The Power of Curated Control:

Rethinking How Crime Intelligence Is Shared

Executive Summary

Serious crimes frequently occur on commercial property, including robbery, organized retail crime, violent incidents, and other threats to people or assets. When these events unfold, enterprises must provide law enforcement with timely, actionable intelligence while maintaining strict cybersecurity, privacy, and governance standards. Granting external access to cameras or internal systems introduces a risk that large enterprises cannot accept.

The challenge is not whether to share intelligence. It is how to share the right intelligence without exposing enterprise infrastructure.

DirectToDispatch™ provides a controlled alternative. Instead of opening entire systems, organizations curate incident-specific content such as selected video clips, audio, location data, or related event details and share only what is necessary to support response. For every verified incident, the enterprise determines what is shared, who receives it, and how long access remains available. All distribution is time-bound, auditable, and reinforced by acknowledgment safeguards.

This model supports verified dispatch events as well as internal investigations, workplace safety incidents, and compliance documentation. By embedding governance into the sharing process, **DirectToDispatch™** enables trusted collaboration between enterprises and law enforcement without compromising data ownership, privacy, or network control.

The Risk of Open Access Models

Cybersecurity and Compliance Exposure

Granting external access to internal security systems increases cybersecurity and regulatory exposure. Modern enterprise cybersecurity frameworks, such as NIST emphasize limiting unnecessary system access and reducing attack surface exposure. Persistent logins to cameras or video management platforms expand the attack surface and require continuous oversight.

While systems may provide audit trails and access controls, organizations must actively monitor those logs, validate appropriate use, and ensure compliance with internal policies and external standards.

For enterprise organizations, this level of ongoing monitoring can conflict with established risk management expectations and operational capacity.

What is intended to improve collaboration can unintentionally introduce sustained compliance and resource demands.

The Failure of All-or-Nothing Integrations

Traditional integration models often create a binary choice. Organizations either isolate their systems, limiting or delaying intelligence sharing during critical events, or grant broad external access that exceeds operational necessity.

Neither approach balances effective collaboration with enterprise control. Isolation restricts response capabilities. Overexposure undermines governance and accountability.

Operational Impact on Response and Coordination

Without a secure and governed sharing pathway, intelligence remains confined within private systems. During verified incidents, dispatch and responding officers may rely on verbal descriptions rather than shared visual context.

Internally, coordination across regions, business units, or leadership levels can slow when intelligence cannot move efficiently and securely.

Connectivity alone does not solve the problem. Sustainable collaboration requires controlled access.

Strategic Advantage: Intelligence Without Access

Curated Intelligence vs. Persistent Connections

Traditional security integrations rely on continuous connectivity. In many cases, this approach grants external stakeholders broad access to cameras or video management systems. While intended to streamline collaboration, persistent connections expand cybersecurity exposure and complicate compliance oversight.

DirectToDispatch™ replaces permanent access with controlled, event-based sharing. Intelligence is intentionally curated and delivered only when required. Internal systems remain closed. Networks remain protected. External partners receive relevant situational context without gaining operational authority.

This shift moves intelligence sharing away from open connectivity and toward governed collaboration.

User-Controlled Sharing Parameters

For every verified event, organizations define clear parameters around intelligence distribution. Access decisions are not made in isolation. In many large enterprises, dedicated teams focused on robbery and violence prevention, corporate security, and loss prevention help determine how intelligence is shared and escalated.

They define:

- What intelligence is curated
- Which internal or external stakeholders receive access
- How long visibility remains available
- How the information supports response and investigative workflows

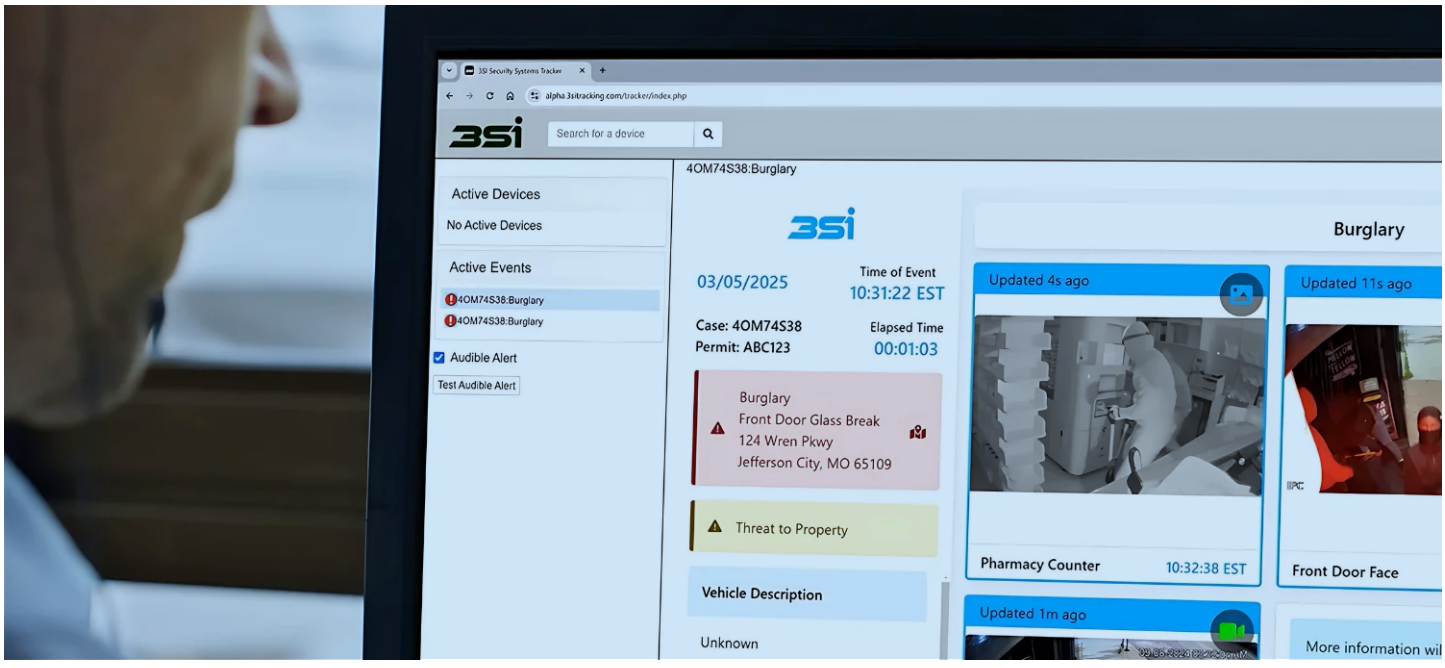
By aligning sharing parameters with established security teams and response protocols, enterprises ensure that intelligence distribution reflects operational realities, not just technical settings.

Designed for Regulated Industries with Multi-Layered Workflows

Retailers, financial institutions, and other enterprise organizations operate within layered security structures. A controlled sharing model supports:

- Internal loss prevention investigations
- Regional security command centers
- Verified dispatch collaboration
- Compliance documentation and reporting

By applying the same governed framework across internal and external workflows, organizations increase system utilization and expand measurable return on investment without increasing risk exposure.



Secure Intelligence Delivery in Practice

Outbound-Only Architecture

DirectToDispatch™ operates through an outbound-only sharing model. Intelligence is intentionally pushed from the enterprise environment through a secure pathway. External stakeholders do not initiate access, and no persistent connection to internal systems is established.

This architecture ensures:

- No inbound system access
- No continuous connectivity
- No expansion of the enterprise attack surface

Real-time intelligence can be delivered without increasing infrastructure exposure.

No Direct System or Network Access

Law enforcement and external partners do not log into enterprise cameras, video management systems, or private networks. Internal infrastructure remains closed and fully under organizational control.

Shared intelligence is event-specific and limited to curated content selected by authorized personnel. Operational authority over systems and data is never transferred.

Acknowledgment-Based Access Controls

Before viewing shared intelligence, law enforcement must acknowledge that the content contains sensitive corporate information intended for emergency and officer safety use only and is not to be shared outside law enforcement.

This acknowledgment reinforces proper handling standards and establishes clear distribution boundaries aligned with enterprise governance requirements.

Flexible Distribution Across Workflows

The same controlled framework supports multiple operational scenarios, including:

- Verified dispatch events
- Responding officer situational awareness
- Internal investigations
- Corporate security escalation

For every event, defined rules guide distribution decisions. Intelligence flows where it is needed while enterprise control remains intact.

Outcomes: Control Without Compromise

Preserved Data Ownership and Governance

Organizations retain full authority over their systems, networks, and intelligence-sharing decisions. No persistent access is granted, and no system control is transferred. Each event is governed by defined parameters and documented through auditable records.

This structure supports regulatory alignment, internal policy enforcement, and executive oversight without introducing additional operational risk.

Improved Response Precision and Officer Safety

When verified intelligence is delivered securely and in real time, dispatchers and responding officers gain clearer situational awareness before arrival. Access to visual context supports:

- More accurate prioritization
- Better-informed tactical decisions
- Safer response planning

Controlled sharing enhances public safety outcomes while preserving enterprise infrastructure integrity

Expanded Operational Value and Measurable ROI

The same governed framework supports a range of enterprise workflows, including:

- Crimes in progress
- Organized retail crime investigations
- Workplace safety incidents
- Fraud and compliance documentation
- Regional security coordination

By enabling secure intelligence sharing across both internal and external use cases, organizations increase system utilization, reduce workflow friction, and strengthen measurable return on investment without expanding risk exposure.

Stronger Public-Private Collaboration

A trusted intelligence exchange enables consistent collaboration between enterprises and law enforcement. Clear access parameters, acknowledgment requirements, and time-limited visibility reinforce professional handling standards on both sides.
Control does not limit collaboration. It makes collaboration sustainable and scalable.

Privacy by Design

Behavior-Based Intelligence

DirectToDispatch™ centers on observable activity and situational context during verified events. Intelligence is shared to support response, coordination, and decision-making, not to enable identity harvesting or continuous surveillance.

The focus remains on incident relevance and operational clarity, ensuring that intelligence serves a defined purpose.

Minimal Necessary Disclosure

Only intelligence directly related to the verified event is curated and shared. Whether distributed internally or provided to dispatch, content is intentionally limited in scope and duration. This approach reduces unnecessary exposure while preserving the value of real-time insight.

Auditability and Governance

All sharing actions are logged and traceable. Defined parameters around access, duration, and acknowledgment create clear oversight controls aligned with enterprise policy and regulatory expectations.

Privacy safeguards are embedded into the architecture itself, reinforcing responsible intelligence sharing without sacrificing operational effectiveness.

Conclusion: Control Enables Scalable Intelligence Collaboration

Scalable intelligence sharing requires trust. Open access models introduce exposure that Large enterprises cannot sustain, while isolated systems limit effective collaboration. A governed, intentional approach creates the foundation for a responsible partnership between private organizations and public safety agencies.

DirectToDispatch™ extends beyond a single-incident response tool. It enables verified dispatch collaboration, strengthens internal investigation workflows, and supports enterprise-wide coordination within a controlled framework. By embedding time-bound access, acknowledgment safeguards, and full organizational authority into every event, intelligence can move where it is needed without increasing system risk.

Control is not a constraint on collaboration. It is what makes collaboration repeatable, defensible, and sustainable.

Organizations that prioritize governed intelligence sharing can support real-time response while preserving privacy, compliance, and operational autonomy.

Achieve improved response precision and officer safety without sacrificing data ownership.

Learn more about **DirectToDispatch™** today Visit 3Si Security