Article technique

# Comment mettre des disques au rebut de façon sûre, rapide et simple

## Introduction

Comme les disques durs et les disques SSD stockent de vastes volumes de données hautement sensibles, les centres de données doivent trouver une solution sécurisée pour les mettre au rebut lorsqu'ils arrivent en fin de vie. Or, les méthodes les plus couramment utilisées, qui consistent à effacer les données puis à détruire les disques (soit en interne, soit par le biais d'un prestataire externe), sont coûteuses et fastidieuses, et ne garantissent pas systématiquement une protection complète des données. Ce document explique comment la technologie d'autochiffrement couplée aux fonctionnalités de Seagate Instant Secure Erase (ISE) peut vous aider à réduire sensiblement les temps, coûts et efforts liés à la mise au rebut de disques durs tout en assurant une sécurité optimale des données.

## Comment mettre des disques au rebut tout en protégeant les données

La durée de vie des disques durs et disques SSD varie de trois à cinq ans, non parce qu'ils tombent en panne, mais simplement parce que les avancées technologiques les rendent obsolètes. Les entreprises se trouvent alors face à un problème majeur. Comment peuvent-elles mettre au rebut leurs disques d'entreprise de façon sécurisée, rapide et peu coûteuse tout en protégeant les données confidentielles qu'ils contiennent ?

La protection des données est un sujet crucial. Les analystes du secteur estiment que 80 % des ordinateurs portables et ordinateurs de bureau d'entreprise (ce pourcentage est même supérieur pour les serveurs d'entreprise) contiennent des informations personnelles et financières confidentielles ou de propriété intellectuelle qui doivent être sécurisées. Diverses réglementations comme les lois HIPAA, Gramm-Leach-Bliley et Sarbanes-Oxley obligent les entreprises à garantir la confidentialité de ces données. De nombreux États se sont même dotés de lois en matière de violation des données, notamment la Californie avec la loi SB-1386 Security Breach Information Act qui oblige à informer les victimes potentielles lorsqu'il est raisonnable de croire que la confidentialité des informations les concernant a pu être menacée. Toutes ces réglementations rendent, par conséquent, les violations de sécurité particulièrement coûteuses. Le coût global d'une violation de sécurité par enregistrement menacé varie entre 50 et 300 $ US selon le niveau de confidentialité des données, et couvre la découverte et la notification, la perte de productivité et de clients, les amendes réglementaires ainsi que la mise en œuvre d'une solution. En résumé, il est impératif que les données contenues sur les disques mis au rebut ne tombent pas entre de mauvaises mains.

# Comment mettre des disques au rebut de façon sûre, rapide et simple

## Des procédures trop longues, trop coûteuses et qui n'assurent pas toujours la protection des données

Les organisations pour lesquelles la protection des données est capitale investissent temps, efforts et argent pour mettre leurs disques au rebut de façon sécurisée. Lorsque les entreprises se débarrassent de leurs disques, elles en effacent généralement le contenu et/ou les détruisent physiquement. Les centres de données confient souvent la destruction de leurs disques à un prestataire externe. Les organisations informatiques peuvent également réaffecter leurs disques en en effaçant le contenu dans le centre de données, puis en les envoyant à un autre centre de données ou un autre site. Or, cette procédure fastidieuse et onéreuse est souvent vouée à l'échec. Pour plus d'informations sur les avantages et inconvénients des méthodes actuelles de mise au rebut des disques, reportez-vous à l'annexe A.

## Disques avec autochiffrement et Seagate Instant Secure Erase : pour la simplification et la réduction des coûts de mise au rebut des disques

La fonction d'autochiffrement avec Seagate Instant Secure Erase pallie les inconvénients présentés par les méthodes actuelles de mise hors service des disques durs en proposant une alternative simple, rapide, peu coûteuse et sécurisée.

Les disques avec autochiffrement assurent le chiffrement complet des disques durs. Parmi toutes les solutions disponibles, les plus sûres utilisent les algorithmes de chiffrement AES-256 ou AES-1288, déclarés conformes aux exigences de sécurité de niveau 2 par l'Institut national des normes et de la technologie des États-Unis (National Institute of Standards and Technology, NIST). Les données destinées à être enregistrées sur le disque sont chiffrées avant même leur enregistrement au moyen d'une puce ASIC dédiée. La clé de chiffrement est stockée dans une zone sécurisée et inaccessible du disque. Lors d'une lecture, les données chiffrées sont déchiffrées avant de quitter le disque. L'autochiffrement est toujours activé : le chiffrement est permanent et ne peut être désactivé. En mode de fonctionnement normal, les opérations de chiffrement sont complètement transparentes. Les disques avec autochiffrement sont semblables aux disques non dotés de cette fonction et ne présentent aucune altération des performances.

## Mise au rebut d'un disque avec autochiffrement avec Seagate Instant Secure Erase

Les disques avec autochiffrement Seagate Secure™ génèrent leur propre clé de chiffrement au moyen d'une méthode déclarée sécurisée par le NIST. Au moment de la mise au rebut d'un disque, l'administrateur en change simplement la clé de chiffrement. Or, sans la clé appropriée, les données contenues sur le disque deviennent instantanément et automatiquement illisibles ; le disque peut alors être reformaté en toute sécurité.

Comparé aux autres méthodes, les disques avec autochiffrement Seagate constituent un gain de temps précieux puisqu'il n'est plus nécessaire de consacrer des heures au traitement de chaque disque. Un disque de 3 To peut être effacé de façon cryptographique en moins d'une seconde en comparaison des 39 heures nécessaires pour écraser trois fois ce même disque. Seagate ISE réduit tous les coûts de nettoyage par destruction ou effacement des données. Les centres de données n'ont plus à effacer les disques, payer leur destruction mécanique ou faire appel à un prestataire externe pour les détruire et s'en débarrasser. Comme le disque dur n'est pas détruit, les lecteurs nettoyés de façon cryptographique peuvent être réaffectés en toute sécurité dans l'organisation, vendus ou donnés pour être réutilisés.

## Conclusion

Les méthodes traditionnelles de mise au rebut et de recyclage des disques sont fastidieuses et coûteuses, et peuvent, malgré tous les efforts du centre de données, ne pas parvenir à garantir une protection complète des données alors que la technologie d'autochiffrement Seagate Instant Secure Erase offre une solution de sécurité optimale. Grâce à un disque assurant le chiffrement automatique des données dès leur enregistrement sur disque, les centres de données désireux de se débarrasser de leurs disques peuvent littéralement jeter leur clé de chiffrement. Les données encore présentes sur le disque ne sont alors plus accessibles... par quiconque. Les centres de données réalisent ainsi d'importantes économies de temps et d'argent tout en mobilisant moins leur personnel, et peuvent véritablement se débarrasser de leurs disques ou les réutiliser sans se soucier de la sécurité des données qu'ils contiennent.

# Comment mettre des disques au rebut de façon sûre, rapide et simple

## Annexe A : Avantages et inconvénients des méthodes traditionnelles de mise au rebut des disques

Les deux principales méthodes de mise au rebut des disques actuellement utilisées sont les suivantes :

- Écrasement des disques
- Destruction physique des disques

Cette section présente les avantages et inconvénients de chaque méthode.

### Ecrasement d'un disque

Que son objectif soit de détruire ou de recycler des disques, le centre de données écrase généralement les données. Avec l'écrasement des données, la sécurité de ces dernières ne risque pas d'être menacée lors de leur acheminement vers un site de destruction et les nouveaux utilisateurs des disques recyclés ne pourront pas accéder à la moindre donnée.

Pour écraser les données du disque, le centre de données utilise un programme qui écrit une combinaison de 0 et de 1 sur chaque emplacement du disque dur, remplaçant ainsi les données utiles par des données parasites qui brouillent les précédentes. En fonction de l'importance des données et/ou des normes sectorielles, plusieurs écrasements peuvent être nécessaires.

Si elles appliquent les normes en matière d'effacement des données, les entreprises peuvent faire en sorte que leurs données soient irrécupérables. Parmi les normes applicables en matière d'écrasement des données, citons la norme 5220.22 du Département de la Défense américain (Department of Defense, DoD) qui précise que tous les disques fonctionnels doivent être effacés trois fois avant d'être mis au rebut ou réutilisés, ou encore la norme 800-88 de l'Institut national des normes et de la technologie des États-Unis (National Institute of Standards and Technology, NIST), qui rend les disques durs irrécupérables après une simple passe de nettoyage.

#### Avantages de l'écrasement d'un disque

Comme l'écrasement ne détruit pas les disques, les périphériques qui les renferment peuvent être recyclés. Une société peut ainsi économiser plusieurs centaines de dollars par disque, en fonction de la durée de vie restante du disque et du coût d'un nouveau disque. Si le disque est destiné à être détruit physiquement, l'effacement empêche que les données qu'il contient ne tombent entre de mauvaises mains.

#### Inconvénients de l'écrasement des données

L'effacement des disques est malgré tout fastidieux, souvent voué à l'échec et onéreux.

**Procédure fastidieuse :** aujourd'hui, les disques durs des centres de données offrent de très grandes capacités de stockage. S'il est déjà fréquent d'y trouver des disques de 3 téraoctets, on verra bientôt l'avènement de disques de 4, voire 5 téraoctets. Avec de telles capacités, l'effacement des données peut prendre plusieurs heures, voire plusieurs jours, selon le nombre de passes effectuées, la taille du disque et la vitesse du système. Il faut, par exemple, 13 heures pour reformater/effacer une fois un disque de 3 To. Généralement, la procédure d'effacement est reproduite trois fois si le disque est destiné à être recyclé, ce qui représente au total 39 heures par disque. Comme les disques deviennent de plus en plus volumineux, le temps nécessaire à leur effacement ne peut qu'aller croissant.

**Échec possible de l'opération :** un disque peut être mis hors service en raison d'erreurs de données ou d'une autre cause de défaillance, or ces problèmes peuvent entraîner l'interruption de l'effacement par expiration du délai imparti, voire son échec complet. Une erreur d'asservissement peut empêcher le disque de localiser certaines données et/ou de les effacer. Par exemple, un client constate que la procédure d'effacement échoue fréquemment. Si la procédure s'interrompt après une heure ou deux, il relance la procédure. Si elle s'interrompt après 8 à 10 heures, il abandonne la procédure et détruit le disque sur site, d'où une augmentation des coûts et des risques de sécurité. Pour cette raison, le personnel des centres de données doit rester à proximité des disques en cours d'effacement et suivre la procédure pour déterminer à quel moment elle a échoué, d'où une hausse des coûts de main-d'œuvre liés à l'effacement.

**Coûts :** parallèlement aux coûts associés à la présence indispensable du personnel du centre de données lors de la procédure d'effacement, le coût des programmes de nettoyage des disques durs peut varier grandement, allant de la gratuité totale avec les freeware à 70 $ US pour une licence mono-utilisateur ou encore près de 4 000 $ US[1] pour une licence pour 1 000 utilisateurs.

### Destruction physique des disques

Les organisations détruisent généralement les disques qu'elles ne recyclent pas. Souvent, les disques sont percés de part en part, broyés, martelés ou écrasés. Les organisations peuvent détruire elles-mêmes les disques, faire appel à une société extérieure pour détruire les disques dans l'enceinte du centre de données ou les envoyer à un prestataire externe qui se charge de la destruction hors site.

[1] Sources : Étude de solutions par Multi-wipe (www.multiwipe.com), iolo Technologies DataScrubber (www.iolo.com), Lsoft Technologies Active@KillDisk (www.killdisk.com), White Canyon Software WipeDrive (www.whitecanyon.com), Jetico BCWipe (www.jetico.com), Kroll Ontrack Eraser (www.krollontrack.com).

# Comment mettre des disques au rebut de façon sûre, rapide et simple

### Destruction sur site

Lorsqu'un disque ne peut pas être effacé, certains centres de données n'autorisent pas sa sortie du centre de données pour des questions de sécurité. La destruction du disque par l'organisation elle-même offre le plus haut niveau de sécurité puisque aucun tiers ne pénètre dans le centre de données. Cette procédure présente, en revanche, différents inconvénients en termes de temps, d'efforts et d'argent. Le coût de la machine nécessaire à la destruction peut être considérable : il faut ainsi compter de 950 $ US pour un petit destructeur manuel à 45 000 $ US pour une unité de la taille d'un copieur grand public.[2] Le personnel informatique doit prendre le temps de détruire les disques. Comme la destruction physique des disques peut nuire à l'environnement, le personnel informatique doit coordonner avec soin leur transport et leur rejet.

### Destruction externalisée sur site

Les organisations peuvent faire appel à des sociétés extérieures pour qu'elles procèdent à la destruction des disques dans l'enceinte du centre de données, et s'assurer ainsi qu'aucun disque non sécurisé ne quitte le site. Avec cette solution, le risque de perte d'un disque est nul. Elle s'avère également pratique puisque le personnel informatique n'est pas mobilisé par la destruction physique des disques et leur évacuation. Cette méthode présente toutefois un inconvénient certain : son coût élevé. Les prestataires externes facturent des frais de transport en plus des frais standard de destruction des disques. Elle présente également un risque de sécurité puisque des personnes étrangères au site pénètrent dans des zones sécurisées.

### Destruction hors site externalisée

Le plus souvent, les sociétés font appel à un prestataire externe pour détruire hors site les disques effacés. Avec cette méthode, aucune société tierce ne pénètre dans le centre de données et le prestataire externe gère les déchets. Cette option peut s'avérer onéreuse, selon la quantité, et n'élimine pas entièrement les risques de sécurité, notamment si le centre de données n'a pas correctement effacé les disques. Par conséquent, les centres de données doivent s'assurer que le prestataire qu'ils embauchent respecte les meilleures pratiques en matière de mise au rebut des disques. Le prestataire externe doit mettre en place une chaîne de responsabilité sans faille : certaines sociétés fournissent des consoles dans lesquelles les clients verrouillent leurs disques et se servent de ces consoles pour acheminer les disques jusqu'aux camions dans l'attente de leur destruction. Le prestataire externe émet ensuite un certificat de destruction pour confirmer que la procédure a bien été respectée du début à la fin.

[2] Sources : Data Devices International (www.datadev.com)

www.seagate.com

Seagate Secure™

AMÉRIQUES Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, États-Unis, +1 408 658 1000
ASIE/PACIFIQUE Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapour 569877, +65 6485 3888
EUROPE, MOYEN-ORIENT ET AFRIQUE Seagate Technology SAS 16-18 rue du Dôme, 92100 Boulogne-Billancourt, France, +33 (0)1 41 86 10 00