

# Panique portable

## L'évolution de l'insécurité quant aux périphériques USB

À mesure que les périphériques USB se sont imposés en tant que supports de stockage utiles, ils sont également devenus un cauchemar pour les entreprises en termes de sécurité. Or, l'utilisation des périphériques USB doit être encouragée en ces temps économiques difficiles pour contribuer à la réduction des coûts de fonctionnement. Affrontez la menace associée aux supports amovibles, contrôlez le flux des données entrantes et sortantes de vos postes de travail et permettez une utilisation gérée de ces outils de productivité en appliquant des règles d'utilisation des périphériques amovibles.

### Présentation

Après quasiment 15 ans de développement, les périphériques de stockage USB se présentent à peu près sous toutes les formes et dans toutes les capacités imaginables, depuis les clés mémoire de 1 gigaoctet (Go) déguisées en sushis jusqu'aux disques durs externes standard offrant des capacités jusqu'à 6 téraoctets (To). Autrefois simple curiosité, ces périphériques sont désormais aussi répandus que la souris et le clavier. Les analystes prévoient que d'ici 2010, 2,8 milliards de périphériques USB auront été commercialisés sur le marché.

Malheureusement, à mesure que les périphériques USB ont évolué en supports de stockage utiles, ils sont également devenus un cauchemar pour les entreprises en termes de sécurité. Le développement de cette technologie a toujours été axé sur la convivialité, la connectivité, le faible coût et les performances, sans grande considération pour la [sécurité des connexions USB](#). Les utilisateurs professionnels ne sont pas les seuls à apprécier

les avantages apportés par les périphériques USB actuels. Les cybercriminels et voleurs de données utilisent de plus en plus les supports amovibles pour introduire des programmes malveillants et dérober des informations sur les ordinateurs. Il suffit de parcourir les journaux régulièrement pour s'apercevoir que des périphériques USB sont très souvent impliqués dans les brèches de sécurité des données les plus médiatisées du moment, via le chargement de programmes malveillants qui provoquent des brèches dans le réseau d'entreprise dorsal, en facilitant la suppression délibérée et furtive de données copiées, ou tout simplement en favorisant la perte de données à cause d'un périphérique non crypté qui se retrouve égaré.

## Perspective historique

N'aurions-nous pas oublié quelque chose ? Lorsque les ingénieurs ont commencé à travailler sur le format du bus série universel (USB) en 1994, leur objectif était de développer une norme unique, économe en énergie et capable de remplacer le nombre croissant de raccordements de périphériques qui encombraient l'arrière de nos PC. La sécurité était bien loin de leurs préoccupations. À l'époque, la plupart des professionnels de l'informatique n'y pensaient guère.

Depuis l'instauration de la norme USB 1.0 jusqu'au déploiement des iPod et clés mémoire USB, en passant par le développement de périphériques de stockage de très grande capacité, l'innovation a toujours porté sur la vitesse, la capacité et la commodité. Avec la version la plus récente de la norme USB 3.0, nous obtenons désormais

des taux de transfert des données de l'ordre de 5 Gbit/s, soit un débit dix fois supérieur à la précédente itération. Dans le même temps, les [lecteurs Flash USB](#) offriront bientôt une capacité de 128 Go, les disques durs externes montant jusqu'à 6 To. Ces avancées changent la donne dans le monde des entreprises, qui voit en ces périphériques d'incroyables accélérateurs de productivité.

Toutefois, à l'heure où le déploiement des premiers périphériques USB 3.0 approche, tous ces avantages pourraient bien être perdus, simplement parce que les temps ont changé en matière de sécurité, mais pas la norme USB.

La sécurité est toujours aussi négligée qu'au premier jour où la norme USB a été conçue.

Type de fichiers	Taille type (Ko)	Nombre type de fichiers par :		
		Clé USB de 512 Mo	Clé USB de 2 Go	Clé USB de 32 Go
Texte / message électronique	15	34,560	139,500	1,984,700
Document	100	5,185	20,920	297,750
Feuille de calcul	1485	350	1,410	20,050
JPG de 10 mégapixels	2250	230	930	13,210

Tableau 1. Capacité de stockage des périphériques USB

## Panique portable - L'évolution de l'insécurité quant aux périphériques USB

- 1994 — Début d'élaboration de la norme USB.
- 1995 — Création de l'USB Implementers Forum (USB-IF), rapidement suivie par le développement du premier silicium USB par Intel.
- 1996 — Sortie de la norme USB 1.0 (basse vitesse) initiale, avec un taux de transfert des données spécifié de 1,5 Mbit/s (187,5 Ko/s).
- 1997 — Plus de 500 produits USB en développement.
- 1998 — L'Apple iMac devient le premier ordinateur grand public à remplacer les connexions périphériques traditionnelles par des ports USB exclusivement. Sortie de la norme USB 1.1 (pleine vitesse) ; c'est la première version à bénéficier d'une adoption à grande échelle, avec un débit spécifié de 12 Mbit/s (1,5 Mo/s), soit plus de dix fois supérieur aux communications en série.
- 2000 — La connectivité USB gagne les systèmes de stockage. Le premier lecteur Flash USB, fabriqué par l'entreprise Trek basée à Singapour et commercialisé par l'intermédiaire d'IBM, est introduit avec une capacité de stockage de 8 Mo, soit cinq fois plus qu'une disquette à l'époque. La norme USB 2.0 (grande vitesse) voit le jour et bénéficie d'un attrait considérable auprès d'un grand nombre de fabricants de matériel informatique. Le débit des périphériques USB atteint 480 Mbit/s (60 Mo/s), soit quarante fois plus que la norme USB 1.1 établie.
- 2001 — Sortie de l'Apple iPod, intégrant la connectivité FireWire 400, avec une capacité de stockage de 5 Go.
- 2003 — Adoption par Apple de la technologie USB pour la synchronisation, avant d'offrir une connectivité opérationnelle totale via FireWire ou USB.
- 2005 — Transition d'Apple vers la norme USB, ne conservant la connectivité FireWire que pour le chargement. On estime à 1,5 milliard le nombre de périphériques USB commercialisés.
- 2006 — Développement par U3 d'une méthode d'exécution automatique d'applications à partir de lecteurs Flash USB, permettant la création d'environnements de travail portables. Les utilisateurs peuvent désormais travailler avec des applications telles que des navigateurs web sur le périphérique U3 ; toutes les informations traditionnelles (telles que les personnalisations, les paramètres, l'historique du navigateur, etc.) sont stockées avec l'application sur le périphérique USB, éliminant du PC toutes les traces d'utilisation de cette application. La technologie d'U3 facilite également la création d'un programme à exécution automatique ou d'un périphérique USB amorçable.
- 2008 — Sortie de la norme USB 3.0 (très grande vitesse), avec un taux de transfert des données plus de dix fois supérieur à celui de la norme USB 2.0. La norme USB 3.0 offre un débit de 5 Gbit/s (625 Mo/s) et la capacité des lecteurs Flash USB atteindra bientôt 128 Go. Dans le même temps, la capacité des disques durs offrant une connectivité USB disponibles dans le commerce s'élève désormais à 6 To.

### Étude des risques

En deux mots, la convivialité, la prédominance du format et l'insécurité inhérente du format USB en font un rêve pour la plupart des escrocs et cybercriminels. Examinons trois des principaux risques et quelques-uns des outils et techniques utilisés par les pirates qui entrent en compte dans ces risques.

### Propagation des programmes malveillants

Les entreprises spécialisées dans la sécurité signalent une augmentation des [programmes malveillants](#) qui se propagent via les périphériques USB et autres supports amovibles. En fait, c'est l'apparition d'un ver de ce type qui a conduit l'armée américaine à bannir l'utilisation des périphériques USB fin 2008. Les programmes malveillants, tels que le ver SillyFDC qui a frappé l'armée américaine, se copient sur tous les lecteurs raccordés aux machines infectées. Ainsi, un périphérique USB qui est connecté à une machine infectée devient infecté à son tour puis, lorsqu'il est raccordé à une autre machine, celle-ci se met également à infecter les autres périphériques USB qui y sont connectés. Cette méthode de propagation des programmes malveillants à la façon d'un ver se copie toute seule sur tous les lecteurs, partages, supports amovibles et dossiers de fichiers d'applications logicielles P2P disponibles. Les méthodes les plus populaires utilisées actuellement sont les suivantes.

#### » La méthode simple de copie de fichiers

Elle s'appuie sur l'ingénierie sociale pour inciter l'utilisateur à cliquer sur une icône d'application afin de lancer cette dernière, qui se copie ensuite sur tous les lecteurs disponibles.

#### » La méthode de modification AutoRun.inf

Elle modifie ou crée un fichier AutoRun.inf sur tous les lecteurs, partages et supports amovibles disponibles. Lorsqu'une clé USB infectée est ensuite insérée dans un autre ordinateur, le logiciel malveillant s'exécute automatiquement sans aucune intervention de l'utilisateur.

### Perte de données

L'utilisation répandue des périphériques USB au sein d'une entreprise peut l'exposer à une [perte de données](#) sur deux fronts majeurs : le vol de données en les copiant sur un périphérique, et le vol de données en les copiant à partir d'un périphérique.

Un troisième risque est la simple perte de données accidentelle due à une erreur humaine. Une méthode simple pour minimiser ce risque consiste à [crypter les périphériques USB](#) de sorte que les données stockées dessus ne puissent pas être dévoilées de manière inadéquate..

Dans le premier cas, Pod-Slurp a été l'un des premiers programmes à mettre en évidence les problèmes d'insécurité des périphériques USB. Le simple fait de connecter un périphérique USB contenant Slurp sur l'ordinateur d'une victime lançait automatiquement les scripts permettant de copier chaque document contenu dans le répertoire Mes documents du PC hôte sur la clé USB. Il était possible de modifier le script pour cibler les feuilles de calcul, les fichiers PowerPoint ou tout autre type de fichier spécifique. De plus, il pouvait facilement être modifié pour envoyer les fichiers par courrier électronique ou FTP au lieu de les copier sur le périphérique USB.

Le second scénario peut pour sa part s'avérer particulièrement dangereux si un utilisateur a transféré en toute innocence du contenu sensible sur une clé USB et décide de l'utiliser sur des ordinateurs publics non sécurisés, tels que les systèmes des centres d'affaires des aéroports, des cybercafés, des hôtels et des bibliothèques.

Lors d'une démonstration en 2005 à l'occasion d'une conférence privée sur la sécurité, l'auteur a présenté un programme qu'il avait conçu appelé "USB-Puke", qui se contentait simplement de créer discrètement une image "dd" (copie bit à bit) de n'importe quelle clé USB qui était insérée dans l'ordinateur portable de l'auteur. L'utilisation de la commande "dd" permettait à l'auteur non seulement d'obtenir des copies de tous les fichiers existants sur la clé USB de l'utilisateur, mais aussi de récupérer des fichiers précédemment supprimés de la clé USB de l'utilisateur qui restaient présents malgré tout dans l'espace non alloué de la clé. La démonstration a ouvert les yeux des participants et a été considérée comme un outil efficace pour éveiller les consciences. Cependant, en raison des risques d'abus, l'auteur n'a jamais rendu le programme public. Depuis, d'autres outils innombrables sont apparus un peu partout avec des attributs similaires et des fonctionnalités encore plus avancées.

Par exemple, HTTP RAT ouvre automatiquement un canal retour via HTTP jusqu'à l'internet public qui permet à une personne à distance de se connecter tout simplement à un PC compromis via Firefox. L'utilisateur à distance peut ensuite parcourir l'ensemble des lecteurs réseau disponibles ou connectés pour choisir quels fichiers dérober à distance via la connexion HTTP. Quant à USB Switch Blade, il extrait tous les hachages de mots

de passe à l'aide de `pwdump` à partir de la machine cible pour les utiliser ultérieurement dans le piratage de mots de passe. Il suffit de se présenter devant la machine de la victime, d'insérer le périphérique USB et de patienter seulement 60 secondes (voire moins), pour repartir tranquillement avec tous les hachages de mots de passe. Les autres variantes incluent la possibilité de récupérer tout l'historique du navigateur en vue d'extraire ultérieurement les références d'identité de l'utilisateur sur des sites financiers, ses identifiants de connexion à MSN Messenger, etc.

### Piratage anonyme

Une fonctionnalité extrêmement utile des [lecteurs USB](#) est leur capacité à agir comme un "PC sur une clé mémoire", via l'utilisation de certains utilitaires de virtualisation et de plate-forme tels que BartPE/PeToUSB, UBCD4, UNetBootin et MojoPac. Cela permet également aux utilisateurs malintentionnés de répliquer tout leur laboratoire de piratage de Windows sur un périphérique USB et de l'exécuter sur pratiquement n'importe quel PC disposant d'un port USB disponible. Lorsque l'utilisateur malintentionné en a terminé, il se contente de retirer le périphérique USB et part sans laisser de trace.

De la même manière, des organisations terroristes ont adopté l'utilisation de logiciels de communications cryptées sur une clé USB. Un terroriste peut ainsi entrer incognito dans n'importe quel cybercafé, brancher un périphérique USB contenant un logiciel tel que Mujahedeen Secrets 2, envoyer des messages électroniques, des fichiers ou avoir des communications par chat à l'aide d'un cryptage de catégorie militaire, puis simplement débrancher le périphérique, ne laissant aucune trace de son utilisation sur le PC du cybercafé.

## USB, mais pas seulement : les risques liés aux autres supports amovibles

Si ce livre blanc met l'accent sur les périphériques USB, il faut comprendre qu'ils ne constituent que le sommet de l'iceberg. La majorité des risques évoqués dans cet article ne se limite pas simplement à la norme USB, mais s'étend à toutes les formes de supports amovibles utilisés aujourd'hui, dont les lecteurs de CD, DVD et Blu-ray, ainsi que les périphériques raccordés via FireWire et eSATA.

### Supports amovibles de type CD, DVD et Blu-ray

Bon nombre des outils de test de pénétration du réseau sur CD populaires actuellement qui sont utilisés par des personnes animées de bonnes intentions peuvent malheureusement aussi être utilisés par une personne malintentionnée et non autorisée aux intentions néfastes. Il peut s'agir par exemple d'introduire un programme malveillant indétectable au cœur du réseau, d'installer des chevaux de Troie ou des enregistreurs de frappe, et de créer des portes dérobées sur le réseau pour offrir aux personnes non autorisées un chemin d'accès direct à travers les

défenses réseau jusqu'au PC compromis. En deux mots, vous prenez de grands risques lorsque vous ne contrôlez pas précisément **qui** peut exécuter **quelles** applications à partir de vos lecteurs de supports amovibles. Il est difficile d'imaginer en quoi permettre l'utilisation non contrôlée d'un lecteur de CD/DVD peut être positif lorsqu'une personne non autorisée lance un disque contenant un élément tel que l'une des boîtes à outils Astalavista.

Le problème n'est pas seulement qu'un lecteur de CD, DVD ou Blu-ray peut être utilisé comme point de départ d'une pénétration sur le réseau. Le volume même d'informations qui peut être extrait d'un réseau pour être mis sur un support amovible au moyen d'une copie non autorisée est en hausse. Beaucoup de personnes ne s'imaginent pas la quantité d'informations qui peut être copiée très rapidement sur un support amovible avant que la personne non autorisée ne reparte tranquillement en leur possession. Le tableau 2 apporte quelques indications.

Une méthode recommandée pour empêcher l'accès non autorisé aux données stockées sur un support amovible consiste à [crypter les CD et DVD](#).

Type de fichiers	Taille type (Ko)	Nombre type de fichiers par :		
		Disque CD	Disque DVD (simple face, simple couche)	Disque Blu-ray (double couche)
Texte/message électronique	15	46,500	297,000	3,200,000
Document	100	6,980	44,500	480,000
Feuille de calcul	1485	470	3,000	32,320
JPG de 10 mégapixels	2250	310	1,975	21,300

Tableau 2. Capacité de stockage des disques CD, DVD et Blu-ray

### Connectivité FireWire : une menace encore plus grande ?

Les menaces liées à FireWire méritent d'être mentionnées dans cet article, car la menace potentielle peut, à certains égards, être encore plus grande que celle posée par les périphériques USB. Citons par exemple la possibilité d'écrire directement dans la mémoire via FireWire, comme l'a montré Adam Boileau, chercheur en sécurité néo-zélandais pour [security-assessment.com](http://security-assessment.com), lors de la conférence Ruxcon en 2006.

En mars 2008, il a publié un outil qui permet de prendre le contrôle de n'importe quel PC Windows, simplement en raccordant un PC basé sur Linux au port FireWire du PC Windows et en exécutant une unique commande. La commande en question écrase littéralement le code de protection des mots de passe au sein de la mémoire Windows, puis le contourne complètement. Vous trouverez une explication détaillée du mode de fonctionnement de l'attaque sur le site [www.pcadvisor.co.uk](http://www.pcadvisor.co.uk).

### Récolter des gains de productivité sans les risques

La définition traditionnelle d'un "poste de travail" d'entreprise est clairement en train d'évoluer. Pour des millions d'employés, les supports portables représentent la prochaine génération de postes de travail, après les PC et les ordinateurs portables. En raison de cette évolution, la sécurité des postes de travail d'entreprise doit également s'accroître pour répondre à une préoccupation de plus en plus grande. En définitive, cette évolution des postes de travail d'entreprise expose un nouveau vecteur de menace que les professionnels de l'informatique doivent traiter et sécuriser.

Utiliser de la résine époxy pour [boucher les ports USB](#) n'est pas la solution. De toute évidence, les gains de productivité amenés par les nombreux périphériques USB disponibles aujourd'hui l'emportent sur le réflexe primaire consistant à bannir explicitement et définitivement l'utilisation de ces périphériques USB. En fait, l'utilisation des périphériques USB doit être encouragée, notamment dans l'environnement économique actuel, pour contribuer à réduire les coûts de fonctionnement, voire à sauver des emplois.

Pour remporter la bataille contre les programmes malveillants mobiles et le vol d'informations, les entreprises doivent développer des politiques claires et approfondies concernant l'utilisation des supports et périphériques amovibles au sein de leur organisation. Elles doivent également déployer des solutions proactives, telles que la suite de sécurité des postes de travail de Lumension® (anciennement suite Sanctuary), pour prendre en charge ces politiques. Alors que la guerre de la sécurité dans l'entreprise continuera d'être longue et éprouvante, les entreprises peuvent remporter un avantage décisif en adoptant une approche offensive pour protéger leurs postes de travail, quelle que soit l'ampleur avec laquelle ils évoluent. Après tout, la notion de "PC sur une clé mémoire" doit améliorer les processus métiers, et non les entraver.

### Suite de sécurité des postes de travail de Lumension

La suite de sécurité des postes de travail de Lumension, anciennement suite Sanctuary, combine les solutions [Lumension® Data Protection](#) et [Lumension® Endpoint Protection](#) pour protéger les postes de travail contre :

- la perte et le vol de données ;
- les applications et périphériques non autorisés ;
- les menaces liées aux programmes malveillants.

Elle assure cette protection sans s'appuyer sur des listes de signatures réactives.

En employant une approche de liste blanche, Lumension permet aux seules applications autorisées de s'exécuter et aux seuls périphériques admis de se connecter à un réseau, ordinateur portable ou PC, ce qui facilite la gestion des systèmes et de la sécurité, tout en offrant la flexibilité nécessaire à l'entreprise.

[Apprenez comment Lumension Data Protection met en vigueur des règles de contrôle des périphériques USB.](#)

[Apprenez comment Lumension Endpoint Protection met en vigueur des règles de contrôle des applications.](#)

### Contre les menaces liées aux supports amovibles

La suite de sécurité des postes de travail de Lumension applique des règles d'utilisation concernant les périphériques amovibles (tels que les lecteurs Flash USB) et d'autres supports amovibles (tels que les CD/DVD) pour contrôler le flux des données entrantes et sortantes de vos postes de travail.

Les applications et les périphériques amovibles sont validés au moment de leur utilisation au sein de l'entreprise. Les applications ou périphériques qui ne sont pas autorisés ne peuvent tout simplement pas s'exécuter.

Grâce à une console centrale, les règles de contrôle des applications et des périphériques peuvent être rapidement établies et appliquées en deux étapes simples : l'identification et l'attribution. La suite de sécurité des postes de travail de Lumension permet aux entreprises de développer des règles d'utilisation granulaires, en travaillant avec les périphériques et les applications au lieu de simplement les activer ou les désactiver. Les règles sont gérées par utilisateur ou groupe d'utilisateurs, ainsi que par ordinateur. Pour les périphériques, les règles sont appliquées en fonction du type de fichier, du volume quotidien, de l'heure de la journée, et de nombreux autres critères. En reliant les règles sur les applications et périphériques aux informations relatives aux utilisateurs et aux groupes d'utilisateurs qui sont stockées dans Microsoft® Windows® Active Directory™ ou Novell® eDirectory™, Lumension permet d'associer immédiatement des groupes d'utilisateurs à des périphériques et applications à la volée, ce qui simplifie considérablement la gestion des ressources des périphériques et applications des postes de travail.

La suite de sécurité des postes de travail de Lumension peut en outre crypter les supports amovibles afin de pouvoir les transporter et les utiliser en toute sécurité sans crainte d'exposer des données confidentielles à des utilisateurs non autorisés. Les utilisateurs peuvent accéder à leurs données cryptées même sur les ordinateurs n'exécutant pas le logiciel client. Les schémas de cryptage centralisés et décentralisés permettent à l'administrateur de [crypter les supports amovibles](#) de manière centralisée ou de laisser les utilisateurs les crypter eux-mêmes et, plus important encore, de contrôler l'utilisation de ces supports cryptés.

Grâce à la flexibilité inégalée de Lumension, les administrateurs peuvent permettre aux utilisateurs de confiance d'autoriser leurs propres applications. Cette option offre le compromis idéal : flexibilité pour les utilisateurs et contrôle pour les administrateurs, via les notifications d'activité. Les capacités d'audit et de génération de rapports permettent aux administrateurs de suivre précisément à quel moment les périphériques et applications sont utilisés, par qui et comment. Ils peuvent également voir les tentatives d'utilisation de périphériques ou applications non autorisés et en effectuer le suivi.

Lumension combine les capacités éprouvées de ses modules de [contrôle des applications](#) et [des périphériques](#) offrant aux entreprises la solution la plus complète pour la gestion de la sécurité des postes de travail... tout ceci à partir d'une seule et même console. La suite de sécurité des postes de travail de Lumension supprime le risque de fuite des données, de programmes malveillants et de logiciels espions, améliore la sécurité informatique et la largeur de bande du réseau, réduit l'effort et le coût associés au support des technologies des postes de travail et assure la conformité aux réglementations. La solution :

- » empêche la fuite des données via les supports amovibles, les programmes malveillants ou les logiciels espions ;
- » assure une protection contre les programmes malveillants, les virus et les logiciels espions ;
- » protège contre les menaces non répertoriées ;
- » contrôle la prolifération des applications et périphériques indésirables ;
- » assure et prouve la conformité aux réglementations régissant le respect de la vie privée et la responsabilité ;
- » maximise les avantages des nouvelles technologies et minimise le risque.

### À propos de Lumension

Lumension, leader mondial de la sécurité des postes de travail opérationnels, développe, intègre et commercialise des solutions logicielles de sécurité qui permettent aux entreprises de protéger leurs informations cruciales et de gérer le risque sur les ressources des réseaux et des postes de travail.

Lumension permet à plus de 5 100 clients dans le monde d'atteindre une sécurité optimale et de connaître la réussite informatique en leur apportant un portefeuille de solutions éprouvées et maintes fois primées incluant des offres de gestion des vulnérabilités, de protection des postes de travail, de protection des données, de génération de rapports et de conformité. Lumension est réputé pour offrir un support aux clients et des services de niveau international 24 h/24, 365 jours par an.

Lumension a établi son siège social à Scottsdale, en Arizona, et possède des bureaux dans le monde entier, notamment en Virginie, en Floride, au Luxembourg, au Royaume-Uni, en Espagne, en Australie, en Inde, à Hong Kong et à Singapour. Lumension : l'informatique sécurisée, le succès optimisé. Pour plus d'informations, visitez le site de Lumension: [www.lumension.com](http://www.lumension.com).



#### Siège international

15580 N. Greenway-Hayden Loop, Suite 100 Scottsdale,  
AZ 85260, États-Unis  
Téléphone : +1.888.725.7828  
Fax : +1.480.970.6323

[www.lumension.com](http://www.lumension.com)

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

#### Documents annexes



Vidéo : Histoire d'une réussite. L'Armée du Salut préserve l'intégrité des données et sa renommée internationale



Vidéo : Sujet d'actualité  
Les périphériques mobiles sur le lieu de travail : trouver le bon équilibre

Livre blanc : La nouvelle économie voit émerger de nouvelles menaces provenant de l'intérieur

Émission sur le web : Protéger les informations de l'entreprise : pourquoi, comment et que faire dans différentes situations

#### Étapes essentielles pour protéger vos informations vitales

Quantifiez le risque encouru avec les périphériques USB non gérés

grâce à Lumension®  
Device Scanner Pro



Émission sur le web : Données en péril : protégez votre entreprise avec Lumension® Data Protection

Livre blanc : Prendre le contrôle de vos données : protégez les informations de votre entreprise contre la perte ou le vol

Protégez vos informations vitales dès aujourd'hui

Appliquez des règles d'utilisation des applications et des périphériques USB

avec la suite de sécurité des postes de travail de Lumension®

