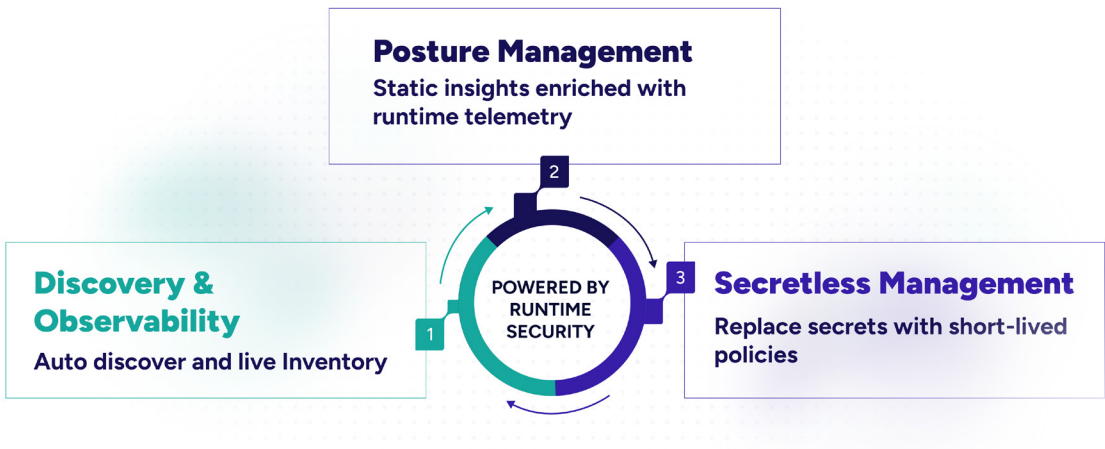


Manage Non-Human Identities in an All-New Way.

No Secrets. No Security Gaps. No Noise.

Secretless Runtime Security Platform for Any NHI.

Hush Security has developed a new standard for securing and managing workload identities and non-human identities. We enable teams to lock down access to any non-human identity with just-in-time access controls, correlating runtime and static telemetry to surface only the risks that matter. Our approach shifts from managing secrets to policy-based controls that are validated and enforced in real time.



Key capabilities

- Replace static secrets with JIT access policies
- Centralize discovery & visibility
- Secure your AI agents and LLMs
- Runtime detection and response
- Automate NHI lifecycle management
- Apply Zero Trust access built on the SPIFFE framework

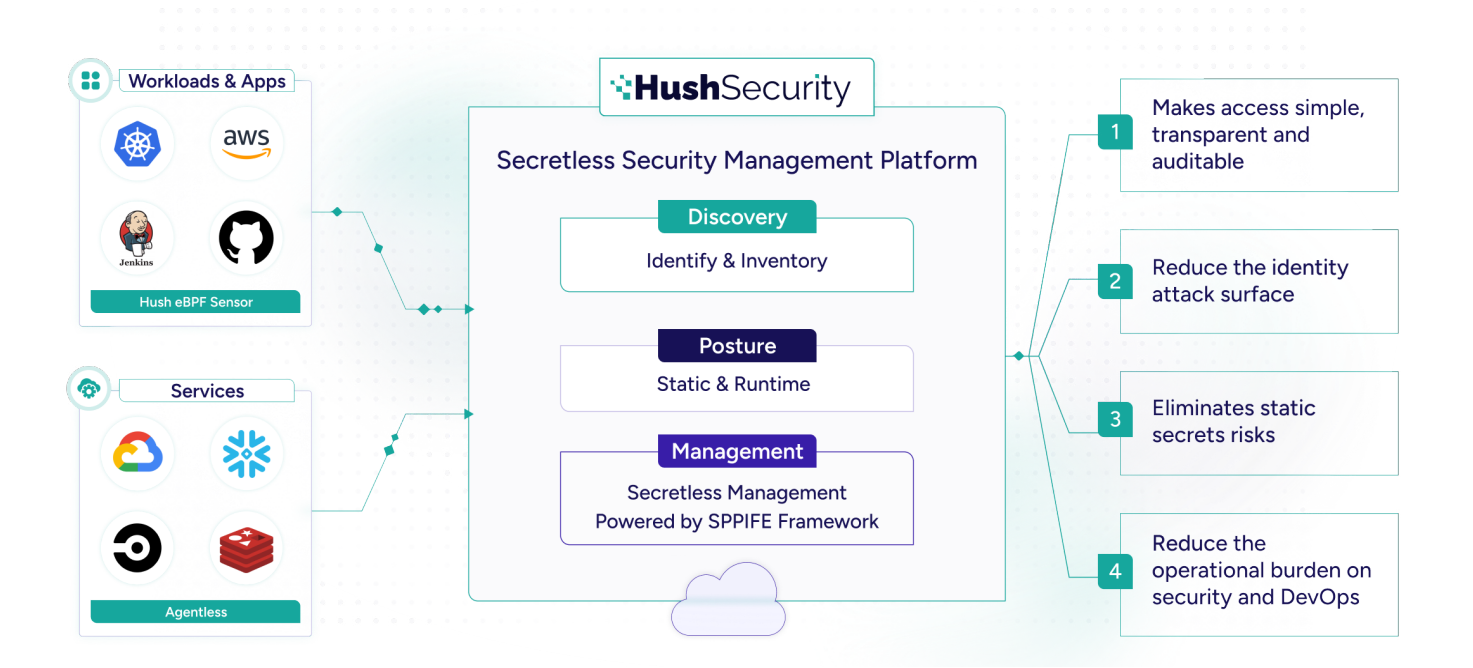
The Non Human Identity Problem is Still Unsolved.

Non-human identities (NHIs) present a growing challenge that most existing tools only partially address. Some solutions offer visibility into the NHI landscape but lack operational controls and lifecycle management. Others provide automation for identity management yet fall short on visibility and posture enforcement. Both approaches overwhelm teams with data, without offering effective ways to remediate risks at scale. Additionally, they lack runtime security and observability which leaves critical security gaps, key layers for detecting and preventing threats early in the identity lifecycle.

As a result, NHIs become difficult for IAM teams to manage and govern, error-prone for developers to implement securely, and a high-risk exposure for security teams.

How it Works?

Our solution is built on three core pillars. First, we provide real-time inventory and discovery of all secrets and NHIs. Next, we correlate this inventory with runtime telemetry, enabling teams to prioritize high-impact risks and respond to threats in real time. Finally, we enforce a secretless access model by replacing static secrets with just-in-time, policy-based access, built on the SPIFFE framework.



Our Unique Approach to NHI Security

Secretless by Design

Runtime-Aware Posture Management

Preventive Security, Not Just Detection

Unified Identity Management Across All NHIs

How Customers Use Us

Replace Static Secrets with Dynamic Polices

- Eliminate the need to manage secrets
- Apply JIT, short-lived access polices
- Apply Zero Trust architecture based on SPIFFE Framework

Automate NHIs Lifecycle Management

- No static secrets means no secrets to manage
- Eliminates long-lived credentials
- Real-time policy revocation

Secure & Monitor Access to AI agents & LLMs

- Prevent LLM hijacking by enforcing policies in runtime
- Apply secretless access to LLMs
- Monitor and govern AI-based identities

Runtime Security & Observability

- Real-Time NHI & Secret Inventory
- Unified Static & Runtime Visibility
- Context-Rich Mapping

Automate your secret migration

- Auto-discover & map all existing secrets
- Streamline migration to a unified, secretless model

Detect & Respond to NHI Threats in Runtime

- Monitor NHI behavior in runtime
- Correlate Posture with Live Activity
- Block Threats Instantly

Still Managing Secrets? Let's Fix That. Get in touch → sales@hush.security

For more information about our secretless access platform, reach out to us at sales@hush.security or visit hush.security.

