Ethan Henderson

Network and Systems Engineer Turned Startup CTO

ethan@gtfo.dev · San Jose, CA
gtfo.dev · blog.gtfo.dev · gnu.foo

PROFESSIONAL SUMMARY

Network and systems engineer turned startup CTO. Led IT for a 100+ person organization — built zero-trust network access, centralized monitoring, and a HIPAA compliance program from scratch. Designed and built a zero-knowledge identity platform from the ground up using secure-by-design principles. Wrote the cryptographic specifications the system runs on, filling gaps where no existing standard applied.

EXPERIENCE

CTO — Kyndex

Jan 2025 – Present

Shared KYC infrastructure for regulated identity verification. Handles government-issued documents and biometric data under zero-knowledge constraints — no plaintext at rest, no server-side exposure.

Built the full platform as sole technical lead — backend services, cryptographic layer, key hierarchy, and security architecture

- Implemented end-to-end authenticated encryption across enclave and edge runtimes — AES-256-GCM with structured key lifecycle, canonical AAD binding, and no plaintext exposure outside the enclave boundary
- Deployed across Cloudflare Workers, Durable Objects, and AWS Nitro Enclaves with KMS-backed key attestation — designed for zero-trust between every service boundary
- Designed a grant lifecycle with state machine enforcement, per-grant claim tokens, mandatory TTL, and atomic claim-count controls

Systems & Network Engineer / Administrator — Shadow Corp

Feb 2024 – Jan 2025

Department head. Built the IT security program for a 100+ person organization from the ground up — no existing infrastructure, no prior compliance posture.

Designed and deployed zero-trust network access from scratch — multi-factor authentication chain from biometric logon through SSO and Kerberos, with shift-length-gated session revocation, across ~150 endpoints

- Built centralized logging and monitoring pipeline — aggregated system, network, and kernel-level telemetry, down to monitoring loaded drivers to detect hardware and software state changes in real time
- Stood up HIPAA compliance program from near-zero — wrote policies, implemented technical controls, and conducted the organization's first self-assessment
- Built the underlying compute environment from scratch — containerized and virtualized the ZTNA, logging, and IAM services across Hyper-V and Docker

PUBLICATIONS & SPECIFICATIONS

Specification	Description
AEAD additional authenticated data canonicalization specification	Deterministic byte representation of authenticated metadata before encryption — ensures cross-implementation interoperability with conformance test vectors.
AEAD encryption envelope wire format specification	Binary wire format for encrypted payloads covering key rotation, algorithm negotiation with downgrade prevention, and envelope encryption for key commitment.

TECHNICAL FOCUS

Area	Details
Architecture & Design	Zero-trust network design, zero-knowledge system design, secure-by-design architecture, AEAD envelope encryption
Compliance	HIPAA, SOC 2, NIST — policy authoring, technical controls, self-assessment
Infrastructure	Centralized logging and monitoring pipelines, Linux security internals (permissions, capabilities, ACLs)
Tooling	Security tooling and automation, formal specification authoring, cryptographic library development

OPEN SOURCE

Project	Description
httprift	HTTP desync research platform. Compiles real web server source to WebAssembly for scoped desync testing with a differential engine for parsing discrepancy detection.
whyno	Linux permission debugger. Traces every permission layer from mount options to POSIX ACLs and reports what's blocking with least-privilege fix recommendations.
canaad	Reference implementation of the AAD canonicalization spec. Ships as a core library, CLI tool, and browser-ready WebAssembly package.