



From Detection to Response: Why Verified Real-Time Reporting Is Reshaping Business Security

Why verified real-time reporting is reshaping business security, and how leaders can close the intelligence gap between an incident and the officers who respond to it.



EXECUTIVE SUMMARY

Detection Is Not Response

When a crime unfolds inside a store, a warehouse, or a bank branch, the decisive variable is not whether an alarm is triggered. It is the quality of the information that reaches the people who respond.

For decades, security systems have reliably signaled that something happened. Now technology lets businesses go further, sharing verified visual intelligence that shows what is actually taking place. Closing that distance between detection and understanding is where verified real-time reporting is reshaping how businesses and law enforcement work together.

This paper makes a single argument: as crime grows more organized and more violent, the organizations that close the intelligence gap, with verified, standardized, securely shared reporting, will see safer and more prioritized outcomes than those that keep relying on raw alerts. The shift is already underway, and the industry is naming it as a priority.

THE INTELLIGENCE GAP

The Problem Is Structural, Not Anecdotal

The pressure on business security is rising, and the data is unambiguous. The National Retail Federation's Impact of Retail Theft & Violence 2025, produced with the Loss Prevention Research Council, found an 18 percent increase in average shoplifting incidents

and a 17 percent rise in violence tied to theft, with most retailers now reporting transnational organized retail crime. These are not opportunistic, one-off events. They are coordinated operations that move across stores, jurisdictions, and borders.

The traditional response was not built for that reality. An alarm confirms that a sensor tripped, but it carries no context. Details are then relayed by manually, through multiple points, each adding delay and stripping detail, until responders arrive with limited situational awareness. While traditional methods provide essential voice communication, an unverified alert gives a police dispatcher little to work with.

The gap is systemic. The FBI has publicly identified information sharing between the private sector and law enforcement as one of the biggest hurdles to combating organized retail crime. With no national system to track these offenses, and every site, agency, and municipality recording events differently, coordinated criminals gain the advantage. Standardized, verified reporting is how that advantage is taken back.

WHY VERIFICATION CHANGES THE OUTCOME

A Raw Alarm Is a Question. A Verified Report Is an Answer.

Closing the intelligence gap is not about speed. It is about sending better information. The difference is a human confirmation step that filters noise and protects staff.

The workflow is deliberately sequenced. An employee triggers an alert. The internal security team receives and verifies the event. The security team then shares the confirmed video and event data with local police dispatchers. That verification step does three things at once: it filters false alarms before they consume a response, it protects employees by keeping them out of the reporting loop with law enforcement, and it produces a defensible, time-stamped record that holds up during investigation or in court.

Federal guidance reinforces the discipline. OSHA's incident investigation resources urge organizations to document every incident, including near misses, rather than treat reporting as an afterthought.

Moving from traditional to verified real-time reporting is a shift across five dimensions:



- Data source moves from verbal descriptions during high-stress moments to verified video and location data confirmed by security professionals.
- Context moves from reporting delays as details are relayed by hand to real-time capture as the event occurs.
- Visibility moves from limited context and communication gaps to full situational awareness before arrival.
- Reliability moves from a high volume of false alarms to human-verified, confirmed events only.
- Coordination moves from reactive to prioritized and informed.

GOVERNANCE IS WHAT MAKES IT SCALABLE

Sharing Intelligence Without Exposing Infrastructure

The reason many enterprises have hesitated to share security data is legitimate. Sharing has historically meant exposing infrastructure. Persistent, open connections expand the attack surface and demand constant oversight. The answer is not less sharing. It is governed by sharing.

An outbound-only architecture resolves the tension. Verified intelligence moves outward to local police dispatchers without opening the internal network to inbound access. Sharing is event-specific and time-bound, so law enforcement receives exactly what a confirmed event requires and nothing more. Operational authority over systems and data is never transferred, and enterprise data ownership is retained. In this model, control is not a constraint on collaboration. It is what makes collaboration scalable across dozens of sites and jurisdictions without compromising privacy or compliance.

FROM ALARM TO PREPARED RESPONSE

Better Information, Safer and More Prioritized Outcomes

The payoff of closing the intelligence gap is a better-informed, more prioritized, and safer response. When reporting delivers verified intelligence instead of a bare alarm, dispatchers gain situational awareness that supports better decision-making and lets responding officers anticipate conditions before they arrive. The industry increasingly agrees on the direction.

In the NRF's 2025 findings, loss prevention leaders pointed to technology-enabled intelligence sharing and multi-jurisdictional cooperation as critical next steps for reducing theft and violence, a shift from reacting to raw alerts toward acting on verified information.

3Si's DirectToDispatch™ is an example of this pathway in practice. It is the secure, trusted priority pathway designed for law enforcement dispatch to access. Utilizing a private-sector interface called the DTD Gateway, verified security intelligence is sent directly to law enforcement for verified threats to property and life crimes in real-time. Because dispatchers see confirmed video and location data, they can prioritize the event and coordinate a safer approach before officers arrive.

CONCLUSION

Reporting as Verified Intelligence, Not a Record Filed After the Fact

As crime grows more organized, the organizations that treat reporting as a source of verified intelligence rather than a record filed after the fact will be best positioned to respond safely and decisively. The building blocks are clear: verified events over raw alerts, one standard across every site, and governed, outbound-only sharing that protects the enterprise while giving responders what they need.



To see how verified intelligence reaches local dispatch when it matters most, **schedule a DirectToDispatch™ Gateway demo** or learn more about **DirectToDispatch™ for organizations.**