

Public security overview

A practical view of identity, policy, regional execution, evidence, control status, and the incident path used for customer diligence.

CURRENT SCOPE

Architecture and build evidence available · certification and remaining deployed proof are not implied

Control record reviewed 2026-08-15

Document v2026-10-10

Buyer summary: distinguish architecture and build evidence from observed release tests. Confirm the release, environment, control owner and exceptions before relying on a result. A named owner or new assessment is not established by this document.

Published by Dayrook, operated by RadiantOS. Confirm current evidence at dayrook.com/security-center and commercial scope at dayrook.com/availability. This document is not certification.

FROM PRINCIPAL TO PROOF

Follow the security boundary through four accountable stages.

Each protected action begins with an authenticated operating context and returns a reviewable result to the workflow that owns it.

01

Identity and tenant scope

Dayrook resolves the principal, active tenant, customer, data region, session assurance, role, and entitlement before protected work reaches a domain owner.

02

Policy and approval

The owning route or service checks RBAC/ABAC, MFA, billing state, approval, consent, purpose-bound secret access, and the current resource state.

03

Regional execution

Selected-region services, workers, PostgreSQL, Valkey, and object storage run the operation; agents and collectors independently verify signed machine instructions and local policy.

04

Evidence and recovery

Allow, deny, material failure, provider result, retry, dead letter, rollback, restore, and customer communication evidence returns to the owning workflow and audit path.

CURRENT CONTROL INFORMATION

Separate provider foundations from evidence still being completed.

Status language is deliberately bounded. Build evidence, provider foundations, deployed workflow proof, and external confirmation are not treated as interchangeable.

PROVIDER FOUNDATION ACTIVE

US and EU platform foundation

Vultr records active US and EU VKE, PostgreSQL, Valkey, load-balancer, and regional storage foundations; remaining public edge, certificate, runtime, and customer-workflow proof stays explicit.

REGIONAL TESTS RECORDED · WORKFLOW PROOF CONTINUES

Tenant and regional database isolation

The requirements record deployed tenant-isolation tests against the canonical US and EU database targets while broader product and provider journeys still require release-specific evidence.

BUILD VERIFIED · DEPLOYED DEVICE PROOF PENDING

Agent and collector command trust

mTLS identities, pinning, signed envelopes, expiry, nonce, replay checks, and local policy are defined and build-tested; real signed-device and collector runs remain release evidence.

CONTROL DESIGN RECORDED · RELEASE PROOF CONTINUES

Encryption and secret boundaries

The security model requires encrypted regional data and state, object encryption for backups, client-side Vault item encryption, purpose-bound secret references, short-lived grants, and no plaintext secret logging. Release-specific runtime and recovery evidence remains part of diligence.

DILIGENCE BOUNDARIES

Make the open proof boundary visible before a claim is made.

The public position distinguishes documented architecture from release evidence, provider receipts, legal commitments, and independent certification.

REPORTING PATH AVAILABLE · RESPONSE PROMISE NOT PUBLISHED

Vulnerability reporting and remediation

Security concerns and suspected vulnerabilities can be routed through the security inquiry path. Triage, containment, remediation, evidence, and disclosure follow the incident process; no public severity-response deadline is claimed without an approved operating commitment.

PROVIDER PROJECTS EXIST · RUNTIME RECEIPTS PENDING

Observability and incident evidence

Sentry projects and PostHog dashboards are provider-recorded, but complete deployed, privacy-reviewed event and incident receipts remain pending.

READINESS WORK · NO CERTIFICATION CLAIM

SOC 2, ISO 27001, HIPAA-ready, GDPR-ready, and PCI posture

Architecture and control requirements support readiness work. Certification, legal compliance, BAA, DPA, or customer-specific claims require the appropriate external audit, assessor, legal review, approved agreement, and current evidence.

What this overview does not claim

It is not a SOC 2 report, ISO certificate, penetration-test attestation, legal opinion, BAA, DPA, uptime commitment, or promise that every product workflow has completed deployed customer proof. Verify the current evidence package for the scope you are evaluating.

ONE INCIDENT RECORD

Contain first, preserve evidence, and close with verified recovery.

The public process describes the operating sequence without publishing an unapproved severity-response deadline.

01

Classify impact and severity, page the accountable operator, and open one incident record.

02

Contain the affected tenant, region, provider, agent, credential, or workflow without expanding access.

03

Record impacted tenants, start and end time, exposure assessment, evidence, decisions, and corrective action.

04

Publish status and customer communication when a user-facing workflow is affected.

05

Close with recovery verification, root cause, prevention work, owners, due dates, and a postmortem where required.

Report a security concern

Route a suspected vulnerability or security concern into the documented inquiry path.

[Report a security concern](#)