

SECURITY EXECUTIVE™

YOUR TRUSTED RESOURCE FOR SECURITY AND RISK EXECUTIVES

JULY/AUGUST 2026

**SPECIAL SCHOOL
SECURITY FOCUS:**
Why School Security
Must Start with the
Fundamentals

PAGE 28

**Beyond Locks
and Keys: Why
Access Control Is
the Foundation of
School Safety**

PAGE 33

**When AI Learns to
Lie: The New Era of
Campus Phishing**

PAGE 38

**Tomorrow's Threats
Demand Today's
Smarter School
Security**

PAGE 60

SPECIAL SECTION:
2026 Security
Innovations Awards

PAGE 30

AI + School Security

As AI threat detection spreads through K-12 security faster than anyone can evaluate it, the answer from the people building and deploying the technology is more layered than any single case would suggest.

Can AI Technology Really Stop School Violence **Before It Happens**



An AI detection system in one district identified six real firearms, while a similar system in another district mistook a bag of chips for a weapon and brought police in with guns drawn. As AI threat detection spreads through K-12 security faster than anyone can evaluate it, the answer from the people building and deploying the technology is more layered than any single case would suggest.



Montgomery County, Maryland's chief safety officer wrote to families at three pilot high schools, Seneca Valley, Bethesda-Chevy Chase and Magruder, on Feb. 8, 2026, describing a short trial period of an AI-powered weapons detection system. The next day, a 16-year-old brought a gun into [Thomas S. Wootton High School](#), a fourth school in the same district that wasn't part of the pilot and shot a classmate. The timing was coincidental, but the questions it raises are not.

Within just a few years, AI threat detection has moved from a novelty discussed at trade shows to something districts feel they can no longer ignore. Ask the people who build and sell these systems and live with the consequences when they succeed or fail, and the answer to whether AI tools actually work is far more layered than any single case makes it look.

This isn't a story about whether AI belongs in school security, since it's already there and expanding faster than most districts can evaluate it; it's a story about what the technology can and cannot currently do, and why the security professionals closest to it keep arriving at the same conclusion from different directions: that the technology was never the variable that mattered most.

NINETY-THREE PERCENT OF SCHOOLS ALREADY WATCH

Ninety-three percent of U.S. schools already have security cameras, according to [National Center for Education Statistics](#) data, a number that has held steady for years and suggests cameras were never really the problem; camera use is widely accepted. The gap security leaders are working to reduce now is the distance between recording an incident for forensic use and proactively detecting an event as it unfolds, and that's where AI has potential. A May 2026 [EdWeek Research Center](#) survey found roughly a quarter of districts now use AI-enabled camera monitoring to flag weapons or physical altercations, a sharp jump from a few years ago.

Daniel Young, founder and chief innovation officer at [Circadian Risk](#), frames AI's value through what he calls the three Ds and three Rs: deter, detect, delay, then respond, report, recover. In his view, AI's most defensible role sits early in that sequence, since proactive security doesn't start inside the building.

"You can't start within the building," Young said. "These individuals have to get to the door. If you're using AI, it needs to be on analytics cameras, on devices where we can actually see these things happening quickly. Catching potential problems from the perimeter inward is key, because the average response time to an active shooter event is under three minutes, so the quicker the detection and response, the less

severe the outcome tends to be.”

Ron Self, director of strategic initiatives at CENTEGIX and a former district end user of the company’s alert platform, measures smart tool use and success from his company’s own data. Drawn from more than 346,000 alerts across 18,000-plus locations in the 2025-2026 school year, CENTEGIX found that 99% of events were everyday emergencies rather than campus-wide threats. Medical events, behavioral incidents, and student elopement were the top concerns.

“The real question districts should be asking isn’t just, will this work during an active threat,” Self said. “The question is, will our staff actually use this technology every single day, and will it also work when the worst day comes?”

Another dimension to this issue is that in the face of rapid deployment and constant innovation, governance hasn’t kept pace with the topic. ASIS International, for example, published its first [School Security Standard](#) within the past year and is already revising it, while the Security Industry Association’s [2026 K-12 School Security Symposium](#) brought vendors, administrators and law enforcement together to work through how the standard fits alongside other frameworks, a sign that deployment is outpacing any shared understanding of how to deploy AI-powered tools effectively and responsibly.

WHEN IT WORKS, AND WHEN IT DOESN’T

The clearest way to understand where these systems succeed and fail is through the incidents themselves, which are mixed enough to unsettle anyone looking for a simple verdict.

A 17-year-old shot and killed a 16-year-old student at [Antioch High School in Nashville](#) in January 2025, after the district’s system failed to identify the weapon. Investigators

attributed the failure to the camera’s positioning relative to the shooter, rather than a flaw in the underlying model. [Nashville Public Schools](#) responded by installing a similar system districtwide, and by March 2026, those systems had detected at least six guns, evidence supporting that the technology can work when positioning and coverage are optimal.

The news cuts the other way in Baltimore County, where a system flagged a [Kenwood High School](#) student’s hand movement while he held a bag of chips as a possible weapon and police responded with guns drawn. A subsequent [inspector general review](#) cleared the system of bias but recommended additional staff training before alerts reach a response team, and in the same report, a security official in a neighboring district running the same system said his program has recorded zero false positives of that severity, crediting the difference to routing alerts to trained security staff rather than building principals.

Even so, the security professionals interviewed for this article don’t see these incidents as evidence that AI doesn’t belong in schools. Guy Bliesner, a school safety and security analyst for the state of Idaho and a founding board member of the [National Council of School Safety Directors](#), arrived at the same conclusion as Young and Self: detection without human verification and follow-through is where these systems break down, not the underlying pattern recognition itself.

“We [schools] do not have an eye in the sky. We don’t have a bunch of people sitting in a room looking at monitors with a radio ready to call out a response team,” Bliesner said. “With many of these false positives, the data may not have been reviewed properly before they decided to call out the cavalry. If we rely solely on AI, it’s like relying solely on a fire alarm system. We get

spurious fire alarms fairly regularly. It doesn’t mean that the system necessarily failed.”

THE OTHER AI

Despite covering different corners of school security, all those interviewed for this article arrive at the same conclusion: the technology is meant to amplify people, not replace them. Bliesner has made that case publicly for years, including to a room full of vendors at the ISC West trade show, where he argued that most of what they sell isn’t a solution at all.

“Security integrators do not provide solutions,” Bliesner said. “They provide tools that, when effectively used to address an identified threat, may be a solution. Most school security failures are human, not equipment, failures. Stuff doesn’t keep schools safe. People keep schools safe.”

That thesis has a name Bliesner has written about under his own byline: the other AI, or “active involvement,” a phrase he uses because the human element mattered in school security long before artificial intelligence did.

Daniel Young makes the same point from the risk-management side of the business. In his experience, the schools with the most impressive countermeasures on paper aren’t necessarily the safest ones.

“The countermeasures, the ones with the best countermeasures, aren’t going to be the winning culture or the winning organization,” Young said. “It’s going to be the organization that understands its risk the best. We look at schools, even the most recent events, and they have countermeasures in place already, and we’re still seeing school shootings. It’s not necessarily a technology issue; it’s a culture issue; the recognition that these tools are there for a reason.”

AI’s real value, in his view, is filling

that gap for people who were never trained to spot threats, much like how an untrained observer might walk right past a health emergency that a doctor would recognize instantly.

“Individuals who are not trained to see that type of thing, and the expectation that they should be aware of it, are two entirely different things,” he said. “That’s where AI can help, amplifying our thought process to an individual who doesn’t have that insight and training.”

Ron Self sees the same balance play out at the product level. The systems he works with were built around a badge a staff member presses to summon help, with AI-triggered detection layered on top of that human step rather than replacing it.

“In a crisis, the person closest to the incident is still the fastest and most reliable sensor in the building,” Self said. “Human intuition and AI technology are not competing



Ninety-three percent of U.S. schools already have cameras. Roughly a quarter of districts have now adopted AI tools designed to detect an incident as it unfolds.

philosophies. They are complementary layers. The AI never gets tired and it never hesitates. A human operator never gets fooled by context. By bringing them together, we close the safety gaps that either one would have if left completely alone.”

Geva Barash, whose firm [Secure Our City](#) designs low-voltage security systems for schools and public safety facilities, pushes the same idea further still, arguing that most people think of school AI as cameras and little else.

“AI is not just for security cameras,” Barash said. “Take a look at the IT racks. You’re using smart tools that leverage analytics to

secure your data, and they learn your data usage patterns so they can notify you of any irregular activity or breaches. AI is used in data protection, device protection, and so forth. We now use vape sensors in many of the schools we work with, and they provide about 30 different readings on air quality, temperature, and the presence of smoke or vaping. There’s definitely a lot of opportunity in schools for the use of AI.”

THE LINE DISTRICTS ARE RELUCTANT TO CROSS

Barash’s most counterintuitive finding from his work with districts is that privacy, in the broad sense, is



Enterprise Security Risk Management

Kroll’s Enterprise Security Risk Management practice provides expert guidance and advisory services to our global clientele as they navigate the most challenging and emerging security and threat-related issues.

Contact one of our experts today QR Code:



rarely the sticking point.

"Privacy is not a major issue," he said. "All the schools have cameras. It's more of a question of whether they're willing to do facial recognition, and how deep they want to use the information they have."

He's taken that same distinction directly to lawmakers, testifying before the Connecticut General Assembly on a proposal to use facial-recognition technology in a public-safety building. He told the room there were no photographs involved, no images stored anywhere, then turned the question back on the assembly members themselves by asking how many of them had a campaign photo on their website, or their own face on a yard sign at election time? Every hand went up.

"So, you're okay with your face being everywhere," Barash told them, "but the one place that doesn't have your face, and lets me recognize you coming in and open the door for you automatically, that's not okay?"

That same split in perception shows up nationally in a patchwork of conflicting laws: New York has moved toward a moratorium on biometric surveillance in schools, while Georgia's HB 268 goes in the opposite direction, mandating panic-alert systems and formal threat-assessment teams. Districts operating across state lines are left to navigate that patchwork with no consistent guidelines, and even when a state does weigh in, the law doesn't settle the harder, day-to-day questions for them.

Self, who has helped hundreds of districts work through their own data retention and privacy decisions, said the variation runs deeper than state lines. No two districts land in the same place, he said, even within the same state.

"If you've seen one school, you've truly only seen one school," he said.

"They each function as their own unique ecosystem." His advice is to start with the people who will actually respond, not a compliance checklist: "There's no need to reinvent the wheel here. There are plenty of ready-to-use resources and blueprints districts can customize for their exact workflow."

WHAT COMES NEXT

The standards effort that began with ASIS's first School Security Standard is already moving into a revision cycle less than a year after publication, and Young has floated the idea of a national compliance index to track how many districts actually meet the standard's baseline requirements, rather than simply buying technology and assuming compliance follows.

"We need to know how many schools are actually complying with the must-have standards," Young said. "It would give us a good sense of where we need to improve."

The [Partner Alliance for Safer Schools](#) is a third major framework districts and security professionals can lean on, alongside ASIS and SIA. PASS released the seventh edition of its free Safety and Security Guidelines this spring, and its July Summer Summit is running a session specifically designed to show districts how to use the two frameworks together: ASIS for overall risk management, PASS for hands-on steps at the campus level, evidence of how much coordination this space still needs.

Bliesner brings a facilities-and-funding lens to the same question, tracking where state and federal security dollars are landing relative to what the incident record suggests should be prioritized, and he's blunt about the mismatch.

"In many cases, we're giving people the security house, or the roof to their security house, when they have no foundation," he said,

pointing to schools where duress panic systems have been mandated even as basic classroom door locks remain unreliable.

THE QUESTION THAT MATTERS

Three threads run through this story, and none cancel the others out. The modest, defensible take is that AI threat detection hasn't yet proven itself either way. It's a tool, and its value depends entirely on the discipline of the humans running it. Technology itself will keep improving, but likely faster than the training, verification protocols, and the use standards built around it.

The sharper take, echoed independently by more than one source in this piece, is that the real story was never AI versus no AI but culture versus countermeasures. A district that buys detection technology without investing in the human systems around it is buying a false sense of security.

And the forward-looking take is that the standard-setting happening right now through ASIS, SIA, PASS, and a growing patchwork of state legislation is racing to catch up with deployment that has already outpaced it. The next few years are likely to determine whether AI threat detection becomes a mature, governed practice or a cautionary case study. ▣



Howard Carder is a seasoned freelance writer specializing in the physical security and professional audio/video industries.

With over 30 years of experience, including a long tenure at a large, global video security company, Howard has crafted compelling content for leading brands and publications across the industry. His expertise spans video security and Pro AV technologies, allowing him to distill complex topics into engaging narratives. Howard's work includes hundreds of case studies, white papers, and thought leadership articles. When not writing, he enjoys playing music and exploring healthy cooking. Learn more at www.hcwriter.com.