Burak Faruk Şahin

Senior DevSecOps & Platform Engineer · Founder, BRF Tech

Istanbul, Turkey · burak@brf.sh · brf.sh · linkedin.com/in/buhack · github.com/brkfun · burak.sh

SUMMARY

Senior platform engineer with **12+ years** designing, deploying, and operating production systems on Docker, Kubernetes, Knative, and serverless stacks. Founder of BRF Tech, a DevOps consultancy that has shipped infrastructure for 15–35 startups and growth-stage companies across iGaming, fintech, retail (Koton), mobility, logistics, and hosting. Deep DevSecOps experience covering WAF, secret management, container scanning, Kubernetes RBAC and Network Policies, mTLS, OIDC/SAML, and audit logging. Proven track record cutting cloud costs by up to 50%, designing multi-tenant platforms (Kubernetes clusters and single-server SaaS alike), and building serverless data pipelines that process 50M+ records per night. Author of **filex**, an open-source (MIT) self-hosted file manager in production across multiple platforms including a 10-tenant hosting deployment, and building **runr.sh**, an open-source serverless platform on Knative that unifies CaaS, FaaS, and AI workloads (agents, multi-agent pipelines, model serving).

Languages: Turkish (native), English (C1). **Open to:** EU/US remote, hybrid, or relocation. Senior / Staff / Lead / Principal IC and CTO roles.

EXPERIENCE

Founder & Principal Engineer · BRF Tech (brf.sh) | Mar 2023 – Present

Solo DevOps & platform consultancy · Remote, Istanbul

- Delivered packaged DevOps engagements to **15–35 startup and scale-up clients** — full-cycle work spanning Kubernetes & Docker, CI/CD, Terraform IaC, monitoring & alerting, GitOps (ArgoCD/Flux), security hardening, FinOps, and cloud migrations across AWS, GCP, Azure, and Hetzner. Often acting as a full DevOps team replacement during early-stage growth.
- Operate a self-hosted production stack on Kubernetes 1.24 with **Knative, Traefik, Longhorn, Sentry, and Kata Containers**, running internal and client services with multi-tenant isolation and Confidential Computing (AMD SEV-SNP / Intel TDX) support.
- Operate a second production estate on **Docker + Caddy (40+ vhosts, single front door with automated DNS-01 wildcard TLS)**: Keycloak SSO across ~20 self-hosted services (mail, files, git, monitoring, media, project management), a Laravel 13 / Filament v5 operations monolith (15+ modules: uptime + status page, notifications, identity rotation, VPN jumphost orchestration, media pipelines), Prometheus/Grafana observability across three sites, GlitchTip error tracking, and automated off-site DR with hourly restic backups and a warm-standby second site.
- Built and run a **local LLM gateway** for client engineering teams: cloud-hosted Ollama + vLLM with OpenRouter-style multi-model routing, allowing developers to use Cursor/IDE agents with cost-controlled, regional models instead of public APIs. Includes RAG pipelines, MCP/ACP agent integrations, and AgentFlow-style multi-agent orchestration.
- Run an **agent-driven engineering workflow**: self-hosted Coder workspaces where Claude Code agents work against MCP servers (file management, project tracking, docs) with confined per-workspace credentials — used daily to ship the company's own products and client work.
- Productized the consultancy as a **25-area service catalog with tiered USD pricing** — covering CI/CD, Kubernetes, IaC, monitoring, security & zero-trust, cloud migration, microservices/service mesh, FinOps, SRE & incident management, GitOps, data engineering, training, network & DDoS, backup/DR, observability, QA automation, and platform engineering / developer portals.

DevSecOps & Solutions Engineer · DTCloud (via BRF Tech) | Aug 2025 – Present

Multi-tenant hosting platform for business customers · Remote, Istanbul

- Designed, built, and operate a **multi-tenant hosting platform** that gives each tenant company mail, file management, and SSO on its own domain — **10 tenant companies (~70 users)** served from a single server: self-hosted Stalwart mail (shared MX), filex file management, and per-tenant Keycloak realms with passkey support and a Turkish-localized login experience.
- Automated **new-tenant provisioning to a single command**: Cloudflare DNS + proxied records, DNS-01 wildcard TLS, Keycloak realm + user seeding from onboarding sheets, mail domain (DKIM/SPF/DMARC), file storage, customer portal, and identity-gated access — idempotent and re-runnable per step.
- Executed a **zero-data-loss migration of 101k+ emails across ~40 mailboxes from Yandex 360** to the platform: parallel, systemd-managed IMAP sync engine with an on-demand migration status dashboard (per-account progress, ETA, failure triage), followed by MX/SPF/DKIM/DMARC cutover across 9 domains with verification records preserved.
- Hardened deliverability from **3/10 to 10/10 (mail-tester)**: fixed double-SPF records left by legacy DNS, enabled platform-wide DKIM signing that automatically covers current and future tenants, and validated SPF+DKIM+DMARC end to end.
- Consolidated per-tenant file services onto **one natively multi-tenant filex instance** (host→tenant realm OIDC dispatch, per-tenant storage isolation, cross-realm user invisibility verified live) — root-caused a subtle production bug to Cloudflare stripping Set-Cookie on 3xx redirects and shipped the fix upstream.
- Built the customer-facing portal as a Filament panel: launchpad, profile self-service with passkey enrollment/removal, and per-user WebPush notifications wired to real-time mail-ingest webhooks (only the actual recipient is notified).

Creator & Sole Engineer · filex — open-source self-hosted file manager (MIT) | 2025 – Present

github.com/BRF-Tech/filex · Go + Vue 3 · single binary / container (ghcr) · in production across multiple platforms

- Architecture: **Go backend** (chi router, goose migrations, driver registries) with **pluggable storage (local, S3, SFTP, WebDAV, FTP), auth (local, OIDC, LDAP, proxy-header), and DB (SQLite/Postgres/MySQL)**; Vue 3 monorepo shipping a native SPA, an embeddable **<filex-explorer> web component**, and a shared core package.
- **Native multi-tenancy**: provider-per-tenant model with host→realm OIDC dispatch, per-tenant storage confinement, and cross-tenant user isolation — powers a 10-tenant production hosting deployment on a single instance.
- Security & governance: **RBAC with per-item ACLs** (owner/editor/viewer grants with inheritance, permission panel, email invites), audit log with **per-token identity attribution** (one shared API key can act as multiple named consumers, unknown identities rejected), confined API tokens with root scoping for embedded integrations.
- **Real-time collaboration**: WebSocket presence (who is in the folder, which file they focus) and live folder updates, with single-use ticket auth so the embedded web component connects cross-origin without exposing durable tokens; API-polling fallback.
- Product surface: public share links with PIN + expiry (folder shares stream as ZIP with a content-signature cache and background warmer), "file drop" public upload links, OnlyOffice document preview, universal file converter integration, ShareX upload endpoint, deep-linkable explorer URLs, i18n (EN/TR).
- **MCP server built in**: file tools plus a full admin surface (~59 tools) so AI agents can operate and administer the instance under confined, per-workspace tokens — used daily by an agent fleet in my own infrastructure.
- Embedded in three production host apps (project platform, admin panel, mobile PWA) via server-side confined proxy tokens (X-Filex-Root) — the host injects credentials server-side, the browser never sees them.
- Release engineering: dual-repo flow (GitLab primary, GitHub public export), tagged releases with GitHub Actions building multi-arch container images to ghcr — **30+ releases** shipped with a local end-to-end pre-release test harness (sqlite backend + instrumented dummy embed host + Playwright).

Creator & Sole Engineer · runr.sh (Pre-release) | 2024 – Present

Open-source serverless & AI platform on Knative · Personal project

- Designing and building an **open-core serverless platform** on Kubernetes/Knative that unifies CaaS (containers), FaaS (multi-file projects), and XaaS (single-file functions) under one developer experience.

- Native AI module with three primitives: **AaaS** (single AI agent), **AgentFlow** (multi-agent DAG pipelines), and **MaaS** (GPU-pooled model serving with OpenAI-compatible inference). Blueprint-as-Code declarative configuration via YAML.
- Multi-tenant by design with schema-per-tenant isolation, RBAC, SSO (OIDC), resource quotas, and Kata Containers / gVisor / Firecracker runtime sandboxing — targeting fintech, government, and air-gapped deployments where data residency and confidential computing matter.
- Path-based API gateway with route-level StripPrefix, multi-region deploy from a single dashboard, scale-to-zero, and event triggers (HTTP, cron, Redis Stream, broadcast) — designed as a self-hostable alternative to AWS Lambda + ECS, GCP Cloud Run, and Vercel.

Senior DevSecOps Engineer · Veribox | Aug 2024 – May 2025

DevOps consultancy · Concurrent engagement via BRF Tech

- Provided senior DevSecOps capacity to Veribox client engagements: hardening Kubernetes deployments, secret management with HashiCorp Vault and External Secrets, container image scanning (Trivy), and CI/CD pipeline security gates.

Senior DevSecOps Engineer · Monotech (iGaming Platform Vendor) | Apr 2023 – Apr 2025

Remote, Zagreb, Croatia · GCP / GKE · ~30 developers, 3 product teams

- Re-platformed a monolithic iGaming application from GCP Serverless to GKE Kubernetes, cutting infrastructure cost by up to **50%** while serving a flagship customer with **100k–500k unique users** plus 3–5 additional tenants. Designed per-customer GKE clusters that **autoscale 20–30 nodes** with pod-level HPA across all in-cluster applications.
- Migrated a customer's stack from India to EU regions to reduce latency for end users and operations; fronted with **Cloudflare CDN, WAF custom rules, rate limiting, and bot management** for production hardening.
- Built a **multi-branch ephemeral environment system**: every dev-xyz branch automatically provisions a xyz.dev.app.tld environment wired to a dev or production database — used both for feature branches and for safely reproducing production bugs against live data.
- Built **DopsDashboard**, an internal Filament-based developer portal that lets engineers manage their own Cloudflare WAF rules, environment configs, and deployment settings without filing ops tickets.
- Implemented **secret management** pipeline using Passbolt + External Secrets Operator (replacing HashiCorp Vault), dispatching credentials and environment values across all clusters from a single source of truth. Enforced **Kubernetes RBAC, Network Policies, Pod Security Standards**, mTLS between services, and TLS via cert-manager + Let's Encrypt automation.
- Delivered an internal **LLM coding assistant** — GPU-backed Ollama service routed to engineering, providing developers with private model access for code generation. Foundation for the multi-model routing approach now used at BRF Tech.
- Standardized DevOps practices across 3 product teams via shared sprints, **Helm charts, Terraform/Ansible IaC, Kaniko-based image builds, GitLab CI, ArgoCD GitOps**, and Sentry/Elastic observability.

Senior DevOps Engineer · Parkos | Aug 2022 – Apr 2023

Remote, Amsterdam, Netherlands · Airport parking marketplace, 7M+ customers, 270+ airports across 14 countries (acquired by CAVU / MAG, 2024)

- Joined the DevOps team during a **scale-up phase**, working on a Laravel-based microservice platform deployed across **AWS and GCP** with parallel, portable Kubernetes manifests for cross-cloud failover and elasticity.
- Used **ArgoCD and Terraform** to scale up the platform's Kubernetes footprint and standardize GitOps deployments across environments.
- Owned production stability for the Laravel application: triaged Sentry-reported errors, diagnosed root causes across the microservice graph, and shipped fixes that measurably reduced the production error rate.
- Engagement ended due to a Dutch DevOps role residency requirement (EU citizenship), not performance.

Senior Software Engineer · Aloware | Feb 2022 – Aug 2022

Remote, Los Angeles, USA · AI-powered contact center SaaS (HubSpot/Pipedrive/Zoho integrations)

- Designed and shipped a **fair-queue messaging system** so that one tenant blasting 3M SMS no longer starved other tenants — per-tenant queue isolation with global fairness across millions of jobs.
- Migrated the Laravel application to **AWS Lambda via Laravel Vapor**, restructuring jobs and adding tests to make the migration safe.
- Cut **Redis and memcache RAM usage** by moving high-volume ephemeral traffic to **MQTT**, removing inappropriate cache usage patterns.
- Upgraded the Laravel codebase from **Laravel 5 to the then-current major version** — a multi-step major upgrade across deprecated APIs and broken dependencies.
- Built **CI/CD from scratch**, optimized pipeline runtime, and introduced a **headless development environment** (the precursor to the per-branch environment system later deployed at Monotech).
- Wrote performance-critical jobs in Go and Node where Laravel/PHP was a bottleneck.

DevSecOps Consultant · Kamion (via BRF Tech) | Nov 2020 – Feb 2022

Istanbul, Turkey · Turkish freight/trucking marketplace startup

- Acted as fractional DevOps for a startup that wasn't ready for a full-time hire: deployed Kubernetes from scratch on AWS with Rancher, then re-deployed onto better-spec services as the company scaled.
- Stack: Laravel + Node + Next.js, AWS + GCP, Kubernetes, Docker Swarm, Redis, Postgres.

DevSecOps Engineer & Acting CTO · C-Level | May 2019 – Feb 2022

Istanbul, Turkey · Product company building B2B SaaS, retail, and mobility platforms · Team grew 6 → 25

- Joined as Fullstack Engineer; transitioned to DevOps as the team grew from 6 to 25, then served as **Acting CTO for the final ~8 months** through the previous CTO's departure — owned engineering leadership, technical direction, and the handover of HRVenue and Carbon Mobility to client teams.
- **Notable production work:**
  - **Koton QCommerce** (rapid grocery/retail delivery, à la Getir): owned end-to-end deploy, maintenance, and ongoing development of a Kubernetes platform on Hetzner with Rancher; powered same-store-pickup courier delivery for Turkey's largest fashion retailer.
  - **Uysal Market QCommerce**: built a similar quick-commerce app with same-hour delivery slots (analogous to Migros Hemen), full software lifecycle ownership.
  - **Europcar Medos**: deployed and re-deployed Kubernetes infrastructure on AWS with Rancher for European car rental operations.
  - **Companity & AppShadow**: designed and built two products from zero — a Facebook Workplace-style internal social platform with gamification (TÜBİTAK-approved), and a mobile app shadowing tool for iOS and Android.
  - **ConnectFilom (for Tofaş)**, **HRVenue (for kariyer.net)**, Topla.app, Rofebo (Istanbullines), and Carbon Mobility — across Docker Swarm and Kubernetes on Hetzner, AWS, GCP, and Azure.

DevOps & Software Engineer · 360DRC | Sep 2020 – Dec 2020

- Joined to lead a cloud migration; pivoted to product engineering when the cloud move was deprioritized — wrote Salesforce plugins, fixed Laravel and Node applications, and worked with Laravel's serverless tooling.

Fullstack Developer · Juvenis | Sep 2018 – May 2019

Istanbul, Turkey · Digital agency

- Brought the agency to modern engineering practice: moved all projects to Git, introduced GitLab/GitHub Actions CI/CD, and added Docker-based deployments — none of which existed before.
- Built **GAPFS** (Generic Admin Panel For Socials), a Laravel + Vue app aggregating data from social platforms for the agency's social media team.
- Built a **Zalenium-powered Instagram automation** that scraped comments on a live video, picked random commenters, generated a video, and republished it — production system using multi-container Selenium.
- Delivered the iData Visametric reservation system for Istanbul consulate appointments.

R&D Developer · Erstream | Jan 2018 – Aug 2018

Istanbul, Turkey · Network operations and telco services

- Hired as a network admin, transitioned to Linux administration, then to R&D engineering when the team needed PHP capacity.
- Shipped **4 R&D projects in 8 months**, spanning network management, monitoring tooling, and outsourced web work — including ownership of full architecture, code, and deployment for each.
- Flagship project: **CCNMS (Closed-Circuit Network Management System)** — an inter-rack mobile-internet network that aggregated metrics from hundreds of servers per pool and shipped data hourly to a central database. **Productized end-to-end and sold to Turkcell, Türk Telekom, and a third operator** as a standalone deployable system. Used Laravel, application-swarming for inter-app communication, MongoDB + Postgres clusters, Redis, memcache, and Python (for self-upgrade and self-installation).
- Also handled outsourced web work for TRT News.

NOTABLE ENGINEERING PROJECT

PaketTaksi OYM — Nightly Fuel Reconciliation at 50M Records

Built at C-Level for PaketTaksi (Istanbul-based last-mile logistics) · AWS Lambda + Laravel Vapor

- Designed, built, deployed, and maintained a serverless reconciliation system that runs as a **scheduled job at 23:55 nightly**, pulls **~50 million fuel-purchase records** from Petrol Ofisi, and reconciles them per-courier (by license plate) into per-courier earnings reports.
- End-to-end runtime: **1–3 minutes** against a 5-minute SLA. Replaced a manual Excel + macro process that took roughly an hour every morning.
- Sole owner: architecture, code, deploy, and ongoing operations. Full CI/CD on Laravel Vapor; ran for years in production.

TECHNICAL SKILLS

Containers & Orchestration: Docker, Docker Compose, Docker Swarm, Kubernetes (1.24+, GKE, EKS, on-prem, K3s), Helm, Kustomize, Rancher, Knative, Istio, Linkerd, Traefik, Caddy, Nginx, Kong, Kata Containers, gVisor, Firecracker, Cloud Hypervisor, QEMU

Cloud & Infrastructure as Code: AWS (Lambda, ECS, EKS, S3, CloudFront, RDS), GCP (GKE, Cloud Run, Cloud Functions), Azure, Hetzner, DigitalOcean, OVH; Terraform, Ansible, Pulumi

CI/CD & GitOps: GitLab CI, GitHub Actions, Jenkins, ArgoCD, FluxCD, Tekton, Kaniko, Laravel Vapor, Helm, Kustomize; canary, blue/green, feature flags (Flagsmith / LaunchDarkly)

Observability & SRE: Prometheus, Grafana, Loki, Tempo, Jaeger, OpenTelemetry, Datadog, Sentry, GlitchTip, Zabbix, Elastic / ELK; SLO/SLI definition, error budgets, on-call rotation, incident response, postmortems, MTTR, runbooks; PagerDuty, Opsgenie

Security (DevSecOps): Cloudflare WAF custom rules, rate limiting, bot management, DDoS mitigation; OWASP Top 10 mitigations (SQLi, XSS, CSRF) at code level; container image scanning (Trivy, Grype); SAST/DAST integration; secret management (HashiCorp Vault, External Secrets, Passbolt, gitleaks pre-commit hooks); Kubernetes RBAC, Network Policies, Pod Security Standards; mTLS, cert-manager, Let's Encrypt automation; OIDC / SAML / OAuth2 (Keycloak, Authelia, Auth0); audit logging, SIEM (Elastic, Loki); zero-trust networking (Cloudflare Zero Trust / WARP), VPN (WireGuard, Pritunl); compliance prep for KVKK, GDPR, SOC 2, ISO 27001

Networking & API Gateway: TCP/IP, DNS, load balancing, ingress controllers, service mesh (Istio, Linkerd), API gateways (Kong, Traefik, Caddy), Cloudflare CDN/Workers, gRPC, NATS

Languages: PHP, JavaScript / TypeScript, Node.js, Python, Go, Bash / shell scripting; Java, Kotlin, Swift; C++ (Unreal Engine 5, hobby)

Frameworks: Laravel (5 → 13), Filament v5, Symfony, Slim, CodeIgniter, CakePHP, Zend; Vue, Nuxt, React, Next.js, Svelte; Django

Data, Streaming & Messaging: PostgreSQL + PostGIS, MySQL/MariaDB, MongoDB, Redis, Memcache, Elasticsearch; MQTT, Apache Kafka, RabbitMQ, NATS; Apache Airflow, Debezium (CDC), PgBouncer, replication, sharding, point-in-time recovery

AI / LLM Platform: Ollama, vLLM, OpenAI, Claude, Gemini; OpenAI-compatible inference; RAG pipelines, vector DBs; MCP (Model Context Protocol) — including authoring production MCP servers; ACP (Agent Communication Protocol); multi-agent orchestration (AgentFlow, Claude Code agent fleets); Claude Code, Claude Agent SDK, LangChain

Backup, DR & FinOps: Restic, Velero, Borg, geo-redundant storage, PITR, RTO/RPO targeting, multi-region active-passive / active-active, DR drills; Kubecost / OpenCost, right-sizing, reserved instances, spot automation, departmental chargeback

Platform Engineering & Testing: Backstage, Port, golden-path templates, service catalog, TechDocs, DORA metrics; Playwright, Cypress, k6, Gatling, visual regression

PERSONAL PROJECTS, OPEN SOURCE & SELF-HOSTED LAB

- **filex** and **runr.sh** — see Experience. **Linux kernel commits**: fixes for the ThinkBook ACPI issue and the Lenovo fingerprint sensor driver.
- **Self-hosted production estate (brf.sh)** — Docker + Caddy platform (40+ vhosts, automated wildcard TLS, Cloudflare Zero Trust mesh across three sites) hosting ~20 SSO-integrated services: Stalwart mail (DKIM/DMARC/MTA-STS), filex, Forgejo git mirror, Keycloak (passkeys), AFFiNE knowledge base, work.brf.sh (a self-built multi-tenant AI project/task platform where Claude agents work against per-project MCP tokens), plugNmeet video conferencing, Immich photos, Navidrome music, GlitchTip error tracking, Prometheus/Grafana monitoring, Coder cloud IDE with agent workspaces, and hourly dual-S3 DR with a warm standby site. Everything operated as code in a single infra monorepo.
- **Kubernetes lab (runr.sh)** — K8s 1.24 + Knative + Traefik + Longhorn + Kata Containers cluster used for runr.sh development, Confidential Computing experiments, and the internal LLM gateway (Ollama + vLLM + multi-model routing for IDE agents).
- **Open-source published packages**: PersianDate (PHP), notification-options (Laravel notification channel package), droneehliyet, burak.sh-website, laravel-test-runner-container (Docker container for Laravel test runs); plus tooling like mcp-outline for Outline integration and bsv3-sidetone — a Python CLI (Typer + hidapi/pyusb + pystray) that reverse-engineers the Razer BlackShark V3 Pro USB control transfers to enable headset sidetone without Razer Synapse.
- **Game development (hobby)** — designing a multiplayer tycoon/restaurant game in **Unreal Engine 5** (C++ core + Blueprint UI + Svelte/CEF for the UI layer), with custom systems for character customization (server-side persistence), overhead NPC order bubbles (CEF-rendered, dirty-flag + visibility-culling for 50+ customers), and runtime dynamic window/floor cutouts via GeometryScript Boolean operations. Also experimenting with Meshy and 3DAI Studio for character/NPC topology and auto-rigging.

EDUCATION

Uludağ University, Vocational School — Computer Programming · Bursa, Turkey

Darüşşafaka — Boarding School (English & French curriculum) · Istanbul

References, project portfolios, and infrastructure case studies available on request.