Présentation CERT IST
9 Juin 2009

Enjeux et Mise en Œuvre du DLP

Alexandre GARRET

Directeur des Opérations – ATHEOS

agarret@atheos.fr

Sommaire

- Constats, Riques & Enjeux
- Qu'est ce que le DLP ?
- Quelle Démarche Adopter ?
- Vision du marché

atheos
L'esprit d'Architecte

CertIST
Industrie Services Tertiaire

Constats et Enjeux

Une Réalité

- **Statistiques de vols d'identités aux US:**
  - Plus de 10 millions de victimes de vol d'identités numériques,
  - Une identité est volée toutes les 4 secondes,
  - Le cout moyen pour restaurer une identité est de $8,000,
  - La victime passe plus de 600 heures pour reprendre son activité.

13 mai 2009 :

« La défense antimissile américaine sur eBay »

Les chercheurs de BT ont passé au peigne fin 300 disques durs trouvés sur eBay. Plus d'un tiers contenaient des informations critiques ou personnelles, dont des secrets militaires américains.

Source : http://www.journaldunet.com/solutions/securite/actualite/des-disques-durs-d-occasion-tres-bavards-sur-ebay.shtml

5 janvier 2009 :

« Orange a laissé un accès libre à 400.000 fiches de ses clients »

Plus de 400.000 fiches clients du Fournisseur d'Accès à Internet Orange) ont été laissées en accès libre sur Internet via un lien officiel de la filiale de France Télécom. Une faille qui semblait exister depuis plusieurs semaines.

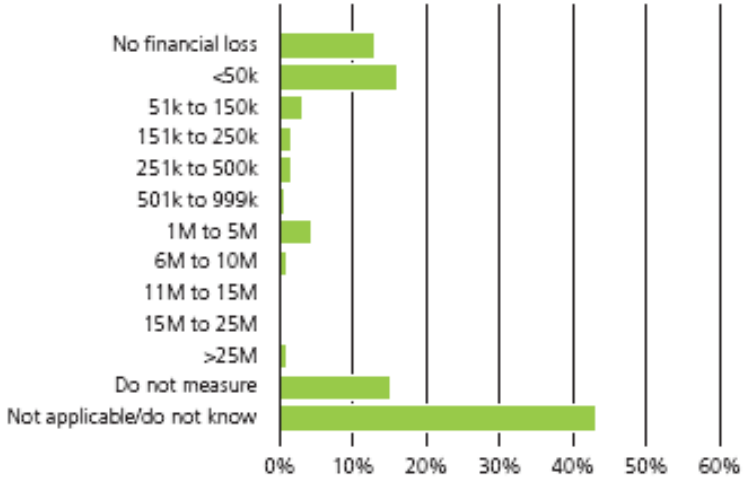
Source : www.generation-nt.com/arnaque-phishing-orange-vol-donnees-bancaires-faux-site-actualite-259711.html

Une montée en puissance

285 MILLION RECORDS WERE COMPROMISED IN 2008.

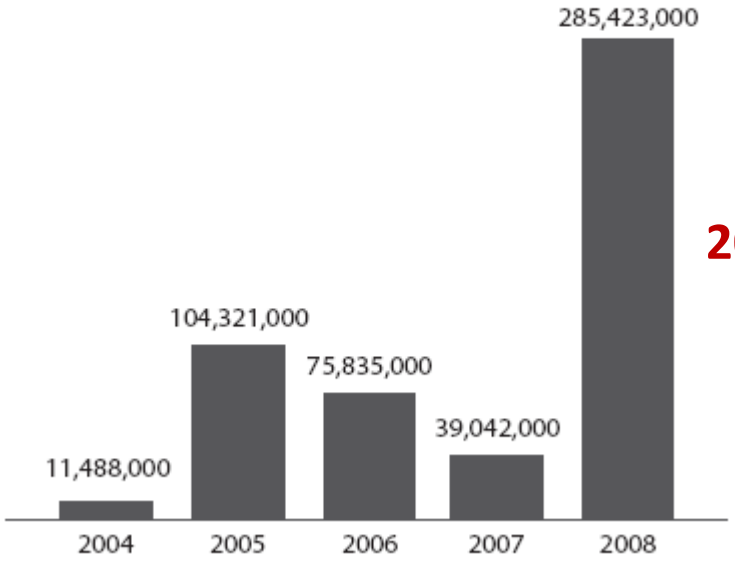
Le cabinet d'études **Gartner** évoque même **une épidémie de fuites de données.**

What was the estimated total monetary damage sustained by the organization including direct costs (e.g., clean up and recovery) and indirect costs (e.g., loss of brand) in USD?



Source Deloitte 2009 Global Security Survey

Figure 27. Number of records compromised per year in breaches investigated by Verizon Business

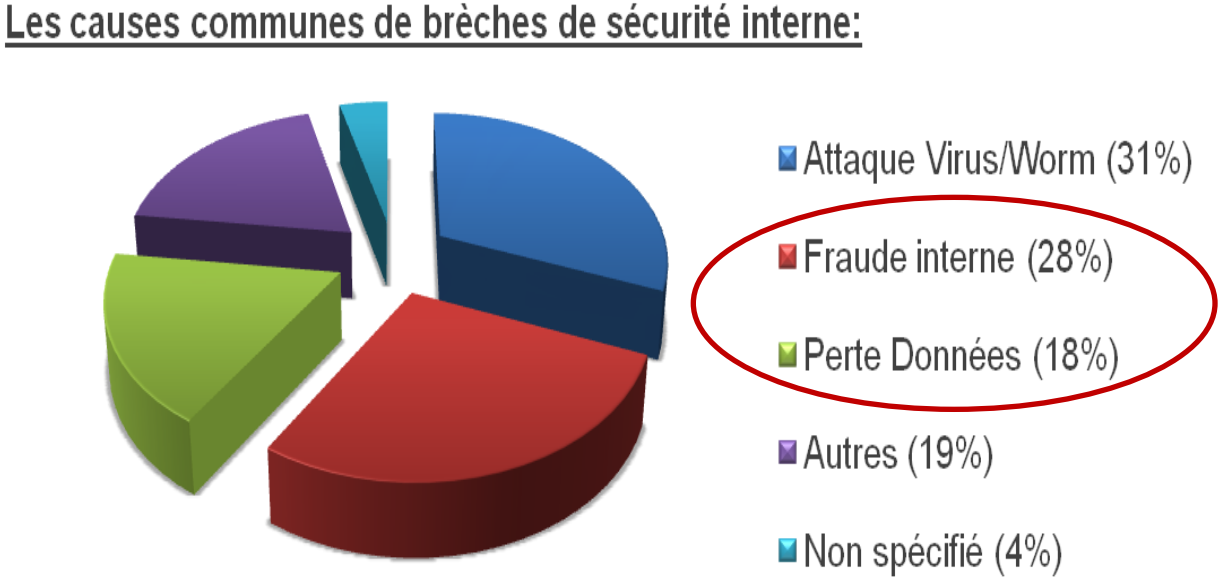


2009 ?

Source Verizon 2009 Data Breach Investigations Report

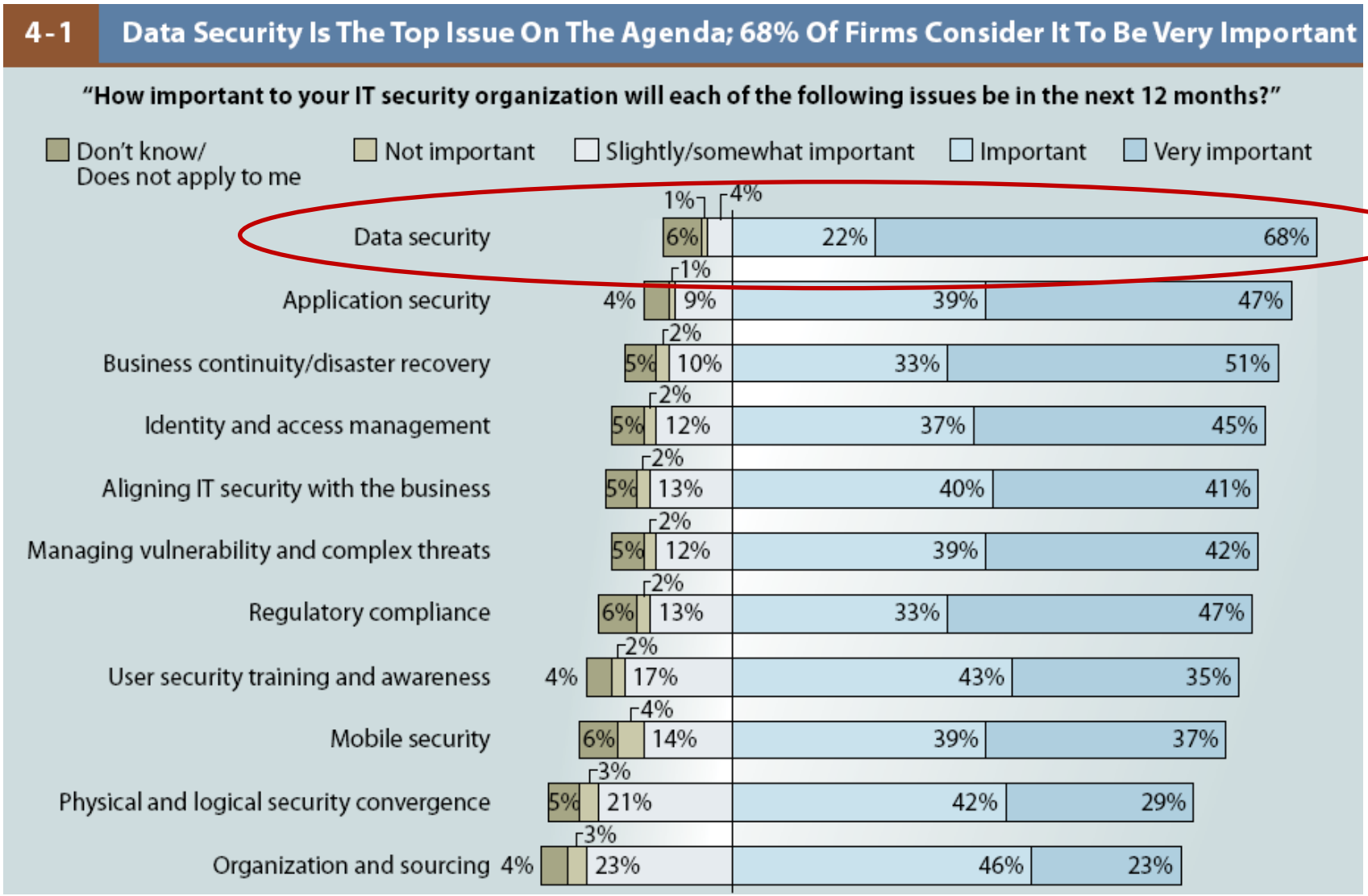
Qui peut être touché ?

- **D'après le "Deloitte's Global Security Survey" :**
  - 49% des sociétés ont eu une violation de leur sécurité interne dans l'année.



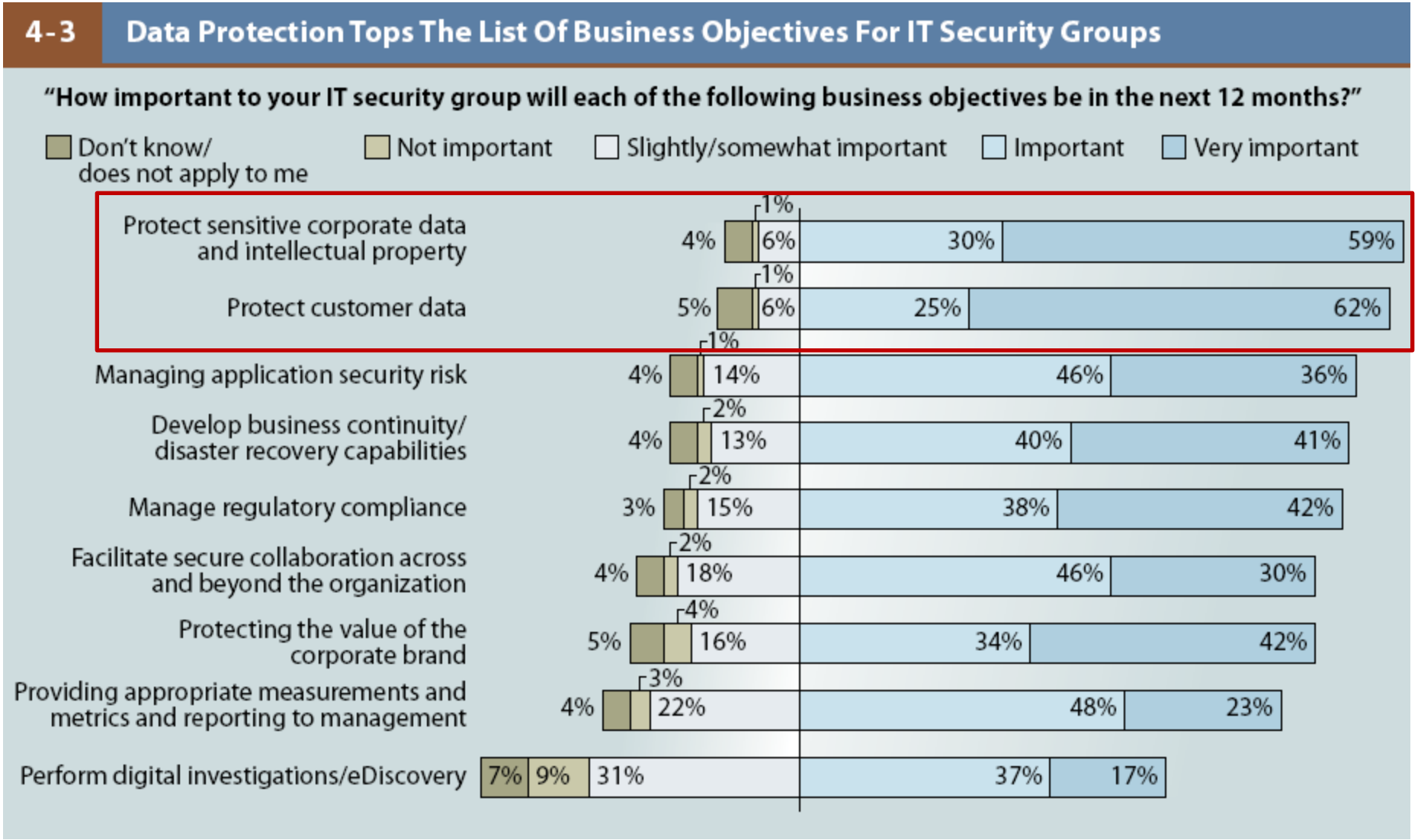
Une Priorité pour Tous

4-1 Data Security Is The Top Issue On The Agenda; 68% Of Firms Consider It To Be Very Important



Source Forrester The state of enterprise IT Security 2008 to 2009

Une Priorité pour Tous



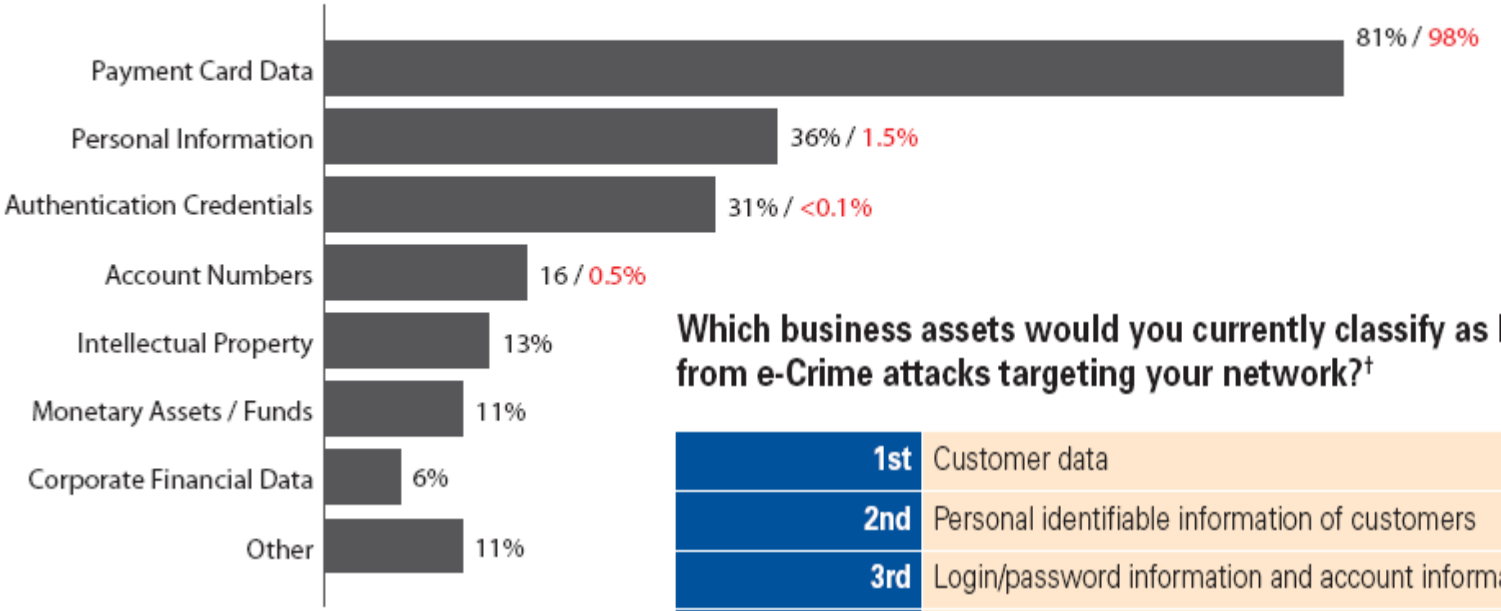
Source Forrester The state of enterprise IT Security 2008 to 2009

Les Risques & Enjeux

- **Limiter les risques et leurs conséquences :**
  - Perte d'image, de clients, de chiffre d'Affaires …
  - Contraventions aux réglementations et pénalités induites
  - Concurrentiel
  - Divulgation d'informations confidentielles, nominatives, R&D
  - Etc …

- **Quels types de données sont les plus concernées ?**

Figure 29. Compromised data types by percent of breaches (black) and records (red)*



Which business assets would you currently classify as high-risk targets from e-Crime attacks targeting your network?†

1st	Customer data	76%
2nd	Personal identifiable information of customers	60%
3rd	Login/password information and account information	53%
and in last place*	Business sensitive information e.g. P and L figures	

Les Risques & Enjeux

- **Maitriser les circuits de l'information et les possibilités de fuite / perte**
  - Echanges sur Internet (messagerie professionnelle, personnelle, instantanée, blog, réseaux sociaux)
  - Echanges sur support (clés USB, x Card, Disque Externe, …)
  - Stockage « mobile » (PC portable, Smartphone)
  - Stockage dans le SI
  - Services en mode ASP
  - Etc …

39% des utilisateurs de clés USB les utilisent pour des transferts entre le travail et le domicile

60% des données professionnelles stockées sur le poste de travail

90% des pertes de données ne sont pas intentionnelles

Les Risques & Enjeux

Par QUI ?

78% des fuites proviennent de personnes internes et autorisées

85% des employés malhonnêtes sont des hommes

49% Appartiennent au Senior Management

49% Pour l'amélioration de leurs conditions financières, de leur pouvoir, voire de leur influence

Les Risques & Enjeux

- Faire face à **l'évolution du modèle de sécurité** :
  - Entreprise étendue
  - Ouverture des « frontières »
  - Passer du modèle de **Vauban** au modèle **Aéroportuaire**

atheos
L'esprit d'Architecte

CertIST
Industrie Services Tertiaire

Qu’est ce que le DLP ?

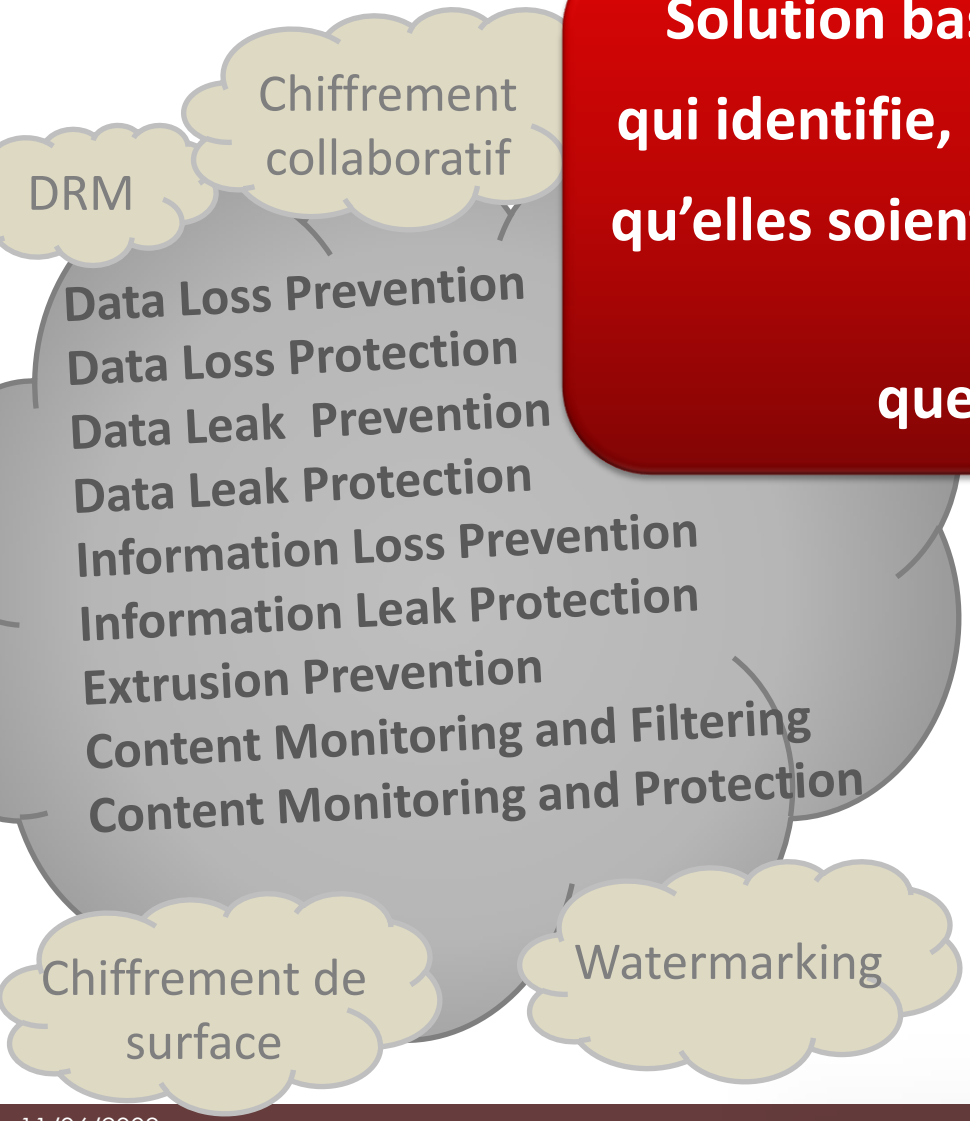
Définition du DLP

Solution basée sur des règles centralisées

qui identifie, surveille et protège les données

qu'elles soient stockées, en cours d'utilisation ou en mouvement

quel qu'en soit le support



- Analyse du contenu en profondeur
- Définition centralisée des règles
- Traitement des informations sur une grande variété de supports, systèmes et emplacement

Définition du DLP

- **Quels types de perte ?**
  - Accidentelle
    - Perte
    - Erreur de manipulation
    - Méconnaissance
    - Etc …
  - Volontaire
    - Vol
    - Piratage
    - Destruction
    - Etc …
- **Typologies des données sensibles :**
  - Données « En Mouvement » – Toutes données qui passe à travers le réseau et vers l'Internet,
  - Données « Stockées » – Données présentes dans les systèmes de fichiers, bases de données ou autres unités de stockage.
  - Données « sur support » mobile – Clef USB, disque externe, Players MP3, portable, ou autre appareil mobile

Les Mécanismes de Fonctionnement

- Network DLP
  - Plateforme Filtrante sur flux Internet (e-mail, IM, FTP, HTTP et HTTPS)
  - Fonctionnement en mode proxy

- Host-based DLP
  - Sur le poste de travail ou serveur
  - Protection des données physiques et des canaux locaux

- Data Identification
  - Identification des données sensibles (par Mot clés, ou Dictionnaires)
  - Utilisation d'Expressions Régulières
  - Recherche et Empreintes de documents Sensibles (FingerPrinting)
  - Utilisation des Meta Data (Extension de fichier, taille du fichier, Etc)
  - Classification a priori (PCI DSS, CNIL …)

atheos
L'esprit d'Architecte

CertIST
Industrie Services Tertiaire

Quelle Démarche Adopter ?

Quelle Démarche Adopter ?

- **Se Poser Les Bonnes Questions :**
  - **Ou** sont les données sensibles et confidentielles de l'entreprise?
  - **Qui** peut manipuler, accéder à ces données
  - **Comment, Ou et Quand** sont transmises ces données et par **Qui** ?
  - Comment peut-on **controller et protèger** ces données ?
  - Quel est le **risque** potentiel pour l'entreprise (En cas de fuite) ?

Quelle Démarche Adopter ?

- **Eviter d'Interdire :**

  - **Interdire** l'usage des clés **USB**
  - **Limiter les** ordinateurs **portables** et **leur utilisation**
  - **Eviter les téléphones mobiles**
  - Limiter le **télétravail**
  - Etc

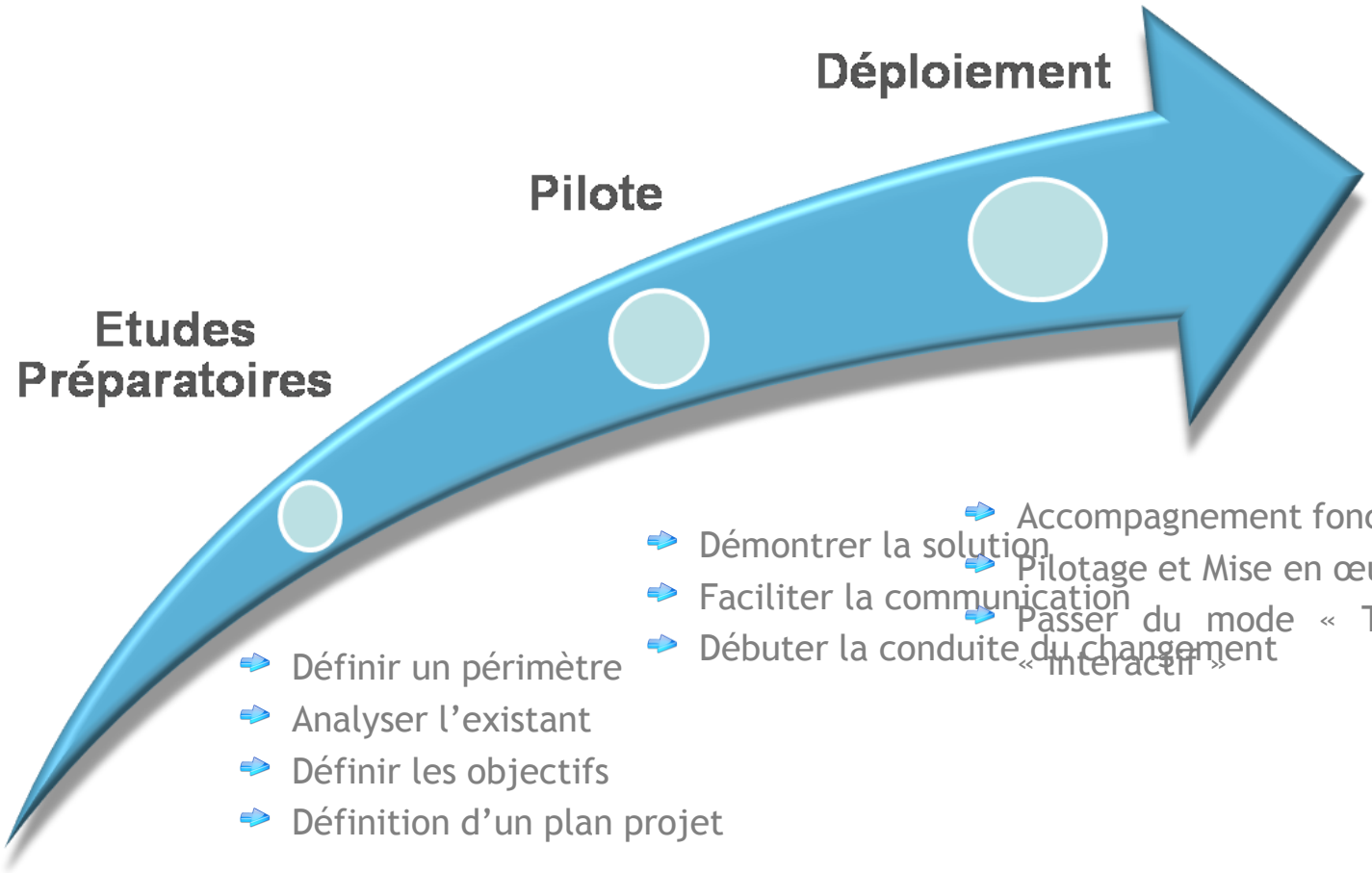
- **Ne pas oublier :**

  - **Mettre** l'utilisateur au **cœur de la réflexion**
  - **Adopter** une **démarche progressiste**

Les données n'appartiennent pas à l'IT mais à leurs producteurs

Quelle Démarche Adopter ?

- **Opter pour une démarche progressive et pragmatique**



Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Objectif et périmètre**
  - Pourquoi mettre en place un dispositif de DLP ?
  - Quel périmètre ?
  - Quels types de données protéger ?
    - Secrets d'enreprise : finances, secrets industriels, plans marketing…
    - Exigences réglementaires : données nominatives, propriété intellectuelle
  - Quels canaux de communication ?
    - Mail, IM, Réseaux sociaux
    - Périphériques amovibles
    - Impressions
  - Quelle fiabilité ?

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Définir les processus de DLP**
  - Acteurs et responsabilités
  - Fonctionnalités nécessaires
  - Contrôle permanent
- **Regrouper les besoins en modules homogènes**
  - Faciliter le déploiement
  - Chercher des résultats visibles le plus tôt possible
- **Définir des priorités**
- **Les exigences viennent autant des métiers que de l'IT**

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Proof of concept**
  - Valider la couverture fonctionnelle et la facilité d'intégration
- **Pérennité de la solution**
  - Technologies
  - Editeur
  - Support des intégrateurs
- **Coût et délais**

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

Exemples de critères d'évaluation

Couverture fonctionnelle
- Postes, réseau…

Fiabilité
- Taux de faux positifs / faux négatifs

Gestion de la politique de sécurité
- Définition et mise à jour
- Intelligibilité du formalisme
- Mise en vigueur des règles (où et comment)

Administration et reporting
- Ergonomie des outils
- Rapports d'audit et de contrôle
- Analyses d'incidents et investigations

Architecture
- Facilité de déploiement
- Intégration dans le SI existant

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Pilotage de la solution**
  - Tenue à jour dynamique des règles
    - Nouveaux projets
    - Nouvelle organisation…
  - Supervision du fonctionnement
  - Coordination business /IT ?
    - Qui décide de la mise en place d'une règle ?
- **Gestion des alertes et incidents**
  - Intégration dans le processus général de gestion des incidents ?
  - Support aux utilisateurs en cas de blocage (notamment faux positifs)
- **Processus de contrôle**
  - Audit / contrôle interne
  - Valorisation des actions du DLP ?

Mise en place en parrallèle de la phase de découverte du contenu

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Au déploiement initial, mais aussi en continu**
  - Découverte de nouveaux contenus, de nouveaux projets…
- **Les solutions sont encore imparfaites**
  - Pas en temps réel
  - Exhaustivité non garantie
- **Modèle de découverte :**
  - Exploration distante
  - Agent local (serveur ou terminal)
  - Intégration applicative

Démarche Générale

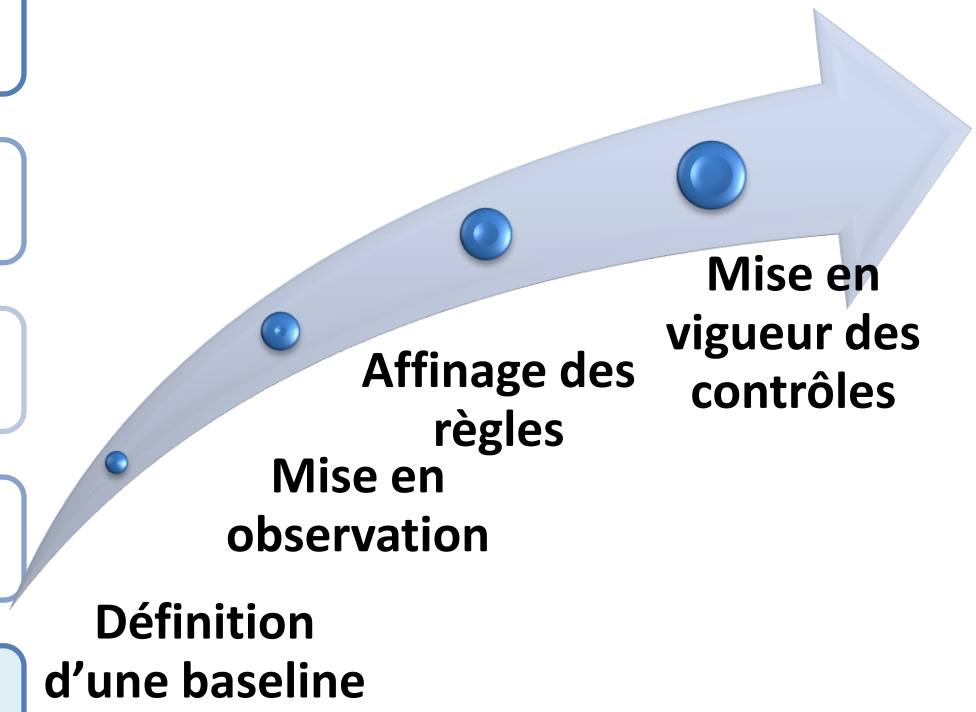
1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

- **Management**
  - Comment décider de la création de règles ?
  - Quel workflow ?
  - Quelle supervision ?
- **Quelles actions ?**
  - Journalisation
  - Notification
  - Restriction d'accès
  - Mise en quarantaine
  - Chiffrement

Démarche Générale

1. Définir ses besoins
2. Formaliser les exigences
3. Evaluer les produits du marché
4. Mettre en place l'organisation
5. Découvrir le contenu
6. Mettre les règles en vigueur

Mise en place progressive



Plusieurs Options de Déploiement

Surveillance et alerte

- Traitement manuel des alertes
- Education des utilisateurs
- → Informations peu sensibles

Conformité

- Recherche d'informations bien identifiées (classification a priori)
- Génération de rapports de conformité
- → Ex : n° de cartes de crédit (PCI DSS)

Protection a priori

- Mise en vigueur de mesures de précaution
- Chiffrement des données en sortie
- → Informations très sensibles

Classification des informations

- Inventaire exhaustif et classification de l'ensemble des informations
- Mise en vigueur ou non de la protection
- → Exhaustivité

atheos
L'esprit d'Architecte

Vision du marché

Des Fournisseurs Nombreux

- **Solutions complètes**
  - CA (Orchestria)
  - EMC/RSA (Tablus)
  - McAfee (Reconnex)
  - Symantec (Vontu)
  - Vericept
  - Workshare
- **Solutions intégrées partielles**
  - Code Green Networks
  - GTB Technologies
  - Websense (PortAuthority)
  - Trend Micro (Provilla)
- **Solutions purement réseau**
  - Clearswift
  - Fidelis Security Systems
  - Palisade Systems
  - Proofpoint
- **Solutions uniquement terminal**
  - NextSentry
  - Verdasys
  - Utimaco

atheos
L'esprit d'Architecte

CertIST
Industrie Services Tertiaire

Merci de votre Attention