

Charting a Secure Course: Navigating Oil & Gas Giant's Network and Security Challenges



Executive Summary

Our showcased customer, a prominent force in the Oil & Gas industry, drives innovation and excellence across the energy sector. With a global footprint, they maintain their dedication to sustainable solutions and operational excellence. Our partner team took on a significant project to tackle the complex networking and security challenges faced by customer. This endeavor aimed to consolidate the network architectures across multiple sites while prioritizing strong security measures. The journey began with the implementation of a secure Direct Connect connection, seamlessly integrated with the Virtual Private Gateway (VGW) to facilitate secure and high-speed data transfers. We set up dedicated accounts using AWS Control Tower for thorough management of security resources, allowing for the enforcement of stringent security control policies (SCPs) and centralized account administration. The deployment of AWS Transit Gateway optimized networking for increased efficiency, while Palo Alto Firewalls strengthened packet inspection, fortifying overall security. We established centralized logging within the log archive account and implemented comprehensive security services in the Audit account to ensure robust monitoring and compliance with industry standards.

Customer Challenges


Customer faced the need to optimize their network architectures and security measures to meet evolving demands. This included achieving compliance standards and unlocking advanced analytics capabilities within their Data Lake. As the customer was not on AWS and we needed to build their AWS environment from scratch, a foundational landing zone was required to establish consistent security controls and governance across their accounts, ensuring a resilient defense against potential risks. Moreover, network security needed to be reinforced to safeguard against unauthorized access and potential breaches, particularly concerning east/west traffic and on-premises inspection.

Goals

The goals to address these challenges would involve implementing a centralized governance framework through AWS Control Tower, ensuring consistent security controls, compliance, and streamlined account management. Additionally, deploying Palo Alto Firewalls would enhance network security, providing robust protection against unauthorized access and potential breaches. This includes safeguarding east/west traffic, on-premises inspection, and ensuring high availability for uninterrupted operations.

Partner Solutions

In addressing customer's intricate networking and security challenges, our team implemented a robust solution centered around AWS Control Tower. A pivotal element of this setup was the creation of a dedicated Security OU within the Control Tower. This Security OU served as the bedrock for centralized logging and auditing, aligning with industry-leading best practices. By structuring the landing zone in a way that supports multi-account governance, we ensured consistent security measures across all facets of Customer's AWS environment.



To enhance security, advanced Palo Alto VM-Series Firewalls were deployed in conjunction with native AWS networking and security services. These firewalls were custom designed to align with Customer's unique requirements.

Several technological solutions were included in achieving the above solution. These solutions include:

1. **AWS Control Tower:**

AWS Control Tower was used to create an Enterprise grade Landing Zone involving multiple accounts with a dedicated use case for each account. Moreover, a centralized Log Archive account was curated to support logging and monitoring. An audit account was created to centralize all security services for the Security team. Furthermore, a centralized Networking account was created with transit gateway and Palo Alto Firewalls in inspection and egress VPCs.

2. **AWS GuardDuty:**

By implementing Amazon GuardDuty, a robust threat detection service, we established continuous monitoring of AWS accounts and workloads for potential malicious activity. This allowed for timely identification and remediation of security threats, enhancing visibility and safeguarding customer's resources.

3. **AWS Security Hub:**

With AWS Security Hub, we helped the customer to meet the compliance standards and ensured continuous assessment and adherence to best practices. We provided them with a comprehensive view of their AWS security posture. This service collected security data from various AWS accounts, services, and third-party products, enabling us to analyze security trends and prioritize addressing the most critical security issues.

4. **AWS Config:**

Through AWS Config, we conducted ongoing assessments and audits of resource configurations across AWS environment. This meticulous evaluation, facilitated by the customer's Security tooling account, ensured adherence to industry best practices and standards.

5. **IAM Access Analyzer:**

We implemented IAM Access Analyzer to enhance their security measures which ensured that resources such as Amazon S3 buckets or IAM roles were only accessible to authorized entities, reducing potential security risks. It identified shared resources within customer's organization and accounts.

6. **Amazon Macie:**

To manage the security posture of customer's Amazon S3 data, we leveraged Amazon Macie which helped providing automated evaluation and monitoring of S3 buckets for enhanced security and access control. This service utilizes machine learning and pattern matching to discover sensitive data.

7. **AWS Detective:**

With Amazon Detective, we accelerated the root cause identification process, allowing for swift and effective security incident response. We empowered customer to efficiently analyze and investigate security findings or suspicious activities using AWS Detective which uses advanced analytics and machine learning.

8. Palo Alto Firewall integrated Gateway Load Balancer:

To fortify network security, a separate networking account was established. This account housed a centralized inspection Virtual Private Cloud (VPC) for east/west traffic, on-premises inspection via Palo Alto Firewall, and a dedicated egress VPC for internet-bound traffic inspection also utilizing Palo Alto firewalls. With a multi-Availability Zone (AZ) configuration for high availability and strategic deployment behind a gateway load balancer, we ensured continuous operation and load balancing between instances.

Result and Benefits

- **Enhanced Security:** The integration of Palo Alto Firewalls with AWS services provided a robust defense against potential security threats, ensuring data protection and compliance adherence.
- **Compliance Adherence:** The centralized logging and security tooling accounts, along with the deployment of services like GuardDuty, Security Hub, and Config, ensured continuous assessment and adherence to industry standards and best practices.
- **Improved Governance:** AWS Control Tower facilitated the creation of a structured OU and account hierarchy, enhancing overall governance and security control.
- **Streamlined Assessment:** Runbooks were prepared to educate the customer on the new security tooling implemented in their environment, simplifying the security assessment process.
- **Efficient Logging and Monitoring:** Centralized logging in the Log Archive Account, coupled with services like Amazon Detective, provided comprehensive monitoring and quick identification of security incidents.
- **High-Performance Analytics:** The secure foundation allowed customer to leverage their Data Lake and Analytics platform with confidence, enabling them to extract valuable insights from their data.

The integration of AWS Control Tower and Palo Alto Firewall proved to be instrumental in fortifying customer's data lake resources. By combining robust security controls, and compliance adherence, the solution provided customer with a secure platform. This comprehensive security architecture sets the stage for continued innovation and success in the cloud-driven analytics landscape.

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.

