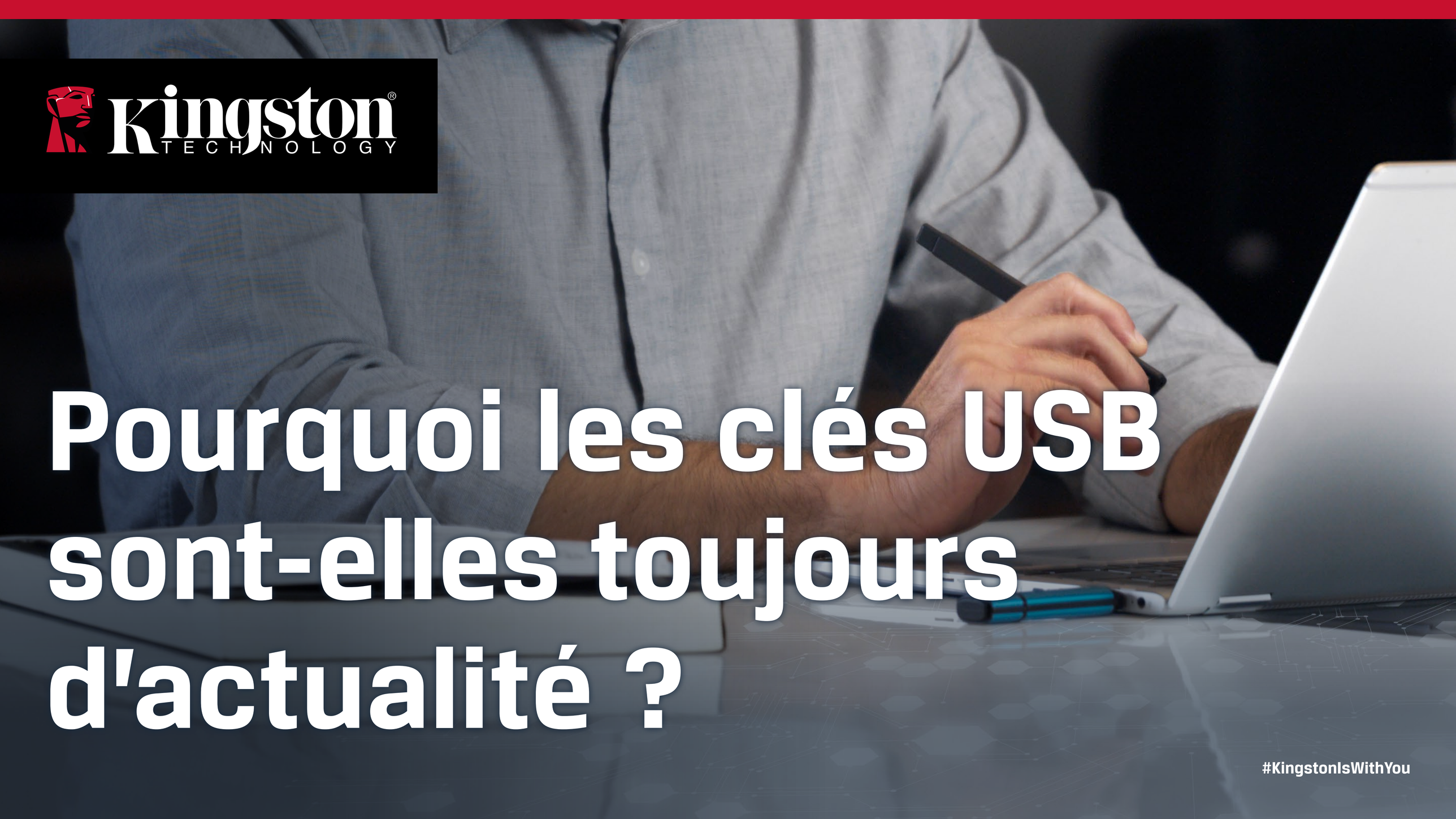

Kingston
TECHNOLOGY
Pourquoi les clés USB sont-elles toujours d'actualité ?
#KingstonIsWithYou

Pourquoi les clés USB sont-elles toujours d'actualité ?

Avant-propos et contenu

À l'ère du numérique actuelle, où 60 % de toutes les données d'entreprise mondiales sont stockées dans le cloud[1], discuter de la pertinence d'une technologie de stockage qui a presque trente ans peut sembler un peu étrange. Pourtant, depuis son introduction, ce basique du stockage n'a cessé d'évoluer et continue de le faire.

Il est loin le temps où les clés USB étaient simplement un moyen standard de connecter des fichiers, des lecteurs et des applications. Les solutions d'aujourd'hui offrent non seulement une vitesse de transfert considérablement améliorée, mais elles fournissent également des supports portables fiables et sécurisés qui s'avèrent indispensables dans de nombreuses situations. Mais comment se fait-il que les clés USB soient encore pertinentes, alors que les solutions de stockage cloud peuvent apparemment offrir de nombreux avantages similaires ?

Dans cet eBook, nous allons discuter de la place des clés USB dans un paysage dominé par le cloud. En nous appuyant sur les avis éclairés d'experts majeurs du secteur, nous explorerons la façon dont les organisations d'aujourd'hui utilisent les clés USB et débattrons de leur place dans le chiffrement basé sur le logiciel, dans les environnements de stockage indépendants et dans la sécurité des données des terminaux.

Table des matières	Pages
Contributeurs	3
L'essor de la clé USB	4
Un stockage portable qui répond à l'évolution de la demande	5-6
Chiffrement : Basé sur le matériel ou sur le logiciel	7-8
Le besoin croissant de protéger les données sensibles	9
Sécuriser les données financières sensibles	10
Accès sécurisé aux données de santé des patients	11
La clé USB dans un avenir de stockage cloud	12-13
Résumé et informations sur Kingston	14

Pourquoi les clés USB sont-elles toujours d'actualité ?

Contributeurs

Cet eBook a été créé avec trois experts du secteur de l'informatique et des technologies émergentes.

Rafael Bloom

Rafael a passé sa carrière à des postes de direction dans les secteurs des produits technologiques, de communication marketing et de développement commercial. Il concentre son activité de conseil sur les nouveaux défis des organisations, des produits et des communications liés aux changements technologiques et réglementaires. Ce travail très diversifié implique une expertise sur la gouvernance et la conformité de l'information, la confidentialité des données et les technologies émergentes telles que l'AdTech, le mobile et la 5G, l'intelligence artificielle et le machine learning.

Tomasz Surdyk

Avec plus de 24 ans d'expérience dans le domaine de la sécurité informatique au niveau gouvernemental, Tomasz est un spécialiste réputé de la sécurité de l'information, des données personnelles et de la cybersécurité. Il a également inspecté des réseaux et des systèmes d'information et de communication traitant des informations classifiées et des données personnelles dans l'administration publique et possède une habilitation de sécurité pour l'OTAN et l'UE. Depuis plusieurs années, il gère sa propre entreprise, spécialisée dans la mise en œuvre de solutions conçues pour renforcer la protection des informations professionnelles et des données personnelles.

David Clarke

David est reconnu comme l'un des 10 principaux influenceurs du "Top 30 des leaders d'opinion et penseurs les plus influents sur les médias sociaux, dans la gestion des risques, la conformité et le reg-tech au Royaume-Uni" de Thompson Reuter et figure dans la liste des 50 premiers experts mondiaux de Kingston Technology. [reg-tech : technologie au service de la réglementation en banque]. Auparavant, David a occupé plusieurs postes de gestion de la sécurité, notamment : responsable mondial de la prestation des services de sécurité et responsable de l'infrastructure de sécurité pour des entreprises multinationales du FTSE 100.

L'essor de la clé USB

Lorsque la première clé USB (Universal Serial Bus) est apparue sur le marché il y a plus de vingt ans, sa compatibilité collective a changé la donne dans le domaine de la technologie informatique. Sa capacité à être utilisée sur un large éventail d'appareils a favorisé son adoption par le grand public. Et l'USB a rapidement évolué : un transfert de données nettement plus rapide, un port USB 3.0 et des capacités de stockage encore plus élevées que lors de la sortie de la première clé USB en 2000.

Depuis lors, cette technologie a parcouru un long chemin en termes de stockage de données mobiles et de besoins en sécurité. L'accent est mis sur la génération actuelle de clés USB, lesquelles sont conçues pour des cas d'utilisation très spécifiques. Du point de vue de l'entreprise, l'augmentation du travail à distance et hybride, l'utilisation de services cloud et les préoccupations en matière de cybersécurité requièrent des solutions plus efficaces. Parallèlement, les exigences réglementaires imposent que les données soient stockées de manière conforme. Ces exigences peuvent être aggravées par des systèmes complexes qui peuvent fonctionner « sur site » et dans le cloud.

Il y a ensuite la question des volumes croissants de données structurées et non structurées, telles que les documents, les e-mails, les photos, les vidéos et les métadonnées. Tout cela vient s'ajouter à la complexité des besoins de stockage évolutifs des entreprises.

Mais si le stockage cloud peut répondre à bon nombre de ces défis, quelle est la pertinence des clés USB dans le paysage professionnel d'aujourd'hui ?

> **De nombreuses personnes pensent que les clés USB sont démodées ou banales en raison de leur utilisation par le passé en tant qu'appareil plus ou moins jetables, peu performants et peu sécurisés. - Rafael Bloom**

Un stockage portable qui répond à l'évolution de la demande

Les anciens schémas d'utilisation des clés USB comme moyen de stockage portable ont presque disparu. Aujourd'hui, les clés USB hautes performances ont émergé pour assurer une sauvegarde en local personnelle et sécurisée, avec une couche supplémentaire de protection et de confidentialité des données. Cela peut être très important pour les données sensibles en termes de conformité telles que les dossiers des RH, les données financières, les dossiers médicaux, la sécurisation de la propriété intellectuelle (IP) et toutes les informations personnellement identifiables (PII). En outre, cette génération de clés USB est dotée de capacités rapides de transfert, de stockage, de sauvegarde et de sécurité des données qui peuvent être utilisées pour :

- les informations réglementaires qui doivent être remises en main propre ;
- les documents juridiques et financiers qui doivent être livrés et imprimés sur site ou hors site ;
- tout environnement potentiellement hostile où les ransomware (ou « rançongiciels ») peuvent constituer une menace ;
- le transfert vers des systèmes d'impression où l'accès au réseau n'est pas autorisé.

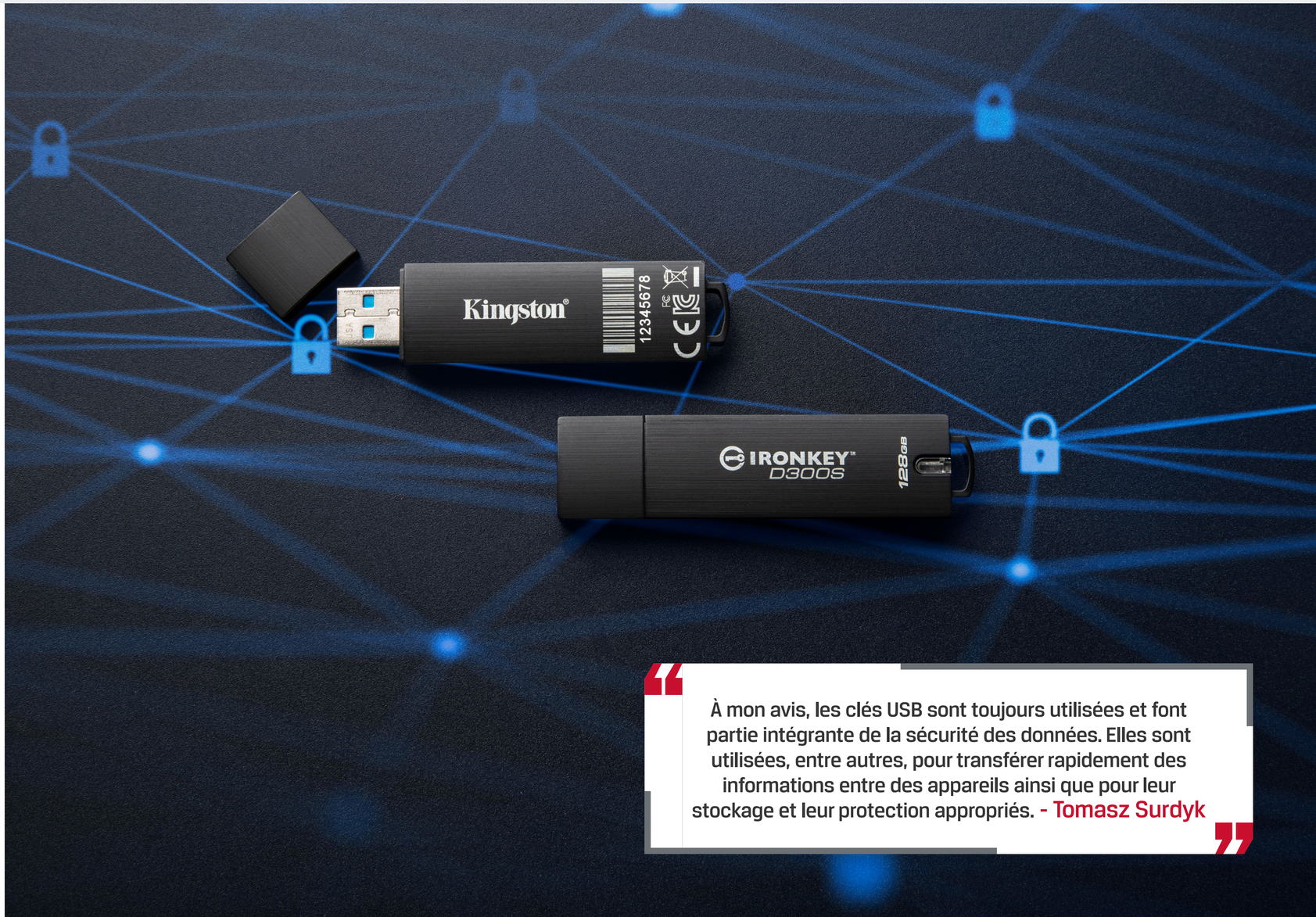
Les principaux fournisseurs de clés USB chiffrées Kingston Technology ont suivi le rythme de l'évolution de la demande avec le lancement de solutions telles que la clé Kingston IronKey™ S1000. Cette clé USB chiffrée, la meilleure de sa catégorie, répond aux normes les plus strictes en matière de protection des données confidentielles grâce à un chiffrement XTS-AES 256 bits et à une puce cryptographique distincte dotée de solides protections anti-piratage. En outre, elle est certifiée FIPS 140-2 niveau 3. Cela signifie qu'elle a été officiellement validée par le gouvernement américain pour son efficacité en tant que matériel cryptographique. Elle est donc idéale pour les organisations qui ont besoin d'une plus grande tranquillité d'esprit en matière de protection des données.

Ces clés USB à chiffrement matériel offrent des solutions de gestion centralisée des périphériques sécurisés, que leurs données soient dans le cloud ou sur site. Le stockage de données chiffrées conforme, facile à utiliser et ne nécessitant aucun logiciel, libère également un temps précieux pour le service informatique, en offrant des solutions conçues pour un déploiement rapide et efficace.

Un stockage portable qui répond à l'évolution de la demande

La sauvegarde et l'archivage sont un autre exemple où les clés USB peuvent être utilisées pour protéger les ressources numériques à long terme, et indépendamment des services cloud tiers. S'il est vrai que les transferts de données volumineux sont facilement gérés dans le cloud, la propriété intellectuelle peut encore être suffisamment sensible pour qu'il vaille la peine de la stocker sur une clé USB chiffrée et sécurisée, laquelle peut être stockée loin d'Internet.

Il y aura toujours des circonstances où une organisation a besoin que les données soient logiquement et physiquement sous son contrôle, surtout lorsqu'elle utilise des clés USB chiffrées. Et il y a des cas où le stockage sur un disque dur/SSD ne peut pas être chiffré. L'utilisation de clés USB chiffrées externes telles que la Kingston IronKey D300S résout ce problème. Cette clé USB est dotée d'un système de chiffrement matériel XTS 256 bits AES (norme de chiffrement avancé), qui est un type de chiffrement par blocs capable de chiffrer des blocs de données de 128 bits. Et lorsque le besoin se fait sentir de chiffrer des données au-delà, AES utilisera le mode de chiffrement par bloc XTS, qui est capable de fournir une meilleure protection des données plus robuste que les modes précédents.



> À mon avis, les clés USB sont toujours utilisées et font partie intégrante de la sécurité des données. Elles sont utilisées, entre autres, pour transférer rapidement des informations entre des appareils ainsi que pour leur stockage et leur protection appropriés. - Tomasz Surdyk

Chiffrement : Basé sur le matériel ou sur le logiciel

Si l'on examine la manière dont les données sont chiffrées, on peut affirmer que le chiffrement matériel est plus facile à gérer et plus sûr que le chiffrement logiciel. En effet, le processus de chiffrement est séparé du reste du système hôte, ce qui le rend beaucoup plus difficile à intercepter ou à casser. La gestion centralisée au niveau des périphériques permet de contrôler les connexions intranet, LAN et Internet, et peut être un excellent outil pour :

- établir et appliquer des politiques d'utilisation des clés USB chiffrées individuelles et/ou de groupe ;
- auditer l'activité des fichiers afin de mieux suivre les données lorsqu'elles entrent et sortent de votre organisation ;
- assurer la sauvegarde à distance du contenu pour le transport de données critiques ;
- désactiver à distance les périphériques lorsqu'une clé USB est perdue ou compromise ;
- réinitialisation à distance des mots de passe en cas d'oubli.

Lorsque les lecteurs autorisés sont correctement gérés de cette manière, cela minimise le risque de copie et de partage de données sensibles. En outre, les clés USB modernes à chiffrement matériel offrent une pléthore de fonctions de sécurité supplémentaires qui empêchent l'accès aux fichiers et aux messages ou leur lecture par toute personne autre que le destinataire prévu.

> **Je pense que le chiffrement matériel est meilleur que le chiffrement logiciel. Les différences entre les méthodes de chiffrement matériel et logiciel sont importantes en termes de vulnérabilité aux attaques par force brute. Dans le cas des appareils à chiffrement matériel, il n'est pas facile de succomber à de telles attaques.**
>
> - Tomasz Surdyk

Chiffrement : Basé sur le matériel ou sur le logiciel

Les entreprises peuvent opter pour le chiffrement basé sur le logiciel en raison de leur coût, mais c'est un argument un peu court. Les solutions basées sur le logiciel partagent les ressources de chiffrement de l'appareil hôte avec d'autres programmes, de sorte que leur sécurité dépend de celle de l'ordinateur et qu'elles nécessitent souvent des mises à jour logicielles qui, si elles ne sont pas correctement gérées, vous rendront vulnérables. Les clés USB chiffrées par logiciel peuvent être soumises à des attaques par force brute illimitées visant à deviner le mot de passe. Et elles n'ont aucun moyen de résister aux attaques par dictionnaire basées sur logiciel, lesquelles peuvent tester des millions de combinaisons de caractères en très peu de temps.

En outre, le chiffrement logiciel est un chiffrement amovible. Tout employé disposant d'un disque chiffré par logiciel peut copier les données, formater la clé USB, et le chiffrement est supprimé. Il peut ensuite recopier les fichiers de données et utiliser la clé USB sans avoir à s'authentifier sur différentes plateformes et systèmes d'exploitation.

Comme nous l'avons mentionné précédemment, avec le chiffrement matériel, le « chiffrement » physique (et le stockage ultérieur des données) se produit indépendamment du système hôte. Cela garantit une couche de défense supplémentaire, si jamais les systèmes étaient compromis.

Cet aspect ne peut être négligé, en particulier pour ceux qui travaillent dans des secteurs tels que la finance, la santé et le gouvernement. En effet, les réglementations telles que le Health Insurance Portability and Accountability Act (HIPAA) et le Payment Card Industry Data Security Standard (PCI DSS) ont souvent des exigences strictes concernant le chiffrement des informations sensibles.

En se conformant à ces réglementations en utilisant des périphériques à chiffrement matériel fort, les organisations éviteront des amendes coûteuses, des poursuites judiciaires et des atteintes à leur réputation. Certes, les clés à chiffrement matériel sont plus coûteux que les clés USB de base moins chères. Mais il faut tenir compte du fait que les frais de seules quelques heures de consultation juridique suffiraient à acheter des centaines de ces clés.

Le besoin croissant de protéger les données sensibles

> Chiffrez toutes les données aussi rapidement que possible, sauvegardez en utilisant une méthode 321 (l'USB pourrait être une option car elle est facilement disponible), et mettez en place une capacité de micro segmentation rapide. - David Clarke

Lorsqu'il s'agit de protéger les données sensibles contre la perte et le vol, chaque organisation a l'obligation de s'assurer que ses appareils disposent de fonctions de sécurité adéquates. Il est également important de considérer que, bien qu'il existe une myriade de cybermenaces en constante évolution, le niveau de maturité numérique et les compétences des utilisateurs en matière de gestion des données des terminaux restent un facteur de risque important s'ils ne sont pas pris en compte. Les menaces (telles que la perte du contrôle des données ou de clés USB, la transmission de données en dehors d'un environnement sûr, l'utilisation de clés USB non chiffrées et le partage de mots de passe) peuvent toutes être le résultat d'un manque de vigilance de la part de l'utilisateur final. Toutes ces situations peuvent être évitées grâce à une formation adéquate, à l'éducation et aux bonnes solutions de clés USB.

> L'organisation devrait disposer d'une carte claire de ses données, y compris le niveau d'importance et/ou de sensibilité de tous ses ensembles de données, avec un plan visant à traiter les données les plus importantes en premier, soit en supprimant physiquement la connexion aux données, soit en mettant cette source de données hors service. Il est essentiel d'être capable d'isoler rapidement les systèmes affectés. Et là encore, disposer d'un plan documenté que vous avez mis en pratique est absolument vital. - Rafael Bloom

La pré-planification et une structure de communication bien rodée jouent également un rôle clé pour faire face à une menace potentiellement empirique. Les cyber-menaces d'aujourd'hui sont destinées à cibler les points faibles des organisations.

Le meilleur moment pour développer un plan pour les clés USB chiffrées est avant qu'il ne soit réellement nécessaire, en intégrant les clés USB chiffrées et les politiques dans la stratégie de sécurité globale de votre organisation. Si vous n'avez pas de plan en place pour les clés USB chiffrées ni de directives, vous n'avez rien sur quoi vous appuyer et votre organisation est exposée à des risques à tous les niveaux. Y compris le non-respect des réglementations, telles que le règlement général sur la protection des données (RGPD), dont l'article 32 stipule spécifiquement que les données sensibles doivent être chiffrées.

> Les utilisateurs gèrent des données sensibles. Leur perte accroît la responsabilité et affecte considérablement l'image et la sécurité de l'entreprise. Afin de protéger les données sensibles, il convient d'utiliser diverses solutions de sécurité, notamment le chiffrement des données. - Tomasz Surdyk

Sécuriser les données financières sensibles

Outre les implications en matière de sécurité, il existe également des normes de conformité auxquelles les solutions de stockage et de sauvegarde des données doivent se conformer. Certaines de ces pratiques, comme la nécessité de gérer et d'appliquer des calendriers de conservation des données, sont communes à tous les secteurs verticaux, tandis que d'autres, comme la migration des données d'entreprise vers le cloud, sont traitées très différemment.

Dans de nombreux secteurs verticaux, tels que les services financiers, des réglementations sont entrées en vigueur et ont rendu obligatoire une bonne gestion des données. Les banques, en particulier, étaient initialement très réticentes à l'idée d'utiliser des tiers pour le stockage et la sauvegarde. Et bon nombre d'entre elles insistent encore pour être propriétaires de toute leur infrastructure de données.

Les institutions financières sont également tenues de se conformer à une liste croissante de réglementations et de normes en matière de sécurité des données, telles que la loi Sarbanes-Oxley (SOX) et le règlement général sur la protection des données (RGPD). Cependant, à mesure que le nombre d'employés et de sous-traitants mobiles augmente, le risque de fuite de données et de non-respect des mandats imposés par ces lois et normes augmente également.

En réalité, les efforts de conformité peuvent être compromis avec une facilité déconcertante si les employés mobiles ne parviennent pas à protéger leurs identités numériques, leurs espaces de travail portables, leurs dossiers clients et les données financières qu'ils transportent. C'est pourquoi de plus en plus d'organisations se tournent vers des solutions de sécurité mobile comme les clés USB chiffrées Kingston IronKey, pour protéger les identités numériques et les applications, quel que soit l'endroit où leurs employés les emmènent.

> **Si l'on considère la tendance générale à une empreinte informatique davantage étendue et l'énorme extensibilité de l'infrastructure du cloud, on comprend pourquoi la plupart des secteurs, et la majorité des PME, ne se préoccupent plus de gérer des salles de serveurs réfrigérées. - Rafael Bloom**

Accès sécurisé aux données de santé des patients

La santé est un autre secteur où la sécurité des données est plus importante que jamais. Les informations sur les patients sont encore plus exposées au risque de vol, avec des brèches exposant 45,67 millions de dossiers de patients en 2021, le plus grand total annuel depuis 2015[2]. En matière de stockage et de sauvegarde des données, les données des patients sont les informations médicales critiques et complètes qui permettent aux prestataires de soins de santé de traiter leurs patients en toute sécurité.

Il peut s'agir des fichiers du dossier médical électronique (DME) du patient contenant les antécédents médicaux, les tests, les photographies et les images radiographiques comme des fichiers administratifs comprenant les dossiers de paie, l'assurance des patients et les comptes fournisseurs. Confrontés à une main-d'œuvre mobile croissante et à un marché mondial des soins de santé en plein bouleversement et en pleine transformation, il n'est pas étonnant que les prestataires de soins de santé d'aujourd'hui se préoccupent de la sécurité des données.

> **Les rançongiciels (ransomware), en particulier, étant un secteur en pleine croissance, toute organisation qui traite des données sensibles doit réfléchir à la manière de fonctionner dans des conditions de contrainte extrême. - Rafael Bloom**

En outre, l'incapacité à anticiper les risques et à respecter des mandats stricts tels que la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) ou la loi sur les technologies de l'information en matière de santé économique et clinique (HITECH) pourrait entraîner une violation coûteuse des données de santé, susceptible d'ébranler davantage la confiance des patients, des partenaires ou les organismes de réglementation.

Avec des solutions telles que la gamme de clés USB chiffrées Kingston IronKey, les organismes de santé peuvent définir des politiques pour les mots de passe, l'utilisation des applications, la récupération, entre autres. Et ce, à partir d'une console unique, que ce soit pour quelques clés ou des milliers d'entre elles. Les travailleurs mobiles et de première ligne peuvent être habilités à soutenir davantage de patients, grâce à des solutions conviviales qui suppriment la nécessité pour les employés d'installer des pilotes ou d'autres logiciels, afin d'accéder en toute sécurité à leurs données stockées. Et les utilisateurs et les administrateurs peuvent facilement et rapidement verrouiller les données, où qu'elles aillent.

La clé USB dans un avenir de stockage cloud

> **Le stockage de données dans le cloud est le présent et l'avenir. Je persiste à dire que la sécurisation physique des données, par exemple en utilisant des clés USB chiffrées, est la plus sûre. Les utilisateurs n'ont pas le contrôle total de ce qui se passe dans le cloud. À l'inverse, nous avons le contrôle sur les données contenues dans les clés USB chiffrées, que nous sécurisons et stockons nous-mêmes. En dehors de nous, personne n'a accès à ces supports.**
>
> **- Tomasz Surdyk**

Maintenant que les avantages des clés USB sont CLAIRS, quel est exactement leur rôle dans un avenir de stockage cloud ?

Il y a dix ans, les clés USB étaient très demandées en tant qu'outil principal pour stocker et transférer des données de manière pratique. Cependant, avec l'impact des nouveaux modèles de travail hybrides et des équipes de plus en plus dispersées, le cloud permet désormais d'accéder rapidement et facilement aux informations stockées via de nombreux appareils. Les clés USB étaient autrefois immensément populaires en raison du confort unique qu'elles offraient pour le transport des fichiers. Mais aujourd'hui, les services de stockage cloud offrent une plus grande facilité de portabilité des fichiers.

Cela dit, le stockage cloud présente encore de nombreuses limites. Une connectivité réseau est nécessaire, ce qui non seulement dicte comment et quand les fichiers peuvent être sauvegardés ou transférés, mais ajoute un problème de sécurité supplémentaire. Lorsqu'une entreprise impose l'utilisation du cloud, elle n'est pas nécessairement en mesure de contrôler l'endroit depuis lequel les données sont accessibles. Par conséquent, le simple fait d'accéder à un VPN en utilisant une connexion Wi-Fi personnelle ou publique ouvre le risque d'être piraté. En outre, les services cloud sont très attrayants pour les pirates ; la majorité de tous les logiciels malveillants (61 %) sont désormais diffusés via des applications cloud[3].

> **Il peut s'avérer judicieux d'envisager ce qui se passerait en cas d'indisponibilité du cloud, les scénarios où les données doivent être disponibles à 100 % et lorsque le stockage à long terme pourrait créer une vulnérabilité.**
>
> **- David Clarke**

La clé USB dans un avenir de stockage cloud

Le chiffrement USB, quant à lui, peut se faire soit par le biais du matériel de la clé USB, soit par un logiciel. Le chiffrement centré sur le matériel et sans logiciel est le moyen le plus efficace de se protéger contre les cyberattaques. Il s'agit d'une excellente solution, non compliquée, pour se protéger contre les violations de données et pouvant répondre à des normes de conformité strictes. En effet, elle offre une sécurité ultime en matière de protection des données, permettant aux organisations de gérer les menaces et de réduire les risques en toute confiance.

Comme elles sont autonomes, les clés USB à chiffrement matériel ne nécessitent pas d'élément logiciel sur l'ordinateur hôte. L'absence de vulnérabilité logicielle élimine également la possibilité d'attaques par force brute, par reniflage et par hachage de mémoire. Les clés USB chiffrées par logiciel présentent également le risque que tout utilisateur puisse désactiver le chiffrement en les formatant sur n'importe quel ordinateur et en les utilisant pour stocker des données sensibles de manière non protégée.

Les clés USB à chiffrement matériel offrent également un moyen physique exceptionnel de sécuriser les données. Elles permettent d'établir des critères d'accès aux informations par un utilisateur ou un administrateur, et peuvent s'intégrer aux solutions pour terminal locales existantes. Cela en fait une solution pratique et rentable pour de nombreux scénarios où le stockage cloud ne fonctionnerait pas, ou ne serait pas une solution aussi efficace. Cela peut être le cas lorsque les données doivent être stockées à partir d'appareils qui ne sont pas en réseau, qui doivent être privées ou auxquelles il faut accéder lorsqu'on est hors ligne.

> **Si, pour une organisation, nous considérons que les données sont « chaudes » ou « froides » en fonction de leur niveau d'utilité au quotidien, il peut être plus efficace de placer les données « froides » dans le cloud et de s'appuyer davantage sur un stockage USB localisé pour les données « chaudes ». Surtout si la continuité des opérations et les hautes performances sont essentielles pour l'organisation, ou dans le cas d'une fonction ou un processus critique en particulier.**
>
> - Rafael Bloom

Synthèse

Si nous ne pouvons pas prédire l'arrivée des innovations futures, ce que nous pouvons offrir, c'est un portefeuille primé de clés USB offrant une gamme dynamique de solutions chiffrées pour tous les niveaux d'exigences de protection des données mobiles. Qu'il s'agisse des clés USB dotées d'un clavier alphanumérique pour une protection par code PIN facile à utiliser, de la certification FIPS 140-2 Niveau 3 pour le plus haut niveau de chiffrement avec protections anti-fraude ou de la technologie SuperSpeed USB 3.1 pour une sécurité optimale, les produits Kingston IronKey sont conçus pour relever vos défis en matière de données. Nos clés USB sont des solutions puissantes et efficaces pour le transport et le stockage des données mobiles.

Notre équipe d'experts spécialisés est prête à vous accompagner à chaque étape de projet de stockage des données. Et elle est à vos côtés pour vous aider à trouver la solution de stockage qui répond à vos besoins, en toute confiance.

Nous avons les compétences et les capacités techniques nécessaires pour vous aider à assurer la sécurité des informations confidentielles et à vous conformer aux nouvelles réglementations. Et ce, qu'il s'agisse d'élaborer un plan USB chiffré, d'identifier les meilleures clés USB pour votre entreprise ou d'établir et appliquer des politiques de sécurité. Par le biais d'un service hautement personnalisé, nous nous engageons à fournir des produits qui soutiennent vos priorités de stockage des données et vous permettent de suivre le rythme sans précédent auquel le monde de l'entreprise évolue.

À propos de Kingston

Kingston, avec ses 35 années d'expérience, dispose du savoir pour identifier vos défis en matière de données mobiles et vous aider à les relever afin que vos collaborateurs puissent travailler sans compromettre votre organisation.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou