Dépliant produit

opentext™

Masquage des données sensibles avec Reflection Desktop

La plupart des violations de confidentialité des données sont le fait de personnes de confiance, qu'il s'agisse d'un professionnel de santé qui vend des informations sur des célébrités à la presse à scandale, d'un employé de la comptabilité fournisseur qui modifie les informations de facturation de façon inappropriée ou d'un employé de banque qui transmet des numéros de sécurité sociale ou de carte de crédit volés à ses complices. De nos jours, il est parfois difficile de faire la différence entre un employé intègre et un fraudeur malhonnête.

Reflection Desktop en bref

- **Connectivité :**
  Connectez les utilisateurs de périphériques mobiles et d'ordinateurs de bureau aux systèmes de serveurs.
- **Facilité d'utilisation :**
  Faites en sorte que les applications serveurs soient aussi simples d'utilisation que les applications Office.
- **Facilité de gestion :**
  Gérez les configurations utilisateur en toute simplicité.
- **Sécurité :**
  Utilisez des couches de sécurité pour protéger les données en transit et au repos.

Ce dépliant produit explique comment le logiciel OpenText™ Reflection Desktop contribue à empêcher les violations de la confidentialité des données, sans rien changer aux applications serveurs.

Les utilisateurs internes malveillants, une menace difficile à combattre

Il est difficile de détecter les fraudes commises à l'intérieur de l'entreprise. Les contrôles classiques, centrés sur les moyens d'éviter les attaques qui viennent de l'extérieur, ne peuvent rien face aux utilisateurs internes bien informés qui disposent d'un accès autorisé aux données confidentielles.

Dès lors qu'un employé malhonnête ou mécontent possède les privilèges d'accès nécessaires, le risque de violation est important. Les chiffres les plus récents révèlent que les organisations américaines ont perdu 40 milliards de dollars à cause de vols et de fraudes commis par leurs employés. D'après le cabinet d'études de marché Forrester, 46 % d'environ 200 décisionnaires technologiques citent les failles de sécurité internes en tant que principal type de faille rencontré au cours de l'année écoulée, et la moitié d'entre eux indiquent que le responsable était un utilisateur interne malveillant.*

Pourquoi les organisations ne font-elles pas davantage pour se protéger ? La réponse est simple : modifier des applications serveurs bien établies pour améliorer leur niveau de sécurité est à la fois compliqué, risqué et coûteux. Même si vous avez la chance de croiser la route d'un expert qui comprend vos plates-formes mainframe, il est toujours hasardeux de toucher à la logique métier, conçue et améliorée au fil du temps, qui régit votre entreprise. Les coûts et les interruptions qui en découleraient seraient bien trop importants.

Une première étape simple

La question est de savoir comment protéger vos clients et votre entreprise sans remodeler les systèmes de serveurs et les processus métiers qui ont nécessité plusieurs décennies de développement. Comment pouvez-vous faire basculer votre entreprise dans le nouvel univers de la sécurité ?

En règle générale, cela nécessite d'ajouter des couches de sécurité. Cette excellente approche peut être mise en oeuvre en plusieurs étapes. Dans le monde du mainframe IBM et de l'AS/400, il existe une première étape simple à mettre en oeuvre : le masquage des données.

Le masquage des données permet d'empêcher les utilisateurs de visualiser les données sensibles sur un écran de serveur, de les recopier, de les prendre en photo, de les imprimer ou de les envoyer par message électronique. Les données sont masquées à l'écran en temps réel, de telle sorte que les employés ne voient jamais les adresses complètes, les dates de naissance, les numéros de carte de crédit, les numéros de sécurité sociale ou toute autre donnée privée. Les employés visualisent uniquement les données dont ils ont besoin pour effectuer leur travail.

Technologie de confidentialité des informations Reflection

Si vous êtes un client Reflection Desktop, vous disposez déjà de fonctionnalités de masquage des données à portée de main. La technologie de masquage des données d'OpenText™

*Keanini, TK. (2015). *Why insider threats are still succeeding. Information Age.* Extrait du 25 janvier 2016, source : **www.information-age.com/technology/security/123459548/why-insider-threats-are-still-succeeding**

Reflection Enterprise Suite vous permet de masquer facilement n'importe quel type de données sur les écrans de serveur, sans apporter de modifications côté serveur.

Cette technologie fait appel aux filtres de confidentialité et aux règles de numéro de compte principal (PAN) de l'outil de confidentialité des informations Reflection :

- **Filtres de confidentialité** : créez des filtres de confidentialité personnalisés pour masquer les données sur les écrans de serveur des applications mainframe IBM et AS/400. Vous pouvez également appliquer différentes règles à ces filtres pour masquer les données lorsqu'elles s'affichent, lorsqu'elles sont saisies et lorsqu'elles sont utilisées (impression d'écran, copier/coller et recopie visuelle [screen scraping] à l'aide d'API et de macros).
- **Règles PAN** : configurez Reflection pour masquer partiellement ou totalement un numéro de carte de crédit sur un écran de serveur en cochant les cases appropriées. Reflection Enterprise Suite utilise une technologie brevetée pour identifier et valider les PAN. Il utilise également l'algorithme Luhn pour garantir le masquage de tous les numéros de carte de crédit, indépendamment de l'emplacement et du mode d'affichage. Les utilisateurs et les administrateurs peuvent choisir parmi diverses options de contrôle, de la reconnaissance basique de carte de crédit aux personnalisations sophistiquées, en fonction de leurs besoins métiers.

Voici quelques exemples de tâches accomplies par les clients OpenText™ à l'aide des règles PAN et des filtres de confidentialité Reflection Enterprise Suite :

- masquer une colonne entière de données ;
- masquer des champs de données financières personnelles ;
- masquer les six derniers chiffres d'un champ de longueur variable ;
- masquer un champ de données qui apparaît à plusieurs endroits d'un même écran ;
- masquer des données en fonction d'instances conditionnelles de base (p. ex., selon les champs de données ou les identifiants d'écran) ;
- masquer des données en fonction d'instances conditionnelles complexes (p. ex., à l'aide de conditions de type « si », « alors » et « sinon ») ;
- masquer plusieurs PAN, notamment comportant des longueurs, des préfixes et des positions de tiret différents ;
- masquer des données affichées entre deux valeurs distinctes ;
- offrir des niveaux de visibilité variables selon le rôle ou la fonction de l'utilisateur.

Les capacités de masquage des données de Reflection Enterprise Suite sont supérieures à celles de tout autre client d'émulation de terminal. En outre, elles constituent également une solution à faible risque, facile à mettre en oeuvre. Pour en savoir plus sur la configuration de la confidentialité des informations à l'aide de Reflection Desktop, téléchargez le document suivant : **https://docs.attachmate.com/reflection/16.0/info-privacy.pdf**.

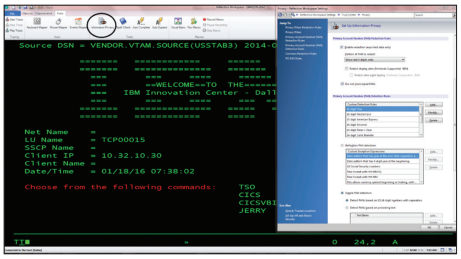

Figure 1. Les filtres et les règles sont stockés dans des fichiers. Vous pouvez donc facilement les gérer selon le rôle ou le groupe d'utilisateurs.

Modifier le paysage des menaces

Chaque organisation doit se confronter à cette dure réalité : elle héberge en son sein des personnes qui peuvent utiliser leurs droits d'accès privilégiés pour commettre des violations de confidentialité préjudiciables. Or, face à ces nouvelles menaces qui émanent d'utilisateurs internes toujours plus aguerris, les approches traditionnelles n'ont plus aucun effet. Votre stratégie de gestion des risques doit évoluer si elle veut être efficace.

Les capacités de masquage des données intégrées de Reflection Enterprise Suite constituent une étape facile à mettre en oeuvre, peu risquée et qui va dans le bon sens. Sans reconcevoir les applications serveurs, vous pouvez protéger les données et simplifier la conformité aux réglementations dans le même temps.

Pour en savoir plus, rendez-vous sur : **www.opentext.com**

Communiquez avec nous

Assurer la conformité aux normes PCI DSS

L'outil de confidentialité des informations Reflection ne s'arrête pas au simple masquage des données sur les écrans de serveur. En cochant les bonnes cases, vous pouvez exiger des connexions chiffrées sur tous les réseaux, y compris sans fil. Vous pouvez suivre la visualisation des numéros de carte de crédit par n'importe quel utilisateur et générer des rapports détaillés si nécessaire. Cet outil facilite ainsi la conformité aux normes PCI DSS. Pour en savoir plus, rendez-vous sur **www.attachmate.com/library/docs/advance-your-pci-compliance-with-reflection-desktop.html**.

261-FR0032-002 | O | 02/24 |