

Une étude de NetIQ confirme l'impact croissant de la sécurité sur la gestion des environnements Active Directory

Les solutions NetIQ offrent une automatisation proactive de la sécurité et de l'administration d'Active Directory

HOUSTON – 19 août 2009 – L'implémentation d'une administration efficace de Microsoft Active Directory est indispensable pour permettre aux directions informatiques de prendre en charge les besoins évolutifs et dynamiques de leurs entreprises. Une récente étude conduite par NetIQ Corporation révèle également l'importance stratégique de la sécurité et identifie les différents défis auxquels se heurtent les administrateurs lorsqu'il s'agit de sécuriser les environnements Active Directory. Face au développement continu de cette technologie dans les entreprises, la sécurisation des ressources métier critiques hébergées dans Active Directory doit devenir une nouvelle priorité.

Selon cette étude approfondie, menée sur un échantillon de plus de 275 personnes, la [gestion des stratégies de groupes](#), la [maintenance des habilitations](#) et la [démonstration de conformité](#) restent les trois principaux challenges entourant l'administration et la sécurité d'Active Directory. Les départements fonctionnels expriment les mêmes préoccupations, 52 % des personnes interrogées désignant l'application des politiques comme première problématique métier et 42 % les problèmes de non-conformité – faisant de la sécurité un challenge de première priorité. De plus, 76 % des participants considèrent aujourd'hui l'administration d'Active Directory comme un composant critique ou important de leurs stratégies de gestion des accès et des identités.

Pour plus d'un sondé sur deux, le contrôle des changements et des accès non-autorisés aux informations sensibles pose des risques particulièrement sérieux pour les équipes en charge des opérations et de la sécurité informatiques. L'incapacité de l'entreprise à détecter les changements, à maîtriser la configuration et à annuler rapidement les habilitations pourraient aggraver considérablement les vecteurs de risque. Pour y faire face, les départements informatiques doivent assurer l'application effective des politiques, minimiser les privilèges des utilisateurs et [contrôler les changements non-autorisés](#) – intentionnels ou non – sur l'ensemble de l'environnement Active Directory.

L'étude dresse d'autres constats instructifs :

- 40 % des personnes interrogées soulignent la difficulté à maintenir les ressources Active Directory en phase avec les besoins métier.
- Pour 85 % des participants, l'environnement Active Directory est géré par les équipes en charge des technologies informatiques, pour 12 % par un département dédié de sécurité et pour 3 % par des éditeurs externes.
- 49 % des sondés estiment que la sécurité a eu, au cours des trois dernières années, une influence croissante sur la politique et/ou l'architecture Active Directory dans leur entreprise.
- Seuls 24 % considèrent leur entreprise bien armée pour détecter les changements non-autorisés dans l'environnement Active Directory.



« Aujourd'hui, Active Directory joue un rôle majeur dans les entreprises et il ne fait aucun doute que les menaces et les risques continueront à se multiplier. Les départements informatiques doivent donc redéfinir leurs systèmes d'administration d'Active Directory pour y inclure la sécurité et la conformité s'ils veulent répondre parfaitement aux besoins de leur entreprise, indique Erin Avery, Directeur Marketing Produit de NetIQ. A travers l'institutionnalisation et l' [automatisation de la sécurité](#) et des contrôles internes dans le cadre de la gestion quotidienne d'Active Directory, les départements informatiques parviendront à une meilleure maîtrise des coûts de conformité – pour, à terme, optimiser l'adéquation aux besoins de l'entreprise. »

À propos de NetIQ

NetIQ, une Business Unit de la société Attachmate, est un leader des solutions globales de gestion et d'administration des systèmes et de la sécurité. Fortes de plus de 12000 clients dans plus de 60 pays et de 12 années d'expérience, les solutions de NetIQ aident les Directions Informatiques à maîtriser les services critiques, à réduire les risques opérationnels et à documenter leur conformité aux stratégies d'entreprise. Le portefeuille de solutions primées de NetIQ couvre notamment l'administration et la supervision des systèmes et de la sécurité, le contrôle des configurations et du changement, l'automatisation des processus IT et la gestion des communications unifiées.

Pour plus d'informations, consultez www.netiq.com

Contact presse : Attachmate NetIQ
Hugues Burghard
hugues.burghard@attachmate.com
Tél: 01 46 04 10 10

###

Copyright © 2009 NetIQ Corporation. Tous droits réservés NetIQ, le logo NetIQ sont des marques ou des marques déposées de NetIQ Corporation aux États-Unis et dans d'autres pays. Tous les autres noms de marques, noms commerciaux ou noms d'entreprises mentionnés ne sont utilisés qu'à des fins d'identification et sont la propriété de leurs détenteurs respectifs.