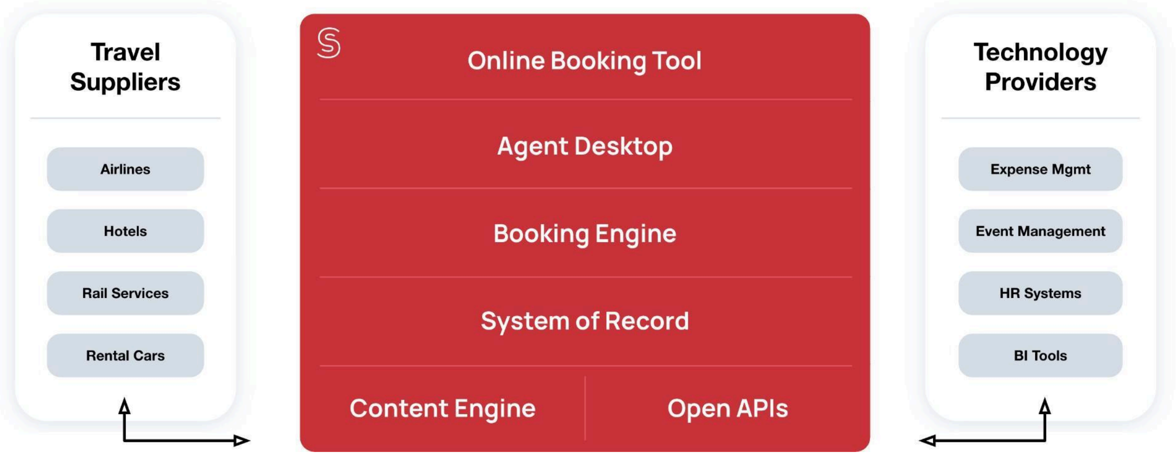
SPOTNANA

Security Whitepaper

Table of contents

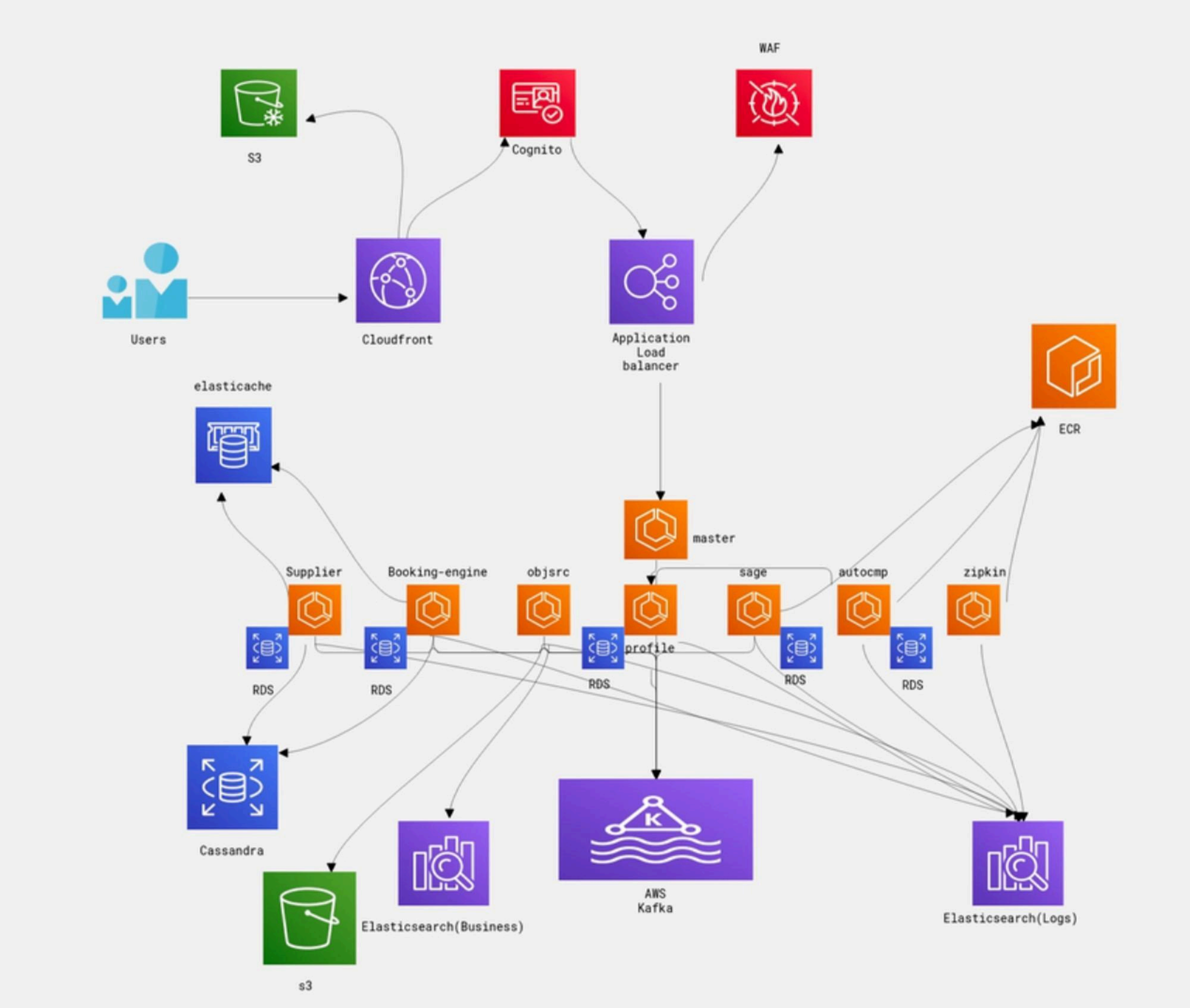
Spotnana overview

Spotnana provides a single cloud-based Travel-as-a-Service (**TAAS**) Platform to corporations, travel management companies, suppliers, and technology providers, enabling the travel industry to lower operating costs, accelerate innovation, and deliver unparalleled travel experiences.



Spotnana's back-end system is hosted in Amazon Web Services (AWS) and made available through APIs for our channel partners, travel suppliers, and Spotnana's own online booking tool (OBT) in a mobile and web application form factor for our corporate customers.

Secure design



Shown above is a simplified diagram of a request as it flows through Spotnana's back-end infrastructure starting from the end-user and through our back-end microservices (shown in orange).

Tenant isolation

Each customer can be viewed as a "tenant" in Spotnana's TAAS platform, where data and information related to a tenant is logically segmented from other tenants through access control mechanisms enforced at the data access layer. From a storage of information perspective, a single database may contain more than one tenant's data and information. From a compute and infrastructure perspective, all tenants share one common infrastructure in a single AWS account.

Role-based access control and authorization model

A typical customer (referred as “org” below) using Spotnana’s TAAS platform for corporate travel has following roles available to them along with a corresponding set of permissions that are managed by an authorization service.

Company admin: Manages an org's travel policies, manages org information (legal entity, offices), manages org level users and their roles.

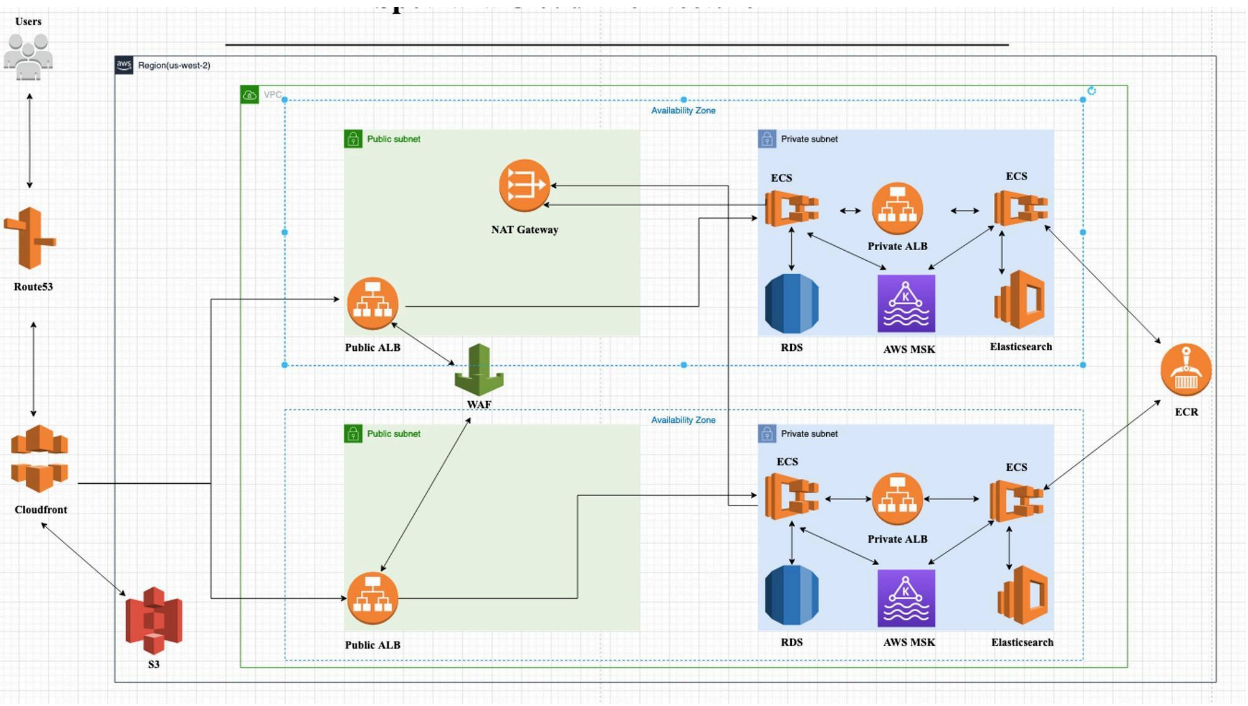
Company travel arranger: Makes booking for all employees of the org.

Travel arranger: Manages bookings for executive staff.

Company reporting admin: Manages org-specific analytics via dashboards and reports.

Traveler: Primary persona that logs into the application for the purpose of searching for and booking corporate travel.

Secure architecture



Denial of service and web application attack prevention

All requests from users are resolved via Amazon Route53 DNS service before hitting Amazon CloudFront content delivery service that provides access to our static web application content stored in an S3 bucket. For requests that need back-end service access, Amazon CloudFront, AWS shield, AWS WAF, and Public Application load balancers provide a comprehensive protection against distributed Denial of Service and common web application attacks.

Availability zones and component level segregation

Spotnana maintains two availability zones within a single AWS US-West2 region for high availability.

Individual back-end services and applications (for example Search, Supplier in diagram above) are segregated as separate Amazon ECS Services running in a single cluster. Each cluster is bound to an individual VPC and each VPC is governed by a unique IAM role that is hardened using industry-best practices.

Environment segregation

Outside of a customer-serving production environment, Spotnana maintains three other environments: pre-prod, QA, and staging in their respective VPCs. Peering between environments is strictly controlled and customer data is never shared between production and lower environments.

Data in transit protection

All requests to Spotnana's TAAS back-end services are encrypted using Transport Layer Security (TLS 1.2), using Amazon Certificate Manager (ACM). This includes requests coming from web and mobile clients as well as any direct API clients.

Data at rest protection

All customer data in all data stores (Kafka, Cassandra, RDS, S3, Elastic Search) in the production environment is always encrypted at rest. Keys for encryption are managed by AWS and are tenant-agnostic.

Secure development, deployment, and operations

Secure SDLC

Spotnana's security team conducts regular reviews of application design, architecture, and features related to security of the platform, along with running static code analysis tools to identify security bugs. Vulnerabilities in containers are managed via a continuous monitoring system under a well established SLA for remediation. Third-party driven penetration testing is conducted at least annually.

Secure deployment

Spotnana uses three different pipelines to push code into production, namely release, bugfix, and hotfix. All changes are tracked at PR level into release pipelines. IAM roles and permissions are implemented to achieve segregation of duties on who can push code to production.

Secure internal access

Spotnana manages internal access to the production environment at network and identity levels. A Spotnana-managed VPN server provides network access to end points in production infrastructure for troubleshooting purposes. Similarly, local accounts and IAM roles are defined for logical access into resources. Except for AWS native root accounts, IAM access to AWS management portal is gated behind a single sign-on connection through the Spotnana identity provider. All access and corresponding permissions follow the principle of least privilege and need to know basis, access is monitored and JIT approved where applicable.

Security logging, monitoring, and incident response

Spotnana employs AWS-native and third-party monitoring tools within the AWS environment to identify and alert staff on reliability and security issues. Specific escalation protocols have been established to inform on-call staff members on issues that need immediate resolution, such as those that may impact availability and customer data confidentiality.

External certifications and internal compliance

In line with the requirements of ISO 27001:2022, Spotnana has implemented an ISMS system and obtained ISO 27001:2022 certification. Spotnana also complies with trust services security criteria under AICPA and has obtained an independent auditor report for SOC2 Type 2 compliance.

Spotnana processes credit/debit payment transactions as a merchant and collects credit/debit payment information on behalf of airlines and related travel suppliers. For all payment related functionality, Spotnana uses a qualified PCI-compliant Third-Party Service Provider (TPSP) for all storage, processing, and transmission of PCI cardholder data in the Spotnana TaaS Platform. PCI cardholder data is never stored, processed, or transmitted within the Spotnana TaaS Platform infrastructure or systems. In accordance with PCI and travel industry requirements, Spotnana validates its own PCI compliance on an annual basis. This process includes verifying the PCI compliance validation status of its TPSPs and submission of an Attestation of Compliance (AOC) to its payment service providers and industry stakeholders (including IATA).

An internal continuous compliance monitoring program has been implemented to maintain an effective control environment. Spotnana undergoes frequent third-party audits to maintain its compliance against ISO27001 and SOC2 security controls.