Kingston TECHNOLOGY

La sécurité optimale des points finaux expliquée et explorée en partenariat avec Matrix42

MATRIX42

#KingstonIsWithYou

La sécurité optimale des points finaux expliquée et explorée en partenariat avec Matrix42

Introduction

Aujourd'hui, la protection des données est une exigence fondamentale pour les gouvernements, les entreprises et les particuliers.

Les violations de données, le piratage et le facteur humain ne sont quelques unes des menaces et des risques qui existent dans tous les secteurs d'activité. Les coûts financiers et de réputation engendrés par une violation de données peuvent être astronomiques. Les exigences des stratégies avancées de la cybersécurité et de la protection des données sur les terminaux dépendent toutes de la fiabilité et de l'efficacité des unités de stockage et de la mémoire.

Le chiffrement, les stockages et les mémoires rapides, l'adoption des meilleures pratiques, les normes rigoureuses et les stratégies de pointe représentent des progrès importants. Les ordinateurs portables et les clés USB égarés exposent les particuliers et les entreprises à des risques de divulgation d'informations personnelles et privées. Kingston propose des solutions de prévention qui minimisent les risques, et complètent le plan de sécurité mis en place ou en cours de développement.

La sécurité optimale des points finaux expliquée et explorée en partenariat avec Matrix42

Contenu

Ce petit eBook consacré aux solutions pour terminaux examine des scénarios de la vie réelle où les clés USB chiffrées de Kingston, leur programme de personnalisation et le logiciel de protection des données EgoSecure de Matrix42 ont résolu des problèmes dans six secteurs d'activité, en apportant une solution adaptée à des besoins métier spécifiques.

Dans ces six secteurs, nous découvrons comment les solutions ont surmonté les défis de la sécurité des terminaux.

Table des matières

Section 1 : Scénario industriel
Secteur public

Situation :

Dans le secteur public, l'utilisation de dispositifs USB est très courante. Par exemple, les services de police doivent copier les photos prises par les auteurs d'infractions au stationnement et leurs fichiers administratifs sur les systèmes centraux en utilisant une liaison USB. Les autorités de police reçoivent les données des enquêtes sur des dispositifs de stockage externes. Ces données doivent être retranscrites et les accès non autorisés doivent être bloqués.

Le défi :

En raison de la forte demande en dispositifs USB, les employés demandent régulièrement des clés USB. L'utilisation de dispositifs de stockage privés et non autorisés doit être bloquée pour des raisons de sécurité. Lorsqu'un employé a besoin d'un nouveau périphérique de stockage USB, il doit être fourni le plus rapidement possible par le service d'assistance aux utilisateurs pour préserver leur productivité. Il est important de noter que l'utilisation des dispositifs USB appropriés ne génère aucun problème de sécurité.

La solution :

En combinant le contrôle des dispositifs, le filtrage des données et leur chiffrement, le scénario suivant a été mis en œuvre :

Les dispositifs inconnus sont généralement bloqués par les terminaux. Les dispositifs de stockage tels que les appareils photos numériques ne sont autorisés que pour certaines fonctions, notamment la lecture de fichiers d'images. Les opérations d'écriture sont généralement chiffrées et ne sont autorisées que sur des périphériques USB autorisés. Tous les accès aux données sont consignés. La gestion des dispositifs autorisés peut être simplifiée par la personnalisation des numéros de série et des identifiants du matériel. Ainsi, la gestion des services Matrix42 permet à l'utilisateur de commander une clé USB Kingston Technology personnalisée sur le portail libre-service. Après un processus d'autorisation, l'utilisation de la clé, ou autre dispositif, USB est automatiquement autorisée avec le logiciel de protection des données EgoSecure.

> “Nos employés apprécient beaucoup que les nouveaux dispositifs USB sont fournis facilement et rapidement après une procédure d'autorisation rapide. Nous sommes très satisfaits du programme de personnalisation de Kingston Technology et de la facilité d'administration que procure la combinaison de la gestion des services et de la sécurité des terminaux Matrix42.”
>
> **Responsable de l'assistance technique, Secteur public**

Section 2 : Scénario industriel
Santé

Situation :

Les dispositifs de stockage externes continuent d'être fréquemment utilisés pour échanger des données en interne et avec d'autres institutions.

En Allemagne, par exemple, les hôpitaux doivent fournir au registre du cancer des informations sur les cas de cancer actuels et leur évolution. Pour faciliter les choses, ces données sont souvent transférées via des dispositifs de stockage mobiles.

Les médecins aiment également copier sur des clés USB leurs documents, notamment des résultats de recherche pour participer à des conférences.

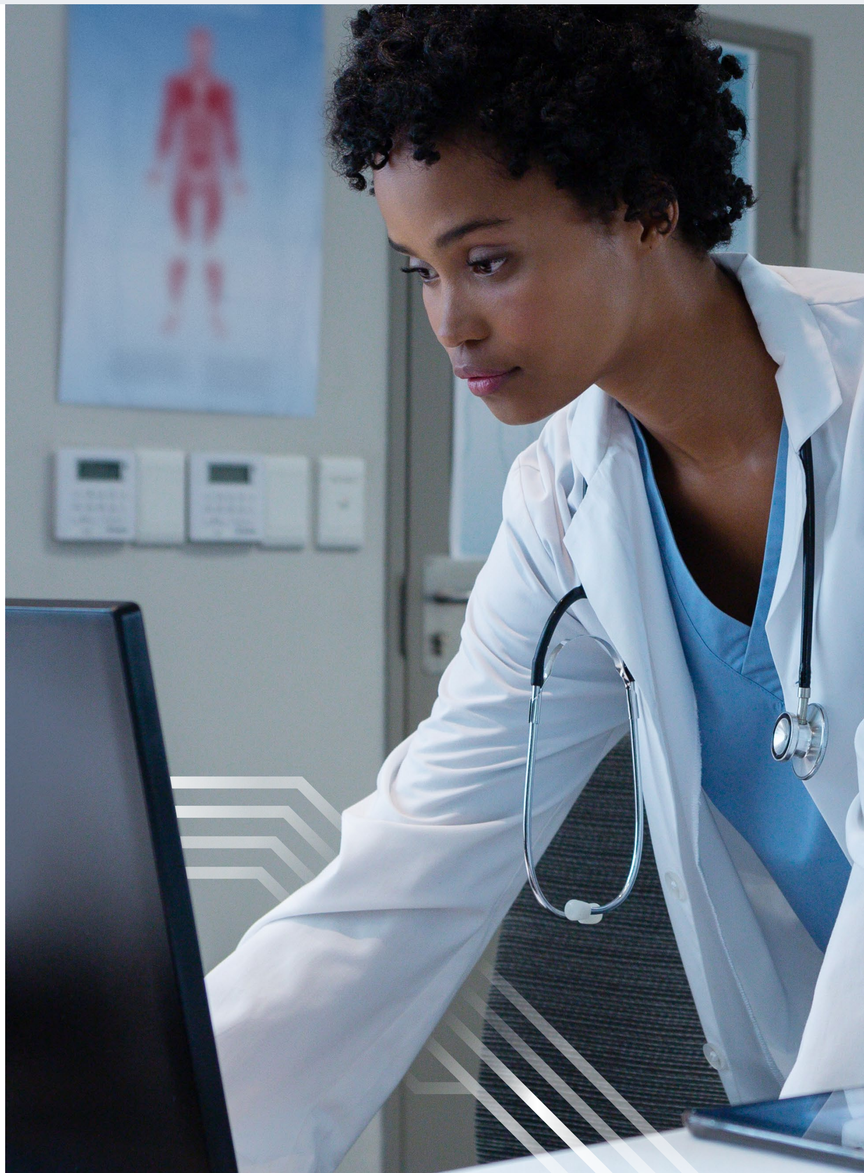
Le défi :

Les données des patients sont extrêmement sensibles et ne doivent pas tomber entre les mains de personnes non autorisées. C'est pourquoi la protection des données doit toujours être actualisée et renforcée. Si un support de données est perdu, cela peut devenir un problème majeur, non seulement à cause du RGPD, mais aussi pour le bien-être des patients. Pour cette raison, il est important que l'accès au stockage de données USB soit contrôlé, surveillé et chiffré.

La solution :

Le logiciel de protection des données EgoSecure combine diverses mesures de protection telles que le contrôle d'accès, l'audit des données, le filtrage et le chiffrement dans une seule solution. Les administrateurs informatiques sont en mesure de décider quels employés ont accès à quels appareils. Des exceptions peuvent être programmées grâce aux numéros de série et aux identifiants du matériel, par exemple. Ces identifiants peuvent être définis grâce au programme de personnalisation de Kingston Technology. Une seule valeur suffit pour configurer l'utilisation des seuls appareils approuvés par l'entreprise dans le logiciel de protection des données d'EgoSecure. Cela permet de réduire considérablement le travail d'administration et de renforcer la sécurité des données (RGPD, CCPA, HIPAA, etc.), car l'accès est chiffré et contrôlé.

> “Nous avions déjà utilisé des clés USB chiffrées Kingston. Maintenant, avec le logiciel de protection des données EgoSecure, nous pouvons également garantir la conformité de la traçabilité des transferts de données des patients au RGPD-UE.”
>
> **CISO, Hôpital universitaire**



Section 3 : Scénario industriel
Finance

Situation :

Les banques sont soumises à diverses exigences de conformité. La norme PCI-DSS (Payment Card Industry Data Security Standard) fait partie de ces exigences. La norme PCI-DSS exige le chiffrement et le filtrage des données, ainsi que l'analyse des vulnérabilités. L'objectif est de minimiser ou de prévenir complètement les menaces et les risques de sécurité informatique.

Le défi :

De nombreux risques de sécurité informatique s'accumulent sur les terminaux, ou tout dispositif connecté à un réseau. Les employés traitent les informations des cartes de paiement des consommateurs et des entreprises et traitent quotidiennement les données sensibles des institutions financières. Ces données sont donc exposées aux diverses menaces du cloud, de la messagerie électronique, des échanges USB et par internet, porteuses de logiciels malveillants, et aux risques de détournement par des tiers si elles ne bénéficient pas d'une protection suffisante. Ce type de risque implique des conséquences financières lourdes pour les banques, en particulier au regard du RGPD, de la norme PCI-DSS mais aussi de loi Sarbanes-oxley. En outre, les cybercriminels tentent constamment d'influencer ou de manipuler les systèmes bancaires de diverses manières et font preuve d'une créativité redoutable. Plus récemment, par exemple, des cybercriminels ont attaqué des distributeurs automatiques de billets en interrompant leur alimentation électrique, afin de redémarré le système avec un dispositif USB amorçable conçu pour extraire de l'argent en contournant les mesures de sécurité existantes.

La solution :

Les systèmes informatiques doivent être sécurisés par des mesures de protection multi-couches. Cette structure de défense combine le contrôle des applications, le contrôle des dispositifs, la détection des anomalies, l'UEBA (User and Entity Behaviour Analytics), la surveillance et le chiffrement intégral des disques avec authentification PreBoot. Avec une solution Matrix42 mis en œuvre dans un écosystème automatisé et intégral, seules les applications autorisées et les dispositifs USB chiffrés sont autorisés. En outre, les activités suspectes ou malveillantes sont détectées et des contre-mesures efficaces sont automatiquement déclenchées. En ce qui concerne l'utilisation des clés USB, la combinaison des clés USB personnalisées de Kingston Technology garantit que tous les dispositifs sont inscrits dans une liste blanche avec un minimum d'efforts et que le chiffrement des données intègre des éléments de traçabilité inattaquables. Cette solution renforce considérablement la conformité, sans effort supplémentaire.

> « Avec la protection des données EgoSecure et la liste blanche, notre système ne peut qu'autoriser et accepter des clés USB chiffrées Kingston. Nous mettons en liste blanche les clés USB chiffrées Kingston avec une identification matérielle personnalisée. Aucun autre dispositif n'est autorisé. Non seulement notre travail administratif est considérablement réduit, mais notre sécurité est largement renforcée ! »
>
> **Directeur informatique, Entreprise financière**

Section 4 : Scénario industriel Automobile

Situation :

Dans l'industrie automobile, les dispositifs USB sont largement utilisés dans divers domaines. Par exemple, les données de recherche sont stockées sur des dispositifs externes et échangées entre les ingénieurs des différents processus. Pour configurer les machines, nous devons transporter des fichiers entre l'environnement informatique et chaque environnement de production. Toutes ces données sont extrêmement sensibles et doivent être protégées contre l'espionnage industriel et le vol de données, sinon le savoir-faire accumulé par l'entreprise pourrait tomber entre de mauvaises mains.

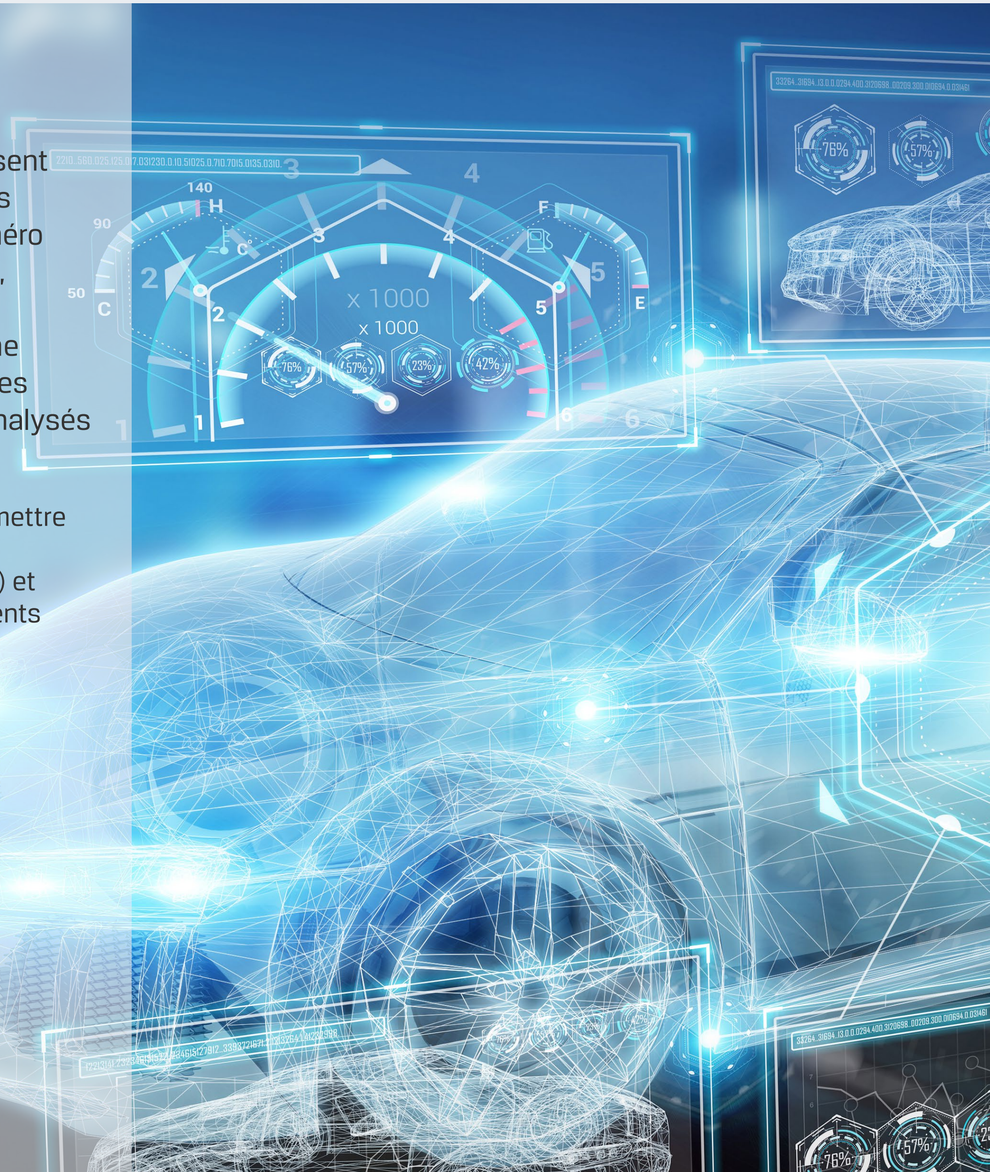
Le défi :

L'industrie automobile est soumise à des exigences de conformité telles que TISAX, la protection des prototypes, ENX, ISO27001, pour les connexions externes, et le RGPD pour la protection des données. Dans TISAX, les articles 9.1, 9.5 et 10.1 du contrôle stipulent que les accès aux données doivent être contrôlés, surveillés, filtrés et chiffrés. Ces mesures doivent également être respectées dans les autres exigences de conformité telles que le RGPD et ISO27001 dans tous les domaines des entreprises automobiles.

La solution :

Les clés USB chiffrées de Kingston Technology sécurisent les données grâce à leur chiffrement matériel. Ces clés peuvent être automatiquement identifiées par un numéro de série personnalisé et un identifiant matériel unique, que le logiciel de protection des données EgoSecure exploite automatiquement pour la mise en liste blanche selon utilisations spécifiques des données. En outre, les mouvements de données peuvent être surveillés et analysés en cas d'activités suspectes.

> “Avec Matrix42 et Kingston Technology, nous avons pu mettre en œuvre la conformité aux exigences TISAX, telles que Control 9.5 (accès aux informations et aux applications) et Control 10.1 (cryptographie) sans imposer de changements majeurs dans le travail des utilisateurs.”
>
> **CTO, équipementier automobile**



Section 5 : Scénario industriel Télécommunication

Situation :

Les opérateurs des télécommunications stockent de nombreuses données sur leurs clients. Ces informations sont très sensibles, notamment en ce qui concerne le RGPD. Des mesures de sécurité importantes sont donc indispensables suffisantes pour prévenir la perte et le vol de données.

Le défi :

Les employés des entreprises de télécommunications utilisent chaque jour des données clients stratégiques. La plupart de ces données sont stockées dans des applications commerciales. Toutefois, les contrats des clients ou même les exportations de bases de données sont souvent exposés aux risques du stockage sur des terminaux et des dispositifs externes. De plus pour échanger les données, les utilisateurs ont souvent besoin d'un stockage externe. Il est donc très important que toutes les méthodes et manipulations de stockage incorrectes soient détectées et corrigées ou protégées.

La solution :

Pour simplifier le processus d'approvisionnement, les clés USB chiffrées de Kingston Technology avec un identifiant produit personnalisé peuvent être rapidement achetées via une liste blanche prédéfinie dans EgoSecure Data Protection et livrées via le catalogue de services Matrix42. Le stockage et l'exportation de données, qui peuvent contenir des informations sensibles, peuvent être automatiquement identifiés et corrigés par une inspection approfondie du contenu basée sur des analyses qui séparent les « données en cours d'utilisation » et les « données au repos » . Les mouvements des données sont enregistrés de manière centralisée. Ainsi, chaque employé peut recevoir le nouveau matériel de stockage commandé, très rapidement après son autorisation. Cette méthode garantit aussi sa conformité au RGPD.

> “Grâce au portail libre-service de Matrix42, nos utilisateurs peuvent demander les supports de stockage dont ils ont besoin. Une fois la commande approuvée et livrée, le périphérique est autorisé par le contrôle des périphériques d'EgoSecure. La combinaison de Matrix42 et de Kingston Technology augmente la productivité et la sécurité dans notre entreprise.”
>
> **CTO, Opérateur de télécommunications**

Section 6 : Scénario industriel
Fabrication

Situation :

Les données numériques sont l'or du futur. Dans les industries manufacturières, ces données incluent les plans de production, les données sur les clients et les fournisseurs, et le savoir-faire des entreprises. Les pertes de ces données entraînent non seulement des pénalités très lourdes au regard du RGPD, mais aussi des problèmes exponentiels et de réputation. Malheureusement, des clés USB sont tous les jours perdues dans des taxis, des blanchisseries, des aéroports, les gares ou des parkings.

Le défi :

Les dispositifs de stockage contiennent souvent des données très sensibles qui ne sont que trop rarement chiffrées. Un autre risque vient des techniciens de service qui utilisent des supports de données externes pour installer des mises à jour sur les machines de production. Ces dispositifs externes sont largement exposés aux attaques de logiciels malveillants circulant dans le réseau.

La solution :

Les clés USB chiffrées de Kingston Technology sécurisent les données grâce à leur chiffrement matériel. Ces clés sont fournies avec un numéro de série personnalisé et une identification matérielle que le logiciel EgoSecure Data Protection utilise automatiquement pour gérer la mise liste blanche selon des utilisations spécifiques des données. En outre, les mouvements de données peuvent être surveillés et analysés en cas d'activités suspectes.

> « Le chiffrement de nos données de production joue donc un rôle très important dans notre système de protection contre le vol. Ces données extrêmement sensibles ne sont autorisées que sur des clés USB chiffrées Kingston approuvées, sous le contrôle du filtrage des fichiers d'EgoSecure Data Protection. Sur tous les autres dispositifs USB, les données de production sont bloquées et l'accès en écriture aux stockages externes est sécurisé par le chiffrement et l'enregistrement à la volée d'EgoSecure. »
>
> **Directeur de la sécurité informatique, Secteur de la fabrication**

Section 7 : Solutions Kingston Technology et Matrix42

Le chiffrement, les stockages et les mémoires rapides, l'adoption des meilleures pratiques, les normes rigoureuses et les stratégies de pointe représentent des progrès importants. Les ordinateurs portables et les clés USB égarés exposent les particuliers et les entreprises à des risques de divulgation d'informations personnelles et privées. Kingston propose des solutions de prévention des menaces qui minimisent les risques, et complètent le plan de sécurité mis en place ou en cours de développement.

Clés USB chiffrées de Kingston Technology

Les clés USB à chiffrement matériel de Kingston intègrent des solutions de protection des données mobiles des deux côtés du pare-feu de l'organisation. Conçues pour protéger des données qui exigent une sécurité absolue, ces clés vous permettront de respecter les normes, les directives et les réglementations propres à chaque secteur d'activité. Les produits sont conformes au TAA, certifiés FIPS et disponibles dans des capacités allant jusqu'à 128 Go, ce qui répond parfaitement aux besoins des entreprises et de l'administration publique.

Programme de personnalisation sécurisée

Vous pouvez personnaliser les clés USB chiffrées de Kingston de diverses façons pour mieux répondre aux besoins de votre entreprise. Ajoutez des caractéristiques sélectionnées pour créer des clés uniques et indispensables. Par l'intermédiaire de votre revendeur habituel, Kingston® propose une procédure de commande aisée et pratique pour toutes vos clés USB chiffrées et personnalisées. La gamme des produits USB chiffrés de Kingston inclut les clés DTVP30, DT4000G2 et IKD300S. Ce programme offre les options les plus fréquemment demandées par les clients, notamment les numéros de série, les mots de passe doubles et les logos personnalisés. Grâce à sa commande minimale de 50 pièces, et un renouvellement à partir de 25 pièces, le programme satisfait exactement aux besoins de votre société.

Protection des données EgoSecure de Matrix42

EgoSecure Data Protection de Matrix42 apporte aux entreprises une gestion de la sécurité à 360° qui répond aux exigences de la prévention et de la protection des dispositifs, des systèmes et des données. La solution automatise l'ensemble du processus, depuis la prévention et la détection aux contre-mesures en cas de dommage, sans perte de productivité.

Synthèse

La protection des données et la cybersécurité peuvent être perçues comme de lourdes responsabilités. Les exigences en matière de travail numérique ont considérablement évolué, les employés ayant la possibilité de décider eux-mêmes quand, où et avec quels appareils ils travaillent. Le bon choix de clés USB protégées par un chiffrement matériel et une gestion logicielle des terminaux apporte aux organisations une meilleur contrôle de leurs dispositifs. Elles peuvent alors bénéficier de la réduction des risques de violation des données et d'une stratégie en conformité continue avec le RGPD.

À propos de Kingston

Avec plus de 30 ans d'expérience, Kingston Technology a toutes les connaissances nécessaires pour identifier et résoudre les problèmes de sécurité de vos terminaux sans jamais compromettre votre organisation.

#KingstonIsWithYou