

SEPTEMBER 2026 | ACTIVE SHOOTER HANDBOOK

www.securitytoday.com

SECURITY

Technology | Education | Solutions

today

ACTIVE SHOOTER HANDBOOK

Preparing for the Unthinkable

There are few words in the security industry that immediately command attention like “active shooter.” For school administrators, teachers, parents and students, those words represent a threat that no community wants to imagine—but one that every school district must be prepared to confront.

Protecting a school campus begins long before an emergency occurs. It starts with a commitment from the entire school community—administrators, school boards, security professionals, teachers, parents, first responders and technology providers—to make campus safety a priority. Everyone has a role, and everyone must buy into the plan.

Technology is an increasingly important part of that equation. Today's schools have access to sophisticated video surveillance, electronic access control, visitor management systems, emergency communications, gunshot detection, intrusion detection and other technologies designed to identify a threat and help prevent an unauthorized person from reaching students and staff. The goal is straightforward: keep the threat outside the building and give school personnel and first responders the information they need to act quickly.

But technology alone cannot protect a campus. The most advanced security system is only as effective as the people operating it.

School staff need a clear understanding of what to do when an emergency occurs. They need training, practice and clearly defined procedures. Teachers should know how to secure their classrooms, communicate with administrators and law enforcement, and account for their students. Administrators must understand how to activate emergency protocols and communicate accurate information. Regular drills and training can help turn a written emergency plan into a practiced response.

Perhaps most importantly, school districts cannot view security as a one-time purchase. Threats change, technology evolves and school campuses change with them. Security programs must be reviewed, tested and updated regularly.

Every child who walks through a school door deserves the



Anastasia Havelia/stock.adobe.com

opportunity to concentrate on learning without having to think about the possibility of violence. Achieving that goal requires more than locked doors or cameras. It requires commitment, technology, training and a campus culture in which security is everyone's responsibility.

We may never be able to eliminate every threat. But with the right preparation, technology and people working together, we can make it much harder for a dangerous individual to reach the children we are entrusted to protect. 🚫

RALPH C. JENSEN

Editor-in-Chief, *Security Today* magazine



Table of Contents

- 3 SHOOTER RESPONSE**
Active Shooter Response: 5 Human Factors You Can't Ignore
 How human behavior can help security teams detect threats earlier and respond faster.
- 5 RETHINKING EMERGENCY RESPONSE**
Why Alerting Isn't the Same as Responding
 An alert needs to become a coordinated response.

- 7 EMERGENCY CALL**
Active Shooter Response Starts Before the Call
 Most campuses have the cameras. Far fewer have tested who can get to them.
- 9 Product Spotlights**
 A collection of threat detection technology and security solutions via an open architecture control system.

Active Shooter Response: 5 Human Factors You Can't Ignore

How human behavior can help security teams detect threats earlier and respond faster.

BY JAMES POPPER, CEO, AMBERBOX

People conceal weapons. They hesitate under stress. They seek safety before reaching for a phone. During an active shooter event, both the attacker and the people in danger may be moving through a facility in seconds. These human factors should shape how organizations approach security.

Technology is most effective when it is built around what people actually do before and during a crisis. Cameras, access control, screening, gunshot detection and emergency communications each play a role. The priority is connecting those systems to identify threats earlier, eliminate avoidable delays and accelerate response when every second matters.

1. Weapons Likely Stay Hidden Until Fired

An active shooter does not need to enter a building with a weapon in plain sight. The weapon may remain concealed until the moment it is used.

In the Secret Service's research on targeted school violence, concealed firearm transport was common among attackers who used firearms. Of 25 firearm attackers studied, 12 carried the weapon concealed in a backpack, 3 in another type of bag and 1 in a waistband. Only 2 (8%) were documented carrying firearms openly into the building after the school day had started.

That creates a critical gap. If security depends on seeing the weapon, what happens when there is nothing to see?

Screening and cameras are important layers, but security planning must account for a weapon that enters undetected. AmberBox provides an additional layer, detecting a firearm discharge without requiring the weapon to be visible or relying on

human visual confirmation.

2. Turn Detection Into Action Automatically

Detection is only valuable if it drives action.

Gunshot detection can trigger a broader security response, integrating with existing systems such as access control, mass notification and cameras. The objective is to connect detection to the systems and procedures already responsible for protecting people and facilities.

AmberBox automatically alerts designated security personnel and initiates an E911 call through its E911 certified telecom platform. A conference bridge connects key personnel directly with police dispatch, eliminating the need for someone onsite to manually initiate the response.

During an active shooter event, people should be focused on getting to safety. The security infrastructure should already know what to do next.

3. Remove the Human Delay From the 911 Call

Calling 911 sounds simple until you consider what has to happen first.

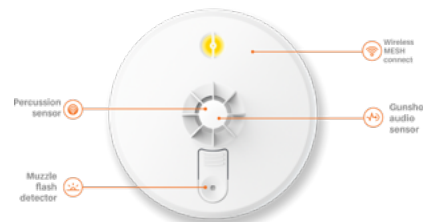
A victim or witness must recognize gunfire, understand what is happening, get to safety, access a phone and communicate the location. AmberBox response data estimates that this process takes an average of approximately 5 minutes following a gunshot.

AmberBox is designed to begin the response workflow in 3.6 seconds. The sequence includes alerts to designated security personnel, an automatic 911 call and a conference bridge connecting key personnel directly with police dispatch. No human confirmation is required to initiate the workflow.

Detection speed matters. But what matters most is how quickly detection turns into action.

4. Design Coverage for Real Buildings, Not Perfect Conditions

An active shooter can move through a facility in seconds, crossing rooms, floors and sight lines as the threat unfolds. Walls, stairwells, offices and equipment can create



coverage gaps, so detection must move at the speed of the incident.

AmberBox uses third generation acoustic gunshot detection, combining percussion and infrared sensing with machine learning sound analysis to authenticate a firearm discharge. Its detection architecture does not require line of sight and provides 360 degree detection at ranges up to 70 feet.

Coverage should reflect the building as it actually exists and how people move through it. Walls, mounting locations, floor plans and potential blind spots all matter.

5. Detect Threats Before the Gunshot

The best opportunity to mitigate a threat may come before a firearm is discharged.

Aggressive behavior, escalating verbal conflict, breaking glass and other disruptive events can signal that a situation requires attention. They do not mean violence is inevitable, but earlier awareness gives security teams an opportunity to assess what is happening and intervene when appropriate.

AmberBox Universal Threat Detection extends detection beyond gunshots to aggressive voice, glass break and blast events using the same sensor hardware. This creates a broader threat detection continuum, surfacing potential warning events, detecting a firearm discharge if one occurs and automating the actions that follow.

Effective security technology is built around the human element. The goal is to remove avoidable delays, connect detection directly to action and give security teams and first responders critical information as quickly as possible.

James Popper is CEO of AmberBox, the leading provider of gunshot and threat detection technology designed to help organizations identify threats and accelerate emergency response.

LEARN MORE:

Learn how AmberBox combines threat detection, third generation gunshot detection, automated E911 notification and integrated emergency response to help corporate offices, manufacturing facilities, entertainment venues and schools identify potential threats earlier and accelerate critical action when every second matters. Visit amberbox.com today.

Every Second Counts.

The average active shooter incident lasts 12.5 minutes. AmberBox detects and dispatches in **3.6 seconds**.



Instant detection
gunshot, glassbreak, blast,
and aggressive voice



E911-certified
alerts sent straight to law
enforcement



Real-time location
tracking for faster, safer
response

Corporate Offices • Manufacturing Facilities • Entertainment & Sports Venues • Retail

Why Alerting Isn't the Same as Responding

An alert needs to become a coordinated response.

BY JOHN STEMBEL

In an emergency, time is the most critical variable. The faster a situation is identified, communicated, and acted upon, the greater the opportunity to protect lives and minimize harm.

Yet across K-12 education, healthcare, and industrial facilities, a gap persists between when an incident begins and when the right people, with the right information, are alerted. That gap is where risk lives, and closing it has become one of the defining safety investments of the next few years.

The Problem With a Generic Alert

Most emergency communication systems, wearable or otherwise, are built around a single question: did something happen? But the more useful question is: what happened, and who needs to respond? Seconds spent interpreting an ambiguous signal are seconds not spent responding, and in a behavioral escalation, a lockdown, or a lone-worker emergency, seconds are the entire margin.

The organizations getting this right are moving toward systems built around distinct, purpose-built workflows rather than a single undifferentiated alert. Three categories tend to cover the vast majority of real-world incidents: a security or active-threat response, a medical response, and a general staff-assist response. When a system can distinguish between these at the moment of activation, rather than after a responder arrives on scene, the entire response chain moves faster, because everyone downstream, from security to facilities to first responders, knows what they are walking into before they get there. Design matters here as much as the underlying technology: physical, tactile differentiation between alert types (rather than a single

button or a counted sequence of presses) holds up better under stress, when fine motor skills are already compromised.

From Alert to Coordinated Response

An alert, however precise, is only the first half of the equation. The second half is what happens next, and this is where many systems on the market stop short.

A wearable device that simply notifies a security team or an on-call administrator has done something useful, but not the full job. The systems delivering the biggest improvements in real-world outcomes are the ones that treat the badge as a trigger for a coordinated, building-wide response: automated lockdown messaging, audio announcements over existing PA infrastructure, visual alerts, and two-way communication, activated automatically, without a person having to relay instructions between systems. For facilities that already operate paging, intercom, or IP-speaker infrastructure, this is a meaningful distinction: does the alert integrate with what you already own, or does it require an entirely separate, proprietary layer of hardware to deliver a coordinated response? Buyers evaluating these systems should ask vendors directly what happens, second by second, in the first ten seconds after activation.

Reliability Can't Depend on the Network Being Fine

Consumer Wi-Fi and cellular networks tend to fail at precisely the moments emergency systems are needed most: power outages, building-wide incidents, or simple network congestion during a large event. A wearable system that depends on either has a built-in failure point.

The more resilient architectures combine multiple independent layers, often Power over Ethernet, long-range low-power wireless (LoRaWAN), and cellular backup, so that no single point of failure takes the system offline. Coverage matters just as much as network type: incidents in K-12 settings, for example, disproportionately happen outside classrooms, in hallways, parking lots, and athletic fields, areas that a system optimized only for "building coverage" may miss entirely.



Extending Response Beyond the Building

Internal coordination is necessary but not sufficient. The organizations closing the response gap most effectively are also connecting their internal alert systems to external emergency response networks. Platforms like RapidSOS allow enriched incident data, including location, alert type, and relevant context, to reach 911 dispatch directly, rather than relying on a verbal call after the fact. That connection can meaningfully reduce dispatch time and give first responders a clearer picture before they arrive.

A Framework, Not a Feature List

For safety leaders evaluating this category, the takeaway isn't a single feature to look for. It's a set of questions. Does the system tell responders what happened, not just that something happened? Does it activate infrastructure you already own, or force you to install a new one? Does it keep working when the network doesn't? And does it extend past your walls to the people who dispatch help? Vendors answer these questions very differently, and the gap between "good on a demo" and "good under real stress" usually shows up in the details.

AtlasIED's Rapid Alert wearable badge is one system built around this thinking, with dedicated workflows, native integration with existing facility infrastructure, and independent network architecture, but the questions above are worth asking of any system under consideration. 📍

Jon Stembel is product manager, security products at Atlas IED

LEARN MORE:

Learn More About How the Rapid Alert wearable security badge gives responders the context they need before they arrive. Three dedicated buttons for lockdown, medical, and security mean no guessing, no ambiguity, just a clear signal in a moment that matters. <https://www.atlasied.com/rapid-alert-wearable-badge>



RAPID ALERT

WEARABLE SECURITY BADGE

ONE PRESS. A MORE INFORMED RESPONSE.

LOCKDOWN | SECURITY | MEDICAL

Staff can request the help they need - no phone, app, or Wi-Fi required.

Rapid Alert gives safety teams real-time situational awareness:
who needs help, where they are, and what response is required.

SEE RAPID ALERT IN ACTION



Tell me more

Atlas IPX
An AtlasIED Brand



Check us out at [AtlasIED.com](https://atlasied.com)
or engage with us on your
favorite social media platform

Active Shooter Response Starts Before the Call

Most campuses have the cameras. Far fewer have tested who can get to them.

BY WILL BROCK

Why the first request for video costs more time than it should

Cameras cover entrances, corridors, parking structures, and residence halls. Large districts may operate thousands of them across more than a hundred buildings. When an officer arrives on campus and needs video, the question is rarely whether the footage exists. The real question is how many people stand between the officer and access to it.

In a traditional response, the officer contacts campus police or security, who then reach out to a security operations center, system administrator, or IT staff member with access to the video management system. The process works, but every handoff costs time and the chain is being assembled while the incident is still unfolding.

The most direct solution is to remove those handoffs and give authorized responders a secure way to access the video themselves.

What “first responders have access” actually means

Campuses often use the same language to describe responder access while meaning very different things. At one campus, a responding agency has pre-authorized entry through a federated system. At another, an officer calls the security operations center and asks an operator what is on screen. Both provide information, but only one delivers a true operational capability.

What separates them is a handful of details that look minor until they matter. Credentials that expired. Permissions nobody finalized. Software that is not installed

where it is needed. Connectivity that was restricted for good reasons and never revisited. A procedure the people expected to use but have never practiced.

“The middle of a critical incident is not the time to install software, exchange credentials, determine permissions, or decide who is authorized to see what,” says Will Brock of Salient.

Who decides what an outside agency can see

The most common failure is not a permission set that is too restrictive or too broad. It is a decision nobody finished making. Campuses devote significant effort to securing video internally, yet outside responder access often remains an unresolved policy question, until an emergency forces an answer under the worst possible circumstances.

A mature approach settles it in advance through role-based permissions: which agencies may connect, which users are authorized, which cameras or facilities they may see, under what circumstances, and how that activity is logged and audited. Correlating video with access-control events belongs to the same discipline, catching a propped door while it is still a maintenance issue rather than a security one.

“Technology can enforce those decisions, but it cannot make them,” says Brock. “Campus security, IT, legal or risk management, and the responding agencies need to establish the policy together.”

Why responders should not need to know your camera names

Even with permissions settled, dispatch describes a location the way people do. The northeast stairwell by the library. The east hallway. Camera lists often describe that same place as a drop number or an installer’s shorthand, and under pressure someone must translate between the two.

The solution is not simply a better naming convention, although consistent naming still matters for maintenance and investigations. It is a system that does the translating. Mapping places cameras



at their real locations with fields of view drawn in, so an authorized user can find the reported area, hover for a live thumbnail, and pull the view forward without knowing what anyone called it.

Thousands of cameras offer little value when the three that matter take minutes to find.

How to find out what will fail before it matters

Scheduled drills test the parts of a plan everyone knows are being tested. A more useful exercise measures the path from request to usable video. Give a responder a location and start the clock. Do the credentials work? Are the permissions, right? Can the user find the area without help? Can they move to adjacent views as the situation changes?

Failures are usually human, not technical. When access depends on one administrator being reachable, that is a single point of failure, not a procedure.

“The purpose of the exercise is not to prove that the system works; it is to discover what will fail while there is still time to fix it,” says Brock.

What a week of work can change

None of those failures needs new hardware to fix. In a week, a campus can bring security, IT, dispatch and the primary responding agency into one room, verify credentials and connectivity, confirm that maps reflect where cameras actually are, and run the timed scenario once. Whatever breaks becomes the priority list. That work will matter more in the first ten minutes of an incident than another camera nobody can find. 

Will Brock is Regional Sales Manager for the Mid-South at Salient Systems, where he works with integrators and end users across the Carolinas and Tennessee.

LEARN MORE:

Salient’s CompleteView VMS serves schools and campuses nationwide, unifying video with access control, analytics, and detection sensors so education and security teams can detect concerns early, respond faster, and review what happened afterward. salientsys.com/industries/k-12-higher-education

VIDEO MANAGEMENT SOFTWARE

Your Security Environment Evolves. Your Video Platform *Should Too.*



Simple

Using your existing cameras, servers, and networks drastically reduces friction of adoption.



Scalable

Centrally manage across sites, scale to operate from anywhere, at any time with our cloud solution.



Flexible

Unlock relevant insights by extending our platform with integrations to drive your operations.



Whether you run one site or a few hundred, you get the same view of your video and the same control over it.

Built on open architecture, CompleteView VMS delivers universal integration, intuitive operator clients, centralized control from a single login, and hybrid cloud services. And with Enhanced Search, investigators search by a person's appearance, clothing, or vehicle type across every compatible camera at once—results in seconds, not hours.

salentsys.com



SALIENT



Scan to see CompleteView
in action



Yury/stock.adobe.com



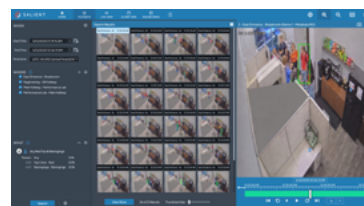
AMBERBOX GUNSHOT DETECTION THIRD-GENERATION TECHNOLOGY WITHOUT LINE OF SIGHT

AmberBox is the leading provider of gunshot and threat detection technology. Leveraging third generation technology, combining percussion, muzzle flash, and machine learning audio sensors that require no line of sight. Detectors mesh wirelessly to automatically alert 911 and security teams within 3.6 seconds. Trusted by Fortune 1000 companies, sports venues, campuses and airports nationwide.
amberbox.com



ATLASIED WEARABLE SECURITY BADGE FOR RELIABLE EMERGENCY REQUEST

The AtlasIED Rapid Alert wearable security badge gives staff and visitors an easy, reliable way to issue an emergency lockdown or request medical or security help anywhere on campus with no phone, app, or Wi-Fi required. Three buttons, three workflows = more informed and effective responses.
<https://pages.atlasied.com/rapid-alert>



SALIENT OPEN ARCHITECTURE CONNECTS THOUSANDS OF CAMERAS

CompleteView's open architecture connects thousands of cameras, access control systems, and analytics, so you can view, record, manage, and search your video in one place. Enhanced Search adds a search layer built on metadata generated at the camera level and indexed within CompleteView's Event Service, delivering faster investigations without significant changes to your existing infrastructure.
<https://www.salientsys.com/products/completeview/>

SECURITY today

Cutting-edge **INDUSTRY NEWS** & the latest
PRODUCT INFO delivered right to your inbox.

Subscribe to our eNewsletter at

securitytoday.com/enewsletter

