2026 REPORT:

The State of Emergency Response and Monitoring

Closing the Gap Between Security and Automatic Safety

NOONLIGHT

Security customers — from homeowners to global enterprises — expect more than standalone products. They want unified systems that deliver situational awareness, protection, and operational efficiency without the burden of stitching together multiple platforms.

In 2026, the competitive edge will belong to those security providers who deliver seamless, scalable solutions under a single brand.

2026 Security Megatrends Report
Security Industry Association (SIA)

The global security industry is at a critical inflection point. Two forces are driving the shift: an overwhelming volume of digital alerts and a growing crisis of false alarms.

Security system owners expect fast, accurate responses when it matters most. But when systems generate nuisance alerts instead of real threat validation, the value of monitoring erodes. False alarms drive customer churn, strain public safety resources, and contribute to widespread alarm fatigue among emergency responders and end users.

In a world saturated with data, the defining challenge for security providers in 2026 is not collecting more information — it is converting meaningful signals into decisive threat prevention and life-saving action.

Despite major advances in technology, many providers still fall short. Tools have improved, but service models have not evolved at the same pace. The result is a widening gap between detection and response.

Closing that gap requires a strategic shift:

- **Leverage Intelligent Automation:** Deploy AI and video verification as frontline filters to reduce false alarms, apply context instantly, and identify genuine threats before human intervention is required.
- **Elevate Verification as a Core Capability:** Transform monitoring agents into true extensions of emergency response by filtering nuisance alerts, validating incidents quickly, and enabling decisive escalation when a real threat emerges.
- **Prioritize Actionable Outcomes Over Raw Data:** Move beyond alert generation to systems that filter noise, apply context, initiate deterrence, and transform signals into fast, reliable emergency response — restoring trust in monitored security.

Four Major Trends Reshaping Security Operations

These pressures are accelerating a shift away from reactive, alarm-driven systems toward a more intelligent, response-oriented security model. Traditional monitoring frameworks — built to detect and notify — are no longer sufficient in an environment defined by scale, speed, and escalating risk.

Security operations are being re-engineered in real time. Automation is moving to the forefront. Artificial intelligence is becoming the primary filter. Human expertise is being redefined. And platforms are consolidating into more unified, scalable architectures.

Together, these trends are redefining the operating model for modern security organizations:

1. **The Shift Toward Automated Safety**
2. **The AI-Driven Frontline**
3. **The Indispensable Human in the Loop**
4. **The Rise of Proactive Safety Ecosystems**

1 The Shift Toward Automated Safety

Security customers now expect systems to do more than detect threats — they expect action. Whether protecting people, assets, or property, demand is rising for intelligent security solutions that deliver proactive, instant, and reliable protection with minimal disruption.

In a hyper-connected world, customers are overwhelmed by the volume of alerts generated by traditional security systems. Rather than forcing users to make immediate, stressful decisions, modern security solutions must intelligently filter data, apply context, and enable autonomous responses across devices and environments.

However, this value is quickly undermined when systems generate false alarms. According to data from Parks Associates, the activity-based security model is driving customer attrition — 35% of users cancel monitoring services because of false alarms or because they believe their systems are unreliable when they need them most.

And, with at least 72% of U.S. homeowners now using some form of home security, providers must meet these expectations to retain customers and remain competitive.

The pressure extends well beyond residential security. Enterprises are facing increasing operational complexity, larger attack surfaces, and escalating financial risk from criminal activity.

Retail shrink alone accounts for more than $100 billion in annual losses in the United States, while equipment and tool theft exceeds $1 billion, and workplace violence contributes more than $130 billion in annual costs. To combat these mounting financial and security risks, organizations can no longer rely on legacy infrastructure or traditional monitoring systems to protect their people and their property.

In response to these pressures, security leaders are turning to artificial intelligence to power the next generation of safety systems. AI is now becoming the primary operational engine for security defense. Industry reporting from Research & Metric notes that the future of security depends on autonomous AI agents capable of processing massive volumes of data to identify anomalies and trigger automated response actions faster than human operators alone can achieve.

2 The AI-Driven Frontline

If AI is becoming the engine of automated safety, it is also emerging as the operational frontline of modern security defense. The industry is undergoing a fundamental shift from passive detection to proactive prevention — an era often described as posthuman automation, where intelligent systems increasingly augment and, in routine monitoring scenarios, replace manual oversight tasks.

Artificial intelligence has matured into a foundational defense technology. According to the Security Industry Association (SIA), AI is increasingly serving as an active defender within modern security architectures, capable of autonomously managing portions of the deterrence and response process.

When a threat is detected, AI-driven systems can automatically initiate countermeasures — such as activating lighting systems, tracking suspect movement, broadcasting audio warnings, and notifying security personnel — often before a human operator reviews the event. In this role, AI acts as a critical first filter, helping address the persistent challenge of false alarms while improving response speed and operational efficiency.

This capability is driven by the rise of agentic AI systems, which can process massive streams of video, sensor, and behavioral data in real time to identify anomalies and escalate verified threats. As security environments become more complex and data-intensive, AI is becoming a necessary layer of defense infrastructure, managing scale and speed that human monitoring teams cannot reliably match alone.

Advanced applications such as AI person detection can automatically analyze video streams to filter out events where no human presence is detected, significantly reducing non-actionable alerts. To improve verification accuracy while preserving privacy, providers are also adopting non-visual intelligence models, including radio frequency (RF)-based AI systems that use Wi-Fi and Bluetooth signals to verify the presence or absence of people in a monitored environment.

By automating initial verification and deterrence workflows, AI transforms traditional monitoring systems into active defense platforms. When combined with human operators who provide real-time oversight, judgment, and escalation coordination, this hybrid model moves the industry closer to delivering fully verified, automated safety outcomes.

3 The Indispensable Human in the Loop

As AI assumes a greater role in detection, verification, and deterrence, the role of human operators is not diminishing — it is evolving. The future of security is not defined by replacing human judgment, but by elevating it into higher-value response and decision-making workflows.

Even as agentic AI acts as a powerful force multiplier capable of achieving high false-alarm filtering rates, human expertise remains a premium capability required to deliver reliable and trusted security outcomes.

AI excels at filtering noise and managing routine automation at scale. However, it continues to struggle with nuanced human context and high-stakes judgment scenarios — such as a person breaking into a construction site as opposed to a worker coming to work 10 minutes early. Security environments often require emotional intelligence, situational awareness, and contextual reasoning that technology alone cannot reliably replicate.

As a result, humans must remain in the loop for complex, ambiguous, or high-risk situations. Human operators play a critical role in validating threats, escalating confirmed emergencies, and providing the emotional reassurance customers expect during crisis events. This combination of technological speed and human judgment is becoming a defining characteristic of modern security services.

This shift also changes how security professionals perform their work. Rather than passively monitoring video walls, operators are becoming proactive response coordinators who use real-time intelligence to anticipate threats and intervene before incidents escalate. This hybrid model directly aligns with growing customer expectations for reliable service outcomes. According to SafeHome.org's 2025 report, professional monitoring remains the most important factor influencing consumer security system adoption decisions.

However, this demand is conditional. Customers do not value monitoring simply as a service — they value monitoring when it produces verifiable, positive outcomes. The security industry is responding to the growing churn risk associated with unreliable monitoring models by embedding human expertise directly into AI-enabled workflows.

Human agents can leverage verified AI insights, assess real-time threat data, and coordinate direct response actions, transforming security services into proactive, outcome-driven safety platforms that improve response speed, accuracy, and overall business value.

4 The Rise of Proactive Safety Ecosystems

As AI and human operators converge into hybrid response models, the security industry is also undergoing a broader structural transformation. The future of security is not just about intelligence or response speed — it is about building integrated safety ecosystems capable of delivering end-to-end protection at scale.

Historically, the security industry has been fundamentally reactive, triggering alarms only after a perimeter breach has already occurred and damage or harm may have taken place. Despite advances in detection technologies, many legacy providers continue operating under this “after-the-fact” security model.

Today, however, a new safety ecosystem is emerging at the intersection of cloud software, real-time intelligence, and verified emergency response workflows. This shift is transforming security from passive monitoring into proactive protection, allowing providers to close the gap between detection and real-world response.

According to SIA’s 2026 Megatrends report, security integrators must now offer at least one end-to-end solution in their portfolio — and the future will belong to providers capable of delivering seamless, scalable safety solutions under a unified brand.

At the foundation of this ecosystem is a shift away from fragmented, on-premises hardware toward flexible, cloud-based software and API-driven platforms. These architectures enable plug-and-play security technologies, including cameras, sensors, and mobile safety devices. Together, a unified experience layer is created integrating video monitoring, access control, and environmental sensing into a single operational view, breaking down security silos and making advanced capabilities accessible across enterprise and consumer environments.

Building on this infrastructure, modern security systems leverage AI to move beyond passive recording toward active deterrence. When threats are detected, AI-driven systems can automatically secure environments by initiating audio-visual warnings and locking doors to discourage escalation. In parallel, human agents can use real-time video analytics and integrated tools to conduct talk-down interventions, monitor situations, and coordinate emergency response communications.

Ultimately, the convergence of cloud infrastructure, real-time insights and human verification is transforming how security providers deliver value. Rather than simply transmitting alerts, modern safety platforms are delivering core customer expectations: reduced disruption, faster verified response, and measurable safety outcomes at scale.

Noonlight: The Infrastructure Powering Automated Safety at Scale

The security industry is evolving quickly — from reactive monitoring to proactive, verified protection. Providers who act now can address rising customer expectations, escalating threats, and the operational challenges of managing real-time alerts to deliver holistic services that combine situational awareness with trusted emergency response.

Noonlight powers that shift. As the infrastructure behind automated safety, we manage operational complexity so partners can focus on building differentiated, scalable solutions that are seamless to the end user. With Noonlight, security providers can rely on a single partner for AI filtering, human verification, and emergency response. This approach reduces the overhead, difficulty, and privacy concerns that come with using multiple vendors.

Why Security Providers Partner with Noonlight

- **Modern API Infrastructure:** Integrate verified emergency response seamlessly with just a few lines of code — bypassing legacy complexity and accelerating time to market.
- **Human Agents Behind Every Alarm:** Authorized agents verify, deter, and escalate with judgment and empathy — prioritizing real emergencies while filtering out false alarms.
- **Verified Response at Scale:** End-to-end AI Person Filtering, incident verification, and emergency coordination without the cost and complexity of building in-house response operations.
- **AI-Powered Insights:** Embedded AI technologies automatically filter non-person and non-actionable events, provide richer verification context through live video, and provide response tools to help agents resolve real threats faster.
- **Proactive Deterrence:** With live talkdown from a human agent, we deter the behavior, and resolve the situation — often before it becomes a dispatch-level incident.
- **Rich, Two-Way Context:** Shared structured incident insights (e.g., routine activity vs. suspicious behavior) enable smarter workflows and stronger customer experiences.

Close the Gap Between Security and Automated Safety

At Noonlight, we combine embedded AI filtering with highly trained human operators to transform real-time data into life-saving action — not digital noise. We remove operational risk — staffing, training, quality control, compliance, and relationships with emergency response agencies — so our partners can focus on building great security and safety solutions.

Partner with Noonlight to address the four trends shaping modern security, as discussed in this report:

1. **A Shift Toward Automated Safety:**
   End-to-end, always-on monitoring and emergency response built to meet market expectations.
2. **An AI-Driven Frontline:**
   Embedded proactive deterrence that filters non-person events automatically and accelerates threat resolution.
3. **The Human in the Loop:**
   Empathetic, highly trained agents who verify incidents, reduce false alarms, and stay engaged until resolution.
4. **The Rise of Proactive Safety Ecosystems:**
   A flexible, API-driven platform that integrates easily into modern security systems with minimal code.

Ready to see how Noonlight powers verified, automated safety in action?

BOOK A DEMO

NOONLIGHT

NOONLIGHT

Noonlight combines advanced technology with real humans to protect and comfort people so they can live freely. Launched in 2013 as a mobile application, Noonlight has since grown into a connected safety platform — partnering with product and service providers to enable modern and affordable 24/7 professional sensor monitoring, video monitoring, false alarm filtering, and data-rich emergency response via an API. Noonlight's technology works everywhere in the United States and Canada plus other select markets, allowing end users to quickly get help in any situation, without requiring a 911 call or the ability to talk or text.

For more information please visit www.noonlight.com