Optiv Executes Secure Google Cloud Platform Implementation

**Business Drivers**
Businesses across all industries, including finance, are increasingly moving to cloud services. Traditional financial services companies are often saddled with legacy systems and outdated processes, leaving them at risk of being outpaced by more innovative competitors. Cloud technology can help counter some of these challenges, but comes with its own complications.

**Business Problem**
Cloud technology allows employees to access data from anywhere, but it also opens the door to malicious actors who may not previously have had access to fully on-premises solutions. Organizations must now be more vigilant and implement stronger security practices to counteract this increased risk. Financial institutions are also subject to strict regulations around their customers' data, and must keep these in mind while planning a cloud transition.

**Optiv’s Approach**
Optiv works with you to identify and align proper security controls using best practices for configuration and implementation to any relevant frameworks. Together, we can determine the critical list of services to be included in the deployment.

**Industry**
Financial

**Desired Outcome**
Deployment of secure Google Cloud Platform through code with patterns and stamps to accommodate enterprise scalability.

**Use Case**
Optiv assisted a high profile financial services client with deployment of the Google Cloud Platform using best practices and providing guidelines to implement security controls designed to create a secure cloud solution.

**Engagement**

**Benefits**
- Documented and implemented security policy to guide safe utilization of GCP
- Reference code providing foundation for application teams to configure services within GCP with security and best practices in mind

**Proposed Roadmap**
- Publish reference code in a central repository and provide guidelines to development and integration teams and require the use of both
- Implement Terraform Enterprise and Terraform Sentinel as compliance measures to validate deployment configurations to ensure strict policy adherence
- Develop data loss prevention, identity and access management, continuous monitoring, logging and auditing strategies
- Implement tools and/or data lifecycle management systems to assist with audit of multi-cloud platforms and adherence to infrastructure security policies and requirements
Customer Deployment
Implemented cloud policy for a client using Google Cloud Platform (GCP) services in the form of three main deliverables:

OPTIV BLUEPRINT
Provided the client a roadmap and steps to create a secure cloud solution to meet the needs of their organization. Each blueprint document outlined the applicable controls that address security topics including, but not limited to:
- Access Control and Management
- Asset Management
- Data Security
- Perimeter Security
- Network Security
- Application Security
- Logging, Alerting and Monitoring

TERRAFORM MODULES
Upon completion of the blueprint, Optiv provided draft versions of Terraform modules to be used as reference code by the application/engineering teams. These reference modules contain the code necessary to implement the security policies outlined in the Optiv blueprints. These modules cannot deploy a service on their own, but may be used by application teams to ensure the security policies are properly configured in the GCP service or common security architecture component, such as Forseti. The Terraform scripts were delivered to the client’s security team and were incorporated into central source control.

DEVELOPER GUIDELINES
The guidelines provide guidance to internal application teams, outlining security concerns and controls, reference the ability to implement these controls via Terraform reference modules, outline the risk rating and whether risk is mitigated or outstanding based on the use of accompanying Terraform Modules. Optiv provided drafts of these guidelines and updated them based on feedback received from the client architecture team.

Implementation Breakdown

GCP SERVICES
- PubSub
- GKE
- GCS - Cloud Storage
- Cloud Functions
- Composer
- DataProc
- KMS
- Big Table

Cloud SQL
Big Query
App Engine
Compute Engine
Data Flow
Spanner
Data Loss Prevention

COMMON SECURITY ARCHITECTURE
- Compliance Validation (Forseti)
- Logging and Monitoring
- IAM
- Organization Policy Constraints

Why Optiv?
Optiv is the only pure-play security services integrator (SSI) that can design, implement and manage an end-to-end cloud program focused on security and aligned to your business goals. Our certified experts can help you gain the agility, security, scale and control you need to stay ahead of the competition.

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved.

Secure your security.”