Étude de cas : Amélioration de la gouvernance des identités et des accès dans le secteur manufacturier grâce à RAC/M Identity™

OKIOK

RAC/M IDENTITY

Contexte

Notre client est un acteur majeur dans l'industrie de la fabrication de pâte à papier, avec une vaste présence à travers les Etats-Unis et le Canada. Avec des dizaines de milliers d'employés répartis sur une centaine de sites, la gestion de la gouvernance des identités et des accès était devenue un défi complexe. Les processus manuels pour les demandes d'accès prenaient non seulement beaucoup de temps, mais entraînaient également des retards, des incohérences, des problèmes de conformité, des risques de sécurité et une augmentation des coûts opérationnels.

Défis

Paysage identitaire complexe

Avec une main-d'œuvre diversifiée répartie sur de nombreux sites, la gestion des identités des employés et des droits d'accès qui leur sont associés était devenue complexe et sujette aux erreurs.

Paysage technologique hybride

L'infrastructure informatique existante est très hétérogène et s'appuie fortement sur la technologie des ordinateurs centraux et des mini-ordinateurs, ainsi que sur des applications classiques sur site, tout en étant en cours de transition vers une architecture informatique moderne, basée sur le SaaS.

Demandes d'accès manuelles

Le processus manuel de demande d'accès existant nécessitait beaucoup de travail et entraînait des retards dans l'octroi ou la révocation de l'accès, ce qui nuisait à la productivité des employés et à la conformité.

Risques pour la sécurité

L'incohérence des pratiques de gestion des identités et des accès a suscité des inquiétudes en matière de sécurité, car l'accès inapproprié à des systèmes et à des données sensibles a accru le risque de violations de données et de menaces internes.

Coûts opérationnels

L'inefficacité des processus manuels a entraîné une augmentation des coûts opérationnels en raison du volume élevé d'interventions de l'équipe informatique et d'un manque de rationalisation des processus.

Questions de conformité

En l'absence de modèle d'accès formel, de flux de travail d'approbation et de processus de revue des accès, il était pratiquement impossible de garantir la conformité avec les politiques de l'entreprise, ainsi qu'avec les exigences légales et réglementaires.

La solution : RAC/M Identity™

Notre client a choisi RAC/M Identity comme la meilleure solution de gouvernance et d'administration des identités (IGA) pour répondre à ses défis en matière de gouvernance des identités et des accès. Le déploiement visait à rationaliser les processus de demande d'accès, à appliquer des contrôles d'accès cohérents et à réduire les coûts opérationnels grâce à l'automatisation.

Mise en œuvre d'un modèle d'accès global basé sur les rôles à l'échelle de l'entreprise

Pour régler le problème du manque d'uniformité du contrôle d'accès et rationaliser le processus de demande et d'approbation d'accès, notre client a fait appel à OKIOK qui, à titre de partenaire stratégique, a mis à sa disposition une équipe d'experts de premier plan ayant une longue expérience de la mise en œuvre réussie de processus améliorés de gestion de l'accès à l'information dans de grandes organisations telles que des banques et des services publics.

Pour ce client, la mission consistait à concevoir et à mettre en œuvre un modèle d'accès complet, structuré et basé sur les rôles, adapté au paysage organisationnel et technique complexe de l'organisation.

Le projet a nécessité des centaines d'ateliers organisés avec des représentants de chaque entité sur une période de plusieurs mois. Le projet a été un grand succès, le modèle d'accès a été livré et mis en œuvre progressivement, dans le respect du calendrier et du budget.

Définir et mettre en œuvre des milliers de règles d'affaires, y compris des règles SOD

En étroite collaboration avec OKIOK, notre client s'est lancé dans une ambitieuse initiative visant à améliorer sa posture de gouvernance des accès. Des milliers de règles d'affaires, y compris des règles de séparation des tâches essentielles, ont été définies pour s'assurer que les droits d'accès sont accordés et gérés conformément aux meilleures pratiques et aux exigences de sécurité tout au long du cycle de vie de l'identité.

Objectif essentiel : Automatiser plus de 90 % des opérations de demande d'accès

L'un des objectifs essentiels de notre client était d'automatiser plus de 90 % de toutes les demandes d'accès. Le but était de réduire les coûts, les efforts et les erreurs résultant des opérations manuelles de gestion des accès. En automatisant les demandes d'accès, notre client visait à éliminer les délais, à augmenter la productivité et à améliorer la satisfaction des employés.

Automatisation des processus critiques du cycle de vie de l'identité

Au-delà des demandes d'accès, notre client a également reconnu l'importance de l'automatisation des processus critiques du cycle de vie de l'identité, y compris l'arrivée, le départ et les mouvements latéraux. En automatisant ces processus, l'organisation visait à minimiser les erreurs, à assurer la cohérence et à rationaliser les transitions des employés.

Résultats obtenus

Réduction des coûts

L'automatisation réussie de plus de 90 % des demandes d'accès a permis de réaliser d'importantes économies en réduisant les tâches manuelles et les frais généraux.

Efficacité et productivité

La mise en œuvre d'un modèle d'accès efficace basé sur les rôles, de demandes d'accès automatisées et de processus de cycle de vie de l'identité a permis de rationaliser les processus d'arrivée et départ, de minimiser les délais et d'améliorer la productivité et la satisfaction des employés.

Réduction des erreurs et des risques

La combinaison d'un modèle d'accès basé sur les rôles et de l'automatisation a également réduit la probabilité d'erreurs dans l'attribution des accès, garantissant que les employés disposent des accès appropriés tout en réduisant les risques liés à l'excès de privilèges.

Amélioration de la conformité

La rationalisation des processus de GIA critiques, la mise en œuvre de flux d'approbation et de résolution formels ainsi que l'application efficace des règles de séparation des tâches améliorent considérablement la posture de sécurité et garantissent la conformité avec le cadre de gouvernance du client.

Les utilisateurs ont rapidement accès aux ressources informatiques dont ils ont besoin en fonction de leur rôle et de leurs responsabilités.

Les campagnes de revue d'accès peuvent être définies et menées au niveau de granularité et à la fréquence souhaitée, en fonction de la criticité des identités humaines et impersonnelle, du niveau des privilèges et des actifs informatiques.

Conclusion

Le partenariat entre notre client et OKIOK, ainsi que les capacités de la solution RAC/M Identity, ont permis de transformer avec succès, la gouvernance des identités et des accès.

En automatisant plus de 90 % des demandes d'accès et des processus critiques du cycle de vie de l'identité, notre client a atteint son objectif stratégique et obtenu des avantages substantiels en termes de réduction des coûts, d'amélioration de l'efficacité et de réduction des erreurs et des risques.

La combinaison d'une relation de partenariat entre le client et OKIOK, d'objectifs stratégiques clairs, d'un leadership et de conseils d'experts, ainsi que d'une technologie souple et avancée, a permis de mettre en place un processus de gestion des identités et des accès plus sûr, plus conforme et plus efficace sur le plan opérationnel.

OKIOK

Pour plus d'informations sur le RAC/M Identity et sur les avantages qu'il peut apporter à votre organisation, veuillez consulter notre site Web à l'adresse www.okiok.com ou contacter notre équipe de vente à l'adresse sales@okiok.com.