



OVERHAUL INTELLIGENCE BRIEF

AI Infrastructure Intel

The cargo-theft threat to the AI hardware supply chain: the crews, the methods, and the controls that hold.

EDITION H2 2026

PREPARED BY THE OVERHAUL INTELLIGENCE TEAM

SEE. PROTECT. CONTROL.

OVER-HAUL.COM

EXECUTIVE SUMMARY

AI hardware is the cargo thief's fastest-growing target, and the theft is now led by fraud.

Thieves follow concentrated value. Consumer electronics, cigarettes, and pharmaceuticals each had their moment, and AI infrastructure is next. Processors, networking gear, memory, and copper are valuable, hard to replace on a deadline, and easy to resell across borders. Overhaul's intelligence team has already recorded more than \$150 million in AI equipment cargo losses. Thefts involving data-center equipment, computing components, and chips are up 34 percent since 2024, and the total value of goods stolen is up more than 110 percent. Individual losses now regularly exceed \$30 million, a single event has topped \$100 million, and thefts at this scale are occurring weekly.

The method has shifted from force to fraud. Across affected high-value technology shipments, deception was used in 92 percent of cases, including fraudulent carrier identities, double brokering, spoofed communications, and falsified paperwork that let crews slip inside legitimate freight transactions. This brief sets out why AI infrastructure is being targeted, how the theft is carried out, and the controls that hold. The pattern is consistent across every section that follows: the crews are organized, the value is concentrated, and visibility alone does not stop the loss.

WHAT IS INSIDE

01	Why this cargo: the buildout and the value	03	04	The true cost: hidden losses	06
02	The method: how loads are taken	04	05	The controls that hold: the Overhaul model	07
03	Where it goes: export diversion	05	06	What to do next: assess, harden, lead	08

\$150M+

AI equipment cargo losses recorded to date

OVERHAUL

+34%

Chip and data-center equipment thefts since 2024

OVERHAUL

92%

Of affected tech shipments taken by deception, not force

OVERHAUL

\$100M+

Largest single AI-cargo theft event on record

OVERHAUL

WHY THIS CARGO

A trillion-dollar buildout has created a target-rich, irreplaceable class of cargo.

The AI buildout is the largest infrastructure investment of the decade, and it concentrates enormous value into shipments that move on ordinary roads. McKinsey projects that data centers will require \$6.7 trillion of capital worldwide by 2030 to keep pace with demand for compute, with \$5.2 trillion of that tied to AI. More than 1,100 hyperscale data centers already operate globally, and every one of them has to be filled with hardware that travels before it is installed.

A single flagship AI server rack costs roughly \$3 million, so a full truckload of AI servers routinely carries eight-figure value, which is consistent with the losses Overhaul records in the field. The exposure is not limited to finished servers. Copper is the connective tissue of every data center, and S&P Global forecasts data-center copper demand rising from 1.1 million metric tons in 2025 to 2.5 million metric tons by 2040. High value, hard to trace, and easy to resell: copper, processors, and networking gear check every box a cargo thief looks for.

\$6.7_T

Global data-center capital investment required by 2030, \$5.2T of it AI-related

MCKINSEY & COMPANY

~\$3_M

Cost of a single flagship AI server rack, so a truckload runs into eight figures

INDUSTRY REPORTING

2.5_M mt

Data-center copper demand by 2040, up from 1.1M metric tons in 2025

S&P GLOBAL

THE VULNERABILITY WINDOW

Value moves long before it is secured on a rack.

Hyperscale campuses take years to build, and hardware flows to site across that entire period. Every mile between the manufacturer and the rack is an opportunity, and the crews targeting AI cargo plan around exactly that window.

THE METHOD

Fraud is the fastest-growing way to lose a load, and the crews are organized.

In the second quarter of 2026, Overhaul recorded 605 cargo theft incidents in the United States, among the highest levels of the past decade even as volume dipped year over year. Electronics were the most-targeted product type at 23 percent of all thefts. Pilferage remained the most common method at 46 percent, followed by full-truckload (FTL) theft at 21 percent, facility theft at 16 percent, and deceptive pickup at 11 percent. Warehouse and distribution-center sites were the most frequently hit location at 37 percent, and the highest-risk window was the early morning, with 28 percent of thefts occurring between midnight and 6 a.m.

The threat actors are not opportunistic. They operate behind legitimate front companies and licensed subcontractors, buy real motor-carrier authorities, accept legitimate loads, and then redirect them. The same networks that move stolen technology also move narcotics, weapons, and people, using recruiters, document forgers, insiders, and established fencing operations to complete the heist.

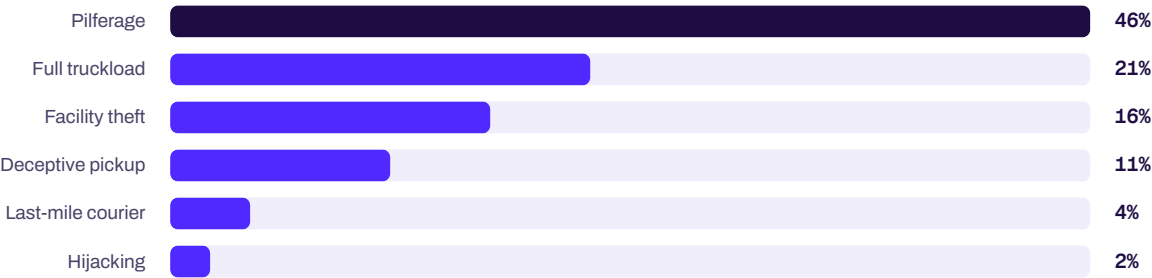
INTEL ALERT · CALIFORNIA

A new method: striking the escort.

On two California highways, crews deliberately struck the security escort vehicles of high-value technology shipments, disabling one by rear-ending it and the other with a precision immobilization (PIT) maneuver. In both cases the escort was forced to stop, the shipment continued alone, and the load was lost. Neither truck was recovered. Escort disruption is now a precursor event, not a hiccup.

Cargo theft by method of theft

US · Q2 2026 · OVERHAUL



605 US cargo theft incidents recorded in Q2 2026 OVERHAUL	46% Pilferage, the most common method of theft OVERHAUL	23% Electronics, the most-targeted product type OVERHAUL	37% Of thefts at a warehouse or distribution center OVERHAUL
--	--	---	---

WHERE IT GOES

Much of this cargo is stolen to order and bound for overseas buyers.

Stolen AI equipment rarely reappears on a street corner. Between 60 and 70 percent of loads stolen in the United States now leave the country entirely, with components moving toward China, Russia, and Iran. Export controls create scarcity, and restricted components trade at roughly double their domestic price on the black market, which means many loads are sold before they are ever stolen.

The risk is now a federal enforcement priority. In 2025, the US Department of Justice charged three individuals with conspiring to divert cutting-edge American AI technology, alleging that approximately \$2.5 billion in advanced AI servers were purchased and that at least \$510 million was diverted to China in a single three-week stretch. The proposed FY2027 budget for the Bureau of Industry and Security would raise its funding by 91.5 percent and add 290 new export-enforcement agents. For a shipper, a restricted chip that surfaces in the wrong country is not only a loss. It is a compliance investigation that can reach every party in the chain.

60-70%

Of US-stolen loads now leave the country entirely

OVERHAUL

\$510M

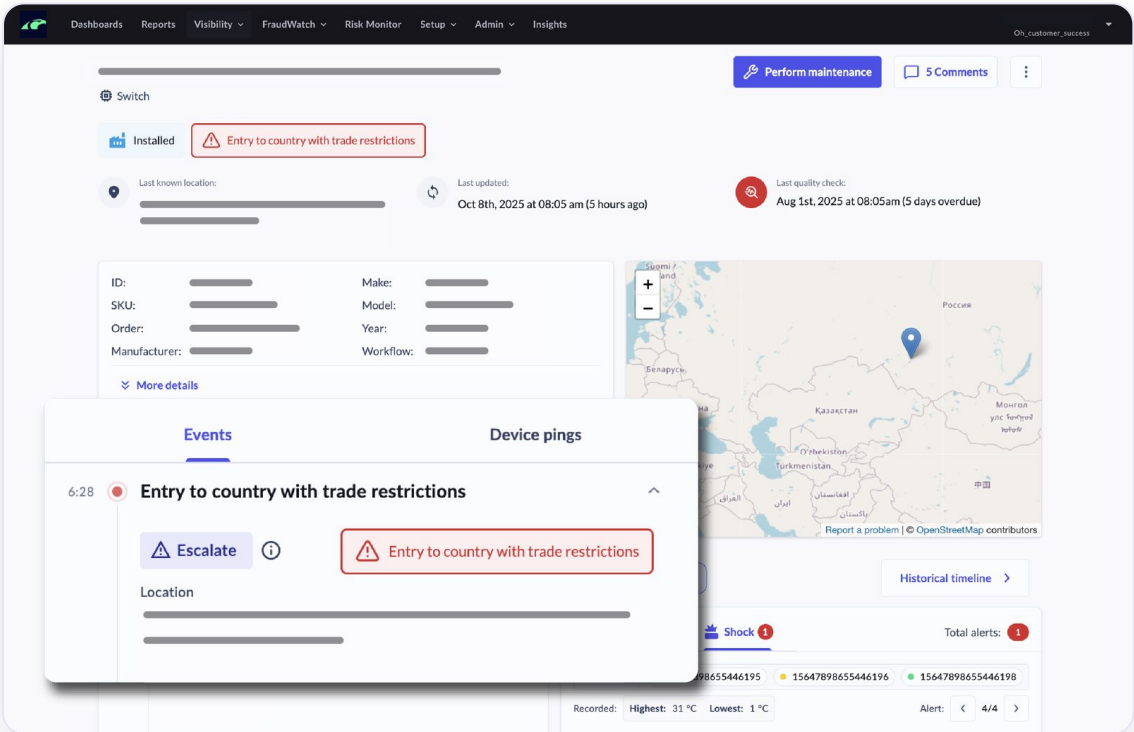
In AI servers diverted to China in one three-week stretch, of \$2.5B purchased

US DEPT OF JUSTICE

+91.5%

Proposed rise in the US export-enforcement budget for FY2027

US DEPT OF COMMERCE



OVERHAUL PLATFORM. ENTRY TO A COUNTRY WITH TRADE RESTRICTIONS IS FLAGGED IN REAL TIME, WITH ONE-CLICK ESCALATION, SO A COMPLIANCE EXPOSURE IS CAUGHT BEFORE IT BECOMES AN INVESTIGATION.

THE TRUE COST

The insurance claim is the smallest part of the loss.

The visible loss, the stolen hardware and the deductible, is only the beginning. Overhaul's intelligence team finds that indirect losses outpace direct losses by roughly three to one, and none of them appear on a claim. They include schedule compression and liquidated damages when a deployment slips, lost contract eligibility, regulatory and compliance exposure, security uplift across the rest of the portfolio, and the erosion of trust with customers and crews. Industry-wide, cargo theft losses in the second quarter of 2026 exceeded \$304 million, more than double the same period a year earlier, even as the number of incidents fell 26 percent. The message is blunt: fewer thefts are costing far more, because each one is bigger and better planned.

3 TO 1

Hidden losses outpace the visible ones.

For every dollar of stolen hardware on the claim, roughly three more are lost to schedule slips, lost eligibility, compliance exposure, and portfolio-wide security uplift. The claim captures the smallest part of the damage.

CASE ON RECORD · PARCEL NETWORK

\$250K in components. Three unauthorized opens. Zero carrier alerts.

A single parcel of memory and solid-state drives, valued near \$250,000, was opened in transit and twice more on arrival while the carrier's tracking showed only a generic in-transit status. An embedded sensor caught what the network never reported. High-value components often move as ordinary parcels, and milestone data does not protect them.

Anatomy of a loss: what the claim captures, and what it misses.



3:1 Hidden losses versus visible, claimed losses OVERHAUL	\$304M+ Industry-wide cargo theft losses in Q2 2026 OVERHAUL	2x Higher loss value than the same quarter a year earlier OVERHAUL	-26% Fewer incidents, yet far higher total losses OVERHAUL
--	---	---	---

THE CONTROLS THAT HOLD

Control across the full shipment lifecycle is what holds.

Device-and-alert tools cover one slice of the problem, the truck in transit. Overhaul runs the whole program end to end, from planning to final deployment, with a team watching cargo around the clock and the authority to intervene the moment it moves the wrong way. Analysts in Overhaul's global security operations centers monitor shipments continuously, coordinate directly with law enforcement, and turn device and sensor data into action rather than an after-the-fact report.

01 · Planning

Vet before it moves

Lane risk scoring, and broker and carrier vetting before a load is booked.

02 · Pre-departure

Verify identity

Driver, tractor, and trailer confirmed against the booking at pickup.

03 · In-transit

Monitor and act

Real-time monitoring, covert tracking, and active risk intervention.

04 · Post-shipment

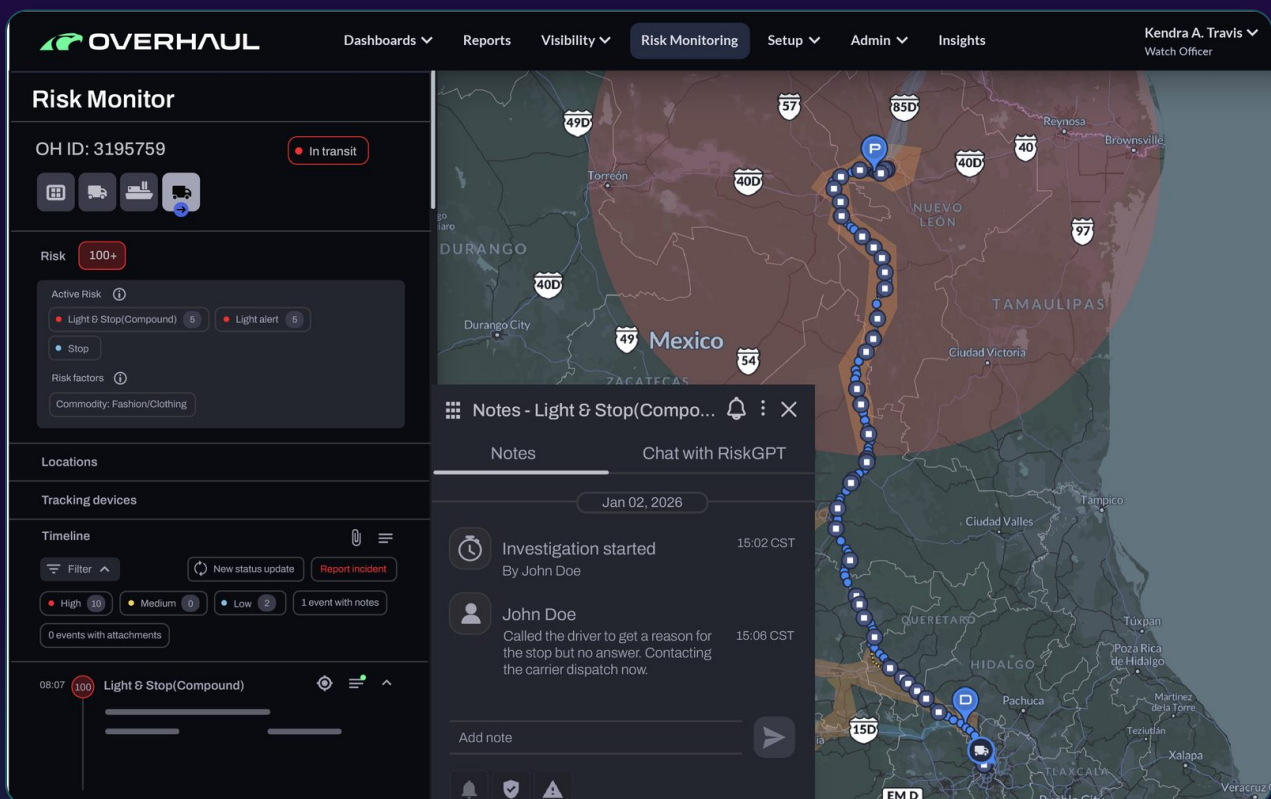
Recover and learn

Recovery, law-enforcement coordination, and intelligence that feeds the next lane.

PROOF ON RECORD

25 of 30 pallets redirected, caught in real time.

A global technology leader shipped more than 30 pallets of restricted, high-value hardware. Overhaul detected that 25 had been redirected to an unauthorized location, alerted the customer immediately, and enabled recovery before the loss became a violation. The result was \$60 million in diversion averted, and \$1 billion in orders unlocked once control was proven.



OVERHAUL RISK MONITOR. A SHIPMENT TRACKED THROUGH A HIGH-RISK CORRIDOR, WITH LIVE RISK SCORING, INVESTIGATION NOTES, AND RISKGPT IN ONE VIEW, SO THE TEAM CAN ACT WHILE THE LOAD IS STILL MOVING.

WHAT TO DO NEXT

Three decisions change the outcome.

Step 01

30 days

Assess

Commission a gap assessment of physical security, supply-chain vetting, and incident reporting across all active lanes and projects.

Step 02

90 days

Harden

Deploy live hardware tracking from manufacturer to site, extend screening to Tier 2 and Tier 3 partners, and brief carriers on the real threat profile.

Step 03

6 months

Lead

Engage Overhaul for in-transit risk management, join an intelligence-sharing program, and make security a contractual requirement.

Move your next shipment under active protection.

Device-agnostic, API-capable, and live in as little as 15 days. See. Protect. Control.

REQUEST A DEMO →

REQUEST A DEMO

over-haul.com/request-a-demo

INTELLIGENCE CONTACT

Danny Ramon, Director of Intelligence
danny.ramon@over-haul.com

CONTRIBUTE INTEL

Share supply-chain intelligence with the Overhaul LE Connect network.

SOURCES & REFERENCES

OVERHAUL FIRST-PARTY INTELLIGENCE

OVERHAUL United States Q2-2026 Cargo Theft Report. Incident volume, product types, methods, locations, and timing.

OVERHAUL AI Infrastructure Intel brief, H2 2026. Recorded AI-equipment losses, hidden-loss ratio, platform metrics.

OVERHAUL Platform figures, over-haul.com. \$1.4T protected, recovery rate, disruptions prevented.

OVERHAUL Intel Alert: Electronics Targeting, Poly-Criminal Network Escalation, 25 Aug 2026. Chip theft growth, deception rate, export flow, escort MO.

OVERHAUL High-Volume AI Parcel Networks case study. \$250K parcel visibility incident.

ACCREDITED THIRD-PARTY SOURCES

US DOJ Three Charged with Conspiring to Unlawfully Divert Cutting-Edge U.S. AI Technology. justice.gov/opa/pr/three-charged-conspiring-unlawfully-divert-cutting-edge-us-artificial-intelligence

S&P GLOBAL Data-center copper demand forecast, 1.1M mt (2025) to 2.5M mt (2040). S&P Global Commodity Insights.

US COMMERCE Bureau of Industry and Security FY2027 Congressional Budget Submission. commerce.gov.

MCKINSEY The cost of compute: a \$7 trillion race to scale data centers. mckinsey.com

INDUSTRY Flagship AI GPU rack pricing (~\$3M). DataGravity; Tom's Hardware.

SYNERGY Hyperscale data center count (1,100+). Synergy Research Group.

Overhaul records only cargo thefts reported by reliable sources, including transportation security councils, insurance companies, and law-enforcement organizations, and reported totals for recent periods typically rise as later reports arrive. Figures are attributed to their source and reporting period. Third-party product and company names are the property of their respective owners and are referenced for identification only. References to enforcement actions are drawn from public records.