimeter access control, surveillance, outdoor gunshot detection, indoor gunshot detection, and integrated response automation**.

The fourth and fifth layers, **outdoor and indoor gunshot detection, are the most consequential gaps** in current venue security posture.

Advanced gunshot detection using dual-factor acoustic and infrared technology delivers **confirmed detection in under one second indoors and under three seconds outdoors**, with a false alert rate low enough that every alert demands immediate response.

When fully integrated, a detection event simultaneously steers cameras, initiates access control protocols, pushes mass notification, and delivers verified location data to 911 dispatch, **without a human in the loop**.

The previous sections of this report identify several consistent themes: an evolving threat landscape, strong public confidence in venue security, staffing and operational challenges, and security programs that have historically focused on access control and entry screening. Together, these findings provide a framework for understanding how leading sports and entertainment venues are approaching preparedness today.

Best-in-class venue security is defined by the integration of multiple layers into a system that functions as a coordinated whole, where a detection event in one layer automatically activates the response capability of every other layer simultaneously. The distinction between a collection of security tools and an integrated security system is the difference between a response that requires human coordination under stress and one that begins automatically, with verified information, in the same second a threat is confirmed.

The Layered Model

No single security measure is designed to address every threat scenario. Instead, leading sports and entertainment venues increasingly rely on a layered security approach, where multiple technologies, operational procedures, and trained personnel work together to support prevention, detection, communication, and response.

Each layer serves a distinct purpose within the broader security program.

PERIMETER ACCESS CONTROL & CREDENTIALING

The first layer establishes the security boundary around the venue by controlling access to restricted areas, back-of-house operations, loading docks, and other non-public spaces. Credentialing systems help ensure that only authorized personnel can access sensitive areas.

ENTRY SCREENING

Walk-through magnetometers, deployed at 94% of professional sports venues, remain the primary weapons screening technology at spectator entrances.[6] Handheld magnetometers and, in some cases, millimeter wave screening systems provide additional screening capabilities where operationally appropriate.

SURVEILLANCE & SITUATIONAL AWARENESS

Surveillance cameras, deployed at 96% of venues, provide visual coverage of key areas throughout the facility. Many venues also supplement traditional video systems with technologies such as video analytics, which were reported by 50% of surveyed venues, to support monitoring and situational awareness.[6]

OUTDOOR DETECTION & MONITORING

Parking lots, tailgate areas, pedestrian plazas, and other outdoor gathering spaces present different operational challenges than the interior of a venue. As discussed earlier in this report, these environments accommodate large crowds before and after events and have become an increasingly important focus of security planning. Some venues are incorporating additional technologies to strengthen awareness and response capabilities in these outdoor areas.

INTERIOR DETECTION & RESPONSE

Once spectators have entered the venue, security shifts from entry screening to maintaining situational awareness across concourses, seating areas, clubs, back-of-house spaces, and other interior environments. Technologies supporting incident detection, communications, and coordinated response may play an important role alongside trained personnel and established emergency procedures.

INTEGRATED COMMUNICATIONS & RESPONSE

The final layer brings these individual components together. Security technologies are most effective when they are integrated with communication systems, emergency notification platforms, access control, surveillance, and established response protocols. This integration enables security personnel and first responders to receive timely information, coordinate decision-making, and respond more effectively during an incident.

Together, these layers illustrate an important principle of modern venue security: preparedness is achieved not through any single technology or procedure, but through a coordinated system in which people, processes, and technology complement one another.

When Every Alert Has to Count

The performance standard for each layer matters as much as its presence. A gunshot detection system that generates frequent false alerts does not compress the response time gap. It expands it, training security teams to treat alerts as noise rather than intelligence until a real event is dismissed as another false alarm.

The standard must be demanding: confirmed detection of a live fire event in under one second indoors and under three seconds outdoors, with a false alert rate low enough that every alert is treated as a genuine event.

Advanced gunshot detection technology operating at this standard, like Shooter Detection Systems, detects gunshots in under one second using dual-factor acoustic and infrared technology. Both signals must be independently confirmed before any alert is generated. A system operating at this level will not alert on acoustic signal alone, regardless of how closely it resembles a gunshot, and will not alert on infrared alone.

The performance data behind that architecture is independently verified. The UK's National Protective Security Authority conducted an 18-month installed environment test of the SDS indoor system, resulting in a 99.9% detection rate and a 0% false alert rate.[10] In over 18 months of continuous operation in a real-world environment, the system did not generate a single false alert. National Technical Systems, a global product testing and inspection firm, conducted a full live-fire test plan against six weapon types, from a .22 LR handgun to a 5.56×45mm rifle, with zero false alerts across eleven non-ballistic sound challenges including air horns, pneumatic nail guns, and human clapping and yelling. The system achieved perfect performance results across all test conditions.[10]

For outdoor environments, the same dual-factor architecture applies, with machine learning algorithms developed and validated specifically for outdoor acoustic conditions including wind, precipitation, vehicle traffic, crowd noise, and the unpredictable reverb of open terrain. The result is detection in under three seconds, with a false alert rate below one per one million hours of operation.[10]

Preparedness is achieved not through any single technology or procedure, but through a coordinated system in which people, processes, and technology complement one another.

When Systems Work Together

Technology is most effective when it operates as part of an integrated security ecosystem rather than as a collection of standalone systems. The value of any detection technology depends not only on its ability to identify an incident, but also on how quickly that information can be shared with the people and systems responsible for coordinating the response.

When a gunshot detection system is fully integrated into a venue's security stack, the following occurs simultaneously and automatically at the moment of detection:

+ Video management systems receive the alert and automatically steer the nearest cameras to the detection location, begin recording, and display the live feed on the security operations center screen.
+ Access control systems initiate lockdown protocols, locking specified doors, securing elevators, or triggering safe egress procedures based on pre-configured response rules.
+ Mass notification systems push alerts to security staff, venue personnel, and building occupants through SMS, desktop alerts, PA systems, digital signage, and mobile applications.
+ Public safety and computer-aided dispatch systems receive verified alert data with precise location information, pushing directly to dispatcher screens and officer mobile data terminals.

Venues should require certified integrations with their existing video management, access control, mass notification, and public safety platforms, with API-based connections that do not require additional wiring or relay devices.

Privacy by Design

Privacy is an important consideration for venue operators evaluating any security technology, particularly technologies deployed in public-facing environments.

Gunshot detection technologies are no exception. As venues assess different solutions, privacy protections should be considered alongside detection performance, system integration, and operational effectiveness. Understanding how a system collects, processes, stores, and transmits data is an important part of the evaluation process.

Some modern gunshot detection systems are designed to identify the acoustic signature of a gunshot rather than continuously recording conversations or collecting personally identifiable information. However, capabilities vary by technology and manufacturer. Venue operators should understand how any proposed system processes data, whether audio is stored or transmitted, and how the technology aligns with applicable privacy regulations and organizational policies.

For sports and entertainment venues, privacy-by-design principles can help ensure that security technologies support public safety while respecting the privacy expectations of spectators, employees, and visitors.

Privacy-by-design principles can help ensure that security technologies support public safety while respecting the privacy expectations of spectators, employees, and visitors.

A Layered Approach to Venue Security

Six integrated layers define best-in-class preparedness at professional sports and entertainment venues.

LAYER 1

Perimeter Access Control & Credentialing

Controls access to restricted areas, back-of-house operations, loading docks, and non-public entry points. The foundation of the security architecture.

LAYER 2

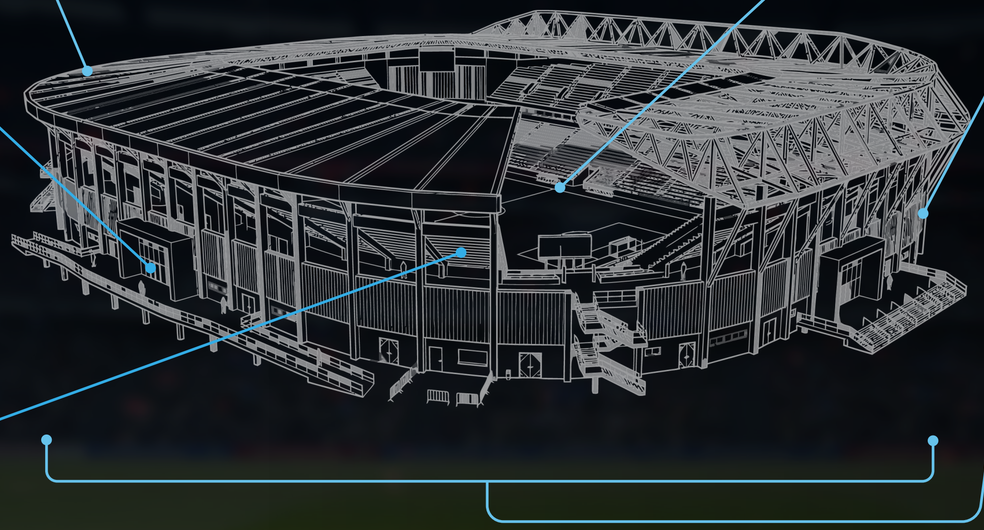
Entry Screening

Walk-through magnetometers (94% of venues), handheld magnetometers (79%), and millimeter wave screeners (10%) provide weapons detection during the controlled fan ingress window.

LAYER 3

Surveillance & Situational Awareness

Surveillance cameras (96% of venues) and video analytics (50% of venues) provide visual coverage of concourses, seating areas, and entry points.



LAYER 4

Indoor Gunshot Detection

CRITICAL GAP

Covers concourses, concession areas, seating bowls, club levels, back-of-house corridors, locker rooms, and administrative spaces. Addresses threats that have passed the entry screening layer. Currently deployed at 13% of venues.

LAYER 5

Outdoor Gunshot Detection

CRITICAL GAP

Sensors deployed across parking areas, tailgate zones, pedestrian plazas, and stadium approaches. Provides automated detection in the open-space environment where 41% of active shooter incidents occur. Currently deployed at a minority of venues.

LAYER 6

Integrated Response Automation

The connective tissue that transforms the preceding five layers into a coordinated system. At the moment of detection: cameras steer to the incident location, access control initiates lockdown or controlled egress, mass notification reaches security personnel and building occupants, and verified location data arrives at 911 dispatch simultaneously.

When these layers work together, the response chain compresses from minutes to seconds, with verified location data reaching security personnel and first responders simultaneously, without depending on a human observer to initiate it.

CRITICAL GAP

Layers 4 and 5 represent the most significant gaps in current venue security deployments. Shooter detection systems are deployed at 13% of professional sports venues as of the NCS4 2024 Venue Security Director Survey.

Source: NCS4 2024 Venue Security Director Survey; FBI Active Shooter Incidents in the United States, 2024; Shooter Detection Systems.

08 Recommendations for Venue Security Leaders

Key Takeaways

Seven actionable priorities, organized in order of foundational importance: outdoor coverage audit, technology stack evaluation, integration gap assessment, staffing-automation balance, fan-facing security communication, pre-game window strategy, and security surcharge consideration.

The outdoor coverage audit is the highest-priority first step. Venues that cannot answer what their response protocol is if a shot is fired in the parking lot during peak pre-game density have identified their most urgent gap.

80% of fans are willing to pay a security surcharge of $0.50 to $5.00 per ticket. At a 50,000-seat MLB venue across an 81-game season, a $1.00 surcharge generates $4.05 million annually.[7]

Preparedness is an ongoing process, not a fixed destination. **The venues best prepared for the future are those that continuously evaluate their security posture and adapt to emerging risks.**

The research presented throughout this report points to a clear conclusion: strengthening preparedness is not about adopting a single technology or policy. It requires a layered approach that aligns people, processes, and technology with today's threat environment.

These recommendations are drawn from the research, from the operational realities documented throughout this report, and from the guidance published by the NCS4, DHS, and the Global Sport Business Journal study. They are organized in order of foundational priority.

1 Conduct an Honest Outdoor Coverage Audit

The single most consequential gap in professional sports venue security is the outdoor and perimeter environment. Before any technology investment decision is made, venue security directors should conduct a systematic audit of their outdoor coverage: parking lots, tailgate areas, pedestrian plazas, approach corridors, and any open space where fans congregate before passing through entry screening.

The audit should answer three questions:

1. **Where are fans concentrated outdoors, and during what windows?**
2. **What detection capability currently exists in those areas?**
3. **And what is the current response protocol if a shot is fired in the parking lot during peak pre-game crowd density?**

Venues that do not have a written answer to the third question have identified their most urgent priority. The NCS4 recommends mapping fan congregation points against existing camera coverage and security staffing positions as a starting framework for that assessment.[6]

2 Evaluate Your Technology Stack Against the Full Threat Timeline

The technology adoption data in this report reveals a security stack built primarily for the entry point and the controlled interior environment. That is the right investment for the threats venues have historically managed most frequently but may not be sufficient for the threat environment that now exists.

Venue security directors should map their current technology investments against the full threat timeline using four zones: before entry, at entry, after entry, and in the outdoor environment. For each zone, the assessment should identify what detection capability exists, what the current notification chain looks like, and how long it would take to get verified information to a security operations center. The gaps that emerge from that mapping, particularly in post-entry detection and outdoor coverage, are where the preparedness gap is widest and where investment will have the most impact.

3 Address the Integration Gap Before Adding New Tools

The most common failure mode in venue security technology investment is acquiring new tools that operate in isolation from the systems already in place. A gunshot detection system that alerts a security operations center screen but does not automatically steer cameras, initiate access control protocols, or push notifications to first responders is a better tool than nothing, but does not represent a best-in-class response capability.

Before evaluating new detection technology, venues should assess the integration capability of their existing security technology stack. Key questions to ask any detection vendor include: Are integrations API-based or relay-dependent? Which specific VMS, access control, and mass notification platforms are certified, not just compatible? And what does the automated response chain look like from the moment of detection to first responder notification? The integration architecture should be a primary evaluation criterion.

4 Rethink the Staffing-Automation Balance

The contracted security workforce that staffs most professional sports venues on game day is trained and deployed for the routine functions it performs most frequently, and automation should be deployed deliberately in the gaps where that workforce is least prepared to act.

Active shooter response training ranks last among contracted security staff training priorities. That is not a failure of intent, but it is a reflection of the operational reality that contracted staff are hired and trained primarily for the routine functions they perform on most game days. Automated detection does not replace that workforce. It provides the detection and notification capability that the workforce is least equipped to deliver in the highest-stakes moment.

Venues should invest in improving active shooter response training for both full-time and contracted staff, with particular attention to incident recognition, escalation protocols, and coordination with automated systems. The NCS4 recommends scenario-based tabletop exercises conducted at least annually, with separate tracks for full-time and contracted staff that reflect their different roles in the response chain. Training should be updated whenever threat intelligence, venue layout, or detection technology changes.[6]

5 Make Security Visible to Fans

The NCS4's 2025 Spectator Safety and Security Survey found that fans who perceive visible security measures feel meaningfully safer at events.[7] Law enforcement presence, K-9 units, surveillance cameras, security personnel in clearly identifiable uniforms, and perimeter barriers all contribute to a security profile that fans can see and respond to positively.

Venues should also communicate security measures proactively before, during, and after events. The NCS4 research identifies active shooter response policy as among the lowest-familiarity policies among fans, not because fans are indifferent to it, but because venues have not consistently communicated what is in place. A dedicated section on the venue website covering security procedures, prohibited items, and emergency protocols gives fans who want that information a place to find it. Pre-event emails, venue apps, and ticketing confirmation communications are effective channels for setting expectations around entry screening, bag policies, and what to do in an emergency. The goal is not to worry fans but to educate them, and an informed fan who understands what security measures are in place arrives with greater confidence in the environment they are entering.

6 Use the Pre-Game Window Strategically

The outdoor crowd concentration problem documented in this report is partly structural and partly behavioral. Among fans, 76% arrive within 30 minutes of game time, creating a predictable window of maximum outdoor crowd density that coincides with minimum security coverage. Similarly, 65% of fans say they would consider arriving earlier if incentives were offered.[7]

Venues that offer meaningful early-arrival incentives, including food vouchers, merchandise, meet-and-greet opportunities, or priority general admission seating, reduce peak outdoor crowd concentration and extend the window during which fans are inside the controlled security environment. The NCS4 recommends this approach specifically as a crowd management and security strategy. Venues should track early-arrival rates before and after incentive programs to measure their effect on outdoor crowd density during the highest-risk pre-game window.

7 Consider a Security Surcharge to Fund the Gap

One of the more striking findings in the NCS4 fan research is the degree to which fans are willing to contribute financially to venue security. In the NCS4's 2025 Spectator Safety and Security Survey, 80% of fans indicated willingness to pay a security ticket surcharge ranging from $0.50 to $5.00, with 68% willing to pay $1.00 or more per ticket.[7] At a venue hosting 50,000 fans per game across an 81-game MLB season, a $1.00 surcharge would generate up to $4.05 million annually if every attendee paid it, a meaningful source of funding for security technology investment.

The security surcharge model is not widely practiced in professional sports, but the fan data suggests the appetite for it exists. Venues considering this approach should frame the surcharge transparently to fans as a direct investment in their safety, consistent with the NCS4 finding that fans who understand what security measures are in place arrive with greater confidence. For venue operators making the internal budget case for security technology investment, the fan willingness data is a meaningful addition to the financial argument.

80% of fans indicated willingness to pay a security ticket surcharge ranging from $0.50 to $5.00, with 68% willing to pay $1.00 or more per ticket. At a venue hosting 50,000 fans per game across an 81-game MLB season, a $1.00 surcharge would generate up to $4.05 million annually if every attendee paid it, a meaningful source of funding for security technology investment.

The Path Forward

Security at sports and entertainment venues has never been static. Over the past two decades, venues have transformed how they manage access control, crowd safety, emergency planning, and spectator experience. As the threat landscape continues to evolve, so too must the strategies, technologies, and operational practices that support public safety.

The findings in this report reinforce a simple but important point: effective security is not defined by a single technology, policy, or procedure. It is the result of a layered approach that combines well-trained personnel, clear operational plans, interoperable technologies, and strong partnerships with public safety agencies. Each layer strengthens the others, creating a security program that is more resilient, adaptable, and capable of responding to a wide range of threats.

Venue operators do not need to start from scratch. The research, frameworks, and security technologies available today provide a strong foundation for continued improvement. The challenge is not simply adopting new tools, but ensuring that security investments are aligned with today's operational realities and integrated into a cohesive strategy.

Ultimately, the goal is not to eliminate every risk. It is to ensure that when an incident occurs, venue personnel have the information, coordination, and capabilities needed to respond quickly, effectively, and with confidence. The venues best prepared for the future will be those that continuously evaluate their security posture, adapt to emerging risks, and recognize that preparedness is an ongoing process — not a fixed destination.



Methodology & Sources

The findings and analysis in this report draw on a combination of primary government research, peer-reviewed academic studies, and independent survey data.

Active shooter incident statistics are sourced from the FBI's annual Active Shooter Incidents in the United States reports for 2022, 2023, 2024, and 2025, published in partnership with the ALERRT Center at Texas State University, as well as the foundational study of active shooter incidents from 2000 to 2013 by Blair and Schweit (Texas State University and FBI, 2014). Venue security data is drawn from the National Center for Spectator Sports Safety and Security (NCS4) 2024 and 2026 Venue Security Director Survey and the NCS4 2023 and 2025 Spectator Safety and Security Surveys, all of which are IRB-approved research studies conducted across professional and intercollegiate sports venues in the United States. Because these studies focus on sports venues, their findings are applied to other large entertainment venues as comparable environments rather than as directly measured data. Technology adoption and threat perception data is sourced from a peer-reviewed study of professional sport venue security directors published in the Global Sport Business Journal in 2025. SAFETY Act program descriptions are drawn from DHS Best Practices in Anti-Terrorism Security (BPATS) documentation published by CCICADA at Rutgers University. Shooter Detection Systems product performance data is sourced from independent third-party testing conducted by the UK National Protective Security Authority and National Technical Systems.

Primary Sources

1. FBI Active Shooter Incidents in the United States, 2022 (published April 2023), FBI and ALERRT Center at Texas State University
2. FBI Active Shooter Incidents in the United States, 2023 (published 2024), FBI and ALERRT Center at Texas State University
3. FBI Active Shooter Incidents in the United States, 2024 (published 2025), FBI and ALERRT Center at Texas State University
4. FBI Active Shooter Incidents in the United States, 2025 (published 2026), FBI and ALERRT Center at Texas State University
5. Blair, J. Pete, and Schweit, Katherine W. A Study of Active Shooter Incidents in the United States Between 2000 and 2013, Texas State University and FBI, 2014
6. NCS4 2024 Venue Security Director Survey: IRB-approved, n=152 surveyed, 52 completed, 34.2% response rate, MLB/MLS/NBA/NFL/NHL
7. NCS4 2025 Spectator Safety and Security Survey: IRB-approved, n=728, 48 states
8. NCS4 2023 Spectator Safety and Security Survey: IRB-approved, n=400, 45 states
9. Global Sport Business Journal (2025), "Professional Sport Venue Threats": peer-reviewed, n=52 venue security directors
10. Shooter Detection Systems product, third-party testing, and certification documentation, including independent testing conducted by the UK National Protective Security Authority (NPSA) and National Technical Systems (NTS)
11. Gun Violence Archive, 2025 data
12. DHS Best Practices in Anti-Terrorism Security (BPATS) Tier III, CCICADA/Rutgers University
13. CNN (July 18, 2021), Police say 3 people were wounded in a shooting outside Nationals Park that sent players and fans scrambling during a game
14. wttw News (August 26, 2023), 2 Women Shot During White Sox Game at Guaranteed Rate Field
15. ESPN (November 24, 2015), Terror at the Stadium
16. National Mass Violence Center, Remembering Las Vegas Route 91 Harvest Music Festival
17. NCS4 2026 Venue Security Director Survey: (IRB-approved, n=74, 57% professional / 43% collegiate, MLB/MLS/NBA/WNBA/NFL/NHL/NWSL/NCAA Division I)

About Shooter Detection Systems

Shooter Detection Systems (SDS) accelerates life-saving response for organizations during active shooter incidents by delivering immediate, precise threat intelligence to security teams and first responders. By enabling responders to pinpoint the location and progression of gunfire within seconds, SDS helps reduce response time and mitigate harm.

Using multi-mode acoustic and infrared technology, edge processing architecture, and more than 50 certified integrations with existing security platforms, SDS provides highly accurate, near-instant detection-to-alert capabilities — operating with privacy at the forefront. The system enhances existing security infrastructure without recording conversations or compromising privacy.

SDS is the only manufacturer whose indoor gunshot detection system holds the highest level of U.S. Department of Homeland Security SAFETY Act Certification and has been validated by premier third-party security authorities worldwide. The indoor system is also NPSA rated and approved for government use in the United Kingdom and Australia. SDS technology also undergoes annual third-party cybersecurity penetration testing.

Trusted by Fortune 500 companies, major universities, healthcare systems, critical infrastructure operators, and government facilities, Shooter Detection Systems is an Alarm.com (NASDAQ: ALRM) company.

Shooter Detection Systems™
AN ALARM.COM COMPANY

For More Information

Visit ShooterDetectionSystems.com | Call 1-844-SHOT911