DEVHAWK

Create a mobile-first dating platform tailored to nocturnal and supernatural use

Mainstream dating apps are designed for diurnal humans and lack the concepts, data, and UX needed by supernatural users (nocturnal availability, lunar cycle impacts, species-specific hazards, and cros

100	30	159	7
QUALITY SCORE	USER STORIES	STORY POINTS	EST. SPRINTS

Generated: February 06, 2026

Version: v1

App Type: Mobile App

Table of Contents

1 Executive Summary

Business Problem

Create a mobile-first dating platform tailored to nocturnal and supernatural users (vampires, werewolves, etc.) that respects their safety, schedules, and secrecy while enabling species-aware matching and verified profiles.

Mainstream dating apps are designed for diurnal humans and lack the concepts, data, and UX needed by supernatural users (nocturnal availability, lunar cycle impacts, species-specific hazards, and cross-species social dynamics). NightBond must deliver a private, high-trust dating environment that models nocturnal schedules, moon-phase-aware scheduling, species-aware matching, and safety features (garlic/silver/UV/wolfsbane alerts), while preventing identity leakage and human catfishing through a confidential species verification process.

> **Current Solution:** No dedicated platform exists; supernatural users use mainstream dating apps or informal community networks that ignore species-specific constraints and safety needs.

> **Why Change:** The target market is underserved: mainstream apps cause dangerous or inconvenient match suggestions, lack safety and verification, and fail to normalize cross-species relationships. A purpose-built app can capture high lifetime value users and a first-mover advantage.

Target Users

ROLE	DESCRIPTION	PRIMARY GOALS
Vampire (including Daywalkers)	Immortal or long-lived nocturnal individuals with daylight sensitivity variances, interest in discrete dating and species-aware matches.	Find compatible partners who respect nocturnal schedules and dietary needs, Maintain secrecy of supernatural identity, Access verified, safe venues and community events
Werewolf (pack-affiliated or lone)	Humans who transform according to lunar cycles, with pack dynamics and territorial concerns; need scheduling that respects transformation days.	Coordinate dates around lunar cycles and transformation windows, Connect with pack-friendly or cross-species-aware partners, Avoid silver/wolfsbane hazards
Cross-species couple / matcher	Users intentionally seeking cross-species relationships; need tooling for negotiation, etiquette, and shared scheduling.	Understand compatibility implications (diet, schedules, clan etiquette), Plan safe, discreet dates, Access moderated forums and shared calendars
Admin / Elder Verifier	Platform operators and appointed elders who verify species claims, manage safety reports, and moderate sensitive community content.	Process verifications reliably and confidentially, Respond to safety incidents, Maintain policy compliance and user privacy

Key Metrics

METRIC	VALUE
Application Type	Mobile App
Deployment Model	Cloud
Total Epics	5
Total Features	14
Total User Stories	30
Total Story Points	159
Estimated Sprints	7
Quality Score	100/100

Success Criteria

- 100k registered users within six moon cycles
- 500 species verifications per week sustained after launch
- Average time-to-first-compatible-match < 3 nights for active users
- 30-day retention >= 40% for active nocturnal users
- Premium conversion rate >= 5% within six moon cycles
- System availability >= 99.9% for core APIs (matching, messaging, scheduling)
- Push notifications never include species or transformation content in notification previews (0 incidents)
- Mean API response time for matching and scheduling endpoints < 300ms
- Average verification turnaround: 48 hours for premium, < 14 days for free tier

2 Discovery & Requirements

Requirements (In Scope)

ID	PRIORITY	DESCRIPTION
REQ-001	P1	A guided mobile onboarding flow to capture species/sub-type, era/age, nocturnal schedule, transformation patterns, dietary preferences, pack/territory, photos (night-vision compatible), relationship goals, and supernatural love language assessment. Includes progressive disclosure and privacy controls for each attribute. Scenarios: A newly turned vampire completes onboarding, uploads night-vision photos, and sets daylight tolerance to 'none' before browsing matches., A werewolf sets recurring unavailability for full-moon windows and shares limited pack affiliation visible only to verified pack members.
REQ-002	P1	Matching service that evaluates compatibility using species-specific attributes (diet, era, pack status, territorial constraints), computes explainable compatibility scores, and surfaces safety notes on match cards (e.g., venue hazards). Supports weight adjustments by users and A/B testing of matching heuristics. Scenarios: The engine deprioritizes matches that conflict on territory boundaries unless both override., A user sees compatibility score breakdown and a short explanation (e.g., 'High schedule overlap; caution: silver content risk').
REQ-003	P1	Integrated lunar calendar that drives availability, date suggestions, and scheduling rules (avoids full moons for werewolves, suggests new-moon evenings for vampires). Includes recurring availability patterns, timezone-aware scheduling, and sunset/sunrise calculations by location. Scenarios: When scheduling a date, the tool disables times during both participants' full-moon blackout windows., A vampire receives an automated sunrise countdown and safe-harbor suggestions if a date is running past dawn.
REQ-004	P1	Secure sign-up/login, device-bound tokens, granular privacy toggles (what profile fields appear in push previews or to non-verified users), and a manual species verification workflow with an admin Elder Council interface and audit logging. Scenarios: A user requests priority species verification via premium flow; the Elder admin reviews and flags outcome., Notifications are filtered so the push preview never contains species or transformation details.
REQ-005	P1	In-app messaging that supports scheduled/dusk-delivery (dawn-delayed messages), voice notes with night-mode audio filters, species-contextualized presence, and optional end-to-end encryption for private conversations. Scenarios: A user composes a message at 10am local and schedules it to deliver at dusk for the recipient., A voice note sent from a noisy street is processed with night-mode filter to reduce ambient noise.
REQ-006	P1	

ID	PRIORITY	DESCRIPTION
		Venue and location safety scoring combining public data, partner menus, and crowd-sourced reports to flag garlic-heavy venues, silver-content risks, wolfsbane sightings, and UV exposure windows; integrates with scheduling and concierge. Scenarios: A vampire receives a garlic-zone alert when a suggested restaurant's menu shows heavy garlic usage., A werewolf gets a warning before accepting a gift-swap event near a reported wolfsbane patch.
REQ-007	P2	Personalized, nocturnally-optimized venue and activity recommendations that respect schedule, species safety, territory, and user preferences. Recommendations learn from user feedback to improve over time. Scenarios: Concierge suggests underground jazz bar with blackout rooms for a cross-species first date., User rates a suggested blood bar; the system adapts future suggestions for similar profiles.
REQ-008	P1	Panic/accelerometer-triggered flow that sends a discreet human-passing message to the date, shares location with a user-designated safety contact, silences notifications for a configurable window, and logs the incident for admin review. Scenarios: A werewolf triggers ETP at a date; the date receives a discreet 'personal emergency' message and the user's pack safety contact is alerted., ETP silences incoming notifications for 6 hours to prevent phone vibrations during transformation.
REQ-009	P1	Secure admin tools for managing species verification requests, reviewing flagged safety reports, moderating community content, and exporting anonymized audit logs for compliance. Includes role-based access control and encrypted storage for sensitive artifacts. Scenarios: An Elder reviewer sees a queue of pending verifications with anonymized evidence attachments and marks outcomes., Support staff triages a clan-conflict report and triggers temporary match restrictions between factions.
REQ-010	P2	Subscription management for premium features: unlimited nightly matches, priority verification, advanced compatibility reports, event access, and UI customizations. Includes integration with Stripe and coupon management. Scenarios: A premium subscriber purchases NightBond Eternal and receives priority verification with a shorter SLA., Billing fails for a subscriber and the system gracefully downgrades features with notification.
REQ-011	P1	System-wide policies and technical controls to prevent exposure of species or supernatural details in push notifications, lock screens, analytics, or third-party integrations. Includes opt-in data-sharing policies and anonymous analytics. Scenarios: A push notification reads 'You have a new message' without species or transformation details., Analytics are collected only as anonymized aggregates unless explicit opt-in is given.
REQ-012	P1	Integrations with lunar-phase APIs (e.g., Moon API), mapping/geocoding services, restaurant/venue data sources, and crowd-sourced hazard reports. Includes sync jobs, rate-limit handling, and fallback local calculations for lunar data. Scenarios: The scheduling engine calls the lunar API to compute next full moon and disables booking for affected users., When map provider rate limits, the system falls back to cached venue hazard data.

ID	PRIORITY	DESCRIPTION
REQ-013	P2	Telemetry for product metrics (retention, match rates), system monitoring (uptime, latency), and fraud detection for suspicious accounts or verification bypass attempts. Alerts for admin teams and automated throttling for suspected abuse. Scenarios: An unusual spike in verification rejections triggers an automated alert to operations., Fraud model temporarily blocks account actions pending manual review.
REQ-014	P2	Moderated, private community spaces and a cross-species compatibility guide with etiquette, shared calendars, and moderated discussions; visibility controls so participation remains private from non-members. Scenarios: A cross-species couple accesses a guide on meeting each other's clan and shares a synchronized calendar overlay., Moderated forum threads allow vets to advise new cross-species daters while protecting identities.

Identified Risks

- Verification throughput risk: Manual Elder verification creates a scale bottleneck that could slow growth and frustrate users.
- Privacy & leakage risk: Push notifications, analytics, or vendor integrations could accidentally expose species information leading to safety breaches and legal liability.
- Data accuracy risk: Venue hazard data (garlic/silver/wolfsbane) will be incomplete and may produce false negatives/positives, creating safety liability.
- Technical complexity: Combining relational, graph, and caching layers increases operational complexity and cost.
- Abuse & fraud: Actors may attempt to game matching, spoof schedules, or create fake verifications; fraud detection models will be necessary early.
- Regulatory risk: Handling sensitive identity attributes (species as protected identity?) could raise novel legal/ethical questions depending on jurisdiction.
- User adoption risk: Niche market estimates may be optimistic; slower-than-expected adoption could make premium revenue projections unreachable.
- ETP reliability risk: False positives/negatives in Emergency Transformation Protocol (sensor-triggered) could endanger users or lead to nuisance incidents.

Tech Stack Recommendations

CATEGORY	TECHNOLOGY	RATIONALE	ALTERNATIVES
Frontend (mobile)	React Native with TypeScript	Mobile-first cross-platform development speeds delivery for iOS and Android, supports native device APIs (camera, location, sensors), and allows a single codebase for dark/night UI optimizations.	Flutter (Dart) — excellent performance and expressive UI Native iOS (Swift) & Android (Kotlin) — best native performance and platform-specific privacy controls
Backend			

CATEGORY	TECHNOLOGY	RATIONALE	ALTERNATIVES
	Node.js + TypeScript (NestJS) or Kotlin + Ktor	Node.js ecosystem supports real-time features (WebSockets/Push), fast iteration, strong package ecosystem for geolocation and third-party integrations. NestJS adds structure for maintainability. Kotlin/Ktor is an alternative for stronger typing and JVM ecosystem.	Python (Django/DRF) — rapid dev, strong data tooling Go — high performance for matching engines and concurrency
Database	PostgreSQL (primary) + Redis (cache & presence) + Neo4j (social graph / matching)	Postgres handles relational profile data, PostGIS extensions support territorial queries; Redis for low-latency presence and scheduling locks; Neo4j accelerates complex relationship queries and compatibility scoring.	CockroachDB (geo-distributed SQL) ArangoDB (multi-model including graph)
Auth & Privacy	Custom authentication with JWT + device-bound tokens, optional end-to-end encrypted messaging (Signal protocol library)	Third-party auth providers risk data sharing; custom auth gives strict control over notification content and privacy. E2EE recommended for sensitive messaging and to prevent species exposure.	Auth0 or Firebase Auth (faster integration but third-party risk) Keycloak (self-hosted identity)
Specialized services	Moon API (lunar data) + Mapbox/Google Maps or OSM (geocoding) + Cloud functions (AWS Lambda/GCP Cloud Functions) + Stripe (payments) + Twilio (SMS) or in-app push provider	Moon API provides authoritative lunar phases and illumination data; mapping for territory and venue lookup; serverless functions for event-driven tasks; Stripe for subscriptions; Twilio for optional OTP or safety alerts.	Self-hosted lunar calculations (astronomy libraries) for independence MapTiler or HERE Maps instead of Google/Mapbox
Hosting & Infra	AWS (EKS/Fargate) or GCP (GKE/Cloud Run) + Cloudflare CDN + Terraform for infra as code	Cloud provider for reliability, horizontal scaling, and managed DB/queue services. Cloudflare for edge caching and WAF to protect privacy-sensitive endpoints.	Azure (AKS) — enterprise-friendly Managed hosting via Platform.sh

Clarifications

Q: What SLA and throughput target should Elder Council verification meet at launch?

> Priority 48-hour turnaround for premium, 2-week for free; capacity plan to reach 500/week at launch with staged scaling to 1,500/week by month 3.

Resolved

Q: Are third-party integrations (venue/restaurant menu data) permitted if contracts involve limited data sharing?

> Yes, but only ingest venue metadata (menus, ingredient tags, material/metal info) via contractual B2B integrations that ensure no user-level or species data is shared externally.

Resolved

Q: Will end-to-end encryption be mandatory for all private messages?

> Make E2EE optional and recommended; provide server-side encryption for non-E2EE messages to allow safety moderation under strict controls and legal processes.

Resolved

Q: Is social media or public sharing explicitly banned even as an opt-in?

> Yes — social media integration and public sharing are disallowed at platform level. Users may export anonymized, non-species personal data for portability per data rights, but not species indicators or supernatural attributes.

Resolved

Q: Acceptable fallback for lunar data if a third-party lunar API is unavailable?

> Implement local astronomical calculations (astronomy libraries) as primary fallback and maintain a cached lunar calendar per region updated nightly.

Resolved

3 Architecture & Technical Design

Architecture Style: Modular Microservices

A mobile-first, privacy-first modular microservices architecture that separates transactional relational data, relationship graph data, real-time presence/messaging, and specialised domain engines (matching, safety, verification). Justification: microservices provide bounded contexts for species-aware rules, verification workflows, and the real-time constraints of nocturnal scheduling while allowing independent scaling (matching/graph vs auth/messaging). The system uses event-driven integration and CQRS read models so graph traversals and recommendation workloads do not block OLTP.

System Components

Mobile App
Technology: React Native + TypeScript

API Gateway & WAF
Technology: Cloudflare + AWS ALB + Kong/Envoy

Auth & Privacy Service
Technology: NestJS + secure enclave integrations (Keychain/Keystore)

User & Profile Service
Technology: NestJS + PostgreSQL

Matching & Scoring Service
Technology: NestJS/Kotlin microservice; rule engine (Drools or custom TypeScript rules)

Graph Service
Technology: Neo4j Aura + sync microservice (Debezium CDC -> Event Bus)

Messaging & Scheduling Service
Technology: NestJS + libsignal (or equivalent) + Redis

Verification & Admin Service
Technology: NestJS + Admin React Console

Data Models

MODEL	DESCRIPTION	FIELDS
User	Authentication and identity anchor — minimal PII; device bindings and privacy settings.	id email_hash device_ids roles privacy_config
Profile	Species-aware public profile content stored with privacy controls (what is visible to whom).	id user_id species availability visibility_rules
Match	Representation of a match instance and state between two users.	id user_a_id user_b_id state compatibility_score
VerificationRequest	Tracks species verification evidence, assigned elder, and audit trail.	id user_id status evidence_refs assigned_elder
EventSchedule	Moon-aware scheduling entries for dates, invites and ETP triggers.	id owner_id start_time end_time hazard_flags

Security Design

Authentication: Device-bound short-lived JWTs + refresh tokens stored in secure enclave; optional hardware-backed keys (Secure Enclave / Android Keystore); token rotation and device revocation APIs

Authorization: RBAC for platform roles (admin/elder/moderator) + ABAC-style rules for species-specific access control and visibility rules

Data Protection: TLS 1.2+ in transit, server-side encryption at rest (KMS-managed keys) for databases and S3; E2EE for messaging via Signal protocol, attachments encrypted client-side

Infrastructure

Hosting: AWS (primary) with optional multi-cloud for critical services

CI/CD: GitHub Actions for pipelines, Terraform for infra provisioning, ArgoCD for GitOps deployment

4 User Stories

5 Epics • **14** Features • **30** Stories • **159** Story Points • **7** Estimated Sprints

Nocturnal & Supernatural Matching Core

Mobile-first onboarding, species-aware matching, and lunar-aware scheduling to enable safe, private dating for nocturnal and supernatural users.

Mobile Onboarding & Supernatural Profile Builder

US-001 Vampire Onboarding: Night-vision photos & daylight tolerance

5 SP | MEDIUM

GIVEN a new user is in the mobile onboarding flow **WHEN** they select 'Vampire', upload a night-vision photo, and set daylight tolerance to 'none' **THEN** the profile persists the photo tagged 'night-vision', the photo's visibility defaults to 'matches-only', and availability defaults to nocturnal-only

GIVEN the user completed onboarding with daylight tolerance set to 'none' **WHEN** they access match search or are included in matching queries **THEN** daytime venues and daytime scheduling slots are excluded from candidate results and available times

Traces to: REQ-001

US-002 Werewolf Full-Moon Blackout & Pack Visibility

5 SP | MEDIUM

GIVEN a werewolf user configures profile settings and enables recurring full-moon unavailability **WHEN** the lunar calendar calculates upcoming full-moon windows for the user's location **THEN** the user's calendar shows recurring blackout windows and scheduling APIs reject invites overlapping those windows

GIVEN the werewolf user sets pack affiliation visibility to 'pack-only' **WHEN** another user views the profile **THEN** pack affiliation is hidden unless the viewer is flagged as a verified member of the same pack

Traces to: REQ-001

Species-Aware Matching Engine & Compatibility Scoring

US-003 Explainable Compatibility Scores & Weight Adjustments

8 SP | MEDIUM

GIVEN two user profiles and system default species-specific scoring weights **WHEN** the matching pipeline runs for candidate generation **THEN** the API returns a numeric compatibility score plus a breakdown by category (schedule, diet, era, territory) and a one-line human-readable explanation

GIVEN a user updates weight sliders for categories (e.g., increases schedule weight by 20%) and saves preferences **WHEN** the matching pipeline runs after the change **THEN** results reflect the updated weights and the returned score breakdown shows the new category contributions

Traces to: REQ-002

US-004 Match Card Safety Notes: Territory & Hazard Surfacing

5 SP | MEDIUM

GIVEN a candidate's territory overlaps the user's blocked zone or a hazard feed flags a venue (e.g., silver hazard) **WHEN** the match card is rendered in the mobile UI **THEN** the card displays a contextual safety note (e.g., 'territory conflict — mutual override required' or 'caution: silver hazard nearby') including a confidence score and link to details

GIVEN both users perform an explicit mutual override for a territory restriction **WHEN** the override is recorded **THEN** the match is surfaced normally but a persistent audit flag is created for Verification/Admin review

Traces to: REQ-002

Moon-Phase Calendar & Smart Scheduling

US-005 Full-Moon Blackout Scheduling Enforcement & Fallback

5 SP | MEDIUM

GIVEN two participants with blackout windows derived from lunar data **WHEN** one attempts to schedule a date that overlaps either blackout window **THEN** those overlapping slots are disabled in the scheduling UI and alternative slots outside blackout windows are suggested

GIVEN the primary lunar API is unreachable and a cached/local lunar calculator exists on server or device **WHEN** scheduling requests are made **THEN** blackout windows are computed locally and the UI marks the data as 'fallback lunar data'

Traces to: REQ-003

US-006 Sunrise Countdown & Safe-Harbor Suggestions (offline fallback)

3 SP | MEDIUM

GIVEN an ongoing date with planned end time approaching sunrise for a participant's location **WHEN** remaining time crosses a configurable threshold (e.g., 30 minutes) **THEN** both participants receive a silent encrypted countdown notification and a ranked list of the top 3 nearby night-friendly safe-harbor venues with hazard/confidence metadata

GIVEN a participant is offline but has local schedule and cached safe-harbor data in encrypted storage **WHEN** the countdown threshold is reached **THEN** the device triggers a local secure notification and displays cached safe-harbor options from encrypted local storage

Traces to: REQ-003

Safety, Privacy & Messaging for Nocturnal Supernaturals

Secure device-bound auth, granular privacy and Elder-driven species verification; scheduled/night-mode messaging with optional E2EE and audio filters; hazard-aware venue scoring integrated with scheduling and alerts.

Authentication, Privacy Controls & Elder Verification

US-007 Device-bound authentication, token rotation and device revocation

8 SP | MEDIUM

GIVEN a registered device and valid credentials **WHEN** the user authenticates successfully **THEN** the system issues a short-lived JWT tied to the device id, creates a refresh token stored in the device secure enclave, and writes a device-registration audit entry

GIVEN a device revocation request (user or admin) **WHEN** revocation is executed **THEN** the revoked device's refresh token is invalidated, active access tokens from that device are blacklisted, other device sessions remain valid, and an audit log entry and in-app notification are created

Traces to: REQ-004

US-008 Granular privacy toggles and premium priority verification request

5 SP | MEDIUM

GIVEN the user has privacy settings set to hide species or transformation details **WHEN** a notification or push preview would be generated **THEN** the preview is obfuscated (generic text) and any species/transformation fields are excluded from push payloads and non-verified user views; an event is logged

GIVEN the user submits a premium priority verification request with payment or entitlement **WHEN** the request is accepted by the payments service **THEN** a VerificationRequest is created with priority flag, the Elder dashboard surfaces the request with SLA metadata, and audit logs record payment-to-request linkage

Traces to: REQ-004

Messaging with Scheduled Delivery & Night-mode Audio

US-009 Scheduled dusk/dawn delivery with lunar API fallback

8 SP | MEDIUM

GIVEN the sender schedules a message for "recipient dusk" and recipient location (or preferred timezone) is available **WHEN** the scheduling service reaches the computed dusk time (using Lunar/Moon Phase API) **THEN** the message is released to delivery respecting recipient privacy settings (obfuscated push if set) and message metadata records scheduled->delivered timestamps

GIVEN the Lunar/Moon Phase API is unavailable or rate-limited **WHEN** the scheduler must compute dusk/dawn **THEN** the scheduler falls back to cached lunar calendar or local astronomical calculation (within configurable tolerance, e.g., ±30 minutes), delivers the message, and logs the fallback event

Traces to: REQ-005

US-010 Night-mode voice note processing and optional E2EE

5 SP | MEDIUM

GIVEN the user records a voice note in a noisy environment and uploads it **WHEN** the client or server-side processor applies night-mode filtering **THEN** the stored audio asset is the processed file, SNR improves to meet the configured threshold (e.g., +6dB), and the message metadata includes a night-mode-processed flag

GIVEN two participants enable E2EE for the conversation via Signal-protocol key exchange **WHEN** keys are exchanged successfully **THEN** messages and attachments (including processed voice notes) are stored only as ciphertext on servers, servers hold delivery metadata only, and the E2EE-enabled state is recorded in audit logs

Traces to: REQ-005

Supernatural Safety Engine & Real-time Hazarding

US-011 Venue hazard scoring and scheduling integration

8 SP | MEDIUM

GIVEN a venue has public menu data, partner feeds, and crowd-sourced reports **WHEN** the Safety Engine runs enrichment and scoring **THEN** it computes a composite safety score using weighted factors, surfaces hazard flags with a human-readable rationale on the venue and scheduling UI, and timestamps the last data refresh

GIVEN a user attempts to schedule a date at a venue with a safety score below the species-specific safety threshold **WHEN** the user proceeds to confirm the booking **THEN** the system either blocks the booking or requires an explicit two-step hazard-acknowledgement (recorded in event audit trail) before allowing the booking

Traces to: REQ-006

US-012 Real-time hazard alerts for events and elder-submitted reports

5 SP | MEDIUM

GIVEN a hazard report (automated feed or Elder submission) geo-affects a scheduled event location **WHEN** the Safety Engine ingests the report and recalculates region scores **THEN** impacted users within the geofence receive in-app hazard alerts (severity and confidence shown), safe alternatives are suggested, and the alert is recorded in the event's audit trail

GIVEN an Elder/admin submits a hazard with confidence level **WHEN** the submission is processed **THEN** the venue/event safety score is recalculated, notifications are delivered according to each user's privacy settings, and the submission is versioned in the verification audit logs

Traces to: REQ-006

Nocturnal Safety, Verification & Date Concierge

Provide species-aware date recommendations, a reliable Emergency Transformation Protocol (ETP), and secure admin/elder verification tooling to protect user safety, secrecy and regulatory compliance.

Date Night Concierge & Learning Recommendations

US-013 Personalized nocturnal venue recommendations

5 SP | MEDIUM

GIVEN a user with species, nocturnal availability windows, territory, hazard preferences and enabled concierge **WHEN** the user requests date recommendations (via UI or API) for a specific date/time window **THEN** the system returns a ranked list of at least 5 venues filtered by schedule compatibility, species-safety rules, territorial restrictions and hazard overlays; each venue includes a confidence score and reason tags (e.g., 'blackout room', 'no garlic') and the response caches the recommendation event for feedback collection

GIVEN the concierge pipeline has access to graph candidates, hazard feeds, lunar data and user preferences **WHEN** the concierge builds candidate venues for the user **THEN** the system persists the recommendation event, candidate metadata and selection signals to the recommendations store so future reranks and ML training can use the data

Traces to: REQ-007

US-014 Venue feedback and adaptive reranking

3 SP | MEDIUM

GIVEN a user has a completed date tied to a recommended venue and the feedback UI is available within 7 days **WHEN** the user submits a rating and structured feedback tags (e.g., 'blackout rooms', 'outdoor seating', 'blood bar') **THEN** the system updates the user's preference vector and flags venue attributes for future ranking and writes the feedback event to the training store

GIVEN there is accumulated feedback across users and the rerank pipeline is scheduled or triggered **WHEN** the ML/rerank pipeline runs (batch or near-real-time) **THEN** future recommendations for the user and similar cohorts are adjusted within 48 hours, and the system can show measurable rank change for affected venues in subsequent recommendations

Traces to: REQ-007

Emergency Transformation Protocol (ETP)

US-015 Panic/accelerometer-triggered ETP with discreet date message and safety contact alert

8 SP | MEDIUM

GIVEN ETP is enabled and device sensor thresholds plus debounce and confirmation rules are met (e.g., accelerometer + location + optional manual panic) **WHEN** an activation occurs on-device **THEN** the client triggers a server incident creation; the system sends a discreet 'personal emergency' message to the active match (non-disclosing phrasing), shares the user's last-known location with designated safety contact(s) per user's preference, creates an immutable incident record with timestamps and sensor evidence, and notifies admin queue for review

GIVEN the recipient receives the discreet message **WHEN** they open the message from their inbox **THEN** the message is obfuscated (no species-disclosing details) and presents an optional 'check on them' quick-action that sends a non-revealing follow-up notification to the ETP originator; the original incident record links the action for admins

Traces to: REQ-008

US-016 ETP local notification suppression and queued delivery

5 SP | MEDIUM

GIVEN ETP activation and a user-configured silence window (default 6 hours) set in privacy settings **WHEN** ETP starts on the device **THEN** the client enters a local suppressed-notifications mode (silence UI, haptics, and visible banners) for the configured duration while the server marks messages to be queued encrypted and not push-delivered; suppression is enforced locally even if network connectivity is lost

GIVEN the silence window elapses or the user cancels ETP early **WHEN** the client resumes normal operation **THEN** queued messages are delivered to the client un-obfuscated with timestamps indicating arrival during the silence window; the incident log records silence duration, cancellation/expiry time and delivery events for admin review

Traces to: REQ-008

Admin Console & Elder Verification Dashboard

US-017 Elder verifier dashboard with anonymized verification queue

5 SP | MEDIUM

GIVEN VerificationRequest records exist with uploaded artifacts (stored encrypted) and SLA timers **WHEN** an Elder opens the verification queue in the console **THEN** the dashboard lists pending requests with anonymized metadata, shows SLA countdowns, provides on-demand encrypted artifact download links (access-controlled), and supports claim/assign actions

GIVEN an Elder submits a verification outcome (approve/reject/request-more-evidence) **WHEN** the decision is saved via the dashboard **THEN** the system writes a tamper-evident audit trail entry, updates the user's verification status in the User & Profile Service, and notifies the user via a privacy-preserving channel configured in their profile

Traces to: REQ-009

US-018 Admin triage for clan-conflict reports and anonymized exports

3 SP | MEDIUM

GIVEN a flagged safety or clan-conflict report exists in the moderation queue **WHEN** an admin triages the report in the console **THEN** the console surfaces suggested policy-based temporary match restrictions (automated recommendations), allows admin to apply restrictions with reason and duration, and records the action with RBAC attribution in the audit log

GIVEN a compliant export request is made with a selected anonymized scope and time range **WHEN** the admin requests export from the console **THEN** the system produces an encrypted export (CSV/JSON) where PII fields are removed or hashed, includes provenance metadata (exportor, time range, hashing salt version), and logs the export event to the tamper-evident audit trail

Traces to: REQ-009

Monetization, Privacy & External Integrations

Implement NightBond Eternal premium billing, privacy-first notification/data handling controls, and resilient external integrations (lunar, maps, hazard feeds) with caching and fallbacks.

NightBond Eternal Subscription & Billing

US-019 Purchase NightBond Eternal subscription via Stripe with coupon

5 SP | MEDIUM

GIVEN a logged-in user with a valid payment method and a coupon code **WHEN** the user confirms the purchase in the app **THEN** Stripe authorizes and captures payment, a subscription record is created in Postgres, premium entitlements and priority verification flag are set on the user's account, and an audit log entry is written

GIVEN the payment flow requires 3DS/MFA or other payer confirmation **WHEN** Stripe returns success after required authentication **THEN** the system marks the subscription active, queues the user for priority verification routing, issues an in-app receipt that omits species/transform details, and records the billing success event

Traces to: REQ-010, REQ-011

US-020 Graceful downgrade on billing failure and restore on payment

3 SP | MEDIUM

GIVEN a recurring billing attempt for a subscription fails **WHEN** the payment failure and retry policy are triggered **THEN** the system notifies the user (in-app + email), starts a configurable grace period, and defers entitlement removal until the grace period expires

GIVEN the user updates payment details during the grace period and a subsequent charge succeeds **WHEN** the successful payment is verified **THEN** premium entitlements are immediately reinstated, any priority verification routing status is reapplied, and a billing audit event is recorded

Traces to: REQ-010

Privacy-first Notifications & Data Controls

US-021 Obfuscated push notifications and lock-screen safe previews

5 SP | MEDIUM

GIVEN the notification generator prepares an outbound notification and the recipient has species-privacy enabled **WHEN** a push notification is dispatched **THEN** the notification text uses generic placeholders (e.g., 'You have a new message'), any species/transformation metadata is excluded from the push/OS preview payload, and sensitive metadata is only available after app-level authentication

GIVEN the user has disabled lock-screen previews or enabled strict privacy settings **WHEN** a push arrives at the device **THEN** the platform push uses silent/obfuscated content or suppressed previews per device capabilities, an encrypted payload is delivered to the app, and the app decrypts it only after the user unlocks the app

Traces to: REQ-011

US-022 Anonymous analytics with opt-in for identified diagnostics

3 SP | MEDIUM

GIVEN the system collects telemetry by default WHEN events are emitted from services or clients THEN only anonymized aggregates (no PII, no species/transformation signals) are persisted to analytics stores and exported to third parties

GIVEN a user explicitly opts in to detailed diagnostics WHEN the consent is recorded in their privacy settings THEN the system collects expanded diagnostic data for that user only, stores the consent flag in the privacy record, and includes consent metadata with any exports

Traces to: REQ-011

External Data Integrations (Lunar, Maps, Hazard Feeds)

US-023 Lunar-phase API integration with local fallback

8 SP | MEDIUM

GIVEN the scheduling engine requests upcoming moon phases WHEN the external lunar API responds successfully THEN the system caches the API response with a TTL, uses the external values for scheduling decisions, and marks the event schedule record source as 'external'

GIVEN the lunar API is rate-limited or unavailable and the cache is missing or stale WHEN a scheduling decision requires moon phase data THEN the system computes lunar phases locally using the onboard algorithm, stores an annotated fallback entry in the cache, uses that result for scheduling, and emits a metric/alert indicating fallback usage

Traces to: REQ-012

US-024 Maps & hazard feed sync with rate-limit fallback and cached venue hazards

5 SP | MEDIUM

GIVEN the scheduled ingest job for venues and hazards runs WHEN map and hazard providers respond normally THEN venue records are enriched with geocoded locations, hazard confidence scores and last-updated timestamps, and these are indexed into Elasticsearch with a confidence flag

GIVEN a user requests venue hazard data and the map or hazard provider is rate-limited or offline WHEN the system cannot fetch live provider data THEN the system serves the most recent cached hazard overlay, displays a staleness indicator to the user, and logs the fallback with a rate-limit metric for operators

Traces to: REQ-012

Safety, Monitoring & Community Toolkit for Nocturnal/Supernatural Dating

Telemetry, fraud detection, and private, moderated cross-species community tools (guides, forums, shared calendars) that preserve secrecy and safety for supernatural users.

Analytics, Monitoring & Fraud Detection

US-025 Event telemetry for retention and match metrics

5 SP | MEDIUM

GIVEN the mobile app and backend are instrumented to emit telemetry events and the telemetry pipeline and schema are deployed **WHEN** a user action occurs (signup, match created, message sent, subscription purchase) **THEN** the event is ingested, schema-validated, stored in the analytics store and visible in the analytics dashboard within 5 minutes

GIVEN KPI definitions and derivation docs (retention, match-rate, DAU) exist in the analytics runbook **WHEN** an automated daily report or an on-demand KPI query runs **THEN** the dashboard shows aggregated KPI values matching the documented derivations and test fixtures

Traces to: REQ-013

US-026 Service-level monitoring and alerting

3 SP | MEDIUM

GIVEN instrumentation (metrics, tracing) and SLOs are configured for API Gateway, Auth, and Matching services **WHEN** a service breaches P95 latency or availability SLO for two consecutive evaluation windows **THEN** an automated alert is sent to the on-call channel containing service name, recent metric snapshots and a link to the remediation runbook

GIVEN an alert is acknowledged by on-call **WHEN** remediation completes or an incident is declared **THEN** the incident is logged with timeline, actions taken, and a post-mortem template is generated and linked to the alert

Traces to: REQ-013

US-027 Automated fraud detection and throttling for verification abuse

8 SP | MEDIUM

GIVEN fraud signals (verification rejection spikes, rapid account creation, geo-spoofing, device anomalies) are ingested into the fraud model **WHEN** the model score exceeds the configured threshold **THEN** the account is placed into a restricted state (rate-limited, limited actions), an automated high-priority ticket is created for manual elder/operator review, and the restriction is recorded in the audit log

GIVEN an account is restricted by automated fraud controls **WHEN** a manual reviewer completes review and marks clear or malicious **THEN** the system lifts restrictions and records reviewer ID and rationale or permanently suspends the account and logs the action in the tamper-evident audit trail

Traces to: REQ-013

Community & Cross-Species Toolkit

US-028 Private compatibility guide with synchronized calendar overlay

5 SP | MEDIUM

GIVEN the user is a confirmed member of a cross-species group and has privacy settings enabled **WHEN** they access the Compatibility Guide page **THEN** the guide content (etiquette, dietary constraints, scheduling rules) is visible only to group members and includes species-specific caution notes

GIVEN two users share a calendar overlay and create an event with daylight and moon-phase constraints **WHEN** the event is saved **THEN** the overlay shows mutual available windows, flags conflicts (e.g., daylight exposure for vampires, full-moon transform for werewolves), and event visibility is limited to group members and explicit event participants

Traces to: REQ-014

US-029 Moderated private forums with identity protection and audit

5 SP | MEDIUM

GIVEN a private forum thread is created with anonymity toggles available **WHEN** a member posts while anonymity is enabled **THEN** the post displays a pseudonym to members, the real identity is accessible only to authorized moderators in the moderator console, and non-members cannot view the thread

GIVEN a moderator takes action (flag, remove post, ban user) in a private forum **WHEN** the action is executed **THEN** the action is recorded in a tamper-evident audit trail with moderator ID, timestamp and reason, and the affected content is hidden from non-moderators while remaining available to auditors

Traces to: REQ-014, REQ-013

US-030 Visibility controls for private community participation

5 SP | MEDIUM

GIVEN visibility toggles exist on group membership and per-thread settings **WHEN** a user enables hidden membership and posts in a private forum **THEN** their activity is visible to group members and moderators only, is omitted from public profile displays, and the membership flag is not exposed to external APIs

GIVEN a user toggles visibility off to reveal membership to a partner **WHEN** the user confirms and saves the change **THEN** the system timestamps the visibility change, informs the affected partner(s) if required, and records consent in the audit log

Traces to: REQ-014

5 Quality Report

100

Quality Score: 100/100

Validation Passed

INVEST Compliance Summary

METRIC	VALUE
Stories Validated	30
Stories Passing	30
Stories Failing	0
Average INVEST Score	4.8/5.0
Lowest INVEST Score	4.7/5.0
Highest INVEST Score	5.0/5.0
Requirement Coverage	100%

Requirement Coverage

100%

Validation Issues

> WARNING — **traceability**
> Missing explicit requirement_ids field on story for traceability.

Recommendations

- Tighten traceability by mapping each story to explicit REQ-xxx IDs in addition to reqs field.
- Consider splitting any 8-point stories if velocity is constrained; none currently flagged.

INVEST Scores by Story

STORY	I	N	V	E	S	T	AVG	PASS
US-001	5	5	5	5	5	5	0.0	No
US-002	5	4	5	5	5	5	0.0	No
US-003	5	4	5	5	5	5	0.0	No
US-004	5	4	5	5	5	5	0.0	No
US-005	5	5	5	5	5	5	0.0	No
US-006	5	4	5	5	5	5	0.0	No
US-007	5	4	5	5	5	5	0.0	No
US-008	5	4	5	5	5	5	0.0	No
US-009	5	5	5	5	5	5	0.0	No
US-010	5	4	5	5	5	5	0.0	No
US-011	5	4	5	5	5	5	0.0	No
US-012	5	4	5	5	5	5	0.0	No
US-013	5	3	5	5	5	5	0.0	No
US-014	5	5	4	5	5	5	0.0	No
US-015	5	4	5	5	5	5	0.0	No
US-016	5	4	5	5	5	5	0.0	No
US-017	5	4	5	5	5	5	0.0	No
US-018	5	4	5	5	5	5	0.0	No
US-019	5	4	5	5	5	5	0.0	No
US-020	5	4	5	5	5	5	0.0	No
US-021	5	4	5	5	5	5	0.0	No
US-022	5	4	5	5	5	5	0.0	No
US-023	5	4	5	5	5	5	0.0	No
US-024	5	4	5	5	5	5	0.0	No
US-025	5	4	5	5	5	5	0.0	No

STORY	I	N	V	E	S	T	AVG	PASS
US-026	**5**	**4**	**5**	**5**	**5**	**5**	**0.0**	No
US-027	**5**	**4**	**5**	**5**	**5**	**5**	**0.0**	No
US-028	**5**	**4**	**5**	**5**	**5**	**5**	**0.0**	No
US-029	**5**	**4**	**5**	**5**	**5**	**5**	**0.0**	No
US-030	**5**	**4**	**5**	**5**	**5**	**5**	**0.0**	No

6 Appendix

Out of Scope

- Public profiles or social media sharing (explicitly disallowed by product principles)
- Standard mirror-based photo verification (not usable for vampires)
- Sharing species or supernatural details in push notification previews or with third parties
- Automated, fully-self species verification without Elder involvement
- Integration with mainstream social sign-on providers that leak user attributes to third parties

Edge Cases

- Daywalker vampires with partial sunlight tolerance require custom scheduling and venue rules.
- Users with multiple supernatural identities or fluid species affiliation (handles multiple profiles or profile flags).
- Werewolf transformations triggered unexpectedly during a date (ETP + offline behavior must be reliable without network).
- Timezone and hemispheric seasonal sunset/sunrise differences (reverse seasons in southern hemisphere).
- Geopolitical or treaty-constrained regions where inter-species interactions are restricted — system must enforce blocking unless explicit mutual override.
- Outage or rate limit on lunar API — local lunar calculations or cached lunar calendar must provide fallback.
- Users attempting to game matching engine by spoofing territory or schedule data (fraud detection needed).
- User device sensors false-positive for ETP (accelerometer noise) — require multi-signal detection and confirmation thresholds.
- Users who opt out of location services but still require safe-harbor suggestions — need manual venue selectors.
- High volume of verification requests causing Elder Council backlog — queueing, SLA escalation, and paid priority required.

Requirement Coverage Matrix

REQUIREMENT	COVERING STORIES
REQ-001	US-001, US-002
REQ-002	US-003, US-004
REQ-003	US-005, US-006
REQ-004	US-007, US-008
REQ-005	US-009, US-010
REQ-006	US-011, US-012

REQUIREMENT	COVERING STORIES
REQ-007	US-013, US-014
REQ-008	US-015, US-016
REQ-009	US-017, US-018
REQ-010	US-019, US-020
REQ-011	US-019, US-021, US-022
REQ-012	US-023, US-024
REQ-013	US-025, US-026, US-027, US-029
REQ-014	US-028, US-029, US-030

Generated by DevHawk on February 06, 2026
Specification v1 • 30 stories • 159 story points