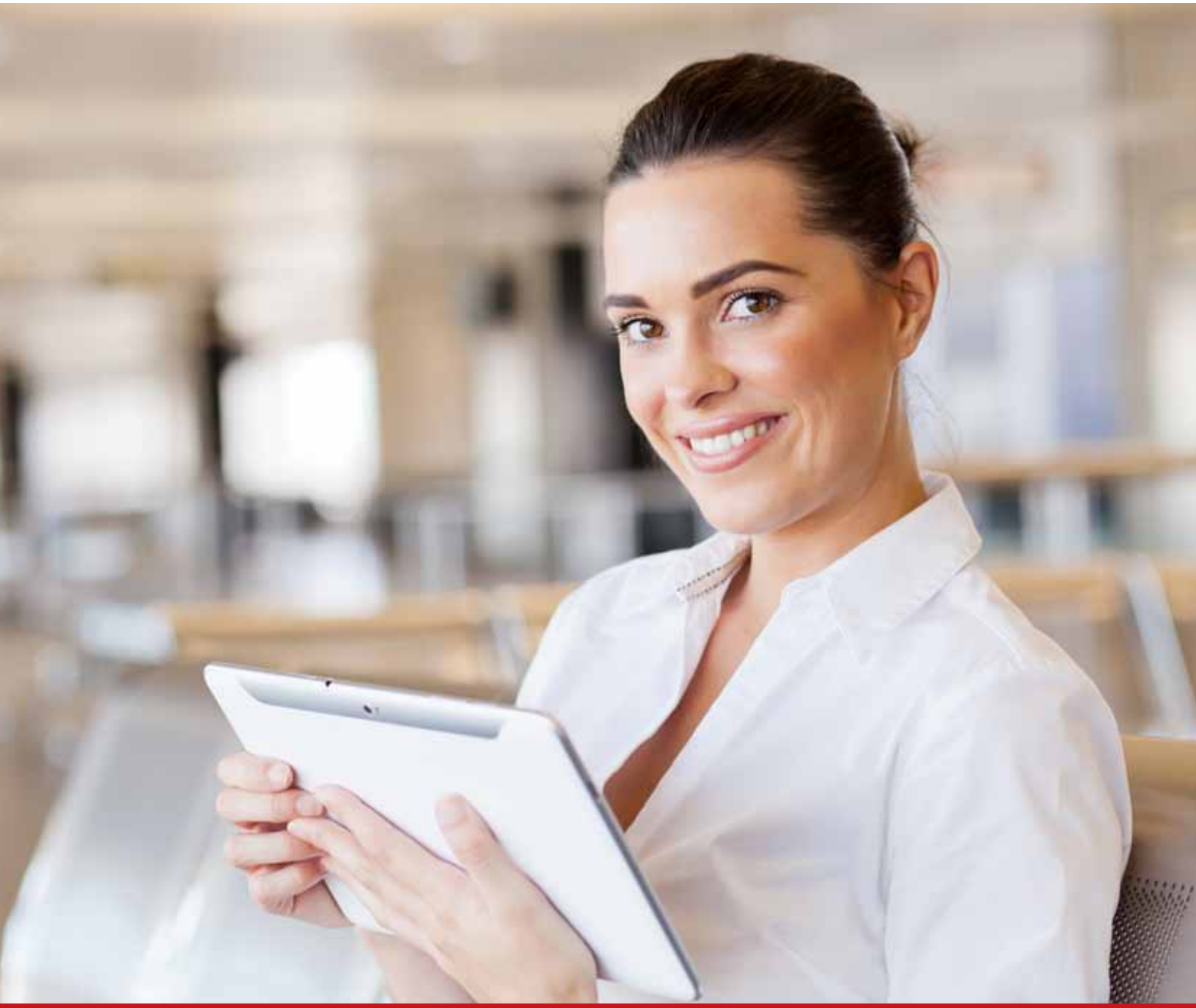
Centrify™



TOP 3

des raisons de donner une identité unifiée aux initiés

Même si le battage médiatique autour de la sécurité informatique concerne, pour la plupart, les pirates et autres attaques externes, les menaces internes peuvent être particulièrement insidieuses et dangereuses, qu'elles soient délibérées ou dues à la négligence d'un employé. Dans sa liste énumérant les huit menaces les plus importantes en matière de cybersécurité pour 2013, Forbes mentionne les menaces internes en n° 3, et remarque que les attaques internes peuvent être « les plus dévastatrices » en raison de l'importance des dommages que des utilisateurs privilégiés peuvent infliger et du type de données auquel ils ont accès.[1]

L'un des facteurs exacerbant les menaces internes est qu'elles peuvent passer inaperçues et échapper à toute détection pendant longtemps. Selon l'étude de Forbes, financée en partie par le ministère américain de la sécurité intérieure et les services secrets américains, il a fallu généralement près de 32 mois pour détecter des fraudes menées par des initiés malveillants dans le secteur financier. Et ce ne sont pas seulement des initiés malveillants qui créent ces risques. Les organisations doivent également se préoccuper de la surface d'attaque croissante dans leurs environnements, ainsi que des problèmes découlant du trop grand nombre de privilèges de leurs utilisateurs.

Il est extrêmement important que les cadres supérieurs et responsables de la conformité informatique se rendent compte du danger posé par des initiés malveillants, l'augmentation de la surface d'attaque et les violations possibles causées par des erreurs ou négligences d'employés. De même, il est essentiel que les organisations soutiennent le déploiement de solutions technologiques pouvant répondre à ces menaces dans l'ensemble de leurs entreprises, et permettant de les atténuer aussi rapidement que possible. Si elles ne prennent pas de mesures rapides, les organisations seront exposées à d'autres risques, et il sera encore plus difficile et coûteux de mettre en place des solutions efficaces.

1. « The Biggest Cybersecurity Threats of 2013 », Forbes, 5 déc. 2012
2. Ibid

Pourquoi mettre l'accent sur les menaces internes, et pourquoi maintenant ?

Plusieurs raisons

1. Les risques de sécurité interne sont plus fréquents et potentiellement plus préjudiciables :

Selon une étude du Ponemon Institute, 34 % des violations de données au Royaume-Uni sont dues à des actes malveillants, notamment de criminels travaillant de l'intérieur, et 37 % des violations sont dues à des négligences d'employés.[3] Une étude antérieure de Ponemon indiquait qu'un tiers des attaques malveillantes venait de criminels travaillant de l'intérieur.[4] Par ailleurs, une étude de Forrester a montré que 75 % des violations de données venaient d'initiés, le plus souvent en raison de négligence ou de manquement aux politiques. Les incidents les plus souvent cités concernent la perte de dispositifs, la mauvaise utilisation involontaire d'informations sensibles, et le vol intentionnel de données par des employés. [5] Les conséquences des violations de données et durées d'indisponibilité, en raison d'actes délibérés ou de négligence d'initiés, peuvent paralyser une organisation, l'exposer à une perte de revenus, porter préjudice à sa marque et donner lieu à des amendes et sanctions règlementaires coûteuses. Pour les organisations britanniques subissant des violations de données, chaque incident a coûté en moyenne plus de 2 millions de livres Sterling en 2012. [6]

2. Des « angles morts » dans l'identification des utilisateurs causent des échecs d'audit :

De nombreuses organisations ne réussissent pas leurs audits, en raison de lacunes dans leurs infrastructures d'identité. Ces « angles morts » peuvent se produire lorsque des identités et droits sont gérés de manière cloisonnée ou sur des serveurs locaux, plutôt que de manière centralisée. Par exemple, l'un des plus grands défis en matière d'identité pour les entreprises (et une cause majeure des échecs d'audit) est le manque de visibilité des comptes administrateurs locaux sous Windows. Cela correspond au compte racine sur un système Linux/Unix. Les échecs d'audit peuvent être tout particulièrement dommageables dans l'environnement actuel dans lequel les règlementations en matière de perte et de protection des données sont de plus en plus strictes dans le monde entier. Les entreprises exerçant des activités au niveau international doivent se conformer à un large éventail de règles et règlementations, pour satisfaire aux obligations en matière d'audit.

Les organisations doivent ainsi pouvoir fournir la preuve que les utilisateurs qui ont accès à certains serveurs et certaines applications disposent des autorisations nécessaires Elles doivent pouvoir fournir une piste d'audit vérifiable, indiquant ce que chaque utilisateur a fait dans le serveur. Ces obligations nécessitent que les politiques de l'organisation appliquent le principe du « moindre privilège », où les utilisateurs se connectent avec leur propre nom et ne disposent que des privilèges dont ils ont besoin pour faire leur travail. S'ils nécessitent un niveau de privilège supérieur (ce que l'on appelle une élévation de privilèges) pour quelque raison que ce soit, cela donne lieu à une action explicite.

3. Enquête de 2013 sur les coûts d'une violation de données, Ponemon Institute et Symantec, juin 2013
4. Enquête de 2010 sur les coûts d'une violation de données, Ponemon Institute et Symantec, mars 2011
5. « Most data breaches come from within », Info Security, 24 sept. 2012
6. Ibid., note de base de page n° 2

3. La complexité des organisations pose un problème croissant :

Avant, il était plutôt simple de gérer les identités des employés : un utilisateur était généralement assis à un bureau avec un seul ordinateur connecté à une application professionnelle, par un simple câble. Mais les choses ont bien changé. Les utilisateurs sont maintenant nomades et utilisent un large éventail de dispositifs, dont certains peuvent être des dispositifs personnels non approuvés ou non enregistrés. La mobilité est, par ailleurs, juste un seul aspect de cette complexité accrue. Les infrastructures informatiques sont de plus en plus diverses et hétérogènes, avec plusieurs silos définis par des services, applications, systèmes d'exploitation ou autres caractéristiques qui les distinguent les unes des autres. La prolifération des services de virtualisation et d'informatique dématérialisée ajoute un degré supplémentaire de complexité à l'environnement informatique. Sans une solution pour unifier les identités des utilisateurs, les organisations risquent d'avoir trop d'identités, ce qui augmente les risques associés, notamment la perte de données, les violations de données, l'indisponibilité des applications, les échecs d'audit et une incapacité d'identifier et de rectifier les problèmes de sécurité interne avant qu'ils ne s'aggravent.

Les responsables avisés des technologies de l'information et de la sécurité reconnaissent que la meilleure façon de relever ces défis avec efficacité et rentabilité, est d'intégrer une solution fournissant aux initiés une identité unifiée sur toutes les plates-formes. En associant les privilèges d'accès et les activités à des personnes spécifiques, l'organisation informatique peut établir le contrôle nécessaire pour minimiser les risques de sécurité, ainsi que la visibilité requise pour assurer la conformité.

Dans l'idéal, la solution de sécurité unifiée doit pouvoir prendre en charge des environnements hétérogènes, unifier toutes les politiques en matière d'identité (authentification, autorisation et audit), et permettre de centraliser la gestion des identités sur une seule console.

Les organisations peuvent également bénéficier d'avantages considérables en termes d'économies et de vitesse de déploiement, en tirant parti d'une solution d'identité unifiée en plus d'une plate-forme existante, comme Microsoft Active Directory. En raison de son omniprésence et de sa capacité de traiter une partie de la fonctionnalité sous-jacente de la gestion d'identité unifiée, Active Directory a de nombreux avantages :

Pourquoi donner aux initiés une identité unifiée ? Et quelles solutions vous permettent de réduire au mieux les coûts et les risques ? Voici les trois principales raisons de donner aux initiés une identité unifiée.

N° 1 Réduire le risque d'échecs d'audit, de menaces internes et d'autres violations de la sécurité.

Avant de déterminer comment l'utilisation d'une identité unifiée réduit les risques pour une organisation, décrivons tout d'abord ce que l'on entend par « identité unifiée », et comment cette identité doit être gérée dans toute l'entreprise.

Avec une identité unifiée, un initié dispose d'un seul identifiant sur les serveurs Windows, Linux et Unix. Les initiés peuvent accéder uniquement aux systèmes et applications dont ils ont besoin pour leur travail, et toutes leurs activités administratives doivent être liées à leur identité.

Pour avoir une identité unifiée, il est également nécessaire d'unifier les politiques d'authentification, d'autorisation et d'audit. L'organisation informatique doit avoir une visibilité complète de tous les systèmes auxquels chaque utilisateur a accès, ainsi que des privilèges élevés dont chaque utilisateur dispose dans chaque système. Elle doit également pouvoir vérifier entièrement ce que chaque utilisateur fait avec ces privilèges, jusqu'aux commandes exécutées et à la capture de sessions entières.

La capacité de créer une identité unifiée pour chaque utilisateur dans l'organisation et d'assurer, de manière centralisée, la gestion, la surveillance et l'audit des activités de chaque utilisateur, permet de réduire considérablement les risques d'échecs d'audit, les menaces internes et d'autres violations de la sécurité en :

- permettant une meilleure visibilité de votre niveau de risque ;
- identifiant des angles morts dans votre environnement de serveur, comme le manque de visibilité des comptes administrateurs locaux sous Windows ;
- assurant une gestion et une exécution cohérentes des politiques d'authentification, d'autorisation et d'audit dans l'ensemble de votre entreprise ; et
- donnant aux auditeurs des preuves de l'identité des personnes et des ressources auxquelles elles ont accès, ainsi que la façon dont elles ont utilisé cet accès.

N° 2 Réduire le coût total de possession en adoptant une approche simplifiée et normalisée en matière de gestion des risques liés à l'identité.

Les environnements informatiques sont de plus en plus hétérogènes, ce qui veut dire qu'ils peuvent être de plus en plus complexes. Vous ne pouvez pas simplement remplacer l'ensemble de votre infrastructure, mais vous pouvez relever les défis de gestion d'identité auxquels sont confrontés des environnements hétérogènes, en mettant en place une solution de gestion d'identité unifiée qui offre les fonctions et fonctionnalités suivantes :

- Prise en charge de toutes les plates-formes utilisées dans l'entreprise. C'est essentiel car, comme indiqué, la plupart des organisations sont très hétérogènes, et le même utilisateur est souvent connecté à plusieurs systèmes. Par exemple, vous voulez être en mesure de gérer des identités pour les plates-formes Windows, Mac, Unix et Linux à partir d'un seul endroit, en utilisant des politiques cohérentes et une identité d'utilisateur unifiée.

- Capacité de gérer de manière centralisée l'ensemble de la politique d'identité à partir d'une seule console pour la gestion des politiques, la surveillance, les audits et la déclaration de conformité.

- Capacité de tirer parti des investissements dans une infrastructure d'identité existante en déployant Active Directory. La gestion de l'infrastructure d'identité depuis un endroit centralisé, en se basant sur Active Directory, offre de nombreux avantages qui réduiront le coût total de possession, en particulier :

  - Pas besoin de remplacer l'ensemble de votre infrastructure de gestion d'identité existante.
  - Pas besoin que le service informatique investisse du temps, de l'énergie et de l'argent dans des formations pour apprendre à utiliser un nouveau système.
  - Pas besoin d'investir dans une toute nouvelle plate-forme.
  - Pas de temps perdu à passer vers une nouvelle plate-forme.
  - Retour sur investissement plus rapide en tirant parti des investissements déjà réalisés dans l'infrastructure d'identité.

En termes de coûts globaux, il est important que les professionnels des technologies de l'information et de la sécurité prennent en compte les coûts potentiels d'un échec d'audit et/ou d'une violation des données. Il est vrai que de nombreuses organisations ne passent pas leurs audits en raison de problèmes liés à la complexité de leurs infrastructures de gestion d'identité existantes, en plus de lacunes dans leurs procédures opérationnelles.

Les audits échouent lorsque l'organisation dispose de politiques incohérentes en matière de mot de passe, voire d'aucune politique, et ne peut donner aucune preuve quant aux personnes qui ont accédé à certaines applications, quels types de droits d'autorisation elles ont, et ce qu'elles ont réellement fait (ou pas) lorsqu'elles ont effectué une opération spécifique.

Avec la solution adaptée, l'organisation peut simplifier la gestion des identités des initiés, et prouver sa conformité sans problème, en mettant en place des politiques en matière de mot de passe, en fournissant des preuves de politiques pour les utilisateurs privilégiés, et en ayant une meilleure visibilité des contrôles d'accès. Il est fondamental que la visibilité, la surveillance et l'exécution viennent toutes d'une fonction de gestion centralisée et contrôlée par le service informatique.

Traditionnellement, la principale difficulté a été de gérer diverses plates-formes avec des politiques d'accès cohérentes, et, dans le cadre de centres de données, de les gérer en utilisant l'infrastructure existante. Gérer l'identité des utilisateurs à partir d'une seule console peut résoudre cette difficulté et permettre de contrôler de manière intégrée l'accès des utilisateurs et les audits sur toutes les plates-formes (Windows, Unix, Linux et autres) sur site ou sur le nuage.

N° 3 Soutenir de manière sécurisée les initiatives commerciales et informatiques de nouvelle génération.

Les entreprises ont besoin de solutions soutenant le déploiement des initiatives critiques favorisant la création d'applications de nouvelle génération. IDC décrit la combinaison des services dématérialisés, des réseaux sociaux, de la mobilité et des données volumineuses comme la prochaine plate-forme informatique d'envergure, qui tirera 80 % de la croissance entre aujourd'hui et la fin de la décennie. [7]

Chacune de ces initiatives peut toutefois amener de nouvelles menaces internes pour l'organisation. Comme le remarque Gartner :

L'ouverture des systèmes, informations et processus d'entreprise, favorisée par les réseaux sociaux, l'exposition à l'informatique dématérialisée, les dispositifs mobiles (en particulier, les dispositifs du grand public et les données volumineuses), amène avec elle un tout nouvel éventail de préoccupations en matière de sécurité et de protection de la vie privée... Les cybermilitants, le crime organisé et les États-nations intensifiant la pression, la sécurité des entreprises doit évoluer, en particulier, pour contrer le risque croissant des menaces internes et des attaques ciblées.[8]

Dans cet environnement, les organisations doivent pouvoir donner à leurs employés les moyens de tirer parti de ces initiatives, mais elles doivent le faire de manière à protéger l'entreprise de tous les dommages et risques potentiels et, dans une moindre mesure, des échecs d'audit ou de la perte de revenus/opportunités en raison de problèmes causés par des menaces internes.

Cela nécessite une infrastructure d'identité modulable, simple à gérer et de plus en plus dynamique, afin de permettre le soutien sécurisé des nouvelles initiatives professionnelles à l'échelle de l'entreprise. En tirant parti des investissements existants et en se concentrant sur une politique d'identité unifiée, les organisations pourront apporter leur soutien aux utilisateurs initiés tout en :

- tirant parti d'un bon investissement dans la gestion d'identité unifiée ;
- continuant de tirer parti de la gestion d'identité sécurisée comme ressource stratégique à l'avenir ; et
- protégeant les investissements et en éliminant le risque d'impasses, tout en adoptant des initiatives de nouvelle génération.

7. « IDC Predicts 2012 Will Be the Year of Mobile and Cloud Platform Wars as IT Vendors Vie for Leadership While the Industry Redefines », IDC, 1er déc. 2011
8. « The Nexus of Forces Changes Everything », thème central de Gartner Symposium/ITxpo 2012, 10 jan. 2013

Aller de l'avant

Il existe des arguments clairs et convaincants en faveur d'une identité unifiée : réduction du coût total de possession, réduction du risque de violation des données, réduction du risque d'échecs d'audit, une infrastructure d'identité plus agile, un retour sur investissements plus rapide et un soutien des initiatives commerciales de nouvelle génération. L'une des premières mesures à prendre pour aller de l'avant est de travailler avec un fournisseur partenaire qui comprend exactement les défis et les opportunités présentés par la gestion d'identité unifiée.

Centrify est clairement leader du marché de la gestion d'identité unifiée, et offre une solution complètement intégrée regroupant la consolidation d'identité, l'authentification, l'identification unique, l'exécution de politiques de groupe, la gestion des privilèges et les audits sur l'éventail de plates-formes le plus large du secteur, sur site et dans le nuage. Centrify intègre des systèmes et applications hétérogènes dans un environnement informatique sécurisé et connecté, centré autour d'Active Directory.

La Centrify Server Suite simplifie la gestion, l'exécution et la visibilité des risques liés à l'identité (qu'ils soient anticipés ou non), en offrant une infrastructure d'identité unifiée avec une seule identité pour les utilisateurs et une seule infrastructure d'identité pour le service informatique. La suite de Centrify couvre plus de 400 plates-formes différentes, et n'est pas intrusive pour l'infrastructure Active Directory existante. Aucune modification schématique n'est nécessaire et aucun logiciel ne doit être installé sur des contrôleurs de domaine.

Si votre organisation n'a pas réussi un audit de sécurité ou n'a pas pris les mesures adaptées pour relever le défi des menaces internes, il est plus que jamais temps de vous lancer, avant que ces risques ne se concrétisent. Voulez-vous en savoir plus ? Veuillez contacter Centrify.

À propos de Centrify

Centrify offre des services d'identité unifiée pour centre de données, nuage et mobile, avec une seule identification pour les utilisateurs et une seule infrastructure d'identité pour le service informatique. Les solutions de Centrify réduisent les coûts et renforcent l'agilité et la sécurité en tirant parti de l'infrastructure d'identité existante d'une entreprise, afin de centraliser l'authentification, le contrôle d'accès, la gestion des privilèges, l'exécution des politiques et la conformité. Les clients de Centrify réduisent généralement leurs coûts associés à la gestion du cycle d'identité et à la conformité, de plus de 50 pour cent. Avec plus de 5 000 clients dans le monde, dont 40 pour cent des entreprises du Fortune 50 et plus de 60 agences fédérales, Centrify est déployé sur plus d'un million de ressources de serveur, d'application et de dispositif mobile, sur site et dans le nuage. Pour de plus amples informations sur Centrify et ses solutions, rendez-vous sur **http://www.centrify.com/.**