Kiteworks

CASE STUDY

FINANCIAL SERVICES | PCI DSS | FEDRAMP

Merchant-Acquirer Secures Issuer Data on Kiteworks (AWS)

A Fortune 500 payment technology company deployed Kiteworks on AWS to provide FIPS-validated, customer-managed encryption and a unified governed-exchange perimeter for sensitive issuer data shared with banking partners.

EMAIL PROTECTION GATEWAY | MANAGED FILE TRANSFER | DATA POLICY ENGINE (ABAC) | CMEK/AWS KMS | SIEM INTEGRATION | ITSM AUTOMATION

THE CHALLENGE

Two audit findings. One hard deadline. A regulated carve-out in flight.

What wasn't working

An internal audit found that encryption key material protecting payment-card data was managed in software -- not through a FIPS 140-3 validated HSM as required by banking clients. A second audit item demanded architectural and network security policy documentation that hadn't been delivered. Meanwhile, the company was carving out its regulated issuer-processing business alongside a broader AWS migration, requiring a full re-architecture of how sensitive data moves between the parent company, the new issuer entity, named banking partners, and downstream service providers -- all under a hard external contractual go-live deadline.

What Kiteworks delivered

Kiteworks secure data exchange -- deployed as a hardened virtual appliance across multiple AWS Availability Zones -- provided FIPS-validated AES encryption with CMEK offload to AWS KMS, closing both audit findings without additional licensing. A dual-deployment architecture (merchant division + card-issuing division) across U.S. and EMEA, with separate PCI CDE and non-CDE tenants, gave the company the structural separation the issuer carve-out required. Dedicated premium support engineers from Kiteworks were embedded in the program from day one.

> "Our risk team has an open audit item. They are looking for an architectural design policy and a network security policy — I have an open audit finding without them."

MANAGER, FILE TRANSFER & SERVICE AUTOMATION
A LEADING GLOBAL PAYMENT TECHNOLOGY PROVIDER

ARCHITECTURE

Multi-region, multi-tenant — built to separate regulated from non-regulated workloads

The deployment spans two AWS regions with distinct tenants for merchants and card-issuing divisions. Separate non-CDE and PCI CDE tenants were provisioned to support the issuer carve-out, ensuring regulated issuer data never commingles with non-PCI workloads. Authentication federates to the corporate identity provider over SAML 2.0, with LDAP group resolution and SCIM provisioning.

Multi-AZ/ multi-region

Hardened virtual appliance across U.S. and EMEA Availability Zones behind a Network Load Balancer. 4-hour RTO via all-inclusive snapshots.

Separate PCI CDE tenants

Distinct non-CDE and PCI Cardholder Data Environment tenants for the issuer carve-out. UAT environments mirror production for safe upgrade validation.

SAML 2.0 + SCIM

Authentication federated to corporate IdP. LDAP group resolution and SCIM provisioning. Hard deadline: November 2026 for full SSO groups integration for a major banking client.

ENCRYPTION & COMPLIANCE

FIPS 140-3 audit findings closed — no additional licensing required

Kiteworks uses FIPS-validated AES via OpenSSL in FIPS mode. CMEK offload to AWS KMS gives the security team a proper key hierarchy — working keys wrapped under a Customer-Managed Encryption Key — with double encryption at rest and key rotation through the admin interface. Because both deployments were already on AWS, the fix required only configuration changes, not re-architecture. UAT validation preceded production rollout. The resulting key-rotation framework is demonstrable to auditors and banking clients. Centralized vulnerability management lets patches deploy quickly across the entire cluster — a material improvement from the prior model.

FIPS 140-3	AES via OpenSSL in FIPS mode, CMEK via AWS KMS
PCI DSS	Separate CDE and non-CDE tenants, full audit trail
FEDRAMP	Kiteworks authorized; 30-day CVE resolution SLA
SIEM	All events exported via syslog; CISO Dashboard analytics

USE CASES

One platform governing four distinct data-exchange patterns

1

Merchant reporting at scale

Hundreds of gift card liability reports delivered weekly to external merchant contacts — accountants, CFOs, operations leads — within a one-hour contractual SLA. Ad hoc secure-send eliminates manual approval bottlenecks without sacrificing auditability.

2

Issuer-to-bank data exchange

Card-issuing division serves major U.S. financial institutions through a dedicated Kiteworks tenant. Each bank has its own authentication requirements, compliance expectations, and contractual deadlines — all managed under a single governance model.

3

ITSM-driven file automation

MFT integrates directly with the enterprise ITSM platform via API. Ticket-driven file movement eliminates manual handoffs for routine inter-entity transfers. Scheduled MFT workflows pull from object-store sources on defined cadences.

4

DLP & ABAC enforcement

Data Policy Engine enforces attribute-based access control across every content channel. ICAP integration with the enterprise DLP platform provides real-time content inspection on all inbound and outbound transfers. All events stream to SIEM via syslog.

RESULTS

Audited, certified, and operationally proven

2
Audit findings closed with no added licensing

2
AWS regions — U.S. and EMEA — under one governance model

1 hour
Merchant report SLA met weekly across hundreds of deliveries

4 hours
RTO target all-inclusive snapshot-based DR

Needs addressed

- ✓ FIPS 140-3 HSM-backed key management resolving open audit findings
- ✓ PCI-compliant exchange across merchant and card-issuing divisions
- ✓ One-hour SLA merchant reporting with on-demand external user access
- ✓ ABAC governance across file sharing, email, SFTP, and MFT
- ✓ DLP integration, SIEM-fed audit logging, ITSM file automation
- ✓ SSO/SAML 2.0 + SCIM for banking clients with hard contractual deadlines

Kiteworks capabilities deployed

- ✓ Kiteworks secure data exchange — multi-AZ on AWS, FedRAMP-authorized
- ✓ CMEK via AWS KMS with FIPS-validated AES and double encryption at rest
- ✓ Email Protection Gateway with S/SMIME and OpenPGP
- ✓ Data Policy Engine (ABAC) with ICAP DLP integration
- ✓ MFT with scheduled workflows and direct ITSM API integration
- ✓ Unified audit log with SIEM export and CISO Dashboard analytics