CASE
STUDY

Security Assessment and Architecture Implementation on GCP Ensures Secure Product Deployments for Multinational Retail Giant

softserve

Client Background

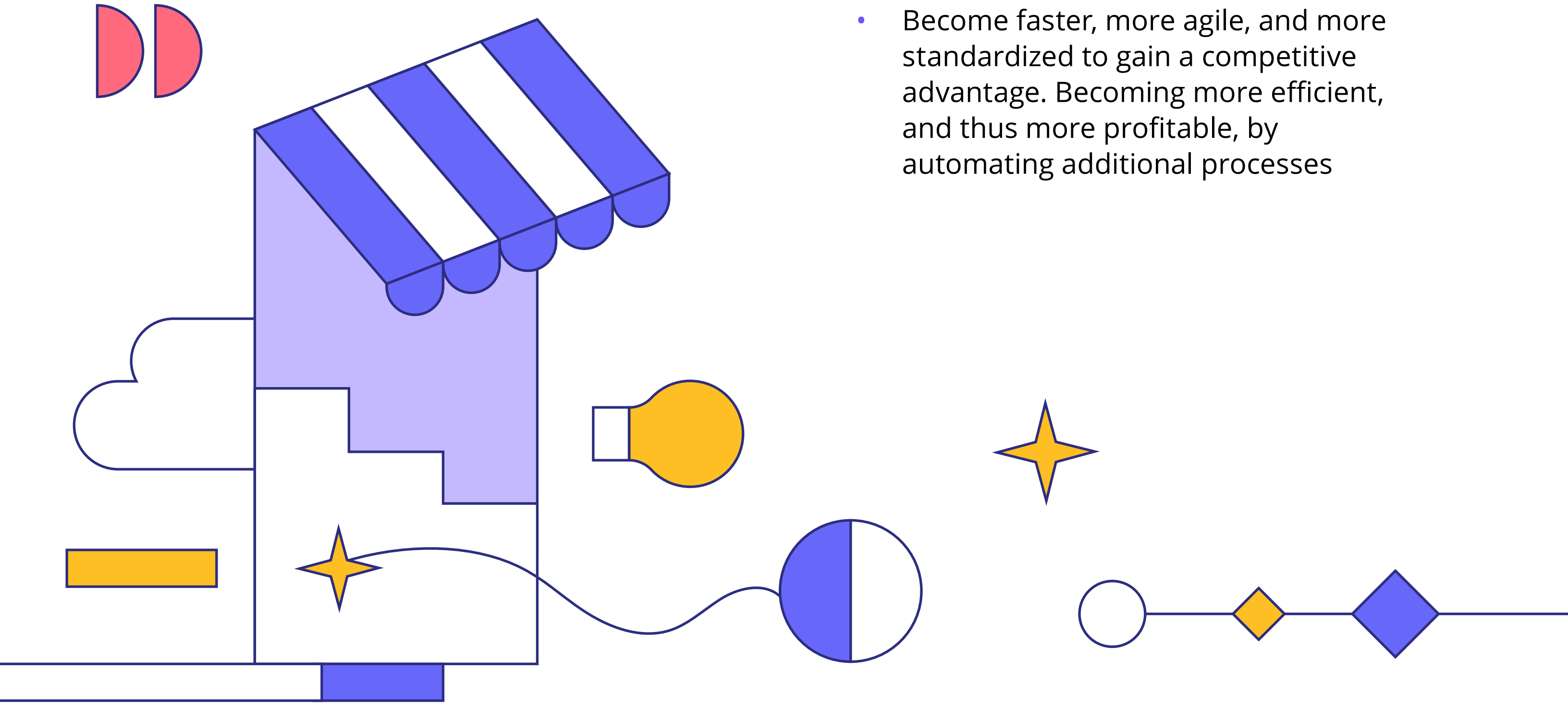
Our client is a retail group that owns and operates hypermarket and grocery chain brands.

Business Challenge

One of our client's Digital Business Units had an initiative to standardize and simplify the way the company would develop, deploy, secure, and maintain its applications utilizing multi-cloud approach. Our client created a universal internal development environment which enabled involved parties to utilize different cloud computing resources, as well as private data center.

Our client needed to achieve the following goals:

- Enable continuous and secure development/deployment/integration of its applications
- Stop hard coding and begin using an internal components library and microservice architecture to decrease operational expenses, increase ROI, and greatly speed time to market
- Simplify how new features of its applications are created to be able to fulfill business requirements faster (ideally in real-time)
- Secure sensitive assets across different computing environments
- Become faster, more agile, and more standardized to gain a competitive advantage. Becoming more efficient, and thus more profitable, by automating additional processes



Project Description

Our client's platform is a PaaS for internal product teams, providing the infrastructure - K8s clusters, SQL/NoSQL DBs, storage - required to run those product apps. The core engine is a resource orchestrator written in Golang, that provides multi-cloud strategy to provision all the resources necessary for product deployment. Google Cloud Platform (GCP) was chosen as a first implementation strategy, with Azure and OpenStack (on-prem) planned for further development. Under the hood, the core engine is generally an API service which does Terraform infra provisioning and deploy services via K8s parameterized manifests. For each product, the core engine creates a GCP project with GKE cluster, SVPC subnet, CloudSQL, GCS, Datastore, etc. The platform itself consists of 4 components (verticals) implementing UI (Explore and Register), Monitoring/Logs (Observe), Costs (Control) and CICD pipeline (Deliver), each communicating with the core engine.

SoftServe was tasked with performing a security assessment and risk mitigation prior to the release of the platform. Additionally with the creation of security architecture and implementation of technical security controls, SoftServe created a custom framework for secure development, operations, and support of the client's solution.

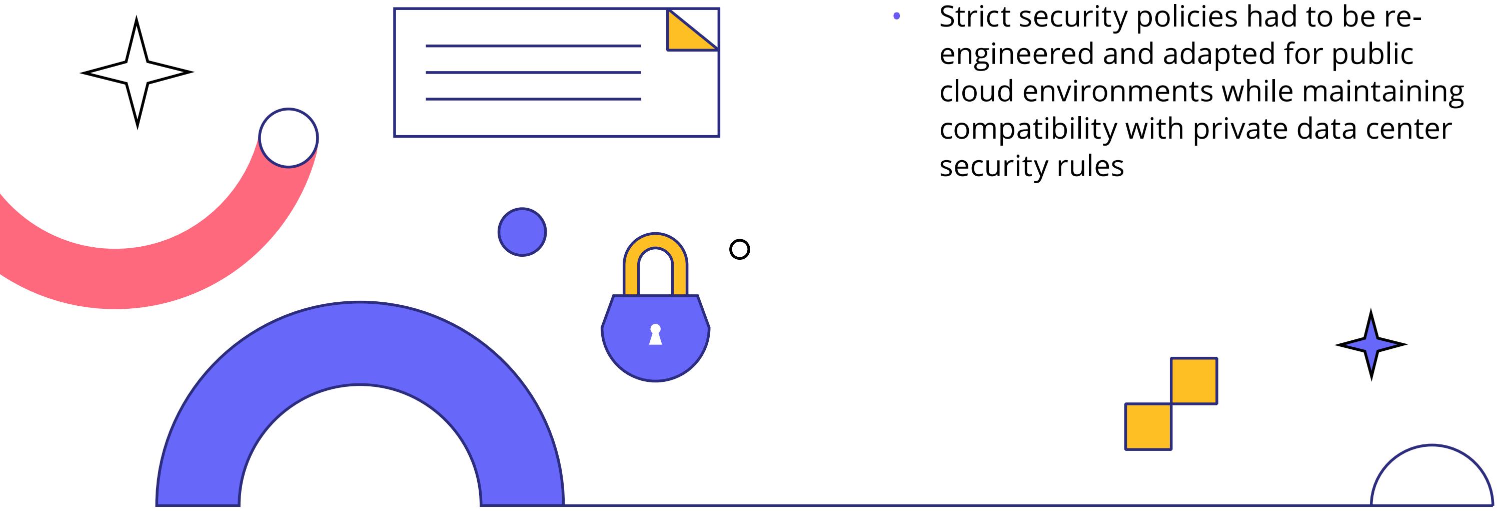
SoftServe overcame the following challenges during this project.

- DC Ops requirement was that only a fully-private VPC could be connected to on-prem networks via a VPN, and all egress traffic should flow through an on-prem HTTP proxy

- The GCP implementation of SVPC had some limitations on the amount of VPC peering, requiring exposure of external IPs for services and k8s masters

- Some GCP services usage was also restricted/limited in a fully-private VPC, like CloudBuild

- Strict security policies had to be re-engineered and adapted for public cloud environments while maintaining compatibility with private data center security rules



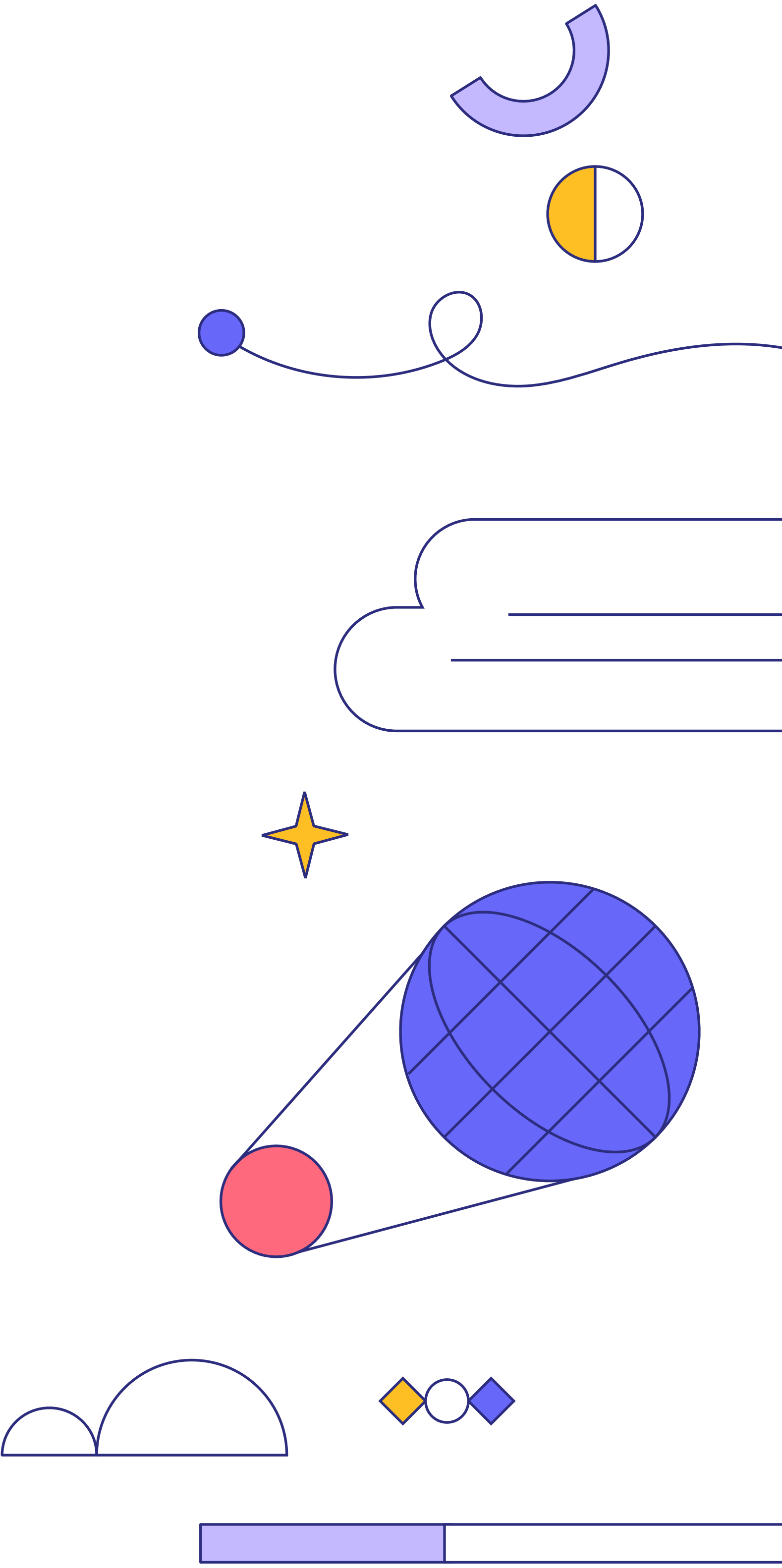
Value Delivered

SoftServe designed a full set of security technical controls along with recommended toolsets and related processes covering not just the cloud infrastructure itself, but also related SLDC, CI/CD, and operational/support activities. This resulted in a unique Information Security Management System (ISMS) framework that is fully aligned with national and international industry standards and is capable of maintaining our client's strong security posture for hybrid computing environments (on-prem and cloud).

The delivered set of security controls also serves as security guidelines that allows for future development of secure services and applications.

From a technical standpoint, SoftServe utilized native GCP security mechanisms as often as possible to provide maximum scalability for services and follow CSPs best practices.

SoftServe delivered robust security standards to ensure our client's new 'layer' is protected according to industry standards. SoftServe also supported the implementation of recommended security strategies and set up standard rules and processes to enable high-level security within GCP.



ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, energy, financial services, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation, from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience is built on a foundation of empathetic, human-focused experience design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy. No matter where you are in your journey.

Visit our **website**, **blog**, **LinkedIn**, **Facebook**, and **Twitter** pages.

NORTH AMERICAN HQ

201 W 5th Street, Suite 1550
Austin, TX 75703
USA +1 866 687 3588 (USA)
+1 647 948 7638 (Canada)

EUROPEAN HQ

14 New Street
London EC2M 4HE
United Kingdom

Level 39, One Canada Square

Canary Wharf, London E14 5AB
United Kingdom
+44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com

softserve