

LIVRE BLANC

Renforcer la cyber-résilience dans le transport et la logistique

—
CONFORMITÉ NIS2 AVEC SOTI ONE**SOTI ONE**

LIVRE BLANC

Renforcer la cyber-résilience dans le transport et la logistique : conformité NIS2 avec SOTI ONE

Résumé

Le secteur du transport et de la logistique est le **système circulatoire de notre économie** – il assure le déplacement des biens et des personnes, avec une dépendance croissante aux technologies numériques. Des chauffeurs routiers utilisant des tablettes pour la gestion des itinéraires aux entrepôts remplis de terminaux de scanning et de capteurs intelligents, la mobilité et l'IoT révolutionnent les opérations. Mais cette transformation numérique s'accompagne de **nouveaux risques cyber**.

Reconnaissant le transport comme une infrastructure critique, la directive NIS2 de l'Union européenne impose des normes strictes de cybersécurité aux opérateurs du transport et de la logistique. Les entreprises doivent sécuriser les échanges de données en temps réel, protéger leur chaîne d'approvisionnement contre les violations et se préparer à des menaces comme les ransomwares, qui pourraient paralyser des réseaux de distribution.

Ce livre blanc examine les **défis spécifiques** auxquels sont confrontées les entreprises logistiques d'Europe de l'Ouest dans le contexte de NIS2 – notamment la gestion de milliers de terminaux mobiles dispersés géographiquement, la prise en compte des vulnérabilités introduites par des partenaires tiers, et l'assurance d'une disponibilité opérationnelle 24h/24 et 7j/7.

Il présente ensuite comment **SOTI MobiControl** et la plateforme SOTI ONE permettent de relever ces défis de front. Des fonctionnalités clés comme la gestion centralisée des appareils, la surveillance continue de leur état de santé, le dépannage à distance et l'application des politiques de sécurité sont mises en avant comme leviers de conformité et d'efficacité opérationnelle.



Nous partageons également des **cas clients anonymisés**, montrant comment des entreprises logistiques ont économisé des centaines de milliers d'euros en déployant SOTI – grâce à une réduction des pannes d'appareils, des déploiements plus rapides et une meilleure sécurité de leur flotte mobile.

Pour les CIOs, CISOs et responsables des opérations dans le secteur du transport et de la logistique, ce livre blanc propose une feuille de route pour transformer les obligations de NIS2 en une **opportunité de modernisation** : renforcer la gestion des terminaux, améliorer la posture de cybersécurité et maintenir la fluidité des livraisons.

Une dernière section propose des actions concrètes comme des démonstrations, des guides et des revues de conformité pour accélérer votre mise en conformité NIS2.

Introduction : La mobilité au cœur de la logistique – et les risques qui l'accompagnent

Dans le secteur du transport et de la logistique, la rapidité et l'efficacité sont essentielles. Qu'il s'agisse d'une entreprise de transport assurant des livraisons transfrontalières ou d'un centre de distribution gérant les stocks, l'échange d'informations en temps réel est **devenu indispensable**. Aujourd'hui, ces échanges reposent sur des ordinateurs mobiles, des terminaux durcis, des systèmes télématiques embarqués et une multitude d'équipements connectés – scanners de codes-barres, traceurs GPS, capteurs de température pour les produits sensibles, etc.

D'une certaine manière, ces terminaux constituent la nouvelle "équipe mobile" qui veille à ce que les colis arrivent à temps et que les opérations se déroulent sans accroc. Mais cette transformation numérique a aussi **attiré l'attention des cybercriminels**.

Le secteur est de plus en plus ciblé par des attaques : une attaque par ransomware qui paralyse le système de répartition d'un transporteur ou une fuite de données impactant un opérateur ferroviaire peut avoir des conséquences sociétales importantes – retards, pertes économiques, voire risques vitaux si des biens essentiels n'arrivent pas à destination. C'est pourquoi la directive NIS2 classe désormais le transport comme un **secteur essentiel** et exige des mesures de cybersécurité renforcées.

Les entreprises doivent **sécuriser** à la fois leurs systèmes informatiques (IT) et leurs systèmes opérationnels (OT), évaluer la sécurité de leurs fournisseurs, et garantir la continuité de leurs services logistiques – y compris en cas de crise.



Pour les équipes IT du secteur, cela pose des questions complexes :

- Comment **maintenir à jour et sécuriser** des milliers de terminaux mobiles utilisés par des chauffeurs et des agents d'entrepôt, sans surcharger une petite équipe informatique ?
- Comment **dépanner à distance** un chauffeur dont la tablette de navigation est défectueuse à 500 km du siège ?
- Nos scanners ou appareils embarqués sont-ils **protégés** contre tout accès non autorisé ?
- Et surtout : comment démontrer aux régulateurs (et aux clients) que nous respectons bien les **exigences de cybersécurité** et que nous sommes capables de **réagir rapidement** en cas d'incident ?

Cette introduction plante le décor pour les opérateurs de transport et de logistique en Belgique, en France, aux Pays-Bas, au Luxembourg et dans toute l'Europe. Les sections suivantes détaillent les **exigences de la directive NIS2 dans ce secteur**, et comment une solution centralisée de gestion des terminaux peut être la clé pour répondre à la fois aux besoins de conformité et d'efficacité opérationnelle.

Principaux défis en cybersécurité et conformité dans le transport et la logistique

1 Une flotte mobile dispersée géographiquement

Les entreprises logistiques déploient souvent des appareils dans plusieurs pays – à bord de camions, dans des entrepôts, sur des quais ou dans des hubs de distribution. Gérer et mettre à jour ces appareils manuellement devient vite ingérable. Il est pourtant crucial de s'assurer que chaque terminal est bien configuré, à jour, et conforme aux exigences de sécurité, même si les utilisateurs sont souvent en déplacement et rarement connectés au réseau interne de l'entreprise.

2 Risque accru de ransomware et d'interruptions

Les ransomwares ciblent de plus en plus les systèmes critiques du secteur : logiciels d'ordonnancement, automatisation d'entrepôt, portails clients... Contrairement à d'autres industries, la logistique repose sur des délais ultra-serrés. Quelques heures d'arrêt peuvent entraîner des retards majeurs, des pénalités contractuelles, ou une rupture de la chaîne d'approvisionnement. NIS2 impose de limiter ces interruptions en ayant des plans de continuité robustes, capables d'isoler et de restaurer rapidement les appareils compromis.

3 Vulnérabilités liées aux partenaires et à la chaîne d'approvisionnement

La logistique est un écosystème collaboratif : sous-traitants, partenaires 3PL, outils interconnectés... Si un prestataire utilise un appareil mal sécurisé (par exemple un smartphone personnel d'un livreur), cela peut compromettre l'ensemble du réseau. NIS2 exige que les entreprises évaluent et maîtrisent les risques liés aux tiers, y compris sur des systèmes qu'elles ne contrôlent pas directement. Cela oblige à étendre les politiques de sécurité à l'ensemble de l'écosystème.

4 Explosion des équipements connectés (IoT)

La logistique moderne intègre de nombreux objets connectés : télématique embarquée, lecteurs RFID, robots d'entrepôt, imprimantes industrielles, etc. Chaque appareil constitue une porte d'entrée potentielle pour une attaque. Plus il y a de terminaux, plus la surface d'exposition augmente. Un simple périphérique oublié – comme une imprimante en réseau – peut être détourné pour saboter des étiquettes ou injecter du code malveillant. Leur supervision et leur sécurisation sont donc indispensables.

5 Des équipes IT limitées face à des exigences croissantes

Historiquement, les entreprises logistiques ont privilégié les gains d'efficacité et la maîtrise des coûts, souvent au détriment des investissements IT. Mais avec NIS2 et la montée des cybermenaces, elles doivent agir vite. Or, les équipes informatiques restent souvent restreintes, et doivent "faire plus avec moins". Automatiser la gestion des appareils et s'appuyer sur des outils efficaces devient vital.

6 Sécurisation des flux de données en temps réel

La logistique repose sur la circulation rapide de l'information : tracking GPS, bons de livraison numériques, mise à jour des stocks... NIS2 impose de garantir la confidentialité et l'intégrité de ces flux. Cela suppose des terminaux chiffrés, authentifiés, et protégés contre les interceptions. La difficulté : rendre cette sécurité transparente pour l'utilisateur final, qui n'est pas un expert IT.

7 Facteur humain et manque de sensibilisation

Comme dans d'autres secteurs, les erreurs humaines restent une menace : ouverture d'un lien de phishing, installation d'une application douteuse, usage inapproprié d'un appareil... NIS2 souligne l'importance de la formation continue et de l'hygiène numérique. Mais dans un environnement dispersé et mobile, comment sensibiliser efficacement des chauffeurs ou magasiniers ? Il faut combiner pédagogie et contrôle technique, en bloquant les comportements à risque par défaut.



SOTI

Les solutions SOTI pour la logistique : sécuriser les terminaux, garantir la conformité

Gestion centralisée et évolutive des appareils

Qu'il s'agisse de gérer 100 ou 100 000 appareils, SOTI MobiControl s'adapte facilement. Sa puissance et sa simplicité permettent à un seul administrateur de superviser des flottes entières à l'échelle mondiale. Pour les entreprises logistiques réparties sur plusieurs sites, cette centralisation change la donne. L'équipe IT peut configurer, sécuriser et surveiller à distance les scanners durcis, tablettes embarquées ou terminaux mobiles utilisés sur le terrain.

Le système prend en charge Android, iOS, Windows et Linux – parfait pour l'écosystème hétérogène du transport. Grâce à des fonctions comme l'enrôlement express, les appareils peuvent être livrés directement sur site et automatiquement configurés à l'allumage. Résultat : des déploiements plus rapides, plus sûrs et sans intervention IT physique. La conformité est assurée dès la mise en service.

Visibilité continue sur la santé des appareils

SOTI MobiControl fournit une vue complète en temps réel : localisation GPS, état de la batterie, applications installées, niveau de sécurité... L'équipe IT est alertée à la moindre anomalie – comme un comportement suspect pouvant indiquer une infection ou une défaillance technique.

Grâce à SOTI Connect, cette visibilité s'étend aussi aux objets connectés comme les imprimantes ou les capteurs. La maintenance devient proactive, évitant les incidents avant qu'ils ne perturbent l'activité. En cas d'audit, cette traçabilité permet de démontrer un pilotage actif de la cybersécurité.

Dépannage à distance et support instantané

Dans le transport, il est impensable de devoir renvoyer un appareil au siège en cas de panne. Grâce à la prise de contrôle à distance, l'IT peut diagnostiquer et corriger un problème à des centaines de kilomètres.

Un chauffeur en panne de tablette peut ainsi être aidé immédiatement, sans délai. Des clients indiquent que ce qui nécessitait auparavant plusieurs jours d'interruption est désormais réglé en quelques minutes. Résultat : moins de retards, un meilleur service, et une conformité renforcée sur les plans de continuité et de réponse aux incidents (exigences NIS2).

Politiques de sécurité robustes

SOTI MobiControl intègre des mécanismes de sécurité puissants : code PIN, biométrie, chiffrement, géorepérage... La Kiosk Mode permet de restreindre les appareils à des applications validées, comme la navigation, la messagerie d'entreprise ou les outils de livraison.

Cela évite les usages non maîtrisés (réseaux sociaux, jeux, apps à risque) et protège les données sensibles. Les mises à jour de sécurité et correctifs peuvent être déployés automatiquement, sans interrompre le travail. Toute la flotte reste ainsi homogène, sécurisée et conforme.

Distribution sécurisée des contenus et des apps

Les collaborateurs mobiles ont besoin d'accéder à des documents (ex. : bordereaux, consignes) ou d'utiliser des applications métier. SOTI permet de gérer cela de manière sécurisée :

- seuls les appareils autorisés peuvent accéder aux fichiers,
- les applications sont déployées, mises à jour ou désinstallées à distance.

Cela garantit que toutes les apps sont validées, à jour et conformes aux politiques de sécurité.

Supervision des imprimantes et de l'IoT via SOTI Connect

Les imprimantes industrielles, capteurs de température, systèmes d'étiquetage ou robots en entrepôt peuvent être centralisés avec SOTI Connect. Peu importe le constructeur ou l'emplacement.

L'IT peut gérer les firmwares, surveiller l'usage, anticiper les pannes et détecter toute tentative de manipulation ou de déplacement. Dans un contexte où NIS2 inclut aussi les systèmes OT, cette visibilité sur les équipements connectés est essentielle.

Analytics et retour sur investissement

La solution SOTI XSight permet d'analyser les données d'usage et d'identifier les points de friction : appareils moins performants, erreurs récurrentes, problèmes par site...

Un client a pu constater que certains scanners posaient problème dans un entrepôt spécifique – permettant d'agir avant que cela n'impacte les délais de livraison.

Les résultats sont concrets : moins de pannes, des déploiements accélérés, des économies significatives. Une entreprise logistique britannique a ainsi économisé plus de 250 000 € par an grâce à l'automatisation et la réduction des interventions IT.



Études de cas : Transport et logistique

Une grande entreprise de livraison montre comment la gestion centralisée des terminaux améliore à la fois la sécurité et l'efficacité.

Notre client opère dans plusieurs pays européens et fournit à ses chauffeurs des terminaux Android pour le **scan des colis et la gestion des itinéraires**. Des tablettes en mode kiosk sont également utilisées dans les dépôts pour suivre les stocks. Avant SOTI, l'équipe IT était dépassée par la gestion manuelle de milliers d'appareils. Les configurations étaient souvent incohérentes, certains chauffeurs retardaient les mises à jour ou installaient des applications non autorisées (comme les réseaux sociaux), entraînant des failles de sécurité, voire des infections par malware.

En cas de panne, l'appareil devait être retourné au siège, un processus pouvant prendre plusieurs jours. Le chauffeur devait alors fonctionner avec un appareil de secours, voire revenir temporairement à une gestion papier.

Depuis le **déploiement de SOTI MobiControl**, la donne a changé.

L'IT gère désormais l'ensemble du parc d'appareils à distance, depuis une **console centralisée**. Chaque terminal applique automatiquement les règles de sécurité via des profils prédéfinis. Si un utilisateur tente de modifier une configuration critique, SOTI la rétablit **automatiquement** ou alerte l'IT.

Les appareils hors-ligne ou présentant des comportements anormaux sont **immédiatement signalés**.

Selon le responsable informatique, des tâches qui demandaient auparavant plusieurs techniciens sont aujourd'hui gérées par **une seule personne**, grâce à l'**automatisation**. Cela a permis à l'équipe de se concentrer sur l'innovation plutôt que sur les urgences quotidiennes.

L'entreprise a aussi utilisé SOTI Snap pour renforcer la **conformité** et former les utilisateurs.

Une **mini-application mobile** a été créée pour former les chauffeurs à la cybersécurité (reconnaître un phishing, adopter les bons réflexes, etc.). Grâce à **SOTI Snap**, cette formation est intégrée directement dans les terminaux, sous forme de modules courts et interactifs.

L'équipe RH peut suivre qui a terminé la formation, mettre à jour le contenu et le redéployer rapidement, sans contact physique ni infrastructure supplémentaire.

Résultat : une hausse significative de la sensibilisation à la sécurité, sans perturber les opérations.

Autre exemple : Fleetoran, un acteur néerlandais du transport de matériaux de construction.

Fleetoran faisait face à une **flotte d'appareils hétérogènes**, souvent personnels, avec des versions d'apps différentes et des failles de sécurité. Chaque appareil nécessitait une configuration manuelle, prenant environ 30 minutes.

Avec SOTI, cette configuration est tombée à moins de 5 minutes par appareil – soit un **gain de temps** de plus de 80 %.

Grâce à des **profils automatisés**, chaque terminal reçoit les applications, réglages et politiques nécessaires dès l'activation.

Les bénéfices sont concrets :

- plus de 250 000 € d'économies annuelles (IT, support, remplacement)
- une flotte d'appareils cohérente et mieux sécurisée
- moins de pannes, moins de retards, meilleure conformité NIS2

L'entreprise utilise également le **Kiosk Mode** pour restreindre l'accès à des apps spécifiques, et la prise de contrôle à distance pour résoudre les problèmes sur le terrain.



“ Le responsable technique résume :

Grâce à SOTI, nous sécurisons nos équipements, intervenons plus rapidement en cas de problème, et avons une vue complète sur ce qui se passe dans nos opérations. ”

Ces exemples montrent que SOTI ne se contente pas de répondre aux exigences de conformité :

- ▶ Il réduit les coûts,
- ▶ Il améliore la productivité,
- ▶ Et il renforce la résilience opérationnelle face aux menaces.

Conclusion et prochaines étapes pour les décideurs de la logistique

Le message est clair : la cybersécurité est devenue aussi essentielle au transport et à la logistique que le carburant ou les systèmes de suivi.

Avec la directive NIS2, l'Europe exige que les acteurs du secteur renforcent leur résilience numérique, protègent leurs opérations critiques et soient prêts à réagir à tout incident – sans compromettre leur efficacité.

Ce livre blanc montre que, avec les bons outils, **conformité et performance** peuvent aller de pair.

La **plateforme SOTI ONE**, avec sa solution **MobiControl**, aide les entreprises à prendre le contrôle de leur flotte d'appareils, à centraliser la gestion, à améliorer la visibilité, et à réduire drastiquement les temps d'arrêt.

En pratique, cela signifie :

- moins de pertes de productivité,
- des appareils toujours sécurisés et à jour,
- une conformité démontrable aux exigences de NIS2,
- des collaborateurs mieux équipés,
- et des économies à réinvestir dans l'innovation.

Les entreprises qui adoptent SOTI gagnent un avantage concurrentiel : elles rassurent leurs clients, répondent plus vite aux audits et s'imposent comme des acteurs modernes et responsables du secteur.

Prêt à passer à l'action ?

Le calendrier de mise en conformité NIS2 avance. Si vous gérez des flottes d'appareils mobiles ou connectés dans la logistique, **c'est maintenant qu'il faut agir**.

ET VOUS N'ÊTES PAS SEUL.

Étapes suivantes

1. Demandez une démonstration personnalisée

Découvrez SOTI MobiControl en action : gérez, sécurisez et surveillez vos appareils comme jamais auparavant. En quelques clics, vous verrez comment simplifier des tâches complexes.

2. Demandez un audit rapide de conformité NIS2

Nos experts vous aident à évaluer votre situation actuelle, identifier les écarts par rapport à NIS2, et établir un plan d'action.

Un "check-up cybersécurité" rapide – mais stratégique.

Conclusion

La conformité NIS2 n'est pas qu'un impératif réglementaire : c'est une opportunité de transformation.

Avec SOTI, votre flotte devient un levier de compétitivité : plus sécurisée, plus réactive, plus efficace.



Téléchargez le **livre blanc complet** ou réservez une **démonstration** avec eutronix.

**ENSEMBLE, FAISONS EN SORTE QUE VOS OPÉRATIONS
RESTENT EN MOUVEMENT – MÊME FACE AUX CYBERMENACES.**



Votre chaîne logistique est-elle vraiment à la hauteur des exigences NIS2 ?

Ne laissez pas la conformité devenir un simple exercice de rattrapage : anticiper dès maintenant, c'est transformer une contrainte réglementaire en moteur d'efficacité et de confiance pour l'ensemble de vos opérations. En vous appuyant sur l'expertise conjointe d'eutronix et de SOTI, vous sécurisez vos terminaux mobiles, fluidifiez vos flux de données et garantisiez la continuité de service que vos clients attendent.

Contactez nos experts dès aujourd'hui.

Nous serons ravis d'échanger avec vous pour adapter notre solution à vos besoins spécifiques.



eutronix Belgique

1300 - Wavre

+32 10 39 49 00

[Contactez-nous](#)



eutronix France

78870 - Bailly

+33 1 34 61 61 46

[Contactez-nous](#)



eutronix Netherlands

4744 RZ Bosschenhoofd

+31 76 52 45 330

[Contactez-nous](#)

A propos d'eutronix

- Entreprise dynamique spécialisée dans les solutions matérielles et les équipements d'automatisation électronique
- Distributeur à valeur ajoutée
- Fondée en 1999
- Siège social en Belgique
- Succursales et filiales en France, aux Pays-Bas et au Royaume-Uni
- Une équipe de plus de 40 personnes

Nos secteurs d'activités

- Santé
- Hôtellerie
- Retail / Commerce de détail
- Loisirs
- Transport et logistique
- Industrie
- Contrôle d'accès et identification des personnes
- Signalisation
- Service sur le terrain
- Oem & IoT