PRESIDIO® | CASE STUDY

FINANCIAL SERVICES

CYBERSECURITY, CLOUD

Financial Services Company

FINTECH PROVIDER ENHANCES ITS ABILITY TO REPORT ON SENSITIVE DATA AND BOLSTERS FIREWALL PROTECTIONS WITH PRESIDIO AND AWS

The Challenge

A global financial services / FinTech leader faced an imminent PCI compliance audit as part of a regular review of its technical and operational standards. The company utilizes AWS extensively to accelerate time to market and deliver business value for its clients. It needed to be able to accurately scope, assess, and report on its environment of more than 400 AWS accounts in short order. As part of the project, the company also sought to ensure that all applications in scope for PCI compliance had sufficient firewall protections in place.

The Solution

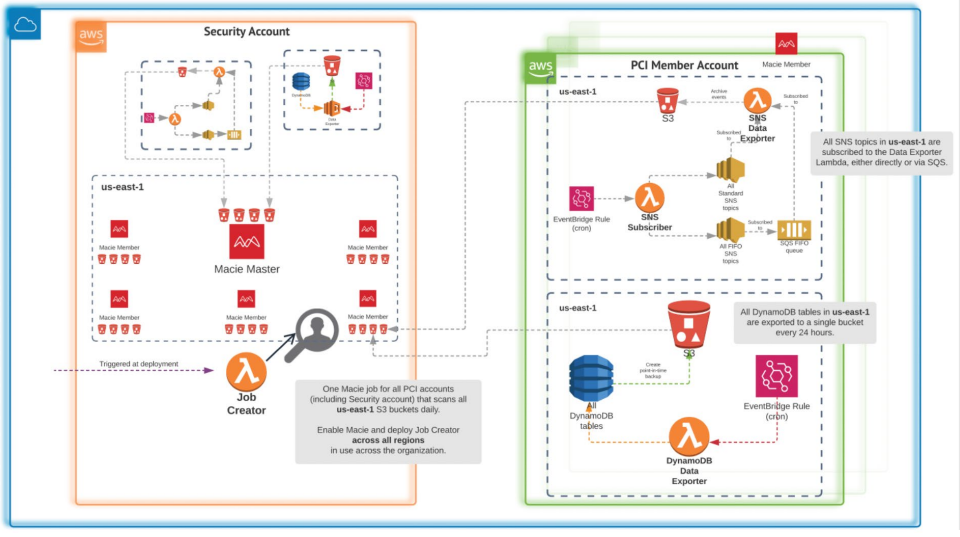
The financial services provider partnered with Presidio to accelerate preparations for the audit. Presidio first implemented a cardholder data (CHD) scanning solution, based on Amazon Macie. Presidio then deployed a set of AWS Lambda functions to archive DynamoDB tables and SNS messages in each region that contained AWS accounts designated for the audit. Presidio also deployed AWS Web Application Firewall (WAF) policies with AWS Firewall Manager to push adequate firewall protections across the AWS deployment.

Cardholder Data Detection with Amazon Macie

To capitalize on the benefits of Amazon Macie, Presidio developed an automated approach to data archival in S3. Python-based Lambda functions, S3 buckets, and minimally permissive Identity & Access Management (IAM) roles were deployed to each region of in-scope AWS accounts and used for DynamoDB table extraction and SNS message archival. The Lambda function first enumerated all DynamoDB tables in the current AWS account and region, then enabled point-in-time-recovery on each table as necessary. The Lambda function then performed a table export to S3 based on a timestamp. An EventBridge rule was created to invoke the DynamoDB export function every 24 hours.

For SNS message archival, a similar approach was used: a Lambda function was deployed to enumerate all SNS topics and then set up subscriptions for each topic. For standard SNS topics, the topics were subscribed to a second Lambda function that would archive the message contents to S3. In the case of FIFO SNS topics, the topics were subscribed to a SQS FIFO queue and the SQS queue was then subscribed to the second Lambda for archival.

All AWS resources were deployed with Terraform. Presidio developed two Terraform modules. The first module deployed the Lambdas for data archival to S3 as well as all supporting resources (S3, IAM, KMS, and SQS). The second deployed an S3 bucket for long-term retention of Macie findings, and automated the Macie job creation.



Centralized Firewall Configurations

Prior to engaging with Presidio on this project, the customer used AWS WAF Classic, and already had planned to upgrade to WAFv2. They wanted to centrally administer WAF policies via Firewall Manager, so Presidio took the reins to perform both tasks. Presidio undertook a full analysis of current WAF policies: global restriction of IP ranges, denial of traffic from restricted countries, and a managed rule set from the AWS Marketplace provided by Fortinet.

Presidio developed a new version of the Terraform module that leveraged WAF v2 resources and kept the same rule groups. Additionally, Presidio deployed the rule groups as WAF policies to AWS Firewall Manager in the customer's designated Security account. This also gave the Presidio team the opportunity to highlight common security group policies in Firewall Manager, which is a capability the customer had not yet adopted. Finally, Presidio created a reference security group in the Security account and subsequently created a Firewall Manager policy based on the security group.

To minimize disruption to existing applications and workloads, the Firewall Manager policies for WAF and security groups were tested in a lab organization owned by the customer. Presidio then refactored the Terraform code to integrate with the customer's infrastructure automation pipeline. Using a new set of naming conventions for the new Firewall Manager policies allows teams to opt in on their terms.

Services / Technology Used

Amazon Macie, AWS Firewall Manager, AWS Lambda, Amazon DynamoDB, Amazon S3, AWS Key Management Service, AWS Identity and Access Management, Amazon VPC Security Groups, AWS WAFv2, Amazon SNS, Amazon SQS, Amazon EventBridge, Terraform, Fortinet

Results / Benefits

By teaming with Presidio and leveraging AWS-native security tooling, the financial services company was able to adequately report on CHD in its environment while guaranteeing firewall configurations remained compliant with PCI DSS.

Presidio brought knowledgeable staff to the engagement that could quickly support development activities in Terraform and AWS. Presidio collaborated with the customer on the design and implementation of both the sensitive data scanning solution powered by Macie, and the new Firewall Manager policies that were deployed. The engagement overall was successful and has created a continued partnership. The company is now able to accurately report on sensitive data across its AWS organization and can confidently attest to the efficacy of its firewall controls.

Partners

aws

FORTINET

HashiCorp

About Presidio

Presidio is a leading global digital systems integrator developing innovative technology solutions to help clients digitally transform their business. We specialize in simplifying IT by modernizing data, applications and infrastructure. Our full lifecycle model of professional and managed services power resilient cloud, security, infrastructure modernization and workforce transformation solutions for 7,000 middle market, enterprise and government clients. With an industry-leading 3:1 ratio of engineers to salespeople, we are uniquely positioned to develop and manage world-class business solutions at consumer speed. Partnering with Presidio allows organizations to capture new digital revenue streams while focusing on their core business. We handle the technical complexity and match spend to business value through flexible payment and consumption solutions.

For more information on how we connect IT of today to IT of tomorrow, visit presidio.com