

# Les solutions d'IAM classiques ne remplissent pas complètement leur rôle

Les cas de piratage informatique sont toujours plus nombreux, avec des dommages conséquents pour les entreprises affectées. Des mesures efficaces existent, mais elles ne sont pas implantées dans les entreprises soit par méconnaissance, soit par manque d'estimation du risque. Didier Assandri

Les Spartiates transmettaient leurs informations sur du parchemin qui avait été préalablement enroulé sur un bâton. Léonard de Vinci nous a transmis ses connaissances sur des manuscrits en écriture spéculaire. Plus près de nous, Enigma servait à l'armée allemande à transmettre ses messages. Qu'y a-t-il de commun à ces trois exemples? Deux choses. Toutes ont été pensées pour pouvoir transmettre des informations uniquement à des personnes autorisées à les lire. Toutes se concentraient sur la protection du contenu, à des degrés divers, en laissant l'accès au contenant sans grande protection particulière. Dans le cas des messages des Spartiates, le destinataire devait posséder un bâton du même diamètre et de la même longueur que celui qui avait servi à écrire le message – appelé une scytale – s'il voulait être en mesure de pouvoir lire le parchemin (un niveau de protection). Pour Léonard de Vinci, il fallait utiliser un miroir pour retrouver une écriture lisible mais il fallait aussi connaître le vieux toscan, car le maître avait pris soin de ne pas écrire en toscan moderne (deux niveaux de protection). En ce qui concerne Enigma, il fallait connaître le jargon militaire, le code de chiffrement et la fenêtre temporelle de transcription car le code était changé régulièrement (trois niveaux de protection).

## Du droit d'accès au droit d'en connaître

Si nous faisons un parallèle avec nos systèmes d'information, il est intéressant de constater que pour l'instant les efforts se sont surtout concentrés sur la gestion des accès et non pas vraiment sur la protection du contenu indépendamment de son emplacement. Une situation qui oblige à réfléchir sur la sécurité des informations et la protection des données (SIPD). Les entreprises sont la plupart du temps ignorantes des dangers encourus, au mieux démunies contre les risques potentiels et il faut souvent un sinistre conséquent, pouvant atteindre des sommes faramineuses, sans compter les dégâts d'image, pour qu'elles se rendent compte de leur vulnérabilité et mettent en place des solutions adéquates, car



Une scytale, utilisée par les Spartiates pour chiffrer leurs missives Source: Wikipedia

des solutions existent, au même titre que la sécurité physique.

Mais quelles sont les raisons de ces fuites de données, qui occasionnent tant de dégâts? Des cas connus, on peut en tirer quelques constats:

- Une grande partie des pertes informatiques sont le fait d'employés désabusés ou indéclicats, ou sont provoquées par inadvertance.
- L'informatique reste pour beaucoup de dirigeants d'entreprises, de conseils d'administration et de managers un monde hermétique et inconnu.
- La surveillance et le contrôle des informaticiens est un élément important de la gestion des risques.
- La quantité de données qui peuvent être stockées sur des clefs USB ou des ordinateurs portables est telle que les entreprises maîtrisent difficilement leurs flux de données.

Il apparaît donc qu'une solution classique de gestion des identités et des accès (IAM) n'est pas forcément en adéquation avec le résultat recherché de protection de contenu de document, c'est-à-dire «le droit d'en connaître»,

car un document sorti du contexte de l'entreprise (clé USB, courriel, CD) n'est plus protégé efficacement, puisqu'il suffit de connaître le code pour accéder au contenu.

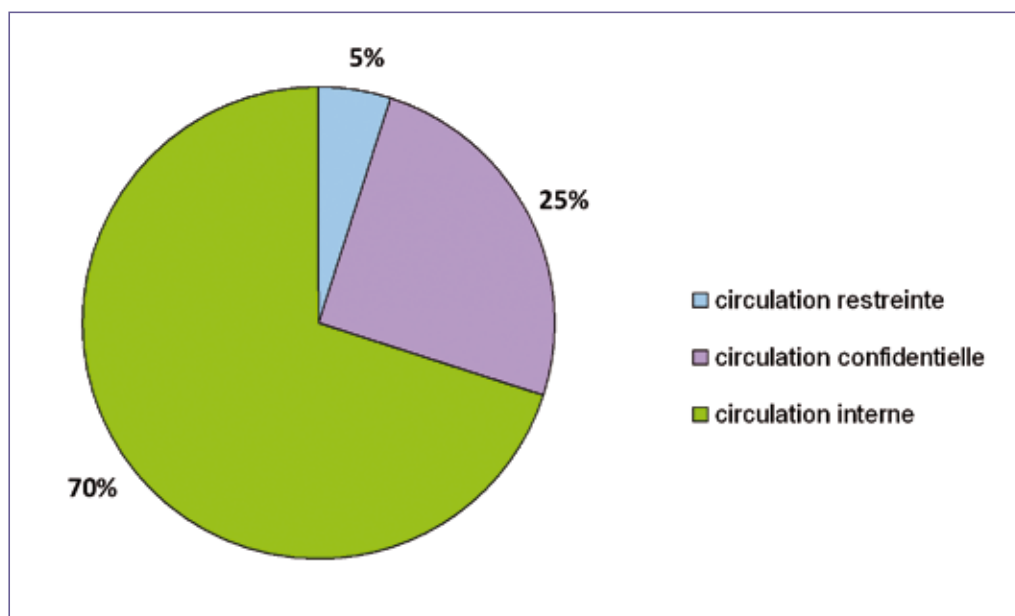
## Les problèmes liés aux solutions d'IAM classiques

Gestion des identités et des accès: quelle entreprise n'a pas planché sur le sujet au cours de ces cinq dernières années? Combien de projets ont réellement vu le jour et surtout combien de projets tiennent leurs promesses? Sans considérer les projets «placebo» du genre SSO ou eSSO, qui ont dans certains cas toute leur raison d'être, mais qui ne sauraient être classés dans la catégorie IAM.

Les réponses pourraient réserver de mau- ▶



**Didier Assandri,**  
Managing Director,  
Solvis Ltd



Répartition des documents par catégorie Source: SOLVIS Ltd

► vaises surprises, car très souvent les projets n'ont pas réuni tous les acteurs nécessaires, c'est-à-dire les départements IT, sécurité et surtout ressources humaines. Les processus n'ont pas été optimisés, les administrateurs systèmes ont toujours main mise sur les accès et surtout les critères de gouvernance d'entreprise en matière de données informatiques n'ont pas été respectés.

### Gestion et protection du contenu

La solution recherchée passerait donc par la mise en place d'une infrastructure permettant l'échange et la consommation d'informations entre utilisateurs habilités à le faire, et ce quel que soit l'emplacement du document – une dématérialisation de la protection des contenus de documents en somme. Une solution qui consisterait moins à se préoccuper de l'accès au document qu'à la protection de son contenu.

La protection du contenu peut être réalisée en mettant en place une solution efficace de gestion des rôles et des accès (RBAC), afin de garantir le contrôle des accès aux applications métiers de l'entreprise et ainsi à leur contenu. La mise en place d'une telle solution passe par une étape de segmentation des documents en fonction non pas du système auxquels ils appartiennent mais du degré de confidentialité de leurs contenus – ce qui conduit *in fine* probablement à l'emploi de trois catégories dans une proportion de 70/25/5:

- **Circulation interne:** il s'agit de tous les documents de l'entreprise qui doivent être protégés de la curiosité des personnes étrangères à l'entreprise. Dans ce cas, un simple logiciel de chiffrement de disque dur suffit.

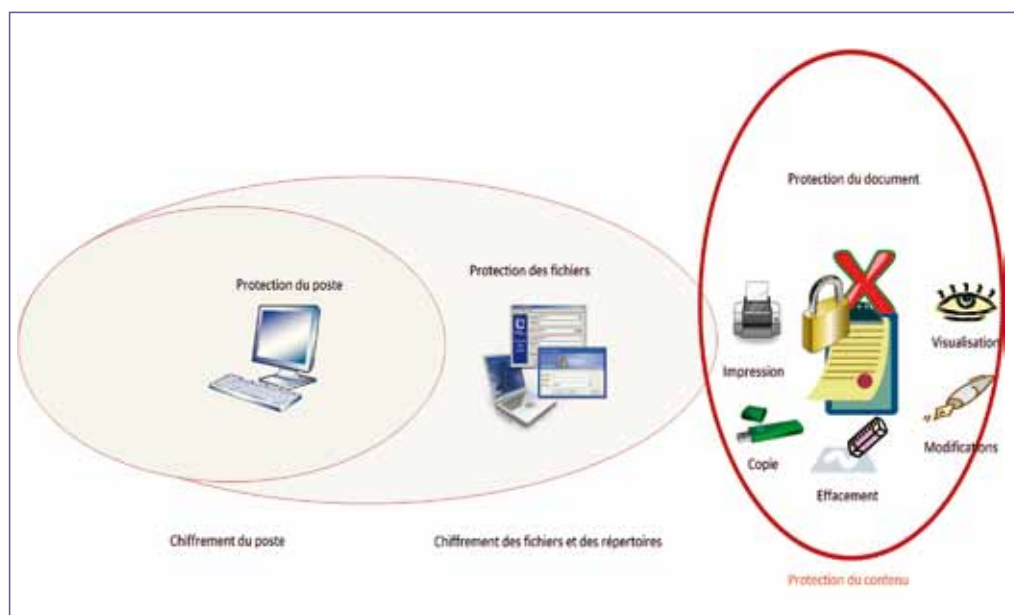
Aussi appelée protection de poste éteint, ces solutions permettent avant tout qu'un portable volé ou perdu ne puisse livrer le contenu de ses données. Une fois allumé et l'utilisateur authentifié, les données sont uniquement protégées par les droits d'accès délivrés par l'administrateur système.

- **Circulation confidentielle:** Ces données nécessitent une protection supplémentaire. Nous parlons alors de chiffrement au niveau fichier ou répertoire. Une telle solution permet une gestion séparée des accès, de sorte qu'un accès système et un accès chiffrement sont nécessaires pour accéder aux données. L'entreprise avisée doit prendre bien soin de séparer les fonctions de distribution des droits systèmes et de distribution des droits de chiffrement, voire de laisser cette dernière

sous la seule responsabilité des propriétaires des données. Si cette solution est robuste et permet une protection réelle contre l'espionnage ou une attaque ciblée, elle n'empêche pas l'employé indélicat de transmettre des données confidentielles à des tiers.

- **Circulation restreinte:** Ces données nécessitent une attention toute particulière et une protection sans faille qui puisse aussi fonctionner en dehors du contexte de l'entreprise; on parle ici de protection du contenu de façon dématérialisée. Ce mécanisme prend en compte différents paramètres comme le domaine pour lequel ce type de document a été validé (semblable à des groupes) mais aussi des paramètres temporels tels que la date ou l'heure. Ainsi, il est possible de définir une politique de contraintes (consommer uniquement si faisant partie du service développement de 8h à 20h en mode connecté et uniquement de 12h à 14h si en mode déconnecté) ou de consommation (contenu non visualisable avant le 1.4.2010 et pour une durée de 10 jours).

La mise en place d'une solution efficace de gestion des rôles et des accès (RBAC) associée à un chiffrement adapté aux différents niveaux de confidentialité des données est la seule réponse possible au piratage des données et la seule garante de la protection de la propriété intellectuelle d'une entreprise. Ce genre de projet devrait connaître une forte croissance au cours des deux prochaines années au vu de l'actualité sur les données informatiques. L'occasion fait le larron et si ces occasions sont moindres grâce à la mise en place de solutions techniques effectives, les entreprises auront rempli leur devoir de diligence. <



Les différents degrés de protection de documents Source: Fastcom Technology