The proposed architecture provides a secure, scalable, and standards-aligned foundation for ShopNimbus’s e-commerce and file-sharing platforms as they migrate to Google Cloud Platform (GCP). The design follows a classic three-tier model—Web, Application, and Database—with deliberate service choices and controls that uphold the principles of Confidentiality, Integrity, and Availability (CIA) while supporting PCI DSS and GDPR compliance requirements.

1. Web Tier – Secure External Entry Point

Incoming traffic is terminated at a Google HTTPS Load Balancer with Cloud Armor providing web-application-firewall and DDoS protection. Only encrypted HTTPS connections are permitted, enforced by firewall rules and TLS certificates managed by GCP. This tier scales horizontally through Compute Engine managed instance groups to maintain performance under variable load.

Security alignment: End-to-end TLS and WAF policies protect Confidentiality; global load balancing and autoscaling strengthen Availability.

2. Application Tier – Isolated Business Logic

Core application logic executes in Cloud Functions within a Private Application Subnet. A NAT gateway controls outbound traffic while a VPC connector enables private communication with the database tier. This serverless approach reduces operational overhead and minimizes the attack surface by ensuring that Google maintains the underlying runtime and patch management.

Security alignment: Private networking preserves Confidentiality; automated scaling and managed runtime enhance Availability and Integrity.

3. Database Tier – Protected Data Store

All persistent data resides in Cloud SQL configured with Private IP only. Encrypted API calls from the application tier ensure secure data transit. Automatic backups, point-in-time recovery, and storage-level encryption are enabled to safeguard data integrity and support rapid recovery from incidents.

Security alignment: Private IP addressing and in-transit/at-rest encryption enforce Confidentiality; managed backups and transaction logging uphold Integrity; regional high-availability options maintain Availability.

4. Cross-Cutting Security Controls

Identity and Access Management (IAM): Role-based access with least-privilege service accounts for each tier limits potential compromise impact.

Monitoring and Incident Response: Security Command Center, Cloud Logging, and Cloud Monitoring provide continuous visibility and automated alerting, ensuring rapid detection and response to anomalies.

Compliance Enablement: Encryption, audit logging, and access controls collectively address key PCI DSS and GDPR requirements.

Summary This architecture delivers a professionally engineered, production-ready cloud environment that balances security, performance, and operational efficiency. By segmenting tiers, enforcing least-privilege access, and embedding encryption and monitoring at every layer, it positions ShopNimbus to meet regulatory obligations and scale confidently as business demand grows.