lookwise®
DEVICE MANAGER

Lookwise Device Manager est une plateforme de cybersécurité OT centralisée et modulaire dotée de toutes les fonctionnalités nécessaires pour protéger et contrôler les équipements essentiels à votre activité.

Les cybermenaces sont une préoccupation majeure pour toutes les entreprises, les cyberdélinquants s'avérant toujours plus agiles et innovants dans le développement de nouveaux logiciels malveillants.
Les systèmes essentiels à l'activité des sociétés étant des cibles très attractives, des mesures de sécurité renforcées sont indispensables.

PROTECTION DES ÉQUIPEMENTS ESSENTIELS

Lookwise Device Manager (LDM) est une solution parfaitement adaptée pour garantir des normes de sécurité élevées à votre outil de travail (guichets automatiques bancaires, terminaux de paiement électronique, systèmes de contrôle des infrastructures critiques).

- Bénéficiez d'une solution multi-constructeur, reconnue et primée, conçue spécialement pour sécuriser vos équipements essentiels contre les activités malveillantes et frauduleuses.
- Protection multi-niveaux complète, facile à mettre en oeuvre dans le cadre de vos politiques de sécurité tout en ayant un impact minimal sur la performance de vos appareils.
- Gagnez du temps et de l'argent en gérant vos opérations de sécurité de manière centralisée, à distance, sur une seule interface graphique.
- Bloquez, détectez e résolvez les incidents de sécurité affectant vos équipements.
- Ayez la visibilité en temps réel de tous vos appareils, logiciels et utilisateurs, et soyez alerté de toute modification.
- Exécutez à distance des actions personnalisées dans un environnement sécurisé et contrôlé.
- Adaptez la visualisation et les autorisations aux besoins spécifiques des différentes équipes opérationnelles.

COMPRENDRE SON ENVIRONNEMENT

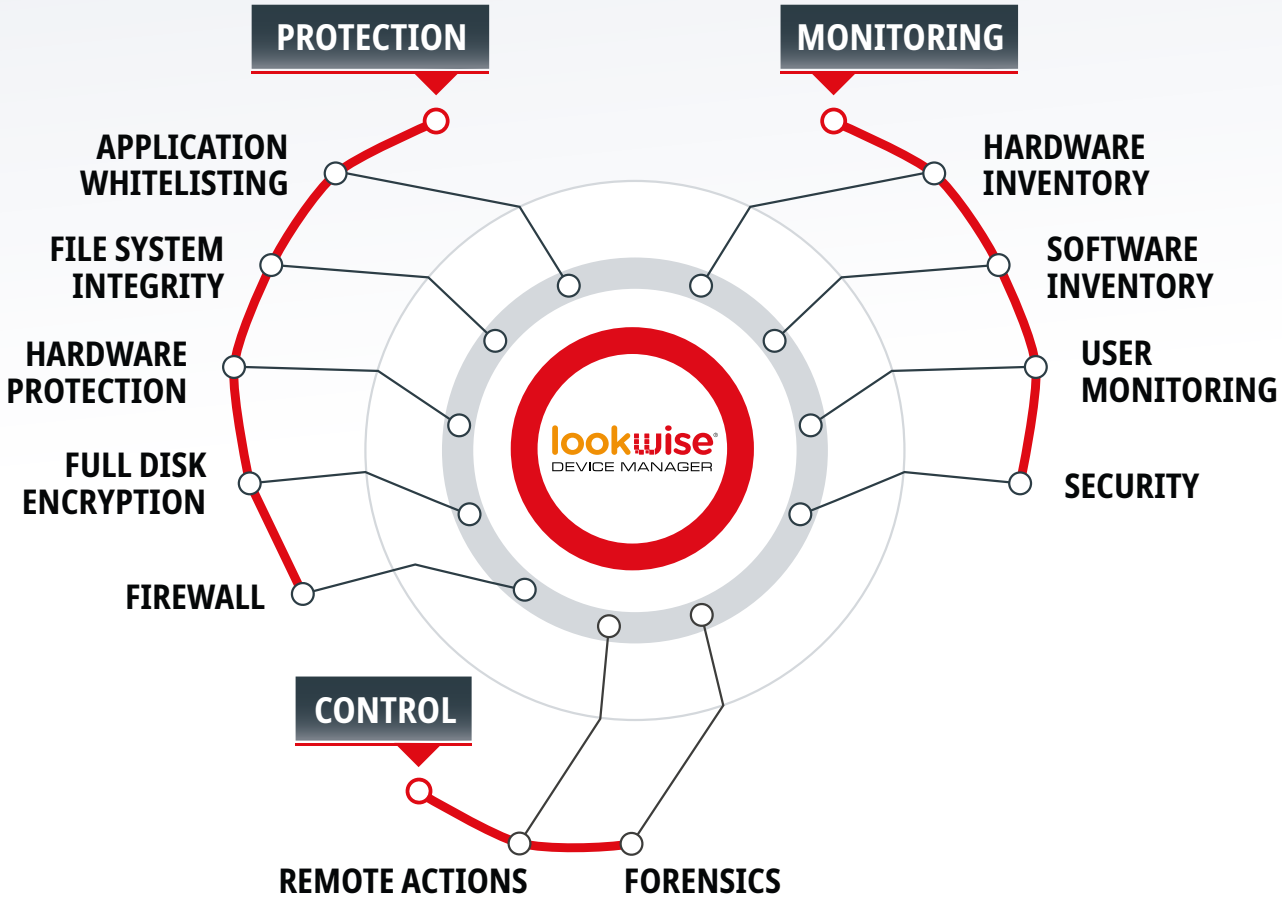
Les équipements essentiels fournissent des services qui doivent être disponibles en permanence. Il est crucial de les sécuriser : les cyber-attaques à leur encontre sont très ciblées et conçues pour repérer toute vulnérabilité logicielle. Les conséquences d'un défaut de maintenance vont de la fraude financière à l'interruption de la continuité des activités, voire au sabotage.

En mettant en place une stratégie efficace de cybersécurité OT, basée sur les technologies de protection adaptées, il est possible de sécuriser les équipements essentiels sans perturber les opérations tout en respectant les réglementations du secteur d'activité.

Lookwise Device Manager est une solution de cybersécurité OT intégrée qui fournit les contre-mesures les plus avancées pour protéger et répondre à la nouvelle génération de cyber-attaques par logiciels malveillants. Il centralise la définition des stratégies et les opérations en un seul point, ce qui vous permet de protéger des milliers d'appareils essentiels et d'assurer la continuité de l'activité et la conformité aux politiques d'entreprise et réglementations de cybersécurité (PCI DSS, NERC...).

MODÈLE DE SÉCURITÉ COMPLET

Lookwise Device Manager est une plateforme modulaire qui offre un ensemble complet de fonctionnalités pour protéger et surveiller vos appareils essentiels, en ajoutant une couche de contrôle supplémentaire qui permet aux utilisateurs d'exécuter des actions à distance personnalisées pour analyser ou réagir à des incidents potentiels.



PROTECTION

Protégez vos appareils contre les attaques ou modifications malveillantes, grâce à la sécurité multi-couches la plus complète, pour contrôler l'accès aux ressources logicielles et matérielles sur la base de listes blanches.

LISTE BLANCHE DES APPLICATIONS

Empêche l'exécution de logiciels malveillants ou suspects en établissant une liste blanche de processus autorisés, en contrôlant les paramètres de la ligne de commande pour les processus sensibles (interprètes ou outils système) et en limitant l'accès aux bibliothèques essentielles.
Réduit la surface d'attaque aux processus nécessaires au bon fonctionnement de l'appareil.

PROTECTION DE L'INTÉGRITÉ DU SYSTÈME DE FICHIERS

Empêche la manipulation incontrôlée de fichiers ou de dossiers essentiels dans le système de fichiers, en appliquant des règles de protection des extensions, répertoires ou fichiers.
Préserve l'intégrité de l'image logicielle certifiée en ne laissant que les processus de confiance modifier les fichiers ou dossiers protégés.

LISTE BLANCHE DE MATÉRIEL

Empêche la connexion de dispositifs informatiques frauduleux ou non autorisés ne figurant pas dans une liste blanche de matériels autorisés. Il limite en outre le niveau d'accès (lecture-écriture) pour les périphériques de stockage autorisés (USB, CDROM, disquette, MTP). Simplifie la configuration en utilisant des listes blanches de périphériques locaux associées à des règles globales de permission ou d'interdiction. Les connexions/déconnexions des périphériques autorisés peuvent également être signalées.

CRYPTAGE COMPLET DU DISQUE

Bloque l'accès au disque dur de l'extérieur du système d'exploitation en utilisant un cryptage par secteur et des clés uniques gérées de manière sécurisée, permettant un démarrage sans surveillance et un décryptage hors ligne.
Préserve la confidentialité des données de stockage, sans interférer avec le bon fonctionnement du dispositif.

SURVEILLANCE

Visualisez en temps réel les logiciels, les équipements et les utilisateurs de vos appareils et contrôlez toute modification qui pourrait s'avérer frauduleuse.

INVENTAIRE DU MATÉRIEL

Fournit aux utilisateurs un inventaire du matériel, avec la possibilité de générer des alertes en cas de connexion ou de déconnexion.

INVENTAIRE DES LOGICIELS

Permet aux utilisateurs d'obtenir un inventaire des logiciels et des correctifs du système d'exploitation installés dans le dispositif, avec la possibilité d'alerter en cas de présence de logiciels non autorisés ou d'absence de correctifs essentiels du système d'exploitation.

MONITEUR UTILISATEURS

Permet d'obtenir la liste des utilisateurs du système d'exploitation local, et d'être alerté en cas de création, modification ou suppression de comptes d'utilisateurs.

MONITEUR FICHIERS ET RÉPERTOIRES

Contrôle et vous alerte lorsque des fichiers ou des répertoires essentiels sont modifiés.

CONTRÔLE

Exécutez à distance des actions sur vos appareils, ce qui facilite les opérations et les activités de maintenance.

Redémarrage et changement de mot de passe à distance

Exécutez des actions à distance adaptées sur les équipements surveillés, en obtenant et en centralisant les résultats.

Extraction d'informations

Récupérez à distance des fichiers ou des répertoires sur les appareils contrôlés.

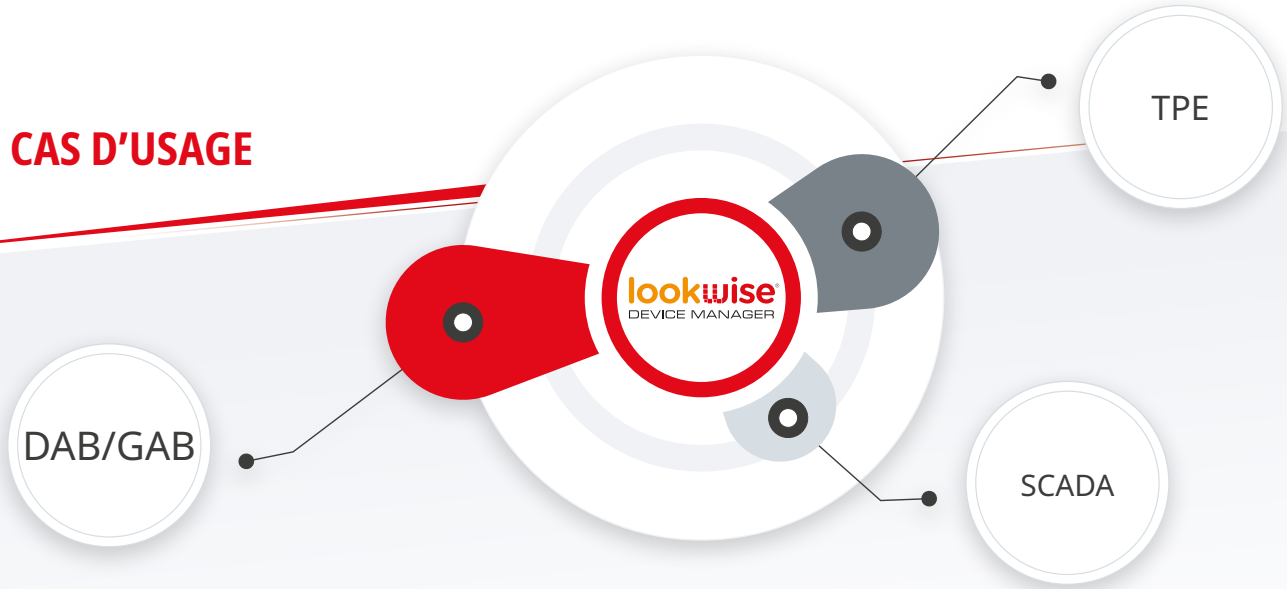
Exécution d'actions à distance

Créez vos propres actions à distance à diverses fins : investigation, reconfiguration, déploiement de correctifs, désinfection de logiciels malveillants.

Exécutez des actions à distance personnalisées sur les appareils, en téléchargeant ou en exécutant des binaires ou des scripts locaux, en obtenant et en centralisant les résultats.

Les actions à distance sont pré-intégrées à la liste blanche des applications et ne peuvent être exécutées qu'à partir de la console LDM (et non localement sur l'appareil).

CAS D'USAGE



AUTOMATES

Les automates bancaires sont des cibles très attractives car ils contiennent de l'argent liquide et gèrent des informations sensibles (numéros de carte bancaires, codes PIN) dans un environnement insuffisamment surveillé.

La grande diversité de matériel et de logiciels, associée à l'absence de politiques proactives de mise à niveau due à des contraintes techniques et économiques, rendent les réseaux de GAB intrinsèquement vulnérables.

Dans ce contexte, les cyber-délinquants font preuve d'agilité et d'inventivité pour produire de nouveaux types d'attaques logicielles ciblées, plus rentables que les attaques physiques traditionnelles.

TERMINAUX DE PAIEMENT ELECTRONIQUE (TPE)

La nature des TPE, qui traitent des données sensibles (numéros de carte, codes PIN), les rend vulnérables aux attaques ciblées et autres actions frauduleuses.

Le contrôle par liste blanche des applications et appareils autorisés permet d'accroître le niveau de confiance dans la sécurité de ces équipements.

SYSTÈMES DE CONTRÔLE DES INFRASTRUCTURES ESSENTIELLES

Les systèmes d'automatisation et de contrôle des infrastructures essentielles dépendent de plus en plus des communications à distance et de l'interconnexion avec l'infrastructures informatique, héritant ainsi de certains de ses risques et vulnérabilités.

Une cyber-attaque contre les systèmes de contrôle peut causer des dommages considérables, allant du refus massif de services courants à la mise en danger potentielle d'infrastructures et de personnes. Il convient donc d'appliquer les normes de sécurité les plus élevées à ces systèmes sensibles.

CARACTÉRISTIQUES

Lookwise Device Manager repose sur la technologie propriétaire d'Auriga, Lookwise TECH. Spécialement conçue pour les environnements distribués et Windows XP/7/10, c'est une solution modulaire, évolutive et souple.

GESTION

- Interface utilisateur graphique
- Création et diffusion de politiques à distance
- Intégration des alertes et rapports sur les résultats
- Tableau de bord sécurité
- Visibilité basée sur les rôles et autorisations
- Intégration de la GIES

COMMUNICATIONS

- Authentification et cryptage
- En continu
- Compression
- Conçu pour supporter les réseaux à connexion instable et à faible bande passante

ARCHITECTURE

- Distribuée
- Modulaire
- Souple, évolutive
- Equilibrage des charges
- Télédistribution des fonctions et mises à jour
- Consommation réduite des ressources