Cyberattaques : vos questions, nos réponses.

Pour les clouds testo Saveris Food Solution et Smart Connect.

1 Les récentes attaques contre les systèmes réfrigération.

À l'automne 2026, des hackers ont à distance chauffé des régulateurs de réfrigération connectés dans des supermarchés à travers l'Europe, jusqu'à +50°C. La surveillance Testo ne peut pas être détournée de cette manière : elle observe votre équipement, mais ne peut pas le commander.

Votre question	Notre réponse
Un pirate pourrait-il modifier les températures de nos réfrigérateurs ou congélateurs via Testo ?	Non. Les capteurs et passerelles Testo sont totalement indépendants de votre installation frigorifique et des autres systèmes du magasin. Ils mesurent et transmettent des températures ; ils n'ont aucune connexion avec les groupes frigorifiques et ne peuvent pas leur envoyer de commandes.
La surveillance Testo augmente-t-elle notre risque de cyberattaques ?	Elle n'ouvre aucune nouvelle voie vers vos systèmes. Les appareils Testo sont séparés de vos installations frigorifiques et des systèmes du magasin, et ne peuvent pas les atteindre. Comme tout appareil connecté, ils ont besoin d'un accès réseau, mais c'est eux qui ouvrent la connexion, par un seul chemin sortant chiffré vers des adresses Testo fixes : aucun port entrant sur le pare-feu, aucun logiciel sur vos ordinateurs.
Les températures enregistrées par Testo pourraient-elles être manipulées à distance ?	Risque négligeable. Chaque capteur signe ses mesures avec un certificat propre à l'appareil, émis par l'autorité de certification de Testo. Toute donnée altérée en cours de route échoue au contrôle de signature dans le cloud et est rejetée.
Les alarmes ou les seuils d'alarme pourraient-ils être manipulés ?	Uniquement par un utilisateur connecté disposant du rôle approprié. Les seuils d'alarme et les paramètres ne peuvent être modifiés que par les utilisateurs autorisés pour ce site ; chaque requête est contrôlée. Le principal risque est le vol d'un compte.
Comment Testo nous aide-t-il si notre installation frigorifique est attaquée ?	Un régulateur compromis ne peut pas masquer une hausse de température aux capteurs Testo indépendants. Votre équipe est alertée dès qu'un seuil est dépassé, et les enregistreurs continuent de mesurer pendant les coupures réseau, de sorte que votre historique HACCP reste complet.
Qu'a fait Testo depuis les attaques ?	Nos équipes de sécurité et nos systèmes de détection des menaces sont en alerte maximale. Les mesures existantes, présentées ci-dessous, couvrent déjà ce type d'attaque : aucune modification d'urgence des produits n'a donc été nécessaire.

2 Comment protégeons-nous vos données ?

Domaine	Nos actions
Chiffrement	TLS 1.2 ou supérieur sur chaque connexion. Les bases de données, les données de mesure et les fichiers sont chiffrés avec AES-256.
Redondance et sauvegarde	Plusieurs centres de données distincts, de sorte que la perte de l'un n'interrompt pas le service. Sauvegardes quotidiennes avec restaurations testées régulièrement ; l'infrastructure peut être reconstruite automatiquement.
Accès	Connexion avec votre compte Testo via Auth0, avec des rôles par site. Le support Testo n'accède à votre compte qu'après votre approbation.
Tests	Contrôles de sécurité et revue par deux personnes (principe des quatre yeux) à chaque modification, analyses automatisées hebdomadaires et test d'intrusion annuel réalisé par des experts indépendants, dernier en date en 2026.
Réponse	Surveillance 24h/24 et 7j/7, avec une équipe d'astreinte. Les vulnérabilités critiques sont corrigées immédiatement, au plus tard sous deux semaines ; les vulnérabilités élevées dans le trimestre.
Normes	Gestion de la sécurité de l'information conforme à la norme ISO/IEC 27001:2022 (certification formelle en cours), NIS2 et OWASP.

3 Quels risques subsistent, et que pouvons-nous faire ?

Aucun système connecté n'est exempt de risques. La sécurité est plus efficace lorsque Testo et vous assumez chacun votre part.

Risque	Ce que fait Testo	Ce que vous pouvez faire
Connexions réseau non sécurisées	TLS 1.2 ou supérieur ; certificats individuels par appareil ; connexions sortantes vers des adresses Testo fixes uniquement.	Placer les appareils Testo dans un VLAN / SSID dédié, avec un accès Internet limité aux adresses Testo ; utiliser des mots de passe réseau robustes.
Comptes utilisateurs volés (hameçonnage, mots de passe réutilisés)	Connexion via Auth0 ; mots de passe stockés uniquement sous forme de hachages salés ; rôles par site.	Utiliser des mots de passe uniques, limiter les droits d'administration à quelques personnes, supprimer rapidement les accès des collaborateurs partis ; activer éventuellement l'authentification multifacteur (MFA) via l'authentification unique (SSO).
Attaques contre la plateforme cloud	Plusieurs centres de données ; réseaux privés ; chiffrement AES-256 ; surveillance 24h/24 et 7j/7 ; sauvegardes quotidiennes.	Exporter régulièrement vos données, ou via l'API optionnelle, si vous souhaitez disposer de votre propre copie.
Interfaces avec d'autres systèmes (API, ERP, BI)	API optionnelle, chiffrée en transit.	Traiter les identifiants d'API comme des mots de passe administrateur ; ne connecter que les systèmes qui ont besoin des données.
Logiciels ou micrologiciels obsolètes	Cloud mis à jour de manière centralisée, rien à installer ; mises à jour du micrologiciel protégées cryptographiquement.	Installer les correctifs ainsi que les mises à jour du système d'exploitation et des applications dès leur disponibilité, sur chaque téléphone, tablette et PC utilisé ; être connecté ne suffit pas. Garder les appareils Testo connectés pour les mises à jour du micrologiciel et remplacer le matériel en fin de vie.
Une alarme passe inaperçue	Alarme dès qu'un seuil est dépassé ; données conservées pendant les coupures réseau.	Tenir à jour la liste des destinataires d'alarmes, afin qu'une hausse de température parvienne à quelqu'un à toute heure.

4 Pour aller plus loin.

Document	Contenu
Numérique – Sécurité et données | ISO 27001, NIS-2 et Data Act	Centre de confiance Testo : l'ensemble des documents relatifs à la sécurité et à la protection des données au même endroit. testo.com/en/company/trust/digital.
Auto-déclaration sur la sécurité de l'information	Toutes les mesures techniques et organisationnelles de sécurité, au niveau de l'entreprise et du produit.
Politique de sécurité de l'information	Périmètre, objectifs et responsabilités du management de la sécurité de l'information de Testo.
Politique de confidentialité testo Saveris	Données personnelles traitées, sous-traitants, lieux d'hébergement et vos droits au titre du RGPD.

Résultats des tests d'intrusion, exigences des pare-feu et accord de traitement des données : demandez-les à votre responsable de compte Testo.