

Une gestion des identités et des accès ajustée contre la fraude

Un assureur en France met en place une gestion efficace des identités qui permet de répondre trois fois plus vite aux requêtes d'audit

L'essentiel

Entreprise

Natixis Assurances Métiers Non Vie (NAMNV)

Secteur

Assurance

Pays

France

Site Web

assurances.natixis.com

Les défis

NAMNV voulait se protéger contre la fraude interne. Pour y parvenir, l'entreprise devait améliorer sa gestion des habilitations et de recertification ainsi qu' améliorer sa capacité à créer des rapports.

Resultats

À présent, ce fournisseur d'assurances peut répondre trois fois plus vite aux requêtes d'audit pour renforcer sa conformité et dispose de données sur la gestion des identités et des accès (IAM) bien plus précises pour se protéger contre la fraude.

Produits

Identity Manager

Password Manager

Aujourd'hui, la fraude constitue une menace croissante aux multiples facettes pour toutes les entreprises.

En France, selon une étude récente conduite par Euler Hermes, l'un des principaux organismes européens de lutte contre la fraude, "80 pourcents des entreprises en France ont subi au moins un cas de tentative de fraude".

Les entreprises du secteur de l'assurance sont davantage exposées au risque que les autres dans la mesure où elles manipulent de grands volumes de données financières sensibles. Dans ce contexte, Natixis Assurances Métiers Non Vie (NAMNV), assureur français, a décidé de minimiser ce qui lui apparaissait comme sa principale vulnérabilité : la fraude interne, souvent facilitée par des pratiques insuffisantes en matière de gestion des identités et des accès.

NAMNV fait partie de Natixis Assurances, la filiale de services bancaires - investissement et entreprises - d'assurance et de services financiers du Groupe BPCE, le deuxième groupe bancaire de France comptant plus

“Avec One Identity Manager, toute incohérence dans le flux de travail peut être facilement identifiée et les vérifications techniques peuvent se faire à la demande, ce qui signifie que nous sommes mieux protégés contre la fraude.”

Adrien Bertrand, administrateur sécurité des systèmes d'information et chef de projet IAM



de 36 millions de clients. Sa mission consiste à assister les conseillers bancaires en matière de solutions d'assurance, à gérer les contrats d'assurance et à créer des solutions d'assurances distribuées dans le réseau du Groupe BPCE. NAMNV compte plus de 250 salariés dédiés à l'assistance des conseillers bancaires, plus de 600 autres dans ses centres de télégestion à Bordeaux et des équipes dans les fonctions administratives, de conformité et de comptabilité.

Une nouvelle identité

NAMNV effectuait auparavant la gestion des identités et des accès (IAM) avec des tableurs Microsoft Excel dont les mises à jour étaient prises en charge manuellement par son équipe informatique. Cette approche ne permettait pas à l'informatique de faire un suivi fiable des requêtes et il fallait plus d'une semaine pour créer le profil d'un utilisateur. Ces lenteurs, combinées au contexte général de fraude tel que le décrit l'étude d'Hermès, ont convaincu NAMNV de revoir complètement son IAM en interne.

L'entreprise a identifié plusieurs objectifs à atteindre avec sa nouvelle solution. Afin de réduire le risque de fraude interne, NAMNV voulait

superviser et automatiser les processus de gestion de cycle de vie des utilisateurs - origine, habilitation et recertification - et mettre en place des flux de gestion enrichis. Elle cherchait aussi à obtenir des rapports plus complets avec un suivi à la demande des données pour répondre aux requêtes fréquentes de ses auditeurs internes. Enfin, NAMNV tenait à automatiser et mettre à jour ses processus tels que la recertification pour libérer le temps de l'équipe informatique en donnant aux managers opérationnels davantage de visibilité et de contrôle.

Étape suivante : le choix de la solution adéquate

Une fois établi son cahier des charges pour la solution d'IAM idéale, l'entreprise a évalué les offres de différents fournisseurs. La solution de One Identity, incluant Identity Manager et Password Manager, s'est distinguée. Son architecture utilise des bases de données ouvertes et s'intègre facilement aux environnements Windows virtualisés, ce qui réduit les délais de déploiement car aucun serveur supplémentaire n'est nécessaire pour traiter les tâches - deux avantages majeurs pour NAMNV. La solution offre de plus des fonctionnalités clés, dont le

suivi des requêtes, la création des profils, la recertification et une visibilité complète des habilitations. En résumé, la solution a doté NAMNV d'un moyen plus rigoureux, efficace et transparent de gérer et d'assurer la gouvernance des identités et des accès.

Une occasion saisie

Grâce à la solution de One Identity, l'équipe de NAMNV dispose désormais de données précises et détaillées à portée de main. Adrien Bertrand, administrateur sécurité des systèmes d'information et chef de projet IAM, indique: “Avec One Identity Manager, toute incohérence dans le flux de travail peut être facilement identifiée, ce qui signifie que nous sommes mieux protégés contre la fraude.”

L'entreprise peut également répondre trois fois plus vite aux requêtes en plus de la part des auditeurs grâce aux capacités renforcées de reporting essentielles à une conformité plus solide. De plus, il est possible de faire le suivi et des extractions de données à la demande pour répondre à des requêtes spécifiques.

Une attente clé de NAMNV consistait à inclure les

managers opérationnels dans le processus d'habilitation. C'est maintenant chose faite avec Identity Manager qui donne aux managers une visibilité complète des droits d'accès des membres de leurs équipes, ainsi que la possibilité de gérer ces droits sur tout le cycle de vie utilisateur. La solution a rencontré un beau succès puisque 100 pourcents des managers l'ont adoptée.

Pour Adrien Bertrand, l'architecture prête pour l'avenir est simple à administrer: "Nous aimons le fait qu'Identity Manager soit une solution prête à l'emploi et nous apprécions la gouvernance des habilitations qu'elle permet. Même quand plusieurs applications sont intégrées à la solution, elle reste simple à gérer. Ça fonctionne, tout simplement!"

À propos de One Identity

La gamme de solutions de gestion des identités et des accès (IAM) de One Identity offre un IAM adapté au terrain qui inclut des solutions prêtes pour l'avenir, intégrées, modulaires et axées sur les opérations pour gérer la gouvernance des identités, les accès et les privilèges.

Learn more: [OneIdentity.com](https://www.oneidentity.com)