



Customer Success

Nedbank

Des outils traditionnels à une gouvernance pointue des identités

Introduction

Nedbank est l'un des quatre plus grands groupes bancaires d'Afrique du Sud qui propose des services bancaires de gros et de détail. Elle a été l'une des premières banques du continent africain à mettre en place des services bancaires sur Internet. L'importance qu'elle accorde à la sécurité numérique lui a permis d'atteindre l'un des taux de fraude les plus bas parmi ses concurrents.

Challenge

La sécurité devenait un fardeau. L'accumulation de solutions patrimoniales et mainframe sur une technologie numérique plus récente devenait laborieuse à gérer et créait des inefficacités qui laissaient place à des risques potentiels. La fourniture d'accès aux utilisateurs était complexe et la demande en ressources informatiques devenait insupportable. Lorsque la situation a été portée à l'attention de l'équipe dirigeante, la gouvernance des identités chez Nedbank est devenue une priorité absolue.

Solution

- Soutenir la transformation numérique de la banque avec une solution de gouvernance des identités qui évolue avec l'entreprise.
- Réduire la charge du personnel informatique qui accorde et certifie les accès.
- Fournir aux utilisateurs un accès plus rapide aux applications et aux données.



Nedbank est une banque sud-africaine qui emploie plus de 33 000 personnes. L'entreprise s'efforce d'aider ses clients à concrétiser leur vision de l'entreprise et à saisir des opportunités grâce à des solutions sur mesure. En 2018, nous avons décerné à Nedbank le prix SailPoint Customer Impact Award. Ce prix récompense les clients pour leur stratégie de gestion des identités qui a eu un impact direct sur l'entreprise et a donné lieu à des résultats concrets. Nous sommes très fiers du travail acharné accompli par Nedbank pour arriver là où elle est aujourd'hui, et nous la félicitons pour son succès. Cet article relate son aventure dans la gestion des identités et les processus qu'elle a mis en place pour générer des résultats probants grâce à une plate-forme de gestion des identités.

Les environnements hérités pèsent sur les équipes IT et les utilisateurs

Les institutions financières disposent souvent de solutions héritées et d'ordinateurs centraux (mainframe). Avec le temps, la technologie s'accumule sur ces systèmes hérités, devenant de plus en plus difficiles à maintenir et à gérer. À mesure que de nouvelles fonctionnalités s'ajoutent, les coûts de maintenance augmentent et l'environnement devenant de plus en plus complexe finit par nuire à l'efficacité. Pour mettre en place un programme de gestion des identités sûr et efficace, Nedbank a dû procéder à de gros changements.

Nedbank rencontrait plusieurs problèmes de gestion des identités au sein de l'entreprise. Des rôles d'identité et des autorisations ont été ajoutés en fonction des besoins de chaque projet. Le nombre de rôles a ainsi proliféré à un rythme effréné ; c'est ce qu'on

appelle souvent « l'explosion des rôles ». L'absence d'une visibilité claire sur les accès entre les équipes et les rôles spécifiques en raison de la disparité des systèmes et de la dépendance à l'égard d'anciens outils obsolètes est devenue la principale préoccupation pour la banque. Par ailleurs, le niveau de complexité technique requis pour accorder et certifier les accès ne permettait pas aux responsables des activités d'assumer la responsabilité des accès de leurs équipes. Nedbank se devait de mieux connaître les accès définis pour chaque rôle et ce qui était réellement attribué.

En plus de cela, les demandes, dont s'occupaient deux informaticiens qui connaissaient les couches des systèmes et leur interaction, devenaient également ingérables. Il était difficile de transmettre au nouveau personnel les années de connaissances que ces deux personnes avaient accumulées en prenant part à

“ Si vous ne renforcez pas les contrôles autour d'un accès non autorisé, vous augmentez le risque potentiel. Avec SailPoint, nous avons réduit les risques financiers et sécurité pour l'entreprise en sachant qui a accès aux applications et aux fichiers.

Louise van Schalkwyk

Head: Centre for Access Governance
Nedbank

de nombreux projets et les différentes couches de sécurité des applications. « Il y a quelques années, une équipe avait ajouté des fonctionnalités à une plate-forme de services client, ce qui a donné un accès supplémentaire à 35 rôles. Par inadvertance, ils ont tenté d'attribuer des capacités de dérogation de crédit aux agents du centre d'appels. Cela fut le signal d'alarme pour nous », a déclaré Louise van Schalkwyk, responsable du Centre pour la gouvernance des accès chez Nedbank.

Cet environnement informatique complexe ainsi que l'immense pression réglementaire visant à sécuriser les informations précieuses des clients dans le secteur des services financiers, ont poussé Louise van Schalkwyk à faire part de la situation à l'équipe de direction de Nedbank. Ils ont reconnu que les systèmes disparates les laissaient sans couche de protection et qu'il devenait nécessaire d'adopter une plate-forme de gouvernance des identités cohérente et moderne en investissant dans le programme de sécurité de l'entreprise.

Investir dans l'avenir

La solution de SailPoint est devenue la base de leur programme de gouvernance des identités, qui allait bientôt atténuer les difficultés liées à l'octroi des accès, fournir un parcours et un historique clairs des approbations des accès et offrir à l'entreprise une solution permettant de construire et de faire évoluer son empreinte numérique. De ce programme est également né le Centre pour la gouvernance des accès (Centre for Access Governance, CAG) de Nedbank, un service dirigé par Louise van Schalkwyk. Le CAG fait le lien entre la configuration opérationnelle et technique du programme de gestion des identités.

Louise van Schalkwyk a entrepris d'intégrer SAP, le système de gestion RH, afin de piloter toutes les activités en aval et de mettre en œuvre des capacités de provisioning et de désactivation des accès, pour servir de base à la stratégie de gouvernance des identités qui allait évoluer en même temps que la banque. Avant d'utiliser SailPoint, Nedbank menait des campagnes de certification manuelles dans son environnement hérité, qui sont aujourd'hui remplacées par des examens trimestriels automatisés des accès dans SailPoint. Depuis sa mise en œuvre, 92 % des droits examinés ont été soit approuvés, soit révoqués. « Les examinateurs des accès ont indiqué qu'avec SailPoint, la certification des accès est devenue rapide et facile à gérer », a déclaré Louise van Schalkwyk. Environ 200 utilisateurs par mois subissent un changement d'accès, et en général l'accès à certaines applications et données est désactivé.

« En fournissant un accès par l'intermédiaire de SailPoint, nous avons vu le temps nécessaire pour configurer l'accès initial des employés aux systèmes et aux données se réduire considérablement. Avant, il fallait six semaines pour que les employés soient opérationnels ; aujourd'hui, ils le sont en un seul jour. Cela apporte une énorme valeur ajoutée. » À mesure que le nombre d'applications embarquées sur SailPoint augmente, une capacité est créée pour la réaffectation des effectifs et des capacités à d'autres fonctions de sécurité. Nedbank a désormais une meilleure visibilité sur les accès dont dispose son personnel et continue de préciser ce qui est nécessaire pour chaque fonction, garantissant ainsi un système avec des privilèges minimums.

Un autre résultat du programme est l'amélioration de l'expérience des utilisateurs. « L'interface utilisateur de SailPoint est simple, épurée et conviviale. Nous savions que cela améliorerait instantanément l'expérience des employés et des managers, en particulier dans le cas d'un provisioning direct », a déclaré Louise van Schalkwyk.

Du point de vue de la sécurité, le processus des fins de contrat de Nedbank s'est considérablement amélioré pour atteindre une automatisation totale. Depuis la mise en œuvre de SailPoint, les scripts manuels ne cessent de diminuer : nous n'avons plus besoin de créer de rapports et de supprimer manuellement l'accès des employés.

Le CAG continue à évoluer et à améliorer les processus de bout en bout sous la direction de Louise van Schalkwyk. « Mon équipe a passé beaucoup de temps à gérer ces changements et à élaborer le matériel de formation pour permettre au personnel et aux managers de comprendre l'importance du programme de gestion des identités et les aider à adopter cet outil. Dans les grandes entreprises, le CAG permet de maintenir l'attention sur le risque et l'atténuation des risques, en particulier pour les accès non autorisés ».

Protection des données au sein de l'entreprise

Ces derniers temps, la gestion et la sécurité des données sont devenues une priorité pour Nedbank. « Nous devons protéger les données non structurées qui traînent sur les partages de fichiers et les autres sites de l'entreprise. Nous avons étendu notre programme de gouvernance des identités pour aider les propriétaires de données à sécuriser l'accès à leurs données. Pour moi, contrôler les accès aux données dans le cadre de notre plate-forme de gestion des identités unique et intégrée représente une plus-value inestimable. » SailPoint permet à Nedbank de gérer activement les accès aux partages et aux fichiers et d'éviter qu'ils ne deviennent obsolètes.



À propos de SailPoint

La capacité de gérer et de sécuriser les identités aujourd'hui a largement dépassé les capacités humaines. SailPoint, le leader de la gouvernance des identités fournit une approche innovante de la sécurité des identités et des accès dans les entreprises. Grâce à l'intelligence artificielle et au Machine Learning, la plateforme de sécurité des identités de SailPoint fournit toujours le niveau d'accès approprié. Les entreprises actuelles, même orientées cloud, peuvent s'assurer que chacun dispose de l'accès exact dont il a besoin, au bon moment. Les solutions intelligentes SailPoint, autonomes et intégrées placent la sécurité des identités au cœur des opérations commerciales en ligne. SailPoint permet ainsi aux organisations les plus complexes d'établir une base de sécurité capable de se défendre contre les menaces les plus pressantes d'aujourd'hui, partout dans le monde.

© 2022 SailPoint Technologies, Inc. Tous droits réservés. SailPoint, le logo SailPoint et toutes les techniques sont des marques commerciales ou des marques déposées de SailPoint Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Tous les autres produits ou services sont des marques commerciales de leurs entreprises respectives.