Ricoh Cloud Services Enhancement of AWS Security for FrieslandCampina

- Improved data protection and security
- Enhanced compliance and auditing capabilities
- Simplified user management and access controls

COMPANY & CHALLENGE

FrieslandCampina is a leading global dairy company based in the Netherlands. Founded in 2008 through a merger of Friesland Foods and Campina, the company has a long history dating back over 150 years. It produces a wide range of dairy products, including milk, cheese, butter, yogurt, and infant nutrition, under well-known brands like Friso, Dutch Lady, and Landliebe. FrieslandCampina operates in over 100 countries, serving consumers, businesses, and the food industry.

FrieslandCampina hosts many mission-critical applications, including inventory management, production monitoring, supply chain tracking, and sales operations, on AWS. As the organisation’s usage of AWS grows, so too does the risk of security breach or attack. Following the completion of an internal security audit, a number of areas were ear-marked for enhancement:

- One of the key challenges was the lack of robust backup protection. The company relied on AWS Backup to protect critical data, but their backups were vulnerable to accidental or malicious deletion due to insufficient protection mechanisms. This posed a serious risk to business continuity in the event of ransomware attacks or human error.
- Additionally, the organisation’s S3 buckets, which stored vast amounts of sensitive data, were not in all cases availing of

the latest AWS security provided by object-level protection, leaving some company data at risk of unauthorised changes or deletion. Given the company's reliance on this data for daily operations, these vulnerabilities needed to be addressed.

- Database patching was another challenge. Their Microsoft SQL Server databases were critical for managing production and sales data, but the manual process of keeping them up-to-date with security patches was both time-consuming and error-prone. Delays in applying patches left the organisation exposed to potential security threats.
- In addition to these issues, the company faced challenges in managing identity and access controls. Its user base, distributed across multiple locations and systems, required tighter integration between the on-premises Microsoft Azure Active Directory (AD) and AWS Identity Center. The lack of integration complicated user management and weakened access control.
- Lastly, the company's IT leadership lacked visibility into user access levels and system vulnerabilities. They had no reliable mechanism for generating automated reports on user access to operating systems and databases, nor could they easily track the overall health and security posture of their AWS environment.

> The AWS security enhancements implemented by Ricoh Cloud Services have helped FrieslandCampina to address its security challenges while optimising its AWS environment. These improvements laid a strong foundation for the company's future growth and digital innovation, ensuring that its AWS cloud infrastructure remains secure.

SOLUTION

In its role as AWS Managed Service provider to FrieslandCampina, Ricoh Cloud Services delivered a programme of security enhancements to mitigate the risks identified by the organisation. The project consisted of seven key deliverables aimed at improving data protection, operational security, and visibility into the company's cloud environment.

1. Introduction of AWS Backup Vault Locks:

To secure the organisation's backups, Ricoh Cloud Services implemented AWS Backup Vault locks. This feature added an additional layer of protection by preventing any deletion or modification of backups for a predefined retention period. This ensured that even in the event of malicious activity or accidental deletion, backups remained intact and recoverable. These vault locks helped the company comply with their disaster recovery policies and regulatory requirements.

2. S3 Bucket Object Locks:

For enhanced data integrity, S3 bucket object locks were configured to prevent the deletion or modification of critical files. By enforcing object-level retention policies, the company could ensure that important data could not be altered for a specified time period. This feature was particularly useful for the organisation's financial records, production logs, and other sensitive data that required long-term retention and integrity.

3. Microsoft SQL Server Database Patching Using AWS Systems Manager (SSM):

To automate and streamline database patching, Ricoh Cloud Services configured SSM Patch Manager to automatically apply critical security patches to MS SQL Server database servers as part of automated monthly patching, reducing human error, and ensuring the environment remained secure. Patch compliance reporting was also set up, giving the organisation real-time visibility into the patch status of its databases.

4. Integration of Microsoft Azure Active Directory with AWS Identity Center:

To centralise user management and streamline identity and access controls, Microsoft Azure Active Directory was integrated with AWS Identity Center. This allowed users to seamlessly authenticate with their existing Azure AD credentials to access AWS resources. Single sign-on (SSO) was enabled, simplifying access management while enhancing security by enforcing multi-factor authentication (MFA) and role-based access control (RBAC).

5. Automated Reporting of Operating System and Database User Access Levels:

Ricoh Cloud Services implemented automated reporting to track and audit user access to operating systems and databases across all EC2 instances in the FrieslandCampina

AWS environment. AWS Systems Manager, CloudWatch, and Lambda were used to generate monthly reporting on user access levels. These automated reports helped ensure compliance with internal policies and external regulations, providing an audit trail for any potential security incident.

6. Implementation of an AWS Trusted Advisor Dashboard:

Finally, to provide ongoing visibility into the organisation's AWS environment and its security posture, Ricoh Cloud Services set up an AWS Trusted Advisor dashboard. The dashboard monitored key areas such as security, performance, cost optimisation, and fault tolerance. By regularly reviewing Trusted Advisor recommendations, the company could quickly identify and address any security vulnerabilities, cost inefficiencies, or underperforming resources.

BENEFITS

As a result of this programme, the company now operates with a significantly enhanced security posture, with particular benefits achieved in the following areas:

1. Improved Data Protection:

The introduction of AWS Backup Vault locks and S3 bucket object locks provided the organisation with critical protection for its backups and sensitive data. With backup vaults and bucket objects secured against deletion or modification, the risk of data loss due to accidental or malicious actions was minimised. This enhancement directly improved business continuity planning and ensured compliance with data retention regulations.

2. Increased Security Through Automation:

Automating database patching using AWS SSM eliminated manual intervention in applying patches, reducing the potential for human error and closing security vulnerabilities faster. As a result, the organisation experienced fewer instances of unpatched databases, ensuring that critical systems remained protected against the latest security threats. This automation also freed up IT resources for more strategic tasks.

3. Simplified User Management and Access Control:

By integrating Microsoft Azure AD with AWS Identity Center, the company gained centralised control over user access. With SSO and MFA in place, users could securely access AWS resources without managing separate credentials, simplifying the IT team's workload and improving access security. This integration also ensured that access control policies were enforced consistently across the entire organisation.

4. Enhanced Compliance and Auditing Capabilities:

The design and implementation of automated reporting for operating system and database access levels provided the organisation with a powerful auditing tool. This feature enabled regular reviews of user access, ensuring compliance with internal policies and regulatory standards.

5. **Proactive Monitoring:**

The AWS Trusted Advisor dashboard gave the organisation a bird's-eye view of its AWS environment, enabling proactive identification of potential security risks, performance bottlenecks, and cost-saving opportunities. The ability to act on Trusted Advisor recommendations allowed the company to continuously optimise its cloud operations while maintaining high levels of security and performance.

In summary, the AWS security enhancements implemented by Ricoh Cloud Services have helped FrieslandCampina to address its security challenges while optimising its AWS environment. These improvements laid a strong foundation for the company's future growth and digital innovation, ensuring that its AWS cloud infrastructure remains secure.

ABOUT RICOH

Ricoh is a leading provider of integrated digital services and print and imaging solutions designed to support digital transformation of workplaces, workspaces and optimise business performance. Headquartered in Tokyo, Ricoh's global operation reaches customers in approximately 200 countries and regions, supported by cultivated knowledge, technologies, and organisational capabilities nurtured over its 85-year history. In the financial year ended March 2024, Ricoh Group had worldwide sales of 2,348 billion yen (approx. 15.5 billion USD). It is Ricoh's mission and vision to empower individuals to find Fulfilment through Work by understanding and transforming how people work so we can unleash their potential and creativity to realise a sustainable future. For further information, please visit www.ricoh-europe.com

RICOH
imagine. change.

www.ricoh-europe.com

The facts and figures shown in this brochure relate to specific business cases. Individual circumstances may produce different results. All company, brand, product and service names are the property of and are registered trademarks of their respective owners.