EFROS · TRANSPORTATION & LOGISTICS SECURITY

Cargo Fraud Defense

One inbox. One stolen truckload.

Cyber-enabled cargo theft is now the fastest-growing freight loss in the country. Here is how it works, and how to find your exposure before the criminals do.

Cargo theft went digital.

The thieves taking the most freight in 2025 never touched a fence or a lock. They compromised an inbox. A single hijacked dispatcher, broker, or accounts-payable email is now enough to reroute a full truckload and make it disappear.

$725M
Cargo theft losses in 2025, up 60% over 2024 (Verisk CargoNet)

+1,500%
Growth in strategic theft since 2022: fictitious pickups, double brokering, document fraud

$273,990
Average value of a single stolen load, up 36% year over year

HOW THE SCAM RUNS

Four steps, no break-in required.

1. **Compromise**
   A phishing email harvests the password of a dispatcher, broker, or payables inbox.
2. **Impersonate**
   Using that identity, the thief posts fraudulent listings on load boards as your company.
3. **Reroute**
   They accept a real load as “you,” then redirect the driver, or change where the payment goes.
4. **Vanish**
   The freight is gone. Shipper, broker, and carrier each assumed the others were legitimate.

> On April 30, 2026, the FBI’s IC3 issued a public warning that cyber-enabled strategic cargo theft is surging across the U.S. freight network.

Find the gap in two weeks.

The Cargo Fraud Defense Assessment maps exactly how an attacker would hit your operation, from the inbox to the TMS. You get a risk-scored report and a prioritized fix list. Then EFROS closes the gaps.

WHAT THE ASSESSMENT COVERS

1. **Autonomous penetration test**
   Horizon3 NodeZero runs a real attack against your external perimeter, the way a criminal would.
2. **Email & BEC defense audit**
   Plus a DMARC, SPF, and DKIM enforcement check. This is the door the thieves use.
3. **External attack-surface scan**
   Everything about your operation an attacker can see from the public internet.
4. **Microsoft 365 hardening review**
   MFA, conditional access, and the mail rules attackers plant to hide their tracks.
5. **Dark-web & credential-leak check**
   Company logins already exposed in breaches and sitting on criminal markets.
6. **Broker, shipper & insurer gap check**
   Where you fall short of the cyber requirements your partners now demand.

FROM ASSESSMENT TO ALWAYS-ON DEFENSE

What EFROS deploys after the report: AI anti-BEC email security that stops impersonation, DMARC enforced to reject, a documented payment-change call-back rule, 24/7 monitoring, and immutable backup that keeps your TMS dispatching through an attack.

> One stolen load, or one day you cannot dispatch, costs more than the assessment. This is the cheapest insurance in your operation.