H33 Eliminates the Last Barrier to Post-Quantum Adoption: Automatic Cryptographic Engine Selection Requires No Expertise

The only platform with 3 FHE engines, 2 ZK provers, and post-quantum signatures pre-integrated. One API call. Zero cryptographic expertise required.

H33 Logo

RIVERVIEW, FL, UNITED STATES, April 8, 2026 /EINPresswire.com/ -- H33.ai, Inc. today announced the general availability of IQ Routing, an intelligent cryptographic routing system that automatically selects the optimal Fully Homomorphic Encryption engine and Zero-Knowledge prover for each operation across three FHE families and two post-quantum STARK systems. The announcement addresses a documented barrier to post-quantum adoption: no single cryptographic scheme is optimal for all workloads, and the expertise required to evaluate and configure multiple schemes simultaneously is not available at most organizations.

> The industry said post-quantum conversion had to cost millions, slow your systems, increase storage, take years, and require infrastructure overhauls. Every one of those claims is false”
>
> *— Eric Beans, CEO, H33.ai, Inc.*

The Challenge: Cryptographic Complexity Is Slowing Adoption

Post-quantum encryption is no longer optional. NIST finalized FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) in 2024. The NSA requires post-quantum algorithms for classified systems by 2030. Federal agencies must complete migration by 2035. The harvest-now-decrypt-later threat is documented and active.

Adoption has been slow despite regulatory urgency. BFV handles integer arithmetic efficiently but is poorly suited to floating-point operations. CKKS handles approximate arithmetic but introduces noise unacceptable for exact integer comparisons. STARK Lookup proofs are appropriate for pre-computed membership verification but cannot handle novel multi-attribute proofs. STARK AIR proofs handle complex circuits but carry higher generation cost. Without intelligent routing, developers must make these selections manually — or select a single scheme and accept the performance and correctness tradeoffs. This requires specialized cryptographic

engineering talent that most organizations do not employ.

IQ Routing is designed to handle this selection automatically, in under 500 nanoseconds per operation.

H33.ai - The World's First Complete Quantum-Proof Security Platform

How IQ Routing Works

FHE-IQ evaluates each operation and routes it to the appropriate engine based on data type, precision requirements, and security context. H33-128 BFV handles integer arithmetic, biometric matching, and fraud scoring at NIST Level 1, using a single 56-bit modulus with no relinearization required for authentication circuits — reducing NTT operations from four to one. H33-CKKS handles floating-point operations and ML inference on encrypted data, with Chebyshev bootstrapping and automated scheme switching. H33-BFV32 is optimized for ARM mobile and edge environments without sacrificing post-quantum security guarantees.

When a pipeline requires both integer comparison and floating-point scoring — a common pattern in fraud detection and biometric authentication — FHE-IQ handles the BFV-to-CKKS scheme transition automatically, without developer intervention. The routing decision adds under 500 nanoseconds of overhead, negligible relative to the cryptographic operation being selected.

ZK-IQ applies the same routing logic to zero-knowledge proof selection. STARK Lookup handles membership proofs, sanctions screening, and credential verification at 0.059 microseconds cached — suited to high-frequency verification of known sets. STARK AIR handles novel proofs: complex attribute verification, compliance circuits, and multi-condition proofs requiring a full Algebraic Intermediate Representation constraint system with Poseidon hash binding and FRI polynomial commitments. Both systems use SHA3-256 hash-based security with no elliptic curve assumptions and no trusted setup, making them post-quantum secure by construction. This is a meaningful distinction from SNARK-based systems such as Groth16 and PLONK, which rely on elliptic curve pairings that are vulnerable to quantum computers.

The developer specifies what needs to be proven. IQ Routing determines the mechanism.

The Complete Platform

H33 offers the following components pre-integrated through a single API: three FHE engines (H33-128 BFV, H33-CKKS, H33-BFV32); two post-quantum ZK provers (STARK Lookup, STARK AIR);

three post-quantum signature families (ML-DSA Dilithium, FALCON-512, ML-KEM Kyber); a 3-key nested hybrid signature combining Ed25519, Dilithium, and FALCON across three independent mathematical families; ArchiveSign for 50-year archival signatures with SLH-DSA; FHE-encrypted biometric matching with k-of-n threshold decryption — plaintext never accessible to any single server; AI Compliance wrapping for any inference endpoint; FraudShield for cross-institution encrypted fraud detection without data sharing; H33-Gateway as a drop-in proxy for existing infrastructure; MedVault for HIPAA-compliant record processing; and QuantumVault for post-quantum migration assessment of existing systems.

Production Performance

Independent measurement on AWS Graviton4 (192 vCPU, 96 workers) recorded sustained throughput of 2,209,429 operations/sec over a 120-second continuous window with variance of ±0.71%. Each operation included the complete pipeline: FHE biometric matching, ZK-STARK proof, Dilithium attestation, and ML threat analysis. No GPUs, FPGAs, or specialized hardware were used. Per-operation pricing at volume is $0.0001.

Independent Verification

A live performance test is available at h33.ai. The test executes 1,000 full-stack post-quantum authentications from the visitor's browser directly to H33's production cluster with no caching or pre-computation. Latency for each request is displayed in real time and observable via the browser's Network tab.

H33's production codebase has been evaluated through HICS (H33 Independent Code Scoring), a ZK-STARK attested, Dilithium-signed code evaluation system with an open-source scoring formula, achieving a score of 100/100. HICS-PQ provides per-library attestation for Dilithium, Kyber, FALCON, SPHINCS+, and all three FHE engines at every release, independently verifiable at h33.ai/pq.

Industry Applications

The platform is currently applied across regulated industries. In banking and financial services: post-quantum transaction attestation, encrypted fraud detection across institutions without data sharing, and FedNow-compatible payment signing. In government and defense: FIPS 203/204 native compliance and CNSA 2.0 readiness. In healthcare: patient record processing without decryption, with field-level PHI encryption. In blockchain: H33 Shield for Solana provides real-time post-quantum block attestation, FHE-encrypted account data, and ZK-STARK on-chain verification, available at h33.ai/solana-shield.

Compliance and Intellectual Property

H33 holds 144 patent claims pending covering FHE engines, ZK-STARK proofs, nested hybrid

signatures, AI-blind processing, and independent code scoring. The platform is pursuing SOC 2 Type II and ISO 27001 certification via Drata, with completion expected June 2026. HIPAA compliance controls are implemented. All cryptographic implementations are NIST FIPS 203/204 native. The codebase includes 58,779 automated tests including randomized property-based inputs across all cryptographic modules.

H33 has also published the H33 AI Trust Standard (HATS) v1.0, a cryptographically-enforced AI trust certification framework covering governance proof, data separation, and quantum-secured audit permanence across three certification tiers. The standard has been submitted to NIST and is available at h33.ai/standard.

Availability

IQ Routing is available to all H33 customers at no additional cost. The platform is available through AWS Marketplace, enabling procurement through existing AWS accounts and enterprise agreements. Enterprise customers already operating within AWS can add H33 without a separate vendor onboarding process. API access and a live browser performance test are available at h33.ai without signup.

Eric D Beans
H33.ai, Inc.
+1 813-464-0945
email us here
Visit us on social media:
LinkedIn
YouTube
X