UST Empowers Healthcare Provider with Cloud Infrastructure and Security Capabilities



Executive Summary

The client is a U.S. health insurance provider offering a personalized approach to healthcare based on the needs of the communities where their members live and work. The client works in tandem with community hospitals and doctors to provide quality, affordable healthcare.

Customer Challenge

Provider Data Transformation (PDT) is a platform that empowers users/patients with the information from various providers covered under their health coverage plans. As a healthcare provider, the client aimed to build a HIPAA-compliant infrastructure. The project met difficulties due to a lack of agility in the provider's data infrastructure. The client sought to resolve the problems by utilizing modern data ingestion and distribution methods, emphasizing the use of industry standards and interoperability.

Why UST

With its extensive cloud expertise, UST was chosen to augment the AWS infrastructure capabilities with additional features to support the PDT application requirements. UST conducted an in-depth analysis to gain an understanding of PDT's current infrastructure and business practices. The discovery phase included:

- Focused interviews and workshops with COE and security
- System assessment
- Data collection sheets
- Questionnaires
- Maturity assessment of current tools and processes

Based on the discovery phase analysis, UST laid out a plan to strategically deliver the capabilities in a phased manner across streams, including cloud security and data security capabilities.

About The Client

The dient is a U.S. health insurance provider, offering a personalized approach to healthcare based on the needs of the communities where their members live and work.

Benefits

- Speed to market by migration to cloud in 5 months
- Flexibility and predictability of features' market presence by adopting Agile Methodologies

AWS Services

- AWS CloudTrail
- AWS CloudWatch
- AWS CloudFormation
- Amazon Simple Notification Service
- AWS Key Management Service
- AWS WAF
- AWS Direct Connect
- AWS Transit Gateway
- AWS Lambda
- AWS Security Hub

About UST

For more than 20 years, UST has worked side by side with the world's best companies to make a real impact through transformation. Powered by technology, inspired by people and led by our purpose, we partner with our clients from design to operation.

Through our nimble approach, we identify our clients' core challenges and craft disruptive solutions that bring their visions to life. With deep domain expertise and a future-proof philosophy, we embed innovation and agility into our clients' organizations – delivering measurable value and lasting change across industries and around the world. Together, with over 26,000 employees in 25 countries, we build for boundless impact – touching billions of lives in the process. Learn more at ust.com.

aws partner network

Advanced
Consulting Partner

Solution Provider

UST Solution

Security Capabilities

The association had minimal documentation for cloud operations. UST rewrote the code and redefined the approach to AWS Key Management Service (KMS), certificate management, backup and archival implementation. They migrated from a decentralized model to a centralized model, including multi-account and multi-VPC scenarios leveraging AWS CloudFormation, Infrastructure as Code (IaC) services, and AWS Lambda functions for provisioning. Additionally, AWS Security Hub was integrated with ServiceNow incident management system.

UST collaborated with PDT, information security and network teams to identify a suitable WAF solution. They included an ingress traffic routing path and eventually deployed it into the ecosystem. It enabled the AWS Transit Gateway for intra-VPC secure connections and then external IPs and services were configured to route via the on-premises network.

AWS Direct Connect was employed to connect the transit gateways and on-premise center, which was further protected by AWS WAF.

Cloud Security and Monitoring

AWS CloudTrail was enabled across all regions and resources. Appropriate naming conventions that helped in the classification of logs were further redirected to SPLUNK monitoring and encrypted by AWS KMS (SSE-KMS). Amazon CloudWatch Alarms were set in place as part of automated smart monitoring and threshold monitoring and to detect any failures, abnormalities or unauthorized events. When detected, e-mail alerts were sent to respective departments via Amazon Simple Notification Service (SNS), ensuring on-time notification and subsequent remediations.

Why AWS?

AWS Network services like AWS VPCs, private subnets, network access controls, security groups and Bastion hosts were deployed at all architecture tiers, ensuring perimeter security. Similarly, data encryptions on AWS S3 buckets, EBS volumes, SSL terminations and bucket policies were implemented as part of data security.

A strong governance model ensures smooth delivery and support, adopting methodologies from Scaled Agile Framework during the engagement lifecycle. UST trained client staff in backlog grooming, sprint planning, user story breakdown and refinements, providing increased predictability and an incremental approach to deploying the features into the application and environments. These changes resulted in operational excellence in the working model.

Leveraging AWS resources and services, UST helped PDT augment existing AWS infrastructure and security foundational capabilities in support of PDT application requirements, bringing in scaling and cost benefits, agility in the infrastructure and speed to market.