



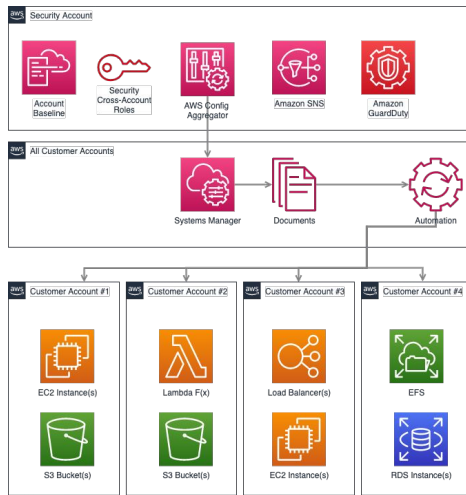
AutoProtect provides insurance products and dealer warranties to vehicle manufacturers and retailers of all types throughout the UK, Europe and globally. **AutoProtect** hosts their applications in a hybrid environment including on-premises and AWS Cloud.

Cloud Challenge

As a data-driven organisation, AutoProtect creates multiple Amazon S3 buckets in order to store customer data. With more than 8.5TB in 80+ Buckets, managing and securing this data became a challenge, more so when new products and features are in testing or validation phases.

StackZone Engagement

AutoProtect participated in a Well Architected Day by nubeGo which highlighted several areas that could be improved according to a comparison against AWS recommend best practices. With 30+ recommendations, they decided to engage with **StackZone** to implement Governance and start building a framework which could be relied on for future growth. By adopting AWS Config and SSM Automation documents, **StackZone** enabled a fully compliant, automated S3 data protection system.



Tools Used

- The entire **StackZone** solution is based on AWS CloudFormation, including but not limited to creating new accounts, deploying IdP for SSO, creating IAM Policies and using Service Catalog with Add-On Solutions. A set of core accounts are created and SCP Organizations are applied to OUs depending on the customer's choice. In addition to CloudFormation, the solution uses AWS Lambda, StepFunctions, CodePipeline and CodeBuild.
- The solution is deployed in multiple regions depending on the customer choice.
- From a security perspective, more than 100 AWS Config rules are applied to every account and aggregated into the security account.
- The **StackZone** solution can help save time by automating the set-up of an environment for running secure and scalable workloads while implementing an initial security baseline through the creation of core accounts and resources. It also provides a baseline environment to get started with a multi-account architecture, identity and access management, governance, data security, network design, and logging.

Realised Benefits

During **StackZone's** onboarding phase, **AutoProtect** found many of their buckets didn't have versioning enabled, and doing it manually would have taken valuable time which they invested in keep building the product. Also, making sure no bucket has public read and writes ensure the data stored in there remains secured and encrypted using AES-256. AWS Config allows **AutoProtect** to continuously audit and assess the overall compliance of the AWS resources configurations with the organization's policies and best practices.

Do you want to take your cloud to **next level?**

Contact Us



“ Relying on an automated security remediation solution gave us the confidence and to build trust across the different areas of the organisation when building new products. ”

Ian Gatley, Chief Technology Office

