PRESIDIO® | Case Study

Financial Services

PCI audit ready across 400+ AWS accounts - on deadline, no gaps in firewall coverage

The Outcome

A global fintech leader facing an imminent PCI compliance audit needed to scan cardholder data across 400+ AWS accounts and ensure every in-scope application had adequate firewall protections. Presidio delivered both on deadline - with automated detection and enforcement the company owns going forward.

How They Got There

Presidio ran two workstreams in parallel. For cardholder data detection: an automated scanning solution using Amazon Macie with Python Lambda functions pushing to DynamoDB and S3 across every region and account, refreshed by EventBridge every 24 hours. For firewall coverage: WAF Classic policies audited and upgraded to WAFv2, centralized through AWS Firewall Manager with Fortinet managed rule sets.

Why It Worked

Compliance audits against environments this large fail when coverage is inconsistent. Manual processes miss accounts. Firewall policies drift. Presidio automated both detection and enforcement - so the company could prove, not just claim, controls were in place across every account.

The Situation

A global fintech leader was approaching an imminent PCI compliance audit. The company uses AWS extensively across more than 400 accounts and needed to demonstrate that cardholder data was properly scoped and that every in-scope application had adequate firewall protections. Manual approaches were unworkable at this scale.

The Approach

Presidio tackled two workstreams simultaneously. For cardholder data detection: Amazon Macie with Python Lambda functions pushing findings to DynamoDB and S3 across every region and account, refreshed by EventBridge every 24 hours. For firewall coverage: WAF Classic audited and upgraded to WAFv2, centralized through AWS Firewall Manager. All infrastructure built in Terraform and validated in a lab before rollout.

The Result

The fintech company entered its PCI audit with automated, documented evidence of cardholder data detection and firewall coverage across all 400+ AWS accounts. The 24-hour automated refresh cycle ensures the compliance posture stays current. Terraform-built infrastructure makes the entire solution repeatable and auditable as the environment continues to grow.

400+

AWS accounts scanned and brought into PCI compliance scope

24-hour

Automated data refresh cycle — no manual intervention required

Repeatable

All infrastructure built as code - repeatable, auditable, scalable

PCI Compliance | AWS | Security | FinTech | WAF | Firewall Manager | Amazon Macie

PRESIDIO®