Securden

Non-Human Identity Management

Non-Human Identity Management

Reducing Exposure and Enforcing Control Over the Usage of Machine Identities

Securden's Non-Human Identity Management platform helps organizations eliminate hardcoded credentials, discover unmanaged secrets, and enforce consistent control over machine identities across DevOps pipelines, applications, and cloud environments. By centralizing visibility and governance, it reduces exposure risks and ensures secure usage of non-human identities at scale.

Overview

Non-human identities—including API keys, service accounts, tokens, and automation credentials—now outnumber human users across most enterprise environments. They are deeply embedded across CI/CD pipelines, infrastructure automation, applications, and cloud workloads.

Despite their widespread use, these identities are rarely governed with the same rigor as human access. Secrets are often hardcoded, duplicated across systems, or left unmanaged—creating significant security gaps.

Securden's platform addresses this by eliminating exposure at the source, discovering existing secrets, and bringing non-human identities under centralized governance.

The Challenge

Modern DevOps and Cloud environments rely heavily on machine identities. However, this rapid growth has led to a fragmented, difficult-to-control landscape.

Common challenges include:

- Hardcoded credentials embedded in scripts, code, and configuration files
- Secrets scattered across repositories, tools, and cloud platforms
- Long-lived and unrotated credentials increasing risk
- Lack of visibility into ownership, usage, and access patterns
- Exposure often detected only after a compromise

As a result, non-human identities have become one of the most common entry points for attackers—and one of the hardest areas to manage at scale.

A Structured Approach to Non-Human Identity Security

Securden Non-Human Identity Management focuses on reducing exposure at its source while bringing existing secrets under centralized governance.

Instead of relying solely on detection after exposure, Securden enables organizations to:

- Eliminate hardcoded credentials
- Discover and onboard existing secrets
- Enforce consistent lifecycle policies
- Establish visibility and control across environments

This approach allows organizations to progressively strengthen their security posture while maintaining alignment with DevOps workflows.

Core Capabilities

Eliminate Hardcoded Secrets

Securden integrates with DevOps tools such as Jenkins, Ansible, Chef, Puppet, and Terraform to enable secure, dynamic retrieval of secrets at runtime.

This removes the need to embed credentials in code or scripts and enforces a clear separation between code and secrets—significantly reducing exposure within CI/CD pipelines and automation workflows.

Discover and Govern Existing Secrets

Securden automatically discovers secrets across Git repositories and cloud platforms such as GitHub, Bitbucket, AWS, and Azure.

Discovered credentials are brought under centralized management, where they can be governed through rotation, access control, and policy enforcement—helping eliminate unmanaged and long-lived secrets.

Policy-Driven Lifecycle Management

Securden enables consistent enforcement of lifecycle policies across all machine identities, including:

- Automated rotation
- Expiry management
- Access restrictions

This ensures that security controls are applied uniformly without manual intervention.

Centralized Secret Vault

All non-human identity credentials are securely stored within a centralized platform, providing:

- Role-based access control
- Frequent credential rotation
- Consistent governance across environments

Exposure Monitoring (Evolving Capability)

Securden is extending its capabilities to monitor where secrets may be exposed across systems and collaboration channels.

This will provide earlier visibility into potential leaks and enable faster response as risks emerge.

Business Benefits

Organizations using Securden can:

- **Reduce risk at the source** by eliminating hardcoded credentials
- **Improve visibility** across all non-human identities and secrets
- **Enforce consistent governance** through policy-driven controls
- **Enable secure DevOps workflows** without slowing development
- **Reduce operational overhead** through automation and centralized management.

Use Cases

Securing CI/CD Pipelines

Replace hardcoded credentials in pipelines with secure runtime retrieval, ensuring secrets are never exposed in build or deployment workflows.

Managing Secrets Across Repositories

Discover and govern credentials stored in Git repositories, reducing the risk of exposed or duplicated secrets.

Controlling Cloud Credentials

Bring cloud-based secrets such as AWS keys and Azure credentials under centralized management and enforce lifecycle policies.

Improving Compliance and Audit Readiness

Maintain centralized visibility, audit trails, and consistent policy enforcement to support compliance requirements.

Crafted for Real-World Non-Human Identity Security

Securden focuses on reducing exposure at its source while enabling consistent governance across environments.

By combining prevention and lifecycle management, it provides a practical and scalable approach to securing non-human identities—without requiring changes to existing DevOps workflows or tools.

Non-human identities are now central to how modern systems operate—but remain one of the least governed areas of security.

Securden helps organizations address this gap by eliminating exposure, centralizing control, and enabling consistent governance across the lifecycle of machine identities.