Security Questionnaire (SOC 2 & CAIQ-style)

A current-state control response for vendor security reviews, organized around the SOC 2 Trust Services Criteria and CSA Cloud Controls Matrix. This is not a SOC 2 report, certification, penetration test, or legal commitment. Companion to the architecture document and security overview.

As of: July 29, 2026 · **Scope:** GaugeDesk desktop, GaugeWright Hub, GaugeDesk Administration, Vend, and GaugeWright-operated Embeddable Panels. Customer-operated deployments and third-party model providers retain their own control responsibilities.

Evidence basis: GaugeDesk `21caddc` · gaugewright-cloud `871288c` · WhippleScript private `db8b4fd` · GaugeWright company source `722079d` · gaugewright-site current deployment · live endpoint, GitHub-control, CI, access, dependency, recovery, SIEM-ingestion, alert, and notification review performed through July 29, 2026.

Status — Operating deployed and evidenced · Available in the downloadable product · Built implemented and tested, not evidenced as operating or released · Partial material gap remains · Planned committed, not built · No unavailable today.

Current posture. GaugeDesk is **not SOC 2 certified** and has not completed an independent penetration test. Its strongest controls are structural: fail-closed authorization, explicit agent abilities, scope isolation, append-only event history, cryptographic audit verification, and credential separation. Its largest remaining gaps are single-maintainer segregation of duties, external assurance, and multi-node availability. The internal baseline now includes protected branches, recurring secret/dependency/SAST scans, release SBOM/provenance generation, public privacy/DPA/subprocessor disclosures, live boundary monitoring, exercised restore and notification paths, and operating Azure security-event collection and alerting for production host and service metadata. Multi-node failover is explicitly deferred behind the current no-SLA, 8-hour internal RTO boundary.

Data-flow fact to read first. GaugeDesk is not local-only inference. Prompts and the context selected for a run are sent in plaintext inside TLS to the configured model provider. GaugeWright-operated public agents use an exact deployment-

authorized credential reference; the agent, browser, durable state, and tools do not receive credential bytes. With a customer-linked model account, the model-provider relationship is the customer's.

#	Domain / SOC 2	Control question	Current response	Status	Evidence
GRC-01	Governance · CC1–CC3	Is there a documented security and architecture model?	Yes. The company security-readiness program defines scope, risk/access/change/vulnerability/monitoring/incident/recovery/privacy controls and evidence expectations; product specifications define invariants, trust boundaries, lifecycles, and append-only ADRs.	Operating Available	DR-0045; company specs; GaugeDesk principles, architecture, ADRs
GRC-02	Assurance · CC4	Are SOC 2, ISO 27001, or other third-party certifications available?	No. There is no SOC 2 report, ISO 27001 certificate, or independent penetration-test report today. SOC 2 Type II and a SAML-scoped penetration test are planned.	No Planned	GaugeDesk `DEFERRED.md`
RSK-01	Risk assessment · CC3.2, CC9.1	Is there a recurring enterprise risk-assessment program?	Yes. DR-0045 establishes annual and material-change reviews, owner accountability, remediation or explicit risk acceptance, and tracking in each owning system. This July 28 audit is the inaugural dated review; the context-limited RSA verifier advisory is explicitly accepted and scheduled for reassessment.	Operating	DR-0045; operations spec; cloud audit policy; threat models
A&A-01	Assurance · CC4.1	Is the security model independently verified?	No. Quint models, adversarial teeth tests, property tests, and CI provide internal engineering assurance, not independent verification.	No Internal assurance	`specs/models/`, audit gate, CI
A&A-02	Assurance · CC4.1	Can a customer obtain audit evidence?	Public source, models, release artifacts, and selected live-verification evidence are available. Managed-service source and production evidence are private, and there is no SOC 2 report or standard customer evidence package.	Partial	Public GaugeDesk repo; private evidence by review
HR-01	People controls · CC1.4, CC6.2	Are workforce security, onboarding, and offboarding controls documented?	GaugeWright is founder-operated. Password/passkey custody and secret boundaries are documented; security training, background-check criteria, and formal workforce onboarding/offboarding are not.	Partial	Company systems and operations specs
IAM-01	Identity · CC6.1	Is SSO supported?	Google OIDC account sign-in is operating. OIDC and SAML verification, PKCE, JWKS rotation, signed-assertion verification, and SAML replay defense are built and tested; enterprise SAML is not evidenced in production.	Operating Built	Tracker `ID-2`–`ID-4`; live account service
IAM-02	Provisioning · CC6.2	Is automated provisioning supported?	Inbound SCIM provisioning/deprovisioning, hashed token storage, rotation, and throttling are built and tested. Operating customer SCIM and outbound synchronization are not evidenced.	Built	SCIM tests; `SEC-5`, `SECAUD-8`
IAM-03	Authorization · CC6.1, CC6.3	Are least privilege and segregation enforced?	Tenant-scoped RBAC, resource ABAC, server-derived capabilities, selected-tenant admission, and no-ambient-authority execution are implemented. Hub, Administration, Vend, Home, and public-session authority are separated.	Operating Available	`INV-1`, `INV-10`, `INV-11`; `ADMIN-ENV`
IAM-04	MFA · CC6.1	Is MFA enforced?	GaugeDesk does not perform a native second-factor challenge. A require-MFA policy is built and delegates the factor to the configured IdP; enforcement depends on customer/Google IdP policy.	Partial	Tracker `SEC-1`, `ID-5`
IAM-05	Authorization · CC6.1	Do access decisions fail closed?	Yes. Missing, stale, ambiguous, or unauthorized bases deny. Home and public targets perform fresh server-side admission rather than trusting navigation context.	Available Operating	`INV-20`; fail-closed model and admission tests

#	Domain / SOC 2	Control question	Current response	Status	Evidence
IAM-06	Sessions · CC6.1, CC6.3	Are session lifetime and idle timeouts enforced?	Enterprise session lifetime and idle-timeout enforcement is built and hashes bearer identifiers in the activity ledger. Hosted account refresh is operating. Customer-specific timeout configuration is not evidenced in production.	Built Partial	Tracker `SEC-2`; Hub auth
IAM-07	Privileged access · CC6.2, CC6.3	Is production access least-privilege and reviewed?	Production secrets are split by function in Infisical; Hub uses Azure workload identity and a path-scoped read-only machine identity. The July 28 review found one repository collaborator and active company Azure/Google identities; Cloudflare remains tied to the founder identity pending account migration. One founder necessarily retains broad authority.	Operating Partial	Systems spec; DR-0044/45; 2026-07-28 access review
DSP-01	Data inventory · C1.1	How is customer data classified and stored?	GaugeDesk separates records, append-only events, content behind handles, and projections. Desktop state uses local SQLite and a native content-addressed workspace store; hosted state also uses Azure volumes and Cloudflare R2/Durable Objects by service plane.	Available Operating	Data primitive; cloud README and edge configuration
DSP-02	Data flow · C1.1, C1.2	Does customer data leave the customer environment?	Yes when invoking remote inference, cloud backup/managed Home, account sync, or public publishing. Model prompts and selected context reach the provider. Public-panel model bytes bypass the author Home and management plane.	Operating (disclosed)	Protection and public-session specs; edge runtime
DSP-03	Isolation · CC6.6, C1.1	Is data isolated between customers and projects?	Authority scopes, Home admission, account scopes, deployment objects, and per-session Durable Objects enforce isolation. Hub and public runtime are live; a completed two-tenant Cloud Home conformance run is not evidenced.	Operating Partial	`INV-1`, `INV-10`; Home runbook; edge tests
DSP-04	Retention and deletion · C1.2, P4	Can data be retained and deleted by policy?	Local transcript deletion uses per-scope key destruction and purges unreachable workspace objects. Hosted retention ceilings and tombstones are built. End-to-end deletion, collection, and backup-erasure verification across every live plane is incomplete.	Available Partial	`SECAUD-6`; content-erasure and session specs
DSP-05	DPA and subprocessors · CC9.2, P3.1	Is a DPA and complete subprocessor list available?	Yes. GaugeWright publishes standard data-processing terms and a current list covering Azure, Cloudflare, GitHub, Google, Stripe, Infisical, and customer-selected identity/model providers. Binding terms are incorporated or signed with the customer; material vendor changes require review.	Available	DPA; subprocessors; legal spec
DSP-06	Privacy program · P1–P8	Is there a public privacy notice and data-subject request process?	Yes. The notice describes roles, categories, purposes, sharing, retention, security, choices, international processing, and verified request handling through the operating company mailbox, Jack@GaugeWright.com. A jurisdiction-specific privacy certification is not claimed.	Available	Privacy notice; legal spec
CEK-01	Encryption at rest · C1.1	Is data encrypted at rest?	AES-256-GCM content encryption, per-scope keys, crypto-erasure, and KMS wrapping are implemented; Azure Key Vault was live-tested. Production-wide application-level KMS configuration was not evidenced. Hardened mode warns rather than fails when the content KEK is absent.	Built Partial	`SEC-4`, `SECAUD-6`, `SECAUD-9`
CEK-02	Encryption in transit · CC6.7	Is data encrypted in transit?	Public web/API/provider paths use TLS; live endpoints accepted TLS 1.2 with valid certificates. The rendezvous relay carries opaque end-to-end encrypted and signed envelopes over plaintext TCP, exposing connection metadata but not payload plaintext.	Operating Partial	Live TLS probe; relay runbook

#	Domain / SOC 2	Control question	Current response	Status	Evidence
CEK-03	Key and secret management · CC6.1	How are keys and secrets managed?	Machine secrets are held in function-separated Infisical projects/paths. Hub delivery uses Azure managed identity, short-lived tokens, a read-only path, an unprivileged agent, and a tmpfs-rendered file. KMS and exact-reference credential boundaries are implemented.	Operating Built	Systems spec; Infisical runbook; public credential boundary
CEK-04	Confidential computing · C1.1	Is confidential computing available?	The AMD SEV-SNP verifier and Azure Key Vault/Secure Key Release adapters are built and tested with real Milan evidence. A generally available confidential-VM service and confidential inference are not operating.	Built Planned	Attestation tracker; cloud attestation module
LOG-01	Audit logging · CC7.2	Are security-relevant actions audited?	Mutations are attributed to the authenticated actor in an append-only event log. Project-content read auditing is available but off by default. Management commands produce durable review and receipt evidence.	Available Partial	`SECAUD-4`; audit and command tests
LOG-02	Log export · CC7.2	Can audit events be exported to a SIEM?	A bounded, ordered, retrying application-audit exporter with failure, drop, and lag counters is built. GaugeWright now operates a central Azure collector for production host and service security metadata, but the product audit exporter remains configured per deployment rather than attached to that company collector.	Built Partial	`SECAUD-3`; cloud monitoring runbook
LOG-03	Audit integrity · CC7.2	Are audit logs tamper-evident?	Entries are SHA-256 chained and the head is signed by the governance key; verification detects edits, relinking, truncation, and missing anchors. An external witness is recommended and not evidenced as operating.	Built Partial	`SECAUD-2`; audit-chain model
LOG-04	Monitoring · CC7.2, CC7.3	Is centralized production monitoring and alerting operating?	Yes. Azure Monitor Agent sends metadata-only production host and service security events to a 30-day Log Analytics workspace. Authentication-anomaly, host-error, and missing-heartbeat rules evaluate every five minutes and route Sev1 alerts to the responder. Exercise `DR-0047-20260729T150800Z` was ingested at 15:07 UTC and fired the authentication alert at 15:10 UTC. Separate 15-minute probes monitor every public boundary.	Operating	DR-0047; cloud `871288c`; Azure workspace, DCR, alerts, and exercise; production monitor
SEF-01	Incident response · CC7.3–CC7.5	Is there an incident-response and breach-notification process?	Yes. The six-stage runbook covers containment, evidence preservation, recovery, notification, and postmortems. DR-0045 establishes the founder responder and annual/pre-customer exercise cadence; a forced alert and recovery notification were exercised July 28. Independent review and a staffed rotation are unavailable.	Operating Partial	Incident runbook; monitor exercise and recovery; DPA
BCR-01	Backup and recovery · A1.2	Are backups and restores tested?	Cloud Home creates encrypted recipient-wrapped restore points and refuses live or non-erased destinations. On July 28 the complete rewrap-and-restore path succeeded against an erased test Home; an annual scheduled exercise preserves evidence. Internal targets are RPO 24h/RTO 8h, not a customer SLA. Desktop users own local backups.	Operating Partial	Recovery run `30369546925`; annual workflow; DR-0045
BCR-02	Availability · A1.1, A1.3	Is there an SLA, status page, and resilient service design?	Public sessions inherit Cloudflare Durable Object recovery. Hub, account, Vend, hosted GaugeDesk, relay, directory, and the current private Home share one Azure VM. There is no uptime SLA, public status page, multi-node failover proof, or capacity test. DR-0047 retains this recoverable single-node posture while the application is polished; failover becomes mandatory before an uptime SLA or outage tolerance shorter than the internal 8-hour RTO.	Partial	DR-0047; cloud deployment and recovery runbooks

#	Domain / SOC 2	Control question	Current response	Status	Evidence
CCC-01	Change management · CC8.1	Are changes authorized, tested, and traceable?	Yes within the founder-operated model. All seven active repositories protect main against administrator force-push and deletion and require linear history. Specifications/ADRs, atomic commits, automated CI, security scans, and traceable emergency-bypass rules govern changes. Founder direct pushes remain permitted; cloud and GaugeDesk core CI are green.	Operating Partial	Branch protection review; CI runs; DR-0045
CCC-02	Segregation of duties · CC8.1	Is independent change approval required?	No. The founder-operated workflow permits the same person to author, approve, deploy, and verify a change. This is understandable at current scale but is not an independently enforced control.	No	Repository settings and operating contracts
TVM-01	Vulnerability management · CC7.1	Are dependencies scanned and patched?	Yes. GaugeDesk, cloud, and WhippleScript run weekly dependency audits plus per-change CI. Findings are remediated or explicitly accepted. The sole live advisory has no fix and is accepted as non-applicable because its dependency performs public-key SEV certificate verification only, never RSA private-key operations.	Operating	Security workflows; cloud audit policy; green scans
TVM-02	Secure code analysis · CC7.1	Are SAST and secret scanning enabled?	Yes. Active source repositories run pinned Semgrep and Gitleaks on main changes, pull requests, and weekly schedules. Both public mirrors have GitHub secret scanning and push protection enabled. Models, linting, tests, and the audit gate add coverage.	Operating	Security workflows; GitHub security settings 2026-07-28
TVM-03	Threat modeling · CC3.2, CC7.1	Is there a documented threat model?	Yes. The architecture covers STRIDE, OWASP LLM risks, MITRE ATLAS, trust boundaries, and mitigations. Formal models exercise authorization, confidentiality, replay, lifecycle, and failure behavior; operational review cadence is not formalized.	Available Partial	Architecture §7; `specs/models/`
STA-01	Software inventory · CC8.1	Is an SBOM produced?	GaugeDesk and WhippleScript release workflows now generate SPDX JSON SBOMs and attach them to each future published release. Releases predating July 28 do not have retroactive SBOMs.	Built Next release	Product release workflows
STA-02	Build provenance · CC8.1	Is formal build provenance available?	GaugeDesk and WhippleScript release workflows now issue GitHub OIDC build-provenance attestations for published artifacts. Newly added security-critical actions are commit-SHA pinned. Releases predating July 28 do not have retroactive attestations.	Built Next release	Product release workflows; pinned attestation action
STA-03	Artifact signing · CC8.1	Are released binaries signed and notarized?	Updater signing is active. A manual macOS lane proves Developer ID signing, notarization, stapling, and Gatekeeper acceptance, but public v0.4.3 predates it. Windows and Linux OS-level signing are absent; the signed APT channel has not published its first eligible release.	Built Partial	Release run `30312798616`; `APT-1`; releases
AIS-01	Application security · CC6.1, CC7.1	How is agent over-reach constrained?	Agents receive an explicit immutable ability ceiling. Offered tools, runtime capabilities, and pre-executor dispatch reject unoffered calls; credentials are never an agent ability. Linux/macOS enforce method isolation. Windows sandboxing and fully verified default-deny per-host egress remain incomplete.	Available Built Partial	`ABIL-1`–`3`; `INV-11`, `INV-24`
AIS-02	Browser security · CC6.6, CC6.7	Are defensive HTTP headers deployed?	Yes. The website, account API, Hub, GaugeDesk, and Vend return HSTS, CSP, X-Content-Type-Options, anti-framing, Referrer-Policy, and Permissions-Policy; Embed returns the compatible non-framing subset. Chrome render checks found no CSP console errors. The shared cookie is Secure, HttpOnly, SameSite=Lax, and scoped to `.gaugewright.com`.	Operating	Live header/Chrome probes 2026-07-28; edge configuration

#	Domain / SOC 2	Control question	Current response	Status	Evidence
AI-01	AI governance · CC3, C1	Is AI risk governed?	The product maps to NIST AI RMF, binds action to admitted authority, records the model data flow, and gates durable/released outputs. There is no organization-wide model inventory, evaluation/bias program, periodic AI risk review, or model-change process.	Partial	Architecture §10; release/review specs
AI-02	Model-provider boundary · C1.1	Is the model-provider flow and credential boundary documented?	Yes. Prompts and selected context reach the provider. Public deployments bind an exact credential reference to a permitted class; only the final-fetch boundary injects authentication, and provider bytes bypass the author Home and management services.	Operating (disclosed)	Public-session spec; cloud and runtime evidence
IPY-01	Portability · C1.2, P6	Can a customer export and leave with their data?	Desktop data is local and event-sourced; Cloud Home export/restore APIs exist. A complete self-service export covering account, hosted work, public-session metadata, billing, and deletion confirmation is not evidenced.	Partial	Local store and cloud export implementation
VND-01	Vendor management · CC9.2	Are service providers risk-reviewed?	The systems directory records each provider's purpose, authority, credential boundary, and status; the July 28 review reconciled operating subprocessors and data flows. DR-0045 requires annual review and pre-use review for new critical subprocessors. A complete current set of vendor SOC reports has not been collected.	Operating Partial	Systems/legal specs; DR-0045; subprocessor list
PHY-01	Physical security · CC6.4	How is physical security handled?	Customer-local devices remain the customer's responsibility. Hosted controls are inherited from Cloudflare and Microsoft Azure; this audit did not find collected vendor SOC reports or a formal shared-responsibility review.	Inherited / Partial	Cloud inventory; vendor assurance gap

Security contact: Jack@GaugeWright.com · Last reviewed July 29, 2026. This questionnaire supersedes prior status statements where they differ. Answers intentionally separate structural product controls from operating processes and independent assurance.