kaspersky BRING ON THE FUTURE

Kaspersky Embedded Systems Security

Une solution de sécurité tout-en-un conçue pour les systèmes embarqués

Le marché des systèmes embarqués est en croissance constante et les cybercriminels y sont attentifs. Entre 2018 et 2019, le nombre de tentatives d'infection sur les distributeurs automatiques et les systèmes de point de vente a augmenté de 28 %.

Les systèmes embarqués sont omniprésents et impactent chaque aspect de notre vie quotidienne. Nous comptons sur eux pour tout, des systèmes de point de vente en passant par les distributeurs automatiques jusqu'aux appareils médicaux et télécommunications. Ce qui représente plus de vecteurs d'attaque que jamais.

Depuis peu, Windows 7 ne propose plus de support et toutes les entreprises doivent mettre à jour rapidement le système d'exploitation de leurs systèmes embarqués et prendre des mesures supplémentaires en termes de protection. Il convient de noter que Windows XP, obsolète depuis plusieurs années, reste le système d'exploitation le plus utilisé sur les systèmes embarqués à l'heure actuelle. C'est une porte ouverte aux pirates.

Les cybercriminels tournent de plus en plus leur attention vers ces appareils embarqués, devenus la principale cible de leurs attaques, pouvant entraîner des dommages financiers considérables. Les entreprises doivent donc être plus vigilantes que jamais pour protéger leurs systèmes et données. Doté d'une puissante Threat Intelligence, d'une détection des programmes malveillants en temps réel, de contrôles complets des appareils et des applications et d'une gestion flexible, Kaspersky Embedded Systems Security est une solution de sécurité tout-en-un conçue spécialement pour les systèmes embarqués.

Avantages

Conception efficace même pour du matériel bas de gamme

Kaspersky Embedded Systems Security a été spécifiquement conçu pour offrir d'excellentes performances, même sur du matériel informatique bas de gamme (à partir de 256 Mo de RAM avec processeur Pentium III) et des logiciels obsolètes (à partir de Windows XP), sans risque de surcharge des systèmes. Les canaux de communication faibles (à partir de 56 kbit/s) ne sont pas non plus un problème, même si la seule option de communication est un modem mobile fonctionnant uniquement en 2G en raison de la faiblesse du signal.

Puissante protection de la mémoire

Notre technologie de prévention des vulnérabilités performante surveille les processus essentiels pour empêcher toute tentative d'exploitation de vulnérabilités non corrigées ou même « zero-day » dans les composants du système. C'est essentiel notamment pour la protection contre les ransomwares tels que WannaCry et ExPetr.

Optimisation de Windows XP

La plupart des systèmes embarqués s'exécutent toujours sur le système d'exploitation Windows® XP qui n'est plus pris en charge. Kaspersky Embedded Systems Security a été optimisé pour être pleinement fonctionnel sur la plateforme Windows XP et sur Windows 7, Windows 8 et Windows 10.

Kaspersky Embedded Systems Security s'engage à prendre intégralement en charge Windows XP pendant encore un certain temps, afin de laisser suffisamment de temps aux entreprises d'effectuer des mises à niveau progressives.

Conformité

L'ensemble unique et complet de composants de protection de Kaspersky Embedded Systems Security (protection contre les programmes malveillants, contrôle des appareils et des applications, gestion des pare-feu, surveillance de l'intégrité des fichiers et audit des journaux) identifie et bloque les actions malveillantes contre vos systèmes, et détecte les différents indicateurs d'une atteinte à la sécurité. Les entreprises peuvent ainsi répondre aux exigences de conformité des réglementations telles que PCI/DSS, SWIFT, etc.

DAB

PDV

Billetteries

Caisse

Vieux ordinateurs

Équipement médical

Protection contre les programmes malveillants
- Facultatif
- Temps réel/à la demande
- Fonctionnalité de prévention des exploits, pour lutter contre les ransomwares et les autres menaces

Protection réseau
- Gestion du pare-feu
- Protection contre les menaces réseau

Configuration requise optimale
- 256 Mo de RAM minimum
- Système d'exploitation : Windows XP et versions ultérieures
- Bande passante réseau : à partir de 56 kb/s

Kaspersky Embedded System Security

Surveillance de l'intégrité du réseau
- Surveillance de l'intégrité des fichiers
- Inspection des journaux

Renforcement des systèmes
- Contrôle du lancement des applications
- Contrôle de distribution des logiciels
- Contrôle des appareils

Fonctionnalités

Puissant anti-malware

Des fonctions proactives de détection et d'analyse assistées par le Cloud sont associées à des technologies traditionnelles pour fournir une protection contre les menaces connues, inconnues et avancées. Un logiciel contre les programmes malveillants facultatif (mais vivement recommandé) peut être désactivé dans les scénarios avec du matériel bas de gamme ou des canaux de communication lents.

Détection des programmes malveillants en temps réel avec Kaspersky Security Network

Kaspersky Security Network (KSN) est le réseau mondial de Threat Intelligence hébergé dans le cloud de Kaspersky. Des millions de terminaux répartis dans le monde contribuent constamment à la surveillance des menaces du monde réel pour nos systèmes, assurant une réponse rapide aux menaces émergentes et évoluées les plus récentes, y compris aux attaques de masse.

Ce flux constant de nouvelles données sur les tentatives d'attaques de programmes malveillants et les comportements suspects crée des diagnostics instantanés de fichiers, pour une protection en temps réel contre les menaces les plus récentes.

Contrôle des applications

L'adoption d'un scénario de blocage par défaut reposant sur le contrôle du lancement des applications optimise la résilience du système face aux violations de données.
En interdisant l'exécution de toute application autre que les programmes et services spécifiés, ainsi que les composants système de confiance, vous pouvez bloquer automatiquement la plupart des formes de logiciels malveillants.
Le contrôle de la distribution logicielle utilise une approche de type « programme d'installation autorisé », ce qui élimine la nécessité de gérer manuellement de longues listes blanches de fichiers créés ou modifiés au cours d'une installation ou mise à jour logicielle. Il suffit de spécifier que le programme d'installation est autorisé et d'effectuer normalement la mise à jour.

Surveillance et contrôle des appareils

La fonctionnalité de contrôle des appareils de Kaspersky vous permet de contrôler les appareils de stockage USB connectés ou tentant de se connecter physiquement aux systèmes de l'entreprise. La prévention de l'accès par des appareils non autorisés élimine un point d'entrée régulièrement utilisé par les cybercriminels comme première étape d'une attaque de programme malveillant.

Toutes les connexions d'appareils USB sont surveillées et consignées. Toute utilisation USB inappropriée est traitée comme une attaque potentielle lors des processus d'investigation et de gestion des incidents.

Gestion du pare-feu Windows

Vous pouvez configurer directement le pare-feu Windows à partir de Kaspersky Security Center, notre console unifiée assurant notamment la gestion des pare-feu locaux. Cela est essentiel quand les systèmes embarqués n'appartiennent pas au même domaine et que les paramètres du pare-feu Windows ne peuvent pas être configurés de façon centralisée.

Network Threat Protection

Network Threat Protection vous protège contre les menaces réseau - cela inclut l'analyse des ports, les attaques par déni de service et les attaques par dépassement de la mémoire tampon. Il surveille constamment les activités réseau et, s'il détecte un comportement suspect, exécute une réponse prédéfinie.

Contrôle de l'intégrité des fichiers*

Les actions exécutées sur des dossiers et fichiers spécifiques dans les limites données. Vous pouvez également configurer le suivi des modifications pour qu'il ait lieu lorsque la surveillance est interrompue.

Inspection des journaux*

Kaspersky Embedded Systems Security surveille les potentielles violations de la protection en analysant les historiques des activités de Windows. L'application prévient l'administrateur de tout comportement anormal détecté, signe d'une cyberattaque potentielle.

Intégration SIEM

Kaspersky Embedded Systems Security peut convertir les événements des journaux d'applications aux formats pris en charge par les serveurs Syslog. Tous les systèmes SIEM peuvent ainsi les reconnaître lors d'un transfert. Les événements peuvent être exportés directement depuis Kaspersky Embedded Systems Security vers un SIEM ou de manière centralisée via Kaspersky Security Center.

Gestion flexible

Les politiques de sécurité, les mises à jour de signatures, les analyses de détection des programmes malveillants et la collecte des résultats sont gérées facilement par le biais d'une console d'administration centralisée unique : Kaspersky Security Center. En outre, tous les clients d'un réseau local peuvent être gérés par l'intermédiaire d'une interface utilisateur graphique locale ou d'une ligne de commande, un atout de poids lorsque vous utilisez les réseaux segmentés et isolés caractéristiques des systèmes embarqués.

* Requiert la licence Kaspersky Embedded Systems Security Compliance Edition

Actualités dédiées aux cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : kaspersky.fr/business
Sécurité informatique pour les entreprises : kaspersky.fr/enterprise

www.kaspersky.fr

Nous sommes reconnus. Nous sommes indépendants. Nous sommes transparents. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur kaspersky.fr/about/transparency

Reconnus.
Transparents.
Indépendants.