

Entro Security: Secret Discovery vs. Secret Elimination

Entro discovers the secrets and non-human identities scattered across code, config, clouds, and pipelines, monitors their use, and detects leakage and exposure. Every leaked key it surfaces is a symptom of one root cause: identity is proved by possession of a static secret. Keyless identity removes the secret.

Vendor and Product Reality

Entro Security is a non-human identity and secrets-security platform. As publicly described, it discovers the secrets and non-human identities scattered across an organization, in code repositories, configuration, cloud platforms, vaults, and CI pipelines, builds context around each one such as what it grants and who owns it, monitors how secrets are used, and detects misuse, leakage, and over-exposure. The product addresses secrets sprawl, the reality that API keys, tokens, and credentials end up copied into many places and forgotten, by making the sprawl visible and monitored so that leaked or dangerous secrets can be found and rotated. It is a capable answer to a genuine and widespread security failure.

The Architectural Choice: Discover the Secret, Keep the Secret

Entro's premise is that secrets exist and must be discovered, monitored, and governed. That premise is correct about the world as it is, and the work is necessary, but it leaves the secret in place. The lifecycle Entro improves, find the secret, assess its exposure, rotate it, monitor for misuse, is a lifecycle that exists only because the secret is the unit of identity and authentication. Every leaked key that Entro surfaces, every over-permissioned token it flags, is a symptom of the same root cause: identity and access are proved by possession of a static secret, and static secrets, by their nature, get copied, stored, exposed, and stolen. Discovering and rotating secrets is harm reduction over an architecture that produces the harm.

What the Keyless Primitive Provides: Eliminate the Secret

Keyless identity removes the secret that secrets-security exists to manage. When a principal proves identity by demonstrating that its present chained state legitimately follows from its validated history, there is no static secret to leak into a repository, no key to over-provision, and nothing to harvest from a captured artifact, because authentication is not the presentation of a stored secret but the demonstration of computed continuity. The entire category of failure that Entro discovers and mitigates, leaked credentials, exposed keys, secrets in code, does not arise where the unit of identity holds no secret. This is the difference between secret discovery and secret elimination: one finds and contains the secrets that exist, the other arranges for the secrets not to exist. Discovery remains valuable for the credentials that legacy systems still require, but for identities that adopt the keyless primitive, there is no secret left to discover.

Category Convergence

Entro demonstrates the scale and cost of secret-based identity, every leaked key it finds is an argument for not having the key. The keyless primitive is that argument's conclusion: eliminate the static secret as the unit of identity, and the discovery-and-rotation treadmill shortens to the legacy systems that still demand secrets. An organization can run secrets discovery over its current estate while migrating its most sensitive identities to keyless continuity, reducing the population of secrets that can leak rather than only watching it. No relationship, endorsement, or infringement is asserted; the comparison is architectural.

Disclosure Scope

The keyless identity mechanism, in which identity is a validated, append-only chain of dynamic hashes proved by computed continuity and holding no static secret to leak, rotate, or harvest, is disclosed in the identity filing (U.S. Application No. 19/388,580, published as US 2026/0126730 A1). This article compares that disclosed mechanism with Entro Security's publicly described secrets and non-human-identity discovery and positions secret elimination as the architectural complement to secret discovery. References to Entro are to public materials and are used for comparison only.

Keyless Identity (</keyless-identity>)

[All 36 steps → \(/inventive-steps\)](/inventive-steps)

Identity from accumulated continuity. Post-quantum by construction.

PRIMARY TECHNICAL DISCLOSURE

- [Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems \(/articles/stateless-device-pseudonymity-and-secure-messaging-in-cognition-native-systems\)](/articles/stateless-device-pseudonymity-and-secure-messaging-in-cognition-native-systems).

SECONDARY TECHNICAL

- [Continuity-Based Biological Identity Using Trust-Slope Validation \(/articles/continuity-based-biological-identity-using-trust-slope-validation\)](/articles/continuity-based-biological-identity-using-trust-slope-validation)
- [Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials \(/articles/keyless-identity/trust-slope-identity\)](/articles/keyless-identity/trust-slope-identity)
- [Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch \(/articles/keyless-identity/dual-source-derivation\)](/articles/keyless-identity/dual-source-derivation)
- [Stateless Symmetric Encryption: Session Keys Derived From Current Identity State \(/articles/keyless-identity/stateless-encryption\)](/articles/keyless-identity/stateless-encryption)
- [Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation \(/articles/keyless-identity/two-stage-auth\)](/articles/keyless-identity/two-stage-auth)
- [Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host \(/articles/keyless-identity/slope-entanglement\)](/articles/keyless-identity/slope-entanglement)
- [Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains \(/articles/keyless-identity/mutation-lineage-log\)](/articles/keyless-identity/mutation-lineage-log)
- [Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification \(/articles/keyless-identity/cross-substrate-validation\)](/articles/keyless-identity/cross-substrate-validation)
- [Quorum-Based Identity Recovery: Peer Attestation After Memory Loss \(/articles/keyless-identity/quorum-recovery\)](/articles/keyless-identity/quorum-recovery)
- [Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links \(/articles/keyless-identity/anchor-rotation\)](/articles/keyless-identity/anchor-rotation)
- [Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation \(/articles/keyless-identity/biometric-reseeding\)](/articles/keyless-identity/biometric-reseeding)
- [Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments \(/articles/keyless-identity/delayed-validation\)](/articles/keyless-identity/delayed-validation)
- [Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices \(/articles/keyless-identity/sparse-checkpoints\)](/articles/keyless-identity/sparse-checkpoints)
- [Predictive Identity Validation: Drift Detection Before Full Discontinuity \(/articles/keyless-identity/predictive-drift\)](/articles/keyless-identity/predictive-drift)
- [Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries \(/articles/keyless-identity/pki-fallback\)](/articles/keyless-identity/pki-fallback)
- [Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions \(/articles/keyless-identity/post-quantum\)](/articles/keyless-identity/post-quantum)
- [Continuity-Identity Processor IC: Silicon-Block Embodiment \(/articles/keyless-identity/continuity-identity-processor-ic\)](/articles/keyless-identity/continuity-identity-processor-ic)
- [Biological-Device Binding Through Continuity \(/articles/keyless-identity/biological-device-binding\)](/articles/keyless-identity/biological-device-binding)

- [Multi-Modal Biometric Continuity Coupling \(/articles/keyless-identity/multi-modal-continuity-coupling\)](/articles/keyless-identity/multi-modal-continuity-coupling).

APPLICATIONS · GENERAL

- [Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents \(/articles/keyless-identity/trust-slope-entanglement\)](/articles/keyless-identity/trust-slope-entanglement)
- [Post-Quantum Enterprise Identity Migration \(/articles/keyless-identity/post-quantum-migration\)](/articles/keyless-identity/post-quantum-migration).
- [Billions of IoT Devices Need Authentication Without Keys \(/articles/keyless-identity/iot-authentication\)](/articles/keyless-identity/iot-authentication)
- [Financial Identity Without Credential Databases \(/articles/keyless-identity/financial-identity-verification\)](/articles/keyless-identity/financial-identity-verification).
- [Patient Identity Through Behavioral Continuity \(/articles/keyless-identity/healthcare-patient-continuity\)](/articles/keyless-identity/healthcare-patient-continuity)
- [Supply Chain Authentication Without PKI \(/articles/keyless-identity/supply-chain-authentication\)](/articles/keyless-identity/supply-chain-authentication)
- [Smart Building Access Through Continuity \(/articles/keyless-identity/smart-building-access\)](/articles/keyless-identity/smart-building-access).
- [Vehicle Operator Identity Binding \(/articles/keyless-identity/vehicle-operator-identity\)](/articles/keyless-identity/vehicle-operator-identity).
- [Displaced Person Identity Without Documents \(/articles/keyless-identity/refugee-identity\)](/articles/keyless-identity/refugee-identity).
- [Component-Level Identity Licensing at the Silicon Layer \(/articles/keyless-identity/silicon-vendor-licensing\)](/articles/keyless-identity/silicon-vendor-licensing)
- [The Agent Identity Wave: Where the Whole Market Is Heading \(/articles/keyless-identity/agent-identity-convergence\)](/articles/keyless-identity/agent-identity-convergence).
- [When the Link Dies, the Identity Has to Live Onboard \(/articles/keyless-identity/drone-swarm-jammed-identity\)](/articles/keyless-identity/drone-swarm-jammed-identity).
- [Forced Off the Keys: Why the Post-Quantum Migration Points Past PKI to Keyless \(/articles/keyless-identity/post-quantum-forcing-function\)](/articles/keyless-identity/post-quantum-forcing-function).

APPLICATIONS · SPECIFIC

- [Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere. \(/articles/keyless-identity/okta\)](/articles/keyless-identity/okta).
- [Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change. \(/articles/keyless-identity/auth0\)](/articles/keyless-identity/auth0).
- [YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability. \(/articles/keyless-identity/yubico\)](/articles/keyless-identity/yubico)
- [CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It. \(/articles/keyless-identity/clear\)](/articles/keyless-identity/clear).

- [Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. \(/articles/keyless-identity/worldcoin\)](/articles/keyless-identity/worldcoin).
- [Jumio Automated ID Verification. The Verification Still Depends on Documents. \(/articles/keyless-identity/jumio\)](/articles/keyless-identity/jumio).
- [Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials. \(/articles/keyless-identity/microsoft-entra\)](/articles/keyless-identity/microsoft-entra).
- [Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets. \(/articles/keyless-identity/ping-identity\)](/articles/keyless-identity/ping-identity).
- [OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential. \(/articles/keyless-identity/onelogin\)](/articles/keyless-identity/onelogin).
- [Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential. \(/articles/keyless-identity/duo-security\)](/articles/keyless-identity/duo-security).
- [Thales HSMs Protect Key Material. The Keys Still Exist. \(/articles/keyless-identity/thales-hsm\)](/articles/keyless-identity/thales-hsm).
- [Entrust Issues Digital Certificates. The Certificate Is a Stored Credential. \(/articles/keyless-identity/entrust\)](/articles/keyless-identity/entrust).
- [DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits. \(/articles/keyless-identity/digicert\)](/articles/keyless-identity/digicert).
- [Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same. \(/articles/keyless-identity/lets-encrypt\)](/articles/keyless-identity/lets-encrypt).
- [Qorvo Secure Elements Authenticate, but Don't Track Continuity \(/articles/keyless-identity/qorvo-secure-element\)](/articles/keyless-identity/qorvo-secure-element).
- [NXP Trust Anchor Stores Keys, Not Trust Slope \(/articles/keyless-identity/nxp-trust-anchor\)](/articles/keyless-identity/nxp-trust-anchor).
- [Infineon Secure Microcontrollers Need Continuity Logic On-Die \(/articles/keyless-identity/infineon-secure-microcontroller\)](/articles/keyless-identity/infineon-secure-microcontroller).
- [Microchip Trust Platform Fits Hardware, Misses Behavioral Continuity \(/articles/keyless-identity/microchip-trust-platform\)](/articles/keyless-identity/microchip-trust-platform).
- [Indicio SSI Network and Anonymo Labs \(/articles/keyless-identity/indicio-ssi\)](/articles/keyless-identity/indicio-ssi).
- [Sovrin Foundation Self-Sovereign Identity \(/articles/keyless-identity/sovrin-foundation\)](/articles/keyless-identity/sovrin-foundation).
- [W3C Decentralized Identifiers \(DIDs\) \(/articles/keyless-identity/w3c-dids\)](/articles/keyless-identity/w3c-dids).
- [W3C Verifiable Credentials \(/articles/keyless-identity/w3c-verifiable-credentials\)](/articles/keyless-identity/w3c-verifiable-credentials).
- [Keycard: Token-Issuer IAM Reaches Toward Identity Continuity \(/articles/keyless-identity/keycard\)](/articles/keyless-identity/keycard).
- [Aembit: External Attestation Is Half the Answer \(/articles/keyless-identity/aembit\)](/articles/keyless-identity/aembit).
- [Astrix Security: Discovery and Governance Without a Substrate \(/articles/keyless-identity/astrix-security\)](/articles/keyless-identity/astrix-security).

- [Oasis Security: Non-Human Identity Governance, Externally Anchored \(/articles/keyless-identity/oasis-security\)](/articles/keyless-identity/oasis-security).
- [Token Security: NHI Catalog Without Cryptographic Continuity \(/articles/keyless-identity/token-security\)](/articles/keyless-identity/token-security).
- [Entro Security: Secret Discovery vs. Secret Elimination \(/articles/keyless-identity/entro-security\)](/articles/keyless-identity/entro-security).

[Keyless Identity overview → \(/keyless-identity\)](/keyless-identity)