Just Run It · Security Overview

Customer-hosted workload automation · One-page brief for security & procurement review

Trevent Services LLC d/b/a Just Run It
https://justrunit.io
justrunit.io@gmail.com · 318-232-2280

Design principle: The control plane is the only tier that touches the database. Agents and operators use **authenticated APIs over HTTPS** — never direct database credentials on worker hosts.

1. DEPLOYMENT TRUST BOUNDARY

Customer-hosted

Software runs in the customer's environment (VM, bare metal, Docker Compose, or Kubernetes). Customer controls infrastructure, network policy, backups, and secrets storage.

No agent → database path

Agents register, heartbeat, claim work, and complete executions via the control-plane **HTTP API** only. PostgreSQL is private to application nodes on an internal network.

2. AUTHENTICATION & AUTHORIZATION

Control	Capability
Local accounts	Username/password with BCrypt hashes; admin user management UI and REST API
RBAC roles	**VIEWER** (read), **OPERATOR** (run/edit in managed workspaces), **ADMIN** (all workspaces, users, groups)
Optional SSO	OIDC (Entra ID, Okta, Keycloak, similar); modes: local, hybrid, or oidc-primary
API & agents	HTTP Basic with local service/operator accounts for machine clients and agents
Workspaces	Personal, group, and platform scopes — row-level visibility on one shared control plane
Audit	Operational audit events with actor attribution for significant actions

3. AGENT SECURITY MODEL

Pull-based workers

- Agents initiate **outbound** HTTPS to the control plane
- No inbound ports required on agent hosts for the platform
- Preferred-agent pinning targets trusted hosts by name

Trusted compute

- Agents execute COMMAND jobs on the host OS (customer-controlled)
- Customer owns script content, allowlisting, and OS hardening

- Treat agent credentials as privileged service accounts

4. DATA & SECRETS

Customer data stays with the customer

Job definitions, payloads, logs, and execution history live in the customer's deployment. Just Run It does not require a multi-tenant SaaS data plane for production use.

Support interactions

If logs are shared for support, they are used only to resolve the ticket. Optional Support Data DPA available when required by customer legal.

5. HARDENING CHECKLIST (CUSTOMER PRODUCTION)

Item	Recommendation
TLS	Terminate HTTPS at load balancer or reverse proxy in front of app nodes
Database	PostgreSQL on private network; strong credentials; regular backups
Bootstrap passwords	Change default admin/operator passwords before production use
Agent accounts	Dedicated least-privilege local account for agent Basic auth; rotate periodically
Network	Allow agents egress only to control-plane API; restrict admin UI by VPN/IP where policy requires
SSO	Prefer hybrid/OIDC with IdP MFA for human operators when enterprise SSO is available

6. WHAT SECURITY REVIEWERS SHOULD TAKE AWAY

- **API-centric control plane** — operators and agents authenticate; database is not exposed to workers.
- **Customer-controlled perimeter** — deploy in your estate; align with existing firewall, IAM, and backup standards.
- **Role + workspace governance** — multi-team use without sharing every definition with every user.
- **Clear responsibility split** — platform provides controls; customer owns host OS policy and job script risk.