A Flavor Innovator's AWS-Enhanced Security Vigilance

Executive Summary

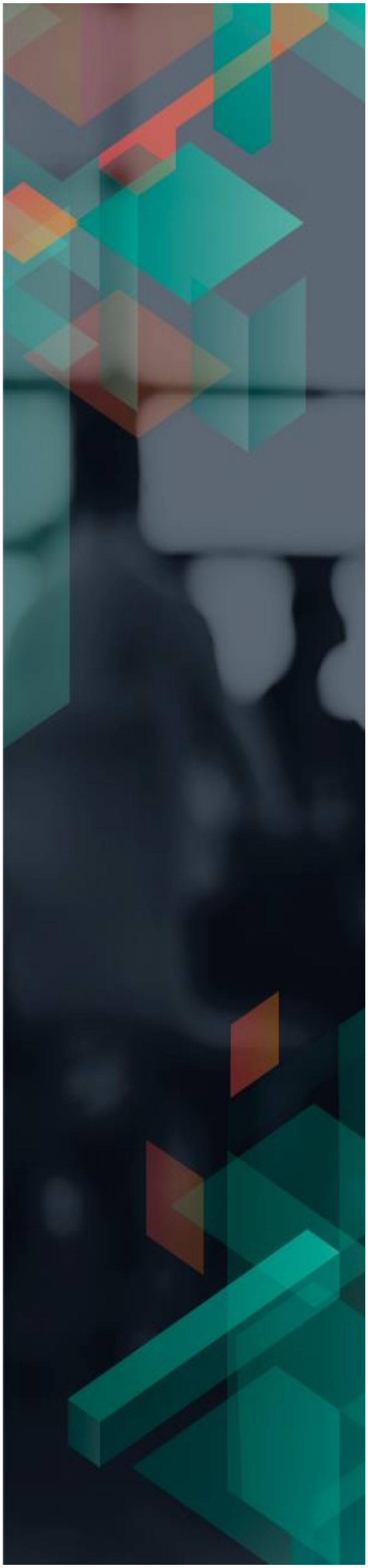
The customer, a global leader in food, beverage, health, bioscience, and sensorial experiences does a lot to continually innovate. They have hosted their enterprise grade applications in AWS using multiple accounts. Our partner helped the customer accelerate their journey by deploying dedicated accounts, an efficient hub-and-spoke network architecture, advanced security measures like Palo Alto Firewalls and a Web Application Firewall, and secure on-premises connections, to fortify the network's security and resilience. Additionally, data protection through SSL/TLS encryption, advanced URL and DNS filtering, and meticulous logging and monitoring tools, including AWS CloudWatch, SNS and CloudTrail, ensure real-time threat mitigation and business continuity. These collective measures exemplify our unwavering commitment to enhancing security and network resilience.

Customer Challenges

Prior to implementing our network security solution, our customer faced some operational challenges in their AWS environment. Managing a centralized network account for all networking requirements, and integrating third-party tools, presented administrative complexities and organizational hurdles. Additionally, the absence of a centralized network architecture led to some fragmentation in their network setup, affecting control and adherence to best practices. Lastly, their existing security measures needed enhancement to ensure comprehensive protection against potential threats and data security.

Goals

The goal of the project is to establish high-performing and secure network infrastructure. This strategic initiative aims to enhance network resilience, protect critical assets, and fortify the network against potential threats. By leveraging a comprehensive suite of AWS partner solutions, the project endeavors to enhance security and streamline network management, all while ensuring compliance with regulatory standards. Ultimately, the project's aims at providing a robust foundation for seamless and secure communication between on-premises data centers and AWS cloud resources, enabling the organization to thrive in an ever-evolving technological landscape.



Partner Solution

1. **Account Management:** The customer has dedicated accounts for various aspects like Network Account for housing the network infrastructure, Audit Account dedicated to auditing and monitoring activities within AWS environment.

2. **Network Architecture:** The network architecture adopts a hub-and-spoke model centered around a Transit Gateway, streamlining network connectivity, and enhancing control, monitoring, and security. This architecture adheres to AWS best practices, emphasizing centralization, secure communication, traffic inspection, and scalability to fortify the customer's network infrastructure.

3. **Network Security**
    a. Active/Active Palo Alto Firewalls: Active/Active configuration of Palo Alto Firewalls was deployed to provide comprehensive security. These firewalls protect against threats and intrusions, ensuring the integrity and confidentiality of data.
    b. Web Application Firewall (WAF): Our solution commenced with a Web Application Firewall implementation with necessary ACLs in front of an Application Load Balancer (ALB) to inspect and filter incoming traffic, protecting web applications from various attacks and vulnerabilities. The ALB then directs all ingress traffic to a pair of Palo Alto firewalls.
    c. Private Virtual Interface (VIF): Private VIF was used to establish a secure and private connection between the on-premises network and AWS VPCs through AWS Direct Connect, preventing unauthorized access.
    d. GWLB for Private Connectivity: Gateway Load Balancer endpoints were used to establish private connectivity between Palo Alto VM firewalls and workload VPCs. This architecture enables firewalls to inspect traffic and enhances network security.

4. **Data Protection**: AWS Certificate Manager was used to create and manage SSL/TLS certificates. These certificates were then employed to encrypt data in transit between users and the internal Application Load Balancer (ALB) holding application workloads.

5. **Advanced Security with Palo-Alto:** Palo Alto Firewalls were deployed to provide advanced security features and centralized control for traffic filtering. Advanced URL Filtering and DNS Security features were enabled on the Palo Alto Firewalls filtering web content and adding an extra layer of protection against web-based threats. Also, Palo Alto Firewalls were integrated with the Gateway Load Balancer for private connectivity to AWS workloads. The Active/Active configuration of Palo Alto Firewalls provides high availability, and additional firewall instances can be added in the future to scale security as needed.

6. **Secure On-Prem Connection:** On-premises connection security was ensured using AWS Direct Connect with Private Virtual Interface (VIF) for a dedicated and secure network link between the on-premises data center and AWS cloud. GRE tunnels provided an additional layer of security by encapsulating data traffic, terminating directly on on-premises routers, and being protected by firewalls at both ends. Palo Alto Firewalls were deployed for traffic inspection and security enforcement, while CloudEOS integration with AWS ensured that only authorized and encrypted traffic flowed between on-premises networks and AWS VPCs.

7. **Logging And Monitoring:** Logging and monitoring in our solution were comprehensive and instrumental for security. Centralized logging was established using AWS CloudWatch, integrated with SNS for timely notifications of security events. Additionally, advanced tools like Prometheus, Grafana, were employed to collect, analyze, and visualize metrics and logs, offering real-time visibility into container activity and security events.

These solutions, in conjunction with AWS best practices, have fortified our partner's infrastructure against potential risks, while the meticulous logging and monitoring mechanisms have empowered the organization with real-time insights for proactive threat mitigation. Our partnership exemplifies a commitment to excellence in security, ensuring business continuity, data integrity, and overall network resilience.

Result and Benefits

The partnership with AWS has yielded substantial benefits for the customer. It has bolstered their security significantly. With advanced measures such as Palo Alto Firewalls, robust protection against emerging threats and breaches was ensured. This has not only safeguarded data but also ensured regulatory compliance. The setup of Direct Connect with Private VIF has provided a reliable and dedicated on-premises connection, enhancing business continuity. Our solution offers automated monitoring and real-time threat detection. Proactive threat mitigation, scalability, and cost-efficiency are additional advantages, all contributing to an efficient and resilient network infrastructure that supports growth and security goals effectively.

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,

Intuitive.Cloud