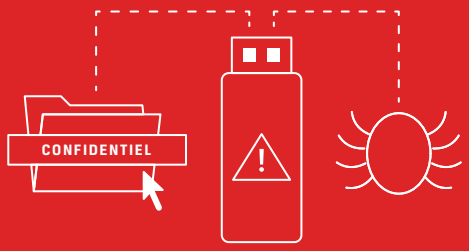
Alerte USB :
Verrouiller vos données



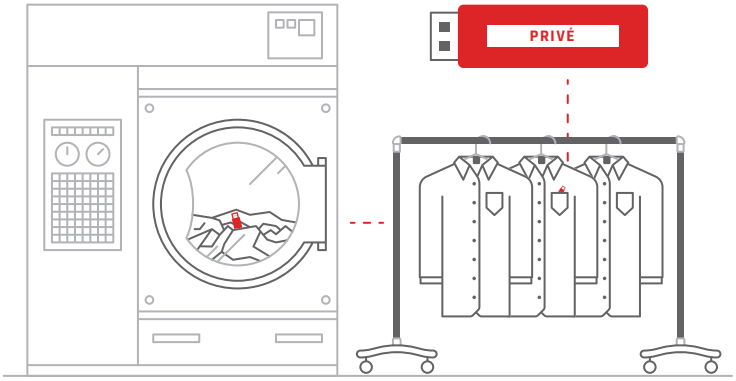
Les clés USB ont révolutionné les transferts de données, mais elles ont aussi introduit des risques de sécurité importants. Grâce à leur portabilité extrême, les clés USB surgissent partout, depuis les poches de veste aux emplacements de parking, et exposent les données à des risques graves. Comment un service informatique peut-il traiter de tels risques sans interdire totalement l'usage des clés USB et perdre tous leurs avantages ?

Quelle est la pire situation ?

Les clés USB peuvent présenter des risques de nombreuses façons :

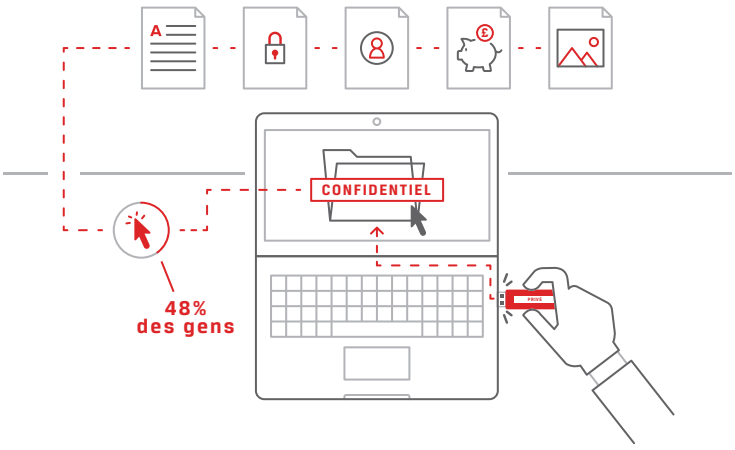
PERDUES

Les services du nettoyage à sec retrouvent chaque année 22 000 clés USB[1]



TROUVÉES

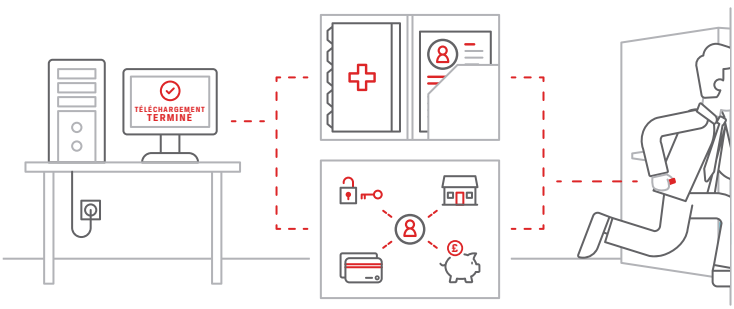
48% des gens qui trouvent une clé USB la connecte et clique au moins sur un fichier[4]



VOLÉES

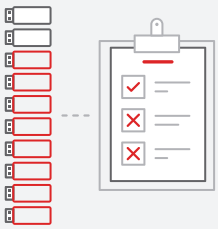
Une clé USB contenant des données sensibles sur **des patients** a disparu d'un service d'urgence hospitalier[2]

Un employé mécontent a utilisé une clé USB pour voler les données bancaires de **~30 000 personnes**[3]



Comment les professionnels de l'informatique gèrent-ils la sécurité des clés USB ?

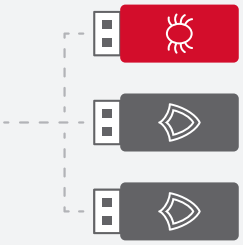
Un sondage Spiceworks ciblant des professionnels de l'informatique a conclu que la plupart des entreprises tiennent compte de la sécurité des clés USB, mais nombre d'entre elles n'ont pas de solution réellement aboutie[5].



80% des entreprises ont mis en place des politiques de sécurité USB

La politique la plus courante : restreindre l'usage des clés USB à des employés ou des services spécifiques.

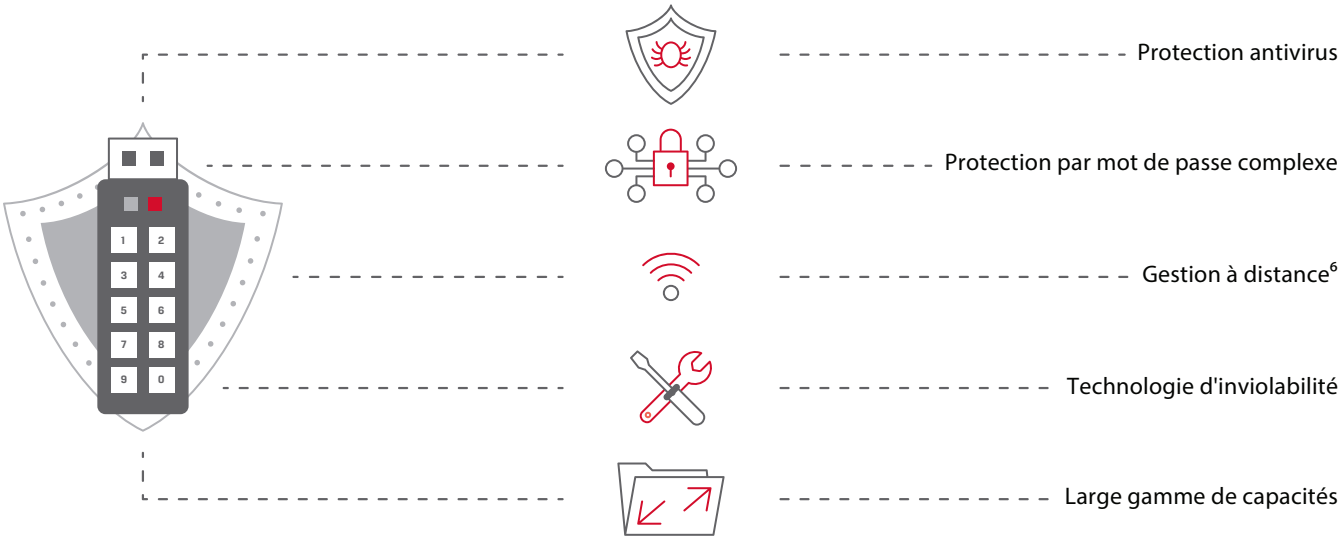
< 20% des entreprises qui utilisent une politique de clés USB imposent l'utilisation de clés USB cryptées



Pourtant, **un tiers** des répondants ont connu une menace ou une violation de la sécurité causée par une clé USB au cours de l'année écoulée.

Les clés USB cryptées ne dévoilent jamais leurs secrets.

Les clés USB cryptées peuvent être de puissants outils pour combler cet écart de sécurité bien trop fréquent. Elles contribuent à renforcer la sécurité et la conformité avec :



Protégez-vous avez Kingston.

Les clés USB cryptées IronKey de Kingston sont conçues pour protéger les données les plus sensibles en appliquant les règles et protocoles de sécurité les plus rigoureux dans tous les environnements, allant des administrations publiques, aux fournisseurs de services médicaux et institutions financières.

Sources :
1. Steve Bush, "22,000 clés USB sont récupérées par les services du nettoyage à sec ," ElectronicsWeekly.com, 14 janvier 2016. www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/
2. Taya Flores, "L'hôpital Arnett dans l'Indiana signale qu'il manque des informations sur un patient," JConline, 5 janvier 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/
3. Tom Brant, "Rapport: Les employés de la FDIC ont causé des violations répétées de la sécurité," PC Magazine, 15 juillet 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches
4. Elie Bursztein, "Les inquiétudes concernant la sécurité des clés USB sont réelles: 48% des personnes utilisent les clés USB trouvées dans les parkings," Elie.net, avril 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
5. Sondage Spiceworks sur 300 décideurs informatiques aux États-Unis, Canada, Europe, au nom de Kingston, février 2017.
6. Pour fournir des solutions de gestion pour ses clés USB cryptées, Kingston Digital s'est allié à DataLocker. www.kingston.com/us/usb/encrypted_security/management-solutions