



Ricoh Cloud Services renforce la sécurité d'AWS pour FrieslandCampina



- Amélioration de la protection et de la sécurité des données
- Amélioration des capacités de conformité et d'audit
- Gestion simplifiée des utilisateurs et des contrôles d'accès

L'ENTREPRISE ET SES DÉFIS

FrieslandCampina est une entreprise laitière mondiale de premier plan basée aux Pays-Bas. Fondée en 2008 par la fusion de Friesland Foods et de Campina, l'entreprise a une longue histoire qui remonte à plus de 150 ans. Elle produit une large gamme de produits laitiers, notamment du lait, du fromage, du beurre, du yaourt et des aliments pour nourrissons, sous des marques bien connues telles que Friso, Dutch Lady et Landliebe. FrieslandCampina est présente dans plus de 100 pays, au service des consommateurs, des entreprises et de l'industrie alimentaire.

FrieslandCampina héberge sur AWS de nombreuses applications critiques, notamment pour la gestion des stocks, le contrôle de la production, le suivi de la chaîne d'approvisionnement et les opérations de vente. Au fur et à mesure que l'utilisation d'AWS par l'entreprise augmente, le risque de violation de la sécurité ou d'attaque s'accroît également. À la suite d'un audit de sécurité interne, un certain nombre de domaines ont été identifiés comme devant être améliorés :

- L'un des principaux défis à relever était l'absence d'une protection robuste des sauvegardes. L'entreprise s'appuyait sur AWS Backup pour protéger ses données critiques, mais ses sauvegardes étaient vulnérables aux suppressions accidentelles ou malveillantes en raison de mécanismes de protection insuffisants. Cela représentait un risque sérieux pour la continuité de l'activité en cas d'attaques par ransomware ou d'erreur humaine.
- En outre, les buckets S3 de l'organisation, qui stockaient de grandes quantités de données sensibles, ne bénéficiaient pas dans tous les cas de l'option.



- La dernière sécurité AWS fournie par la protection au niveau de l'objet, laissant certaines données de l'entreprise exposées au risque de modifications ou de suppressions non autorisées. Étant donné que l'entreprise dépend de ces données pour ses activités quotidiennes, ces vulnérabilités devaient être corrigées.
- La mise à jour des bases de données constituait un autre défi. Leurs bases de données Microsoft SQL Server étaient essentielles pour la gestion des données de production et de vente, mais le processus manuel de mise à jour des correctifs de sécurité prenait beaucoup de temps et était source d'erreurs. Les retards dans l'application des correctifs exposaient l'organisation à d'éventuelles menaces de sécurité.
- Outre ces problèmes, l'entreprise a été confrontée à des défis en matière de gestion des identités et des contrôles d'accès. Sa base d'utilisateurs, répartie sur plusieurs sites et systèmes, nécessitait une intégration plus étroite entre Microsoft Azure Active Directory (AD) sur site et AWS Identity Center. Le manque d'intégration compliquait la gestion des utilisateurs et affaiblissait le contrôle d'accès.
- Enfin, les responsables informatiques de l'entreprise manquaient de visibilité sur les niveaux d'accès des utilisateurs et les vulnérabilités des systèmes. Ils ne disposaient d'aucun mécanisme fiable pour générer des rapports automatisés sur l'accès des utilisateurs aux systèmes d'exploitation et aux bases de données, et ne pouvaient pas non plus suivre facilement l'état de santé général et la posture de sécurité de leur environnement AWS.



Les améliorations de la sécurité AWS mises en œuvre par Ricoh Cloud Services ont aidé Friesland-Campina à relever ses défis en matière de sécurité tout en optimisant son environnement AWS. Ces améliorations ont posé des bases solides pour la croissance future et l'innovation numérique de l'entreprise, en veillant à ce que son infrastructure cloud AWS reste sécurisée.





SOLUTION

Dans son rôle de fournisseur de services gérés AWS pour FrieslandCampina, Ricoh Cloud Services a livré un programme de renforcement de la sécurité pour atténuer les risques identifiés par l'organisation. Le projet comprenait sept éléments clés visant à améliorer la protection des données, la sécurité opérationnelle et la visibilité de l'environnement cloud de l'entreprise.

1. Introduction à AWS Backup Vault Locks :

Pour sécuriser les sauvegardes de l'organisation, Ricoh Cloud Services a mis en place les verrous AWS Backup Vault. Cette fonctionnalité a ajouté une couche de protection supplémentaire en empêchant toute suppression ou modification des sauvegardes pendant une période de rétention prédéfinie. Ainsi, même en cas d'activité malveillante ou de suppression accidentelle, les sauvegardes restent intactes et récupérables. Ces serrures de chambre forte ont aidé l'entreprise à se conformer à ses politiques de reprise après sinistre et à ses exigences réglementaires.

2. Verrouillage des objets dans le S3 Bucket :

Pour améliorer l'intégrité des données, les verrous d'objets des godets S3 ont été configurés pour empêcher la suppression ou la modification des fichiers critiques. En appliquant des politiques de conservation au niveau des objets, l'entreprise pouvait s'assurer que les données importantes ne pouvaient pas être modifiées pendant une période donnée. Cette fonctionnalité s'est avérée particulièrement utile pour les dossiers financiers de l'organisation, les journaux de production

et d'autres données sensibles nécessitant une conservation et une intégrité à long terme.

3. Corrections des bases de données Microsoft SQL Server à l'aide d'AWS Gestionnaire de systèmes (SSM) :

Pour automatiser et rationaliser les correctifs des bases de données, Ricoh Services gérés a configuré SSM Patch Manager pour appliquer automatiquement les correctifs de sécurité critiques aux serveurs de base de données MS SQL Server dans le cadre des correctifs mensuels automatisés, réduisant ainsi l'erreur humaine et garantissant que l'environnement reste sécurisé. Un rapport de conformité des correctifs a également été mis en place, donnant à l'organisation une visibilité en temps réel sur l'état des correctifs de ses bases de données.

4. Intégration de Microsoft Azure Active Directory avec AWS Identity Center :

Pour centraliser la gestion des utilisateurs et rationaliser l'identité et les contrôles d'accès, Microsoft Azure Active Directory a été intégré à AWS Identity Center. Cela a permis aux utilisateurs de s'authentifier de manière transparente avec leurs identifiants Azure AD existants pour accéder aux ressources AWS. L'authentification unique (SSO) a été activée, ce qui a simplifié la gestion des accès tout en renforçant la sécurité en appliquant l'authentification multifactorielle (MFA) et le contrôle d'accès basé sur les rôles (RBAC).

5. Rapport automatisé sur les niveaux d'accès des utilisateurs au système d'exploitation et à la base de données :

Ricoh Cloud Services a mis en place un reporting automatisé pour suivre et auditer l'accès des utilisateurs aux systèmes



d'exploitation et aux bases de données sur l'ensemble des instances EC2 de l'environnement AWS de FrieslandCampina. AWS Systems Manager, CloudWatch et Lambda ont été utilisés pour générer des rapports mensuels sur les niveaux d'accès des utilisateurs. Ces rapports automatisés ont permis de garantir la conformité avec les politiques internes et les réglementations externes, en fournissant une piste d'audit pour tout incident de sécurité potentiel.

6. Mise en place d'un tableau de bord AWS Trusted Advisor :

Enfin, pour assurer une visibilité permanente de l'environnement AWS de l'organisation et de son niveau de sécurité, Ricoh Cloud Services a mis en place un tableau de bord AWS Trusted Advisor. Ce tableau de bord surveille des domaines clés tels que la sécurité, les performances, l'optimisation des coûts et la tolérance aux pannes. En examinant régulièrement les recommandations du Trusted Advisor, l'entreprise a pu rapidement identifier et corriger les failles de sécurité, les inefficacités en termes de coûts ou les ressources peu performantes.

LES AVANTAGES

Grâce à ce programme, l'entreprise fonctionne désormais avec un dispositif de sécurité considérablement renforcé, avec des avantages particuliers dans les domaines suivants :

1. Amélioration de la protection des données :

L'introduction des verrous AWS Backup Vault et des verrous S3 bucket object a fourni à l'organisation une protection critique

pour ses sauvegardes et ses données sensibles. Les espaces de sauvegarde et les objets de stockage étant protégés contre la suppression ou la modification, le risque de perte de données due à des actions accidentelles ou malveillantes a été réduit au minimum. Cette amélioration a permis d'améliorer directement la planification de la continuité des activités et de garantir la conformité avec les réglementations en matière de conservation des données.

2. Une sécurité accrue grâce à l'automatisation :

L'automatisation des correctifs des bases de données à l'aide d'AWS SSM a éliminé l'intervention manuelle dans l'application des correctifs, réduisant ainsi le risque d'erreur humaine et comblant plus rapidement les vulnérabilités en matière de sécurité.

En conséquence, l'organisation a connu moins de cas de bases de données non corrigées, garantissant que les systèmes critiques restent protégés contre les dernières menaces de sécurité. Cette automatisation a également permis de libérer des ressources informatiques pour des tâches plus stratégiques.

3. Gestion simplifiée des utilisateurs et contrôle d'accès :

En intégrant Microsoft Azure AD à AWS Identity Center, l'entreprise a obtenu un contrôle centralisé de l'accès des utilisateurs. Grâce au SSO et au MFA, les utilisateurs ont pu accéder en toute sécurité aux ressources AWS sans avoir à gérer des identifiants distincts, ce qui a simplifié la charge de travail de l'équipe informatique et amélioré la sécurité d'accès. Cette intégration a également permis de s'assurer que les politiques de contrôle d'accès étaient appliquées de manière cohérente dans l'ensemble de l'organisation.

4. Amélioration des capacités de conformité et d'audit :

La conception et la mise en œuvre de rapports automatisés pour les niveaux d'accès au système d'exploitation et à la base de données ont fourni à l'organisation un outil d'audit puissant. Cette fonction a permis des examens réguliers de l'accès des utilisateurs, garantissant la conformité avec les politiques internes et les normes réglementaires.

5. Surveillance proactive :

Le tableau de bord AWS Trusted Advisor a donné à l'organisation une vue d'ensemble de son environnement AWS, permettant l'identification proactive des risques de sécurité potentiels, des goulets d'étranglement en matière de performances et des possibilités de réduction des coûts. La possibilité d'agir sur les recommandations du Trusted Advisor a permis à l'entreprise d'optimiser en permanence ses opérations dans le nuage tout en maintenant des niveaux élevés de sécurité et de performance.

En résumé, les améliorations de la sécurité AWS mises en œuvre par Ricoh Cloud Services ont aidé FrieslandCampina à relever ses défis en matière de sécurité tout en optimisant son environnement AWS. Ces améliorations ont posé des bases solides pour la croissance future et l'innovation numérique de l'entreprise, en veillant à ce que son infrastructure cloud AWS reste sécurisée.

À PROPOS DE RICOH

Ricoh est un fournisseur de premier plan de services numériques intégrés et de solutions d'impression et d'imagerie conçues pour soutenir la transformation digitale des lieux de travail, des espaces de travail et optimiser les performances de l'entreprise. Basée à Tokyo, l'activité mondiale de Ricoh touche des clients dans environ 200 pays et régions, grâce à des connaissances, des technologies et des capacités organisationnelles cultivées au cours de ses 85 ans d'histoire. Au cours de l'exercice clos en

mars 2025, le groupe Ricoh a réalisé un chiffre d'affaires mondial de 2 527 milliards de yens (environ 14,5 milliards d'euros). La mission et la vision de Ricoh sont de permettre aux individus de trouver l'Epanouissement par le travail en comprenant et en transformant la façon dont les gens travaillent afin de libérer leur potentiel et leur créativité pour réaliser un avenir durable. Pour de plus amples informations, veuillez consulter le site : www.ricoh.fr.

RICOH
imagine. change.

www.ricoh.fr

Les faits et chiffres mentionnés dans cette brochure concernent des projets spécifiques. Des circonstances individuelles peuvent produire des résultats différents. Tous les noms de sociétés, marques, produits et services appartiennent à leurs propriétaires respectifs et sont des marques déposées par ceux-ci. Copyright © 2025 Ricoh Europe PLC. Tous droits réservés. Toute modification et/ou adaptation et/ou reproduction, en partie ou en intégralité, et/ou insertion dans d'autres travaux de la présente brochure, de son contenu et/ou de sa mise en page sans l'accord écrit de la société Ricoh Europe PLC est interdite.