

# Strengthening Network Security: A Robust Architecture for a Leading Healthcare Provider



## Executive Summary

The customer, a New Jersey based leading non-profit health care systems provider is known for providing exceptional patient outcomes and experiences., they are committed to provide the highest quality care delivered at the right time, at the right place, and at the right cost. To address the customer's complex networking and security challenges, our partner team embarked on a transformative project. This initiative unified multi-site network architectures while ensuring robust security standards. It began with a secure Direct Connect connection, seamlessly interfacing with the Virtual Private Gateway (VGW) for enhanced security and low-latency data transfers. AWS Network Firewalls fortified security, and dedicated accounts were established using AWS Control Tower for comprehensive security resource management, enabling strict security control policies (SCPs) and centralizing account management. AWS Transit Gateway streamlined networking for efficiency, while Palo Alto Firewalls deployed in the on-premises data center environments enhanced packet inspection, bolstering overall security. Centralized logging within the log archive account and comprehensive security services in the Audit account ensured robust monitoring and compliance with industry standards.

## Customer Challenges

The customer faced a challenge in scaling up their security posture to match with their ever growing AWS workloads They needed to bolster threat detection and incident response capabilities, ensuring protection against malicious activities and unauthorized access across their AWS accounts and workloads. Compliance with security benchmarks, such as CIS AWS Foundational Benchmarks, and enforcing security best practices were crucial requirements. Additionally, the customer sought to secure network traffic patterns, both within AWS and between on-premises and AWS-hosted resources, while dealing with the intricacies of multi-account architecture and AWS Control Tower. A comprehensive security solution was imperative to address these challenges effectively.

## Goals


The implementation goals were to enhance network security and compliance within AWS. This involved deploying AWS Control Tower, centralized logging, and robust security services for streamlined network connectivity, improved visibility, and efficient monitoring.

## Partner Solution

To address the healthcare client's vast and complex challenges the AWS Partner implemented a meticulous and robust solution for the client. The key features of it are:

1. Control Tower and Account Orchestration: Leveraging AWS Control Tower, our partner orchestrated the creation of dedicated AWS accounts tailored for specific services, including an Audit Account for centralized security management, a Log Archive account for efficient log storage and analysis, and a Network Account for housing networking resources like




- 
2. Comprehensive Network Architecture: Our solution commenced with the design and implementation of a comprehensive network architecture within AWS. This architecture, driven by the principles of service-oriented security, scalability, and operational readiness, provided a robust foundation for the customer's network infrastructure.
  3. Dedicated VPC for Security: To fortify security and streamline network management, we established a dedicated Virtual Private Cloud (VPCs). This VPC was strategically designed to facilitate specific security functions, ensuring efficient traffic inspection and control.
  4. Efficient Network Connectivity with AWS Transit Gateway: The adoption of AWS Transit Gateway significantly simplified network connectivity by creating a hub-and-spoke model. This design improved communication among various workloads and use cases while reducing network complexity.
  5. Advanced Security with AWS Network Firewalls: Seamless integration of AWS Network Firewalls provided advanced traffic filtering and inspection capabilities. This enhanced layer of security ensured all network traffic adhered to rigorous security standards.
  6. Secure On-Premises Connections via AWS Direct Connect and Palo Alto Firewalls: Through AWS Direct Connect, we established secure, high-speed connections between the customer's on-premises data centers and AWS cloud resources. This setup facilitated rapid and secure data transfers, essential for uninterrupted operations. Moreover, deep packet inspection was done by Palo Alto Firewalls ensuring that egress traffic was rigorously scrutinized.

Our solution's integration of AWS Control Tower and dedicated accounts, combined with a robust network architecture and service-oriented security measures, successfully tackled the customer's complex networking and security challenges. The resulting AWS network not only met stringent security and compliance standards but also set the stage for optimized performance and future growth.

### **Results and Benefits**

The implementation of our service-centric network solution delivered substantial results and benefits to the customer:

- A. Enhanced Network Security: The integration of AWS Network Firewalls, Palo Alto Firewalls, and Transit Gateway bolstered network security. Comprehensive traffic inspection and filtering ensured the highest level of security for data in transit, safeguarding against potential threats.
- B. Streamlined Network Management: The adoption of AWS Transit Gateway simplified network connectivity across workloads and use cases. This streamlined approach reduced network complexity, minimizing operational overhead and enhancing overall efficiency.



C. Seamless On-Premises Connectivity: AWS Direct Connect provided fast, secure, and dedicated connections between on-premises data centers and AWS cloud resources. This ensured uninterrupted data transfers critical for the customer's operations.

D. Centralized Security Controls: Centralized security management through AWS Control Tower and dedicated accounts offered a unified view of security across the entire AWS environment. This simplification of security controls and monitoring promoted efficient governance.

E. Improved Compliance: With AWS Security Hub and AWS Config in place, the customer gained comprehensive visibility into their security posture. This enabled them to align with industry best practices, ensuring continuous compliance with regulatory requirements.

F. Future-Ready Network: The solution positioned the healthcare provider for future growth and scalability. The modular, service-oriented architecture can easily accommodate new workloads and evolving security needs.

G. Cost Optimization: By optimizing network design, consolidating security controls, and enhancing operational efficiency, the customer achieved cost savings in managing their AWS network infrastructure.

In summary, the Partner's solution not only met the client's immediate security and networking challenges but also provided a strong foundation for future growth. Enhanced security measures, streamlined network management, and improved compliance have transformed their AWS network into a secure, efficient, and cost-effective platform for their critical operations.

## About Intuitive.Cloud

Intuitive is a global cloud innovation company that partners with the world's leading enterprises to deliver high-impact, end-to-end solutions and drive extraordinary business outcomes. We are one of the fastest growing (CRN & INC5000 recognized) Cloud & SDx solutions and services companies in the Americas supporting enterprise customers on a global scale. Intuitive Superpowers: Cloud FinOps, Cloud Infrastructure Engineering, Cloud Native+AppSecOps+DevSecOps, DataOps, AI&ML, CyberSecurity & GRC, Digital Workspaces (M365), Hybrid Cloud, SDDC, SD-WAN, SDN

