Case Study — Payments Automation Platform (GlobalPayex)

Security Posture Review & Resilience Roadmap — Fidantis Strategies

Client

GlobalPayex is a B2B payments/AR automation platform operating on AWS with EC2-based deployments, managed load balancers, VPN/IP allowlists, and a multi-AZ failover design.

Strengths

- Resilient infrastructure: multi-AZ with EC2/ALB; documented failover within ~15 minutes.
- Mature CI/CD basics: GitHub → Jenkins with environment-specific branches and Nexus artifacts.
- Access controls at the edge: self-managed VPN with static IPs and IP-based firewall rules.
- Foundational crypto: HTTPS/SFTP; at-rest encryption via AWS & MongoDB Atlas defaults.
- Security testing: external black-box testing and DAST (ZAP proxy).
- Compliance: SOC 1 Type 2, SOC 2 Type 2; GDPR in final stages.
- Onboarding security training; basic BCDR coverage for production apps.

Key Gaps & Risks

- No field-level encryption for PII/TII; MongoDB collections/indexes not protected at the column/field level.
- Keys fully cloud-managed; no customer-managed KMS or rotation policy.
- Support operations DR not documented (Freshservice/Mahaar); undefined RTO/RPO for non-prod.
- IAM/RBAC depth unclear; MFA enforcement for VPN/AWS not confirmed; limited access reviews/audit trails.
- Limited monitoring/telemetry: no consolidated SIEM/log correlation; IDS/IPS/WAF not clearly in scope.
- CI/CD security gaps: no SAST/container image scanning; secrets/credential storage controls not detailed.
- Risk register not actively maintained; retention policy lacks purge/archival lifecycle; training not refreshed.
- No formal incident response plan or vulnerability disclosure program.

Recommendations (Priority)

High:

- Implement application/field-level encryption for sensitive collections in MongoDB (e.g., client-side FLE).
- Introduce customer-managed keys (KMS/CMKs) with rotation and separation of duties.
- Define and document BCDR for support operations with explicit RTO/RPO targets.
- Complete GDPR program and initiate PCI-DSS readiness (encryption and access controls).

Medium:

- Publish an Incident Response Plan with runbooks, roles, and breach notification workflows.
- Establish recurring security awareness (quarterly/semiannual) with phishing simulations.
- Reactivate the risk register with ownership and quarterly reviews; align to audit readiness.
- Expand testing: add white-box reviews, SAST, and container scanning in CI/CD.
- Centralize logging (SIEM); enable GuardDuty/CloudTrail org-wide; consider WAF/IDS.
- Define data classification, archival, and purge schedules aligned to contractual/legal standards.
- Enforce MFA for VPN and AWS; least-privilege IAM roles; periodic access recertification.

90-Day Plan

Day 0–30

- Enable MFA across VPN/AWS; tighten IAM roles and disable legacy access.
- Turn on GuardDuty/CloudTrail/CloudWatch centralization; define log retention baselines.
- Publish initial IRP and on-call escalation; schedule a 60-minute tabletop.
- Draft RTO/RPO thresholds for critical services and support tools.

Day 31–60

- Pilot client-side field-level encryption for one high-sensitivity collection.
- Onboard logs to a SIEM and define alert triage; add WAF rules/Cloudflare security features.
- Integrate SAST and container scanning; harden secrets management.
- Document BCDR for Freshservice/Mahaar & non-prod; perform a restore test.

Day 61–90

- Roll out FLE to remaining sensitive datasets; enforce KMS key rotation.
- Run a full tabletop/restore drill; publish after-action updates to runbooks.
- Adopt data lifecycle (archival/purge); finalize GDPR artifacts; start PCI evidence collection.
- Stand up a lightweight VDP (responsible disclosure) with intake workflow.

At-a-Glance

Platform: B2B Payments/AR Automation

Cloud: AWS (EC2/ALB, EFS/S3; Cloudflare/IP allowlists)

Pipeline: GitHub → Jenkins → Nexus

Database: MongoDB Atlas

Certifications: SOC 1/2; GDPR in progress; PCI planned

Source

Fidantis walkthrough & preliminary assessment summary (internal).