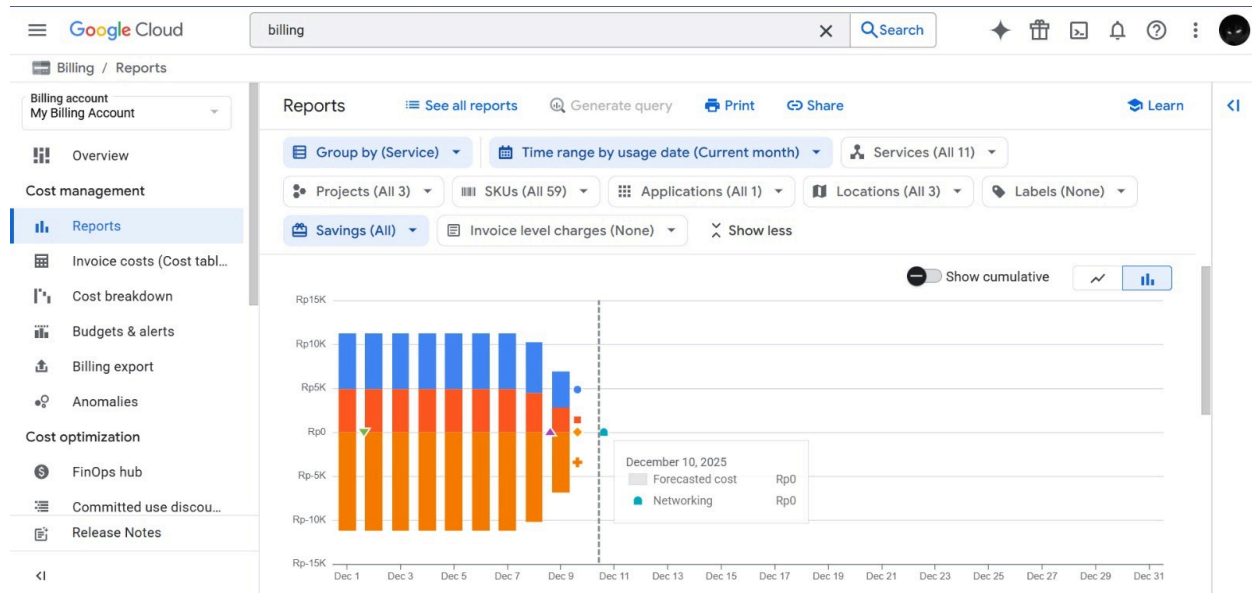


## Analisis Biaya & Efisiensi Cloud (Cost Analysis)

Gambar: Grafik Billing (Cost Analysis)



1. Analisis Grafik Penggunaan (Usage vs Credits) Berdasarkan grafik *Billing Reports* per tanggal 10 Desember 2025, terlihat struktur biaya sebagai berikut:

- **Total Usage Cost (Bar Biru & Merah):** Infrastruktur memunculkan biaya kotor (gross cost) sekitar **Rp 10.000 - Rp 12.000 per hari**. Biaya ini berasal dari operasional *Cloud SQL* (Database) dan *Compute* (Cloud Run).
- **Discounts/Credits (Bar Oranye):** Grafik menunjukkan nilai negatif (ke bawah) yang menyeimbangkan biaya penggunaan secara simetris. Ini merepresentasikan **Promotional Credits** atau **Free Tier** dari Google Cloud Platform yang secara otomatis memotong tagihan.
- **Net Cost (Titik Garis Rp 0):** Hasil akhirnya (Net Cost) berada di garis **Rp 0**. Artinya, tidak ada biaya tunai yang harus dibayarkan.

2. Alasan Efisiensi Biaya (Why Low Cost?) Rendahnya biaya operasional ini dicapai berkat penerapan arsitektur **Serverless** menggunakan **Google Cloud Run**:

- **Mekanisme Scale-to-Zero:** Berbeda dengan *Virtual Machine* (VM) tradisional yang menyedot biaya 24 jam non-stop meskipun tidak ada pengguna, Cloud Run memiliki fitur *Scale-to-Zero*.
- **Pay-as-you-go:** Server Frontend dan Backend kami otomatis "mati" (idle) saat tidak ada traffic/request masuk. Google hanya menagih biaya hitungan detik saat server memproses permintaan user.
- **Optimasi Resource:** Karena aplikasi ini masih dalam tahap MVP (Iterasi 1 & 2), penggunaan CPU dan Memory masih sangat rendah sehingga sepenuhnya tertutup oleh kuota *Free Tier* bulanan.




Laporan Security Audit

Status Keamanan: Baseline Security (MVP Level)


Tanggal Audit: [10 Desember 2025]

Berikut adalah hasil analisis keamanan pada infrastruktur Three-Tier Google Cloud Platform yang telah dibangun:

1. Network & Infrastructure Security (Keamanan Jaringan)

Kontrol Keamanan	Status	Keterangan Teknis
HTTPS/TLS Encryption	<div> Aman</div>	Seluruh trafik dari User ke Frontend dan Backend dienkripsi secara otomatis menggunakan sertifikat SSL/TLS yang dikelola oleh Google Cloud Run. Data tidak dapat disadap di tengah jalan ( <i>Man-in-the-Middle Protection</i> ).
Database Isolation	<div> Aman</div>	Database Cloud SQL dikonfigurasi menggunakan <i>Private IP</i> dalam jaringan VPC internal. Database tidak memiliki IP Publik, sehingga tidak bisa diakses langsung dari internet terbuka ( <i>Anti-Brute Force</i> ).
DDoS Protection	<div> Aman</div>	Menggunakan infrastruktur Google Front End (GFE) yang secara bawaan memiliki mitigasi terhadap serangan DDoS dasar sebelum trafik mencapai server aplikasi.

2. Application & Data Security (Keamanan Aplikasi)

Kontrol Keamanan	Status	Keterangan Teknis
Container Security	<div> Aman</div>	Aplikasi berjalan di atas container (Docker) yang terisolasi. Jika satu service crash atau diserang, tidak akan langsung mempengaruhi service lain atau host system.

<b>Input Validation</b>	⚠️ <b>Parsial</b>	Frontend menggunakan validasi dasar (HTML5 <b>required</b> attributes) untuk mencegah input kosong. Namun, validasi sisi server (Backend sanitization) masih perlu ditingkatkan untuk mencegah <i>XSS/SQL Injection</i> tingkat lanjut.
<b>Secret Management</b>	✅ <b>Aman</b>	Kredensial database tidak di-hardcode di dalam kodingan aplikasi, melainkan dikelola melalui <i>Environment Variables</i> di Cloud Run dan Terraform State yang dijaga kerahasiaannya.

### 3. Access Control (Manajemen Akses)

Kontrol Keamanan	Status	Keterangan Teknis
<b>Developer Access</b>	✅ <b>Aman</b>	Akses ke Google Cloud Console dibatasi menggunakan <i>IAM (Identity and Access Management)</i> . Hanya anggota kelompok yang terdaftar yang memiliki hak <i>Owner/Editor</i> untuk mengubah infrastruktur.
<b>User Authentication</b>	❌ <b>Future Work</b>	<b>(Risiko Diterima)</b> Saat ini aplikasi diset <b>--allow-unauthenticated</b> (Publik) untuk kebutuhan demo MVP. Siapapun yang memiliki link dapat mengakses fitur. Implementasi <i>Google Identity Aware Proxy (IAP)</i> atau <i>OAuth2</i> dijadwalkan untuk Iterasi 3.