Nick Clark · Published June 22, 2026 · PDF

Astrix Security: Discovery and Governance Without a Substrate

Astrix discovers and governs the service accounts, keys, tokens, and integrations that proliferate across the enterprise, flagging over-privilege, staleness, and anomalies. It makes the non-human-identity estate observable and governable. It does not change what those identities are made of.

Vendor and Product Reality

Astrix Security is a non-human identity security platform. As publicly described, it discovers the service accounts, API keys, OAuth tokens, secrets, and integrations that proliferate across an organization's SaaS and cloud estate, maps the access each holds, and governs them: flagging over-privileged or stale credentials, detecting anomalous behavior, and helping rotate or revoke what should not exist. Non-human identities now vastly outnumber human ones in most enterprises, and almost none of them are managed with the rigor applied to employee accounts; Astrix addresses that gap directly, and its prominence, including reported acquisition interest from a major networking and security vendor, reflects how seriously the market now takes the problem.

Its contribution is visibility and governance over an existing population of non-human identities. The structural question is what those identities are made of.

The Architectural Choice: A Governance Overlay

Astrix governs identities; it does not replace the primitive they are built on. The service accounts, keys, and tokens it discovers are still stored secrets issued under existing infrastructure, and Astrix sits above them as a discovery, posture, and detection layer. This is valuable and necessary, but it is an overlay on a foundation it does not change. The credentials remain static artifacts whose compromise yields access, the trust still terminates in issuers and stored keys, and the governance, however thorough, is reactive to a population of secrets that continues to exist and to be the thing attackers target. Astrix makes the secret-based estate observable and governable; it does not remove the secret as the unit of identity.

What the Keyless Primitive Provides

Keyless identity changes the foundation Astrix governs over. When a non-human identity is an append-only chain of validated dynamic hashes with a computed trust value rather than a stored key or token, much of what an overlay must discover, govern, and remediate no longer exists to be managed. There is no static secret to leak, rotate, or over-provision, because there is no static secret; standing is computed from validated history rather than granted by an issued artifact, and it decays on its own absent renewal rather than persisting as a stale credential. Discovery and governance remain useful, but they operate over identities that cannot be replayed from a captured secret and that carry their own continuity. The overlay and the primitive are complementary: governance over the credentials that remain, and elimination of the credential as the unit of identity for the rest.

Category Convergence

Astrix proves the scale of the non-human-identity problem and the market's demand to bring it under control. The keyless primitive attacks the same problem at its root by changing what a non-human identity is, so that the population an overlay must govern

shrinks rather than grows. An organization can run discovery and governance over its current estate while migrating the identities that matter most toward computed continuity, retiring stored secrets rather than perpetually managing them. 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 with a computed trust value, device entanglement, and quorum recovery, holding no static secret to discover or rotate, 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 Astrix Security's publicly described non-human-identity discovery and governance and positions the keyless primitive as a change of foundation beneath the governance overlay. References to Astrix are to public materials and are used for comparison only.

Keyless Identity (/keyless-identity)

All 36 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)

SECONDARY TECHNICAL

- 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)

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

- Post-Quantum Enterprise Identity Migration (/articles/keyless-identity/post-quantum-migration)
- Billions of IoT Devices Need Authentication Without Keys (/articles/keyless-identity/iot-authentication)
- Financial Identity Without Credential Databases (/articles/keyless-identity/financial-identity-verification)
- Patient Identity Through Behavioral Continuity (/articles/keyless-identity/healthcare-patient-continuity)
- Supply Chain Authentication Without PKI (/articles/keyless-identity/supply-chain-authentication)
- Smart Building Access Through Continuity (/articles/keyless-identity/smart-building-access)
- Vehicle Operator Identity Binding (/articles/keyless-identity/vehicle-operator-identity)
- Displaced Person Identity Without Documents (/articles/keyless-identity/refugee-identity)
- Component-Level Identity Licensing at the Silicon Layer (/articles/keyless-identity/silicon-vendor-licensing)
- The Agent Identity Wave: Where the Whole Market Is Heading (/articles/keyless-identity/agent-identity-convergence)
- When the Link Dies, the Identity Has to Live Onboard (/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)

APPLICATIONS · SPECIFIC

- Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere. (/articles/keyless-identity/okta)
- Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change. (/articles/keyless-identity/auth0)
- YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability. (/articles/keyless-identity/yubico)
- CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It. (/articles/keyless-identity/clear)
- Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. (/articles/keyless-identity/worldcoin)
- Jumio Automated ID Verification. The Verification Still Depends on Documents. (/articles/keyless-identity/jumio)
- Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials. (/articles/keyless-identity/microsoft-entra)

- Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets. (/articles/keyless-identity/ping-identity)
- OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential. (/articles/keyless-identity/onelogin)
- Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential. (/articles/keyless-identity/duo-security)
- Thales HSMs Protect Key Material. The Keys Still Exist. (/articles/keyless-identity/thales-hsm)
- Entrust Issues Digital Certificates. The Certificate Is a Stored Credential. (/articles/keyless-identity/entrust)
- DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits. (/articles/keyless-identity/digicert)
- Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same. (/articles/keyless-identity/lets-encrypt)
- Qorvo Secure Elements Authenticate, but Don't Track Continuity (/articles/keyless-identity/qorvo-secure-element)
- NXP Trust Anchor Stores Keys, Not Trust Slope (/articles/keyless-identity/nxp-trust-anchor)
- Infineon Secure Microcontrollers Need Continuity Logic On-Die (/articles/keyless-identity/infineon-secure-microcontroller)
- Microchip Trust Platform Fits Hardware, Misses Behavioral Continuity (/articles/keyless-identity/microchip-trust-platform)
- Indicio SSI Network and Anonyome Labs (/articles/keyless-identity/indicio-ssi)
- Sovrin Foundation Self-Sovereign Identity (/articles/keyless-identity/sovrin-foundation)
- W3C Decentralized Identifiers (DIDs) (/articles/keyless-identity/w3c-dids)
- W3C Verifiable Credentials (/articles/keyless-identity/w3c-verifiable-credentials)
- Keycard: Token-Issuer IAM Reaches Toward Identity Continuity (/articles/keyless-identity/keycard)
- Aembit: External Attestation Is Half the Answer (/articles/keyless-identity/aembit)
- **Astrix Security: Discovery and Governance Without a Substrate (/articles/keyless-identity/astrix-security)**
- Oasis Security: Non-Human Identity Governance, Externally Anchored (/articles/keyless-identity/oasis-security)
- Token Security: NHI Catalog Without Cryptographic Continuity (/articles/keyless-identity/token-security)
- Entro Security: Secret Discovery vs. Secret Elimination (/articles/keyless-identity/entro-security)

Keyless Identity overview → (/keyless-identity)