Case 03: Security and Compliance

This customer had a common FinServ requirement. The customer did not want any data to traverse the public internet, for obvious reasons. So they had a security strategy that included a technical requirement to use private APIs to access Google Cloud resources. They saw this as fundamental to their security strategy. Additionally, they wanted to know how the Cloud Provider secured Standards Certifications, and what they did to stay current. They were concerned that the provider might lose a certification that they were relying on for business.

A large financial company wanted to improve their security posture, a common FinServ requirement...

Security

- Business Requirement: Data cannot traverse the public Internet.
- Technical Requirement: Must have private API access to Google Cloud services as a good security practice and to minimize data exfiltration.

Compliance

- Business Requirement: Cloud provider must earn the trust of the business. How does Google Cloud maintain the latest standards around security, availability, process integrity, privacy, and confidentiality?

The first thing we did was make sure all access to Google Cloud was through secure methods, including SSL, VPN, Interconnect, and private API.

We decided to use a new feature that was in alpha, called VPC Service control. https://cloud.google.com/vpc-service-controls/ This enables a security perimeter. For example, BigQuery could be placed inside a security perimeter, and then could only be accessed at a private endpoint. And then there were standards and compliance such as ISO and SOC. We provided these to the customer - and they needed to sign agreements to be covered by Google's guarantees about these standards.

We mapped that to technical requirements and Google Cloud's products and services…

Security

- Ensure all traffic to Google Cloud is through secure methods, such as SSL/TLS, VPN, Interconnect, and private APIs / private endpoints.

Compliance

- Google Cloud has Standards, Regulations & Certifications that would meet their compliance requirements and help earn their trust in our platform.

And this is how we implemented that technical requirement.

VPC Service Controls / Secure Google Cloud API

- Restrict access to user's Google Cloud resources based on the Google Cloud Virtual Network or IP range.
- Restrict the set of Google APIs and Google Cloud resources accessible from user's Google Cloud Virtual Network.

Standards, Regulations & Certifications

- Products regularly undergo independent verification of:
- Security / Privacy / Compliance Controls
- Certifications
- ISO 27001, 27017, and 27018 and SOC 1, 2, and 3 certifications.
- An interesting point about both security and compliance, is that it is a "shared responsibility" model. So although we provided secure access and layered protection, the customer needed to use IAM to manage access to its employees and implement secure practices in its procedures. Also, the standards compliance covers the cloud resources, but not the customer's application. So they may need to take extra steps to ensure that the overall solution is compliant.