

Les outils de DLP

(Prévention contre la perte d'information)

Pierre Samson
Spécialiste des ventes, Solutions de sécurité
Montréal

Agenda

- Qu'est-ce que le DLP – définitions et synonymes
- Le cas d'affaire pour le DLP
- Types / Composantes d'une solution DLP
 - Points d'accès (« Endpoint »)
 - Réseaux
 - Découverte / Identification

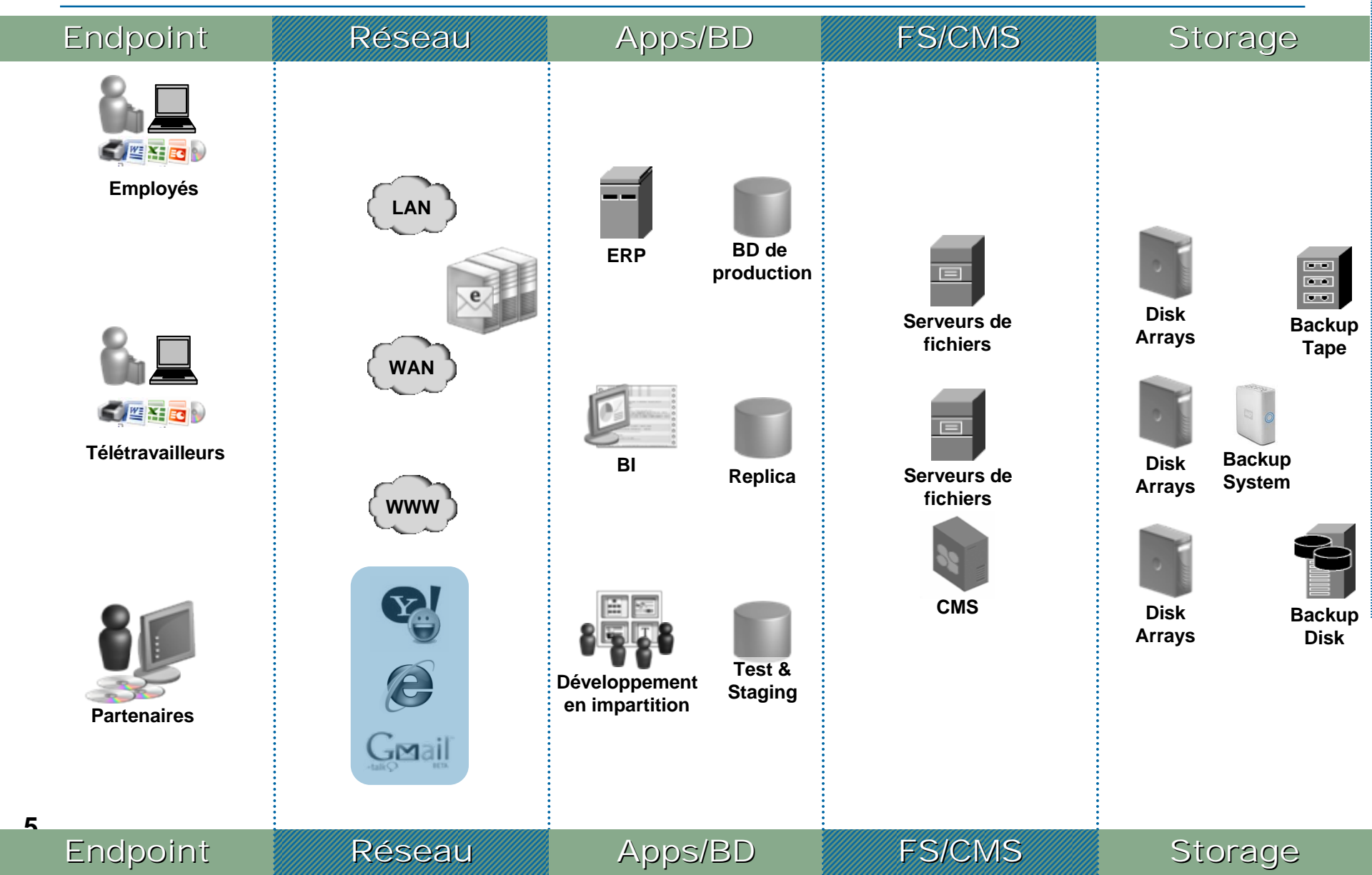
Ce qu'est le DLP

- **Nombreux synonymes :**
 - Protection / Prévention des fuites de données
 - Protection / Prévention de la perte d'information
 - Protection / Prévention des fuites d'information
 - Prévention d'extrusion
 - Surveillance du contenu et filtrage
 - Surveillance du contenu et protection

Ce qu'est le DLP

- Selon Forrester
 - Fait référence à des produits qui détecte, et de façon optionnelle, préviennent les violations aux politiques corporatives en rapport à l'usage, le storage et la transmission d'informations sensibles.
- Selon Wikipedia
 - DLP est un terme de sécurité informatique faisant référence aux systèmes qui identifient, surveillent et protègent les données en usage (end-point), en transit (réseaux) et au repos (storage).
- Selon « DLP for Dummies »
 - La prévention de la divulgation, que ce soit de façon intentionnelle ou accidentelle, d'informations allant des informations personnelles devant être protégées, pour des raisons légales, jusqu'au informations reliées à la propriété intellectuelle et aux secrets commerciaux.
- ...plus toutes les définitions utilisées par les manufacturiers selon leurs agendas respectifs

Où sont nos données... elles sont extrêmement mobiles et en transformation



Qu'est-ce que l'information sensible

Croissance des revenus

Réduction des coûts

Clientèle

Continuité des affaires

Conformité

Initiatives d'affaires

Information sensible

(ex: cartes de crédit,, propriété intellectuelle, informations personnelles - PII)

Données réglementées

Conformité

- Cartes de crédit (PCI)
- Informations personnelles sur les individus (PII)
- Dossiers médicaux (HIPAA)
- Données financières (SOX, GLBA)

Données non-réglementées

Propriété intellectuelle

- Code source, "Blue prints"
- Plans d'architecture
- Nouveaux médicaments

Données stratégiques ou opérationnelles

- "Roadmap"
- Plans d'affaires & modèles
- Fusions et acquisitions, données marketing

Les données sensibles

- Les données en transit (« in motion »)
 - Toutes les données sur « le fil ».
 - HTTP, FTP, IM, P2P, SMTP
- Les données inerte (« at rest »)
 - Serveurs de fichiers, bases de données, serveurs web, etc.
 - SAN, ruban, etc.
- Les données active (« in use »)
 - Données qui quittent via les médias rétractables
 - Impression

Le risque ?

- 1 courriel sur 400 contient de l'information confidentielle;
- 1 fichier sur 50 est exposé de façon dangereuse;
- 4 compagnies sur 5 admettent avoir déjà perdu des données d'un portable;
- 1 compagnie sur 2 admet avoir déjà perdu des données d'une clé USB.

Les coûts de la perte ou fuite de données :

Quelques statistiques

- Coûts des fuites de données :
 - En hausse de 43 % depuis 2005;
 - Coût moyen : 6.3 millions \$;
 - Coût moyen par enregistrement perdu : 197 \$; 239 \$ pour les sociétés du secteur financier.
- Coûts reliés à la perte de revenus :
 - En hausse de 30 % depuis 2005;
 - Représentent 65 % des coûts reliés à la fuite d'information (comparé à 54 % en 2006).

Source : Ponemon Institute, Novembre 2007

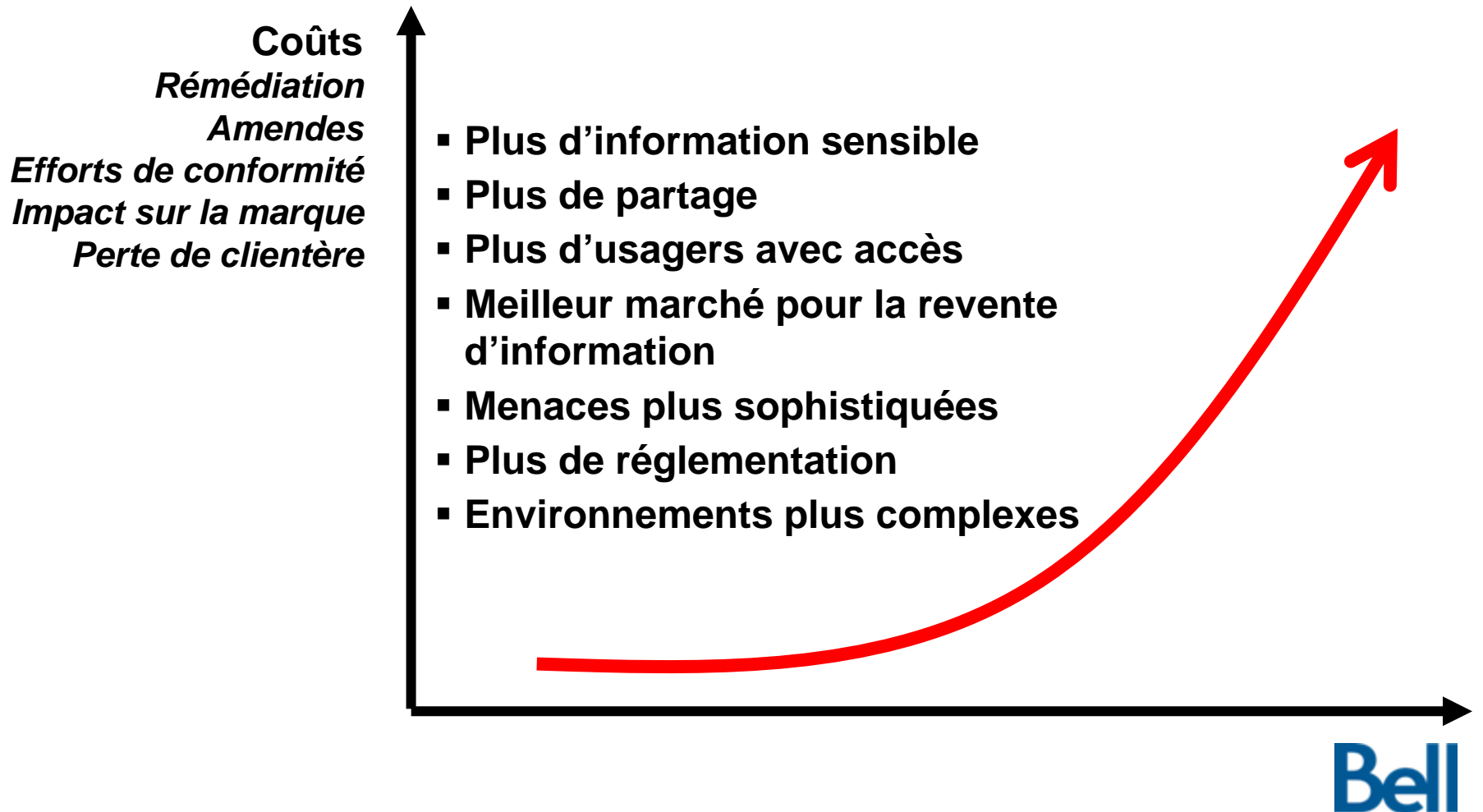


La perte de données peut être très coûteuse, sur plusieurs points de vue

- Le 2 janvier 2007 un grand détaillant annonce un bris de sécurité
- Impact sur la marque
 - La une des journaux : la fuite la plus publicisée au monde
 - Des millions de clients affectés
 - Ennui majeur pour les clients : le Bureau des véhicules automobiles inondé d'appels
- Impact sur les revenus
 - La compagnie a enregistré une charge de de \$196m pour avoir compromis des données de clients
- Aspects légaux
 - 27 recours collectifs déposés devant plus d'une douzaine de législations
 - Les demandants incluent des détenteurs de cartes, des émetteurs, des marchands et des fonds de pension



Les coûts augmentent sans améliorer les résultats

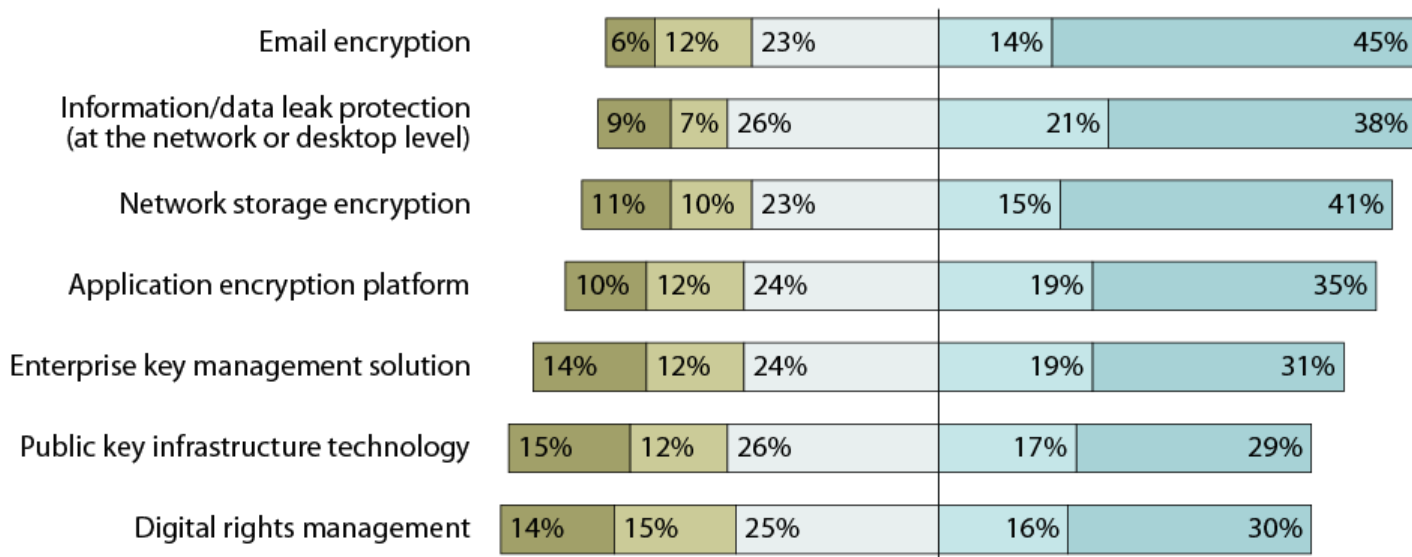


Le DLP en 2009

About One-Fifth Of Firms Will Pilot Or Adopt Data Leak Prevention In The Next 12 Months

“What is your organization’s interest in adopting each of the following data security technologies?”

Don't know
 Not interested
 Interested, but no plans to adopt
 Will pilot or adopt in the next 12 months
 Already adopted



Base: 881 North American and European enterprise IT security decision-makers who have data security challenges within their organization (percentages may not total 100 because of rounding)

Source: Forrester Research, “The State of Enterprise Security: 2008 to 2009,” December 2008.



Les composantes du DLP

- **Sécurisation des réseaux**
 - Analyse du trafic réseau à la recherche de transmission d'informations non autorisées et prise d'action appropriée;
 - Couvre courriels, IM, FTP, HTTP, HTTPS, etc.;
 - Alertes et rapports de violations;
 - Premières générations d'outils DLP, habituellement moins coûteux et plus simple d'implantation;
 - « Data in motion ».

Les composantes du DLP

- Sécurisation au point d'accès (« endpoint »)
 - 50 % des données perdues le sont via les points d'accès;
 - Serveurs et postes de travail (principalement portables);
 - Unités de stockage et médias rétractables;
 - USB, disques externes, lecteurs CD / DVD
 - Appareils mobiles ou sans fils;
 - Téléphones et PDA's Bluetooth, IdDA, WAP WiFi
 - Va permettre de bloquer ou permettre :
 - Impression, sauvegarde, export, gravure
 - Applications malicieuses
 - Peut enforcer l'encryption
 - « Data in use » et « Data at rest »

Le problème des clés USB

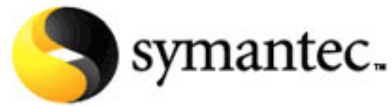
- 320 000 fichiers sensibles ont été transférés illégalement sur une clé mémoire par un employé de Boeing et transmis au Seattle Times;
- Les informations personnelles de 8 000 étudiants du Texas A&M Corpus Christi, dont leur numéro de sécurité sociale, ont été perdues à Madagascar lorsqu'un professeur en vacances sur la côte africaine a emporté les données avec lui sur une clé à mémoire Flash2;
- Des clés mémoire contenant des renseignements personnels sur des soldats américains et des informateurs secrets, notamment, ont été vendues en Afghanistan par des adolescents, à 40 dollars pièce;
- Le Wilcox Memorial Hospital de Kauai a prévenu 130 000 patients actuels et anciens de la disparition d'une clé mémoire contenant des informations médicales personnelles;
- Des voleurs de données ont réussi à pénétrer le système de CardSystems Solutions, un prestataire chargé de traiter les transactions par carte bancaire, et à dérober plus de 40 millions de numéros de cartes bancaires de différentes marques, selon MasterCard International;
- Des dossiers médicaux confidentiels étaient stockés sur une clé mémoire USB qui a été emballée et vendue comme neuve à un agent immobilier.

Les composantes du DLP

- Découverte / Identification
 - Outils automatisés;
 - Politiques pré-définies;
 - Serveurs et postes de travail;
 - « in use », « in motion » et « at rest »;
 - Doit couvrir autant les données réglementées que les données sensibles;
 - La puissance et la précision de la technologie va réduire le nombre de « faux positifs ».

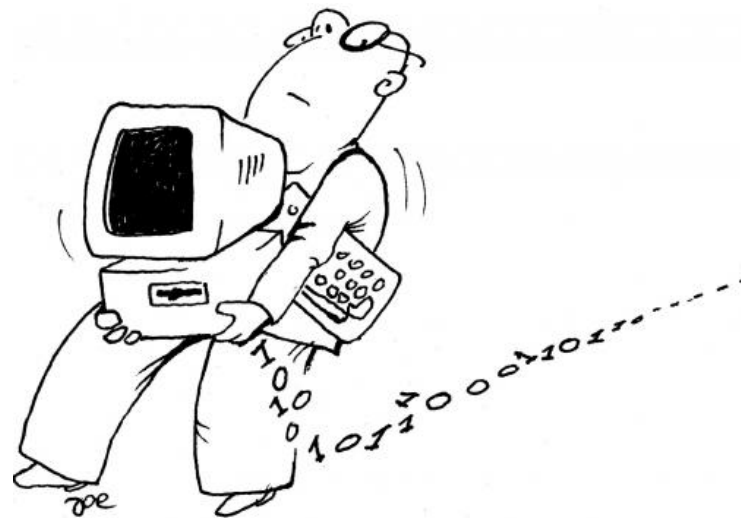
Partenaires DLP de Bell

- Les principaux (selon Forrester...)



- Les autres (...toujours selon Forrester)





Merci !