HYPERCISO

Security leadership as a service, with the record to prove it

A virtual CISO engagement run on one platform: frameworks, risks, policies, tasks, evidence, assets, vulnerabilities, vendors and incidents in a portal your team signs in to, with an AI copilot that proposes and a person who approves.

Who it is for

Organizations that need a CISO's judgment and a defensible security program without a full-time hire: regulated small and mid-size businesses in healthcare, payments, financial services, gaming and property management, companies facing a customer security questionnaire or a first audit, and any team whose compliance work currently lives in spreadsheets and email. HyperCISO is delivered as a HyperHaze engagement; the same multi-tenant platform is available to consultancies that run vCISO engagements for their own clients.

How an engagement runs

- **Onboarding in one sitting.** A five-step wizard captures your organization profile and target frameworks, the engagement scope (Full vCISO, Policy Development, Framework Readiness or Maturity Goal), a secure intake, and a baseline assessment across access control, asset management, data protection, incident response and security awareness. Kickoff tasks are created for every scope you select.
- **A questionnaire that turns answers into work.** Your vCISO builds a questionnaire specific to your organization; every "no" or "partial" answer generates the remediation task the question recommends, tagged with the framework and domain it came from.
- **A weekly rhythm.** Every Monday the platform snapshots your posture and the copilot reviews the program and drafts recommendations for your vCISO to approve. Daily jobs send task reminders and scan your software inventory for new vulnerabilities.
- **Reporting you can hand upward.** The Reports page and its executive PDF give leadership compliance per framework, open risks, policy status and a written executive summary.

What ships today

Real-time compliance

- Select the frameworks that apply; each brings a paraphrased requirement set with links to the official reference.
- Mark every requirement compliant, not compliant or not applicable, with an evidence summary, notes and linked evidence files; set an audit due date per framework.
- Framework rollups on the dashboard, the Reports page and the executive PDF. A cross-framework mapping table lets one requirement's status and evidence inform its counterparts in other standards.

Risk register

- Strategic, compliance, operational, financial and reputational risks scored by likelihood and impact from low to critical.
- Mitigation plan, strategy, owner and due date per risk; status moves from open through mitigating to accepted, transferred or closed.

Policy library

- Policies with owner, version, version history, control mapping and framework link; status draft, under review, approved or expired, with next-review dates.
- Documents stored privately and served through short-lived links; copilot drafts and revisions arrive as Markdown drafts for a person to finalize.

Tasks and reminders

- Governance, technical and compliance tasks with priority, due date, assignee, framework and linked control; comments and evidence on every task.
- Recurring tasks (daily to yearly) regenerate themselves on completion; assignment and due-date reminder emails, with reminder windows set per customer, per user or per task.

Evidence vault

- Upload once, reuse everywhere: evidence attaches to requirements, tasks, vendors and incidents.
- Files live in a private bucket with no direct client access; uploads go through the server and downloads use signed URLs after an ownership check.
- A per-customer freshness window flags evidence that is stale or missing, in every posture snapshot and in your vCISO's compliance view.

Asset inventory and vulnerability watch

- Applications, services, infrastructure and endpoints with owner, environment and criticality, linked into the stack each application depends on and to the vendor behind each service.
- Import an application's npm manifest (package.json, or the full package-lock tree) to inventory its components at exact versions.
- A daily scan matches every component against OSV.dev and flags CVEs on the CISA Known Exploited Vulnerabilities list. Findings carry severity, fixed version and a status workflow (open, in progress, resolved, ignored, not affected), auto-resolve when the fix ships, and escalate to an incident in one click. New critical and high findings reach your vCISO by email the same day.

Vendor risk

- A register of the providers you depend on, by category, criticality, data classification and risk rating, with contacts and a review cadence that produces next-review dates.
- Vendor evidence reuses the evidence vault; vendors link to the assets they serve and to any incident they cause.

Incident response

- Incidents by category and severity with a status workflow from open through investigating and contained to resolved and closed.
- A timeline of detection, triage, containment, eradication, recovery and communication events; linked assets, vulnerabilities, vendors and evidence; remediation tasks; root cause and lessons learned on the record.

Posture trends and reporting

- Weekly snapshots of compliance per framework, open and overdue tasks, open risks by level, policies due for review, evidence gaps, vulnerabilities, incidents and vendor reviews overdue, charted as trends.
- A Reports page with an executive summary, compliance by framework, risk and policy breakdowns, and an executive PDF export.

AI copilot

- For your vCISO: chat grounded in your program through read-only tools, a weekly program review with recommendations, policy drafting and revision, compliance status suggestions, meeting-prep briefings and an executive narrative for the Reports page.
- Reads the evidence files linked to a requirement, within fixed limits, to check that the evidence supports the status.
- For your team, on request: a read-only assistant that answers questions about your own program under your own permissions.

How the AI is governed

- **Proposals, never actions.** Every change the copilot wants to make, whether a task, a risk, a policy draft, a compliance status or a framework mapping, is a recommendation in a queue until a person approves it. Approval re-validates the payload, applies it once, and records who approved it and what was written.
- **Grounded in your data, scoped by the database.** The copilot reads through tools over your own program; the tenant is fixed server-side and the model never chooses it. The team assistant runs under the asking user's own row-level permissions.
- **Every run is logged first.** Kind, model, status and token usage are recorded before the model is called; if the record cannot be written, the run does not happen.
- **Your text is data, not instructions.** Questionnaire answers, notes and evidence file contents are treated as untrusted input. Evidence reads are capped at 10 MB per file, 15,000 characters of text and five files per run.
- **A known model, chosen per customer.** Anthropic Claude through the Vercel AI SDK, pinned per customer when required.
- **An honest boundary.** The copilot does not scan your network, does not make compliance determinations and does not replace your vCISO. It prepares work for a person to review.

Security architecture

- **Tenant isolation is enforced in the database.** Every tenant row carries its tenant and is guarded by Postgres row-level security built on shared helper functions; user sessions never bypass it, and service-role jobs always filter by tenant explicitly.

- **Private files.** Evidence and policy documents sit in private buckets with no direct client access: uploads go through the server, downloads through short-lived signed URLs after an ownership check.
- **Least privilege by role.** Per-app roles (administrator, user, read-only) for your team; a separate super-admin role for HyperHaze operators, who open a customer's view through a bridge that still runs under row-level security. Archived customers are locked out of every app.
- **Deterministic scanning.** Vulnerability matching uses OSV.dev and the CISA KEV catalog as data sources, never model output; every scan run is logged with what it found.
- Data is encrypted in transit and at rest by the managed hosting providers; scheduled jobs authenticate with a shared secret; the platform has been through an internal security review with findings remediated.
- **An honest boundary.** HyperCISO is a managed multi-tenant service: HyperHaze operators can see your program data because delivering the engagement requires it, and every AI run against it is logged. Model calls go to Anthropic's API under commercial terms that exclude training on them. There is no self-hosted edition.

Deployment

	As a HyperHaze engagement	As a platform for your practice
MODEL	Scoped vCISO engagement delivered by HyperHaze; your team signs in to the HyperHaze portal	Your consultancy runs its own clients as tenants; HyperHaze operates the platform
FOOTPRINT	Operated for you	Operated for you: per-client tenants, roles and app enablement, plus the operator console with intake wizard, questionnaire builder, framework catalog, copilot and operations
GETTING STARTED	Onboarding by engagement agreement	Partner onboarding by agreement

Stack: Next.js and React on Vercel; Supabase (Postgres 17 with row-level security, authentication and private storage) hosted in AWS us-west-2; Anthropic Claude through the Vercel AI SDK; Resend for email. TypeScript throughout.

Frameworks in the catalog

Requirement sets ready today: CIS Controls, NIST CSF, HIPAA, PCI DSS and PCI DSS SAQ A, FTC Safeguards Rule (GLBA), SOC 1, SOC 2 and SOC 3, SOX, GLI-11, GLI-19 and GLI-33, NIGC, Nacha Operating Rules (ACH), MA 201 CMR 17.00, NY SHIELD Act, and records retention for HOAs.

Catalog entries whose requirement sets are built during onboarding: ISO/IEC 27001 and 27002, NIST SP 800-171, HITRUST CSF, HITECH, NIGC MICS, GDPR, CCPA/CPRA, COPPA, CIPA, CISA and ITAR. Requirement sets are paraphrased and maintained by HyperHaze; every requirement links to its official reference.

Surfaces

Web, responsive from phone to desktop, in light and dark themes, from the HyperHaze portal alongside any other HyperHaze app your organization uses. Notifications and reminders by email.

Roadmap

Phase-level, no dates.

- **Now:** requirement sets for the remaining catalog frameworks, starting with ISO/IEC 27001 and NIST SP 800-171; the team assistant opened to more customers; a curated cross-framework mapping library.
- **Later:** manifest import beyond npm; evidence collection from cloud and identity providers; customer security questionnaires answered from the evidence vault; single sign-on for customer teams.

Proof in use

HyperCISO has run customer engagements in production since early 2026, alongside HyperHaze's own security program. The weekly review, the daily vulnerability watch and the reminder jobs run unattended.