



Travel Agency Platform Rebuild

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1

Rebuilding a Global Travel Booking Platform: 80% Faster Checkout, PCI-DSS Compliance, and Peak-Season Resilience

1

1.1

Executive Summary

1

1.2

The Challenge

1

1.3

Our Approach

2

1.4

Implementation

2

1.5

Results & Impact

4

1.6

Technologies & Services Used

4

1.7

Conclusion

5

About The Origami Corporation

1

Rebuilding a Global Travel Booking Platform: 80% Faster Checkout, PCI-DSS Compliance, and Peak-Season Resilience

1.1

Executive Summary

A leading travel agency was losing customers due to slow booking performance and perceived payment security gaps. We executed a full-stack rebuild across web and mobile, architected a payment orchestration layer integrating 15 providers, and led a comprehensive compliance-audit-pci-dss program. The result: booking workflows process 80% faster, cart abandonment was reduced by half, and the platform successfully resisted coordinated DDoS attacks during peak holiday demand—all while achieving PCI-DSS compliance and improving customer trust.

1.2

The Challenge

The client’s legacy monolith struggled under seasonal spikes and global traffic patterns:

- Slow page loads and multi-step checkout friction drove high abandonment.
- Limited payment options and regional routing caused declines and drop-offs in key markets.
- Incomplete PCI-DSS controls left the business exposed to compliance risk and reputational damage.
- No systematic DDoS protection meant peak campaigns were vulnerable.
- Mobile experiences lagged, with inconsistent performance and missing native payment capabilities.

The business imperative was clear: modernize the platform end-to-end to improve speed, resiliency, and trust—without disrupting ongoing revenue.

1.3 Our Approach

We delivered a holistic transformation across web-development, mobile-development, payment-integration, compliance-audit-pci-dss, and ddos-protection: - Discovery and benchmarking: instrumented baseline performance and conversion metrics to guide priorities. - Architecture re-design: decomposed the monolith into API-first services with a scalable, cache-forward architecture. - Customer-first UX: streamlined checkout across web and mobile, minimizing steps and latency. - Payment orchestration: unified 15 payment providers under a single, fault-tolerant abstraction for global coverage. - Compliance by design: embedded PCI-DSS requirements into the build, with formal audit and validation. - Defense in depth: implemented multi-layer DDoS and application security protections. - Controlled rollout: used blue/green deployments, canary releases, and feature flags to manage risk.

1.4 Implementation

1) Web-development architecture and performance

- Front end: Rebuilt the booking experience using React and server-side rendering (Next.js) for fast time-to-first-byte, route-based code splitting, and prefetching of critical assets. Implemented image optimization and Brotli compression, backed by a global CDN for static and edge-cached dynamic content.
- Services: Implemented stateless, containerized microservices (NestJS/Node.js) behind an API gateway with request validation (OpenAPI), idempotency keys for checkout endpoints, and circuit breakers/timeouts to isolate failures.
- Data layer: Migrated to PostgreSQL with read replicas and connection pooling; added Redis for session and query caching; introduced a background job queue (RabbitMQ) for asynchronous tasks (ticketing confirmations, email dispatch, webhooks).
- Query optimization: Audited slow queries, added targeted indexes, and applied read/write separation to stabilize p95 latencies during surge traffic.
- Observability: Standardized OpenTelemetry tracing across services, with metrics/dashboards for throughput, error rates, and cache hit ratios. Established SLOs for checkout latency and availability.

2) Mobile-development for iOS and Android

- App foundation: Developed a cross-platform React Native application to align UI/UX with the web while leveraging native modules for performance-sensitive flows.
- Native payments: Integrated Apple Pay and Google Pay for one-tap checkout; enabled biometric authentication for stored payment tokens; supported deep links from marketing campaigns to prefilled booking flows.

- Performance: Implemented offline caching for recent searches, skeleton screens, and prioritized rendering of price and availability data to reduce perceived wait times.

3) Payment-integration with a provider-agnostic orchestration layer

- Unified API: Built a payment orchestration layer that abstracts 15 different payment providers (cards, wallets, BNPL, and local methods) behind a single API and schema. Merchandising logic selects optimal providers by region, currency, and risk profile.
- Smart routing and failover: Employed configurable routing rules to balance authorization success rates against fees and latency; implemented provider failover and automatic retries for transient errors.
- Tokenization and vaulting: Minimized PCI scope by tokenizing PANs and storing only tokens within the booking system; integrated a PCI-compliant vault and detached sensitive processes from the general application network segments.
- 3DS2 and SCA readiness: Enabled frictionless 3D Secure 2 flows where possible, triggering step-up authentication only when risk engines indicated.
- Reconciliation and webhooks: Built idempotent webhook processors and automated reconciliation jobs to align provider settlements with internal ledgers.

4) compliance-audit-pci-dss program

- Gap analysis: Mapped existing controls to PCI-DSS requirements and identified deficiencies across network segmentation, key management, vulnerability management, and logging.
- Remediation: Implemented TLS 1.2/1.3 everywhere; enforced strong cryptography at rest (AES-256) and HSM-backed key rotation; centralized logs to a SIEM with immutable retention and alerting; enforced MFA and least-privilege IAM; instituted file integrity monitoring, quarterly ASV scans, and annual penetration testing.
- Policies and procedures: Documented secure SDLC, change management, incident response, and access review processes; trained engineering and operations teams.
- Validation: Partnered with a Qualified Security Assessor to review controls and produce a Report on Compliance, achieving PCI-DSS compliance on the new platform.

5) ddos-protection and application security hardening

- Edge protection: Deployed a global CDN with Anycast, WAF rulesets, and bot management. Implemented geo-fencing and reputation-based filtering for Layer 7 traffic.
- Rate limiting and anomaly detection: Added adaptive rate limiting at the API gateway and per-user quotas for sensitive endpoints; deployed request scoring to throttle automated scraping without impacting real users.

- Network resiliency: Built multi-AZ redundancy with health-based failover; introduced autoscaling policies tied to request rate and queue depth to absorb flash crowds.
- Hardening: Security headers, content security policy, strict transport security, and secure cookie practices; regular dependency scanning and SCA in CI/CD.

6) Migration and release strategy

- Data migration: Ran dual-write patterns and change data capture to backfill new schemas with zero downtime.
- Progressive rollout: Used feature flags, canary percentage rollouts, and blue/green deployments to validate performance and error budgets before full cutover.
- Runbooks and drills: Created operational playbooks and conducted load tests and game days ahead of holiday peaks.

1.5 Results & Impact

- 80% faster booking processing: End-to-end booking workflows now complete in a fraction of the previous time thanks to SSR, aggressive caching, and optimized queries. Customers experience noticeably faster searches, selections, and checkout.
- 50% reduction in cart abandonment: A streamlined checkout, mobile wallets, and improved payment reliability materially increased conversion.
- Expanded global reach: Integration with 15 payment providers unlocked local payment preferences and reduced friction across key regions, improving authorization reliability and customer confidence.
- Proven resilience under attack: During peak holiday booking season, the platform sustained high loads and successfully defended against DDoS attempts without customer-visible disruption.
- Compliance and trust: Achieved PCI-DSS compliance with audited controls, strengthening brand trust and reducing regulatory risk.
- Operational excellence: Enhanced observability and SLOs improved incident response, while autoscaling and queue-based back-pressure stabilized performance under surges.

Collectively, these outcomes delivered a faster, safer, and more reliable booking experience that directly translates to higher conversion and sustained revenue during the agency's most critical sales periods.

1.6 Technologies & Services Used

- Services: web-development, mobile-development, payment-integration, compliance-audit-pci-dss, ddos-protection

- Front end: React, Next.js (SSR), React Native (iOS/Android), global CDN, image optimization
- Back end: Node.js (NestJS) microservices, API gateway, OpenAPI validation, Redis caching, RabbitMQ job queue
- Data: PostgreSQL with read replicas, connection pooling, targeted indexing
- Security and compliance: TLS 1.2/1.3 everywhere, AES-256 at rest, HSM/KMS-backed key management, SIEM with centralized logs, MFA/least privilege IAM, WAF, bot management, rate limiting
- Payments: Payment orchestration layer with provider-agnostic API, tokenization and vaulting, 3DS2/SCA, webhook processing and reconciliation
- Platform and tooling: Containers, Kubernetes-based autoscaling, OpenTelemetry tracing, metrics dashboards and alerting, CI/CD with SAST/DAST and dependency scanning

1.7 Conclusion

By unifying modern engineering practices with compliance-by-design and layered security, we transformed a fragile legacy stack into a performant, resilient, and trusted travel booking platform. The rebuilt system processes bookings 80% faster, halves abandonment, and confidently sustains peak-season demand while meeting PCI-DSS requirements. This project demonstrates how an integrated approach—spanning web-development, mobile-development, payment-integration, compliance-audit-pci-dss, and ddos-protection—can unlock measurable business outcomes and long-term competitive advantage.

About The Origami Corporation

The Origami Corporation is a leading technology consulting firm specializing in cloud migration, DevSecOps, cybersecurity, and digital transformation. We help organizations navigate complex technological challenges and achieve their business objectives through innovative, secure, and scalable solutions.

Connect With Us

Follow Us Online

LinkedIn: [The Origami Corporation](#)

Facebook: [@theorigamicorporation](#)

X (Twitter): [@OrigamiGlobal](#)

Telegram: [@theorigamicorporation](#)

Contact Information

Europe & Americas

- **Email:** office@theorigamicorporation.com
- **Phone:** +359 878 686 627

Asia-Pacific, Middle East & Africa (APMEA)

- **Email:** office.apmea@theorigamicorporation.com
- **Phone:** +41 77 924 2245

Ready to Get Started?

SCHEDULE A MEETING

Ready to transform your technology infrastructure? Contact us today to discuss how we can help your organization achieve similar results.