TRULY AGENTIC (INDEPENDENT ENGINEERING PRACTICE — ANIL PERVAIZ)

MVSP (BYOC Profile) v1.0

Minimum Viable Secure Product (MVSP) vendor readiness baseline adapted for single-tenant Bring-Your-Own-Cloud (BYOC) AI governance deployments.

November 24, 2026

Security Questionnaire Response

https://trulyagentic.io

security@trulyagentic.io

Response Summary

Answer	Count	Percentage
Yes	11	91.7%
Partial	1	8.3%
No	0	0.0%
N/A	0	0.0%
Total	12	100%

Business Controls

3/4 controls satisfied

ID	Question	Answer	Explanation
MVSP-1.1	Do you maintain a documented vulnerability disclosure process?	YES	Published at https://trulyagentic.io/.well-known/security.txt and routed to security@trulyagentic.io with a 3-business-day initial response commitment.
MVSP-1.2	Is customer operational data segregated from other customers?	YES	Strongest possible physical & account segregation: each deployment runs inside the customer-owned AWS, GCP, or Azure account with zero shared multi-tenant data stores.
MVSP-1.3	Have you completed an independent annual penetration test or SOC 2 audit?	PARTIAL	Adversarial regression suites (ASI01–ASI06) run continuously in CI on synthetic harnesses, and full source/IaC artifacts are open for prospect CloudSec audit under Mutual NDA. Formal third-party CPA/pentest reports are planned alongside enterprise contract milestones.
MVSP-1.4	Is customer training, testing, or subprocessor disclosure transparent?	YES	Public Privacy Policy (trulyagentic.io/privacy) and this Trust Center list every web/email subprocessor explicitly and confirm zero customer data egress from BYOC environments.

Application Design & Authentication Controls

3/3 controls satisfied

ID	Question	Answer	Explanation
MVSP-2.1	Are user authentication and SSO federated to customer identity providers?	YES	Customer runtimes integrate with OIDC/SAML workload identity (Okta, Microsoft Entra ID, Google IAM, AWS IAM OIDC), while write approvals verify named Slack/Teams user identities.
MVSP-2.2	Are authorization checks enforced consistently on every sensitive action?	YES	Every tool execution passes sequentially through Control 1 (Identity/Registry), OWASP Scanner, Control 2 (PolicyEngine), Control 3 (ApprovalGate), and Control 5 (Fail-Closed Ledger).
MVSP-2.3	Do hosted web properties avoid unnecessary tracking cookies?	YES	trulyagentic.io and trust.trulyagentic.io serve zero advertising cookies, zero third-party ad pixels, and route analytics strictly through cookieless/consent-respecting telemetry.

Application Implementation & Supply Chain Controls

3/3 controls satisfied

ID	Question	Answer	Explanation
MVSP-3.1	Are secrets kept out of source repositories and encrypted at runtime?	YES	Secret hygiene checks ensure .env files remain gitignored, production web keys sit in encrypted Cloudflare Pages secret_text bindings, and BYOC runtime credentials stay inside customer Secrets Manager / Key Vault.
MVSP-3.2	Are dependency versions locked and GitHub CI actions pinned?	YES	Repositories use committed lockfiles (pnpm-lock.yaml / package-lock.json), automated dependency monitoring, and SHA-pinned GitHub Actions steps with minimal workflow token permissions.
MVSP-3.3	Are security headers and TLS 1.2+ enforced across public endpoints?	YES	All public endpoints on trulyagentic.io and trust.trulyagentic.io sit behind Cloudflare edge TLS 1.2+ with HSTS, X-Content-Type-Options, and strict CORS/origin validation.

Operational Controls

2/2 controls satisfied

ID	Question	Answer	Explanation
MVSP-4.1	Are immutable audit logs generated and exportable to customer SIEMs?	YES	PostgreSQL append-only hash chains prevent DELETE/UPDATE mutations and stream to customer-owned WORM buckets (S3 Object Lock / GCS Retention Lock) for SIEM ingestion.
MVSP-4.2	Are customer backups and disaster recovery controlled by the customer cloud policy?	YES	Because runtime state lives inside the customer cloud account, automated database snapshots, WORM retention policies, and regional failover follow the customer CloudSec policy directly.