GEOTAB

# Securing the Supply Chain: A 2026 Blueprint for Countering Smarter Theft

## Modernizing Fleet Security from Risk to Resilience

# Executive Summary:
# Modernizing Fleet Security from Risk to Resilience

Cargo theft is no longer a line item for shrinkage. It is a top threat to the global supply chain, a multi-billion-dollar illicit industry that is draining fleet resources, undermining customer trust, and placing drivers under sustained safety pressure.

In North America, cargo theft reached record levels in 2024, with a 27% increase year over year. The estimated average value per theft also rose sharply, reaching $202,364, up from $187,895 in 2023, with annual losses of up to $35bn. While the boardroom discusses the costs of doing business, organized crime groups are tearing through logistics networks with military precision. The days of opportunistic smash-and-grab are fading. In their place, strategic theft is rising. It is a sophisticated brand of fraud where thieves can walk in, sign the papers, and drive away with millions in inventory.

### The Core Conflict:

The threat has evolved, but fleet defenses have not. Geotab's research reveals a clear technology gap. Criminal tactics have shifted toward digital deception and identity fraud, while many fleet security strategies remain dangerously analog. The industry knows what works, including real-time GPS vehicle and asset tracking, AI-powered 360 degree cameras, and driver verification protocols, yet deployment remains stalled by perceived barriers - including costs of implementation, integration complexity and driver acceptance.

This hesitation is increasingly misaligned with broader market realities. The global market for tracking devices and real-time data loggers used in general cargo applications is expected to grow rapidly, with active devices forecast to increase from 4.9 million in 2024 to 16.2 million by 2029. At the same time, insurance is one of the fastest growing operating expenses for fleets. Fleets that delay modernization face rising costs and diminishing protection as traditional risk management approaches lose effectiveness.

**Emily Williams**
AVP Transportation Business Development, Geotab

## KEY FINDINGS:

**The Threat is Unrelenting:** While some fleets operate unscathed, the threat is growing for many. 38% of fleet professionals are more concerned about cargo theft now than they were 12 months ago. In Europe, companies have reported staggering average incident rates, turning logistics hubs into high-risk zones.

**The Human Toll is Critical:** This isn't just about lost goods, it's about lost people. **47%** of North American respondents agree that the stress and personal safety risks of theft are significant factors in driver burnout and turnover. In Europe, that figure climbs to **88%**.

**The Consumer Pays:** The public is waking up to the cost. 30% of consumers believe they ultimately bear the financial burden of theft through higher prices.

**The Tech Gap:** We are failing to deploy the tools we have. While **58%** agree an effective strategy requires multiple layers of technology, nearly a quarter of the industry still relies on "a strong lock and a vigilant driver".

**This white paper outlines the 2026 blueprint for resilience. It is a call to move beyond the padlock and embrace a multi-layered defense strategy, leveraging an ecosystem of tools that already exist to turn the supply chain from a target into a fortress.**

# The Evolving Threat Landscape

Today, the modern cargo thief is just as likely to be holding a clipboard as a crowbar. The industry is witnessing a seismic shift toward more strategic theft, crimes of deception that use modern tools to exploit the chaotic speed of commercial logistics.

The data paints a chilling picture of vulnerability in the shift to strategic theft. While **52%** of respondents still identify unattended trucks in unsecured lots as the primary threat, a growing sophisticated threat has emerged. **23%** now flag strategic theft through fraud or deception as their greatest risk.

The threat has evolved from roadside robbery to bureaucratic deception. Through unauthorized double brokering and fictitious pickups, syndicates act as legitimate intermediaries to secure loads, only to disappear with the assets. This creates an administrative fog that leaves fleets exposed and vulnerable. This shift requires a pivot in defense: from physical barriers to digital verification.

## Global Hotspots and Behaviors

Theft isn't random, it has a heartbeat. Geotab's telematics data shows risk fingerprints across the globe. These are anomalies that demonstrate how drivers are altering their operations.

**The Night Run:**
In Europe, nighttime driving spikes to **40%** on weekends (compared to 25-26% on weekdays). In Brazil and Asia, weekend night driving hits **30%.** Drivers are pushing through the darkness, likely avoiding stops in high-risk zones.

**The Idling Indictment:**
In theft-prone regions, trucks aren't shutting down. Brazil has seen a **42%** increase in idling time while Asia is up **26.5%.** This isn't necessarily inefficiency, it could be anxiety. Drivers are keeping engines running, ready to move at a moment's notice.

# The Human Cost of Cargo Theft

For too long, the industry has treated the driver as the last line of defense. This strategy is not just failing, it adds additional stress onto the workforce.

## Stress Fuels Driver Turnover

Drivers are on the front lines, **47%** of US respondents agree that the day-to-day stress and personal safety risks of cargo theft are driving burnout and resignation. In the EMEA region, that number skyrockets to **88%.**

Every hijacked load or parking lot confrontation chips away at the workforce. Drivers are being asked to act as logistics experts and security guards at the same time, and many are responding by leaving the industry.

Despite the pressure, many fleets are still in denial. When asked about their security philosophy, **23%** of respondents stated that "a strong lock and a vigilant driver" are the most important security elements.

This is a dangerous fallacy. A vigilant driver cannot verify a spoofed bill of lading, and a strong lock cannot stop a syndicate that has cloned a company identity. Continuing to place the burden of security on overburdened drivers is a strategy designed to fail.

The consequences of cargo theft reach far beyond the stolen load. **18%** of fleet managers identify the loss of customer trust and potential business as the most damaging secondary impact of theft. When cargo disappears, confidence in the carrier declines. Consumers feel the effect as well, with 37% attributing higher prices to supply chain crime.

Left unaddressed, this becomes a systemic crisis of confidence. The only way to reverse it is through prevention.

# The Tech Gap: Why Fleets are Falling Behind

The industry is hesitating at a time when speed and verification are increasingly critical. Fleets have access to technology that can track shipments in real-time and confirm who is operating their vehicles, yet adoption remains uneven. As a result, key vulnerabilities persist. Our data shows a fragmented security landscape, where some fleets are modernizing while others are not, creating clear opportunities for organized crime groups. This gap is not accidental. It reflects where theft activity is most likely to concentrate.

01

**The Cost Barrier: Short Term Savings, Long Term Risk**

In a tight economic environment, delaying investment in security technology can feel financially responsible. In reality, it often increases risk. **37% of respondents cite the upfront cost of hardware and subscriptions as the biggest barrier to adoption.**

This hesitation is creating a security gap. While fleets weigh the cost of new technology, organized crime groups assess the value and vulnerability of the cargo itself.

In the EMEA region, **22% of fleet managers report relying solely on insurance to manage losses.** This reactive approach assumes theft will occur rather than prioritizing prevention. It also overlooks reputational damage and the loss of customer trust, costs that financial reimbursement cannot address. As insurance costs continue to rise, this strategy is increasingly unsustainable.

02

**The Adoption Divide**

The industry is increasingly split between fleets that are investing in modern security and those that are not. While **41% of fleets report using GPS tracking, only 23% have adopted camera or video solutions.** This gap creates blind spots that are easy to exploit. GPS alone can show the location of the vehicle, but cannot confirm identity of the operator or elaborate on the environment.

03

**Integration Complexity**

Integration complexity often slows large fleets as new safety technologies must work with legacy systems. A unified approach built on open API architecture allows tools such as smart locks, cameras, and sensors to connect in a single dashboard. OEM pre-installations also reduce rollout friction by using factory-installed hardware instead of retrofits. The telematics unit then acts as a central IoT hub, connecting devices and turning multiple data streams into a single operational view.

04

**Driver Acceptance and Privacy**

Driver acceptance remains a barrier to video adoption due to privacy concerns. Fleets can address this by positioning cameras as a tool for driver protection. Event-based recording captures footage only during safety triggers such as collisions or harsh braking rather than constant monitoring. In-cab alerts provide real-time feedback so drivers can correct behaviour immediately. AI privacy redaction can also blur faces or bystanders before footage uploads, protecting identities while preserving evidence for liability disputes.

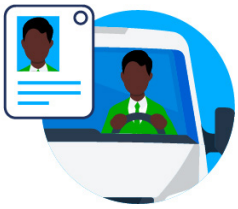
# The Multi-Layered Technology Defense Strategy

The era of the padlock is over. To defeat a syndicate that operates like a Fortune 500 company, you need a strategy that is equally sophisticated. The blueprint for 2026 is built on multi-layered defense, a philosophy of overlapping elements that ensures if one wall is breached, another stands ready.

## The Holy Grail of Data: Location and Verification

When theft happens, speed and identity are the currencies that matter.

**Speed:**
**44%** of fleet managers state that precise, real-time GPS location is the **most critical information** needed during a theft event. Without it, recovery is a guessing game.



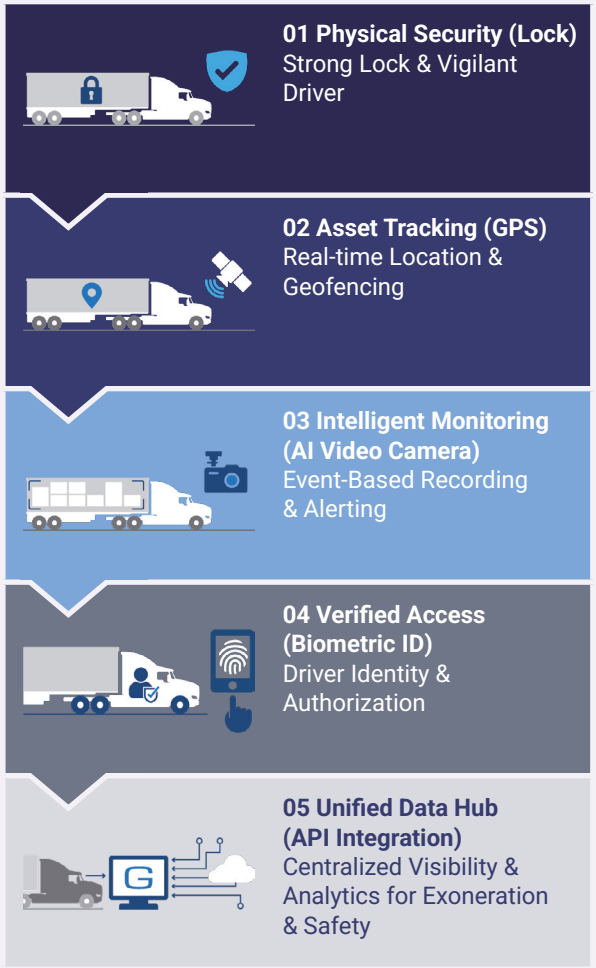
**Identity:**
Strategic theft relies on impersonation. **52%** of respondents agree that video or **photo verification of the driver** at the point of pickup is critical to preventing fraud. If you can verify the driver before the cargo moves, you stop the crime before it starts.

No single tool is a silver bullet. Real security comes from integration. 58% of North American respondents, and 30% of EMEA, agree that an effective strategy requires multiple layers working together, like driver training, smart sensors, and data analysis.

## The Law Enforcement Connection

Data is useless if it stays trapped in a silo. Police cannot act on a hunch, they need actionable intelligence. **31% of respondents say the ability to share live tracking data** directly with law enforcement is the most critical tool for recovery. Modern defense means building a digital bridge between the fleet manager's desk and the police cruiser.

### CARGO THEFT: LAYERS OF DEFENSE




Moving from isolated tools to a unified, intelligent defense system.



GEOTAB

# The High Cost of Doing Nothing

The argument that technology is too expensive is mathematically flawed. In 2026, security prevention must be viewed as a fixed operational cost, whereas theft is an uncapped liability that can bankrupt a carrier.

## The Economic Pressure Cooker

Economic headwinds are driving demand for black-market goods, incentivizing organized crime groups to broaden their targets. They are no longer just hunting electronics; they are stealing food, beverages, and household staples. These groups are industrializing theft: standardizing techniques across regions and cargo types, and using strategic fraud and identity theft to cross jurisdictional lines, making recovery nearly impossible without digital proof.

## Proof of Resilience:

The market is tightening. Insurers are increasingly demanding proof of digital security (telematics and cameras) before offering renewals or favorable deductibles. Security is becoming a prerequisite for doing business.

## COST OF THEFT VS. COST OF PREVENTION

| | Cost of Theft (Reactive) | Cost of Prevention (Proactive) |
|---|---|---|
| DIRECT COST | **$205,000-$215,000**<br>Replacement of Goods + Deductibles + Freight Payment Forfeiture* | **Basic: $100-$300**<br>**Advanced: $300-$850**<br>Hardware + Installation Fees |
| ONGOING COST | **+20% to +30%**<br>Increased Insurance Premiums | **$20-$50**<br>Fleet Management Platform (Software Subscription) |
| OPERATIONAL COST | **$448-$760 / day per vehicle minimum**<br>Vehicle Downtime + Rental Costs + Administrative Costs + Legal Fees | **$15-$25 / night**<br>Secure Parking Fees |
| HUMAN FACTOR | **$12,800 per driver (turnover alone)**<br>Driver Medical/Insurance Costs and/or Driver Turnover & Recruitment (High Cost) | **$30-$100/driver**<br>Driver Safety Training |
| STRATEGIC FACTOR | **Incalculable**<br>Loss of Customer Trust / Brand Damage | **$1-$3 per load**<br>Identity Verification Tools |

## The Bottom Line:

Fleets can choose their level of protection, but they can no longer choose to ignore the threat. A tiered approach, scaling from basic tracking to full biometric verification, allows companies to match their defense to their risk. But in the face of 2026's sophisticated threat landscape, doing nothing is the most expensive strategy of all.

***Replacement of Goods $202,364 (Average)** CargoNet (2024 Report): The average value of a cargo theft incident rose to over $200k in 2024.
**Deductibles $2,500 – $10,000 Commercial Insurance Avg:** Standard fleet deductibles range widely, but many fleets are raising them to $5k-$10k to combat rising premium costs.
**Freight Payment Forfeiture $1,130 – $2,500ATRI:** Based on an average operational cost of ~$2.26/mile. If a 500-1,000 mile load is stolen, you lose the revenue you would have invoiced for that trip.

# Future-Proofing Against Organized Crime

As we look into 2026, the supply chain stands at a crossroads. The data is clear: we are entering a period where technology gaps will determine the winners and losers in the logistics industry. Organized crime has industrialized, evolving into a sophisticated business model that exploits every analog weakness in our digital world.

The fleets that continue to rely on the insurance and locks model are fighting a losing battle. They face uncapped liabilities, spiraling insurance premiums, and critically, the loss of their most valuable asset: their drivers. As shown in our findings, nearly half of North American fleet managers already link theft stress to driver burnout. Continuing to place the burden of security on drivers is not just a strategic error; it is a catalyst for a workforce crisis.

The fleets that bridge the gap, adopting a multi-layered defense strategy that unifies real-time GPS, AI video verification, law enforcement data sharing, and advanced trailer management solutions will do more than just protect their cargo. They will insulate their bottom line, retain talent, maintain customer trust, and contribute to a safer, more resilient global industry.

## YOUR 2026 ACTION PLAN:

### Move Beyond Cost Objections:

Start viewing security as operational insurance. Calculate the true cost of doing nothing, including costs to replace a burnt-out driver, and the reputational damage of lost customer trust. The investment in hardware is a fraction of the cost of a single major theft.

### Automate Security:

Remove the vigilant driver from the equation. Asset trackers and cameras create an automated perimeter that detects, records, and alerts without human intervention. Let your drivers drive, let the technology watch.

### Integrate Your Systems:

Data silos are vulnerabilities. Leverage Geotab's open-platform architecture to unify security data with your existing TMS. Speed is the enemy of theft, integrated data is the fuel for recovery.

GEOTAB®

geotab.com