

THREATDEFEND FOR TRANSPORTATION & LOGISTICS

Protecting uptime, delivery operations, and digital dispatch systems

Relevant ThreatDefend Modules



Falcon EDR/XDR

Secure TMS platforms, handhelds, dispatch consoles, and driver endpoints



Falcon Identity

Monitor login activity and enforce secure access to portals and mobile apps



Falcon Discover

Gain visibility into connected devices, cloud tenants, and shadow IT



Falcon Exposure

Prioritize vulnerabilities tied to delivery chains and fleet uptime



Cribl Stream

Manage logs from logistics apps, warehouse platforms, and route planners

Top Cybersecurity Threats Facing Transportation & Logistics

1

Ransomware Disruption

Interrupting delivery timelines by locking dispatch or routing systems

2

Account Misuse

Compromised driver, admin, or vendor accounts used to reroute goods or access systems

3

Visibility Gaps

Inability to detect or trace issues across distributed logistics infrastructure

Take Action

Transportation companies must protect uptime, secure access, and meet cyber requirements in a supply chain ecosystem that demands resilience and speed.

Why It Matters

Logistics providers are critical to global commerce. Delays or breaches impact customer trust, violate SLAs, and create ripple effects across entire supply chains.