

Intrusion Detection Technology Beyond the Horizon

By Glenn Longley, Chief Product Officer



Photo by Etienne Girardet on Unsplash

March 25, 2026



Intrusion detection systems have evolved dramatically since a shopkeeper first affixed a bell to their store's front door to alert them when a customer entered. The quantum leap in electronic intrusion detection came in the mid-1800s when telegraph lines and call boxes were used to signal intrusion alerts to remote locations. A lot has changed since then, yet the basic premise of intrusion detection remains the same — detect an intrusion, notify the right people, and initiate a response.

Fast forward to 2026. New modern intrusion system solutions incorporate sophisticated communication and sensor technologies capable of integrating with various security and building automation systems. Wireless communication networks now link smart system controllers to many different types of sensors and devices at the edge, capturing volumes of data processed on powerful platforms in the cloud. These new and more versatile capabilities continue to drive the demand for the next generation of intrusion detection systems with higher levels of embedded intelligence, ease of deployment, and implementation for mainstream applications.

Challenges of Legacy Intrusion Systems

The primary expectation for intrusion detection technology is that it accurately detects and alerts authorities of potential threats. Yet even as these systems become more advanced, the environments they're intended to protect are becoming increasingly more complex with spaces that are larger, more dynamic, and require higher levels of security. This poses several longstanding challenges for end-users and system installers alike.

Facilities constructed of new, more durable materials and the number of electronic systems implemented within these structures can present interference challenges for certain types of wireless communications. And although hard wired systems overcome these transmission issues, they are significantly more expensive to install and sustain, effectively pricing them out of range for the large majority of potential SMBs.

Legacy wired and wireless intrusion systems are also somewhat limited in intelligence, lacking the ability to provide real-time insights and system health monitoring with limited reporting for audits and investigations. It's also difficult, if not at all possible, to integrate most legacy intrusion detection systems with modern security and building automation platforms, rendering them as stand-alone silos. And as these legacy intrusion systems continue to age, they become more difficult to sustain, increasing their total cost of ownership over time, but more importantly, decreasing their effectiveness.

ADVERTISEMENT



Legacy intrusion detection systems also pose additional challenges to resellers and systems integrators. Installations slowed by rigid or wired infrastructure is perhaps the most significant, followed by difficulties surrounding the integration of third-party devices and other system management and control software platforms. Scalability is also an issue for legacy intrusion systems when expanding system coverage and integrating multiple site locations.

Defining Best-in-Class Intrusion Detection Solutions

When evaluating legacy and even new modern intrusion detection solutions, the best performance criteria to consider relate to speed of detection, notification, and response/acknowledgement. These are often quantified as mean time to detect, mean time to acknowledge, and mean time to respond or contain an event. The faster these events take place, the better the outcome, and the more confidence users and resellers will have in the system.

Looking for quick answers on security topics? **Try Ask SDM, our new smart AI search tool.**

Ask SDM →

Once a potential threat is detected, it's imperative that the activated edge device effectively communicates that an alert condition is in progress. This requires reliable transmission methods to keep communication consistent in busy RF environments. To ensure optimal signal transmission, best-in-class wireless solutions will include features like 902 to 928 MHz frequency hopping over multiple channels, system health monitoring, mesh networking capabilities, and fast and easy sensor and edge device integration. This short list of capabilities goes a long way in ensuring high performance, reliable system communications and heightened security, even in complex building environments.

Another highly sought feature is remote management. The new imperative for intrusion detection systems across every level of application — from SMBs to multi-tenant, multi-location enterprise organizations. New modern intrusion platforms provide remote management via mobile devices with a single pane of glass view and intuitive user operation. Overall, better system visibility drives faster decisions and smoother system management.

Security and More

Advancements in management software and sensor technologies are also playing a role in expanding the applications for intrusion detection systems beyond traditional security. Modern intrusion detection solutions can accommodate a wide range of edge devices that monitor environmental conditions, equipment operation, water detection, smoke, CO, location trackers, wearable duress (panic) buttons, and more. These devices capture tremendous volumes of data that can be used for a wide variety of applications, further increasing the return on investment (ROI) for modern intrusion detection system technology.

Intrusion Innovations

New intrusion detection solutions from Inovonics will incorporate more intelligence and capabilities for both mainstream applications and advanced enterprise integrations. Good news for SMBs looking for more effective and cost-efficient intrusion system solutions, as well as for enterprise level users looking to scale and enhance existing systems. And perhaps even great news for systems integrators and resellers who can leverage new intrusion detection solutions to expand their customer base and generate new business opportunities.