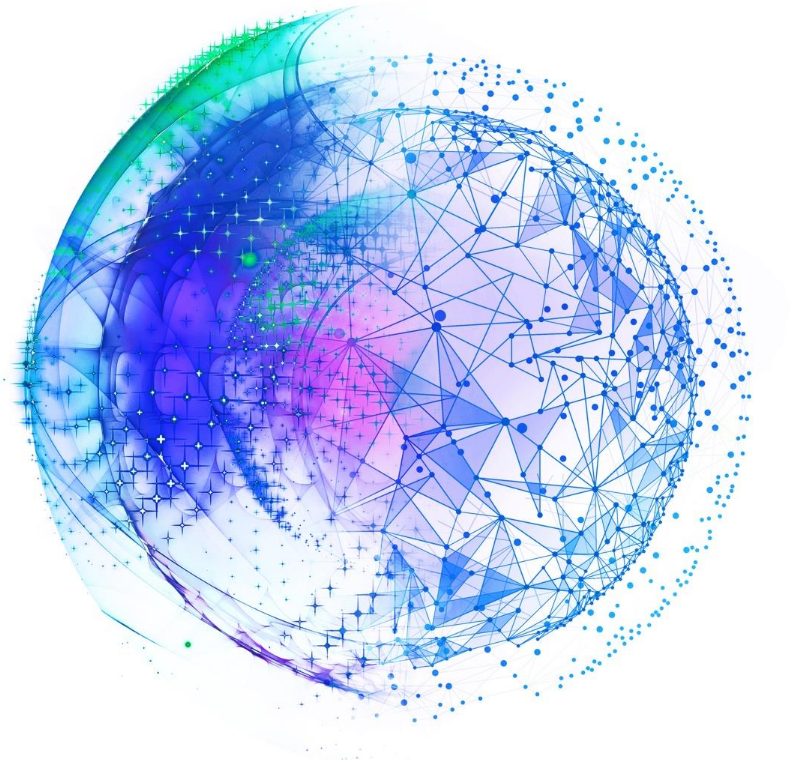
Deloitte.



Helping a large public bank exit an on-premise data center and colocation facility

CHALLENGE	A large public bank was struggling to migrate from their data center due to a shortage of resources with strong security skills, siloed infrastructure management, and outsourcing multiple cyber capabilities to various vendors while continuing to operate select services, resulting in limited coordination and greater cyber risk.
APPROACH	Deloitte developed a migration roadmap that we then followed to migrate their workloads with minimal refactoring while preserving their network schemes.
OUTCOME	The bank avoided costs associated with their aging data center while also enabling their digital transformation efforts in a way that can scale as needed to support their business goals.

Our client, a large public bank, wanted to transition away from their on-premise data center and colocation facility to the cloud. They struggled with several challenges during the migration, including:

- A lack of visibility into asset information tied to threat data to make informed decisions regarding response
- A shortage of resources with strong security skills
- A number of outsourced cyber capabilities to numerous vendors that resulted in limited coordination and increased cyber risks to the organization
- Siloed infrastructure management tools and too much technology given client's IT security staff size and infrastructure
- IT and security infrastructure tested and deployed manually with inconsistent and insecure approach

To help with these challenges, Deloitte developed a migration roadmap for the client that detailed the plan to exit the on-premise data centers and colocation facilities. Deloitte also migrated the client's workloads in a way that reduced refactoring and preserved network schemes.

Through our managed services, we provided:

- 24/7 operations of the hybrid environment that adhered to the cyber compliance requirements
- Easy access to incident alerting and response
- Amazon Web Services (AWS) Security best practices for threat monitoring, cloud security posture, AWS Infrastructure Vulnerability and Monitoring
- Automated data feeds from AWS CloudTrail to manage the ServiceNow instance of CMDB for AWS accounts to enable a Qlik dashboard to monitor and triage security events linked with Service Now
- A configured Prisma Cloud with 750 use cases/policies and 239 AWS-specific use cases to monitor security leading practices in the customer's AWS environment
- Threat detection capabilities to monitor AWS accounts and workloads for suspicious API calls and unauthorized deployments
- Web Application Firewall (WAF) and Palo Alto Next-Generation firewall services that protect layer 3, 4, and 7 attacks

Our managed services helped the bank quickly migrate from the data center to a hybrid solution that helped the bank avoid costs associated with its aging data center. This also enabled their digital transformation efforts and provided a highly scalable infrastructure.

Scope and complexity

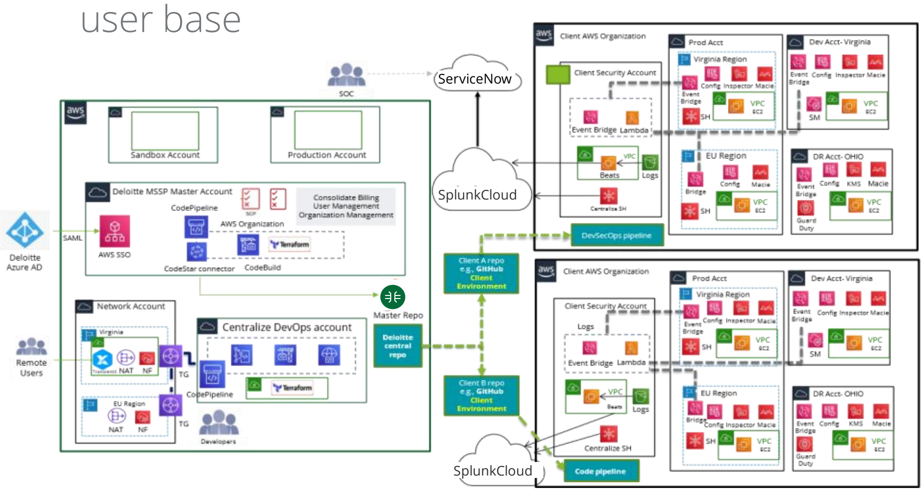
The project involved deploying, protecting, and managing:
AWS EC2 instances
AWS Firewall Manager
Lambda
AWS WAF
AWS Advance SHIELD
GuardDuty encryption keys and certificate manager
AWS Transit Gateway
Prisma Cloud

Cloud compliance frameworks for privacy and data protection criteria that meet standards and regulations like HIPAA, ISO 27001, SOC2, CCPA, PIPEDA, MITRE ATT&CK, CIS AWS Foundations Benchmark v1.3, CSA CCM, GDPR, HITRUST CSF V9.3, NIST-800, SOC2, ISO27001, and PCI DSS v3.

Industry compliance frameworks: Palo Alto Networks firewall, TrendMicro, Cloudstrike, Okta ASA/SSO, Prisma Compute, Nessus, Hashicorp Key vault, ServiceNow, etc.

Cloud reference architecture | Cyber cloud managed services

Illustrative architecture for securely deploying AWS to support multiple enterprise applications and user base



Contact us:

Aaron Brown
Cyber Cloud Managed Services Leader
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
aaronbrown@deloitte.com

Fiona Williams
Advisory AWS Alliance Leader
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
fwilliams@deloitte.com

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.