eutronix
innovate. automate. elevate.

www.eutronix.eu

WHITE PAPER

Driving Cyber Resilience in Transportation & Logistics

—

NIS2 COMPLIANCE WITH SOTI ONE

SOTI ONE

WHITE PAPER

Driving Cyber Resilience in Transportation & Logistics: NIS2 Compliance with SOTI ONE

Executive Summary

The transportation and logistics industry is the circulatory system of our economy – moving goods and people with ever-increasing reliance on digital technology. From truck drivers using tablets for route management to warehouses filled with scanning devices and smart sensors, mobility and IoT are revolutionizing operations. But this digital drive comes with new cyber risks.

Recognizing transport as critical infrastructure, the EU's NIS2 directive imposes strict cybersecurity standards on transportation and logistics operators. Companies must secure real-time data exchanges, protect their supply chains from breaches, and be prepared for threats like ransomware that could halt distribution networks.

This white paper examines the unique challenges that logistics firms in Western Europe face under NIS2 – including managing thousands of mobile endpoints across geographies, addressing vulnerabilities introduced by third-party partners, and ensuring 24/7 uptime in delivery systems.

It then showcases how SOTI MobiControl and the SOTI ONE Platform help tackle these challenges head on. Key features such as centralized device management, continuous visibility into device health, remote troubleshooting, and security policy enforcement are highlighted as enablers of both compliance and operational efficiency. We share anonymized success stories where logistics companies have saved hundreds of thousands of euros by implementing SOTI, through reduced device downtime, faster deployments, and improved security of their mobile fleet. For CIOs, CISOs, and operations managers in

transport and logistics, this paper provides a roadmap to turn NIS2 obligations into an opportunity – to modernize device management, strengthen cybersecurity posture, and keep shipments on schedule. A concluding section outlines actionable next steps like demos, guides, and compliance reviews to accelerate your journey toward NIS2 readiness.

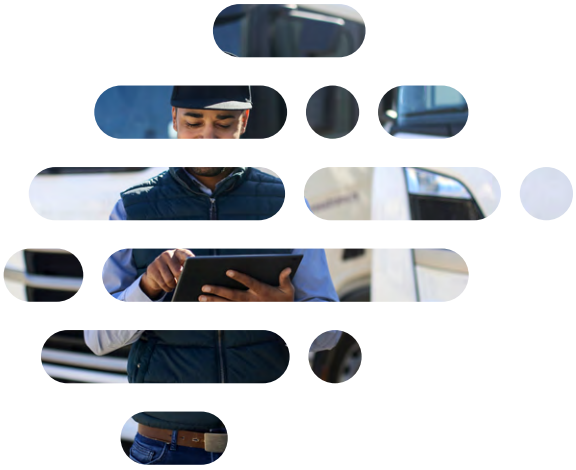
Introduction: Mobility at the Wheel of Logistics – and Its Risks

In the world of transportation and logistics, speed and efficiency are king. Whether it's a trucking company delivering goods across borders or a distribution center managing inventory, timely information flow is critical. Today, that flow is facilitated by mobile computers, rugged handhelds, vehicle telematics units, and a plethora of connected devices (barcode printers, GPS trackers, temperature sensors in cold-chain logistics, etc.).

In many ways, these endpoints are the new "crew" ensuring packages arrive on time and operations run smoothly.

However, the flip side is that the industry has become a prime target for cyber threats. A ransomware attack that brings down a shipping company's dispatch system or a breach that manipulates a rail operator's data can have **destructive ripple effects throughout society** – delaying goods, harming businesses, even endangering lives if critical supplies don't reach their destination. That's why NIS2 classifies transport as an essential sector and demands robust cybersecurity measures from operators.

Companies must secure both their IT and OT (operational technology) systems, vet the security of their vendors, and ensure continuity of critical logistics services even under duress.



For logistics IT teams, this means grappling with challenges like:

- How do we keep thousands of mobile devices used by drivers and warehouse staff up-to-date and secure, without burdening a small IT department?
- How can we instantly support a driver with a malfunctioning navigation tablet 500 km away?
- Are our barcode scanners and vehicle-mounted devices protected against unauthorized access?
- And how do we prove to regulators (and customers) that our cybersecurity and incident response capabilities meet the new standards?

This introduction frames the stakes for transportation and logistics companies in Belgium, France, the Netherlands, Luxembourg and across Europe. In the sections that follow, we'll detail the challenges of NIS2 compliance in this sector and how a unified endpoint management solution can become a linchpin for both compliance and smoother operations.

Key Cybersecurity and Compliance Challenges in Transport & Logistics

1. **Geographically Dispersed Mobile Fleet**
Logistics firms might have devices spread across multiple countries – in trucks, ports, warehouses, and hubs. Managing and updating these devices manually is nearly impossible. Ensuring each one complies with security policies (correct configurations, latest patches) is a huge challenge, especially as drivers are always on the move and devices may only intermittently connect to company networks.

2. **Ransomware and Downtime Threats**
The transport sector has been increasingly hit by ransomware, which can disrupt routing systems, warehouse automation, or customer-facing portals. Unlike some industries, logistics runs on tight delivery timelines – a few hours of system downtime can create backlog and contract violations. NIS2 pushes operators to minimize the risk of service disruption, so companies need rapid disaster recovery and the ability to isolate and fix infected devices quickly before malware spreads.

3. **Supply Chain & Third-Party Vulnerabilities**
Logistics is inherently collaborative, involving partners, subcontractors, and clients' systems. A weakness in a contractor's device (say a courier's unsecured smartphone used for deliveries) can introduce vulnerabilities into the whole network. Verifying that external drivers or 3PL providers adhere to your security standards is tough. NIS2 requires evaluating and managing these external risks, meaning logistics companies must extend certain security controls to devices and systems beyond their immediate ownership.

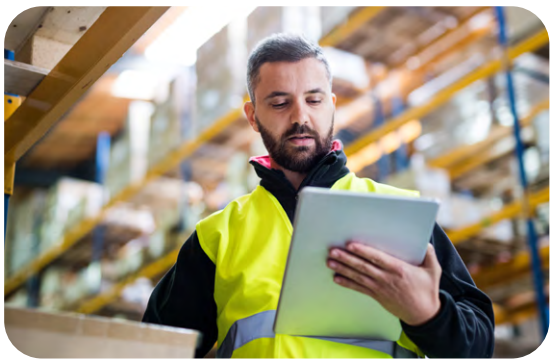
4. **Proliferation of Connected Devices**
Modern logistics operations employ IoT extensively – telematics units in trucks, smart fleet management devices, RFID readers, autonomous warehouse robots, industrial printers for labels, etc. Each connected device is a potential entry point if not managed. The more devices, the more attack surface. For example, an unsecured warehouse printer could be hacked to disrupt printing of picking lists, stalling shipments. Ensuring all these non-traditional endpoints are updated and monitored is a key challenge.

5. **Limited IT Staff & Budget Focus**
Traditionally, many logistics companies prioritized efficiency and cost-cutting in operations, sometimes at the expense of IT investment. Cybersecurity might not have been top-of-mind. Now, under NIS2's mandate (and given rising threats), they must ramp up capabilities quickly. Yet many still have lean IT teams that must do more with the same resources. Automation and effective tools are needed to bridge this gap.

6. **Real-Time Data Protection**
Real-time data exchange is vital (e.g., live GPS tracking, instant electronic proof-of-delivery, real-time inventory updates). NIS2 mandates securing these data flows to ensure confidentiality and integrity. That means devices must use encryption, strong authentication, and be protected against eavesdropping or tampering. A challenge here is making security seamless; drivers shouldn't have to be IT experts to connect securely from anywhere.

7. **Employee Awareness & Human Error**
Drivers and warehouse workers, like any employees, can be tricked by phishing or might misuse devices (like installing a game that contains malware). NIS2 emphasizes regular training and cyber hygiene. In practice, logistics firms need ways to educate and update a distributed workforce on security practices – and possibly enforce certain behaviors via technology (for example, blocking access to risky websites on corporate devices).

In summary, transportation and logistics companies operate in a high-wire act: they must keep goods flowing at pace, across borders and partners, and keep a vigilant eye on a myriad of devices and systems that could be targeted by cyberattacks. The next section explains how SOTI's mobile and IoT management solutions are tailor-made to mitigate these challenges, strengthening security while streamlining device deployment and support.



SOTI

SOTI Solutions for Logistics: Securing Endpoints, Ensuring Compliance

Unified, Scalable Device Management

Whether you have 100 devices or 100,000, SOTI MobiControl scales to manage them with ease. In fact, it's so powerful and user-friendly that a **single IT person can manage over 100,000 Android devices worldwide using SOTI MobiControl**. This centralization is a game-changer for dispersed logistics operations. From headquarters, IT can remotely manage configuration and security for every rugged scanner, in-cab tablet, and mobile computer in the field. The platform supports Android, iOS, Windows and Linux, covering the variety of devices found in transport environments. With SOTI's **Express Enrollment** features, new devices can be provisioned in minutes – shipped directly to a remote site and automatically configured on first boot. This ensures rapid deployment of secure devices as you expand or replace units, with minimal hands-on IT effort. Crucially, central management means uniform enforcement of security policies across the fleet, which is essential for NIS2 compliance. No device falls through the cracks.

Real-Time Device Visibility & Health Monitoring

SOTI MobiControl provides deep visibility into each device's status: you can see where a device is (via GPS), what apps are running, memory/battery levels, and if any **security or compliance risks** are present. For instance, if a driver's handheld starts operating outside of its normal parameters (perhaps indicating a malfunction or malware), SOTI can alert IT. The platform's dashboard can highlight devices that haven't checked in (maybe lost signal or turned off), so you can follow up proactively. This visibility extends to IoT endpoints via SOTI Connect – e.g., you can monitor printer performance and catch issues early. By having a finger on the pulse of every device, logistics companies can prevent small problems from snowballing into major outages. And if auditors ask for proof of monitoring, these capabilities demonstrate an active stance on risk management.

Remote Troubleshooting & Zero-Touch Support

Logistics firms often cannot afford to bring devices back to a central office for fixes – that wastes days and disrupts workflows. SOTI MobiControl's **Remote Control** function enables 100% remote support. IT staff can virtually take over a device's screen, push settings or patches, and even reboot devices remotely. In practice, this means when a truck driver has a tablet issue on the road, they can call IT and have it resolved without leaving the cabin. One logistics company reports that with SOTI, issues that previously took "several days of lost productivity" (shipping hardware back and forth) are now solved immediately over the air. By dealing with problems swiftly, you **reduce downtime and keep deliveries on schedule**.
For NIS2, this agility in incident response and recovery is exactly what regulators (and your customers) want to see. It demonstrates resilience.

Robust Security and Compliance Features

SOTI MobiControl embeds numerous security controls to protect devices and data. You can enforce device authentication (PIN/biometric) and encryption, ensuring that if a device is lost or stolen, logistics data (like manifests, customer info, or access credentials) isn't exposed. **Geofencing** capabilities allow setting rules based on location – for example, you might restrict a warehouse device so it only functions within the facility's perimeter, adding a layer of physical security.
The platform's **Kiosk Mode** is especially useful in logistics: it locks devices to approved apps only. For instance, a delivery driver's tablet might be limited to the dispatch app, maps, and a communication tool – nothing else. This prevents distractions and eliminates the risk of malware from unsanctioned downloads. It also protects sensitive supply chain data on the device by isolating it within controlled apps. SOTI also makes it easy to push OS updates and security patches company-wide at scheduled times, so all devices stay up-to-date without disrupting operational peak hours. By keeping devices hardened and standardized, companies can meet NIS2's requirements for up-to-date systems and controlled access.

Secure Content and Application Management

In the logistics field, employees often need access to documents (e.g., customs forms, safety procedures) or in-house apps for various tasks. SOTI enables secure distribution of content via its content management features – ensuring files are only accessible within a secure container on authorized devices. For application management, SOTI supports deploying private enterprise apps as well as managing public app store apps. You can remotely install, update, or remove apps on devices in bulk. This is critical for plugging security holes (e.g., quickly removing an app found to be vulnerable) and for rolling out new capabilities. It also ties into compliance: for example, if NIS2 or internal policy says an end-of-life app must not be used, SOTI can guarantee it is scrubbed from all endpoints.

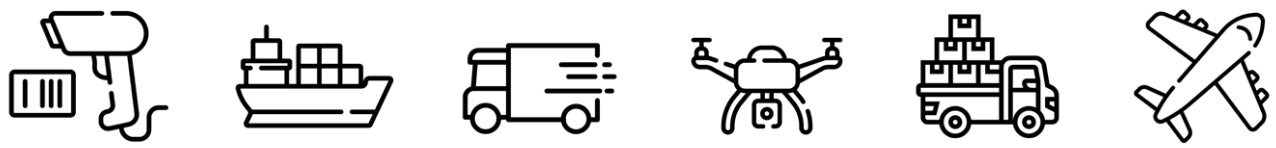
IoT and Printer Security with SOTI Connect

In a logistics warehouse or hub, industrial printers, smart conveyors or sensors are part of daily operations. **SOTI Connect** extends SOTI's management to these devices, providing a **single point of control for diverse printer makes and models across locations**. IT can rapidly deploy new printers with standardized settings, monitor their usage (e.g., how many labels printed, any errors), and run remote diagnostics. Importantly, it addresses a commonly overlooked gap: printer security. SOTI Connect allows enforcing password policies on printer control panels, pushing digital certificates, and even tracking a printer's physical location. If someone moves a printer or tampers with it, IT knows. Firmware updates can be done remotely as well, meaning security patches for printers are not neglected. This ensures that attackers can't, for instance, exploit an outdated printer OS to pivot into your network. Considering NIS2's focus on securing supply chain and OT systems, having printers and similar devices under watch is a significant compliance and security win.

Analytics and ROI Optimization

An added benefit of SOTI ONE for logistics is analytics through tools like SOTI XSight. This isn't directly a compliance feature, but it helps optimize operations by analyzing device data for recurring issues or performance bottlenecks. For example, analytics might show that a particular model of scanner is failing frequently in a certain warehouse – insight you can use to preempt downtime. Optimized, well-functioning devices indirectly support security (fewer weird workarounds or shadow IT when official tools work well) and certainly improve ROI. One UK logistics company using SOTI reported saving **more than £250,000 per year** in device management costs and productivity gains – a compelling figure for budget-conscious organizations. Part of these savings came from cutting device setup time by over 80% (from 30 minutes per device to under 5 minutes) through SOTI's automation, and part from reducing travel and shipping costs due to remote support. These efficiencies free up resources that can be reinvested into further security improvements or other innovations.

A robust EMM solution helps keep logistics operations secure and running. Above: a conceptual image of mobile security – devices are protected by enforced policies (shield icon) that can be toggled company-wide. SOTI MobiControl ensures every field device stays in "security ON" mode by default.



Success Stories in Transportation & Logistics

A large delivery provider exemplifies how centralized mobility management yields both security and efficiency gains

A large delivery provider exemplifies how centralized mobility management yields both security and efficiency gains. Our partner operates across multiple European countries, equipping drivers with Android handhelds for scanning packages and receiving routes, and using tablet kiosks in depots for inventory tracking. Before SOTI, their small IT team was overwhelmed trying to manage these thousands of devices manually. Devices often had inconsistent settings; some drivers would delay OS updates or install unauthorized apps (like social media), leading to security gaps and even occasional malware infections.

When a device malfunctioned, it had to be mailed back to HQ, taking days – during which a driver had to use a spare or paper-based process, slowing deliveries.

After adopting SOTI MobiControl, The delivery provider saw a dramatic turnaround.

The IT team now manages the entire **global device fleet from one console**, with profiles ensuring every device is compliant with corporate security policies. If a driver attempts to disable a security setting, SOTI will automatically re-enable it or alert IT. Devices that fall out of contact or show signs of compromise are immediately flagged.

According to our customer IT manager, what used to require a whole team's effort is now largely automated – one admin can handle what ten people struggled with before. In fact, they noted that **one administrator now oversees about 5,000 devices single-handedly**, something only possible with SOTI's powerful automation (echoing the scale achieved by Delivery Hero in a similar context). This has allowed our partner to reassign staff to proactive improvement projects rather than firefighting device issues all day.

Crucially, our partner also leveraged SOTI Snap (the rapid app development component of SOTI ONE) to improve compliance and training.

They created a simple mobile app for drivers that delivers short cybersecurity training modules and quizzes directly on their handhelds – covering topics like recognizing phishing or proper device handling. Thanks to **SOTI Snap's easy distribution**, every driver was periodically prompted to complete these modules, which are tracked centrally. This creative approach significantly increased employee participation in security awareness training (a NIS2 objective) without pulling drivers into classroom sessions.

The HR team could update the training content through SOTI Snap and push it out instantly to all devices.

Another success story comes from a Dutch logistics firm (we'll call them "Fleetoran") specializing in construction materials transport.

Another success story comes from a Dutch logistics firm (we'll call them "Fleetoran") specializing in construction materials transport. Fleetoran faced issues with drivers using personal phones for work, resulting in inconsistent app versions and security postures. They also had about 20 apps that each driver needed (navigation, delivery scheduling, timesheets, etc.), and setting up a new device for a driver took nearly half an hour of manual configuration.

After implementing SOTI MobiControl and providing company-issued devices, Fleetoran achieved a configuration time per device of under 5 minutes – a reduction of over 80%.

This was done by creating a profile in SOTI that auto-installs all required apps and settings when a device enrolls. The **time savings equated to over €250,000 annually** considering their device volumes and the reduced need for IT staff overtime. Moreover, device security improved drastically: with **SOTI's Kiosk Mode limiting access to essential apps and its Remote Control enabling fast troubleshooting**, Fleetoran virtually eliminated the days of downtime that used to plague them when devices had to be sent in for support.

A SOTI representative noted that by deploying the **SOTI ONE Platform**, Fleetoran gained the ability to "troubleshoot issues remotely, secure devices and apps from external threats, and stay up to date on compliance needs" – exactly the multifaceted value required to thrive under NIS2.

Today, Fleetoran reports that drivers start their day with fully functional tools and confidence that those tools are secure, while management rests easier knowing they have visibility and control to nip any security issue in the bud.

These stories underscore a common theme: integrating a solution like SOTI can turn device management into a strategic asset rather than an operational headache.

Companies not only tick the compliance boxes (with documented security controls, audit logs, training, etc.), but also derive cost savings and productivity boosts.
The journey to NIS2 compliance thus becomes an opportunity to modernize and streamline, as much as it is a regulatory response.

Conclusion & Next Steps for Logistics Leaders

The writing is on the wall: cybersecurity is now as fundamental to transportation and logistics as fuel in the trucks or software in the warehouse.

The NIS2 directive is accelerating a mindset shift in the industry – security and compliance are no longer "IT problems" but core components of business continuity and service reliability. For CIOs, CISOs, and operations executives in logistics, the question isn't whether to enhance cybersecurity around mobile and IoT devices, but how best to do it without impeding the fast flow of logistics operations.

This white paper has shown that with the right tools, particularly a robust mobile and endpoint management platform, you don't have to choose between security and efficiency.

SOTI MobiControl and the SOTI ONE Platform deliver both: they empower your lean IT teams to manage vast, distributed device ecosystems with unprecedented control and automation, while also improving end-user experience (drivers, warehouse staff get better support and reliable devices). In the context of NIS2, SOTI provides the technical means to implement many required measures – from asset inventory and access control to incident response and continuous monitoring – in one coherent solution. The result is a logistics operation that's **cyber-resilient** (able to withstand and rapidly recover from attacks) and compliant by design, all without breaking stride in daily deliveries.

By adopting SOTI's platform, companies in trucking, rail, air cargo, and warehousing have reported tangible benefits: dramatic cuts in device downtime, significant cost savings on IT and support, and increased confidence from their clients and partners in the security of their services. These outcomes speak to a competitive advantage; as NIS2 elevates the bar, those who invest early in compliance and security will gain trust and possibly market share over those who lag. There's also peace of mind in knowing that a lost device won't turn into a data breach headline, or that a cyber incident can be contained with minimal service impact because you had the tools to act immediately.

Now is the time to act

NIS2 deadlines are looming, and cyber threats continue to evolve. Ensuring your mobile operations are secure and compliant should be high on your 2025 agenda.

THE GOOD NEWS IS, YOU DON'T HAVE TO NAVIGATE THIS ALONE.

Next Steps

1. Book a Demo
See SOTI MobiControl in action in a live demo tailored to a transport/logistics scenario. Watch how easily you can locate a device, update its software, or remotely resolve an issue. Seeing is believing – and it's the first step to envisioning how it fits in your operation.

2. Request a NIS2 Readiness Consultation
Our SOTI experts can conduct a brief review of your current device management setup and identify gaps relative to NIS2 requirements. We'll share best practices and suggest a roadmap to achieve compliance efficiently. Consider this a friendly check-up on your cyber health – with actionable insights you can use immediately.

In conclusion

In conclusion, aligning with NIS2 is not just about avoiding fines or meeting a legal obligation – it's about building a stronger, smarter logistics operation for the future. By leveraging the SOTI ONE Platform, you can turn your fleet of devices into a competitive edge: highly secure, deeply integrated, and reliably performing day in and day out.

Contact eutronix today to start this journey.

LET'S ENSURE THAT WHILE YOUR TRUCKS AND PACKAGES MOVE FAST, YOUR CYBERSECURITY REMAINS ROCK SOLID.

Your customers, partners, and regulators will thank you – and you'll sleep better at night knowing you have full control of your mobile world. Safe and secure travels on the road ahead!

www.eutronix.eu

Is your supply chain really up to speed with NIS2 requirements?

Don’t let compliance become a simple catch-up exercise: anticipating now means transforming a regulatory constraint into a driver of efficiency and confidence for all your operations.
By drawing on the joint expertise of eutronix and SOTI, you can secure your mobile terminals, streamline your data flows and guarantee the continuity of service your customers expect.

Contact our experts today.
We look forward to discussing how we can tailor our solution to your specific needs.

eutronix Belgium
1300 - Wavre

+32 10 39 49 00

Contact us

eutronix France
78870 - Bailly

+33 1 34 61 61 46

Contact us

eutronix Netherlands
4744 RZ Bosschenhoofd

+31 76 52 45 330

Contact us

About eutronix

- Dynamic company specializing in hardware solutions and electronic automation equipment
- Value-added distributor
- Founded in 1999
- Headquarters in Belgium
- Branches or subsidiaries in France, the Netherlands and the United Kingdom
- A team of 40+ people

eutronix’s markets

- Healthcare
- Hospitality
- Retail
- Leisure
- Transport & logistics
- Industry
- Access control & people identification
- Signalling
- Field service
- Oem & IoT