Fiche solution ESG

Partage mobile de fichiers : le juste équilibre entre productivité, sécurité et contrôle

Date : mai 2015 **Auteur :** Terri McClure, analyste en chef

Résumé : la consumérisation de l'IT et le BYOD confrontent les services IT à un véritable dilemme : comment autoriser les employés à utiliser les terminaux de leur choix au travail sans compromettre la sécurité des données de l'entreprise ? Il est également de plus en plus difficile de satisfaire les exigences réglementaires alors que les données de l'entreprise sont éparpillées sur de multiples terminaux. Heureusement, certains éditeurs comme Acronis s'emploient à développer des solutions permettant à la fois aux salariés de travailler comme ils l'entendent et aux entreprises de respecter leurs obligations de conformité et de sécurité.

Contexte

L'informatique mobile n'est plus une simple tendance. Selon une étude ESG de 2014, 32 % des entreprises interrogées jugent la mobilité IT essentielle à leur activité et à la productivité de leur personnel, quand 55 % l'estiment très importante.[1] Les principales priorités des entreprises qui ressortent de cette étude consistent à contrôler leur environnement, à protéger leurs données et à favoriser la mobilité de leurs salariés, en parvenant à un juste équilibre entre les impératifs de sécurité et de productivité.

L'étude souligne également les difficultés qui accompagnent souvent l'adoption de l'IT mobile. Parmi les plus citées figurent la préservation de la confidentialité et de l'intégrité des données utilisées sur le réseau par des terminaux mobiles et de celles stockées sur des terminaux mobiles, et l'instauration des règles de sécurité pour les terminaux mobiles.

L'obligation de préserver la confidentialité et l'intégrité des données est particulièrement importante pour les entreprises des secteurs réglementés. L'étude menée en 2013 par ESG sur la synchronisation et le partage de fichiers d'entreprise (Enterprise File Sync and Share - EFSS) dans les environnements réglementés indique que 4 répondants sur 5 ont été audités au cours des 5 années précédentes, ⅓ à plus de 5 reprises, et qu'⅓ des entreprises auditées ont échoué à un audit au cours des 5 années précédentes. Le coût d'un audit négatif est variable selon le secteur, mais il peut se chiffrer en centaines de milliers de dollars en fonction de la gravité des manquements identifiés.[2]

Les solutions de protection du partage de fichiers et de la collaboration rencontrent ainsi un grand succès auprès des sociétés des secteurs réglementés, qui sont 46 % à avoir déployé des offres EFSS. Mais 60 % des sondés déclarent savoir ou suspecter que le personnel utilise des comptes d'EFSS personnels plutôt que ceux mis à disposition par la société.

[1] Source : rapport d'étude d'ESG, « *The State of Mobile Computing Security* », février 2014.
[2] Source : rapport d'étude d'ESG, « *OFS Considerations in Highly Regulated Industries* », juin 2013.

Et même si 92 % des entreprises découragent l'utilisation de comptes EFSS personnels, formellement ou non, près de 70 % des participants qui connaissent ou soupçonnent l'existence de cette pratique estiment probable que des données réglementées soient stockées sur des systèmes EFSS personnels.[3]

Les services IT des entreprises doivent impérativement s'emparer de ce problème, récupérer les données réglementées stockées sur des comptes personnels et sécuriser les données mobiles. Les employés y ont surtout recours pour gagner en productivité, pour accéder plus facilement aux fichiers et les partager via leurs terminaux mobiles. L'étude sur l'IT mobile démontre combien il est essentiel de trouver un juste équilibre entre contrôle, sécurité et productivité. Pour ce faire, les services IT doivent examiner attentivement les solutions de partage en ligne de fichiers et de collaboration afin de sélectionner celles qui conjuguent le mieux simplicité d'utilisation et moyens de contrôle.

Qu'attendent les utilisateurs d'une solution EFSS ?

Il existe sur le marché quantité de solutions EFSS qui prétendent allier la simplicité d'utilisation des offres grand public et la sécurité IT et les contrôles qu'exigent les entreprises. Mais qu'en est-il réellement ? La simplicité d'utilisation est un critère important, car si la solution EFSS est jugée trop compliquée, les utilisateurs continueront de lui préférer les alternatives grand public. ¼ des administrateurs d'environnements de partage de fichiers interrogés à l'occasion d'une autre étude ESG de 2014 constatent que les employés continuent d'utiliser leurs comptes EFSS personnels au travail même si l'entreprise a déployé une solution en interne.[4] Pourquoi ? Certainement parce que les solutions grand public sont plus simples à utiliser et que les utilisateurs savent comment elles fonctionnent.

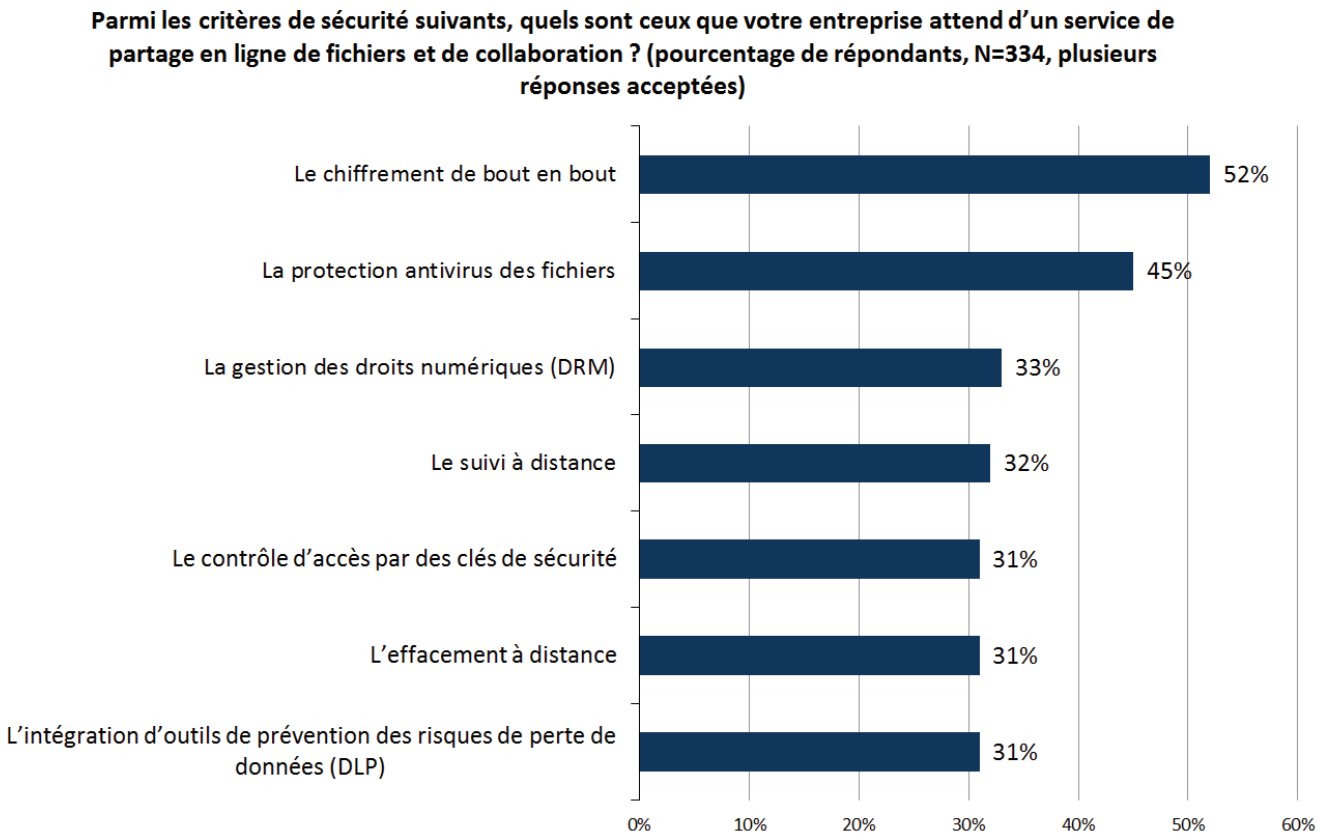
Cette étude s'est également intéressée aux critères que les professionnels IT attendent d'une solution EFSS, ses caractéristiques générales et plus spécifiquement ses fonctions de sécurité. Concernant les caractéristiques générales, les réponses obtenues soulignent majoritairement l'importance de la compatibilité de la solution avec les processus et workflows existants. Les trois premiers critères (chacun pour 31 % des répondants) sont que la solution s'intègre aux applications en place, qu'elle supporte la synchronisation entre plusieurs types de terminaux et qu'elle soit évolutive.[3] En 4ème position vient l'intégration aux logiciels et aux outils d'audit, autrement dit les préoccupations de responsabilité d'utilisation. Outre les exigences d'intégration, l'étude révèle que 97 % des sondés ayant déjà souscrit des solutions EFSS dans le Cloud souhaiteraient pouvoir conserver une partie, voire l'intégralité de leurs données sur site, d'une part pour garder le contrôle du stockage de leurs données, et d'autre part pour valoriser leurs investissements infrastructurels. Autrement dit, ils veulent une solution capable d'étendre leurs systèmes de fichiers (répertoires d'utilisateurs, serveurs de fichiers, SharePoint, etc.) à leur personnel mobile.

Mais quand ESG interroge les utilisateurs sur leurs critères de choix, la simplicité d'utilisation est l'une des 10 priorités citées par ¼ des sondés.[4] Pour résumer, une bonne solution EFSS est une solution qui peut s'intégrer à l'environnement IT existant, qui est auditable, qui est compatible avec différents types de terminaux et qui est suffisamment simple d'utilisation pour que les utilisateurs ne soient plus tentés de manipuler des données professionnelles avec leurs comptes personnels.

Mais quand on aborde la question de la sécurité, tout se complique ! Comment garantir à la fois la sécurité des données et la simplicité d'utilisation ? En effet, l'ajout de fonctionnalités de sécurité complique souvent l'environnement. Mais pour bien protéger les données EFSS, il faut au minimum des mécanismes de chiffrement pour éviter que quiconque intercepte les données et puisse les lire, un antivirus pour limiter les risques de contamination des nombreux utilisateurs qui vont se partager les données, et une clé de sécurité pour contrôler les accès et empêcher quiconque de déchiffrer les données (cf. Figure 1).[5] La liste est encore longue, mais les entreprises des secteurs réglementés qui sont soumises à des audits doivent assurément s'équiper d'outils de journalisation et de reporting de façon à prouver que les données n'ont pas pu être modifiées, consultées ou partagées sans autorisation.

[3] Source : Ibid.
[4] Source : Ibid.
[5] Source : Ibid.

FIGURE 1. Le Top 5 des critères de sécurité d'une solution EFSS



Source : Enterprise Strategy Group, 2015.

La difficulté est donc d'intégrer des fonctions de sécurité sans compliquer l'utilisation de la solution aux yeux des salariés, afin qu'ils cessent d'utiliser leurs comptes grand public. Il n'est pas question de choisir entre la facilité d'intégration des applications et des solutions de partage de fichiers sur site préexistantes, la convivialité et la sécurité. La solution doit réunir tous ces critères : s'intégrer aux environnements préexistants, être sûre et simple à utiliser, fonctionnelle, et permettre d'identifier qui accède aux données, comment et ce qu'il en fait. Malheureusement, peu d'offres satisfont actuellement l'ensemble des attentes des professionnels IT tout en restant suffisamment intuitives pour les utilisateurs.

Acronis Access Advanced : le juste équilibre entre contrôle, sécurité, conformité et productivité

La solution d'Acronis répond à ces critères. Elle est conçue pour s'intégrer à tous types d'environnements IT, y compris Active Directory. Elle offre aux administrateurs les caractéristiques de sécurité suivantes :

- Configuration de règles (pour limiter les conditions d'ouverture, d'affichage et de modification des fichiers par des applications spécifiques, par exemple).
- Création de liens sécurisés, à durée limitée.
- Restriction de la synchronisation ou de la mise en cache des fichiers sur les terminaux mobiles.
- Authentification bifactorielle par carte à puce (CAC/PIV).
- Conservation des données dans les systèmes de fichiers sur site existants, avec instauration d'un accès mobile.

Elle facilite la mise en conformité :

- Journaux d'audit.
- Chiffrement FIPS 140-2.

Elle stimule la productivité des utilisateurs :

- Clients simples d'utilisation, compatibles avec tous types de terminaux.
- Administration basée sur les rôles, confiée aux seuls experts des processus métier : les administrateurs de chaque service.
- Création et modification de documents Office et annotation de PDF au sein de l'environnement Acronis chiffré.
- Distribution de contenus par synchronisation unidirectionnelle, qui attribue automatiquement la dernière version des fichiers aux seuls utilisateurs autorisés.

Cette liste n'est pas exhaustive. Ce n'est qu'un échantillon des fonctionnalités d'Acronis Access Advanced pour aider les professionnels IT à trouver le juste équilibre entre productivité du personnel, sécurité et conformité.

Ce qu'il faut retenir

Les terminaux personnels étant désormais largement utilisés au travail, il n'y a rien d'étonnant à ce que les applications grand public envahissent les entreprises. Mais leur utilisation expose les informations confidentielles et sensibles à des risques, plus grands encore pour les entreprises appartenant à des secteurs réglementés. Les services IT n'ont donc d'autre choix que de déployer des solutions pour contrôler les accès et protéger les données.

Mais ils ne peuvent pas satisfaire les obligations de contrôle, de sécurité et de conformité au détriment de la productivité du personnel. Les services IT ont donc besoin de solutions suffisamment conviviales pour que les employés puissent se les approprier sans formation spécifique, à l'image des outils grand public qu'ils utilisent chez eux. Ces solutions doivent aussi embarquer tous les outils de sécurité essentiels à la protection des données internes des entreprises. Et pour les environnements réglementés, elles doivent proposer en plus des mécanismes de contrôle et d'identification pour restreindre l'accès aux données aux seuls utilisateurs autorisés, préserver l'intégrité des données et inclure des outils de reporting en cas d'audit.

Acronis l'a bien compris et propose une solution complète en réponse à l'ensemble de ces besoins, parfaitement adaptée aux environnements mobiles d'aujourd'hui, qui concilie sécurité et productivité.