Guide Cybersécurité Retail Alimentaire

Protéger les installations frigorifiques, les systèmes de supervision et la continuité d'exploitation. Version destinée aux enseignes de distribution alimentaire, exploitants de magasins, installateurs frigoristes, intégrateurs GTB/GTC et prestataires de maintenance.

Document original de CAREL France SAS | Mise à disposition à titre informatif par HEYTEC

Pourquoi ce guide ?

Les systèmes frigorifiques sont aujourd'hui des infrastructures critiques du magasin.

Ils pilotent : les meubles frigorifiques, les chambres froides, les centrales frigorifiques, les pompes à chaleur, les systèmes de récupération d'énergie, les alarmes techniques, le suivi énergétique…

La digitalisation croissante des magasins permet d'améliorer la performance énergétique et la maintenance prédictive, mais elle expose également les installations aux risques cyber.

Une attaque réussie peut entraîner : la perte de supervision du magasin, l'arrêt partiel ou total de certains équipements, une perte de produits réfrigérés ou surgelés, des interventions d'urgence coûteuses, des impacts significatifs sur l'activité commerciale.

La bonne nouvelle est que la plupart des risques peuvent être fortement réduits grâce à quelques règles simples de conception et d'exploitation.

Les risques les plus courants

1/ Exposition directe d'un superviseur sur Internet

Historiquement, de nombreuses installations ont été configurées avec :

- une adresse IP publique
- une redirection de port sur le routeur
- un accès distant ouvert depuis Internet.

Cette pratique reste aujourd'hui le principal facteur de risque.

Un équipement visible publiquement peut être détecté automatiquement par des outils de scan utilisés quotidiennement par des acteurs malveillants.

Un superviseur frigorifique ne devrait jamais être accessible directement depuis Internet.

CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

2/ Utilisation de mots de passe faibles ou partagés

Les comptes génériques de type : Admin, Administrator, Service, Maintenance constituent un risque majeur lorsqu'ils sont utilisés par plusieurs intervenants.

Les mots de passe par défaut ou inchangés représentent encore aujourd'hui une des principales causes de compromission.

3/ Systèmes non mis à jour

Comme tout équipement informatique, les superviseurs et passerelles de communication nécessitent des mises à jour régulières.

Une version logicielle ancienne peut contenir des vulnérabilités déjà connues publiquement.

4/ Accès fournisseurs non maîtrisés

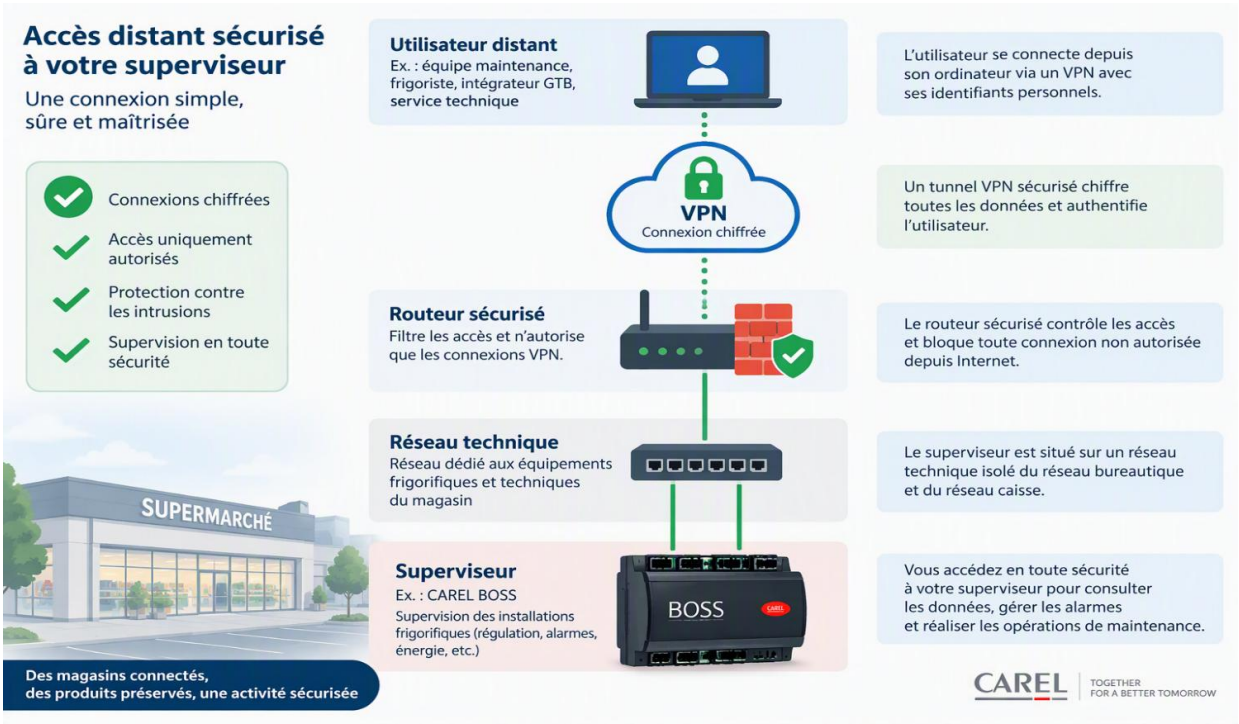
Un magasin peut parfois disposer simultanément d'accès : frigoriste, intégrateur GTB, client utilisateur, télésurveillance…

Sans gouvernance claire, il devient difficile de savoir : qui se connecte, quand, avec quels droits.

Les 5 règles d'or de la cybersécurité frigorifique

1. Ne jamais exposer directement le superviseur

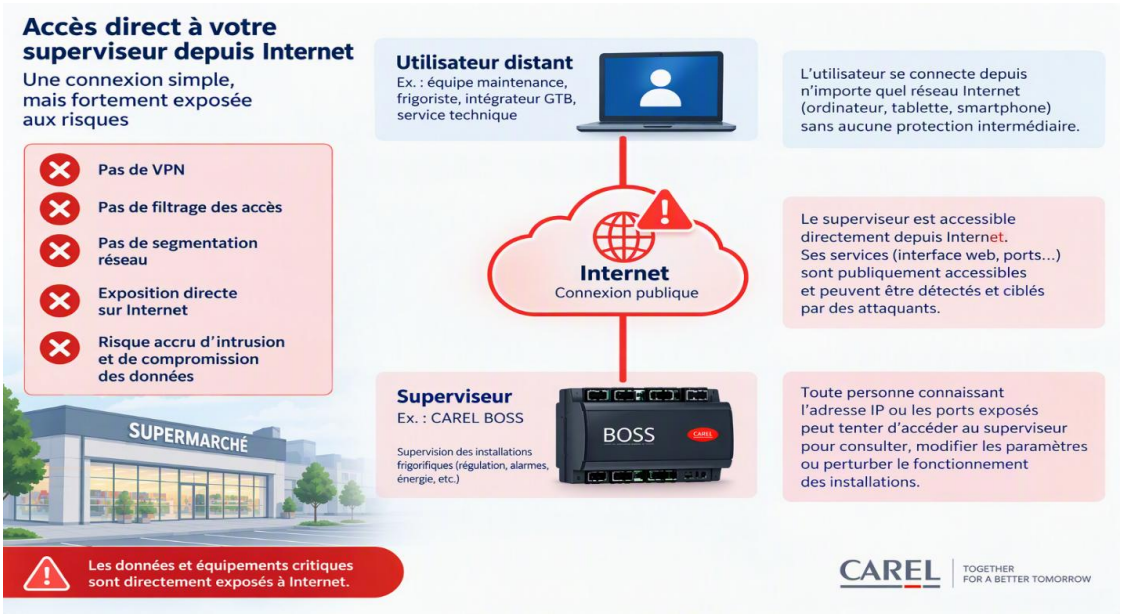
✅ Bonne pratique :



CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

❌ Mauvaise pratique :



2. Utiliser un VPN pour tous les accès distants

Le VPN doit constituer l'unique point d'entrée.

Il permet : l'authentification des utilisateurs, le chiffrement des échanges, la traçabilité des connexions, le contrôle des accès.

Une enseigne disposant de plusieurs centaines de magasins doit privilégier une architecture VPN centralisée pilotée par sa DSI.

3. Segmenter les réseaux

Un réseau frigorifique ne devrait pas partager le même environnement que : les caisses, le Wi-Fi clients, les terminaux bureautiques, les systèmes administratifs.

4. Gérer rigoureusement les comptes utilisateurs

Chaque intervenant doit disposer : de son propre compte, de droits adaptés à sa fonction, d'une traçabilité individuelle.

À éviter : comptes génériques, mots de passe partagés, accès permanents pour les sous-traitants.

5. Maintenir les équipements à jour

Il est recommandé de vérifier au minimum : les superviseurs, les automates, les passerelles IP, les équipements VPN, les équipements réseau.

Une revue annuelle des versions installées devrait être intégrée au contrat de maintenance.

Auto-évaluation rapide

Niveau de risque faible ✅

- Superviseur non exposé sur Internet
- VPN obligatoire
- Comptes nominatifs
- Réseau segmenté
- Mises à jour régulières
- Sauvegardes vérifiées

Niveau de risque moyen ⚠️

- VPN partiellement déployé
- Mots de passe partagés
- Documentation incomplète
- Versions non vérifiées

Niveau de risque élevé 🚨

- Adresse IP publique
- Ports ouverts
- Comptes génériques
- Aucun suivi des versions
- Aucun contrôle des accès distants

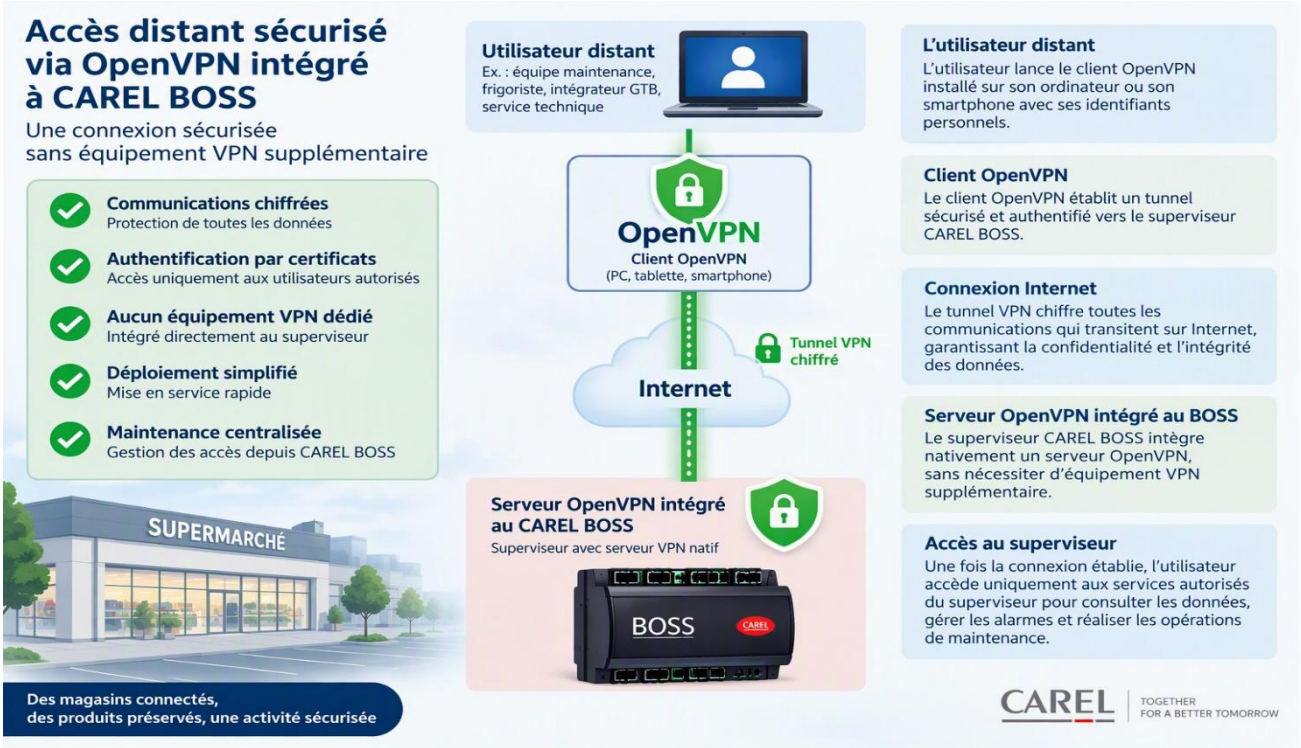
CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

Alternatives au VPN géré par le client (ou son sous-traitant)

1/ OPENVPN Intégré CAREL Boss

Le client **OpenVPN** est intégré nativement dans votre superviseur Boss et peut être utilisé sans aucun logiciel supplémentaire. Toutes les opérations nécessaires à la configuration, à la gestion et à la maintenance de la solution via le serveur **OpenVPN** doivent être effectuées par le client. Cette option peut être choisie par les clients disposant des compétences requises pour gérer un canal de communication sécurisé à l'aide d'outils standard.



Rapprochez vous de votre responsable IT et de votre intégrateur CAREL pour configurer cet accès VPN sans cout matériel ou logiciel supplémentaire.

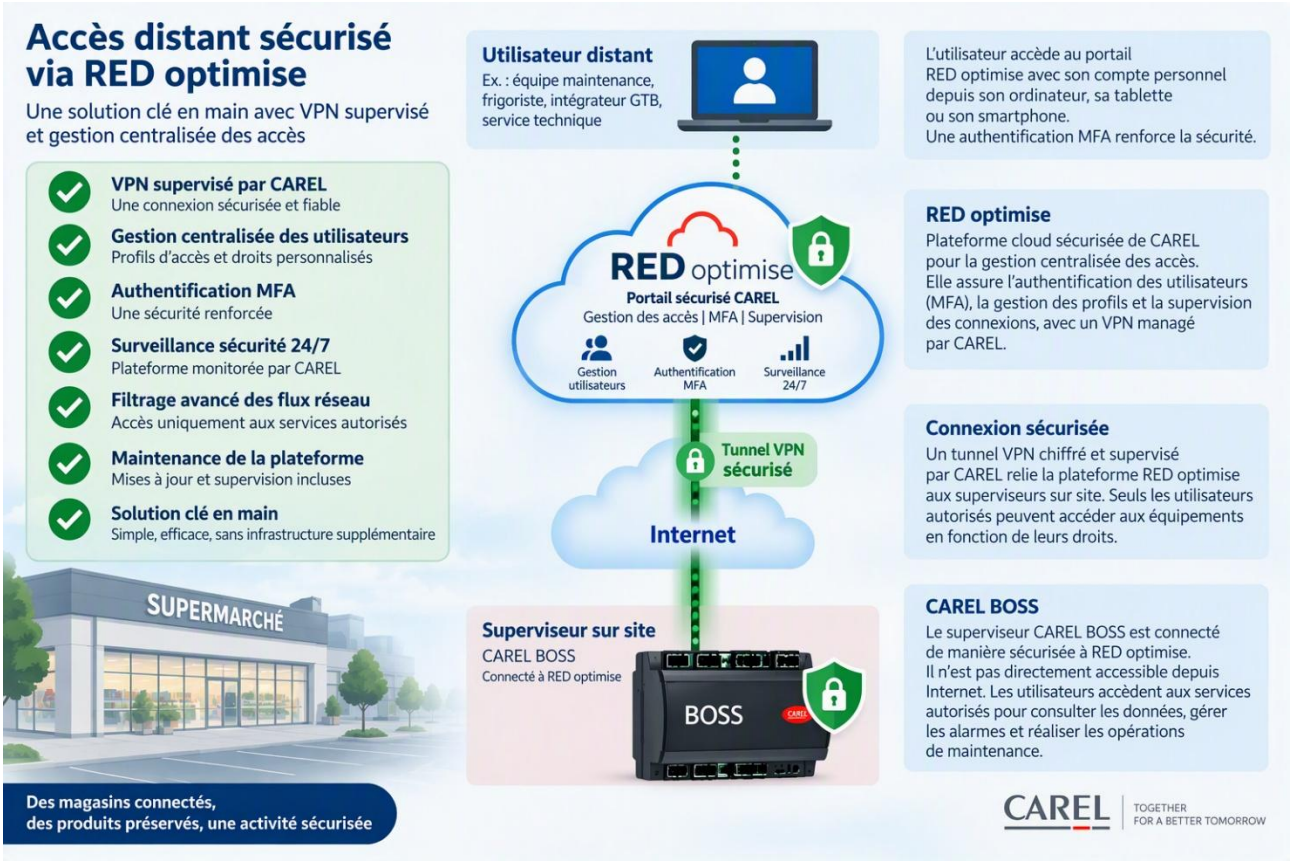
CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498

2/ Gestion d'un canal sécurisé par la connexion des superviseurs à RED Optimise.

RED Optimise propose une solution « clé en main » pour renforcer la sécurité des clients.

Pour les clients à la recherche d'une solution « clé en main » destinée à sécuriser leurs superviseurs Boss, l'offre « Contractor - Basic » constitue la solution d'entrée de gamme.



Cette offre « Contractor- Basic » prend en charge et optimise la gestion opérationnelle des activités de maintenance via une interface simple et intuitive, grâce à :

- un accès sécurisé aux sites, assuré par un canal VPN surveillé en permanence, ainsi qu'une gestion centralisée des utilisateurs et des profils
- un tableau de bord de suivi de l'état et des versions de tous les superviseurs installés, facilitant la planification des mises à jour logicielles dès la disponibilité de nouvelles versions.

Plus précisément, RED Optimise intègre les fonctionnalités de sécurité de plateforme suivantes :

« **Security by design** » (sécurité dès la conception) : mesures de sécurité physiques et logiques

- communications chiffrées via HTTPS/TLS et VPN
- filtrage avancé du trafic réseau
- évaluations périodiques des vulnérabilités et tests d'intrusion
- conformité aux normes et directives de cybersécurité reconnues, notamment les référentiels du NIST et les informations sur les vulnérabilités basées sur les CVE
- authentification multifacteur (MFA)

Gestion de la plateforme et surveillance continue par CAREL, incluant :

- une surveillance de l'infrastructure 24h/24 et 7j/7
- une surveillance des applications 24h/24 et 7j/7
- une surveillance de la sécurité 24h/24 et 7j/7
- quatre environnements distincts pour le développement, les tests, l'assurance qualité et la production (Dev, Test, QA et Prod)
- un provisionnement automatisé de l'infrastructure et une gestion des configurations.

Les frais d'accès à la solution RED Optimise réside dans la souscription à un abonnement annuel par magasin ainsi que des frais de mise en service (unique) par magasin.

Si vous êtes intéressé par la solution RED Optimise, contacter votre interlocuteur CAREL qui vous transmettra les conditions d'utilisation et de souscription au service

Division Project & Dealer

CAREL France SAS

Document original CAREL - Avis de non-responsabilité

Le présent document, intitulé « Guide Cybersécurité Retail Alimentaire », est un document original de CAREL France SAS. Il est mis à disposition par HEYTEC exclusivement à titre informatif. HEYTEC n'en est pas l'auteur et n'assume aucune responsabilité quant à son contenu.

HEYTEC ne garantit ni l'exactitude, ni l'exhaustivité, ni l'actualité des informations, des indications techniques ou des recommandations qu'il contient. Dans les limites autorisées par la loi, HEYTEC décline toute responsabilité pour les dommages directs ou indirects résultant de l'utilisation, de l'interprétation ou de la mise en œuvre des informations ou recommandations figurant dans ce document.

Pour toute question technique ou contractuelle, veuillez vous référer à CAREL et à sa documentation officielle.

Disponibilité en Belgique et prestations de HEYTEC

Certains produits, solutions ou services mentionnés dans ce document peuvent ne pas être disponibles en Belgique ou ne pas être proposés ou pris en charge par HEYTEC. Leur mention ne constitue ni une offre ni un engagement de HEYTEC. La disponibilité et les conditions applicables doivent être confirmées au préalable auprès de HEYTEC.

CAREL France Sas
1, rue Paul Rieupeyroux - 69800 Saint Priest (France)
Phone (+33) 04 72 47 88 88 - Fax (+33) 04 78 90 08 08
carelfrance.fr - carelfrance@carel.com

SAS au capital de 100.000 Euros
RCS Lyon B 414 896 498
APE 4652 Z
N. Intracom. FR 56 414896498