Optiv Enables Fortune 50 Health Insurance Provider to Strengthen their Cloud Security Program

**Business Drivers**
Cloud services are an incredible asset to health insurance providers. Providers can reduce their costs by centralizing patient records, while leveraging big data to make more informed decisions. Patients also benefit from more control over their personal data. While the cloud can solve for many challenges, it often presents some of its own.

**Business Problem**
Cloud technology allows employees to access data from anywhere, but it likewise opens the door to malicious actors. Well-meaning employees, who may not have previously had access to on-premises solutions could also gain unnecessary permissions. Organizations must be more vigilant and implement stronger security practices to counteract increasing risks.

**Optiv’s Approach**
Optiv works with insurance providers to identify proper security controls and best practices for configuration and implementation of cloud platforms. We can help your organization safely migrate to, and utilize, cloud-based resources. When helping design, implement and manage security programs, the controls and practices used are determined based on the data and services to be hosted or provided from the cloud.

**Industry**
Health Insurance

**Desired Outcome**
Identification of proper security controls and best practices to securely accelerate the client’s modernization and digital transformation efforts.

**Use Case**
Optiv provided cloud security expertise to restructure and rethink the client’s AWS implementation, harden their security and close knowledge gaps.

**Business Benefits**
- Enabled better AWS account management by restructuring AWS Organizational Units
- Improved security through updated IAM policies using CloudFormation templates
- Reduced costs and downtime by migrating data to the cloud using Snowball and Snowball Edge
- Streamlined creation, maintenance and deployment of server images through a custom Amazon Machine Image builder
- AWS configuration to ensure HIPAA compliance
- Central management of IAM to take full advantage of available services

**Proposed Roadmap**
- **AWS configuration to ensure HIPAA compliance**
- **Central management of IAM to take full advantage of available services**
Customer Deployment

Optiv leveraged best practices alongside Amazon and Splunk services to assist our client in implementing effective security controls.

Our cybersecurity experts restructured the existing Amazon Web Services (AWS) hierarchy, including organizational units (OUs) and service control policy, providing current and future state AWS OU diagrams. We also assisted the client in restructuring their AWS identity and access management (IAM) strategies. This included deployment and ongoing management of users, policies, providing CloudFormation templates, IAM polices and roles for the client to use going forward. Optiv ordered and assisted with the implementation and use of Snowball and Snowball Edge devices to migrate data from on-premises to AWS, providing ordering process documentation to the client. We also provided AWS knowledge, best practices and support to teams requesting access to perform tasks within the environment.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

Our experienced consultants and engineers also provided troubleshooting services and assistance with knowledge gaps within the security, cloud and operations teams. Optiv provided feedback on security guardrail documentation, as well as architecture input and support to deploy transit gateway within the environment. We reviewed the client’s Splunk deployment and provided insight into proper ingestion and aggregation of logs.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

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.

Implementation Breakdown

CLOUD SERVICES
- AWS cloud services

IAM
- CloudFormation Templates

DATA MIGRATION
- AWS Snowball and Snowball Edge devices

AMAZON MACHINE LEARNING
- CodeCommit repository
- CodeBuild projects and build specifications
- CloudWatch event rules
- Packer templates
- Chef/Ansible configuration files
- Simple Notification Service topics
- Python Lambda functions

Optiv leveraged best practices alongside Amazon and Splunk services to assist our client in implementing effective security controls.

Our cybersecurity experts restructured the existing Amazon Web Services (AWS) hierarchy, including organizational units (OUs) and service control policy, providing current and future state AWS OU diagrams. We also assisted the client in restructuring their AWS identity and access management (IAM) strategies. This included deployment and ongoing management of users, policies, providing CloudFormation templates, IAM polices and roles for the client to use going forward. Optiv ordered and assisted with the implementation and use of Snowball and Snowball Edge devices to migrate data from on-premises to AWS, providing ordering process documentation to the client. We also provided AWS knowledge, best practices and support to teams requesting access to perform tasks within the environment.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

Our experienced consultants and engineers also provided troubleshooting services and assistance with knowledge gaps within the security, cloud and operations teams. Optiv provided feedback on security guardrail documentation, as well as architecture input and support to deploy transit gateway within the environment. We reviewed the client’s Splunk deployment and provided insight into proper ingestion and aggregation of logs.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

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 leveraged best practices alongside Amazon and Splunk services to assist our client in implementing effective security controls.

Our cybersecurity experts restructured the existing Amazon Web Services (AWS) hierarchy, including organizational units (OUs) and service control policy, providing current and future state AWS OU diagrams. We also assisted the client in restructuring their AWS identity and access management (IAM) strategies. This included deployment and ongoing management of users, policies, providing CloudFormation templates, IAM polices and roles for the client to use going forward. Optiv ordered and assisted with the implementation and use of Snowball and Snowball Edge devices to migrate data from on-premises to AWS, providing ordering process documentation to the client. We also provided AWS knowledge, best practices and support to teams requesting access to perform tasks within the environment.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

Our experienced consultants and engineers also provided troubleshooting services and assistance with knowledge gaps within the security, cloud and operations teams. Optiv provided feedback on security guardrail documentation, as well as architecture input and support to deploy transit gateway within the environment. We reviewed the client’s Splunk deployment and provided insight into proper ingestion and aggregation of logs.

Optiv created, maintains and continuously improves upon a custom Amazon Machine Image builder for the client, providing the client with a CodeCommit repository, CodeBuild projects and build specifications, CloudWatch event rules, Packer templates, Chef/Ansible configuration files, Simple Notification Service topics, Python Lambda functions and process documentation.

Our experienced consultants and engineers also provided troubleshooting services and assistance with knowledge gaps within the security, cloud and operations teams. Optiv provided feedback on security guardrail documentation, as well as architecture input and support to deploy transit gateway within the environment. We reviewed the client’s Splunk deployment and provided insight into proper ingestion and aggregation of logs.