Kaspersky Embedded Systems Security

kaspersky

Défis de sécurité intégrés

1. **Logiciel obsolète et vulnérable.** Les longs cycles de vie peuvent impliquer l'exécution de systèmes d'exploitation et d'applications qui ne sont plus pris en charge et qui contiennent des vulnérabilités non corrigées risquant d'être exploitées.
2. **Mises à jour de sécurité erratiques.** Même lorsque le logiciel est encore pris en charge, des failles peuvent survenir au niveau des correctifs. Les problèmes liés à la mise à jour de plusieurs appareils géographiquement dispersés, la nécessité de les déconnecter pour les mettre à jour (créant ainsi un déni de service temporaire) et la nécessité de tester les mises à jour avant de les déployer sont autant de facteurs qui peuvent contribuer à retarder l'application de correctifs.
3. **Continuité des processus.** La mise hors service, même temporaire, de certains types d'appareils, comme les équipements médicaux, peut s'avérer très problématique, ce qui augmente davantage le délai de déploiement des correctifs.
4. **Lieux publics.** De nombreux appareils embarqués sont utilisés dans des espaces publics ouverts, une situation qui accroît considérablement le risque de manipulation. Les dispositifs de sécurité au niveau du réseau n'assurent aucune protection contre l'infection physique directe de l'appareil.
5. **Nature intrinsèquement risquée.** Comme ils sont souvent directement associés à des opérations financières et qu'ils traitent des informations personnelles confidentielles, les appareils embarqués sont des cibles particulièrement attrayantes pour les cybercriminels.

Une solution de sécurité tout-en-un conçue pour les systèmes embarqués (et plus encore)

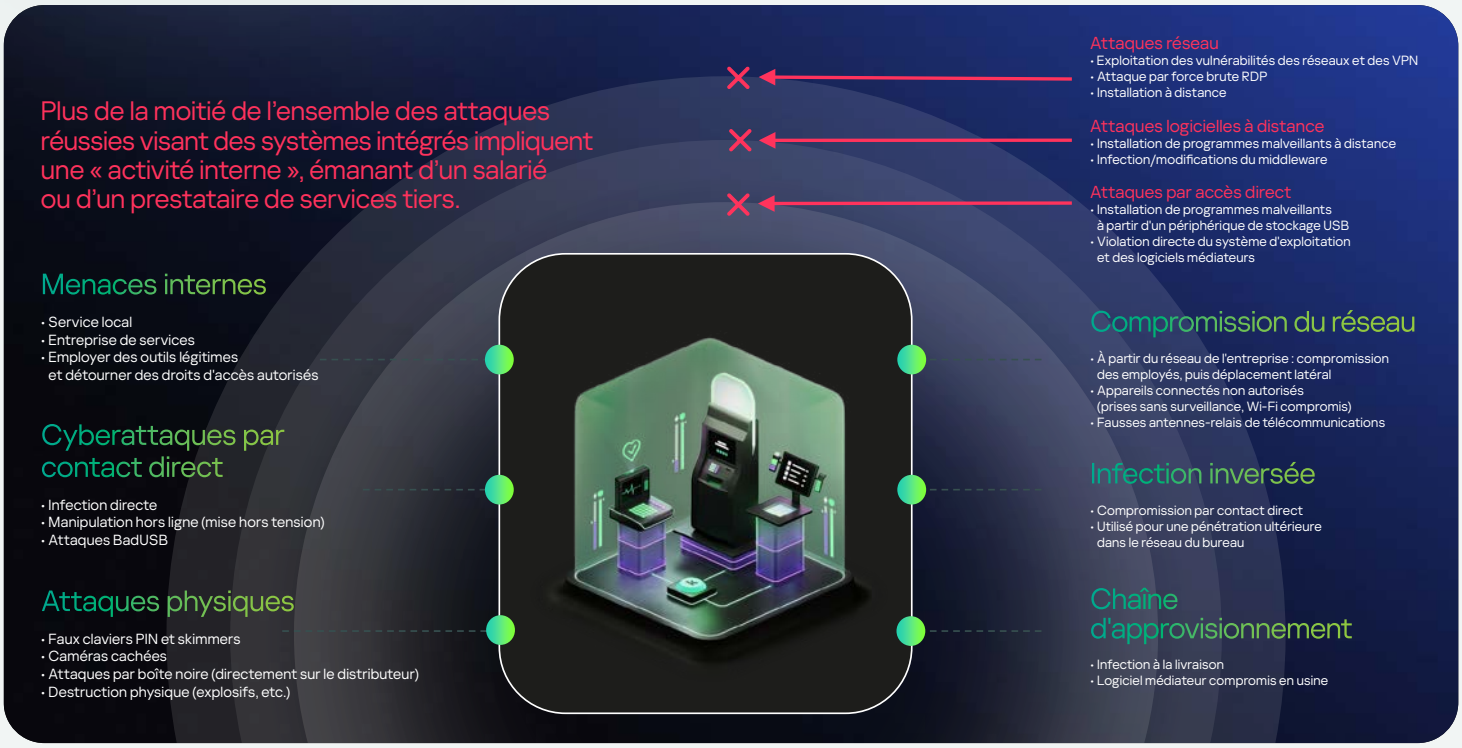
Les systèmes embarqués sont omniprésents, et nous interagissons avec eux tous les jours. Nous dépendons d'eux pour tout, des systèmes de point de vente aux distributeurs automatiques de billets, en passant par les équipements médicaux et les stations-service automatiques. À mesure que le marché des systèmes embarqués se développe, les cybercriminels progressent, affinant leurs tactiques, techniques et procédures pour s'adapter aux particularités de ces systèmes très répandus.

Paysage des menaces

De nouveaux modèles d'activité criminelle comme les programmes malveillants en tant que services continuent d'émerger, faisant baisser le niveau de compétences des aspirants criminels. Les anciennes versions de Windows restent en service même si elles ont depuis longtemps atteint leur fin de prise en charge, Windows XP étant le système d'exploitation le plus répandu dans les appareils embarqués. Des millions d'appareils et d'ordinateurs embarqués continuent d'utiliser d'anciens systèmes d'exploitation vulnérables qui, pour une raison ou une autre, ne sont pas mis à niveau. C'est une porte ouverte aux pirates.

Entre-temps, les systèmes embarqués sous Linux gagnent rapidement en popularité, et les cybercriminels en prennent note, adaptant leurs techniques et créant des outils entièrement nouveaux adaptés aux particularités de ces systèmes. Il est dangereux de surestimer la sécurité inhérente à Linux et, bien que les pirates informatiques n'aient commencé à s'intéresser aux appareils embarqués sous Linux que depuis peu, ils sont en train de rattraper le temps perdu. De plus, le fait que les solutions actuelles de cybersécurité destinées aux appareils embarqués fonctionnant sous Linux soient limitées par rapport à l'offre disponible pour Windows ne facilite pas les choses.

Les entreprises doivent faire preuve d'une ingéniosité inégalée pour protéger leurs systèmes et leurs données. Doté d'une puissante Threat Intelligence, d'une détection complémentaire des programmes malveillants et d'une prévention des exploits, de contrôles complets de renforcement du système et d'une gestion flexible, Kaspersky Embedded Systems Security est une solution de sécurité tout-en-un conçue spécialement pour les systèmes embarqués. Elle offre un niveau de protection unique pour les anciens systèmes qui ne sont plus pris en charge par la plupart des fournisseurs de cybersécurité, et offre désormais le même niveau de protection pour les appareils plus modernes fonctionnant sous le système d'exploitation Linux.



Systèmes embarqués : modèle de menace

Défis liés à la sécurité embarquée

6 **Réglementations strictes.** En raison des informations financières et d'identification personnelles qu'ils ont tendance à traiter, de multiples appareils embarqués sont régis par des réglementations exigeant une approche de sécurité particulièrement diligente.

7 **Menaces internes.** Selon les données Kaspersky, plus de 50 % de l'ensemble des attaques réussies visant des systèmes embarqués impliquent une « activité interne », émanant d'un salarié ou d'un prestataire de services tiers.

8 **Popularisation de Linux.** Les plateformes embarquées gagnent rapidement en popularité, offrant une plus grande flexibilité et permettant l'utilisation d'un plus large éventail de configurations. Les cybercriminels en ont pris note, et le choix de solutions de sécurité modernes et spécialisées est beaucoup plus limité que ce qui est disponible pour Windows.

Bénéfices

Protection optimale pour tout scénario intégré :
Kaspersky Embedded Systems Security offre une protection multi-couches afin de garantir une sécurité optimale pour les appareils présentant des niveaux de puissance et des scénarios de mise en œuvre différents. Ceci inclut la prise en charge des plateformes fonctionnant sous différents systèmes d'exploitation comme Windows et Linux.

Protège les systèmes existants et les nouveaux systèmes
Kaspersky Embedded Systems Security a été optimisé pour fonctionner pleinement sous Windows XP, 7, 8, 10 et 11. Kaspersky continuera à prendre en charge Windows XP dans un avenir proche, ce qui laissera aux clients suffisamment de temps pour procéder à une mise à niveau lorsqu'ils seront prêts. Kaspersky Embedded Systems Security prend également en charge les architectures les plus récentes fonctionnant sous Windows ou Linux.

Faibles ressources, hauts niveaux de protection
Kaspersky Embedded Systems Security a été conçu pour fonctionner de manière efficace même sur du matériel bas de gamme.

Partie intégrante d'un écosystème unifié, la sécurité des systèmes Kaspersky Embedded fonctionne comme un composant organique d'une famille de solutions, gérée via la même console que les autres produits Kaspersky et bénéficiant d'une visibilité centralisée ainsi que d'un flux de travail unifié.

Principales fonctionnalités

Renforcement du système (contrôles de sécurité). Comprenant des contrôles d'applications, d'appareils et de mise à jour, ces technologies de renforcement des systèmes permettent l'utilisation exclusive des applications, des périphériques et des sources de mise à jour fiables. Cela empêche le lancement et l'exécution de programmes non autorisés, notamment les programmes qui pourraient être utilisés à des fins malveillantes.

Solutions de protection complémentaire contre les programmes malveillants. Un niveau de sécurité avec engagement détecte les menaces connues, inconnues et avancées avec une logique de détection précise et utilise la Threat Intelligence locale ou basée dans le cloud, ainsi que des modèles heuristiques et de Machine Learning s'exécutant sur site ou dans le cloud. La technologie spécialisée de protection contre le chiffrement assure une protection de vos appareils contre les ransomwares.

Prévention des vulnérabilités. Cette fonction empêche l'exploitation des vulnérabilités présentes dans les composants de Windows et les applications tierces en aidant à lutter contre les attaques plus avancées, notamment celles qui visent à contourner le contrôle des applications en mode blocage par défaut et qui utilisent des techniques sans fichier.

Protection contre les menaces réseau. Cette fonction empêche toute intrusion dans le système d'exploitation en offrant une protection contre les attaques d'analyse des ports et les attaques par force brute, ainsi que les cyberattaques qui exploitent les vulnérabilités liées au réseau pour compromettre l'appareil ciblé. Cette action permet de bloquer l'un des principaux vecteurs d'attaque dirigés contre les systèmes embarqués.

Surveillance de l'intégrité et prise en charge de la conformité. Les fonctions d'intégrité des fichiers et de surveillance des accès au registre[1] suivent les actions exécutées sur les clés, fichiers et dossiers de registre spécifiés et peuvent bloquer toute modification indésirable. Ainsi, elles détectent non seulement les intrusions basées sur des programmes malveillants, mais également les modifications en accès direct/hors ligne apportées aux ressources stratégiques. Ces mesures sont souvent spécifiquement recommandées dans les réglementations de protection des données, et leur mise en œuvre contribue à maintenir votre conformité.

Prise en charge des systèmes anciens et peu performants. Prend en charge même les systèmes embarqués peu puissants s'exécutant sur du matériel obsolète et des systèmes d'exploitation non pris en charge, jusqu'à Windows XP SP2. Vous pouvez continuer à utiliser d'anciens appareils ou ordinateurs de bureau en toute sécurité jusqu'à ce que vous soyez prêt à procéder à une mise à niveau.

Inspection des journaux[1]. Les éventuelles violations de sécurité sont détectées grâce à la surveillance et à l'inspection des journaux d'événements Windows. L'application prévient l'administrateur de tout comportement anormal détecté, signe d'une cyberattaque potentielle.

Gestion flexible – sur site ou dans le cloud. Selon vos besoins, la sécurité de vos systèmes embarqués peut être gérée soit depuis un serveur de gestion sur site, soit depuis la console SaaS Kaspersky Security Center dans le cloud, en même temps que les autres solutions Kaspersky. Même si la gestion sur site se révèle pratique lorsqu'un haut niveau de confidentialité est requis, la console SaaS dans le cloud opérée par l'éditeur permet de réaliser des économies à la fois au niveau des dépenses d'investissement et d'exploitation, pour des processus de travail sécurisés plus rapides et une maintenance allégée.

[1] pour Windows uniquement

Gestion du pare-feu. Le pare-feu du système d'exploitation peut être configuré directement depuis Kaspersky Security Center, ce qui vous offre la praticité d'une gestion locale du pare-feu via une console unique et unifiée. Cela est essentiel quand les systèmes embarqués ne sont pas dans le domaine et que les paramètres du pare-feu Windows/Linux ne peuvent pas être configurés de façon centralisée. Pour le système d'exploitation Windows, un pare-feu propriétaire au niveau des applications est disponible, ce qui réduit davantage la surface d'attaque grâce à une gestion plus granulaire des connexions réseau des applications.

Faible niveau de connectivité. Étant donné que de nombreux types d'appareils embarqués sont souvent installés à distance, il n'est pas rare que la connectivité soit médiocre, en raison d'une mauvaise couverture cellulaire, d'interférences provenant de sources radio proches, etc. Kaspersky Embedded System Security reste stable même en cas de bande passante très faible, ce qui permet de maintenir une protection fiable même pendant les périodes prolongées sans connectivité.

Intégration de la détection et de la réponse gérées : la solution s'intègre au centre des opérations de sécurité de Kaspersky pour une surveillance 24 h/24, 7 j/7 et une réponse rapide. Cela permet de détecter et de contenir rapidement les attaques complexes visant les appareils embarqués, évitant ainsi des pertes financières importantes pour l'entreprise.

Services professionnels et support Premium

La maintenance adéquate du cycle de vie d'une solution de sécurité requiert des efforts, et en raison des particularités des appareils embarqués qui les différencient des terminaux ordinaires, il peut être particulièrement fastidieux de préserver la sécurité des systèmes embarqués. Kaspersky Professional Services offre une assistance à chaque étape de ce cycle de vie, du déploiement et de la mise à jour, de la configuration et de l'optimisation des performances, jusqu'à la migration vers du matériel plus récent. De plus, notre support Premium prévoit une résolution prioritaire et professionnelle des incidents, grâce à un ingénieur avant-vente dédié, disposant d'une expertise inégalée.

Produits et services connexes

Kaspersky Threat Intelligence : une sélection de services polyvalents qui offre une vue d'ensemble des cybermenaces ciblant votre organisation, en combinant des sources de renseignements, des flux de données sur les menaces et des recherches internes, analysées par nos experts en sécurité.

Évaluation de la sécurité des systèmes de paiement : l'analyse complète de vos distributeurs automatiques et appareils de point de vente vous donne une image claire de vos niveaux de sécurité actuels, ce qui vous permet de renforcer davantage votre sécurité, d'en optimiser la configuration et de combler les éventuelles failles de sécurité.

Gamme de produits Kaspersky Next : combine une protection exceptionnelle des terminaux et des contrôles de sécurité puissants avec la transparence et la rapidité de l'EDR et la visibilité et les outils puissants du XDR, dans une gamme de produits flexible à plusieurs niveaux.

Secteurs d'activité

- Services financiers
- Transport et tourisme (billetterie)
- Vente au détail
- Accueil/Réception
- Soins de santé
- Systèmes du gouvernement et non commerciaux
- Divertissement

Appareils

- DAB
- Billetteries
- Stations services
- Terminaux d'achat
- Point de vente
- Équipement médical
- Terminaux obsolètes
- Machines à sous et jeux d'arcade

Industries utilisant des appareils embarqués

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr, dans lequel 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

Reconnu. Transparent. Indépendant.