SIA
SECURITY INDUSTRY ASSOCIATION

Perimeter PREVENT

Takeaways From Perimeter PREVENT 2025

Lessons, Tactics, Strategies And Insights From The Premier Event In Perimeter Security

3B PROTECTION
BALLISTIC / BLAST / BREAK-IN

CORNING

Databuoy

ECHODYNE

evolon

GIBRALTAR
the power of innovation

GLOBAL GRAB
We Exist To Protect.

HERCULES HHS
HIGH SECURITY

HEXAGON

ISC

MOTOROLA SOLUTIONS

NASATKA SECURITY

oosto
Vision AI for Good

PureTech SYSTEMS
AUTONOMOUS AI-BOOSTED AWARENESS

smartPerimeter.ai

UTILITY Security

In June 2025, the Security Industry Association (SIA) hosted Perimeter PREVENT – a high-impact event focused on the critical issues related to perimeter detection, alerting and defense. More than ever, perimeter security requires layered and strategic approaches. This event, developed with guidance from SIA's Perimeter Security Subcommittee, shared expert insights on these strategies and how to apply them to high-value environments including government and commercial facilities, critical infrastructure, data centers, public events and more.

At Perimeter PREVENT 2025, top corporate security leaders gathered in Washington, D.C., with government security personnel, specifiers, engineers, system integrators and solutions providers for an all-day symposium featuring educational presentations, networking opportunities and an open forum to present questions and ideas. Here are some of the key takeaways from this year's event:

PERIMETER SECURITY DESIGN

- Perimeter security is moving from more of a reactive stance to a proactive, layered one that "deters, detects and denies."
- It's important for facilities to have a strategy upfront that can support the long-term security goal. While not every layer and technology needs to be installed on day one, the strategy must be scalable and nimble so that as new threats come, the facility can address them.
- Facilities must consider from the beginning: Who is the target, what are you protecting against and who are the potential actors that could break into your site?
- Emerging technologies and trends in perimeter security include artificial intelligence, which will become more of a player in the video space over the next few years, and environmental sensors, which will expand in their use cases across different verticals on the inner part of the perimeter.
- There is a shift toward selling open solutions, open APIs and not being as proprietary in the industry.

SECURING SPORTS AND LARGE EVENTS

- Securing large events, like sports games and tournaments, formerly was focused on "guards, gates and guns" and addressing local, physical and predictable threats, but this sector has shifted in the wake of an evolving threat landscape that now includes things like cyberattacks, drone incursions, vehicle attacks and misinformation campaigns designed to incite panic. Today's events face a wide range of threats, each bringing a new layer of planning and personnel, and no single layer of security is sufficient.
- Major events need to be treated like "temporary cities," and technology and security should be designed into the planning and operations.
- When securing a large event, it is important to first assess which threats need to be defended against and then develop a layered approach to address them (which could include elements like screenings, fencing, cameras layered with artificial intelligence to detect unusual activity, hostile vehicle mitigation to protect queue lines, K-9 dogs to detect explosives and other suspicious materials and/or prescreening of authorized vehicles).
- Perimeter security today isn't just physical defense – it's a living system, and cybersecurity and physical threats need to be monitored side by side.

> Today, the perimeter is virtual, dynamic and constantly shifting.
>
> — **Cathy Lanier**, *chief security officer, National Football League (NFL)*

ENHANCING DATA CENTER SECURITY

- Data center security is critical to build in from the start, and what is needed to effectively protect a facility varies by site. There is a shift to performance-based specifications that address the security needs of each site.
- It's important for security professionals to think about how they design security into the network and leverage the infrastructure already in place.
- The way sites integrate into their communities is critically important. One aspect of this is the visual impact of perimeter security of these sites and using design principles like crime prevention through environmental design.

INTEGRATING SECURITY FOR POWER COMPANIES

- As the power grid becomes more interconnected and reliant on digital technologies, these risks intensify. Protecting power facilities includes leveraging integrated security systems that combine physical and cybersecurity measures for comprehensive protection, including video surveillance, access control, intrusion detection and cybersecurity threat monitoring.
- Power sites face a variety of threats every day, such as disgruntled customers when their power is off, foreign threat actors and people breaking in to steal copper. Each of these threats must be considered and mitigated differently, and substations require around-the-clock security, which comes with security personnel and staffing needs.
- Access control strategies for power companies include a layered approach, with outer perimeter technologies like vehicle deterrence systems and physical barriers, inner perimeter technologies like credential-based access control, biometric authentication systems and visitor management systems and security personnel like guards at entry points and mobile patrol units.
- Utilities providers do a great deal of reporting and information sharing in order to effectively coordinate with stakeholders like law enforcement and responders. Power companies do training and drills with law enforcement so that they can protect critical infrastructure and safely respond in the event of an incident.

> We have to put in as many layers [of protection] as possible.
>
> — **Sam Queeno**, *director of security, American Electric Power Company*

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

- CPTED principles focus on clearly defining property boundaries and limiting access points through features like fencing, lighting and landscaping to make potential intruders easily visible and discourage entry. Key principles include natural surveillance, natural access control, territorial reinforcement and maintenance.
- CPTED can include things like prioritizing calming colors, installing public art and traffic circles and can vary in different communities due to different communities' preferences and cultures.
- CPTED can deter crime because when an environment is designed and manicured, it appears harder to get away with crime or negligent activity.
- There are differences in how these principles are applied globally. ISO Standard 22341 provides guidelines for establishing basic preventive measures through environmental design.

> All it takes is one technology to fail and then [someone] can breach the facility. So what CPTED does is take all the layers and add more layers beyond that – an additional means to deter and delay.
>
> — **Mark Schreiber**, *principal consultant, Safeguards Consulting*

SAFETY ACT RECOGNITION FOR PERIMETER SECURITY

- The U.S. Department of Homeland Security's (DHS) Support Antiterrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) is a powerful but underutilized statute that offers substantial liability protection to companies deploying qualified antiterrorism technologies and encourages the innovation, deployment and procurement of these technologies.
- Going through the SAFETY Act process and earning SAFETY Act certification and/or designation allows products to be truthfully marketed as antiterrorism products and encourages security companies to build products toward that direction, driving investment and meeting duty of care – a win-win for protecting the public and protecting sellers and facilities from liability.
- The Federal Acquisition Regulation requires government projects to consider SAFETY Act-designated products, giving those providers a competitive advantage.
- SAFETY Act protection eligibility has evolved from just security products to include service providers, integrators, venues and facilities. Eligible product categories include countersurveillance security officers, explosive detection canine teams, crash-rated bollards, sensors, access control, ID credentialing, drone and counter drone technologies, surveillance cameras, crash-rated wedge barriers and more. Facilities that earn SAFETY Act designations include multiuse campuses, data centers, stadiums, malls, government facilities, hospitals, theaters, colleges and universities, museums and residential facilities.
- Find more information and resources on SAFETY Act certification on the DHS webpage.