



TRACKTICK



Owning the Data, Owning the Outcome

Global Automotive Manufacturer's Security Story



INDUSTRY: Automotive Manufacturing

REGION: Americas Region

PLATFORM:  trackforce® | TRACKTIX

PROFILE: Fortune Global enterprise manufacturer
with **14,000+ employees** across
55+ locations throughout the Americas

Running a Security Program Without Owning the Data

When a new Chief Security Officer joined the Americas division of a global automotive manufacturer, he inherited more than just a security program.

He inherited its problems. The team was small, the program was immature, and operational oversight had long been managed remotely from an overseas headquarters with minimal regional accountability. Over 12 years, this team matured into four regional teams throughout the Americas. But early on, the obstacles were more fundamental than headcount.

The security program was fully dependent on outsourced guard service providers, and crucially, so was all of its data. Every incident report, patrol log, guard schedule, and operational record lived inside the service provider's systems. The corporation owned none of it.

This created four compounding challenges that made effective security leadership nearly impossible:

- 1. No data ownership.** If the security guard contract changed, years of institutional security data could vanish overnight, with no contractual protection to prevent it.
- 2. No standardized reporting.** Across 55+ locations, there was no consistency; sites relied on their own processes, often clipboard-based, with no consistent taxonomy. One security guard might log an event as "theft," while another might log it as "robbery." A vehicle collision was recorded as "destruction of property" at one site and "vehicle accident" at another. Without consistent classification, trend analysis was out of the question.
- 3. No ability to analyze at scale.** Without a centralized data repository, there was no way to identify patterns across sites, track incident trends over time, or use security data to drive strategy or justify investment.
- 4. Report quality that was essentially unusable.** Handwritten incident reports were frequently misspelled, inconsistently formatted, and unsuitable for any external audience. "There was no way I could ever show these reports to executives or submit them to a court," the CSO recalled.

The result was a security function that was reactive, siloed, and invisible to the broader business. **"I didn't have the data needed to be an effective CSO and a valued business partner."**



THE INFLECTION POINT

A Contract Rebid That Changed Everything

The situation reached a breaking point during a routine procurement cycle.

When the guard services contract came up for rebid, the CSO realized he risked losing access to TrackTik, a platform that had been introduced by the incumbent guard firm, if a new vendor was selected who didn't use it.

Rather than accepting that risk, he made a decisive move. He negotiated a direct corporate license with TrackTik, independent of the security guard company, and embedded a non-negotiable requirement into the new security guard services scope: any winning vendor must utilize the TrackTik platform



A Corporate-Owned, Deeply Customized Platform

With direct ownership secured, the security team undertook a phased buildout, configuring TrackTik not just as a reporting tool, but as a critical component of a maturing enterprise security program.

System Integration

The manufacturer's existing incident management system, a legacy platform built internally with limited ongoing support, was integrated with TrackTik so that every report auto-populated into the corporate system. The elimination of double entry streamlined operations and ensured that guard time was respected.

Manufacturing-Specific

Customization Incident categories were tailored to the realities of a manufacturing environment. A component missing from the production line required different classification than a stolen personal item. These distinctions were embedded directly into the platform's drop-down menus, creating the foundation for meaningful, defensible analytics.

Hot Works Permitting

The platform was extended to support the internal fire department's hot works permit process, documenting welding, grinding, and other spark-risk activities on the plant floor to enable consistent safety compliance tracking.

Mobile Deployment Guards

Were equipped with iPads and smartphones and trained to use TrackTik's mobile interface. The transformation was immediate: handwritten, barely legible reports gave way to standardized, photo-supported, professionally formatted records that could be shared with any department, legal team, or external auditor.

CTPAT Compliance Documentation

As a manufacturer importing components internationally into a free trade zone, the company faced rigorous U.S. Customs CTPAT audit requirements. TrackTik was configured to document 13-point truck gate inspections, complete with photos, timestamps, and seal verification, giving auditors immediate, defensible proof of compliance and dramatically reducing audit preparation time.



Security Becomes a Trusted Business Function

The shift from vendor-held data to corporate-owned intelligence changed everything, not just for the security team, but for the business.



Cross-Departmental Impact

Security data captured in TrackTik was fed directly to the logistics, safety, facilities, environmental, and HR departments, when the incident was directly related to that respective department. The security function became a data provider for the business, not just a reactive response team.



Logistics Improvements

Driving Major Annual Savings: Gate data revealed that the security team was forcing numerous truck turnarounds per week due to bill-of-lading mismatches at the outbound gate. By surfacing this as a measurable trend rather than a point-in-time complaint, the data shifted accountability to the logistics team and drove process improvements that saved the company significant time and money each month.





Armed Security Justification Backed by Data

With 14,000 employees on a single campus, the CSO believed around-the-clock armed security was essential. Rather than advocate on instinct alone, he built an evidence-based case using TrackTik data, tracking recovered weapons on campus, assault incidents, high-risk terminations, and workplace violence trends over time. The result was executive approval for an annual budget increase to implement armed security response teams. That same data continued to demonstrate ROI by tracking the deterrent effect in subsequent years.



Data-Driven Budget Strategy That Cut Costs

With a multi-million-dollar national guard services contract, TrackTik data became the foundation for annual budget planning. The platform enabled the CSO to make the case for new investments where data showed rising risk, and to create efficiencies where incident history showed no activity warranting a physical presence. "We stopped guessing and started using actual data. TrackTik gave us the evidence to defend every dollar we spent and justify every post we eliminated," the CSO noted.



Scheduling Accountability and Dark Hour Detection

The workforce management module exposed a common gap in service delivery: when a guard called out sick, supervisors would fill the post themselves, appearing to close the "dark hour" while leaving their own supervisory zone uncovered. The company instituted contract penalties for overtime and dark hours, improving accountability and ensuring the corporation received the coverage it was paying for.



Compliance Audit Readiness

Preparation time for CTPAT, OSHA, and internal audits dropped significantly. Documentation was instantly accessible, and audit scores improved consistently year over year as the program matured.



THE STRATEGIC TAKEAWAY

Own Your Platform

The lesson from this CSO's 12-year journey is direct and transferable.

"Owning and having full access to the data made me a more effective CSO. After having TrackTik implemented for a period of time, it tells a story that we use to drive policy and process improvements with a positive impact on the business. I didn't want security to be that necessary line item that just costs the company money. I always wanted to be able to tell a story of how security is a value add to the business."

When guard contracts change, as they inevitably do, corporations that rely solely on their service provider's platform risk losing years of institutional security data overnight. The better path is to negotiate a direct corporate license, embed the platform requirement into every guard services scope of work, and use the data you own to make smarter decisions across every dimension of security and operations.

The platform that arrived through a guard company's door became one of the most powerful strategic tools in the CSO's arsenal, because the company made it theirs.

