Singtel

Securing logistics in the age of bots, boxes and breaches

Autonomous vehicles are reshaping how goods are transported and delivered. From driverless trucks to robotic warehouse systems, logistics is entering a new era of connectivity. By 2035, autonomous trucking alone could represent a **$600 billion** opportunity.[1] But this shift doesn't stop at the highway.

Warehouse picking
AI-guided robots adapt in real time

Inventory management
Predictive systems maintain optimal stock levels

Last-mile delivery
Autonomous drones and vehicles navigate complex terrain

Every connected device is a potential breach point

As autonomy gains ground, the number of digital endpoints embedded in logistics is exploding. While each one helps streamline operations, it also expands the attack surface. By 2030, the world will see **over 40 billion IoT devices.**[2] What powers autonomous operations also introduces new risks.

Robots
Performing tasks, collecting data, and syncing with control systems

Warehouse management systems (WMS)
Cloud-connected and mission-critical

RFID readers
Tracking goods across supply chains in real time

Cameras and sensors
Monitoring movement, safety, and environmental conditions

But many of these devices still run with open vulnerabilities

Unauthenticated access
Default credentials or exposed control interfaces

Firmware flaws
Outdated software that attackers exploit with ease

Unsecured traffic
Data in transit that's unencrypted or misrouted

In logistics, digital threats create physical disruption. A compromised robot can halt fulfilment. A hijacked WMS can derail inventory flows. An exploited sensor can take down temperature-controlled shipments.

Cyber attacks are disrupting supply chains at alarming rates

Cyber criminals are hitting logistics systems where it hurts: third-party vendors, warehouse platforms, and transport networks. The goal is disruption. The transportation and warehousing sector now accounts for **64.33% of cyber threats targeting supply chain disruptions**. Warehouse management systems, logistics software, and cloud Transportation Management Systems (TMS) are increasingly exploited to halt operations and create bottlenecks.[3]

The average cost of a breach in this sector is
$4.18 million.[4]

For small logistics firms, the impact is often irreversible.
60% shut down within six months
of a major cyber attack.[4]

The U.S. alone accounts for
53.85%
of ransomware incidents in logistics, likely due to its vast supply chain network and reliance on digital logistics platforms.[3]

Weapons of a supply chain sabotage

Phishing & social engineering
AI-crafted lures targeting frontline workers

Ransomware
Disabling telematics, freezing TMS platforms, and halting fleet operations

IoT vulnerabilities
Exploiting weak authentication, unsecured APIs, and misconfigured devices

Third-party risk
Compromising one vendor to bring down entire ecosystems

When logistics stops, business stops

JAS Worldwide (2024)[4]
A ransomware attack brought global freight operations to a halt. Customers lost visibility into shipments for days, leading to widespread disruption. Even with local workarounds, the outage exposed the fragility of digital-first logistics and the high cost of reactive security.

➔ **When visibility goes offline, trust and control follow.**

KNP Logistics (2023)[4]
Once one of the UK's top privately owned freight firms, KNP collapsed after a cyber attack crippled its systems and compromised financial data. Within weeks, the company filed for insolvency, laid off staff, and ceased operations entirely.

➔ **One breach is enough to take down an entire business.**

Operational downtime
translates directly to lost shipments, missed SLAs, and revenue loss

Customer trust erodes
fast when visibility disappears and timelines slip

Regulatory non-compliance
leads to fines, audits, and lasting reputational damage

Powering the connected logistics chain with Singtel

From fleet sensors to cross-border tracking systems, every connected endpoint in logistics is a potential entry point. Securing the supply chain means securing the network it runs on.

Singtel's enhanced Multi-Domestic Connectivity solution, developed in collaboration with floLIVE and Lenovo Connect, provides logistics operators with what today's environment demands:
secure, compliant, and global IoT expansion.

- Localised by design to meet telecom and data regulations in 190+ markets
- Centrally managed local connectivity with seamless switching between mobile networks via multi-IMSI and the latest eSIM IoT Standards - eUICC (SGP.32)
- Real-time visibility and control via a unified Aggregator Connectivity Management Platform (CMP)
- Built for Original Equipment Manufacturers (OEMs) to expand to overseas markets — faster, more efficiently, and with full compliance

Secure your logistics operations in the age of autonomy

Discover more

References

1 EY, Embracing the automation revolution in trucking, 2023
2 IoT Analytics, State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally, 2024
3 SOCRadar, GLOBAL LOGISTICS & TRANSPORTATION INDUSTRY Threat Landscape Report, 2025
4 Built for mission-critical industries already trusted by global automotive OEMs